

A solid teal horizontal bar.

ApeosWare Management Suite 2 Features Guide

- (1) This manual may not be edited, modified or copied in whole or part without the written consent of the publisher.
- (2) Some parts of this manual are subject to change without prior notice.
- (3) The screen shots and the illustrations in this manual are used as examples. They may differ from yours depending on the model, the software, or the OS.

Refer to "Setup Guide" for "About Manuals and Accessory Tools", "Conventions", and trademark.

Product information is provided at our Internet homepage. Visit https://www.fujifilm.com/fbglobal/eng/product/aw_manage_suite

Table of Contents

1 ApeosWare Management Suite Overview

ApeosWare Management Suite Features	9
Provided Features and Options	13
Edition	13
Feature list	13
User Type and Operation Screen	18
User Type	18
Login to ApeosWare Management Suite	20
ApeosWare Management Suite Operation Screen	21
Administrator Screen	21
Items on Pages	30
User Screen	33

2 System Settings/Server Monitoring

Settings from a Web Browser	38
Network Settings	40
Currency Settings	43
Display Settings	44
Job Log Settings	45
Temporary Folder Settings	48
Change Administrator Password	50
Service Display Order Settings	50
Control Panel Customization Settings	52
Security Settings	53
Supplies Usage Status Save Settings	54
External Terminal Settings	54
User Portal Settings	55
System Settings	56
Service Settings	58
Folder Settings	59
Notification Settings	60
System Status	60
Service Status	61
Folder Status	63
Advance Settings When Using Modern Authentication	64
Notes	65
Advance Setting When Using Login with Microsoft Entra ID	66
Set the existing Microsoft Entra ID security value group	66

Set the enterprise application	66
Add the API access permission to the enterprise application created	67
Creating Microsoft Entra Domain Services	68
Installing Certificates for Secure LDAP	69
Installing Certificates Required for Authentication (Base64)	69
Performing the settings for Microsoft Entra Domain Services	69
Advance Setting When Using Login with a QR Code	70
Using [AliPay]	70
Using [WeChat]	72
What if?	72
Rebuild Index in SQL Server	73
Impossible to send email messages when an antivirus software has been installed	74
When distributed print servers are not displayed correctly after installation	74

3 Device Management

Settings and Confirmation in a Web Browser	75
Device Group List (All Device Groups)	76
Device Group List (Details of Device Group/Sub-Device Group)	90
Device List	95
Device automatic registration settings	99
Settings of update conditions of device data	100
Device Status	100
Maintenance	104
Remaining Toner	104
Remaining Paper	105
Drum Status	106
Status Notification Settings	107
Job log collection status	109
Operation from the Device's Control Panel	112
Control Panel's Screen	112
Access to ApeosWare Management Suite from Control Panel	119
What if?	124
When user information is not updated because of registered card ID	124
When you connect IC Card Gate to a network	124
When free capacity of server HDD has become smaller	125
Cautions when using print management functions without using user management ...	125

4 User Management

Settings and Confirmation in a Web Browser	126
User Group List	128
User Group List (Details of User Groups)	131

User List (All Users)	132
User List (Details of Users)	139
Access Profile List	140
User Import List [User Import] Tab	149
User Import List [Account Import] Tab	166
User Import List [Associate User/Account] Tab	167
Domain list	169
Authentication Settings	172
Keyword Condition Policy	176
Condition	177
Supported Fonts	178
Print Policy	179
Watermark	180
Header/Footer	182
QR Code	184
FUJIFILM BI Direct Federation	185
Attribute Correspondence in Import	188
User Import	188
Account Import	192
User/Account Association Import	194
User Information Registration by Users	195
Register the card ID using the card reader connected to a PC	195
Register the card ID using the card reader connected to a device	196
Read the login QR code displayed on the device and register the external ID.	197
What if?	199
Actions to take if the network is not connected or is unstable	199
Precautions at the Time of Updating User Information to the Device	199
Change a Password of Apeos_Admin Users from the Command	199
Changing a password and property by users themselves	200

5 Cost Management

Settings and Confirmation in a Web Browser	201
Account Group List	201
Account List	204
Price Policy	211
Price Policy List (Price Policy Details)	215
Replenishment Schedule	216
Settings	219
Setting and Check from Command Line Tools	222
Overview of command line tools	222
Update of account balance	222
Check of account balance	230

Repair of recovery file	233
Cost Management Operation	235
Start Cost Management	235
Devices For Cost Management	235
When You Select an Account	235
Associate an account with a job without account specification	237
Add Favourite Accounts	237
Precautions for Cost Management Operation	237
Confirming the Accounting Result	239
Viewing the cost management report	239
Confirming the cost management report	240

6 Download Management

Settings from a Web Browser	241
Files	241
Printers	243
Administrator Information	245
Print Settings Default Value	246
Header/Footer Default Value	247
Download of File/Printer	248
Download files	248
Installation of printer drivers	249

7 Print Management and Operations

Settings and Operation from Web Browser	250
Side Menu Configuration	250
Preparations	251
Print Server List	252
Print Queue List	253
Print Rule List	258
Print Job List	260
Print Settings	261
Mode Schedule List	266
Print Operations	268
Overview of Print Operations	268
Preparation for Print	269
Perform Print Job	270
Perform Web Print	272
Perform Print E-mail	273
On Guest Print	273
Receive Notification with Popup Messenger	274

Perform Approval Print Job	277
Preparation for Approval Print	277
Operation by Approval Requester	278
Operation by Approver	278
Notes and Restrictions on Printing	280
GX Server Restrictions	280
Restrictions on Printing from iOS Devices	280
Print Application Server Configuration Restrictions	281
What if?	282
FAQ	282
What is Page Description Language?	282
Information Retrieved by Prescanning	284
Print Job Status	285
Uninstall Popup Messenger	286
Printing from Chromebook	286

8 Setting Scan and File Management Service

Settings from a Web Browser	288
Setting Items by the User with [System Manager] permission	290
What the users of File Management Service can do	300
Other Settings	302
Device and Device Group Settings	302
Device Body Settings	302
Temporary Folder Settings	302
Setting File Management Service	302
How to Operate the Device	303
Menu Window	303
Email a Scanned Document	304
Link with File Management Service	305

9 Mobile Device Settings and Operations

Preparations	309
ApeosWare Management Suite Settings	309
Install Application for a Mobile Device	309
Preparation for using an NFC tag	309
Prepare QR Code	310
Install Application to Display a File	310
Operating Mobile Device	310
Login	310
Menu Window	311
[General Feature]	311

[Service Feature]	312
[File Management Service]	313
Select a Device	314
Use ApeosWare MS Mobile 2 from Mobile App	315

10 Image Log Control

Settings and Confirmation in a Web Browser	316
Extract/Save Settings	317
Archive/Delete Settings	320
Restore Archive	321
Monitoring Start Time	323
Monitoring Pattern	324
Monitoring Settings	324
Common Settings	329
Image Log Receiving Status	330

11 Job Log Accounting/Report

Settings and Confirmation in a Web Browser	332
Report Name List	332
Accounting/Analysis Report	339
Custom Report List	341
Search Job Log	342
Search Image Log	344
Monitoring History search	350
Output items of search results	352
Calculation of Paper Reduction	356
What are “actual paper reduction” and “possible paper reduction”?	356
How Are Actual Paper Reduction and Possible Paper Reduction Calculated?	357
Calculation of Actual Paper Reduction	360
Calculation of Possible Paper Reduction	362
Converting an Account ID Value	365

12 Maintenance

Backup and Restoration	366
Overview	366
Options	369
Back up	372
Restore	373
Description and Handling of the Exit Code	374
Changing Server Information	376
Overview	376

Options	376
Execution example	380
Operation Log	388
Notes	389
Troubleshooting	390
Flow of troubleshooting	390
Using Diagnostics Utility	390
Starting Diagnostics Utility	391
Checking Connection Status	391
Checking Windows Information	396
Collecting Operation Logs	397
Outputting Detailed Logs, Changing the Log Size Limit	398
Showing Logs	398
Starting or Stopping ApeosWare Management Suite Services	399
Starting ApeosWare Management Suite Services	399
Stopping ApeosWare Management Suite Services	399

Appendix

Formats of Job Log Files (SOAP Collection)	401
Basic Structure of Job Log Files	401
Items Recorded in Job Log Files (by Service Type)	403
Details of Job Logs of Devices Corresponding to SOAP Retrieval	406
Format of Each Item	410
Details of Items	416
Formats of Job Log Files (Printer MIB Collection)	424
Basic Structure of Job Log Files	424
Format of Each Item	424
Troubleshooting for Image Log	427
Error message	427
Dealing with Image Log Troubles	432
Image log search menu is not displayed.	432
Documents processed by the device are not reflected in the image log search results.	432
Monitoring results email does not come.	433
Restore data that became an error due to hardware.	434

1 ApeosWare Management Suite Overview

ApeosWare Management Suite Features

ApeosWare Management Suite is software designed to manage multifunction devices and printers (hereinafter referred to as devices) and their users, while integratedly performing authentication, output management, and log accounting.

This section describes the system configuration and the main features of ApeosWare Management Suite.

Device Management

Creates device groups and register the devices to be monitored. You have to specify how to authenticate for each device group. You can also set information in Address Book and Folder to the devices, and monitors and configures the device security settings.

In addition, monitors the devices and displays current status and meter information to the web browser. You can set the feature so as to notify the administrator by email if an error occurs.



Refer

"3 Device Management" (P.75)

User Management

Register and manage the users who use devices. You can directly register user's information, moreover, automatically register it by loading the file in the external or the authentication server, such as Active Directory.

User information in ApeosWare Management Suite can be used to create FUJIFILM BI Direct user accounts.

The user who is allowed to register the user information by him/herself can register the card ID (PAN) by reading the card into the IC card reader.



Refer

- "4 User Management" (P.126)
- "User Information Registration by Users" (P.195)

Cost Management

Allows managing the scan and the output by a user by converting the amount of the device used into money.

Setting an output limit and a discount schedule allows you to comprehensively reduce the operating costs. You can categorize and tally the costs by business project or by section, and output the accounting report to issue billing statements.



Refer

"5 Cost Management" (P.201)

Download Management

Manages the files of printers and software to distribute to users.

Users can download or automatically install files such as printer drivers or installers, which the administrator added, on the users' PC.



Note

This feature is supported by only devices used in Japan. The downloaded printer drivers and files are supported by only Japanese OS.



Refer

"6 Download Management" (P.241)

Print Management

Manages the whole printing features, such as print queue registration and print job operation.

You can configure print environment suitable for various situations, such as Print On Demand, Web Print, Guest Print and Output Limit Print.

Using Popup Messenger, an accessory tool, allows informing client PCs of the print job acceptance results by Popup.



Refer

"7 Print Management and Operations" (P.250)

Link Scan Settings with File Management Service

Provides a simple flow processing and sending scanned documents. You can send scanned documents attaching to email, store it in Shared Folder and deliver it File Management Service linking with the device.

Enabled you to print the file stored in File Management Service or Shared Folder accessing from the control panel of the device.



Refer

"8 Setting Scan and File Management Service" (P.288)

Operating Mobile Device

Performs ApeosWare Management Suite features using a mobile device.

Prints the file inside the mobile device with the device managed by ApeosWare Management Suite, and uploads documents, linking with File Management Service.



Refer

"9 Mobile Device Settings and Operations" (P.309)

Image Log Control

Stores images processed by devices, searches them according to need, and monitors them based on conditions.

Later learns what information is handled when by whom on devices used in offices, etc.

Periodically monitors documents processed by devices, and when documents that contain the keyword specified in advance are found, notifies them by e-mail.



Refer

"10 Image Log Control" (P.316)

Accounting report creation

Creates accounting sheets and graphs by using the job log collected. You can create accounting reports by user or by device. Moreover, create graphs of power consumption and paper consumption, and analysis reports.

Moreover, tallies job logs using Job Log Analyzer, an accessory tool. Job Log Analyzer is a macro program of Excel which creates an accounting report and a graph tallying job logs. Graphs and lists are prepared in advance, accounted from various categories such as per user, organization, and device.



Refer

- "11 Job Log Accounting/Report" (P.332)
- "Job Log Analyzer User Guide"

Job Logs Management

Collects job logs from the device at a specified interval and stores the job logs collected as a file.

You can set it so as to notify the administrator by email if an error occurs in collecting job logs.



Refer

"Job Log Settings" in "Installation and Operation Guide"

Server Monitoring

Monitors service operation and usage of a storage on the server, and displays the latest situation on the web server. When an error occurs, records it on the event log and notifies it to the administrator by email.



Refer

"Server Monitoring" in "Installation and Operation Guide"

Document Distribution by Flow

Processes, delivers, outputs and stores automatically the document which is scanned by multifunction device, are received by fax or are on the server.

You can process the images, convert the format and process the OCR of a document loaded. You can change the storing location and the destination by the unique information to the document or the time to be accepted.



Note

Flow Management Option is required to use this feature.



Refer

"Features Guide Flow Management Option"

Updates Software

Update Service, an accessory tool, updates the software of ApeosWare Management Suite and applies patches for errors.

Update Service is the tool that starts automatically once the PC has been started, checking the software installed in the PC, updates it automatically.



Refer

- How to set the tool → "Setup Guide"
- More information on how to operate" → "Help for Accessory Tools"

Accessory Tools

ApeosWare Management Suite provides the following accessory tools.

Diagnostics Utility (Diagnostics Utility)

Diagnostics Utility is a tool that checks the connection between the PC and the servers, and collects operation logs and Windows information. You can use it on the ApeosWare Management Suite server and the client PC for diagnosing the system and solving troubles.

Diagnostics Utility enables you to diagnose the error and retrieve the log when an error occurs.



Refer

"12 Maintenance" (P.366)

Data Input Console (Data Input Console)

Data Input Console is a batch registration tool reading information of the device and the print queue from the CSV format file.

Use the feature to initialize ApeosWare Management Suite, or register or update a large volume of information.



Refer

- How to start the tool → "Setup Guide"
- More information on how to operate → "Help for Accessory Tools"

Provided Features and Options

This section describes the provided features and options of ApeosWare Management Suite.

Edition

ApeosWare Management Suite has two following editions.

- Entry Edition

It is the edition packaged basic features.

- Enterprise Edition

It is the edition that is added some features to Entry Edition.



Note

You are not allowed to upgrade from Entry Edition to Enterprise Edition.

Feature list

Available features of each edition are as follow.

○: Can be used as standard.

△: Can be used when an option license (sold separately) is added.

×: Not Available

Features	Entry Edition	Enterprise Edition	Options Can Be Added
Server Configuration			
All-in-One Configuration	○	○	
Server Multiplexing Configuration	×	○	
Distributed Configuration	○	○	
Device Management ^{*1}			
Device and Device Group Management	○	○	
Device Auto Registration	○	○	
Device Data Update	○	○	
Displaying Device Status/Meter Information	○	○	
Status Notification Settings	○	○	
Displaying Job Log Collection Status	○	○	

Features	Entry Edition	Enterprise Edition	Options Can Be Added
User Management			
User and User Group Management	○	○	
Access Profile Settings	○	○	
Link to Remote Authentication Server (Domain)	○	○	
Import User	○	○	
Import Account	△	○	Cost Recovery Option
Authentication Settings	○	○	
FUJIFILM BI Direct Federation  Note This feature is only available in Japan.	○	○	
Keyword Condition Policy Settings  Note This feature is not available in some countries and regions. For details, contact our dealers.	△	△	
Print Policy Settings	○	○	
User Data Registration	○	○	
Cost Management			
Account Management	△	○	Cost Recovery Option
Create Price Policy	△	○	Cost Recovery Option
Replenishment Schedule Settings	△	○	Cost Recovery Option
Download Management (Japanese OS only)			
Printer Driver Distribution	○	○	
Software Distribution	○	○	

Features	Entry Edition	Enterprise Edition	Options Can Be Added
Print Management			
Print Server Management	○	○	
Direct Print	○	○	
Guest Print (E-mail/Web Print)	△	○	
Print On Demand	△	○	On Demand Print Option
Cost Management Print	△	○	Cost Recovery Option
Approval Print  Note This feature is not available in some countries and regions. For details, contact our dealers.	△	△	
Auto Masking  Note This feature is not available in some countries and regions. For details, contact our dealers.	△	△	
Print Rule Settings	○	○	
Print Job Operation	○	○	
Popup Messenger (Popup Messenger)	○	○	
Extension of analysis method of print jobs	△	△	Additional OS Parser Option
On Demand Terminal  Note This feature is only available in Japan.	△	△	On Demand Print Terminal, Cost Recovery Option
Scan Settings			
Scan Settings	○	○	
OCR processing for scan documents	○	○	
Bar code processing for scan documents	△	△	OmniPage Barcode Reader Option

Features	Entry Edition	Enterprise Edition	Options Can Be Added
Link with File Management Service			
Link with Shared Folder/FTP server	○	○	
Link with Google™ Drive	○	○	
Link with DocuShare*2	△	△	Scan & Connect for DocuShare Device License
Linking with Microsoft® SharePoint® Server*2	△	△	Scan & Connect for SharePoint Services Device License
Link with Salesforce*2	△	△	Scan & Connect for Salesforce Services Device License
Link with OneDrive®*2	△	△	Scan & Connect for OneDrive Device License
Link with SharePoint Online*2	△	△	Scan & Connect for SharePoint Online Device License
Link with ABBYY® FlexiCapture®*2 *4	△	△	Scan & Connect for ABBYY FlexiCapture Device License
Image Log Control			
Image Log Reception	△	△	ApeosWare Management Suite 2 Image Log Management Option Receiving Server License
Image Log OCR	△	△	Any of the following licenses • ApeosWare Management Suite 2 Image Log Management Option OCR License • ApeosWare Management Suite 2 Image Log Management Option OCR CJKE Thai License • ApeosWare Management Suite 2 Scan OCR Option
Image Log Control	△	△	ApeosWare Management Suite 2 Image Log Management Option Registering Server License
Operating Mobile Device			
Print from Mobile Device	○	○	
Upload/Download from Mobile Device	○	○	
Accounting report creation			
Accounting/analysis report creation	○	○	
Cost management report creation	△	○	Cost Recovery Option
Job Log Analyzer	○	○	
Job Logs Management			
Collecting Job Logs	○	○	
Job Log Settings	○	○	

Features	Entry Edition	Enterprise Edition	Options Can Be Added
Server Monitoring			
Server Monitoring Feature	○	○	
Notification Settings	○	○	
Displaying Service Status/Folder Status	○	○	
Document Distribution by Flow			
Flow Management and Execution	△	△	Flow Management Option
OCR (only Japanese OS)	△	△	OCR for DocuWorks Japanese Option
OCR (only English OS)	△	△	OCR for DocuWorks English Option
OCR (only Chinese/Korean/Thai OS)	△	△	OCR for DocuWorks Multi Language Option
OmniPage OCR	△	△	Scan OCR Option ^{*3}
OmniPage Barcode Reader	△	△	OmniPage Barcode Reader Option
QR Code Reader	△	△	Paper Form & QR Option
Form Analysis	△	△	Paper Form & QR Option
Attribute Processing (only Japanese OS)	△	△	Attribute Processing Option
Database Query (only Japanese OS)	△	△	Database Query Option

*1 To register devices to ApeosWare Management Suite, "{Number of units of devices to register} Device License" is required to be authenticated with License Activator in advance.

*2 Licenses for the number of devices to connect to File Management Service simultaneously are required.

*3 When OmniPage OCR feature is used in the distributed configuration with a separated flow server, Scan OCR Option is required in the flow server side. If not operated in the distributed configuration, it is included in Flow Management Option.

*4 Link with ABBYY FlexiCapture is available only on the devices of FUJIFILM Business Innovation.

User Type and Operation Screen

This section describes user types operating ApeosWare Management Suite and the operation screens.

User Type

Apeos_Admin User

Installing ApeosWare Management Suite causes a built-in user to be created with the name as shown below.

User ID	Apeos_Admin
Password	FujiFilm_11111

A password is case sensitive. The User ID is not case sensitive.

This user is hereinafter referred to as "Apeos_Admin User".



Note

- Be sure to change the Apeos_Admin User password before operating for the first time. For the method to change password, refer to "Change Administrator Password" (P.50).
- When you update from a version ApeosWare Management Suite 2.0 or later to ApeosWare Management Suite 2.2, the password remains the same as with the password before the update. The default password is "FujiXerox_11111".

The following are characteristic of Apeos_Admin User.

- Can set the features by accessing all the pages of the administrator screen of ApeosWare Management Suite. Logging in to ApeosWare Management Suite brings the user to the portal page on the administrator screen.
- Accessing the user screen of ApeosWare Management Suite is not permitted.
- Has browse permission to the reports. Accessing the [Report] page allows creating and managing the reports.
- Apeos_Admin Users are not displayed on the user list, nor are they even if they are searched.
- Changing and deleting Apeos_Admin User properties are unable.
- Does not have Device Permissions.



Refer

Administrator Screen→"User Type and Operation Screen" (P.18)

Access Permissions to the Operation Screen

The users other than Apeos_Admin users are allowed to access to each screen by setting the permissions.

The following are the types of Permissions. You can set multiple types of Permissions per person.

If a user who has multiple administrator permissions logs in to ApeosWare Management Suite, the page to be displayed is determined by the "priority order" as shown below.

Permissions	Descriptions	Pages to Be Displayed After Logging in	Priority Order
System Management	Includes all the permissions for [User Management], [Account/Balance Management], [Guest Job Management] and [Device Management]. Enables you to access all the pages except [Report] on the administrator screen and set the features.  Note System Manager permissions include the system management permissions of Flow Management Option.	The portal page on the administrator screen	1
View and edit report	Enables you to aggregate the job logs collected from the device and create the report by accessing the page to manage reports.	[Report] page on the administrator screen	2
Guest Job Management	Enables you to operate a job by accessing the pages related to the print job and the scan job.	The [Print Job List] page on the administrator screen	3
Account/Balance Management	Enables you to add an account and update the balance by accessing the page to manage the account.	The [Account List] page on the administrator screen	4
User Management	Enables you to add, update and delete a user by accessing the page to manage users.	The [User List] page on the administrator screen	5
Device Management	Enables you to add, update and delete a user by accessing the page to manage users.	The [Device List] page on the administrator screen	6
Image Log Control	Enables you to set and check image logs.	[Image Log Control] page on the administrator screen	7
Image Log Search/Monitoring	Enables you to search and monitor image logs.	[Monitoring Settings] page on the administrator screen	8
Access to User Portal	Enables the user to handle the user information and the logs by him/herself by accessing the page to the user screen.	The portal page of the user screen	9
On Demand Print Terminal Management	Enables the user to change the print mode temporarily with the terminal for On Demand Print Terminal.  Note The users set only this permission cannot log in to the operation screen of ApeosWare Management Suite.	-	10



- Administrator Screen, , User Screen → "ApeosWare Management Suite Operation Screen" (P.21)
- "Operation Permission in Flow Management" in "Features Guide Flow Management Option"
- The terminal for On Demand Print Terminal → "Features Guide On Demand Print Terminal"

Login to ApeosWare Management Suite

This section describes how to log in to ApeosWare Management Suite.

1. Configure the following at the web browser.

- Bypass proxy server
- Enable JavaScript™

2. Perform the following steps.

■ For ApeosWare Management Suite server

Select [FUJIFILM ApeosWare Management Suite] > [Admin Portal Mega Menu] on Startup menu in Windows program.

■ For a client PC

(1) Start the web browser.

(2) Enter the following URL into the address bar.

`http://{Host name}/Login`

- Enter the host name or the IP address of ApeosWare Management Suite server in {Host name}.
- Specify “https” for SSL communication.
- If the port number was changed from the default value when the server was installed, enter a colon (:) and the port number after {Host name}.
- This is case sensitive.



Note

- When accessing by SSL communication, enter the name that corresponds with the common name (CN) on the SSL certificate in {Host name}.
- When using Microsoft Entra ID, the URL to be entered is as described below.
`http://{Host name}/Login/MicrosoftEntraID?MicrosoftEntraID={DNS domain name}`
 - Enter the host name of the ApeosWare Management Suite server in {Host name}.
 - Enter the domain name set in [Service Settings] > [User Management] > [Domains] > [Create Domain] in {DNS domain name}. However, if [Different from Microsoft Entra ID] was checkmarked when creating the domain, input the “Microsoft Entra ID domain.”

3. Enter the user information and log in.

A page according to the user’s permission is displayed.



Note

- A user with system administrator permission is created automatically when ApeosWare Management Suite is installed. Enter this user information for the first login.
For details of the user set by default, refer to “Apeos_Admin User” (P.18)
- When logging in with the Microsoft Entra ID, click [Login with MS] and enter the authentication information. However it is necessary that users used in login must be associated with the enterprise application created in advance.



Refer

- “Access Permissions to the Operation Screen” (P.18)
- “Set the enterprise application” (P.66)

ApeosWare Management Suite Operation Screen

There are two types of the operation screen, “administrator screen” and “user screen”.

Administrator Screen

Administrator Portal

It is displayed when a user who has administrator permission logs in. Allows doing the settings and operating the jobs of the whole system.

In ApeosWare Management Suite, operate the menu or side menu and display a page to configure items.



Note

Displayed menu differs depending on the license and administrator’s permission. The screens shown below indicate the state where Apeos_Admin user or a system administrator is logged in. For other administrators, only the items allowed to the role will be displayed.



Refer

About administrator→“User Type” (P.18)

Menu

Side menu

The screenshot displays the Administrator Portal interface. The top navigation bar includes 'Portal', 'Report', 'Device/Job Status', 'Service Settings', and 'System Settings'. The left sidebar, labeled 'Side menu', contains 'Basic Settings' (with 'Easy Settings' sub-item), 'Frequently Used Settings' (with 'Device Registration' and 'User Registration' sub-items), and 'System Information'. The main content area, labeled 'Menu', shows 'Device Status' for 05/12/2022 10:07 am. It includes a table with columns 'Type' and 'Status' for various device components: Device Failure (OK), Print Job (no job), Job Error (operating normally), Toner (needs replacement), Paper (needs loading), and Drum (needs reordering). The 'System Information' panel on the right shows 'FUJIFILM Business Innovation' notices, license information (warning: needs activation within 24 days), and service status (1 error, 0 attention, 1 unknown, 7 OK).

The following functions can be selected from the side menu of Administrator Portal.

Side menu	Descriptions
Basic settings	Allows easy settings of ApeosWare Management Suite. However, there are the following restrictions. • Device authentication mode: Local authentication will be selected. • Device group to which the device belongs: InitialDeviceGroup will be specified. User group to which the user belongs: Default Group will be specified. • The shared folder you specified will be specified as the forwarding destination of scanned files. • Access profile: This can only be selected from among the previously provided access profiles. It is also possible to associate to all the devices registered.  Refer Access Profile⇒“Access Profile List” (P.26)
Easy Settings	Display the menu for basic settings.
Frequently Used Settings	
Device Registration	Shortcut to [Device List].
User Registration	Shortcut to [Users (All Users)].

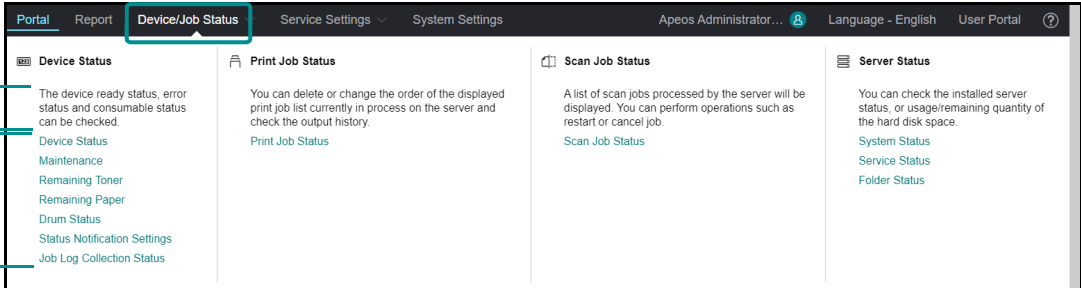
The following information is displayed at the right side area of Administrator Portal. Click the links on the message to display each detailed page.

Device Status	Display the status of the registered devices.
System Information	Latest number of announcements from us, the license status, and service status are displayed.
Usage Status	The device usage is displayed with a graph or chart.

[Administrator Portal] menu

Hovering a cursor over the [Device/Job Status] and [Service Settings] menu will display the description of each function and links. Select a function to configure.

Select a function of [Device/Job Status] menu to configure.



The screenshot shows the Administrator Portal interface. The 'Device/Job Status' menu is expanded, showing four sub-menus: Device Status, Print Job Status, Scan Job Status, and Server Status. Each sub-menu has a description and a link to a detailed page. The 'Device Status' sub-menu is highlighted with a red box. To the left of the menu, there are two labels: 'Descriptions' and 'Link', each with a red bracket pointing to the corresponding part of the menu items.

Select a function of [Service Settings] menu to configure

Descriptions

Link

Clicking the [Report] or [System Settings] menu will display each top page. From the side menu of the top page, select a function to configure.

The following charts show items that are possible to operate in each menu.

[Report] menu

Side menu	Descriptions
Report Name	
User/User Group	Creates reports on the paper usage and the price by user or user group.
Account Report	Creates reports on the paper usage and the price by account or cost center code.
Device/device groups	Creates reports on the paper usage and the price by device or device group.
Sustainability Reports	Creates each reports that compile from the environment's point such as the analyzing reports displayed the reducing amount for papers or the possibility amount for paper reducing, summary reports displayed the rate of reduction for CO2 or power consumption, and graphs displayed power consumption of devices.
Print Report	Creates print job reports by job origin or application.
Fax Report	Only the job data related to fax communication is extracted from the job log, and downloaded as a CSV format file.
Image Log Monitoring Report ^{*1}	Creates reports on the image log summary by user or user group. Displayed only when the image log feature is enabled.
Approval Print History	Creates reports of keyword search history and operation history of Approval Print. Displayed only when the Approval Print feature is enabled.
 Note This feature is not available in some countries and regions. For details, contact our dealers.	
Accounting/Analysis Report	Creates the report by setting Accounting Conditions and Display Items of Accounting List Report, Accounting Graph Report, and Analysis List Report.
Supplies Report	Creates reports of toner, drum, and meter information.

Side menu	Descriptions
Custom Report	
Custom Report List	Create reports by specifying job type, period and format.
Extended Report	
Search Job Log	Searches job logs by specifying search conditions such as device, user, and date and time.
Search Image Log ^{*1}	Searches image logs by specifying conditions such as device, user, and date and time.
Monitoring History ^{*1}	Searches image logs based on Monitor Settings.

*1 These items are displayed only when Image Log Management Option license is authenticated.

[Device/Job Status] menu

Description/Link	Descriptions
Device Status	
Device Status	Displays errors with registered devices and the state of consumables.
Maintenance	Executes the meter information of the device and turns it off.
Remaining Toner	Checks the remaining toner of a device.
Remaining Paper	Checks the remaining paper of a device.
Drum Status	Checks the drum status of a device.
Status Notification Settings	Configures the condition for device status that are notified by e-mail.
Job log collection status	Job log collecting status is displayed.
Print Job Status	
Print Job Status	Displays the status of print job executed by all users. Allows you to hold release for the print job and cancel it.
Scan Job Status	
Scan Job Status	Displays the status of scan job executed by all users. Allows you to restart for the scan job and cancel it.
Server Status	
System Status	Displays the use status of the CPU and memory of the main server and separation server.
Service Status	Displays the availability status of the service to be monitored.
Folder Status	Displays the status of disk capacity of the folder.
Image Log Status ^{*1}	
Image Log Receiving Status	Displays the reception status of image logs.

*1 These items are displayed only when Image Log Management Option license is authenticated.

[Service Settings] menu

Description/Link	Descriptions
Device Management	
Device Groups	Creates, deletes, displays the property and reflects to the devices for device groups and sub-device groups. Device group is a group to manage the devices authentication/the totaling settings, the communication settings, the panel settings, and the registration data (the destination addresses or the boxes).
Device List	Registers and deletes devices, and displays the properties.
Settings - Device automatic registration settings	Configures the schedule to automatically search for devices on the network and register them.
Settings - Settings of update conditions of device data	Configures the interval or the time at which the settings are reflected to devices.
Download Management ^{*1}	
Files ^{*1}	Adds and deletes the files or folders that distribute to the users.
Printers ^{*1}	Adds and deletes print settings (the color mode or the screen settings) for the print driver which distributes to the users.
Settings ^{*1}	Configures the default for print settings or administrator information that allow the general users to execute.
Scan Settings	
Email Settings	Configures the E-mail address to send scanned data.
Common Settings	Configures the settings for scanning.
File Management Service Settings	
Shared Folder Settings	Configures to link with Shared Folder in Windows.
DocuShare Settings ^{*2}	Sets the settings to link with DocuShare. DocuShare is web-based file management and utilization software achieving effective use of information assets.
SharePoint Settings ^{*2}	Sets the settings to link with SharePoint®. SharePoint is a file management service provided by Microsoft Corporation.
Salesforce Settings ^{*2}	Sets the settings to link with Salesforce. Salesforce is a cloud service provided by salesforce.com Co., Ltd.
Google Drive Settings	Configures to link with Google Drive. Google Drive is an on-line storage provided by Google Inc.
OneDrive Settings ^{*2}	Configures to link with OneDrive®. OneDrive is a file management service provided by Microsoft Corporation. As for OneDrive, only OneDrive for Business is targeted.
SharePoint Online Settings ^{*2}	Configures to link with SharePoint® Online. SharePoint Online is a file management service provided by Microsoft Corporation.
ABBYY FlexiCapture Settings ^{*2}	Configures to link with ABBYY FlexiCapture. ABBYY FlexiCapture is document processing software provided by ABBYY.

Description/Link	Descriptions
Cost Management	
Account Groups	Creates, copies and deletes account groups, and displays the properties. Configures when Account Group associates same price policy and replenishment schedule with the account.
Accounts	Creates, copies and deletes accounts, and displays the properties. The accounts manage the usage of copy and print in monetary amounts.
Price Policy	Creates, copies and deletes price policies, and displays the properties. For price policy, configures the information such as the cost for each service on devices, time discounts and premiums.
Replenishment Schedule	Creates, copies and deletes replenishment schedules, and displays the properties. For replenishment schedule, configures the schedules for balance replenishment and reset.
Settings	Configures the calculating system for the charge or the notice when the balance is a few.
User Management	
User Group List	Creates, copies and deletes user and sub-user groups, and displays the properties. User Group can be associated with the account.
Users	Creates and deletes users, displays the properties, switches a valid/invalid state, and releases the lock.
Access Profile List	Creates, copies and deletes access profiles, and displays the properties. For access profile, configures the function and the operation that the user can use such as the permission for using the function, the display screen for login, the access to the file management service, the load limitation for the cost management and the access to the user portal.
User Import List	Creates, copies and deletes imports, and displays the properties. Configures how to import user and the schedule when importing the user and the account information from the external authentication servers.
Domains	Creates and deletes domains, displays the properties, and changes the priority of authentication. Configures the import-source domain when importing user information from the Active Directory, LDAP, or Microsoft Entra Domain Services (Microsoft Entra ID DS) server by [User Import].
Authentication Settings	Configures the authentication-related functions.
 Note This feature is only available in Japan.	Configure the settings to use single sign-on authentication for FUJIFILM BI Direct.
 Note This feature is not available in some countries and regions. For details, contact our dealers.	Displays a list of registered keyword condition policies.

Description/Link	Descriptions
Condition  Note This feature is not available in some countries and regions. For details, contact our dealers.	Displays a list of registered conditions and adds and deletes conditions.
Supported Fonts  Note This feature is not available in some countries and regions. For details, contact our dealers.	Displays a list of supported fonts and adds and deletes fonts.
Print Policy	Displays a list of registered print policies and adds and deletes policies.
Watermark	Displays a list of registered watermarks and adds and deletes watermarks.
Header/Footer	Displays a list of registered headers/footers and adds and deletes headers/footers.
QR Code	Displays a list of registered QR codes and adds and deletes QR codes.
Print Management	
Print Queue List	Creates and deletes print queues, and displays the properties.
Print Job List	Displays the status of print job executed by all users. Allows you to hold release for the print job and cancel it. This function is same as [Print Job Status] in [Device/Job Status] menu.
Print Rule List	Creates, copies and deletes print rules, and displays the properties. The Print rule is set to the print queue. According to configure print rules, it is possible to print by the same settings.
Print Settings	Configures guest print, mail print, print job and on-demand print.
Print Server List	Adds and deletes print servers, and displays the properties. Print server is a server installed a print management function. Separating main server and print server is possible.
Mode Schedule List	Creates and deletes print mode schedule, and displays the properties. For print mode schedule, configures print mode in print queue for the automatically switching schedule by the time period.
Server Monitoring Settings	
Notification Settings	Configures the notification when the abnormalities occurs in the server service and the notification to E-mail address.
Monitor Settings	Configures the service to monitor.

Description/Link	Descriptions
Flow Management ^{*3}	
Flow List ^{*3}	Displays the list of flow configured by [Owner] who logs in as users. Creating new flows and verifying, editing, activating, deactivating, deleting, downloading and uploading flows are possible. However, when logs in by Apeos_Admin user, displays all flows.
Job List ^{*3}	Displays the list of flow job configured by the job owner who logs in as users. Preferentially executing, suspending, reexecuting and deleting jobs are possible. However, when logs in by Apeos_Admin user, displays all jobs.
Suspended Job List ^{*3}	Displays the list of suspended operation job configured by the job owner who logs in as users. Referring, resuming and deleting jobs are possible. However, when logs in by Apeos_Admin user, displays all suspended operation jobs.
Service Settings ^{*3}	Configures the operating environment of flows such as the flow creator and the processing of the prohibition format.
Image Log Control ^{*4}	
Extract/Save Settings	Configures OCR settings of extract processing and encryption and compression of save processing.
Archive/Delete Settings	Configures the save period of image logs and image log processing method after the save period is ended.
Restore Archive	Restores data archived after the image log retention period is expired as search targets.
Image Log Monitoring Setting	Configures to monitor image logs.
Common Settings	Makes common settings of image logs.

*1 These items correspond to Japanese devices. Downloaded printer driver and files only correspond to Japanese OS.

*2 Optional. These items are displayed when the license is authenticated.

*3 These items are displayed when Flow Management Option license is authenticated.

*4 These items are displayed only when Image Log Management Option license is authenticated.

[System Settings] menu

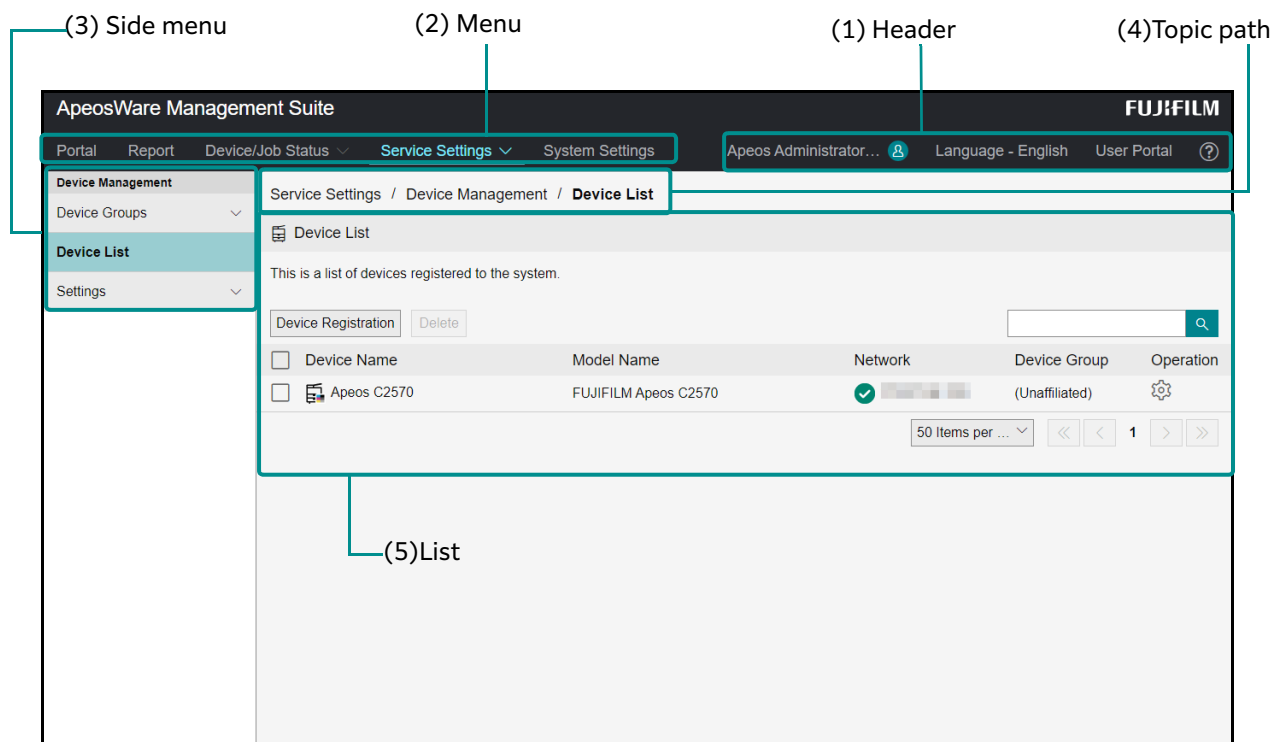
Side menu	Descriptions
Common Settings	
Network Settings	Configures the items for network settings to be used commonly in each service.
Currency Settings	Configures the kind of currency and the number of decimal places. This is used when configuring the fee structure.
Display Settings	Sets the display order of last name and first name of a user name that will be displayed in the Administrator Screen, User Screen, and Device Control Panel.
Job Log Settings	Configures the items about whether to save job logs, the retention period and accounting.
Temporary Folder Settings	Configures a temporary folder for data passing to and from the devices for the scan and mobile services.
Change Administrator Password	You can change an Apeos_Admin user's password.
Service Display Order Settings	The display order of services on the device panel will be set.
Security Settings	Sets the encryption method of print data on the print server.
Control Panel Customization Settings	Executes Control Panel Customization Settings of the devices.
Supplies Usage Status Save Settings	Sets conditions to save the supplies usage status.
External Terminal Settings	Sets the port numbers of the connected external terminals.
 Note This feature is not available in some countries and regions. For details, contact our dealers.	
User Portal Settings	Sets the reports to be displayed on the user portal.
System Information	
Notices	Displays the list of announcements from us mainly intended for administrators.
License Information	Displays the license authentication information of the installed product.

Items on Pages

List Page

This page is selected from between the [Report], the [Device/Job Status] and the [Service Settings] menu.

The [Device List] shown below can be displayed when you select [Service Settings] > [Device List].

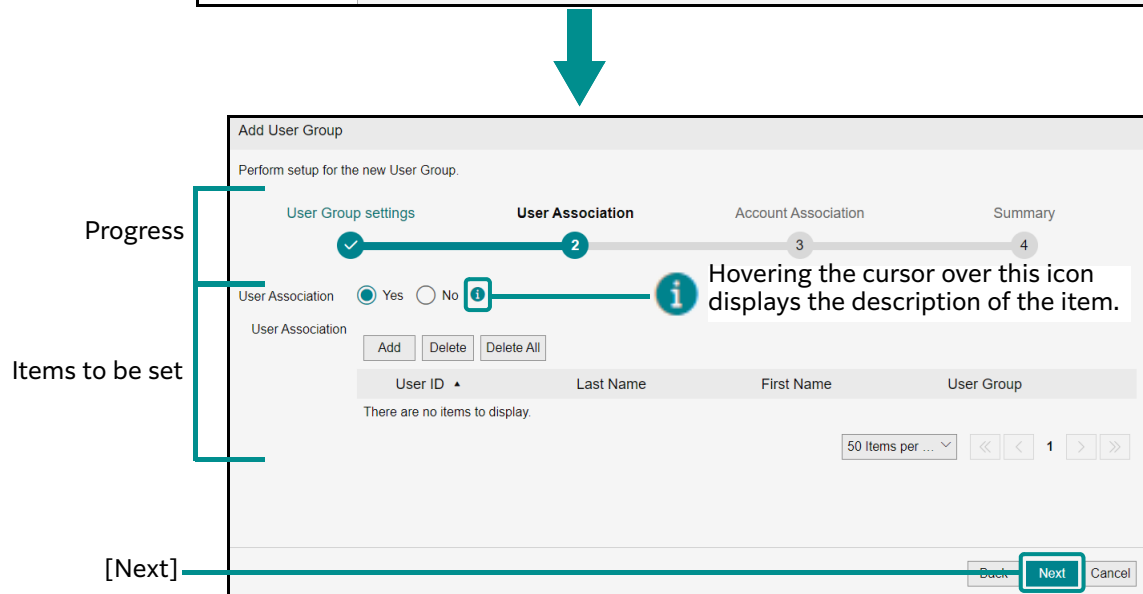
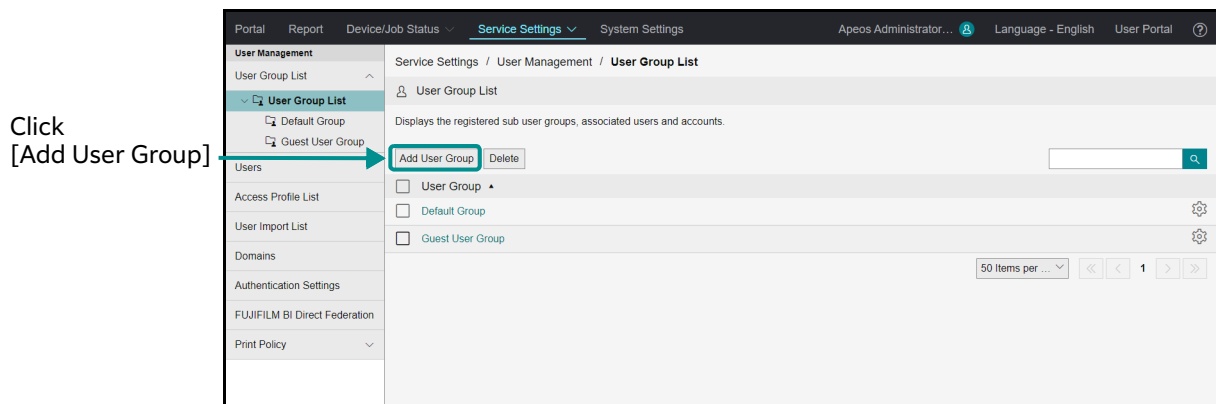


Items	Descriptions
(1) Header	
[Log out]	Logs out.
[Language-]	Changes languages. Changing a language causes a portal page to appear.  Refer "Access Permissions to the Operation Screen" (P.18)
[User Portal]	When the access to user portal by the access profile is permitted, a "[Portal] menu" (P.33) for the user is displayed on another tab on the web browser.
[Help]	The following can be displayed. • ApeosWare Management Suite Product Information • Frequently asked questions • Instruction manuals • Version information
(2) Menu	 Refer • "Administrator Portal" (P.21) • "[Administrator Portal] menu" (P.22)
(3) Side menu	
(4) Topic path	The hierarchy is displayed. If there are links, click one to move to another tier.
(5) List	A list of the items selected on the side menu is displayed. Click the Create button to display the creation page "Creation Page" (P.31). Click the  icon on the right end of an item to display, copy or delete its properties.

Creation Page

This page is displayed by clicking the creation button on the list page.

Clicking the [User Group List] button on the [User Group List] page causes the [Add User Group] below to appear.



Specify items and click [Next] to proceed to the next page.

Progress of the creation is displayed on the top of the page.

On the [User Association] page, associate a user with User Group. You also associate the account, device, etc. by the same operation.

Click [Add]

List of users to associate

[Add] or [Add All]

When removing a user from the list, place a check mark in the checkbox on the list, and then click [Delete].

[Next]

When reaching to the [Summary] page at the last, the specified information is displayed. After confirming, click [Save]. The user group is set in ApeosWare Management Suite.

Items that have been set

[Save]

User Screen

It is displayed when the user having the administrator authority clicks [User Portal] on the header menu on the Administrator Screen. Also, when a user who is granted an access right only to [User Portal] logs in, the same screen appears.

For users who belong to Guest User Group, you can use the [Access to User Portal] settings to set the Web Print-dedicated screen as the user login screen.

On the User Screen, you can operate your own job or change user properties, such as password.

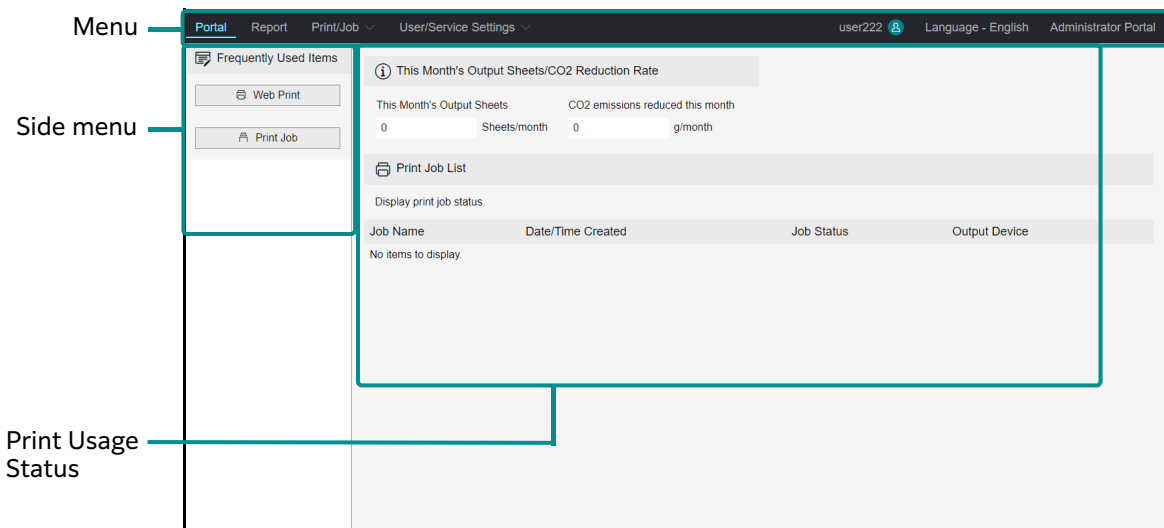


Note

- The access permission to [User Portal] is granted only when the Access Profile associated with the user is set to display the User Portal.
- Web Print-dedicated User Screen is displayed when [Access to User Portal] in the properties of Guest User Group, to which the guest user belongs, is set to [Allow Web Print only]. When [Configure in Access Profile] is selected, the setting for Access Profile associated with the user will take effect.
- If two or more users are using a single guest user account, fees for each user cannot be managed accurately. Therefore, do not use the cost management function.

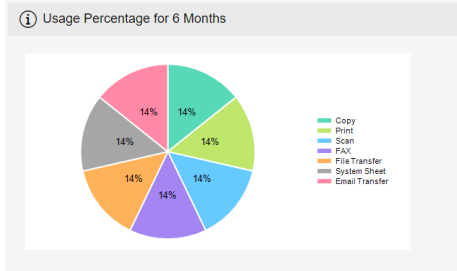
User Portal

We call the portal page on the user screen “User Portal”. The user portal displays frequently used settings, print usage status, and print job list.



The print usage status displays CO2 emissions calculated from the user print record.

Items	Description
Sheets this month	Display the total amount of print output of this month. The amount of the output prints is updated not just after printing, but after the job log aggregation.
Balance (Specified Account)	Displays the balance of the account associated with the user under cost management.
CO2 emissions reduced this month (g/month)	Displays the CO2 emissions reduced this month. “2-Sided Print” and “Pages per Side Print” enable you to reduce CO2 emissions.

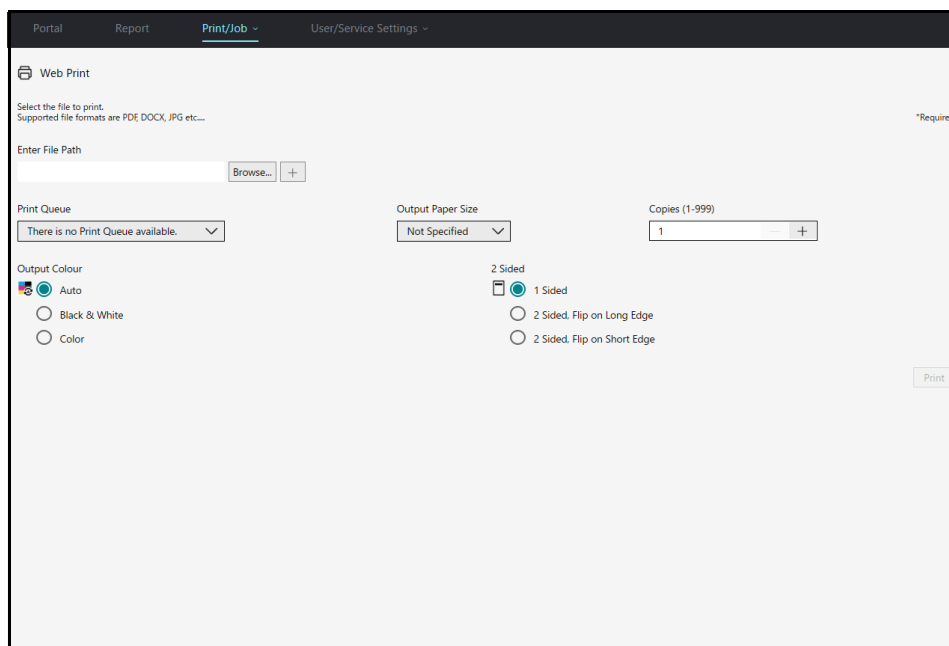
Items	Description
Usage Percentage for 6 Months ^{*1 *2}	Displays the percentage of output pages among all the jobs whose pages are included and that are associated with the user ID of the operating user in a pie chart.  Displays the pie chart for "Usage Percentage for 6 Months" in order of percentage size. The color for each job type is fixed.
Usage Transition for 6 Months ^{*1 *2}	Displays the total output pages of all the jobs whose pages are included and that are associated with the user ID of the operating user by month in a bar graph. Displays the output pages for the job log retention period when the period is less than 6 months.
This Month's Black & White/Color Output Status	Displays the black & white and color pages of print, copy, and scan respectively.
List of Print Jobs On Hold	Displays up to 5 on-demand print jobs (job name, date of creation) on hold.
Job Log List	Displays up to 5 latest job logs (document name, results, service type, job end data/time).
Print Job List	Displays up to 20 latest print job statuses (job name, date of creation, job status, output device).

*1 This is not reflected immediately after job processing, but after the job log aggregation.

*2 For correct accounting, prioritize the job owner name in the job log items used to identify the job owner. For details refer to "2 [Job Owner Identification Method]" (P.47).

Web Print-dedicated User Screen

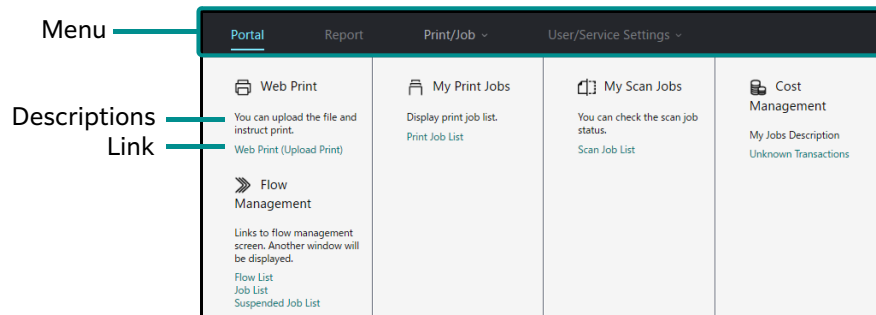
When [Access to User Portal] in the properties of Guest User Group, to which the guest user belongs, is set to [Allow Web Print only], this User Screen is displayed when the guest user logs in. The logged in guest user cannot access the [Portal] and [User/Service Settings] menus.



User Screen Operation

Hovering a cursor over the [Print/Job] and [User/Service Settings] menu will display the description of each function and links.

The Web Print-dedicated [Portal] page contains only the [Print/Job] menu, and an access to [Portal] or [User/Service Settings] is not available.



The following charts show items that are possible to operate in each menu.

Header

Items	Descriptions
[Log out]	Logs out.
[Language-]	Changes languages. Changing a language causes the screen to be transitioned to portal page, etc.  Refer Transition Destination → "Access Permissions to the Operation Screen" (P.18)
[Administrator Portal]	Displays the portal page (P.21) for administrator on another tab on the web browser.

[Portal] menu

Side menu	Descriptions
Frequently Used Item(s)	
Web Print	Shortcut to [Web Print].
Print Job	Shortcut to [Print Job List].
Usage Status	Displays the usage status of devices.



Note

The Web Print-dedicated [Portal] page does not provide an access to the [Portal] menu.

[Print/Job] menu

Description/Link	Descriptions
Web Print	
Web Print (Upload Print)	Uploads the file and instructs to print.
My Print Jobs	
Print Job List	Displays the print job status executed by login users. Allows you to hold release for the print job and cancel it.
Documents Requiring Approval	
 Note This feature is not available in some countries and regions. For details, contact our dealers.	
List of Documents Pending Approval	Displays a list of the documents for which approval is requested by login users. Allows you to stop, resend request, cancel, and view approval requests for approval request documents and transfer of the approver.
List of Documents Requiring Approval	Displays a list of the documents for which approval is requested by login users. Allows you to approve, reject, and view documents for which approval is requested and transfer the approver.
History of Documents Pending Approval	You can check the history of the documents for which approval is requested by login users.
My Scan Jobs	
Scan Job List	Displays the scan job status executed by login users. Allows you to restart for the scan job and cancel it.
Cost Management	
Non Account Associated Job List	Displays the jobs which are not associated with any account. You can associate the job with an account.
Flow Management ^{*1}	
Flow List ^{*1}	Displays the list of flow configured by [Owner] who logs in as users. Creating new flows and verifying, editing, activating, deactivating, deleting, downloading and uploading flows are possible.
Job List ^{*1}	Displays the list of flow job configured by the job owner who logs in as users. Preferentially executing, suspending, reexecuting and deleting jobs are possible.
Suspended Job List ^{*1}	Displays the list of suspended operation job configured by the job owner who logs in as users. Referring, resuming and deleting jobs are possible.

*1 These items are displayed when Flow Management Option license is authenticated.

Web Print-dedicated [Print/Job] menu

Items	Descriptions
Web Print	
Enter File Path	Click [Browse] and select the file to print.
Print Server	For the distributed server configuration, select the print server.
Print Queue	Select the print queue.
Output Paper Size	Select the output paper size.
Number of Copies	Set the number of copies.
Output Color	Set the output color.
2 sided	Set whether to execute 2 sided printing.

[User/Service Settings] menu

Description/Link	Descriptions
File Management Service Settings	
Shared Folder Settings ^{*2}	Configures to use Shared Folder that the administrator sets up.
SharePoint Settings ^{*2}	Configures to use SharePoint that the administrator sets up.
DocuShare Settings ^{*2}	Configures to use DocuShare that the administrator sets up.
Salesforce Settings ^{*2}	Configures to use Salesforce that the administrator sets up.
Google Drive Settings ^{*2}	Configures to use Google Drive that the administrator sets up.
OneDrive Settings ^{*2}	Configures to use OneDrive that the administrator sets up.
SharePoint Online Settings ^{*2}	Configures to use SharePoint Online that the administrator sets up.
ABBYY FlexiCapture Settings ^{*2}	Configures to use ABBYY FlexiCapture that the administrator sets up.
User Management	
User Properties	Enables you to change the user password. ^{*4} In addition, the user allowed for change by the administrator can change a mail address and a storage location of the Scan to My Folder feature.
Download Management ^{*3}	
File Download ^{*3}	Downloads the distribution file registered by the administrator onto the client PC.
Printer Download ^{*3}	Downloads the print driver registered by the administrator onto the client PC.
Cost Management	
Favourite Account	Configures the frequently used account from the account that users are available.

^{*2} Only items, which are allowed the access to login users by access profile, are displayed.

^{*3} These items correspond to Japanese devices. Downloaded printer driver and files only correspond to Japanese OS.

^{*4} The password changed here is a login password for the user screen. However, in the case with a remote user, the password on the remote authentication server will be used for login regardless of the password that is set here.



Note

The Web Print-dedicated [Portal] page does not provide an access to the [User/Service Settings] menu.

2 System Settings/Server Monitoring

Settings from a Web Browser

You can set server monitoring and check, and system settings from a web browser. This section describes what you can do with each page.

- System Settings

Pages	Descriptions
Network Settings	Sets network environments to use on ApeosWare Management Suite.  Refer "Network Settings" (P.40)
Currency Settings	You can specify the currency to set the price policy and the account balance on Cost Management.  Refer "Currency Settings" (P.43)
Display Settings	Sets the display order of last name and first name of a user name that will be displayed in the Administrator Screen, User Screen, and Device Control Panel.  Refer "Display Settings" (P.44)
Job Log Settings	Sets the settings to output a job log file, the retention period and the data accounting. Enables you to output user information to a file.  Refer "Job Log Settings" (P.45)
Temporary Folder Settings	Sets a work folder used to send and receive data between the device and ApeosWare Management Suite.  Refer "Temporary Folder Settings" (P.48)
Change Administrator Password	You can change the Apeos_Admin user password automatically created in installing.  Refer "Change Administrator Password" (P.50)
Service Display Order Settings	The display order of services on the device panel will be set.  Refer "Service Display Order Settings" (P.50)

Pages	Descriptions
Security Settings	Encrypts files on the print server.  Refer "Security Settings" (P.53)
Control Panel Customization Settings	Executes Control Panel Customization Settings of the devices.  Refer "Control Panel Customization Settings" (P.52)
Supplies Usage Status Save Settings	Sets conditions to save the supplies usage status.  Refer "Supplies Usage Status Save Settings" (P.54)
External Terminal Settings  Note This feature is not available in some countries and regions. For details, contact our dealers.	Sets the port numbers of the connected external terminals.  Refer "External Terminal Settings" (P.54)
User Portal Settings	Sets the display of the reports to be displayed on the user portal.  Refer "User Portal Settings" (P.55)

- Service Settings > Server Monitoring Settings

Pages	Descriptions
Notification Settings	Sets notification settings to notify by email when an error has occurred.  Refer "Notification Settings" (P.60)
Monitor Settings	
System Settings	Sets conditions to monitor the availability status of the CPU and memory of servers.  Refer "System Settings" (P.56)
Service Settings	Sets a server to be monitored and a service to be monitored.  Refer "Service Settings" (P.58)
Folder Settings	Sets conditions to monitor folders by server.  Refer "Folder Settings" (P.59)

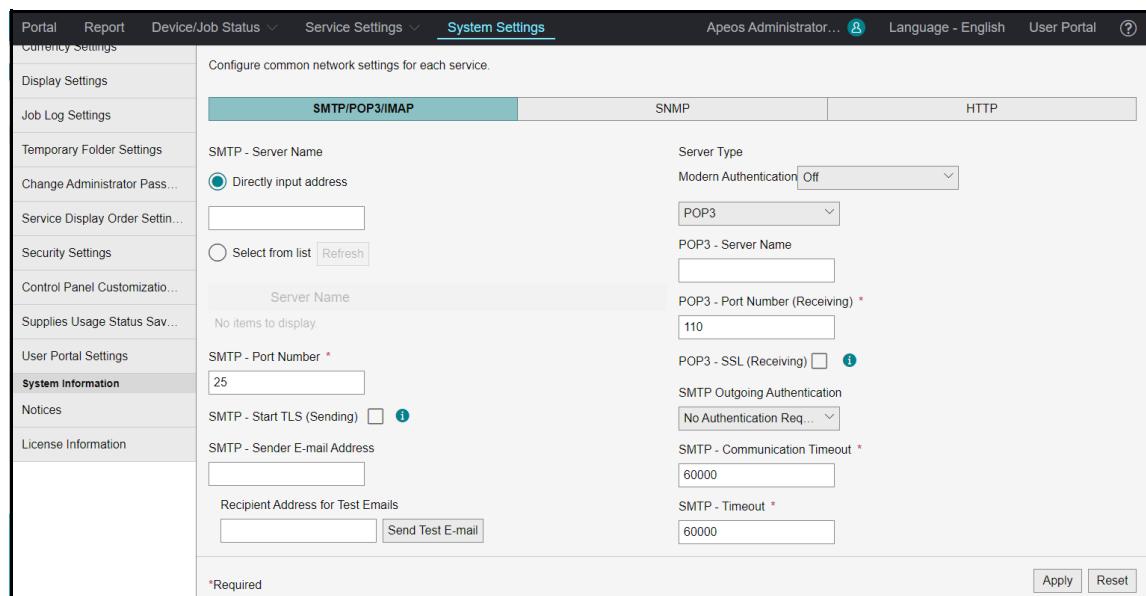
- Device/Job Status > Server Status

Pages	Descriptions
System Status	Displays the use status of the CPU and memory of the main server and separation server.  Refer "System Status" (P.60)
Service Status	Displays Active/Deactivate status of the service to be monitored.  Refer "Service Status" (P.61)
Folder Status	Displays the usage status of the user data folder used by ApeosWare Management Suite.  Refer "Folder Status" (P.63)

Network Settings

How to Display

Select [System Settings] > [Network Settings] of the administrator screen menu.



Portal Report Device/Job Status Service Settings **System Settings** Apeos Administrator... Language - English User Portal

Configure common network settings for each service.

SMTP/POP3/IMAP SNMP HTTP

SMTP - Server Name
☒ Directly input address

☐ Select from list
 Server Name
 No items to display

SMTP - Port Number *

SMTP - Start TLS (Sending) ☐ ⓘ

SMTP - Sender E-mail Address

Recipient Address for Test Emails

Server Type
 Modern Authentication

 POP3 - Server Name

 POP3 - Port Number (Receiving) *

 POP3 - SSL (Receiving) ☐ ⓘ

SMTP Outgoing Authentication

SMTP - Communication Timeout *

SMTP - Timeout *

*Required

Page Summary

Sets the items relevant to networks to use on ApeosWare Management Suite.

[SMTP/POP3/IMAP] Tab

Sets the mail server to use on ApeosWare Management Suite. When using the following features, make sure to set up the mail server.

Features	Settings
Server Monitoring	Notify by email about error detection and recovery of the service in ApeosWare Management Suite.
Device Management	Notify by email the error and the security alert in the device. Notify by email periodically the device status.
Print Management	Print a received email.
Scan Settings	Distribute a scanned document attached to an email.
Document Distribution (Flow Management Option)	Distribute a document attached to an email. interactive notifications, completion notifications, error notifications

**Note**

When you have blocked incoming and outgoing email messages by an antivirus software, you cannot send an email. In that case, you are required to stop blocking junk email messages. For details, refer to "Impossible to send email messages when an antivirus software has been installed" (P.74).

[SMTP - Server Name]/[SMTP - Port Number]

Specifies the server name of the outgoing mail server (the host name or the IP address) and the port number. You can select the server name by directly inputting address or from the list.

**Note**

After selecting [SMTP - Sender E-mail Address], clicking [Select from List] > [Update] searches the candidates for server name.

[SMTP - Start TLS (Sending)]

Sets whether [SMTP - Start TLS (Sending)] is valid or invalid. If [SMTP - Start TLS (Sending)] is enabled, the communication between this server and SMTP server is encrypted. Also the change of [SMTP - Port Number] may be required. If the SMTP server does not support Start TLS, transmissions will not be encrypted even when [SMTP - Start TLS (Sending)] is enabled.

[SMTP - Sender E-mail Address]

Specifies sender's email address.

**Note**

- When using modern authentication, the account used for authentication must match [SMTP - Sender E-mail Address].
- When using modern authentication in [SMTP Outgoing Authentication], the scan sender is to use [SMTP - Sender E-mail Address].
- When using the e-mail sending function in Flow Management Option, it is necessary to manually change [Sender] to [SMTP - Sender E-mail Address].

[Recipient Address for Test Emails]

Specifies the recipient address of the test email. This is used to confirm whether the input SMTP server and the sender email address are set correctly.

Sends the test email to the recipient address using the input settings by clicking [Send Test E-mail].

[Modern Authentication]

Specify whether to use modern authentication. When using this, set this in advance.

**Refer**

"Advance Settings When Using Modern Authentication" (P.64)

When using this, select [On] and specify the following.

- OAuth provider
Select either Exchange Online or Gmail.
- Application (client) ID
Enter the ID set on the authorization server.
 - For Exchange Online
Log in to Microsoft Azure as a user with Azure management permissions, and in [Register app] of [Microsoft Entra ID], register ApeosWare Management Suite. In the summary field of the registered app, enter the [Application ID] that can be found.
 - For Gmail
Log in to the Google Cloud Platform (GCP), go to [APIs & Services] and then [Credentials], and enter the ID created in [OAuth client ID].
- Client secret
Enter the ID set on the authorization server.

[POP3 - Server Name]/[POP3 - Port Number (Receiving)]

Specifies the server name of the incoming mail server (Host name or IP address) and the port number.



Note

The default port number is 110. If a different port is used, set the port number according to the environment.

[POP3 - SSL (Receiving)]

Sets whether the SSL communication of the port for e-mail receiving is executed. If [POP3 - SSL (Receiving)] is enabled, the communication between this server and POP3 server is encrypted. When the POP3 server is set to SSL reception only, you need to change [POP3 - Port Number (Receiving)] to 955.

[SMTP Outgoing Authentication]

If not using modern authentication, when using authentication when sending with SMTP, select [POP before SMTP] or [SMTP AUTH], and then enter the login information to be used for the authentication.



Note

When [POP before SMTP] is selected, the default port number is 110. If a different port is used, set the port number according to the environment.

If using modern authentication, either [Authenticated] or [Authentication Required] will be displayed. Click [Authentication Required], and the authentication screen will be displayed according to the OAuth provider.



Note

After setting to [Authenticated], implementation of authentication will be necessary again when performing the following processes.

- When performing backup restoration of ApeosWare Management Suite
- When the user has disabled the access token

For details on disabling the access token, refer to information from each OAuth provider.

[SMTP - Communication Timeout]

Specifies the timeout time for SMTP communication (unit: millisecond).

[SMTP - Connection Timeout]

Specify the timeout time for SMTP communication (unit: millisecond).

[SNMP] Tab

Enter [SNMP - Retry Interval] (unit: millisecond) and [SNMP - Retry Count] to retry if no response on SNMP connection.

[HTTP/SOCK] Tab

Specify the name and the port number of the HTTP proxy server. Perform settings when accessing external services such as Google Drive. If you do not use linking with file management service, you can leave this item as blank.

To coordinate with a cloud service, such as OneDrive, set the HTTP proxy server corresponding to the network configuration in which the ApeosWare Management Suite server is located.

Specify HTTP/SOCKS to use a proxy server for advanced authentication. No proxy server will be used if this is left blank. You can specify an HTTP proxy server, a SOCKS proxy server, or both an HTTP proxy server and a SOCKS proxy server.

Currency Settings

How to Display

Select [System Settings] > [Currency Settings] of the administrator screen menu.

The screenshot displays the 'Currency Settings' page within the ApeosWare Management Suite. The left sidebar contains a navigation menu with categories like 'Common Settings', 'Network Settings', 'Currency Settings' (highlighted), 'Display Settings', 'Job Log Settings', 'Temporary Folder Settings', 'Change Administrator Password', 'Service Display Order Settings', 'Security Settings', 'Control Panel', 'Customization Settings', 'External Terminal Settings', 'Supplies Usage Status', 'Save Settings', 'User Portal Settings', 'System Information', 'Notices', and 'License Information'. The main content area shows the 'Currency Settings' configuration. It includes a breadcrumb trail: 'System Settings / Common Settings / Currency Settings'. Below this, there's a description: 'Sets currencies used when configuring price policies.' The configuration fields are: 'Currency Name' (a dropdown menu showing 'Japan Yen (¥)'), 'Currency decimal digits' (a dropdown menu showing '0'), 'Billing Device Currency Name' (a dropdown menu showing 'Point'), and '*Conversion Rate' (a text input field with '1' and increment/decrement buttons). At the bottom right, there are 'Apply' and 'Reset' buttons.

Page Summary

You can specify the currency to set the price policy and the account balance on Cost Management.

The default values of the currency name and the currency's decimal digits conform to the regional and the language settings of the server that ApeosWare Management Suite is installed on.

[Currency Name]

Select a currency name from the dropdown list box.



Note

- When a job is executed after setting the currency name, you can no longer change the set currency name. Re-installation is required to change the currency name.
- Even when you change the currency, the price policy and balance values will remain the same (they will not be converted based on the exchange rate). Make sure to select the unit that is appropriate for your operating environment.

[Currency decimal digits]

Specify currency decimal digits. The default of currency decimal digits is changed as the currency name is changed. You can change it individually.

[Billing Device Currency Name]

Select a currency name used for the billing device connected to the terminal used for On Demand Print Terminal. When selecting the currency that is different from [Currency Name], specify [Conversion Rate].



Note

This feature is available only in Japan.

Display Settings

How to Display

Select [System Settings] > [Display Settings] of the administrator screen menu.

Portal Report Device/Job Status Service Settings System Settings

Common Settings
Network Settings
Currency Settings
Display Settings
Job Log Settings
Temporary Folder Settings
Change Administrator Password
Service Display Order Settings
Security Settings
Control Panel Customization Settings
External Terminal Settings
Supplies Usage Status Save Settings
User Portal Settings
System Information
Notices
License Information

System Settings / Common Settings / Display Settings

Display Settings
Configures the screen display.

User Name Display Order
(Last Name)/(First Name) ▼

Apply Reset

Page Summary

Sets the display order of last name and first name of a user name that will be displayed in the Administrator Screen, User Screen, and Device Control Panel.

Job Log Settings

How to Display

Select [System Settings] > [Job Log Settings] of the administrator screen menu.

Page Summary

Sets the settings to save a job log file, the retention period of job log and the accounting. Also, you can output the user information, which is used for the accounting on Job Log Analyzer, to a file.

[Save Job Log] Tab

[Storage Location]

Specify the job log folder.

To store a job log file to ApeosWare Management Suite server, select [Local]. To store it a shared folder in remote PC, select [Other Machines on the Network].



Note

- Storing a job log file to the local requires the full control rights of Network Service account to the stored folder.
- Confirm that the available storage space is sufficient in the drive in the stored folder of the job log file.

[Path]

Specify the path to the storing location of job log files.

Specify the absolute path if [Local] is selected on [Storage Location]. Example: D:\foldername\sub
When you select [Other Machines on the Network] on [Storage Location], specify the path by UNC format beginning with “\\”.

Example:

\\ComputerName\FolderName\sub
\\192.0.2.1\FolderName\sub



Note

If [Storage Location] or [Path] has been changed during operation, only the job logs after changing are output to the folder changed. When a file has already been output in the past, it will not be re-output.

[User Name]/[Password]

Specify these when you select [Other Machines on the Network] on [Storage Location]. Enter the user name and the password to connect with the shared folder.

[Domain Name or Computer Name]

Specify these when you select [Other Machines on the Network] on [Storage Location]. Enter the shared folder domain name or computer name.

[Encoding Type]

Select the encoding of the job log file.

[Saved Contents]

Specify whether to include the document name information in the job log file stored and whether to include the user principal name in the user name. If you don't want to record the document name in the job log for security reasons, check the [Remove Document Name].

When you create graphs by document type with Job Log Analyzer, the document name is required to be included in the job. In this case, remove the check at [Remove Document Name].

To include the user principal name in the user name, select a checkbox for [Include UPN].



Note

When you make a change to [Encoding] or [Saved Contents] during operation, the change will be applied to the job logs on and after you make the change. When a file has already been output in the past, it will not be re-output.

[Storage Location Sub Folder Name]

Select one from the following

- [Job Start Date]
- [Job End Date]
- [Job Log Collection Date]

This date will be used as the date information when deleting the job log exceeding the retention period from ApeosWare Management Suite, or aggregating on Job Log Analyzer. Moreover, it is used as the subfolder name to output the job log file.

Note the following to set it.

- If the [Job Start Date] value is empty in job log, the [Job End Date] is used as the [Storage Location Sub Folder Name]. If the [Job End Date] is empty, the [Job Start Date] is used. If both of them are empty, the [Job Log Collection Date] value is used. If all of them are empty, the job log is not monitored.
- For Printer MIB Collection, the [Storage Location Sub Folder Name] becomes the job log collecting date because it does not retrieve the job start date and the job end date.

[Interval]

Specify the timing to output the job log file.

To output the job log file at the specified time once a day, select [By Day] and then enter the time to be output.

To output the job log file at the specified interval, select [By Minute] and then specify the interval (minute) to be output.

[Save User Information]

Clicking [Run User Information Saving] outputs all user information registered in ApeosWare Management Suite to the location specified in [Storage Location] and [Path]. You can use the output user information for the accounting on Job Log Analyzer.

When you uncheck the checkbox for [Display User Group in Hierarchy View], the user Information is output without hierarchical information.

The attributes of output user information are the followings:

- User ID
- Display name
- External Accounting ID
- User group
- Card ID (PAN)



Refer

Details on output format, etc. → “Help for Job Log Analyzer”

[Job Log Retention Period] Tab

[Retention Period for Job Log in Database]

Enter the number of days for retaining the job log in the ApeosWare Management Suite database. The job log data is deleted from the ApeosWare Management Suite database once the retention period has expired.



Note

- The log of the device whose collection type is [Printer MIB (SNMP)] is stored the job log file, and then deleted from the database. Therefore, the retention period specified here is not applied.
- The job log which is covered under Auto Report Settings by Schedule and has not been created a report is not deleted.
- The job log file stored as a text file does not have a retention period. The file remains unless it is deleted manually.

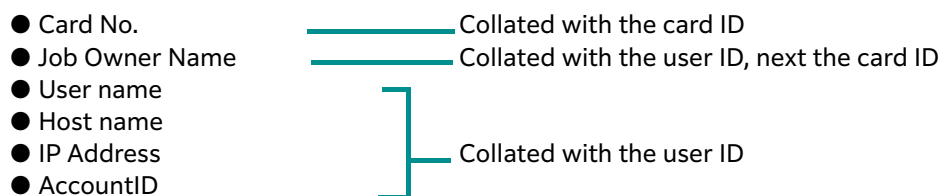
[Accounting Settings] Tab

[Job Owner Identification Method]

Add the job log item to be used to specify the job owner to [Items to Set and Priority]. Assign property sorting the items if necessary.

ApeosWare Management Suite decides the job owner by collating from the top the user ID or the card ID (PAN) registered in the database with the item specified to [Items to Set and Priority] among the job log items.

Job log items are collated as below.



If the job log owner name agrees with the alternate user ID (if set more than one, agrees with one of them), the representative user ID of the alternate user IDs becomes the job owner.



Note

“AccountID” is the ID used for accounting which is set in the device. It is unrelated to “Account” used on Cost Management.



Refer

“Alternate User ID” in “Installation and Operation Guide”

[User Name for Unidentified Cases]

Enter the character string to be used as the owner if the job owner cannot be specified.

[CO2 Load for A4 Paper]

Sets the CO2 load coefficient to use when aggregating the CO2 load for each job.

[Rebuild Accounting Results]

Select whether to rebuild the daily accounting data.

If [Rebuild during the next accounting] is selected, the daily accounting data is rebuilt the next aggregation (at midnight or at the time the scheduler starts).



Note

- It may take a long time to rebuild the daily accounting data. Set [Rebuild during the next accounting] only when rebuilding the current daily accounting data are required because of changing the user information.
- The data may be lost by rebuilding data. For example, if you set the job log retention period to “30 days”, the data 30 days ago or earlier is discarded by rebuilding.

Temporary Folder Settings

How to Display

Select [System Settings] > [Temporary Folder Settings] of the administrator screen menu.

The screenshot shows the 'Temporary Folder Settings' page within the 'System Settings' menu. The left sidebar contains a list of settings categories, with 'Temporary Folder Settings' highlighted. The main content area displays the following fields and options:

- System Settings / Common Settings / Temporary Folder Settings** (breadcrumb)
- Temporary Folder Settings** (title)
- Configures temporary folder used for transferring data between the device when using the scan or mobile feature.** (description)
- Temporary Folder (Network Path)** (text input field)
- User Name** (text input field, value: AWMS_Device_Access)
- Password** (password input field, value:
- User Type** (radio buttons: ☐ Domain User, ☒ Local User)
- Domain Name or Computer Name** (text input field)
- Apply** and **Reset** buttons at the bottom right.

Page Summary

You can set a work folder to temporarily store the data to be exchanged between the device and ApeosWare Management Suite when using scan or mobile feature.

You can set the local folder on the ApeosWare Management Suite server or the shared folder on the remote PC as a temporary folder.

A temporary folder is required the following settings.

Temporary Folder location	Required Settings
Local Folder	Set the folder being a temporary folder as to be shared, and give full control rights for Network Service account.
Shared Folder on the Remote PC	Give the full control rights of the PC account on the ApeosWare Management Suite server to the shared folder.



Note

- Available only in domain environment when you specify the shared folder on the remote PC.
- Confirm that the available storage space is sufficient in the drive specified to the temporary folder.
- A temporary folder is used when the data is sent and received between the device and ApeosWare Management Suite. Therefore, it is required to be the shared folder accessible from the device.

[Temporary Folder (Network Path)]

Specify the path to the temporary folder by UNC format beginning with “\\”.

In the case of a local folder, specify the server name or the IP address of ApeosWare Management Suite server as a network folder.

Example: \\servername\sub\192.0.2.1\sub

[User Name]/[Password]

Enter the user name and the password to connect to the temporary folder.

To specify the shared folder on a remote PC, specify the user name and the password accessible to the remote PC. To specify the local folder, specify the user name and the password accessible to the ApeosWare Management Suite server.

[User Type]

Select [Domain User] when the shared folder in the remote PC to the temporary folder and select [Local User] when the local folder is specified.

Enter the domain name to [Domain Name] when [Domain User] is selected.

Change Administrator Password

How to Display

Select [System Settings] > [Change Administrator Password] of the administrator screen menu.

The screenshot shows the 'System Settings' page in the ApeosWare Management Suite. The left sidebar contains a list of settings categories: Common Settings, Network Settings, Currency Settings, Display Settings, Job Log Settings, Temporary Folder Settings, Change Administrator Password (highlighted), Service Display Order Settings, Security Settings, Control Panel, Customization Settings, External Terminal Settings, Supplies Usage Status, Save Settings, User Portal Settings, System Information, Notices, and License Information. The main content area shows the 'Change Administrator Password' page. It includes a breadcrumb trail: System Settings / Common Settings / Change Administrator Password. Below this is a heading 'Change Administrator Password' with a key icon and a subheading 'You can change the ApeosWare Management Suite default administrator (Apeos_Admin) password.' There are three input fields: 'Current Password', '*New Password/Pin', and 'Confirm Password/Pin'. An 'Apply' button is located at the bottom right of the form.

Page Summary

You can change an Apeos_Admin user's password. The Apeos_Admin user is a built-in user that is created when ApeosWare Management Suite is installed.

It is created.



Note

Be sure to change the Apeos_Admin User password before operating for the first time. In addition, it is recommended to change the password regularly.



Refer

"Apeos_Admin User" (P.18)

[Current Password]

Enter Current Password. This is case sensitive.

[New Password]

Enter the new password. Re-enter the password to confirm. This is case sensitive.



Note

Conform the minimum number of characters for and the character types available to passwords to [Service Settings] > [User Management] > [Authentication Settings].

Service Display Order Settings

Page Summary

Configure the order of services to be displayed with devices on the network, such as multi-function printer and printer. On the settings screen, a list of available services with ApeosWare Management Suite is displayed. The order of displayed services is the same as with the order shown on the ApeosWare Management Suite Portal Screen for the device.

When the service display order is modified, the list of services will show the modified order. After modifying the service display order, when a license for new service is added, the added service will appear at the end of the list.

The result of modification will be reflected when you log in to the ApeosWare Management Suite Portal Screen for the device.



Note

Regarding the services requiring the license, only the ones with valid license are displayed.

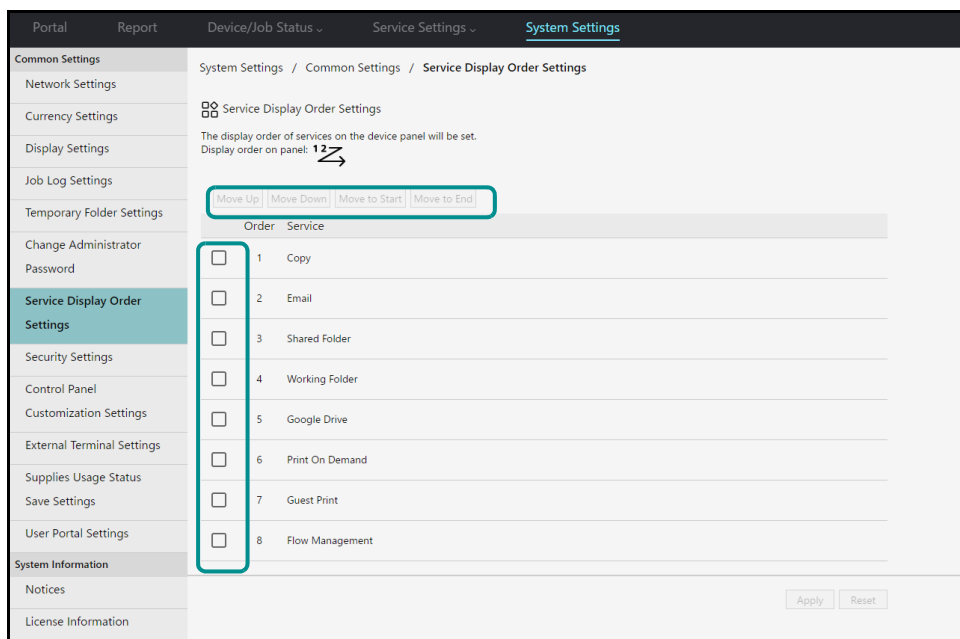


Refer

"License Activation" in "Setup Guide"

How to Display

1. Change the settings of [Service Display Order Settings] according to the following steps.
2. Select [System Settings] > [Service Display Order Settings] from the menu on the administrator screen.
3. Modify the display order by performing the following operation.
 - (1) Place a check mark to the left of the icon for [Service] you wish to change.
 - (2) Click the upper buttons ([Move Up], [Move Down], [Move to Start], or [Move to End]) to move the item to the desired position to display.



Note

The order of two or more services can be changed at the same time, but the original order among the selected items will be maintained.

When check marks are placed to [Copy] and [Shared Folder]

Order before the change		Order after the change	
		For [Move Up]	For [Move Down]
☒	Copying	Copying	Email
	Email	Shared Folder	SharePoint

Order before the change		Order after the change	
		For [Move Up]	For [Move Down]
☒	Shared Folder	Email	Copying
	SharePoint	SharePoint	Shared Folder
	DocuShare	DocuShare	DocuShare

Control Panel Customization Settings

How to Display

Select [System Settings] > [Control Panel Customization Settings] from the menu on the administrator screen.

The screenshot shows the 'System Settings' page with the 'Control Panel Customization Settings' sub-menu selected. The left sidebar lists various settings categories: Common Settings, Network Settings, Currency Settings, Display Settings, Job Log Settings, Temporary Folder Settings, Change Administrator Password, Service Display Order Settings, Security Settings, Control Panel Customization Settings (highlighted), External Terminal Settings, Supplies Usage Status, Save Settings, User Portal Settings, System Information, Notices, and License Information. The main content area for 'Control Panel Customization Settings' includes a breadcrumb trail 'System Settings / Common Settings / Control Panel Customization Settings', a title 'Control Panel Customization Settings', a description 'Perform settings for the screen displayed on the control panel during Custom Authentication.', and three settings: 'Display QR Code for Connection' (radio buttons for On and Off, with 'On' selected), 'Display Logo' (a checkbox and a file upload button), and 'Custom Labels/Settings' (two text input fields and a plus button). At the bottom right are 'Apply' and 'Reset' buttons.

Page Summary

When a device of FUJIFILM Business Innovation uses Custom Authentication, the display of the operation panel is customized based on these settings.



Note

Customization of the login screen is applied only while on-line.



Refer

"Operation from the Device's Control Panel" (P.112)

[Display QR Code for Connection]

Select whether to display the QR code in the login screen of the device.

[Display Logo]

You can display the uploaded logo in the login screen of the device.

Click [Browse] and select the file for logo. You can select a gif, jpg, png, or bmp file of 198 x 59 pixels.

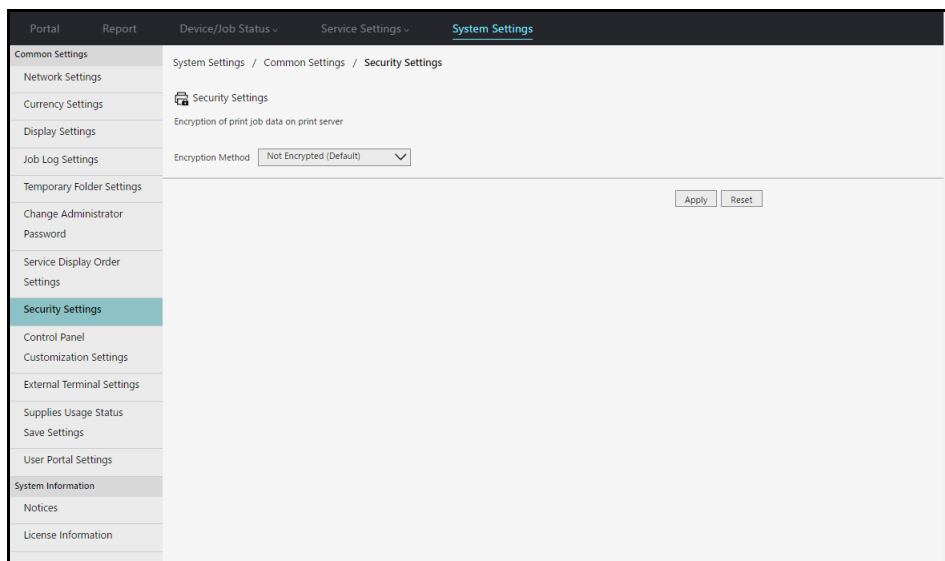
[Custom Labels/Settings]

You can set arbitrary characters in 2 rows in the login screen of a device: up to 15 characters in the custom label and up to 256 characters in the setting value. You can set up to 9 double-byte characters or 29 single-byte characters in the setting value displayed on the operation panel. When the number of characters exceeds the one that can be displayed, the [i] button is displayed. When this button is pressed, all the characters are displayed.

Security Settings

How to Display

Select [System Settings] > [Security Settings] from the menu on the administrator screen.



Page Summary

Encrypts and retains print data of jobs on hold or standby on the print server. This setting is not a measure to completely prevent data leakage from the server.

Select the encryption method from the pull-down menu.

[Not Encrypted], [AES-256], [SEED], or [ARIA] can be selected.

Supplies Usage Status Save Settings

How to Display

Select [System Settings] > [Supplies Usage Status Save Settings] from the menu on the administrator screen.

The screenshot shows the 'System Settings' page with a sidebar menu on the left. The 'Supplies Usage Status Save Settings' option is highlighted in the sidebar. The main content area shows the breadcrumb 'System Settings / Common Settings / Supplies Usage Status Save Settings'. Below this, there is a section titled 'Supplies Usage Status Save Settings' with a description: 'Configures the settings related to saving the supplies usage status. The supplies usage will be saved every day at the specified time, and you will be able to check it in the report.' There are two input fields: 'Information Retention Period' with a value of '365' and a unit of 'days', and 'Supplies Usage Status Saved On' with a value of '12:00 AM' and a '+' button. An 'Apply' button is located at the bottom right of the main content area.

Page Summary

Sets conditions to save the supplies usage status. You can save the usage status of supplies at the specified time everyday and check it in a report.

[Information Retention Period]

Set the information retention period in the range of 1 to 730 days in increments of one day.

[Supplies Usage Status Saved On]

Set the information save time in the range of 0:00 to 23:59.

External Terminal Settings



Note

This feature is not available in some countries and regions.
For details, contact our dealers.

How to Display

Select [System Settings] > [External Terminal Settings] of the administrator screen menu.

Portal Report Device/Job Status Service Settings System Settings

Common Settings System Settings / Common Settings / External Terminal Settings

Network Settings

Currency Settings

Display Settings

Job Log Settings

Temporary Folder Settings

Change Administrator Password

Service Display Order Settings

Security Settings

Control Panel Customization Settings

External Terminal Settings

Supplies Usage Status

Save Settings

User Portal Settings

System Information

Notices

License Information

External Terminal Settings

Configures the external terminal.

*KJ Card Reader - Port Number

8092

Apply Reset

Page Summary

Set the port number to communicate with a usable external terminal.

Set the port numbers of the connected external terminals in the range from 0 to 65535.



Refer

- “Checking and Changing Device Information” (P.97)

User Portal Settings

How to Display

Select [System Settings] > [User Portal Settings] of the administrator screen menu.

Portal Report Device/Job Status Service Settings System Settings

Common Settings System Settings / Common Settings / User Portal Settings

Network Settings

Currency Settings

Display Settings

Job Log Settings

Temporary Folder Settings

Change Administrator Password

Service Display Order Settings

Security Settings

Control Panel Customization Settings

External Terminal Settings

Supplies Usage Status

Save Settings

User Portal Settings

System Information

Notices

License Information

User Portal Settings

Sets the report to be displayed on the dashboard of the user portal.

This Month's Black & White/Color Output Status Do Not Display

Usage Percentage for 6 Months (Print/Copy) Do Not Display

Usage Transition for 6 Months Do Not Display

List of Print Jobs On Hold Do Not Display

Job Log List Do Not Display

Print Job List Do Not Display

Apply Reset

Page Summary

Set the reports to be displayed on Dashboard of the user portal.

Whether or not to display the following items can be set.

- Usage Percentage for 6 Months
- Usage Transition for 6 Months
- This Month's Black & White/Color Output Status
- List of Print Jobs On Hold
- Job Log List
- Print Job List

System Settings

How to Display

Select [Service Settings] > [Server Monitoring Settings] > [Monitor Settings] > [System Settings] from the menu on the administrator screen.

The screenshot shows the 'System Settings' page within the 'Service Settings' section. The left sidebar contains a menu with 'Server Monitoring Settings', 'Notification Settings', 'Monitor Settings', 'System Settings' (highlighted), 'Service Settings', and 'Folder Settings'. The main content area is titled 'System Settings' and includes a sub-header 'Configure settings related to system monitoring.' Below this, there is a 'System Monitoring' toggle set to 'On'. Five configuration items are listed, each with a text input field and a unit: 'CPU/Memory Usage Rate Check Interval' (3 minutes), 'CPU Usage Rate Threshold' (85 %), 'Number of CPU Warning Detections' (10 times), 'Memory Usage Rate Threshold' (85 %), and 'Monitoring History Retention Period' (30 days). Each item has an information icon. At the bottom right are 'Reset' and 'Apply' buttons.

Page Summary

Sets conditions to monitor the availability status of the CPU and memory of servers.

[System Monitoring]

Specify whether to monitor the system. Select [On] to monitor the system.

[CPU/Memory Usage Rate Check Interval]

Set the check interval in the range of 1 to 5 minutes in increments of 1 minute.

The check results are displayed in [System Status] and [Service Status].



- "System Status" (P.60)

[CPU Usage Rate Threshold]

Set the threshold to determine a CPU usage rate error in the range of 50 to 100% in increments of 1%.

[Number of CPU Warning Detections]

Set the number of times exceeding [CPU Usage Rate Threshold] that is used for judgment of an error in the range of 1 to 10 times in increments of 1.

When it is judged as an error, error detection mail is sent to the mail address specified in [Notification Settings]. When the rate falls below the threshold and returns to the ready status, restoration detection mail is sent.



Refer

"Notification Settings" (P.60)

[Memory Usage Rate Threshold]

Set the threshold to determine an memory usage rate error in the range of 60 to 100% in increments of 1%.

[Number of Memory Warning Detections]

Set the number of times exceeding [Memory Usage Rate Threshold] that is used for judgment of an error in the range of 1 to 10 times in increments of 1.

When it is judged as an error, error detection mail is sent to the mail address specified in [Notification Settings]. When the rate falls below the threshold and returns to the ready status, restoration detection mail is sent.



Refer

"Notification Settings" (P.60)

[Monitoring History Retention Period]

Set the retention period of CSV files that record monitoring history in the range of 5 to 100 days in increments of 1 day.

CSV file storage location:

- {Folder of data storage directory}\Data\Mon\ResourceMonitoringResult
In default setting, {Folder of data storage directory} is "C:\FUJIFILM\ApeosWare MS".

File name:

- minute-yyyyMMdd.csv
Output a file in increments of minutes after monitoring starts.
Output format: Time (HH:mm), CPU Usage Rate (%), Memory Used (GB)/Total Memory (GB)
- hour-yyyyMMdd.csv
Output a file at the timing when first monitoring output in minutes is conducted at 0 min 0 sec of each hour (1 o'clock, 2 o'clock, 3 o'clock ..., 0 o'clock (24 o'clock)).
Output format: Time (HH), CPU Usage Rate (%), Memory Used (GB)/Total Memory (GB)
- date-summary.csv
Output a file at the timing when first monitoring output in hours is conducted at 0 hour 0 min 0 sec everyday.
Output format: Date (yyyy/MM/dd), CPU Usage Rate (%), Memory Used (GB)/Total Memory (GB)

When the year changes and the monitoring results are first output to a CSV file, the CSV file is renamed and a new CSV file is generated.

The file name after renaming is date-summary_YYYY.csv.

20 years of monitoring history is saved, and CSV files older than 20 years are deleted at the time the monitoring history is appended.

Service Settings

How to Display

Select [Service Settings] > [Server Monitoring Settings] > [Monitor Settings] > [Service Settings] from the menu on the administrator screen.

Portal Report Device/Job Status **Service Settings** System Settings

Server Monitoring Settings

Notification Settings

Monitor Settings

System Settings

Service Settings

Folder Settings

Service Settings / Server Monitoring Settings / Service Settings

Monitor Settings

Check the service(s) you want to monitor and click [Apply].

Host Name	Service Name	Activity Monitored
☒	World Wide Web Publishing Service	Service Availability
☒	ApeosWare Management Suite Core Service	Service Availability, Java Memory Unused Capacity, Available Storage Space
☒	ApeosWare Management Suite Multi Task Service	Service Availability
☒	ApeosWare Management Suite Flow Management Service	Service Availability, Java Memory Unused Capacity, Available Storage Space
☒	ApeosWare Management Suite Printer Port Service	Service Availability
☒	SQL Server (FXAW)	Service Availability, Occurrence of Memory Pressure / Index Fragmentation
☒	ApeosWare Management Suite Update Service	Service Availability
☒	ApeosWare Management Suite Email Print Service	Service Availability

Reset Apply

Page Summary

Select the checkboxes for the server and service to set as the monitoring targets. The items to be monitored on the service are below.



Refer

"Details of Monitoring" in "Installation and Operation Guide"

Service Name	Details of Monitoring
SQL Server (FXAW) *1	• SQL Server Connection • SQL Server Memory Pressure • SQL Server Index Fragmentation *2
World Wide Web Publishing Service	Service monitoring
ApeosWare Management Suite Multi Task Service	Process monitoring
ApeosWare Management Suite Core Service	• Service monitoring • JavaVM memory • Available Storage Space
ApeosWare Management Suite Update Service	Process monitoring
ApeosWare Management Suite Printer Port Service	Process monitoring
ApeosWare Management Suite Flow Management Service	• Service monitoring • Spooler monitoring • JavaVM memory
ApeosWare Management Suite Email Print Service	Process monitoring
ApeosWare Management Suite Image Log Management Core Service	• Process monitoring • Service monitoring • JavaVM memory • Available Storage Space *3
ApeosWare Management Suite Image Log Management Receive Service	• Process monitoring • Service monitoring • JavaVM memory • Available Storage Space

Service Name	Details of Monitoring
ApeosWare Management Suite Image Log Management Receive Service	• Process monitoring • Service monitoring • JavaVM memory • Available Storage Space
ApeosWare Management Suite Image Log Management Search Service	• Process monitoring • Service monitoring • JavaVM memory
ApeosWare Management Suite Proxy Service	• Process monitoring • HTTP monitoring (main server only, added for MFDEX applications) • CPU/memory usage monitoring
ApeosWare Management Suite mDNS Service ^{*4}	• Process monitoring

*1 Not monitored in case the database server is separated from the main server in distributed configuration.

*2 We provide the command to rebuild fragmented index. For details refer to "Rebuild Index in SQL Server" (P.73).

*3 In the case of a reception server, the available storage space is not monitored.

*4 ApeosWare Management Suite mDNS Service may fail to start if there is a service with a conflicting port number (5353/udp). In these cases, stop the conflicting service and restart.
ApeosWare Management Suite mDNS Service is used to search for the ApeosWare Management Suite logical printer when using "Print from iOS Device".

Folder Settings

How to Display

Select [Service Settings] > [Server Monitoring Settings] > [Monitor Settings] > [Folder Settings] > {IP Address} from the menu on the administrator screen.

Page Summary

Sets conditions to monitor folders by server.

[Folder Monitoring]

Specify whether to monitor the folder. Select [On] to monitor the folder.

[Monitoring Interval]

Set the notification interval in the range of 1 to 24 hours in increments of 1 hour.

[Monitoring Condition]

Set the available folder space that is used as a monitoring condition in % or GB for each drive.

Notification Settings

How to Display

Select [Service Settings] > [Server Monitoring Settings] > [Notification Settings] from the menu on the administrator screen.

The screenshot shows the 'Notification Settings' page. The breadcrumb trail is 'Service Settings / Server Monitoring Settings / Notification Settings'. The page title is 'Notification Settings'. A description states: 'You can get email notifications on the status of the server you are monitoring (error or warning) and the status of the folders. Up to 200 notification addresses can be registered.' There is a toggle for 'E-mail Notification' set to 'On'. Below it, a text input field is labeled '*Add the following e-mail address to the Notification Address' with a placeholder 'Enter E-mail Address' and a '+' button. At the bottom right are 'Reset' and 'Apply' buttons.

Page Summary

You can set the settings to issue a notification by email when an error occurs, the CPU and/or memory operation rate exceeds the threshold, and recovery from these statuses is detected in the server to be monitored which has been specified in the [Monitor Settings] page.

[E-mail Notification]

To notify the server status monitored by email, select [On], and specify the recipient's email address. Click and you can set more than one.



Note

The settings are not required if you don't need E-mail Notification. However, the server is monitored and the event log is recorded regardless of whether to set the settings or not.



Refer

Settings for sending email → "Network Settings" (P.40)

System Status

How to Display

Select [Device/Job Status] > [Server Status] > [System Status] from the menu on the administrator screen.

The screenshot shows the 'System Status' page. The breadcrumb trail is 'Device/Job Status / Server Status / System Status'. The page title is 'System Status'. A description states: 'Displays the OS CPU and memory usage status.' Below this is a table with the following data:

Host Name	CPU Usage Rate	Memory Used	Total Memory	Memory Usage Rate
tsd010101-01-01-01-01-01-01	7%	6.9GB	8.0GB	86%

Page Summary

Display the CPU Usage Rate, Memory Used, Total Memory, and Memory Usage Rate of the main server and separation server of ApeosWare Management Suite.

[Host Name]

Display the name of the server.

[CPU Usage Rate]

Display the CPU Usage Rate of each server.

[Memory Used]

Display the memory usage rate of each server.

[Total Memory]

Display the total memory implemented in each server.

[Memory Usage Rate]

Display the memory usage rate of each server.

Service Status

How to Display

Select [Device/Job Status] > [Server Status] > [Service Status] from the menu on the administrator screen.

Page Summary

Displays the availability status and service status, etc. of the service to be monitored.

Portal	Report	Device/Job Status	Service Settings	System Settings	Apeos Administrator...	Language - English	User Portal	?
Server Status								
System Status								
Service Status								
Folder Status								
Device/Job Status / Server Status / Service Status								
Service Status								
Displays the availability of each service to be monitored.								
Host Name	Service Name	Availability St...	Service Sta...	PID	CPU	Memory	Operation	
2 days 11h 14min 10s ago	ApeosWare Management Suite Printer Port Service	Error	Stopped	-	-	-		
2 days 11h 14min 10s ago	World Wide Web Publishing Service	Ready	In Progress	11960	0%	3,988K		
2 days 11h 14min 10s ago	ApeosWare Management Suite Flow Management Service	Unknown	In Progress	3656	0%	1,032K		
2 days 11h 14min 10s ago	ApeosWare Management Suite mDNS Service	Ready	In Progress	3220	0%	1,368K		
2 days 11h 14min 10s ago	SQL Server (FXAW)	Ready	In Progress	1184	17.41%	286,504K		
2 days 11h 14min 10s ago	ApeosWare Management Suite Multi Task Service	Ready	In Progress	3276	0%	457,092K		
2 days 11h 14min 10s ago	ApeosWare Management Suite Proxy Service	Ready	In Progress	7560	0%	13,228K		
2 days 11h 14min 10s ago	ApeosWare Management Suite Core Service	Ready	In Progress	2288	0%	1,020K		
2 days 11h 14min 10s ago	ApeosWare Management Suite Email Print Service	Ready	In Progress	3252	0%	32,956K		

[Availability Status]

The following contents are displayed.

Availability Status	Descriptions
 (Ready)	No error detection
 (Error)	Error detected during alive monitoring
 (Note)	Error detected during resource monitoring while not detected during alive monitoring
Unknown	Availability Status could not be retrieved



Note

When error (the available storage space falls below a fixed amount) is detected, this screen is not displayed.



Refer

About alive monitoring and resource monitoring → “Details of Monitoring” in “Installation and Operation Guide”

[Service Status]

Display any of “Executed,” “Stop,” “Started,” “Resumed,” “Stopped,” “Suspend,” or “Suspended” according to the activation status of the service to be monitored. The display is automatically updated every 60 seconds. When acquisition of the service status fails, “-” is displayed.

[PID]

Display the process ID of the service to be monitored. If acquisition of the process ID fails when the service is stopped, etc., “-” is displayed.

[CPU]

Display the CPU use rate of the service to be monitored. If acquisition of the CPU use rate fails when the service is stopped, etc., “-” is displayed.

[Memory]

Display the memory usage rate of the service to be monitored. When acquisition of the memory usage rate fails, “-” is displayed.

[Operation]

When the service status is “Executed” or “Stopped”, click  of the service to be operated in the list. When the service is being executed, select [Stopped] or [Restart], and when the service is stopped, select [Start].

The service operation confirmation dialog box is displayed.

If you click [OK], the user information input dialog box is displayed. Enter a user name and password. When you do not specify the domain, enter “.”.



Note

- When ApeosWare Management Suite Core Service is stopped, the screen cannot be displayed. In this case, access the PC in which the ApeosWare Management Suite server is installed and start ApeosWare Management Suite Core Service from the service management tool.
-  is not displayed in ApeosWare Management Suite Core Service, SQL Server (FXAW), and World Wide Web publishing service.
- When you click the [Service Name] link, the detailed service information window is displayed, and you can check the Details of monitoring and operation status. In the case of ApeosWare Management Suite Core Service, you can select [Stopped] or [Restart] of the service from this detailed service information window.

This operation is displayed only for the target services shown below.

Service Name	Main Server	Print Application Separation Server	Print I/O Separation Server	Image Log Core Server	Image Log Receiving Server	Image Log Server
ApeosWare Management Suite Core Service	☐	☐	☐			
ApeosWare Management Suite Multi Task Service	☐	☐				
ApeosWare Management Suite Printer Port Service	☐	☐	☐			
ApeosWare Management Suite Email Print Service	☐	☐				
ApeosWare Management Suite Flow Management Service	☐					
ApeosWare Management Suite Update Service	☐	☐	☐			
ApeosWare Management Suite Image Log Management Core Service	☐			☐	☐	☐
ApeosWare Management Suite Image Log Management Receive Service	☐				☐	☐
ApeosWare Management Suite Image Log Management Search Service	☐			☐		☐

Folder Status

How to Display

Select [Device/Job Status] > [Server Status] > [Folder Status] from the menu on the administrator screen.

Page Summary

Displays the usage status of “{Data storage location folder}\Data” folder. This folder is referred to as “Data Folder”.

Portal

Report

Device/Job Status

Service Settings

System Settings

Server Status

System Status

Service Status

Folder Status

Device/Job Status / Server Status / Folder Status

Folder Status

Displays usage status of folder disk space.

Host Name	Folder Name	Full Path	Maximum Capacity	Unused Capacity	Usage	Usage Rate
KARAFStorageMonitor	KARAFStorageMonitor	C:\FUJIFILM\ApeosWare\MSKData	119.5GB	76.5GB	43.0GB	36%

The following items of “Data Folder” are displayed on the [Folder Status] page.

- The maximum capacity of a folder (GB)
- The available space of a folder (GB)

- The usage of a folder (GB)
- The utilization rate of a folder (%)



Note

- Specify the data storage folder when installing the program. If default setting is not changed, "C:\FUJIFILM\ApeosWare MS" is applied.
- A storage folder and a temporary folder of job log files are set under "Data Folder" by default. The storage folder and the temporary folder of job log files can be changed in [System Settings] on the administrator screen. When the storage location is changed from the default settings, the folder is not subject to being monitored.

Advance Settings When Using Modern Authentication

From [System Settings] > [Common Settings] > [Network Settings], set [Modern Authentication] to [On], and specify "Exchange Online" or "Gmail" for the OAuth provider to enable using modern authentication. However, when using these, settings must be configured in advance.

When using "Gmail"

Check that connecting to Google Drive on the Internet from the ApeosWare Management Suite 2 server is possible.

1. Access the Google Cloud Platform (<https://console.cloud.google.com/>).
2. Either select a project, or create a new project.
3. Click [Library] under [APIs & Services], and enable [Google API].
4. Click [OAuth consent screen] under [APIs & Services].
5. For [User Type], select [Internal] and click [CREATE].
6. Set the [App name], [User support email], and [Developer contact information].
For [App name], "FUJIFILM ApeosWare Management Suite" is recommended.
When creating the application ID and client secret in a personal Gmail account, add a Gmail account to use for the test user.
7. Click [SAVE AND CONTINUE].
8. Click [ADD OR REMOVE SCOPES], then select API: <https://mail.google.com/> and click [Update].
9. Click [SAVE AND CONTINUE] and check the details.
10. Click [Credentials] under [APIs & Services].
11. Click [Create credentials], and select [OAuth client ID].
12. For [Application type], select [Web application].
13. Set the [Name] and [Authorized redirect URIs], and click [CREATE].
In [Authorized redirect URIs], set either or both of the following according to the used functions.
 - Using Email
<https://{FQDN}:{ApeosWare Management Suite Https Port}/Admin/GlobalSetting/NetworkSetting/AuthorizationComplete>

■ Using Print E-mail

<https://{FQDN}:{ApeosWare Management Suite Https Port}/Admin/Print/Admin/GmailAuthorize>

For {FQDN}, set the ApeosWare Management Suite 2 main server host name. The IP address cannot be set. The host name to set must be in a format that can be accessed from client PCs and multifunction devices.

14. Record the client ID and client secret.

15. From the ApeosWare Management Suite 2 administrator screen, access [System Settings] > [Common Settings] > [Network Settings].

16. Enter the application ID and client secret acquired when the application was registered to the Google Cloud Platform into [Application (Client) ID] and [Client Secret].

When using “Exchange Online”

1. Register ApeosWare Management Suite as an app.

- (1) Sign in to Microsoft Azure as a user with Microsoft Entra management permissions.
- (2) From [Microsoft Entra ID] > [Register app], register ApeosWare Management Suite. Also, select Multi-tenant accounts for [Supported account types].

2. From [Certificates & secrets] of the app, create a client secret.
Follow the Microsoft Entra ID manual for methods on how to create.

3. Add the following to the redirect URI from [Authenticate] > [Web] of the registered app.
Set either or both of the following according to the used functions.

■ Using Email

<https://{FQDN}:{ApeosWare Management Suite Https Port}/Admin/GlobalSetting/NetworkSetting/AuthorizationComplete>

■ Using Print E-mail

<https://{FQDN}/Admin/Print/Admin/ExchangeAuthorize>

For {FQDN}, set the ApeosWare Management Suite 2 main server host name.

4. Set the following as API access permissions.

■ Using Email

SMTP.Send
offline_access

■ Using Print E-mail

IMAP.AccessAsUser.All
POP.AccessAsUser.All

Notes

- When changing the ApeosWare Management Suite 2 main server host name, update the redirect URI host name to the main server host name after the change.
- When installing ApeosWare Management Suite 2, set the SSL configuration. If already installed, change the settings so that it uses an SSL configuration.
- When installing ApeosWare Management Suite 2, set the host name to FQDN. If already installed, change the settings so that it becomes FQDN.

Advance Setting When Using Login with Microsoft Entra ID

For authentication using Microsoft Entra ID, it is necessary to perform settings in advance, such as security, etc.

Before setting this up, please make sure you have two things in place

- Prepare at least one Microsoft Entra user with a "Microsoft Entra ID P1 or higher license". In the following steps, please use this Microsoft Entra user to configure Azure.
- To use Microsoft Entra Domain Services, a separate contract with Microsoft is required. Please refer to the Microsoft website for details.

Set the existing Microsoft Entra ID security value group

1. Access Microsoft Azure Portal (<https://portal.azure.com/>).
2. Sign in as the Security Administrator, Conditional Access Administrator, or the Global Administrator.
3. Click [Microsoft Entra ID] in the portal menu.
4. Click [Properties] .
5. Click [Manage security defaults].
6. Select [Disabled (not recommended)] under [Security defaults].
7. Click [Save].

Set the enterprise application

1. Access Microsoft Azure Portal (<https://portal.azure.com/>).
2. Sign in as the Security Administrator, Conditional Access Administrator, or the Global Administrator.
3. Click [Microsoft Entra ID] in the portal menu.
4. Click [Enterprise applications] on the left menu bar.
5. Click [New application].
6. Click [Create your own application].
7. Enter the application name in [What's the name of your app?].
8. In [What are you looking to do with your application?], select [Integrate any other application you don't find in the gallery (Non-gallery)], and click [Create].
The application will be added.



Note

The application ID displayed in the overview of the created application is used in domain creation. Record it in a memo or similar.

When a Microsoft Entra ID user that has been newly added using import of the Active Directory uses the linkage functions of ApeosWare Management Suite and Microsoft Azure, it is necessary to link them to the enterprise application.

9. Click [Assign users and groups] in [1. Assign users and groups].
10. Click [Add user / group].
11. Select the user to be registered, and click [Select].
To delete a selected user, click [Remove] against the user to be deleted.
12. Click [Get started] in [2. Set up single sign on].
13. Click [SAML].
14. Click [Edit] in [(1) Basic SAML configuration].
15. Enter [Identifier (Entity ID)] and [Reply URL], and click [Save].
[Identifier (Entity ID)]: Can be set as desired.
[Reply URL]: `https://{IP}/Login/MicrosoftEntraID/AzureResponse`



Note

- The set [Identifier (Entity ID)] and the [Login URL] of [(4) set up {Application name}] are used when creating a domain. Record it in a memo or similar.
- The value to be entered for "{IP}" of the [Reply URL] varies depending on whether or not the ApeosWare Management Suite host name is set on FQDN.
If the host name is set on FQDN: Enter the host name set in FQDN. Do not enter the IP address.
Authentication is not possible.
If the host name is not set on FQDN: Enter the "ApeosWare Management Suite server IP address" being used.
- The [Certificate (Base64)] of [(3) SAML Certificates] is used when creating a domain. Therefore download it.

Add the API access permission to the enterprise application created

1. Access the Microsoft Azure Portal (<https://portal.azure.com/>).
2. Sign in as the Security Administrator, Conditional Access Administrator, or the Global Administrator.
3. Click [Microsoft Entra ID] in the portal menu.
4. Click [App registrations] on the left menu bar.
5. Click [All applications], and select the registered app.
6. Click [Authentication] in [Manage] on the left side.
7. Click [Yes] on [Allow public client flows]>[Enable the following mobile and Desktop flows], and click [Save].
8. Click [API permissions] in [Manage] on the left side.
9. Click [Add a permission] > [Microsoft Graph] > [Delegated permissions] in that order.
10. Check [User] > [User Read], and click [Add permission].
The access permission will be added. At this time the access permission added is not yet activated.

11. Click [Grant admin consent for {Tenant name}] adjacent to [Add a permission].
12. Click [Yes] to indicate agreement.
The access permission added will be activated.

Creating Microsoft Entra Domain Services

1. Access Microsoft Azure Portal (<https://portal.azure.com/>).
2. Sign in as the Security Administrator, Conditional Access Administrator, or the Global Administrator.
3. Click [All resources] in the portal menu.
4. Click [Create].
5. Enter “domain” in the search box, and select [Microsoft Entra Domain Services] from the results displayed.
 **Note**
If [Microsoft Entra Domain Services] is not listed, select [Azure AD Domain Services].
6. Click [Create].
7. Set [Resource group], [DNS domain name], [Region], and [SKU].
[Resource group]: Can be set as desired.
[DNS domain name]: Set so that the number of characters is 15 or less.
[SKU]: Select an arbitrary SKU.
8. Click [Review + create].
 **Note**
For the other settings, it is not necessary to change them from the default settings.
9. Check the settings, and click [Create] > [OK] in that order.
Deployment starts. Creating can take up to a maximum of 1 hour.
A notification indicating the status of progress of deployment of Microsoft Entra Domain Services is displayed in the portal. If [Notifications] is clicked, the detailed status of progress of deployment is displayed.
10. When deployment is completed, click [Go to resource].
Microsoft Entra Domain Services is deployed.
 **Note**
Deployment of Microsoft Entra Domain Services takes time.
When provisioning of the managed domain is completed, the domain status is shown as [Running] in the [Overview] tab.
11. Click [Configuration diagnostics] in the left side menu bar.
12. Click [Run], and the configuration of the services of the managed domain created will be diagnosed.
 **Note**
If a problem arises in the diagnosis, click [Fix] to correct the setting that was causing the problem.

Installing Certificates for Secure LDAP

Refer to the following URL to set up Microsoft Entra Domain Services for Secure LDAP configuration.
<https://learn.microsoft.com/entra/identity/domain-services/tutorial-configure-ldaps>



Note

If the certificate used for Secure LDAP configuration corresponds to any of the following, please install a CA certificate on the ApeosWare Management Suite server.

- If the certificate cannot be confirmed as secure with the root certificate of the ApeosWare Management Suite server
 Install the root CA certificate corresponding to the certificate on the server
- If the certificate requires an intermediate certificate for authentication from the root certificate
 Store the CA certificate of the intermediate certificate authority on the server.
- If the server certificate is of a type that is not authenticated from the root certificate
 Store the CA certificate of the root certificate authority on the server.

Installing Certificates Required for Authentication (Base64)

1. Copy the Certificate (Base64) downloaded in “Set the enterprise application” (P.66) to the ApeosWare Management Suite environment.
2. Double click the copied certificate, and click [Install Certificate].
3. Select [Local Machine], and click [Next].
4. Set as follows.
 Select [Place all certificates in the following store].
 Enter “Trusted Root Certification Authorities” for the certificate store.



Note

When importing is completed, restart the ApeosWare Management Suite server. If the server is not restarted, errors will occur, such as when a domain is created, etc.

Performing the settings for Microsoft Entra Domain Services

Setting the Receiving Security Rules for Network Security Groups (aadds-nsg)

1. Access Microsoft Azure Portal (<https://portal.azure.com/>).
2. Sign in as the Security Administrator, Conditional Access Administrator, or the Global Administrator.
3. Click [All resources] in the left side menu bar.
4. Click [aadds-nsg].
5. Click [Inbound security rules] > [+Add] in that order.
6. Enter the setting items, and click [Add].
 Source: IP Addresses
 Source IP address / CIDR range: Can be set as desired.
 Source port range: *
 Destination: Any

Service: Custom
Destination port range: 636
Protocol: TCP
Action: Allow
Priority: 401
Name: AllowLDAPS

Setting the DNS Zone for External Access

1. Click [All resources] on the Microsoft Azure Portal home screen.
2. Click the DNS domain created at "Creating Microsoft Entra Domain Services" (P.68).
3. Note the address provided in "Secure LDAP external IP address."
Login to the ApeosWare Management Suite main server.
4. Open the hosts file in "C:\Windows\System32\drivers\etc".
5. Add the following sentence to the lowermost line of the file.
{IP} {Domain name}



Note

- For {IP}, enter that provided in "Secure LDAP external IP address" in procedure 3..
- Enter the DNS domain name created at "Creating Microsoft Entra Domain Services" (P.68) in {Domain name}.

Checking that the Microsoft Entra Domain Services settings are correctly set

1. Execute the command prompt with administrator authority on the ApeosWare Management Suite main server.
2. Execute the following commands.
dism /Online /Enable-Feature /FeatureName:TelnetClient
telnet{IP or domain name} 636



Note

For {IP or domain name}, enter that provided in "Secure LDAP external IP address" in procedure 9, or the DNS domain name created at "Creating Microsoft Entra Domain Services" (P.68).

3. Enter "ctrl +]", next enter "quit," and press <Enter>.
Terminate telnet.

Advance Setting When Using Login with a QR Code

It can be opened with [Service Settings] > [User Management] > [Authentication Settings] > [QR Code Login Settings] > [Mobile App Settings].

The function can be enabled from the setting screen for each service (ApeosWare MS Mobile 2 / AliPay / WeChat).

However, in the case of AliPay and WeChat, it is necessary to access each service and set it in advance.

Using [AliPay]

1. If you do not have an AliPay corporate account, access the AliPay account application page (<https://>

memberprod.alipay.com/account/reg/index.htm), then apply for and obtain a corporate account.

2. Access the Alipay open platform registration page (<https://open.alipay.com/platform/home.htm>).
3. Create an account using the Alipay application, or email address / telephone number.
4. Click [网页 / 移动应用 (Web / mobile application)], and access the Web / mobile application creation page.
5. Set the [应用名称 (Application name)], [应用图标 (Application icon)].
It is recommended that the [应用名称 (Application name)] is [ApeosWareManagementSuite].
6. Set the account you want to use in [绑定商家账号 (Business account binding)].
7. Select [网页应用 (Web application)] for the [应用类型 (Application type)].
The application ID will be displayed below the application name in the top left of the screen displayed after saving.
8. The application ID, which appears below the application name displayed in the top left of the screen after saving, will be displayed.
Set the application ID in the ApeosWare Management Suite.
9. Click the [开发设置 (Development settings)] button on the left side.
10. Click [接口加签方式 (Interface signature method)] > [设置 (Installation)] in that order.
 - (1) Select [密钥 (Secret key)] in [加签方式 (Signature method)] of [设置加签方式 (Set check-in method)].
 - (2) With [生成密钥文件 (Create key file)], create the [应用私钥 (Application secret key)] and [应用公钥 (Application public key)] automatically in accordance with the instructions on the screen.
Set the [应用私钥 (Application secret key)] in the ApeosWare Management Suite.
The [应用公钥 (Application public key)] is used in (4).
 - (3) Perform [安全验证 (Security verification)] in accordance with the screen.
 - (4) Enter the [应用公钥 (Application public key)] created in (2) in [上传 (Upload)], and click [确认上传 (Confirm upload)].
 - (5) Download the [支付宝公钥 (Alipay public key)] at [下载 (Download)], then set it in the ApeosWare Management Suite later.
11. Click [授权回调地址 (Permission call back address)] > [设置 (Installation)] in that order.
Set the following URL in [授权回调地址 (Permission call back address)].
<https://{FQDN of the ApeosWare Management Suite}:{Https Port of the ApeosWare Management Suite}/application/AuthService/sso/authorize>
12. After setting the above, click [提交审核 (Apply)], and the application for the app is completed.
13. Click [控制台 (Console)] menu > [网页 / 移动应用 (Web / mobile application)] tab in that order, to display a list of web / mobile applications.
14. Check that the status of the web application created is [已上线 (Online)].
If the status is [开发中 (Under review)], it is necessary to wait until the review is completed.
If the status is [已驳回 (Rejected)], check the reason for rejection from [详情 (Details)].
15. Click the [详情 (Details)] link on the web application created to display the Details page.
16. Click [产品绑定 (Product binding)] on the left side, next click [去绑定 (Binding)].
17. Click [获取会员信息 (Acquire member information)] > [确定 (OK)] in that order, and check [获取会员信

息 (Acquire member information)].

When the [获取会员信息 (Acquire member information)] status is [已开通 (Can be used)], the authentication function can be used.

Using [WeChat]

1. Access the [微信开放平台 (WeChat open platform)] (<https://open.weixin.qq.com/>) page.
2. After clicking the [网站应用 (Website application)] tab, click [创建网站应用 (Create website application)].
3. Set the [网站应用名 (Website application name)].
It is recommended that the [网站应用名 (Website application name)] is [ApeosWareManagementSuite].
4. Set the [应用官网 (Application official site)] to the following URL.
<https://{FQDN of the ApeosWare Management Suite}:{Https Port of the ApeosWare Management Suite}/application/AuthService/sso/authorize>
5. Download the website information registration table with [网站信息登记表扫描件 (Scan website information registration table)], enter the associated information, then print and seal it, and upload it.
6. Upload a 28*28 pixel image and a 108*108 pixel image at [网站应用图片 (Website application images)].
7. Click the [下一步 (Next)] button, and go to the [填写网站信息 (Enter site information)] tab.
8. Set the following FQDN in [授权回调域 (Authentication call back domain)].
{FQDN of the ApeosWare Management Suite}
9. Click [提交审核 (Submit for review)].
10. Click the [管理中心 (Management center)] menu > [网站应用 (Website application)] tab in that order.
[网站应用 (Website application)] will be displayed.
11. Check that the status of the [网站应用 (Website application)] created at [网站应用一览 (List of website applications)] is [已通过 (Passed)].
12. Click [查看 (Display)] on the web application created.
[应用详情 (Application details)] will be displayed.
13. Acquire the [AppID] and [AppSecret] below the web application name, and then set them in the ApeosWare Management Suite.
14. Click [申请开通 (Application open)] of [微信登录 (WeChat registration)], and open with the [微信登录 (WeChat registration)] function.

What if?

This section describes System Settings and Server Monitoring.

Rebuild Index in SQL Server

Rebuilds the SQL Server index if a message for providing notification regarding the index fragmentation occurrence in SQL Server is output to the Windows application log. Executing the command causes the index to be rebuilt for the table specified.

Execute this action while there is no problem with the operation, such as during the time of light ApeosWare Management Suite processing load.



Note

This operation is not available in case the database server is separated from the main server in distributed configuration.

1. Log on to the ApeosWare Management Suite server as an Administrators group user.
2. The command prompt window appears.
3. Enter the following command, and then press the <Enter> key.

```
cd {Installation folder}\WinSvc\Mon\bin
```

By default, {Installation folder} is "C:\Program Files\FUJIFILM\ApeosWare MS".

4. Enter the following command, and then press the <Enter> key.

```
awms_sqsrv_index_rebuild -d {Host name} -i {Instance name} -n {Port number} -u {User name} -p {Password} -t {Table name}
```

Available options are as follows. Option -d, -u, -p are mainly used for the configuration that the database is separated from. Also, during the installation of ApeosWare Management Suite, when SQL Server Express is installed automatically, you can omit the options -u and -p.

Option	Descriptions
-d {Host name}	Specify the host name of the database. If omitted, it is "localhost"
-i {Instance name}	Specify the instance name of the database. If omitted, it is "FXAW".
-n {Port number}	Specify the port number of the database from the range of 0 - 65535. If omitted, it is "1433".
-u {User name}	(Can be omitted when access is possible with Windows authentication) Specify the user name when connecting to the database using SQL Server Authentication. If this option is specified, -p is required to be specified as well.
-p {Password}	(Can be omitted when access is possible with Windows authentication) Specify the password when connecting to the database using SQL Server Authentication. If this option is specified, -u is required to be specified as well.
-t {Table name}	Specify the table name including the database name as the format of "{Database name}.{Schema name}.{Table name}". Entering this item is mandatory. You can check the fragmented table by "YYYY-MM-DD hh:mm:ss.xxx+0900 - 0054-250003-MON: Table with fragmented index is found. ({Database name}.{Schema name}.{Table name} index=xxxxx)" in the Windows application log. If there are multiple table names, separate them with comma to specify.

Example:

```
awms_sqsrv_index_rebuild -t  
DBName1.SchemaName1.TableName1,DBName2.SchemaName2.TableName2
```

The SQL Server index is rebuilt.

In the case of a normal completion, a message [Index fragmentation has been resolved. {Table name}] is displayed. The others are displayed, follow the message.



Note

It takes a long time to finish rebuilding.

Impossible to send email messages when an antivirus software has been installed

You may fail to send email when you install ApeosWare Management Suite on a PC with an antivirus software, such as McAfee VirusScan, installed. This occurs because the antivirus software is set to block email sending.

To make it perform normally, remove the following files from the settings to block email sending.

- C:\Program Files\FUJIFILM\ApeosWare MS\JRE\jave.exe
- C:\Program Files\FUJIFILM\ApeosWare MS\WinSvc\Mon\bin\MonSvc.exe

When distributed print servers are not displayed correctly after installation

If several distributed print servers are installed at the same time, they may not be set up correctly. If they are not set up correctly, re-install the print servers.

1. Remove the network cables of the print servers not displayed on the print server list screen.



Note

By removing the network cables, set a status in which the main server cannot be communicated.

2. Uninstall the print servers.



Note

In the "Do you want to keep the file in data storage location for future use?" dialog, select [No].

3. Connect the network cables to the print servers to set a status in which the main server can be communicated.
4. Re-install the print servers.
5. After the installation completion of the print servers, reboot the main servers.

3 Device Management

Settings and Confirmation in a Web Browser

You can set and confirm a device from a web browser. This section describes what you can do with each page.

- [Service Settings] > [Device Management]

Types of Pages	Descriptions
Device group list	
All device groups	Create and manage device groups that unify devices.  Refer "Device Group List (All Device Groups)" (P.76)
Details of device groups/sub-device groups	Add lower sub-device groups, a device and registration data (addresses, folders, IP addresses, filter domains) to a device group and sub-device group you have selected.  Refer "Device Group List (Details of Device Group/Sub-Device Group)" (P.90)
Device List	Register a device you searched to ApeosWare Management Suite and add it to a device group.  Refer "Device List" (P.95)
Settings	
Device automatic registration settings	Set a schedule at the time of device automatic registration settings  Refer "Device automatic registration settings" (P.99)
Settings of update conditions of device data	Setting time and intervals at which the setup content is updated to a device.  Refer "Settings of update conditions of device data" (P.100)

- [Device/Job Status] > [Device Status]

Types of Pages	Descriptions
Device Status	All device status is displayed.  Refer "Device Status" (P.100)

Types of Pages	Descriptions
Maintenance	Meter information on all devices is displayed. You can specify power-off of a device.  Refer "Maintenance" (P.104)
Remaining Toner	Remaining toner of all devices is displayed.  Refer "Remaining Toner" (P.104)
Remaining Paper	Remaining paper of all devices is displayed.  Refer "Remaining Paper" (P.105)
Drum Status	Displays the drum status of a device.  Refer "Drum Status" (P.106)
Status Notification Settings	Set notification conditions when you notify device status by e-mail.  Refer "Status Notification Settings" (P.107)
Job log collection status	Job log collecting status is displayed.  Refer "Job log collection status" (P.109)

Device Group List (All Device Groups)

How to Display

Select [Service Settings] > [Device Management] > [Device Groups] in the administrator screen menu.

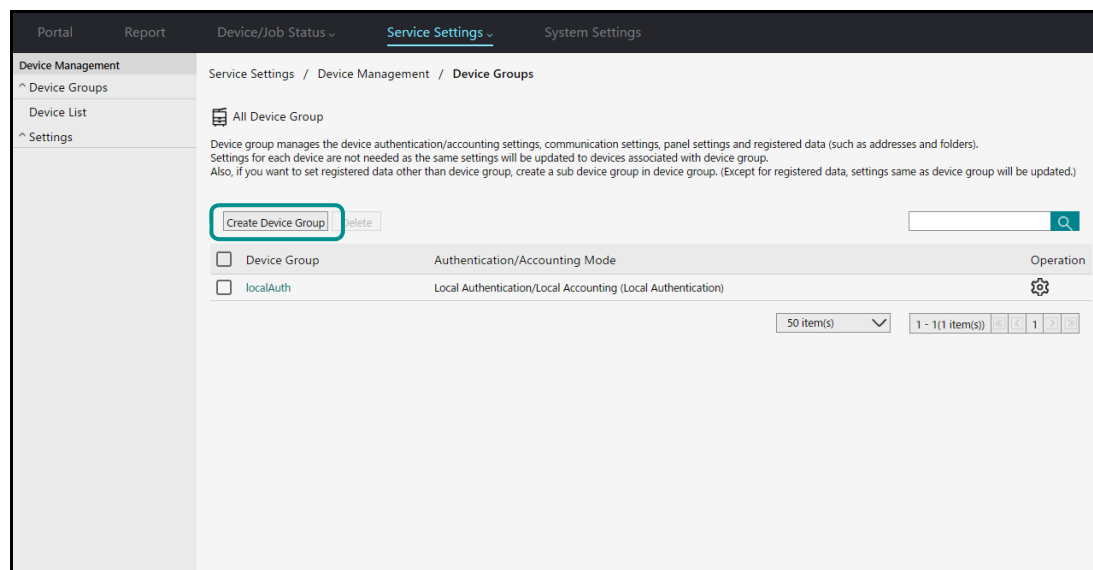
Page Summary

Create and manage device groups that unify devices. You can update to an actual device the addition of a device group, change and deletion of property, and setup information.

 Refer
"Device and Device Group Management" in "Installation and Operation Guide"

Add Device Group

Select [All Device Groups] in the side menu and click [Create Device Group].



(1)Basic settings

Specify the following item, and then click [Next].

The [Authentication/Accounting Settings] that you set here is applied to all devices affiliated with a device groups.

[Device Group Name]

Enter the device group name.

[Description]

Enter descriptions for the device group as necessary.

[Cost Management Settings]

- [Price Policy]

Set this item for cost management.

Select the price policy to be associated with a device group from the drop-down list box. If the price policy is not set for a device that is affiliated with a device group, the price policy you set here is applied.



Note

In the [Cost Management] menu too, you can associate a device group with the price policy. The same settings are applied in either operation.



Refer

For details on priority order of the price policy g → “Priority Order of the Price Policy” in “Installation and Operation Guide”

[Authentication/Accounting Settings]

- [Authentication/Accounting Mode]

Select the device authentication and accounting method from the following.

For details of each item, refer to “Authentication/Accounting Settings Type” in “Installation and Operation Guide”.

- Local Authentication/Local Accounting (Local Authentication)
- Local Authentication/Network Accounting (Network Authentication)
- Remote Authentication
- No authentication
- Off (Manage authentication in device)
- Custom Authentication



Note

- When [Authentication/Accounting Mode] is set to [Custom Authentication], confirm that the communication with TCP port number 8050 is allowed between the ApeosWare Management Suite server and the device in advance.
- Regarding the ports to be used for communication between the server and the related devices, refer to "Register the Port to the Router as an Exception" in "Setup Guide".
- If you use any device other than our products or Fuji Xerox's, add it to a device group for which you set [Off (Manage authentication in device)].
- If the authentication method settings on a device are set to "No authentication," you cannot use on-demand printing or guest printing from the ApeosWare Management Suite portal screen. If you wish to use on-demand printing or guest printing on a device set to use "No authentication," refer to the URLs in "Using the Web Applications Features" (P.121), and register the URLs for on-demand printing and guest printing in the external access settings of the device.

Other Settings

The main settings are as shown below. The setting items depend on the [Authentication/Accounting Mode] you have selected.



Note

- When the [Display Details] button is displayed, if you click it, the items are displayed.
- If you select [Off (Manage authentication in device)] in [Authentication/Accounting Mode], there are no setting items.

○: Setting

Blank: No setting

Setting Items	Local Authentication/Local Accounting	Local Authentication/Network Accounting	Remote Authentication (ApeosWare Authentication Agent)	Remote Authentication (Kerberos)	Custom Authentication	No authentication	Descriptions
Feature for authentication/ accounting mode	☐	☐				☐	Select a checkbox on the features for authentication and accounting. You can select multiple templates. • Copying • Printing • Scan • Faxing  Note For [Remote Authentication] and [Custom Authentication], all items of copying, printing, scanning, faxing are automatically set to [Yes].
Use of password	☐	☐	☐	☐		☐	To execute authentication of the user in a device, specify whether you use a password. If you use a password, select [Yes].  Note This setting is effective for users registered in the device itself. In the case with a remotely authenticated device, the password entry field is displayed in the general user authentication even if set to [No].
Allows printing without specifying users	☐	☐	☐	☐		☐	Select whether you allow a printing request without a user name and a specified password.
Alternate description of userID	☐	☐				☐	As necessary, change the description of [User ID] displayed when you push the <authentication> button in the control panel.

Setting Items	Local Authentication/Local Accounting	Local Authentication/Network Accounting	Remote Authentication (ApeosWare Authentication Agent)	Remote Authentication (Kerberos)	Custom Authentication	No authentication	Descriptions
Alternate description of accountID		☐				☐	As necessary, change the description of [AccountID] displayed when you push the <authentication> button in the control panel.
Storage location of authentication information		☐					Select the storage location of authentication information from [Hard Disk], [NVM]. NVM stands for non volatile memory.
Verification of authentication information		☐					Select whether to verify authentication information.
Verification of printing/direct fax		☐					Select whether to verify authentication information for print jobs and direct fax.
User input items		☐					Select the items you can enter in the control panel of the device for authentication. • User ID and AccountID • User ID only
Authentication system settings			☐	☐			Select software for authentication. Select [ApeosWare Authentication Agent] if you have ApeosWare Management Suite as the authentication server.
Primary Server IP Address/Host Name			☐		☐		Select the IP address or host name of the primary server.
Communication Protocol			☐		☐		Select the communication protocol from [HTTP] and [HTTPS].  Note It is recommended to select [HTTPS] and operate with communication with the ApeosWare Management Suite server encrypted.

Setting Items	Descriptions				
	No authentication	Custom Authentication	Remote Authentication (Kerberos)	Remote Authentication (ApeosWare Authentication Agent)	Local Authentication/Network Accounting
	Local Authentication/Local Accounting				
Port Number		☐		☐	The port number is displayed.  Note If not especially required, use the port number as is.
Guest Account Information			☐		Select whether to use the guest account. When you select [Yes], set the guest account password.
Kerberos server 1 to 5			☐		Enter the authentication server name, the host name and port number of primary server, and the host name and port number of secondary server.
The number of times of retry		☐			Set how many times you retry until it is determined as offline when the device cannot connect to ApeosWare Management Suite.
Use Secondary Server		☐		☐	Select whether to use the secondary server. When you enter [Yes], set the IP address or host name of the secondary server, the communication protocol, and the port number.  Note If not especially required, use the port number as is.

Setting Items	Descriptions					
	No authentication	Custom Authentication	Remote Authentication (Kerberos)	Remote Authentication (ApeosWare Authentication Agent)	Local Authentication/Network Accounting	Local Authentication/Local Accounting
		☐				
		☐				
		☐				
		☐				
Require PIN/Password Input		☐				
Access device that cannot connect to network		☐				
FUJIFILM BI Direct Federation Settings	☐	☐	☐	☐	☐	☐



Refer

"Installation and Operation Guide"

(2) Communication Settings

The information set here is applied to all the devices that are affiliated with a device group. However, if you set a device separately, the setting for the device is prioritized.

[Administrator Information Settings]

Specify the device administrator ID and a password.

[SNMP Settings]

Set the SNMP protocol, port number, and communication timeout time for searching a device.



Note

If not especially required, use the port number as is.

- **SNMP v1/v2**
Set the community name, port number, and communication timeout time.



Note

If the protocol is [SNMP v1/v2] in any device other than our products or Fuji Xerox's, be sure to enter [Community Name (Read/Write Only)]. Otherwise, you cannot retrieve device status.

- **SNMP v3**
Set the authentication user name, the authentication method and password, the encryption method and password, the port number, and the communication timeout time.

[Other Communication Settings]

Enter the SOAP port number and HTTP port number.

The HTTP port number is used in Internet Services.



Note

If not especially required, use the port number as is.

Status Monitoring Settings

- **[Monitor Status]**

Specify whether to monitor device status.

If you monitor it, select [Yes] and specify the following.

- **[Status Monitoring Interval]**
Enter intervals at which you monitor a device. The contents of the [Device Status] page and [Maintenance] page are automatically updated and displayed at intervals you specifies here.
- **[Retrieve device status when SNMP trap is received]**
If you get device status upon receipt of notification of status change (SNMP trap) from the device, select [Yes].
If you retrieve device status on a periodic basis, select [No].

Job Log Collection Settings

- **[Collect Job Log]**

Specify whether to collect a device's job logs.

To collect job logs, select [Yes] and specify the next.

- **[Collection Interval]**
To collect job logs at specified intervals, select [Specify by minutes] and specify collecting intervals (minutes).
To collect job logs at specified intervals every day, select [Specify by days] and specify collecting time.



Note

- If you add a device, the first job log collecting is executed when the device and communication are established and status is updated. After the first collecting, [Collection Interval] set here is executed.
- In the [Device/Job Status] > [Device Status] > [Job Log Collection Status] page, you can confirm whether there is an omission about a job log.



Refer

“Job log collection status” (P.109)

- [Job Logs for Collection]
For the first collecting, select either of [Job logs created after model is identified] or [All job logs in device] for collecting.
After the first collection, only job logs that are newly added after the previous collection are collection targets.



Refer

“Job Log Settings” in “Installation and Operation Guide”

Image Log Control Settings

Displayed when ApeosWare Management Suite 2 Image Log Management Option Receiving Server License is enabled.

- [Image Log Control]
Select whether or not to conduct image log control.
If you conduct image log control, select [Yes] and specify the following items.
- [Assurance Level]
Select [High] or [Low] as the level to guarantee creation of image data that is controlled as logs.
When [Low] is selected, image data may not be created according to circumstances.
- [Resolution]
Select the resolution.
The resolution affects the accuracy of OCR. To enhance the accuracy of OCR, it is recommended to set higher resolution.
- [Page Range]
Select the page range.
- [Image Log Target]
When conducting image log control, select a checkbox for the features that are image log control targets.
- [Transfer Image Log]
Select whether or not to transfer image log. If you conduct image log control, select [Yes].
- [Transfer Destination]
Select the transfer destination from a list of the IP addresses of the installed receiving servers.
- [Transfer Protocol]
When [Transfer Image Log] is [Yes], select the transfer protocol. When [HTTPS] is selected, [Port Number] is changed to [443].
- [Port Number]
Enter the port number.
- [Assurance Level]
Select [High] or [Low] as the level to guarantee transfer of created image logs to the server.
Image logs that are not transferred for some problems are saved in the device as “unsent logs.”
When the number of unsent logs exceeds the maximum image logs that can be stored in the device, they are processed as shown below.

- [High]: The device stops accepting new jobs.
- [Low]: Old image logs are deleted.
- [Logs to Transfer]
When [Assurance Level] is [High], select Logs to Transfer. In the case of [Low], [Accumulate & Transfer] is displayed, and it cannot be changed.
- [Transfer Timing]
When [Logs to Transfer] is [Accumulate & Transfer], select the transfer timing. When selecting [Schedule Transfer], set the transfer time.

Print Settings

- [Retrieve Device Job Status]
Specify whether to monitor jobs.
- [Retrieve Device Status]
Specify whether to monitor device status.
- [Communication Protocol]
Select the communication protocol when sending the print job to the device. When [Communication Protocol] is [IPP] or [IPPS], enter the IPP/IPPS port number.



Note

[IPP] and [IPPS] can be selected when Cost Recovery Option is not added to Entry Edition of ApeosWare Management Suite, and when the Cost Recovery function is not installed in the Enterprise Edition.

(3) Device panel settings and registered data management

The information you set here is applied only to a device just under the group (exclusive of lower sub-device groups).

[Device Panel Settings]

These items can be set when [Authentication/Accounting Mode] is one of the following.

- [Local Authentication/Local Accounting (Local Authentication)]
- [Local Authentication/Network Accounting (Network Authentication)]
- [Remote Authentication] (select [ApeosWare Authentication Agent for] the authentication system)
- [Custom Authentication]

Add the menu buttons to access ApeosWare Management Suite features to the home screen of a device.

- [Device Menu]
Set to [Display] the features to add to the device home screen.
- [Server URL]
Enter the server's URL for access to each feature.

In default settings, ApeosWare Management Suite server's URL that you are visiting is displayed. For operation of a number of servers, change to [Server URL] as necessary.



Note

- The custom service is used for this feature. To use the custom service, settings are necessary in the device. For details, refer to the "Using Custom Service" (P.120).
- In some models, you cannot use the custom service. In that case, you can access ApeosWare Management Suite from a device using the external access feature. Refer to "Using the Web Applications Features" (P.121).



Refer

"Device Home Screen" (P.113)

[Manage Registered Data]

To manage registration data in a device, select a checkbox on the relevant items in [Type of Registered Data to Manage]. You can manage the following items.

- Address
- Folder
- IPv4 Address Filters
- IPv6 Address Filters
- Filter domains (domain allowing transmission and reception or not)



Note

- If you select the checkbox for [IPv4 Address Filters] or [IPv6 Address Filters], be sure to add ApeosWare Management Suite server's IP address to the IP address on the setting page of device group or sub-device group. Otherwise, the server will not be able to be connected to a device.
- When you uncheck the checkbox for [Type of Registered Data to Manage] and perform Update Device, the settings in the device are deleted.



Refer

"Manage Registered Data" in "Installation and Operation Guide"

(4) Security Monitoring Settings

The expectation values for security monitoring settings will be configured in the device when the values are updated to the device.

[Category]

Select the category you want to enable/disable monitoring and set the expectation values. The following is a list of categories that are shown.

- User Authentication and Permissions
- Protect Management Feature
- Stop Unnecessary Network
- Protect Communication Data
- Protect Saved Files in Device
- Prevent Setting and Operation Errors
- Protect Device Software
- Log Management and Protection

Setting Items

After you select a category, selecting [Monitor] will display the setting items corresponding to the category.

For details of each setting item, refer to the device manual.

Also, the settings will not take effect with the devices that do not have features you specified in the setting item.

For availability of your specified features, check the device manual and the device settings.

(5) Associate With a Device

[Associate With Devices]

[On]

When adding a device to the device group, select [On], and select the device to permit use according to the following procedure.

(1) Click [Add] to display the [Add Device] dialog box.

(2) Attach the check mark to the device that you wish to add, and then click [Save].



Note

- When you remove the check mark for [Display Unaffiliated Device(s) Only], all the devices are displayed.
- Selecting a device affiliated with another device group causes an affiliated device group transition.

[Off]

Select when you are not adding a device.

(6) Overview

After you check the configured settings, clicking [Save] will create the device group.

You can click [Edit] for each item to change the settings.

Checking Device Group Information

Click  of the device group to be edited in the list and select [Properties].

You can check and edit the content configured for the device group. You can edit the items of some features in "Add Device Group" (P.77).

Update device information in a device group to an actual device

Click  of the device group to be updated in the list and select [Update].

The [Update Device] dialog box is displayed.

Update the setup information to an actual device. Only a device just under the device group that you selected in the list is updated (not a lower sub-device group).

Update method

- [Update Refreshed Settings Only]

Only information that has been changed since the previous update is updated.

- [Overwrite All Settings]

All information is updated. Select when you have changed the authentication method or if a mismatch has occurred with the setting content.

[Update]

Click when you operate update. After the device is updated, the [Device Update Result] dialog box is displayed.

[Device Update Result] Display items in the dialog box

Device Name, Location, Model, Network, Device Group, Update Status, and Update Reason are displayed.

Update Reason is displayed when the update status is wait retry, updated, or update failed.

The update status and descriptions are as follows.

Update Status	Descriptions
Update Canceled	Update has been aborted because of one of the following reasons. • An administrator clicked [Aborted] while operating update. • An error occurred in ApeosWare Management Suite. • [Failed (Service Error)] was occurring.
Not completely updated	Information set in ApeosWare Management Suite is not completely updated to a device.
Differences are being calculated	Information to be updated is being calculated before update.
Being updated	Processing update
Wait retry	Not powered or no communication.
	A device port is not activated.
	Because other processes are being performed such as doing jobs or operating the device control panel, update is not available.
	Because another software is updating, update is not available.
	Rebooting failed.
	Items that are not suitable for the device are set.
Updated	Update has been successfully completed.
	Some information has been updated. Some information has not.
Update failure	Authentication failed in a device administrator or SNMP.
	Items that are not suitable for the device are set.
	The signature verification of the device plug-in/custom service setting is valid, so it cannot be updated. If using the custom authentication or custom service, the signature verification must be set to be invalid.
	Failure for some reason other than above.
Failure (service error)	An service error occurred. Reboot ApeosWare Management Suite Core Service.

Check of update status details

You can check for each device.

Click the link of Device Group in the list. Display the [Device] tab, click  of the device that you wish to check, and select [Update Status Details].

The [Update Status Details] dialog box is displayed, and you can check the update status details.

[Device Name]

The name of the selected device is displayed.

[IP Address/Host Name]

The IP address or the host name of the selected device is displayed.

[Date/Time Updated]

The date and time of last execution of Update Device is displayed.

[Update Status]

The status of update to a device is displayed.



“[Device Update Result] Display items in the dialog box” (P.87)

[Reason]

The reason for update status is displayed.

The reasons and descriptions are as follows.

Reason	Descriptions
-	None.
Power Off/ Communication Error	Not powered or no communication.
Port Inactivated	A device port is not activated.
In Use	Because other processes are being performed such as doing jobs or operating the device control panel, update is not available.
Unacceptable	Because another software is updating, update is not available.
Rebooting Failed	Rebooting failed.
Unsupported Device	Items that are not suitable for the device are set.
Ready	Update has been successfully completed.
Skipped	Some information has been updated. Some information has not.
Authentication Failed	Authentication failed in a device administrator or SNMP.
User Synchronization Error	The signature verification of the device plug-in/custom service setting is valid, so it cannot be updated. If using the custom authentication or custom service, the signature verification must be set to be invalid.
Other Errors	Other reason than failure in authentication, unsupported, or user synchronization error.

The details displayed in the [Update Status Details] table are as follows.

[Error Level]

The error level is displayed.

[Category]

The category of the error is displayed.

[Subcategory]

The identifier is displayed only if the details of the error-occurred category can be identified.

[Message]

The detail of the [Error Level] is displayed.

Deleting device groups

Click  of the device group to be deleted in the list and select [Delete].

Even if you delete a device group, [Authentication/Accounting Settings] of a device that has been affiliated with the device group remains.

If you delete a device group, the following information is deleted from an affiliated actual device too.

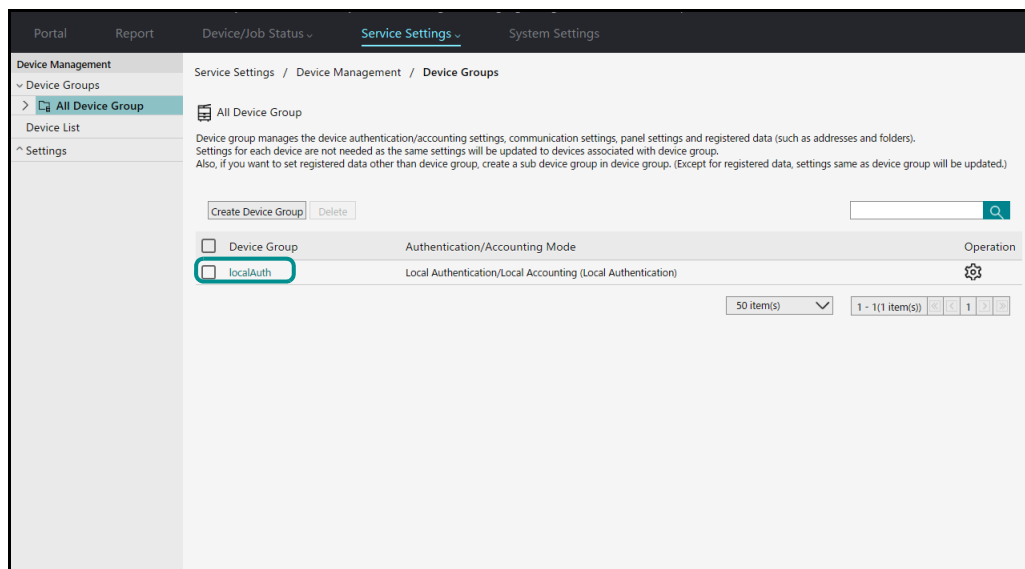
- Address
- Folders and inside documents
- IP address

- Filter domains

Device Group List (Details of Device Group/Sub-Device Group)

How to Display

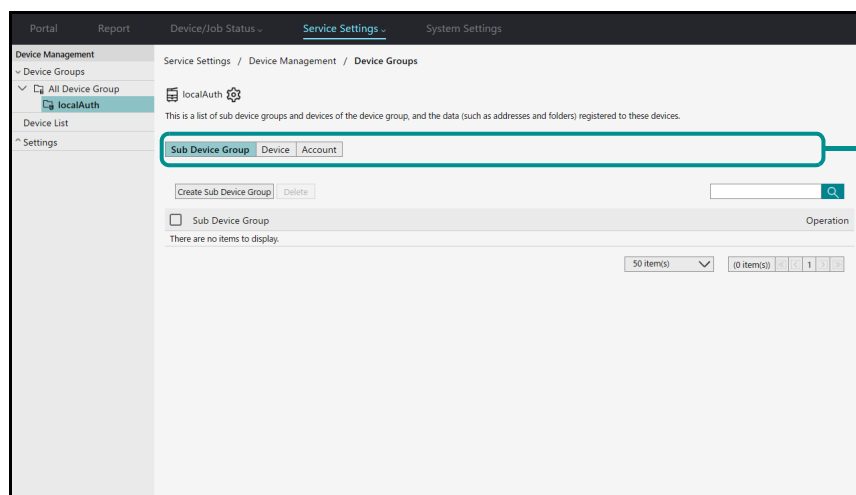
Click existing device groups and sub-device groups in the side menu, or click the names of groups in the device group list.



Page Summary

Add lower sub-device groups, devices, registration data (addresses, folders, IP address, filter domains) to the device group and sub-device group you have selected.

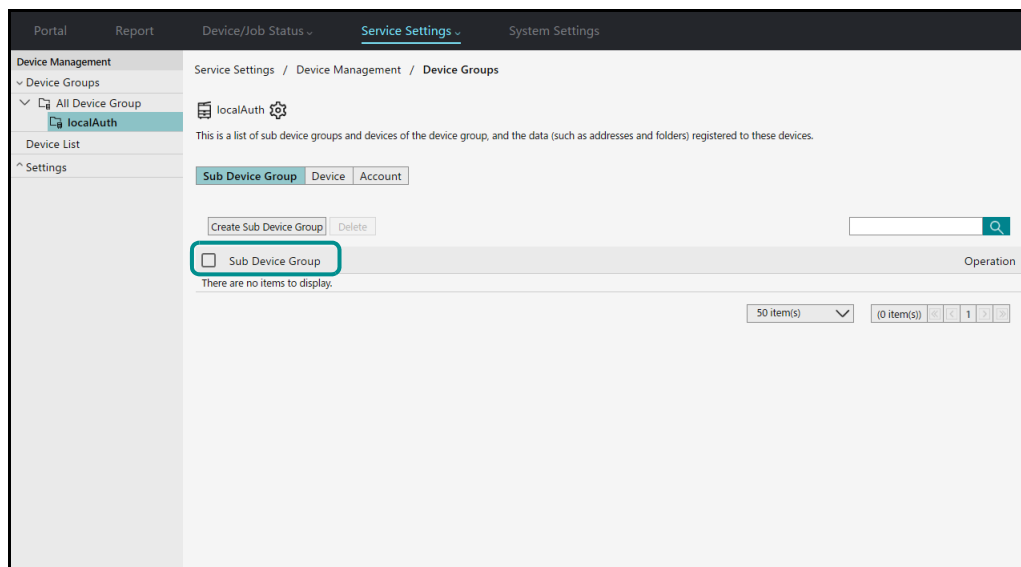
For registration data tabs, only the items with a checkbox selected for [Type of Registered Data to Manage] are displayed.



Registration Data Tabs
(Only the items with a
checkbox selected for
[Type of Registered Data to
Manage] are displayed.)

Creating Sub-device Group

Display the [Sub Device Group] tab and click [Create Sub Device Group]. Add a lower sub-device group to the device group (or sub-device group) you have selected.



(1) Basic Items

Specify the following item, and then click [Next].

[Sub Device Group Name]

Enter the sub-device group name.

[Description]

As needed, enter descriptions for the sub-device group.

Cost Management Settings

- [Price Policy]

Set this item for cost management.

Select the price policy to be associated with a sub-device group from the drop-down list box. If the price policy is not set to a device that is affiliated with a sub-device group, the price policy you set here is applied.



Note

In the [Cost Management] menu too, you can associate a sub-device group with the price policy. The same settings are applied in either operation.



Refer

“Priority order of the price policy” in “Installation and Operation Guide”

Device Group Information

The information set in the selected device group is displayed. Clicking [Display Details] displays the information that is set as Authentication/Accounting Feature.

You can set the following items only when [Authentication/Accounting Mode] of the device group that the sub-device group is affiliated with is [Custom Authentication].

- The number of times of retry
Set how many times you retry until it is determined as offline when you cannot connect to ApeosWare Management Suite.
- [Require PIN/Password Input]
You can set this item only when [Authentication/Accounting Mode] of the device group that a sub-device group is affiliated with is [Custom Authentication].
Set whether you use PIN or a password at the time of authentication. Select a checkbox if you use it.
The setup content is applied when you select [Follow Device Group Settings] in [Require PIN/Password Input] of access profile associated with a user.
- [Access device that cannot connect to network]
You can set this item only when [Authentication/Accounting Mode] of the device group that a sub-device group is affiliated with is [Custom Authentication].
Specify whether to allow a device to be used even when it cannot connect to ApeosWare Management Suite server because of a network failure, etc. If you allow it, select a checkbox.
However, authentication with a offline device is available only with the card authentication. This enables the card authentication and authentication by user ID input for an offline device. Moreover, in offline, you can only use a single feature of the actual device such as copy or fax.
For offline users, [Access device that cannot connect to network] in access profile needs to be set to [Allow].
You can register up to the maximum of 10,000 users.



Refer

"Installation and Operation Guide"

FUJIFILM BI Direct Federation Settings

The information set in the selected device group is displayed.

(2) Device panel settings and registered data management

The information you set here is applied only to a device just under the group (exclusive of lower sub-device groups).

[Device Panel Settings]

These items can be set when [Authentication/Accounting Mode] of the device group that a sub-device group is affiliated with is one of the following.

[Local Authentication/Local Accounting (Local Authentication)]

- [Local Authentication/Network Accounting (Network Authentication)]
- [Remote Authentication] (select [ApeosWare Authentication Agent for] the authentication system)
- [Custom Authentication]

Add the menu buttons to access ApeosWare Management Suite features to the home screen of a device. For details of each item, refer to "Add Device Group" (P.77) "(3) Device panel settings and registered data management".

[Manage Registered Data]

Select a checkbox for the items to manage in a device. The setting of an affiliated group is displayed in default setting. You can manage the following items.

- Address
- Folder

- IPv4 Address Filters
- IPv6 Address Filters
- Filter domains (domain allowing transmission and reception or not)

**Note**

If you select the checkbox for [IPv4 Address Filters] or [IPv6 Address Filters], be sure to add ApeosWare Management Suite server's IP address to the IP address on the setting page of device group or sub-device group. Otherwise, the server will not be able to be connected to a device.

**Refer**

"Manage Registered Data" in "Installation and Operation Guide"

(3) Associate With a Device

[Associate With Devices]

[On]

When adding a device to the sub-device group, select [On], and select the device to associate according to the following procedure.

(1) Click [Add] to display the [Device] dialog box.

(2) Attach the check mark to the device that you wish to add, and then click [Save].

**Note**

When you remove the check mark for [Display Unaffiliated Device(s) Only], all the devices are displayed.

[Off]

Select when you are not adding a device.

(4) Overview

After you check the configured settings, clicking [Save] will create the sub-device group.

You can click [Edit] for each item to change the settings.

Checking Sub Device Group Information

Click  of the sub-device group to be edited in the list and select [Properties].

You can check and edit the content configured for the device group. You can edit the items of some features in "Add Device Group" (P.77).

Updating information on a device in a sub-device group to an actual device

Display the [Sub Device Group] tab. Click  of the sub-device group to be updated in the list and select [Update].

Update the setup information to an actual device. Only the device just under the device group that you selected in the list is updated (not a lower sub-device group).

Update method

- [Update Refreshed Settings Only]

Only information that has been changed since the previous update is updated.

- [Overwrite All Settings]

All information is updated.

[Update]

Click when you operate update.

[Device Update Result]

Refer to “Update device information in a device group to an actual device” (P.87).

Delete sub-device groups

Display the [Sub Device Group] tab. Click  of the sub-device group to be deleted in the list and select [Delete].

If you delete a sub-device group, the following information is deleted from an affiliated actual device too.

- Folders and inside documents
- IP address
- Filter domains
- Address

Checking and Changing Device Information

Click the [Device] tab.

The list of the device affiliated with the device group you have selected (or sub-device group) is displayed. You can check the update status of the device, reason of update, and security monitoring results.

When you check and change the information of each device, click  and select [Properties]. You can change the same items as in “Checking and Changing Device Information” (P.97).

Add Device

Click the [Device] tab.

When you click [Edit List, property of the group is displayed and you can add a device.

Adding addresses

Display the [Recipient] tab.

The list of the recipients set in the device group (or in the sub-device group) selected is displayed. To add a recipient, click [Add Recipient]. Specify recipient information by fax, IP fax (SIP), Internet fax, e-mail, server.



Note

The options loaded in a model and device do not allow you to set some devices.

Adding folders

Display the [Folder] tab.

The list of the folders set in the device group (or in the sub-device group) selected is displayed. To add a folder, click [Create Folder] and specify the following information.

[Access Restriction]

Select how to restrict access to a folder.

[Specify Owner]

If you click [Select], the [Select Owner] dialog box is displayed. In [Access Profile] of the [Select Owner] dialog box, access profile associated with a device group (or sub-device group) is displayed. When you select access profile, associated users are displayed, so select a user you want to be the owner of folders.

**Note**

- When the user you specified as the owner of folders is deleted, folders and documents inside them are deleted.
- If the owner of folders is changed, the owner's documents before change are deleted.
- If you delete folders, documents inside them are deleted.

[Processing after document is retrieved]

Specify whether those documents are automatically deleted after you take out documents from folders.

[Processing after retention period has passed]

Specify whether you delete reserved documents when retention period set in a device is over.

Adding IP addresses

Display the [IPv4 Address Filters] tab or the [IPv6 Address Filters] tab.

The list of the IP addresses set in the device group (or in the sub-device group) selected is displayed. To add an IP address, click [Create IPv4/v6 IP Filters] and specify information on the IP address of the PC to be allowed to be connected to a device.

**Note**

When you set [IPv6/v4 Address Filters] to be managed in [Type of Registered Data to Manage] of a device group you have selected (or sub-device group), be sure to add ApeosWare Management Suite server's IP address to the IP address. Otherwise, the communication between ApeosWare Management Suite and the device will be impossible (the IP address of ApeosWare Management Suite server is not added in the default settings).

Add domains that allowing/not allowing transmission and reception

Display the [Filter Domains] tab.

The list of the filter domains set in the device group (or sub-device group) you have selected is displayed. To add an filter domain, click [Create Filter Domain].

When you set [Specify Allowed Domains] in [Type of Registered Data to Manage] of the device group (or sub-device group) you have selected, add the domain in which a device allows reception of e-mail. When you set [Specify Blocked Domains] in [Type of Registered Data to Manage], add the domain in which a device does not allow transmission and reception of e-mail.

Display an account

Display the [Account] tab

The list of the accounts associated with the device group that you have selected (or the sub-device group) is displayed.

**Note**

You can set an account with [Service Settings] > [Cost Management] in the administrator screen.

Device List

How to Display

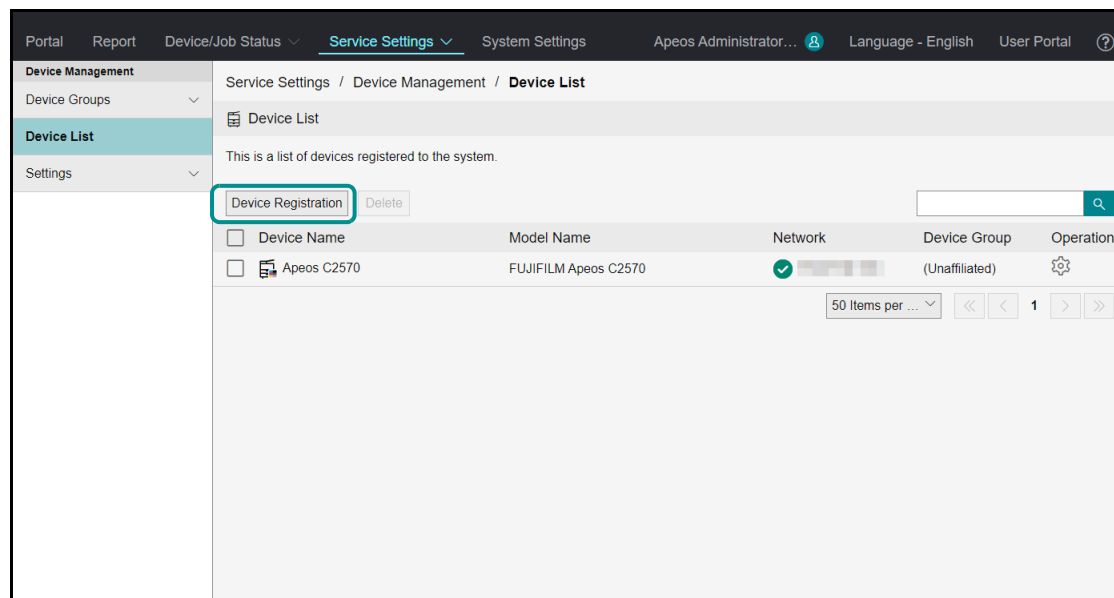
Select [Service Settings] > [Device Management] > [Device List] in the administrator screen menu.

Page Summary

Register a device you searched to ApeosWare Management Suite and add it to a device group. You can register a device, and change and delete property.

Device registration

Click [Device Registration]. The main settings are as shown below.



(1) Select a device

Specify a device to register in ApeosWare Management Suite, and then click [Next].

You can select from a device that is detected after searching a network automatically or you can directly enter the IP address of a device to register. Clicking on [Device Search Method/Specify Method Settings] enables you to select either searching a device on the network or entering the information manually.



Note

If entering the IPv4 address into the IP address of the device to be registered or host name, do not place 0 before the value of the address.

(2) Device Group/Cost Management Settings

[Select device group to associate the device]

Select a device group or sub-device group to affiliate a device with.

[Device Group Information]

The information of device group to affiliate the device with is displayed.

[Price Policy]

Select the price policy to be associated with a device for cost management.



Note

- [Price Policy] is displayed in the [Others] tab in the device property screen.
- In the [Cost Management] menu too, you can associate a device with the price policy. The same settings are applied in either operation.



Refer

“Price Policy” in “Installation and Operation Guide”

(3) Communication Settings

Specify the following item, and then click [Next].

When you specify the device group (or the sub-device group) that is affiliated with a device in [Select device group to associate the device] of “(2) Device Group/Cost Management Settings”, set whether the communication settings of the affiliated group are carried over.

If the communication settings of the affiliated group are carried over, select [Common Settings with Device Group].

If communication settings are separately specified for a device, select [Individual Settings] and specify the following items.

[Administrator Information Settings]/[SNMP Settings]/[Other Communication Settings]/[Status Monitoring Settings]/[Job Log Collection Settings]/[Image Log Control Settings]/[Print Settings]

For details on these settings, refer to “Add Device Group” (P.77) > [(2) Communication Settings].

[Print Server Linkage]

Specify whether to link the print server. To link the print server, select [GP Controller] in [Print Server Linkage], and then enter the [IP Address/Host Name] and [LPR Queue Name].

To perform a print server linkage test print, click [Print].

(4) Overview

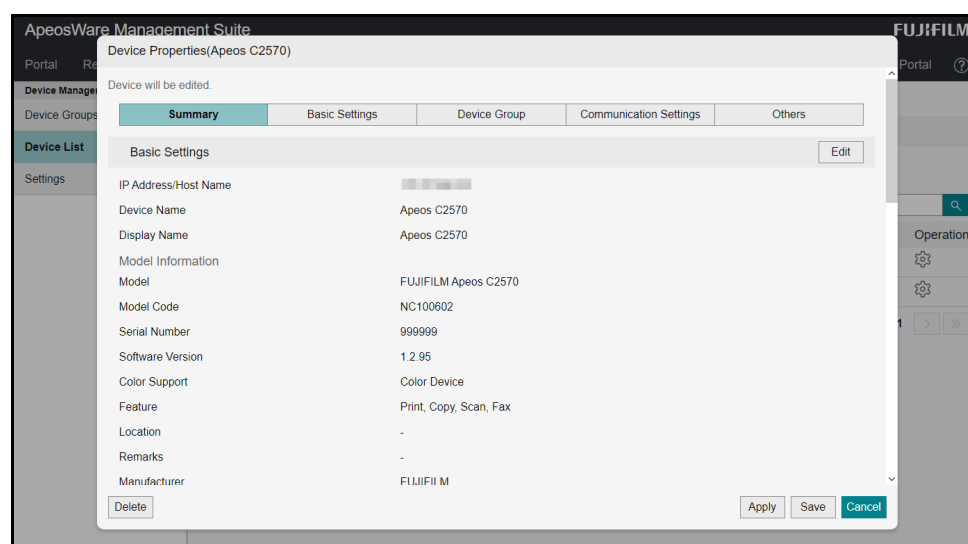
After you check the configured settings, clicking [Save] will register the device.

You can click [Edit] for each item to change the settings.

Checking and Changing Device Information

Click  in the device list and select [Properties].

You can display and edit the content configured for the device. The items you can display and edit are the functions set in “Device registration” (P.96), security monitoring results, and others (cost management settings and external terminal settings).



[Security Monitoring Results]

The monitoring target security settings are displayed in the list.

- [Category]
The category specified in [Create Device Group] > [Security Monitoring Settings] is displayed.



Refer

- For [Create Device Group], refer to “Add Device Group” (P.77).
- “[Category]” (P.86)
- [Attribute Name]
The attribute name that belongs to [Category] is displayed.
- [Current Value]
The attribute value obtained from the device by device security monitoring is displayed. This field becomes blank when device security monitoring is not supported or device security monitoring cannot be obtained.
- [Expected Value]
The attribute value of Security Monitoring Settings specified to the device group to which the device belongs is displayed.
- [Security Monitoring Results]
 - [Match]
This is displayed when [Current Value] and [Expected Value] are matched.
 - [Mismatch]
This is displayed when [Current Value] and [Expected Value] are not matched.
 - [(Unsupported)]
Displayed when the target attribute is not supported.

[Others]

- Cost Management Settings
You can select a registered price policy.
- External Terminal Settings
This is displayed when one or more valid CAL licenses of external terminals exist.
When using an external terminal, associate it with the device. Select an external terminal to use from the drop-down list in the [External Terminal] field and then specify the IP address of the external terminal to be associated with the device in [IP Address].
Connect the external terminal via network. The IP address of an external terminal must be a fixed IP or IPv4.

Delete a device

Click  of the device list and select [Delete].

Perform this action when you want to put a device out of the management of ApeosWare Management Suite or when you have removed a device.



Note

- Even if you have removed information of a device from ApeosWare Management Suite, the information written in the actual device by an updating operation remains unchanged.
- A same external terminal cannot be associated with multiple devices.

Device automatic registration settings

How to Display

Select [Service Settings] > [Device Management] > [Settings] > [Device Auto Registration Settings] from the menu on the administrator screen.

Page Summary

Set device automatic registration settings. When automatic registration is enabled, ApeosWare Management Suite searches devices on a network and registers any unregistered device automatically (in default settings, schedules are not set).

Make sure about the following things before you start.

- Power on a device
- The following ports are activated on a device
 - SOAP port
 - SNMP port
 - WSD port (only when you select WSD in protocol to be used for search)
- The ApeosWare Management Suite server is not rejected by IP filters.



Note

WSD stands for Web Services on Devices.

Device automatic registration settings

[Auto Registration Schedule]

When you search and register a device at specified time automatically every day, select [Specify by days] and specify time of day.

When you search and register a device automatically once a week, select [Specify by weeks] and specify day of the week and time of day.

If you do not register a device automatically, select [Do not perform].

[If operating using dual stack, add IPv6 mode information first]

When you add IPv6 mode information first before the other during the dual stack operation of IPv4 and IPv6, select a checkbox.

[Replace IP address with host name for the device to be added]

Select a checkbox when you change the IP address of the device to add to a host name.

[Search Settings for Auto Registration]

When you set conditions on which you search, click [Set] and specify protocols that you use for search, a search method and communication timeout.

Settings of update conditions of device data

How to Display

Select [Service Settings] > [Device Management] > [Settings]> [Device Data Condition Update Settings] from the menu on the administrator screen.

Page Summary

Set intervals, time of day, and a retry method so that you can update to an actual device the information of a device which you add, change, and delete in ApeosWare Management Suite.

Set update conditions of device data

[Auto Update Schedule]

To update the setup information to a device on a periodic basis, select [Specify by minutes] and specify [Update Interval].

To update the setup information to a device at specified time every day, select [Specify by days] and specify the time to update to a device.

If you do not want to update to a device on a periodic basis, select [Do not perform].

[Restart when update failed]

Specify whether you retry or not when update fails.

- Update to a device can fail when the same user ID or card ID is registered in a device. Some of the user IDs or card IDs are updated to a device in the first update and other user information can be successfully updated in the second update.
- If an error occurs, with [Restart when update failed] set to [Off], in update to a device at specified intervals and time of day, correct the error information and update to a device manually. Just correcting the error information is not enough to update to a device automatically. If you update manually once, automatic update is performed according to the setting thereafter.
- If update to a device fails with an error resulting from the same card ID registered in a device, you can avoid an error by changing the value of files set.



Refer

"When user information is not updated because of registered card ID" (P.124)

Device Status

How to Display

Select [Device/Job Status] > [Device Status] > [Device Status] from the menu on the administrator screen.

Page Summary

Display the status list of registered devices. You can select a status and extract a device for display. There are following types of device status.

Status	Descriptions
	Normal status.
	A phenomenon is occurring at error level.
	Some phenomenon (paper jam) is occurring at a error level.
	Some phenomenon is occurring at a warning level.

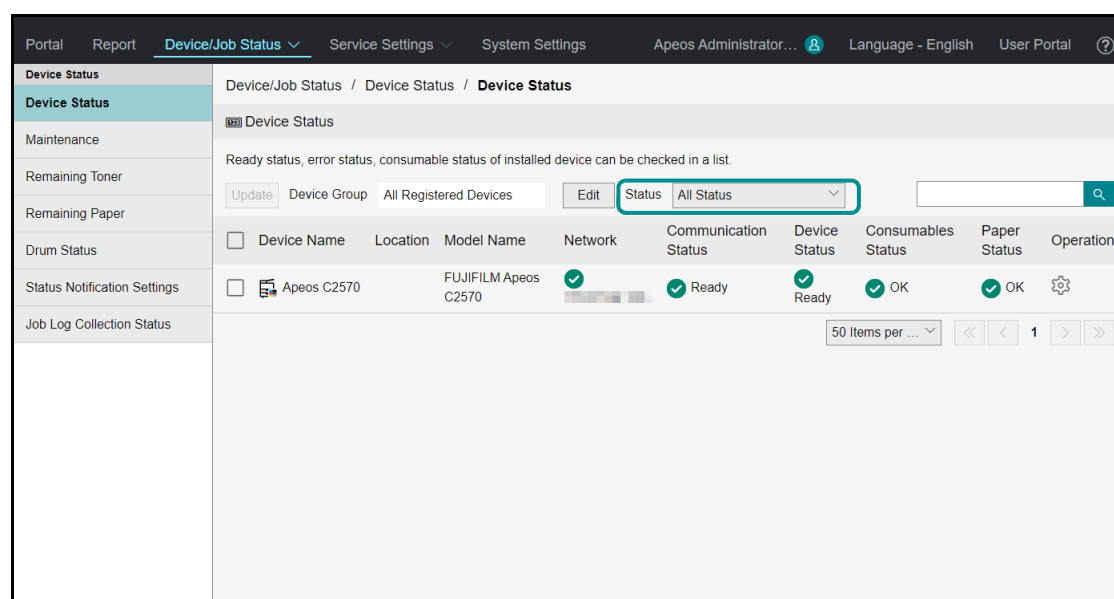
Extracting Device Registered in Specific Device Group

Click [Edit] to select the device group in which the device is registered.

Extract a device and display status

Select the condition of a device to display at [Status].

When the device supports Internet Services, click  and select [Device Status] to activate Internet Services and check the details.



[Status]

- [All Status]
Devices with all status are displayed
- [Communication Error]
The device in which some error of communication is occurring is displayed.
- [Machine Warning/Error]
The device in which some error of the device is occurring is displayed.
- [Consumables Warning/Error]
The device in which some warning or error of toner is occurring is displayed.
- [Paper Warning/Error]

The device in which some warning or error of paper is occurring is displayed.



Note

- The causes can be different by model.
- When the administrator is operating in device management mode or a customer engineer is operating, [Action Required] is displayed in some models. In that case, maintenance is not necessary.

Status type

The number inside () is priority order when some phenomena are occurring in one device. For example, [Clear the Paper Jam] is displayed when both phenomena of [Clear the Paper Jam] and [Out of Paper] are occurring at the same time.

- Ready

The device is working normally.

- No retrieval (1)

- No communication has been made with the device.
- The device is offline.
- [Status Monitoring Settings] of the device is set to [Off] and manual update is not executed either.

- No response (2)

Though it tried to retrieve information on a device, communication is timeout and it is not able to communicate with a device.

- Response (SNMP error) (3)

Impossible to retrieve information on a device for the following reason.

- SNMP response error
- SNMP community name mismatch
- SNMP timeout

- Clear the Paper Jam (4)

Paper is jammed

- Out of Paper (5)

No paper

- Out of Toner (6)

No toner

- Door/Cover Open (7)

The cover and door are open.

- Action Required (8)

The error that needs maintenance is occurring in the device. The main reasons are as follows.

- The output tray is full.
- Failure has occurred to consumables other than paper and toner.
- Failure has occurred to the exit tray.
- Failure has occurred to the feeding tray.
- Time to replace the drum or the time is approaching.
- Setting of the drum is wrong.
- The waste toner container is full or about to be full.

- Paper supply (9)

Paper is getting low.

- Replace Toner(10)

Toner is getting low.

- Action Required (11)

The warning that needs maintenance is occurring in the device.

Update information on a device

Select a checkbox for a device to refresh in the [Device Status] list and click [Update]. The latest status of a device is displayed.

Device/Job Status / Device Status / **Device Status**

Device Status

Ready status, error status, consumable status of installed device can be checked in a list.

Update Device Group All Registered Devices Edit Status All Status

☐	Device Name	Location	Model Name	Network	Communication Status	Device Status	Consumables Status	Paper Status	Operation
☒	Apeos C2570		FUJIFILM Apeos C2570		Ready	Ready	OK	OK	

50 Items per ... << < 1 > >>



Note

You can update a device automatically. If you set [Monitor Status] to [Yes] in [Status Monitoring Settings] of [Communication Settings], it is automatically updated at the intervals that you set in [Status Monitoring Interval].

Checking Device Alert Information

In the [Device Status] list, click of the device you want to operate, and select [Alert Details] from the displayed menu to check the device alert information.

ApeosWare Management Suite

Alert Details - <Apeos C2570>

Occurred On	Level	Description
2022/12/09 09:38:45	Warning	071-450 Tray 1 is Near empty. Add paper to Tray 1. Printing can continue.
2022/12/09 09:38:45	Warning	072-450 Tray 2 is Near empty. Add paper to Tray 2. Printing can continue.
2022/12/09 09:38:45	Warning	073-450 Tray 3 is Near empty. Add paper to Tray 3. Printing can continue.
2022/12/09 09:38:45	Warning	074-451 Tray 4 is empty. Add paper to Tray 4. Printing can continue.
2022/12/09 09:38:45	Warning	075-451 Tray 5 is empty. Add paper to Tray 5. Printing can continue.

OK

Maintenance

How to Display

Select [Device/Job Status] > [Device Status] > [Maintenance] in the administrator screen menu.

Page Summary

Meter information on the total amount of copied and printed paper is displayed. You can power down a device. For meter information, the displayed content depends on models and contract details.

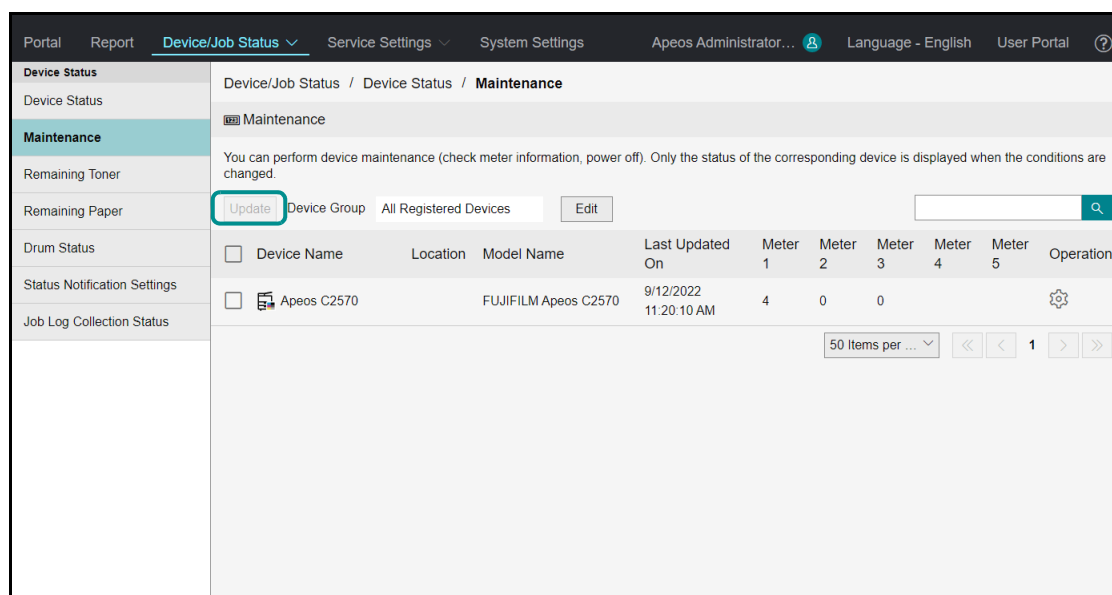
When the device supports Internet Services, click  and select [Device Status] to activate Internet Services and check the details.

Extracting Device Registered in Specific Device Group

Click [Edit] to select the device group in which the device is registered.

Update device meter information

Check the checkbox of the device to update on the list of [Device Maintenance], and click [Update]. The latest meter information of the device is displayed.



The screenshot shows the 'Maintenance' page in the ApeosWare Management Suite. The page has a dark header with navigation links: Portal, Report, Device/Job Status (selected), Service Settings, System Settings, Apeos Administrator..., Language - English, and User Portal. The left sidebar contains a list of menu items: Device Status, Device Status, Maintenance (selected), Remaining Toner, Remaining Paper, Drum Status, Status Notification Settings, and Job Log Collection Status. The main content area shows the 'Maintenance' section with a sub-header 'Device/Job Status / Device Status / Maintenance'. Below this is a message: 'You can perform device maintenance (check meter information, power off). Only the status of the corresponding device is displayed when the conditions are changed.' There is an 'Update' button (highlighted with a red box) and a 'Device Group' dropdown menu set to 'All Registered Devices'. Below this is a table with columns: Device Name, Location, Model Name, Last Updated On, Meter 1, Meter 2, Meter 3, Meter 4, Meter 5, and Operation. The table contains one row for 'Apeos C2570' with a checkbox in the 'Device Name' column. The 'Last Updated On' column shows '9/12/2022 11:20:10 AM'. The 'Meter' columns show values: 4, 0, 0. The 'Operation' column has a gear icon. At the bottom right, there is a pagination control showing '50 Items per ...' and navigation buttons.



Note

You can update a device automatically. If you set [Monitor Status] to [Yes] in [Status Monitoring Settings] of [Communication Settings], it is automatically updated at the intervals that you set in [Status Monitoring Interval].

Power down

Click  of a device which you want to power down in the [Device Maintenance] list and select [Power Off].



Note

In some models, power off is not available in the ApeosWare Management Suite menu.

Remaining Toner

How to Display

Select [Device/Job Status] > [Device Status] > [Remaining Toner] in the administrator screen menu.

Page Summary

You can check the remaining toner of a device.

When the device supports Internet Services, click  and select [Device Status] to activate Internet Services and check the details.

Checking Remaining Toner of Specific Device

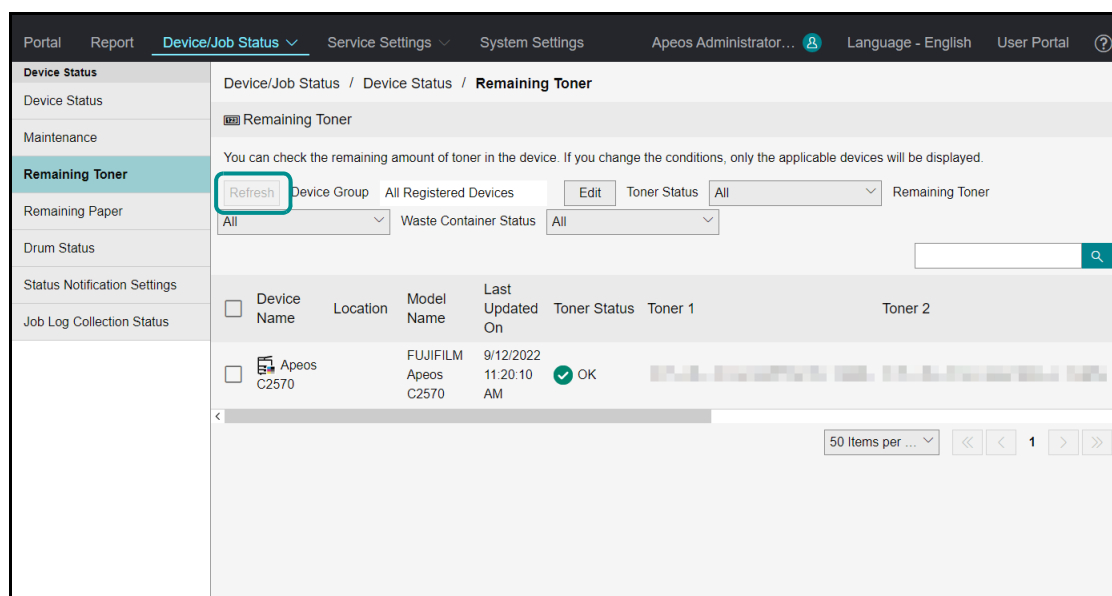
Click [Edit] to select the device you want to check the remaining toner.

Check the Toner Status, Remaining Toner, and Waste Container Status by filtering.

Select Toner Status, Remaining Toner, or Waste Container Status to check from the pull-down menu. Only the device of the selected status is displayed.

Update Remaining Toner Information

Select the checkbox for a device to update in the [Remaining Toner] list and click [Refresh]. The latest remaining toner amount is displayed.



Remaining Paper

How to Display

Select [Device/Job Status] > [Device Status] > [Remaining Paper] in the administrator screen menu.

You can display it by any of the following.

- Select [Device/Job Status] > [Device Status] > [Remaining Paper] in the administrator screen menu.
- Click "XX devices are out of paper" in [Device Status] in the portal screen.
The screen in which only the devices in the "out of paper" status are filtered is displayed.

Page Summary

You can check the remaining paper of a device.

When the device supports Internet Services, click  and select [Device Status] to activate Internet Services and check the details.

Checking Remaining Paper of Specific Device

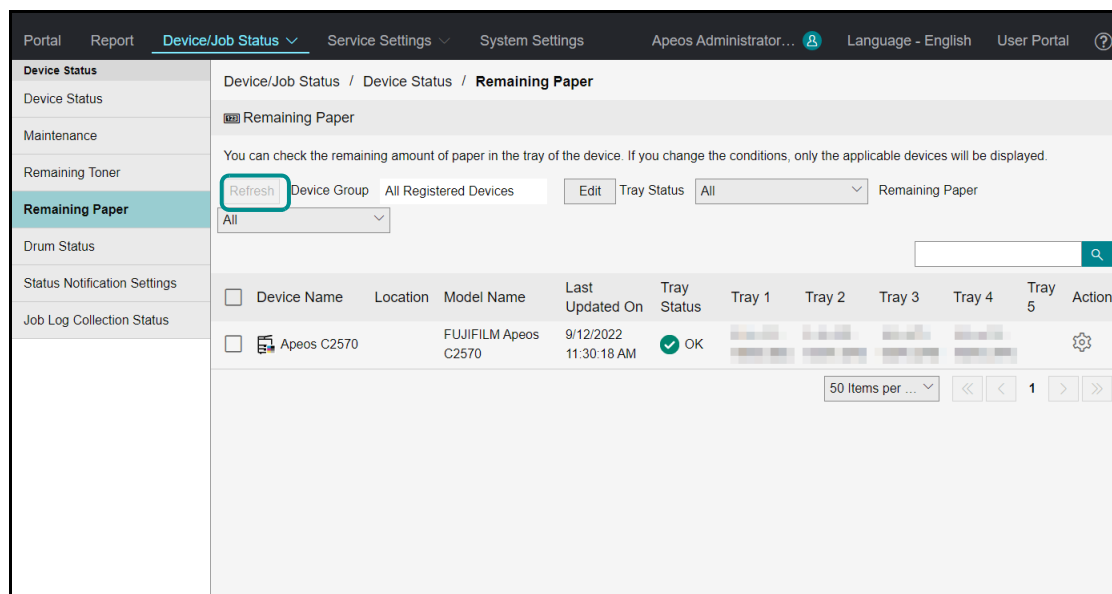
Click [Edit] to select the device you want to check the remaining paper.

Check the Tray Status/Remaining Paper by filtering.

Select Tray Status/Remaining Paper to check from the pull-down menu. Only the device of the selected status is displayed.

Update Remaining Paper Information of Device

Select the checkbox for a device to update in the [Remaining Paper] list and click [Refresh]. The latest remaining paper amount is displayed.



Drum Status

How to Display

Select [Device/Job Status] > [Device Status] > [Drum Status] from the menu on the administrator screen.

Page Summary

You can check the drum status of a device.

When the device supports Internet Services, click  and select [Device Status] to activate Internet Services and check the details.

Check the drum status of a specific device.

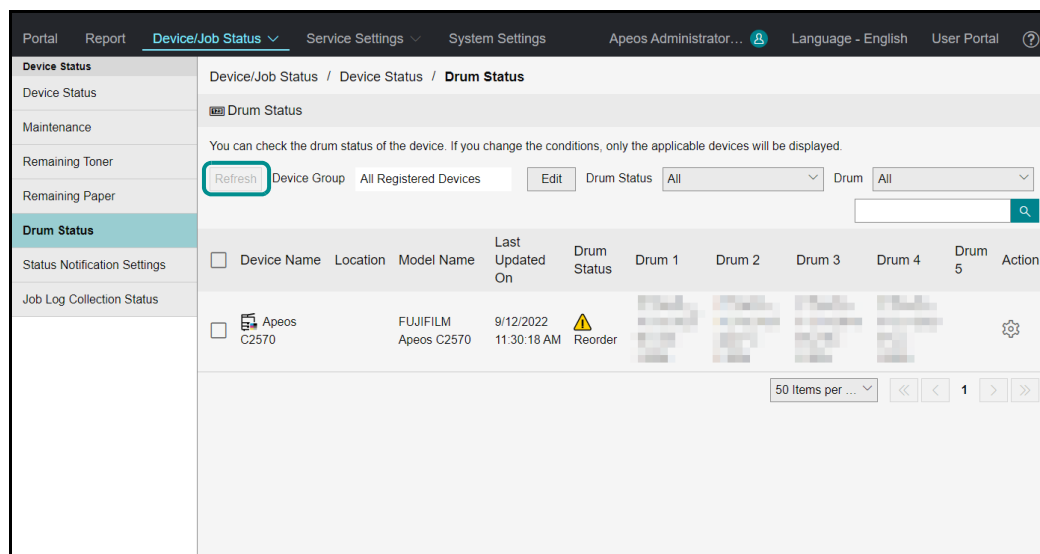
Click [Edit] to select the device you want to check the remaining toner.

Check the drum status by filtering.

Select the drum status to check from the pull-down menu. Only the device of the selected status is displayed.

Refreshing information on the drum status of a device

Select a checkbox for a device to refresh in the [Drum Status] list and click [Refresh]. The latest drum status is displayed.



Status Notification Settings

How to Display

Select [Device/Job Status] > [Device Maintenance] > [Status Notification Settings] in the administrator screen menu.

Page Summary

Set notification conditions, a device for monitoring, and notification destination when you notify the latest device status by e-mail.

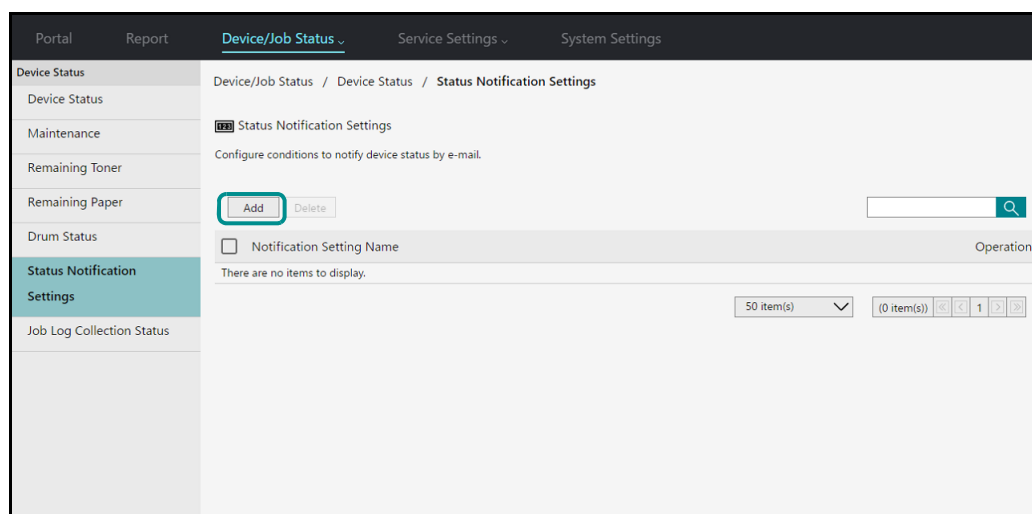


Refer

Settings for sending email → "Network Settings" (P.40)

Add notification conditions

Click [Add].



(1) Details

Specify the following item, and then click [Next].

[Notification condition settings when warning/error is detected]

For making an e-mail notification when a device detects a warning or an error, select [Yes] and select the notification status.

- [Notification Status]

Specify a target status for notification. When the device is ready for notification status with a checkbox selected, an e-mail message is sent. You can specify several statuses.

Notification Status	Descriptions
Out of Toner	No toner left
Replace Toner	Little toner left
Out of Paper	No paper left
Paper supply	Paper little left
Paper jam	Paper is jammed
Cover open	The cover is open
Action Required	Other things to be dealt with (tray failure, replacement of a drum and so on) have occurred
No Response	No response from the device
Response (SNMP error)	In spite of response from the device, SNMP error is occurring
Errors of job log collecting	An omission or an error of file storage or some errors occurred while job logs are collected.  Note Notification of an error of job log collecting is sent separately from an e-mail message of the above notification.
Security setting mismatch	A deviation has occurred from the security setting that was applied beforehand.

Periodical Notification Condition Settings

- [Periodically notify monitored device status]

When you send an e-mail message on a periodic basis regardless of whether the status of a specified device has changed, select [Yes] and set the notification interval.

- [Notification Interval]

When you notify at a specified interval, select [Interval] and specify an interval (minutes) for notification. When you notify once a day, select [Daily] and specify time for notification. When you notify once a week, select [Weekly] and specify a day of the week and time for notification. When you notify once a month, select [Monthly] and specify a day and time for notification.

(2) Device monitoring

Specify the following item, and then click [Next].

[Monitor All Devices]

If you monitor all devices for notification, select [On]. If you limit the number of devices for monitoring, select [Off] and specify the following items.

- [Monitor Device Group(s)]

When you monitor a device group for notification, select [On], then click [Add] and select the target device group.

[Monitor Device(s)]

When you monitor an individual device for notification, select [On], then click [Add] and select the target device.

(3) Notification destination

Specify the following item, and then click [Next].

[Notification Destination User]

Specify the notification destination name and the e-mail address of the e-mail recipient. You can click  and specify more than one address.

Clicking [Add User Address] enables you to select a user from the user name list containing the registered e-mail address.

[Send Test E-mail]

Sends the test e-mail to all the addresses specified in [Notification Destination User].

(4) Overview

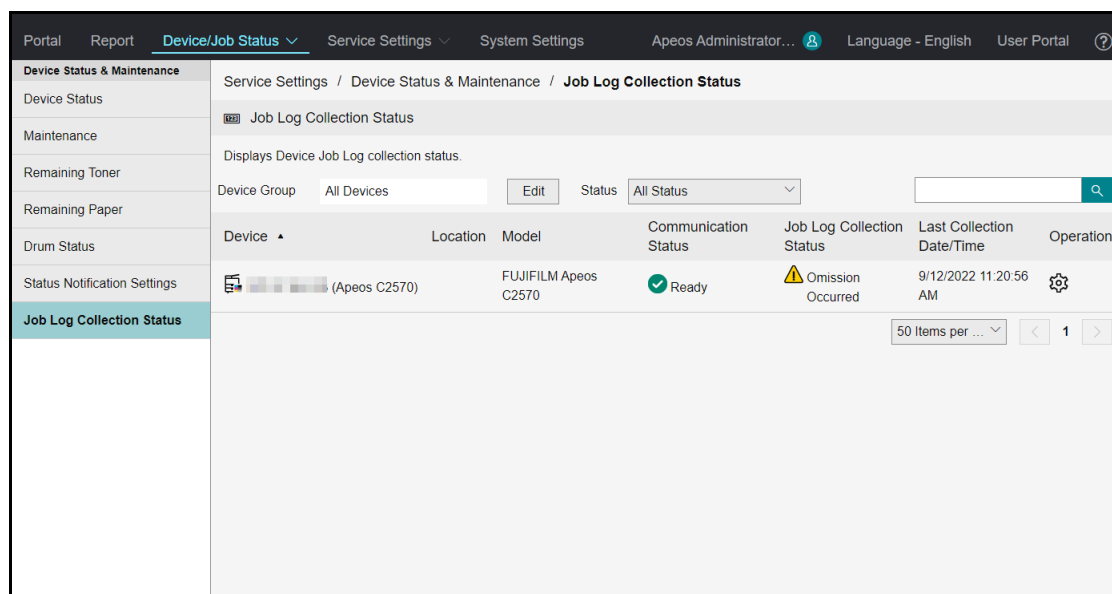
After you check the configured settings, clicking [Save] will register the device.

You can click [Edit] for each item to change the settings.

Job log collection status

How to Display

Select [Device/Job Status] > [Device Status] > [Job Log Collection Status] in the administrator screen menu.



The screenshot shows the 'Job Log Collection Status' page. The breadcrumb trail is 'Service Settings / Device Status & Maintenance / Job Log Collection Status'. The page title is 'Job Log Collection Status'. Below the title, it says 'Displays Device Job Log collection status.' There are filters for 'Device Group' (All Devices) and 'Status' (All Status). A table displays the job log collection status for a device. The table has columns: Device, Location, Model, Communication Status, Job Log Collection Status, Last Collection Date/Time, and Operation. The data row shows a device with model 'FUJIFILM Apeos C2570', communication status 'Ready', and a job log collection status of 'Omission Occurred' (indicated by a yellow warning icon). The last collection date/time is '9/12/2022 11:20:56 AM'. At the bottom right, there is a pagination control showing '50 Items per ...' and a page number '1'.

Device	Location	Model	Communication Status	Job Log Collection Status	Last Collection Date/Time	Operation
 (Apeos C2570)		FUJIFILM Apeos C2570	 Ready	 Omission Occurred	9/12/2022 11:20:56 AM	

Page Summary

Job log collecting status is displayed. You can confirm whether an omission of job logs and replacement of a device are occurring. You can select a status and extract a device for display.

The types of the status of job log collecting are as follows.

Status	Descriptions
	Normal status.
	A phenomenon is occurring at error level.
	Some phenomenon is occurring at a warning level.

Extract a device and display status

Select the condition of a device to display at [Status].

[All Status]

Display all devices for job log collecting.

[Unknown]

Display a device whose status is unknown.

[Ready]

Display a device in which job log collecting is normally performed.

[No Response]

Display a device on which you tried to receive information but were not able to communicate with.

[Omission Occurred]

Display a device in which you were not able to collect job logs for some causes. For details on omission, refer to "Concerning an Omission" in "Installation and Operation Guide".

[Device Replaced]

Display a device that has been replaced with another device with the same IP address. For details on device replacement, refer to "Concerning Device Replacement" in "Installation and Operation Guide".

[Communication Error]

Display a device whose information you were not able to retrieve for the following reasons.

- An error occurred in SNMP communication with a device.
- An error occurred in Internet Services communication with a device.
- An error occurred in SOAP communication with a device.

[Job Log Collection Error]

Display a device in which an error occurred during the job log collecting.

- The job log information that was received from a device was wrong.
- ApeosWare Management Suite does not support the model.
- Job logs were not received after replacement because of replacement of devices
- Failure in initialization of gathering service and of gathering processing
- Errors other than above

[File Save Error]

Display a device in which an error on a job log file is occurring.

- No storage location of job log files
- No the access rights to storage location folders of job log files and files
- Shortage of disk capacity in storage location of job log files
- Errors other than above occurs while making a job log file

Clear information on the occurrence of an omission

After the resolution of an omission of job logs, you can delete the display of the occurrence of an omission. To do that, click [Clear Omission] of a device in which an omission occurred in the device list of [Job Log Collection Status] page.

Operation from the Device's Control Panel

This section describes operation from the device control panel.



Note

- In case that the cost management feature was enabled during the installation, to use the device of [Custom Authentication], associate the account to the user who uses the device regardless of whether to use the cost management future or not. If the account is not set, the error “There is no available account” occurs when logging in to the device or accessing ApeosWare Management Suite from the device.
- You cannot use remote control panel functions while using the control panel of a device.
- During remote operation, the screen you are using on the client computer is displayed on the control panel of the device. When entering passwords on login or other screens, the password will not be displayed on the control panel. However, items such as the user ID will be displayed, and may be read by a third party.

Control Panel's Screen

Authentication ID that is authenticated with a device

When the authentication method of a device is [Custom Authentication], you can use one of the following for ID to authenticate users.

- User ID
- PAN (manual entry of the Card ID)
- External ID



Note

In [Authentication Mode] under [Authentication Settings], if the [Allow Authentication by Email Address] checkbox is selected, authentication is possible by entering the e-mail address into the user ID entry field.

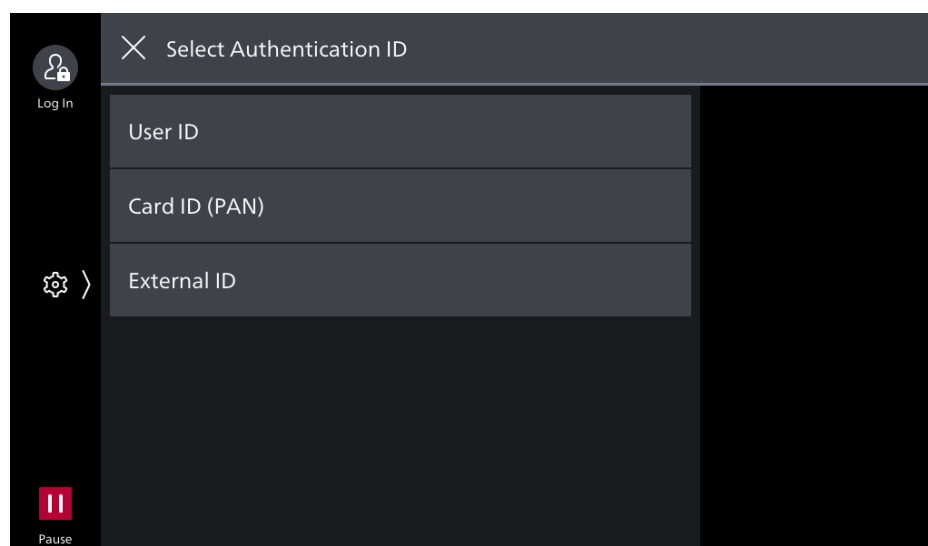


Refer

“[User Authentication settings]” (P.172)

For which authentication ID to use during operation, you can select it in [Enter Authentication ID] of the [Service Settings] > [User Management] > [Authentication Settings] page.

Users perform authentication operation using the authentication ID set in [Enter Authentication ID]. When several authentication IDs are set, a selection screen for a login method is displayed in a device's control panel and users can select what authentication IDs to use.



When a authentication method of a device is [Local Authentication] or [Remote Authentication], use User ID for authentication.

Authentication using the IC card reader

If you use IC card reader in a device set to [Custom Authentication], select a checkbox for [Authentication Mode] > [Card Authentication (Device Only)] in the [Authentication Settings]. If you do not select a checkbox, the card authentication is not available.

When an authentication method is [Local Authentication] or [Remote Authentication] in a device, if you set a card reader and enable it, card authentication becomes valid automatically.

Authentication Using QR code

When using Log in with QR code on a device of [Custom Authentication], information specific to the mobile application needs to be set in [Service Settings] > [User Management] > [Authentication Settings]. If it is not set, authentication using QR code is not available.



Refer

"Advance Setting When Using Login with a QR Code" (P.70)

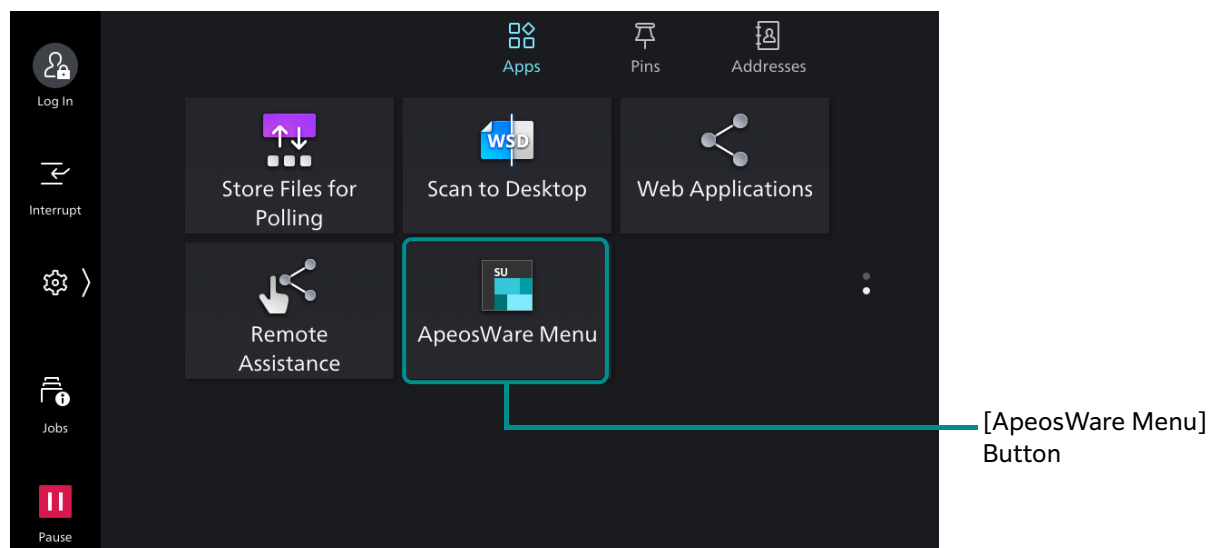
Authentication Using KJTech Reader

If you use KJTech reader in a device set to [Custom Authentication], select a checkbox for [Authentication Mode] > [Card Authentication (Device Only)] in the [Authentication Settings]. If you do not select a checkbox, the KJTech authentication is not available.

When an authentication method is [Local Authentication] or [Remote Authentication] in a device, if you set a KJTech reader and enable it, KJTech authentication becomes valid automatically.

Device Home Screen

It is the menu screen managed with a device. The following content is displayed depending on settings.



[ApeosWare Menu] Button

The screens that transits when you push this button are one of the following, depending on the content of [Display screen at login] of access profile associated with a user.

- Print On Demand
Display the operation screen of Print On Demand in ApeosWare Management Suite.
- Device Home Screen

Displays the home screen of a device.

- ApeosWare Management Suite Menu

Display the portal screen of ApeosWare Management Suite.



Refer

"ApeosWare Management Suite Portal Screen" (P.116)



Note

After you push the menu button of each feature or the [ApeosWare Menu] button, the login screen may be displayed. In that case, each screen is displayed after authentication.

Feature menu buttons

The feature menu buttons you set to display in [Device Panel Settings] > [Device Menu] when creating a device group are displayed. When you push the button, after connecting to ApeosWare Management Suite, the operation screen of each feature is displayed.

ApeosWare Management Suite Login Screen

This is the screen displayed for authentication for Custom Authentication.

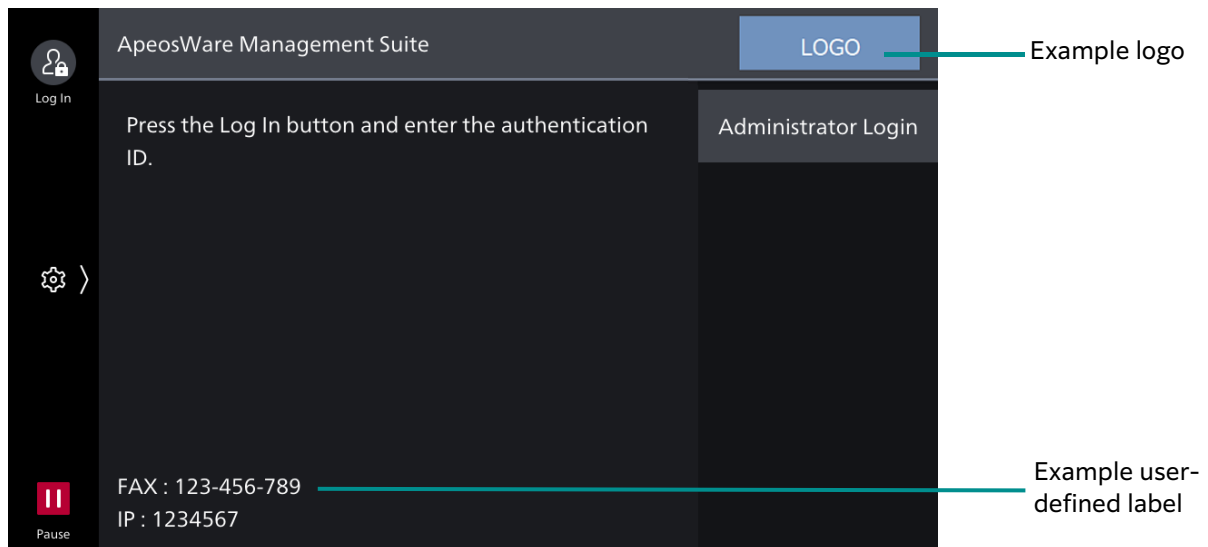
You can display the logo, QR code for connection, and custom label that are set in [System Settings] > [Control Panel Customization Settings].



Refer

"Control Panel Customization Settings" (P.52)

An example of the ApeosWare Management Suite login screen is shown below.



Select Accounts screen of ApeosWare Management Suite

This is the screen displayed to select the account of the user who had logged in.

Depending on some settings, the Select Accounts screen of ApeosWare Management Suite screen is not displayed and the portal screen of ApeosWare Management Suite is displayed.

Depending on some settings, the account cannot be changed after transition to the ApeosWare Management Suite screen.



Note

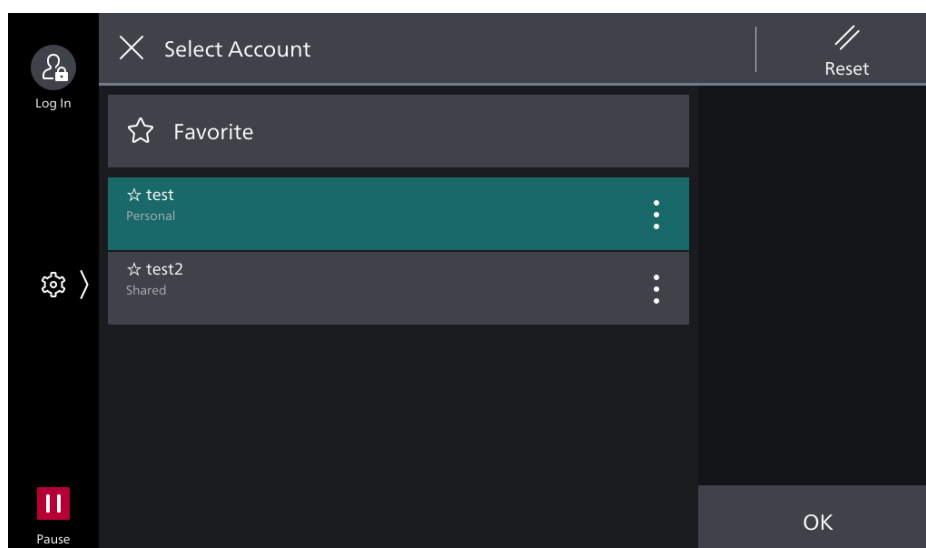
- This screen is displayed when multiple accounts associated with a user exist.

- Even though only 1 account is associated with a user, this screen is displayed when the account is not set to the specified account or when a check mark is attached to [Always Show [Select Accounts] After Authentication] in [Account Selection Settings on Multifunction Device] .
- This screen is displayed even though the account associated with a user is not sent, when a check mark is attached to [Allow] in [Using shared account that all users can use]. However, a user is limited to the user who is not set to [Force stop when minimum balance is reached].
- Even though [Using shared account that all users can use] is not allowed, this screen is displayed when a check mark is attached to [Always Show [Select Accounts] After Authentication] in [Account Selection Settings on Multifunction Device].
- When [Stop] is set to [Force stop when minimum balance is reached], any accounts cannot be changed after transition to the ApeosWare Management Suite screen.
- Even though [Force stop when minimum balance is reached] is not set and when [Using shared account that all users can use] is not allowed, any accounts cannot be changed after transition to the ApeosWare Management Suite screen.



Refer

- “(3) Associate with users” (P.129)
- “[Using shared account that all users can use]” (P.145)
- “[Force stop when minimum balance is reached]” (P.144)
- “[Account Selection Settings on Multifunction Device]” (P.221)



[Favorite]

Add the selected accounts to the list of [Favourite Account].

If the selected accounts are already added, delete those accounts from the list.



Note

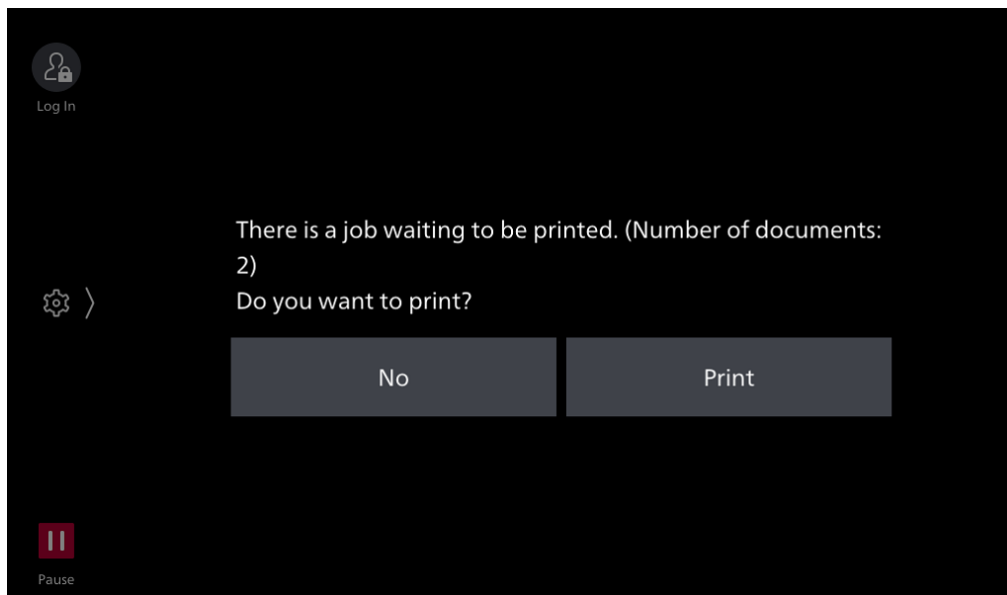
The displayed screen of [Favorite] depends on the items set in [Default Settings] under [Account Selection Settings on Multifunction Device].

Print Confirmation screen

Screen displayed after authentication if [Auto Print at Login] for the access profile associated with the user is set to [Select on confirmation screen], and there is at least one job pending.

Select [Print] to print all jobs available for printing.

Select [No] to display the screen selected in [Display screen at login].



ApeosWare Management Suite Portal Screen

The screen that ApeosWare Management Suite manages.

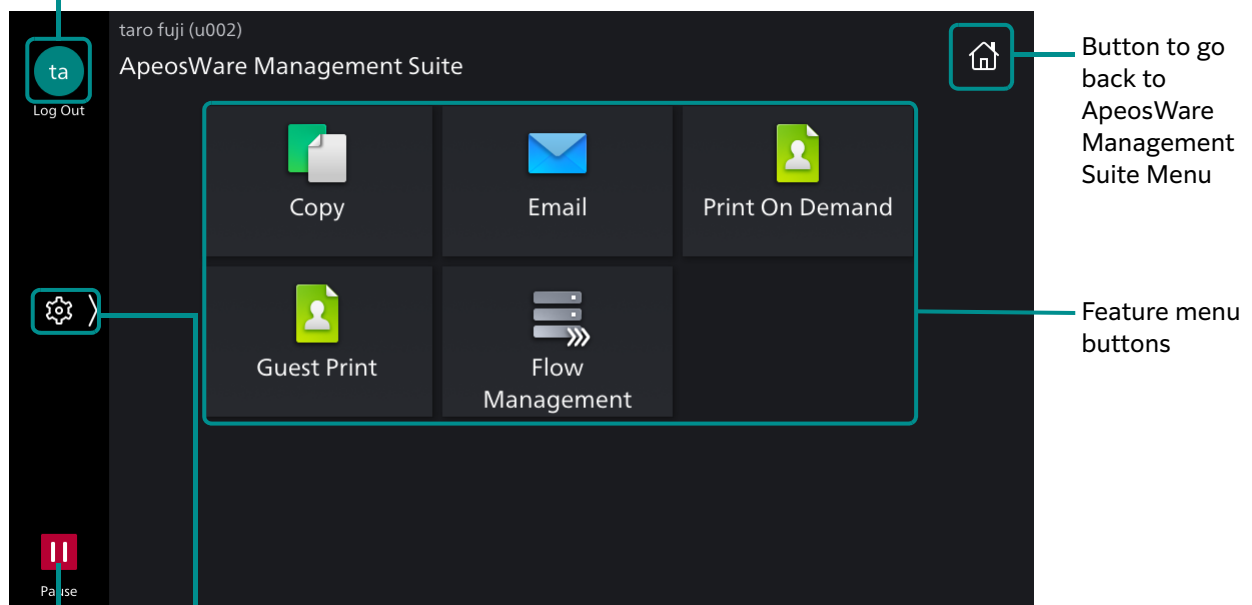


Note

Depending on the access profile settings associated with the user, the usage status screen, the operation screen of Print On Demand, or the screen to select account may be displayed right after the logging in.

The beginning letters of login user display name are shown.

When clicked, the user is logged out from ApeosWare Management Suite.



Display job list Display your status of usage



The (Display your status of usage) Button

The status of usage is displayed.

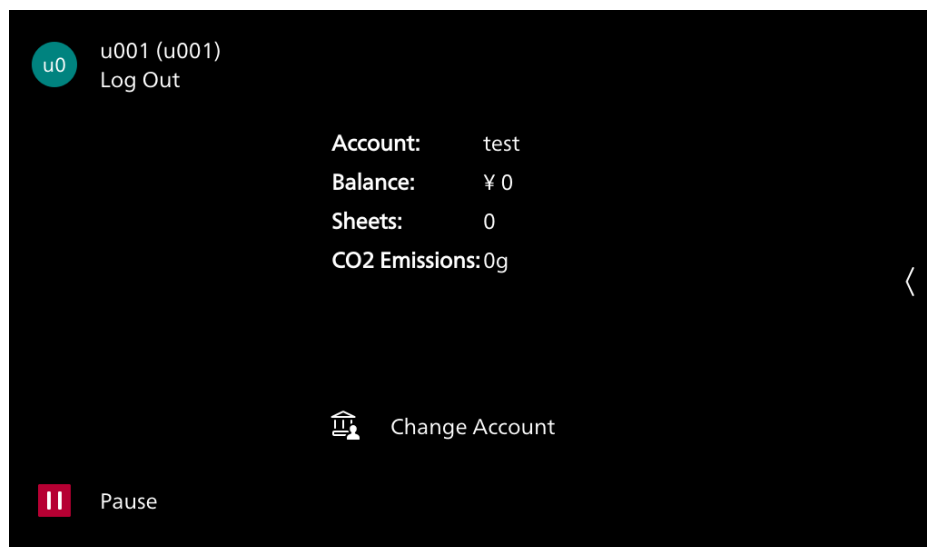


Note

"Account" used in cost management has nothing to do with "AccountID" set in a device.

- [Standard]

Displays the print record of the logged in user.



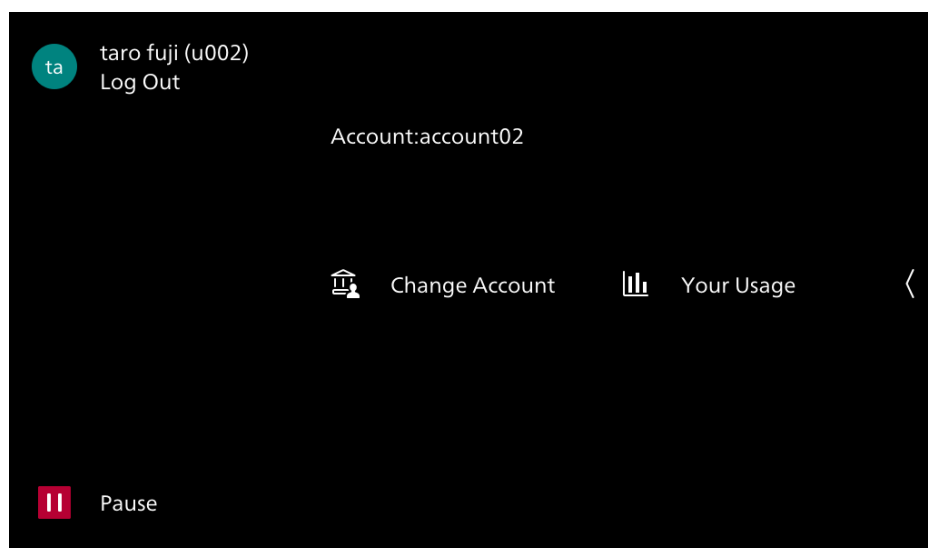
The following contents are displayed.

Items	Description
Account ^{*1}	The account that is selected is displayed.
Balance ^{*1}	Displays the balance allotted to the account.
Output sheets	Displays the number of output sheets of this month. Note The amount of the output prints is updated not just after printing, but after the job log aggregation.
CO2 Emissions (g)	Displays the CO2 emissions reduced this month. "2-Sided Print" and "Pages per Side Print" enable you to reduce CO2 emissions.
(Change account) button	If you push the button, the screen to select an account is displayed.

*1 It is displayed only when [Display balance in Device] is enabled in account settings.

- [Detailed (With Cost Reduction Information)]

Displays the actual copy/print output amount and the cost reduction information of the logged in user.



 Pushing the (Your Usage) button displays the accounting result of job logs for the month for the logged in user. When an account is set to the logged in user, the following contents are displayed.

Items	Description
Accounting period	The target range for job log accounting is displayed.
User name	The name of logged in user is displayed.
Number of Pages ^{*1}	Displays this month's output impressions of copy/print.
Amount ^{*1}	Displayed when [Display balance in Device] on the account settings is disabled. Displays the amount of money cost based on the price policy. The settings for discount/additional charge on the price policy are not reflected in the amount.
Usage ^{*1}	Displays actual rates of Color, 2-Sided, and N-up. If the actual rate does not reach the target, the screen to call attention is displayed.
Target	Displays the target value set on the access profile.
Balance	Displayed when [Display balance in Device] is enabled in the account settings. Displays the allotted balance.
Output Equivalent	Displayed when [Display balance in Device] is enabled in the account settings. Displays remaining possible output impressions by calculating with the balance. When there are differences in the charge on the settings, the settings of the highest and lowest are displayed as indications.

^{*1} Updated not just after copying or printing but the after the job log aggregation.

When no account is set to the logged in user, the following contents are displayed.

Items	Description
Number of Pages ^{*1}	Displays this month's output impressions of copy/print.
Usage ^{*1}	Displays actual rates of Color, 2-Sided, and N-up. If the actual rate does not reach the target, the screen to call attention is displayed.
Target	Displays the target value set on the access profile.

*1 Updated not just after copying or printing but the after the job log aggregation.

Pushing the  (Change account) button displays the screen for selecting an account.



Note

On the [Favourite Account] tab, the favourite account the user set is displayed. For the setting method, refer to "Add Favourite Accounts" (P.237).
On the [Recently Used Account] tab, accounts that recently executed jobs are displayed, up to 10 accounts.



(Display Job List) Button

A list of jobs for the logged in user appears.



(Back to Menu) Button

The screens that transits when you push this button are either one of the following, depending on the content of [Display screen when "Home" button is pressed] of access profile associated with a user.

- Device Home Screen

Display the menu screen of a device.



Refer

"Device Home Screen" (P.113)

- ApeosWare Management Suite Menu

Display the portal screen of ApeosWare Management Suite.

Feature menu buttons

The menus to be displayed depend on the setting status of option license and the setting content of [Access to File Management Service] associated with logging users. When you push the button, the operation screen of each feature is displayed.

Access to ApeosWare Management Suite from Control Panel

There are two ways to access each feature of ApeosWare Management Suite from a device's control panel.

- Using Custom Service

The menu buttons of each feature registered in custom service (service operated with the web browser built in a device) are displayed in the control panel. You can access each feature by pushing this menu buttons.

- Using the Web Applications Features

Select and access the URL of the destination from the menu of web applications of the control panel. Set the URL of the destination in advance.



Note

- For the device where the menu button is displayed as custom service, you do not need to set web applications.
- Link with the e-mail transmission of scanned documents and file management service does not correspond to the web applications feature.
- In some models, you cannot use the custom service and web applications.

Using Custom Service

To use the custom service, you need to set as followings.



Note

To use this feature, the External Access kit or the customized extension kit needs to be enabled on a custom service-enabled device. The usage environment depends on devices. For details, refer to the device manual in use.

Settings from a Web Browser

Set [Authentication/Accounting Mode] of the device group that a device is affiliated with to one of the following.

- Local Authentication/Local Accounting (Local Authentication)
- Local Authentication/Network Accounting (Network Authentication)
- Remote Authentication (authentication system: ApeosWare Authentication Agent)
- Custom Authentication

The [ApeosWare Menu] button is displayed by default in the menu screen of a device.

If you want to add each feature menu, change [Device Menu] of the service to display to [Display] in [Device panel settings and registered data management] > [Device Panel Settings] when you set a device group or sub-device group.



Refer

- "[ApeosWare Menu] Button" (P.113)
- "Add Device Group" (P.77)

Device settings

Display the [Tools] screen in the device control panel and set [Web Browser Setup] as followings.

Items	Setting Content
Web Applications Version	v5 or v4  Note For devices where [V5] can be set in [Web Applications Version]. It is recommended to set [V5]. V6 cannot be used.
Use of Cookie	Yes or confirm storage
Use JavaScript	Yes

Using the Web Applications Features

To use Web Applications Features, display the [Tools] screen from the control panel of the device and set [Web applications service setup], [Web Browser Setup], and [Machine Clock/Timers] as following.



Note

- To use this feature, the External Access kit needs to be enabled on an external access-enabled device. The usage environment depends on devices. For details, refer to the device manual.
- If you set the web applications link in Flow Management Option, the setting is different from what is described here. For the setting, refer to "2 Flow Management Environment Settings" of "Features Guide Flow Management Option".

Web applications service setup

Items	Setting Content
URL (When external access version is V5)	In the case with a FUJIFILM Business Innovation device or a Fuji Xerox device, with a Controller ROM software version of the following or later • Japanese models: 1.60.0 or later, or 1.100.0 or later • Overseas models: 1.60.0 or later, or 1.145.0 or later • Print On Demand http(s)-p0://{Server name/IP address}/MFD/Print/FollowMePrint/Default?DisplayMode=NB • Guest Print http(s)-p0://{Server name/IP address}/MFD/Print/TokenPrint/Default?DisplayMode=NB • User Data Registration http://{Host name}/UDR In the case with a Fuji Xerox device with a Controller ROM software version of lower than the above • Print On Demand http(s)-p0://{Server name/IP address}/MFDEX/Print/FollowMePrint/Default • Guest Print http(s)-p0://{Server name/IP address}/MFDEX/Print/TokenPrint/Default • (In case of FUJI XEROX ApeosPort-VI or earlier) User Data Registration http-p0://{Host name}/UDR • (In case of FUJI XEROX ApeosPort-VII or later) User Data Registration http-p0://{Host name}/UDR/?mode=9

Items	Setting Content
URL (When external access version is V4)	In the case with a FUJIFILM Business Innovation device or a Fuji Xerox device, with a Controller ROM software version of the following or later - Japanese models: 1.60.0 or later, or 1.100.0 or later - Overseas models: 1.60.0 or later, or 1.145.0 or later - Print On Demand http://{Host name}/MFD/Print/FollowMePrintV3/Default - Guest Print http://{Host name}/MFD/Print/TokenPrintV3/Default  Note In the case of a device manufactured by us, if the external access version is V4, the user's self-registration function is not available. In the case with a Fuji Xerox device with a Controller ROM software version of lower than the above - Print On Demand http://{Host name}/MFDEX/Print/FollowMePrintV3/Default - Guest Print http://{Host name}/MFDEX/Print/TokenPrintV3/Default - User Data Registration http://{Host name}/UDR
Use user ID for connection	Unused
User ID for connection	None
Password for user ID for connection	None
Notify external service of device/authentication information.	Yes If there is an item to select the type of servers, select "FUJIFILM BI server".
Notify user permission information	No



Note
{Host name} is the host name or the IP address of the ApeosWare Management Suite server. Specify "https" if the ApeosWare Management Suite server is in the SSL configuration. If you have changed your port number from the one in default settings, specify a colon (:) and port number after {Host name}. This is case sensitive.

Web Browser Setup

Items	Setting Content
Web Applications Version	v5 or v4  Note For devices where [V5] can be set in [Web Applications Version]. It is recommended to set [V5]. V6 cannot be used.
Delete cash when finished	No
Use JavaScript	Yes
Use cash	Yes
Use of Cookie	Yes
Warning for redirect	[Warn if re-directed to different host] or [Off]

External Access Parameter Settings

Add parameters to external access setting URLs to change some functions.

Example) <http://awms.example.com/MFD/Print/FollowMePrint/Default?lang=ja>

Items	Parameters	Descriptions
Language Setting	lang=[ja/en/ko/zh-tw/zh-cn/th]	Change the display language. ja: Japanese en: English ko: Korean zh-tw: Traditional Chinese zh-cn: Simplified Chinese th: Thai
Print without List	autorelease=[yes/no]	Switch whether to display the list screen for selecting print jobs and confirming detailed information from the device control panel. The default setting is "Print with list". yes: Print without list no: Print with list

Machine Clock/Timers

Items	Setting Content
Valid time for Print On Demand	For Print On Demand, set valid time for print. If you do not receive a print job within the time set here after direction for print, the print direction becomes invalid.  Note With the direction of a print job in large amounts at a time and a complicated print job that takes time to process, it may time out before receiving them. Set appropriate time considering the situation.

To use IC Card Gate (only for Print On Demand)

To execute Print On Demand using IC Card Gate series connected to the network, configure the settings on the side of IC Card Gate as follows.

Settings on IC Card Gate

Features	Settings
Print Service	PrintXchange Print On Demand
Connection path	Specify the following URL. *1 http://{Host name}/MFD/Print/FollowMePrintV3/Default?uiless=yes
User Name/Password	To use Basic Authentication, specify the user ID and password which are registered and set in Windows and Internet Information Service (IIS) on the ApeosWare Management Suite server. When the Basic Authentication is not used, it is not required.
Authentication System	When authenticating with ApeosWare Management Suite, select [ApeosWare Authentication Agent].
Alias specified on installation (Primary)	/MFD/AuthAgent/

*1 {Host name} is the host name or the IP address of the ApeosWare Management Suite server.
Specify "https" if the ApeosWare Management Suite server is in the SSL configuration. If you have changed your port number from the one in default settings, specify a colon (:) and port number after {Host name}. This is case sensitive.

What if?

This section describes the operation of device management.

When user information is not updated because of registered card ID

If the card ID registered in a device is set for a user, an error occurs and update to a device fails.

If you lend a card to a user temporarily or reset the card ID set for a user for another user, the above things occur and updating user information to a device fails. Change the value of a setting file according to the following procedure.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Open the following file with a text editor.
Folders: {Folder of data storage directory}\Data\karaf\etc
File name: dm-custom.properties

{Folder of data storage directory} is as follows if the default settings are not changed.
C:\FUJIFILM\ApeosWare MS
3. Change the setting value of "com.fujifilm.fb.apeosware.dm.devsync.user.replaceCardID" to "true" and overwrite and save it.

`com.fujifilm.fb.apeosware.dm.devsync.user.replaceCardID=true`

4. Reboot the PC.



Note

With this setting, when you update user information to a device, the card ID that is already registered in a device is deleted and then new card ID is registered. Therefore, if you fail in registration of the card ID due to occurrence of an error after deletion, the relevant user may not be able to log in.

If you fail in registration of the card ID and retry it, it can be successful. Therefore, operate by setting [Restart when update failed] to [On] in [Device Data Condition Update Settings].



Refer

"Settings of update conditions of device data" (P.100)

When you connect IC Card Gate to a network

If you use the IC Card Gate series connected to a network, for the setup in IC Card Gate, specify the following to set an alias.

/MFD/AuthAgent

When free capacity of server HDD has become smaller

If the free capacity of HDD with the server has become smaller, move or delete the log files.

If the job log retention period is reduced significantly, a large volume of job log data is deleted from the database all at once. As a result, the size of transaction log (AWM2.ldf) can become bloated. In such a case, execute the following command after bloating of transaction log occurs so as to compress the size of transaction log.

[INSTALLDIR]¥WinSvc¥Mon¥bin¥awmsshinkDBLog.bat

The default value for [INSTALLDIR] is "C:¥Program Files¥FUJIFILM¥ApeosWare MS". Execute the command as a user of the Administrators group.

While this command is being executed, the system performance may degrade. Avoid executing the command during the business operating hours and during the date change processing time of ApeosWare Management Suite (from 0:00 until around 2:00 during the night).

Cautions when using print management functions without using user management

When using print management functions without using ApeosWare Management Suite user management, it is not necessary to register users in user management or register accounts in cost management.

If you wish to use on-demand printing refer to "Using the Web Applications Features" (P.121), and register the URL for on-demand printing in "Web applications service setup" on your device.

When not using user management, the print management function generates print jobs based on printer driver user information in order to identify print job users. This is not linked to users registered in user management. Even if users are registered, associated print functions cannot be used.

4 User Management

Settings and Confirmation in a Web Browser

You can set the settings for the user and confirm them with a web browser. This section describes what you can do with each page.

- [Service Settings] > [User Management]

Pages	Descriptions
User Group List	
User Group List	Create and manage the user groups that unify users.  Refer "User Group List" (P.128)
Details of user groups	Add association with lower groups and users, and with accounts to the user group and sub-user group you have selected.  Refer "User Group List (Details of User Groups)" (P.131)
User List	
All Users	Register and manage the users who use devices. Then, switch their validity and invalidity and unlock them.  Refer "User List (All Users)" (P.132)
Details of users	Add association with an account and delegated users to the selected user.  Refer "User List (Details of Users)" (P.139)
Access Profile List	Determine access rights to usable devices and each feature.  Refer "Access Profile List" (P.140)
User Import List	
User Import	Import user information from the remote authentication server and files, and register it in ApeosWare Management Suite.  Refer "User Import List [User Import] Tab" (P.149)
Account Import	Import account information from files and register it in ApeosWare Management Suite.  Refer "User Import List [Account Import] Tab" (P.166)

Pages	Descriptions
User Import List (Continued)	
Associate user/account	Imports files that coordinate the User ID and account name and associate users with accounts.  Refer "User Import List [Associate User/Account] Tab" (P.167)
Domain list	Sets the remote authentication server to work with.  Refer "Domain list" (P.169)
Authentication Settings	Sets user authentication.  Refer "Authentication Settings" (P.172)
FUJIFILM BI Direct Federation  Note This feature is only available in Japan.	Configure the settings to use single sign-on authentication for FUJIFILM BI Direct.  Refer "FUJIFILM BI Direct Federation" (P.185)
Keyword Condition Policy  Note This feature is not available in some countries and regions. For details, contact our dealers.	Sets the keyword condition policy.  Refer "Keyword Condition Policy" (P.176)
Condition	Sets the condition.  Refer "Condition" (P.177)
Supported Fonts	Sets the supported fonts.  Refer "Supported Fonts" (P.178)
Print Policy	Sets the print policy.  Refer "Print Policy" (P.179)
Watermark	Sets the watermark.  Refer "Watermark" (P.180)
Header/Footer	Sets the header/footer.  Refer "Header/Footer" (P.182)
QR Code	Sets the QR code.  Refer "QR Code" (P.184)

User Group List

How to Display

Select [Service Settings] > [User Management] > [User Group List] from the menu on the administrator screen.

Page Summary

Create and manage the user groups that unify users. You can create user groups, change property, copy, and delete them.

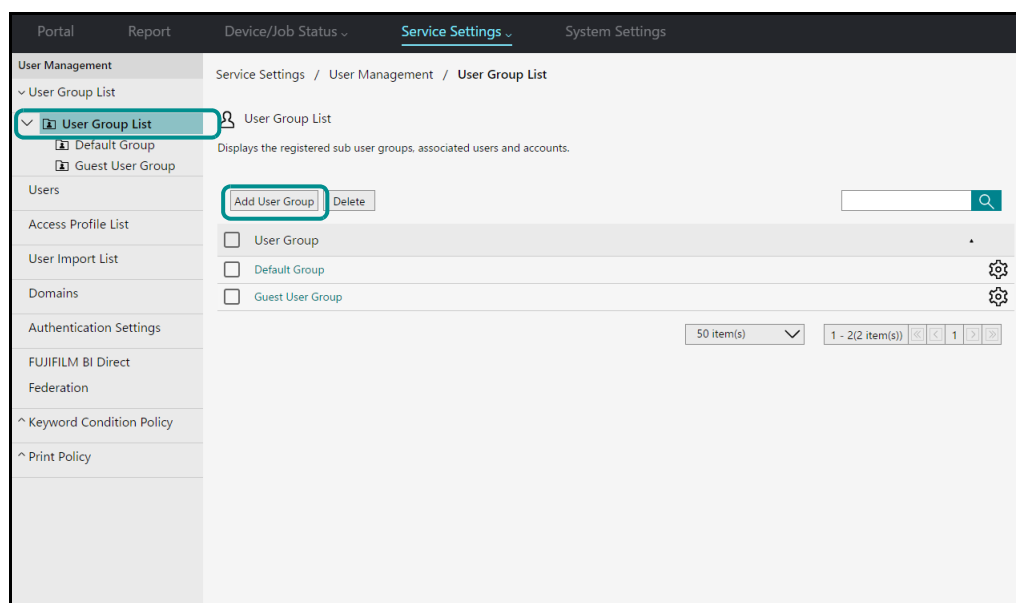


Refer

About user and user group → “Installation and Operation Guide”

Creating user groups

Select [User Group List] in the side menu and click [Add User Group].



(1) User group settings

Specify the following item, and then click [Next].

[User Group Name]

Enter the user group name.

[Description]

As needed, enter descriptions for the user group.

[Parent User Group]

Specify the parent user group that user groups are affiliated with. When you click [Change], the created user group is displayed and you can select the user group.

[Access Profile]

Select access profile. For the users affiliated with this user group, the access profile set here is applied if access profile is not set.

You can also click “Create Access Profile” under the drop-down list box to create a new access profile.



Refer

"Adding access profile" (P.140)

[External ID]

Enter the external ID as necessary.

The external ID is available when you coordinate the external system with user groups.

[Access to User Portal]

- [When setting with Access Profile]
Set the privilege using Access Profile.
- [When allowing Web Print only]
Regardless of the settings of Access Profile, only Web Print is allowed on the User Portal screen.

(2) Associate with users

Specify the following item, and then click [Next].

[User Association]

[On]

When you add users to user groups, select [On] and add the users according to the following procedure.

(1) Click [Add] to display the [Add User] dialog box.

(2) Attach the check mark to the user to be added, and then click [Add].



Note

- The user can be added only when the user is enabled.
- To add all users, click [Add All] in the [Add User] dialog box.
- To narrow down from the users displayed in the [Add User] dialog box, enter the user ID or a part of user's name you want to search into , and then press the <Enter> key.
- To delete the user association, click [Delete] or [Delete All].
- Selecting a user affiliated with another group causes an affiliated user group transition.

[Off]

Select when you do not associate users.

(3) Associate with users

Specify the following item, and then click [Next].

[Account Association]

Set this only for cost management. A user can use all the accounts associated with him/herself and with the affiliated user group.



Note

In the [Cost Management] menu too, you can associate accounts with user groups. The same settings are applied in either operation.

[On]

If you associate accounts with user groups, select [On] and associate the account according to the following procedure.

(1) Click [Add] to display the [Add Account] dialog box.

(2) Attach the check mark to the account name to be associated, and then click [Add].



Note

- The account can be added only when the account is enabled.
- To add all accounts, click [Add All] in the [Add Account] dialog box.
- To narrow down from the accounts displayed in the list of accounts to associate with, enter a part of account name you want to search into , and then press the <Enter> key.



Refer

[Enable Account] (P.205)

(3) When you have associated several accounts with the user group, use [Default Account] to select the default account for the users associated with the user group.



Note

To delete the account association, click [Delete] or [Delete All].

[Off]

Select when you do not associate accounts with the user group.

(4) Overview

After you check the configured setting, clicking [Save] will create the user group.

You can click [Edit] for each item to change the settings.

Checking User Group Information

Click  in the user group list and select [Properties].

You can display and edit the content configured for the user group. You can edit the same items as in “Creating user groups” (P.128).



Note

User Group ID in the displayed items is the value automatically specified by the system. Impossible to be changed.

Copying User Groups

Click  in the user group list and select [Copy].

You can copy the settings of a user group, and create a new user group. When copying, you can edit the setting items. You can edit the same items as in “Creating user groups” (P.128).



Note

The user association information will not be copied.

Deleting user groups

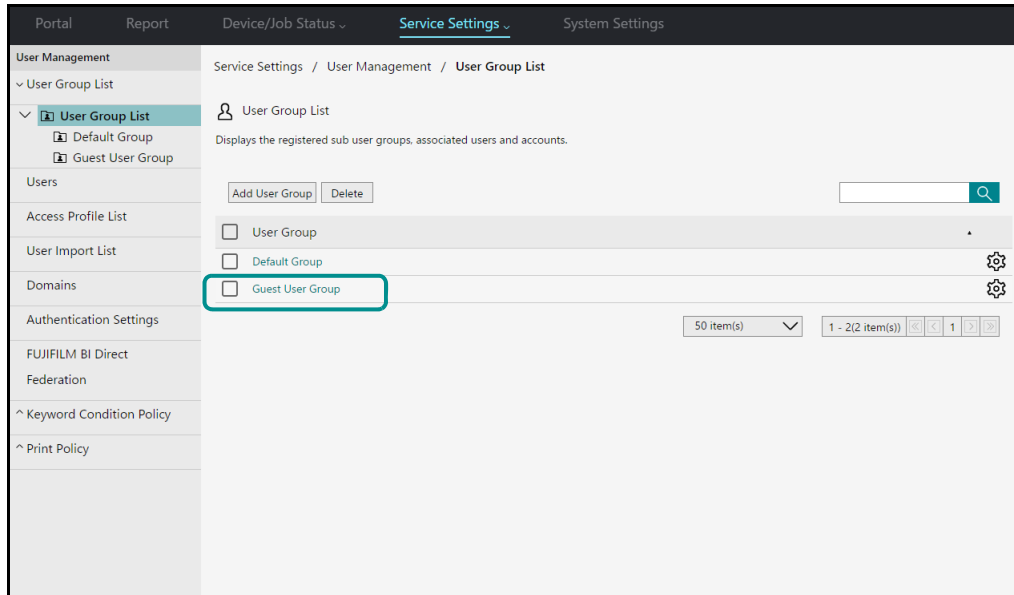
Click  in the user group list and select [Delete].

When there is any user in the user groups to be deleted or there is any lower user group, all users and user groups in the groups are moved to the default user groups (Default Group) with the same hierarchy structure.

User Group List (Details of User Groups)

How to Display

Click existing user groups and sub-user groups in the side menu, or click the names of groups in the user group list.

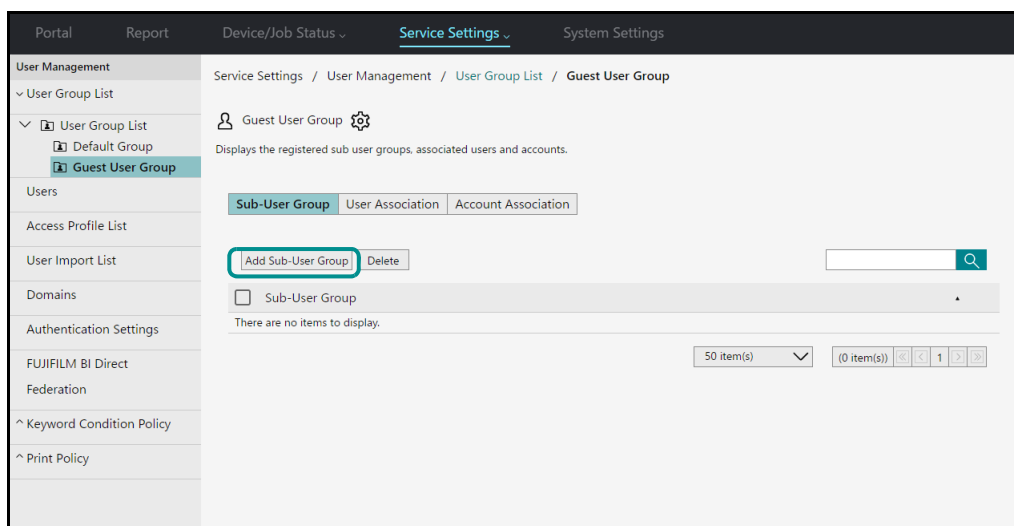


Page Summary

Add association with lower sub-groups, the associated users, and accounts to the user group and sub-user group you have selected.

Creating sub-user groups

Display the [Sub-User Group] tab and click [Add Sub-User Group]. Add lower sub-user groups to the user group (or sub-user group) you have selected.



The items to be set are the same as in "Creating user groups" (P.128).

Checking Sub-User Group Information

Click  in the sub-user group list and select [Properties].

You can display and edit the content configured for the sub-user group. You can edit the same items as in "Creating user groups" (P.128).

Copying Sub-User Groups

Click  in the sub-user group list and select [Copy].

You can copy the settings of a sub-user group, and create a new sub-user group. When copying, you can edit the setting items. You can edit the same items as in “Creating user groups” (P.128).



Note

The user association information will not be copied.

Deleting sub-user groups

Display the [Sub-User Group] tab. Click  of the sub-user group to be deleted in the list and select [Delete].

The operation is the same as that in “Deleting user groups” (P.130).

Changing User Association

Display the [User Association] tab.

The list of the users affiliated with the user group (or sub-user groups) selected is displayed. When you click [Edit List], the User Association page is displayed and you can add or delete users.

Note that the users associated with “Default Group” cannot be deleted from the list.

Changing Account Association

Display the [Associate Account] tab.

The list whose accounts are affiliated with the user group you have selected (or sub-user groups) is displayed. When you click [Edit List], the Account Association page is displayed and you can add or delete accounts.

User List (All Users)

How to Display

Select [Service Settings] > [User Management] > [Users] from the menu on the administrator screen.

Page Summary

Register and manage the users who use devices. You can add users, edit and delete property, switch validity and invalidity and unlock the users.



Note

The order for [First Name] and [Last Name] displayed in the list depends on [Display Settings] in [Common Settings].

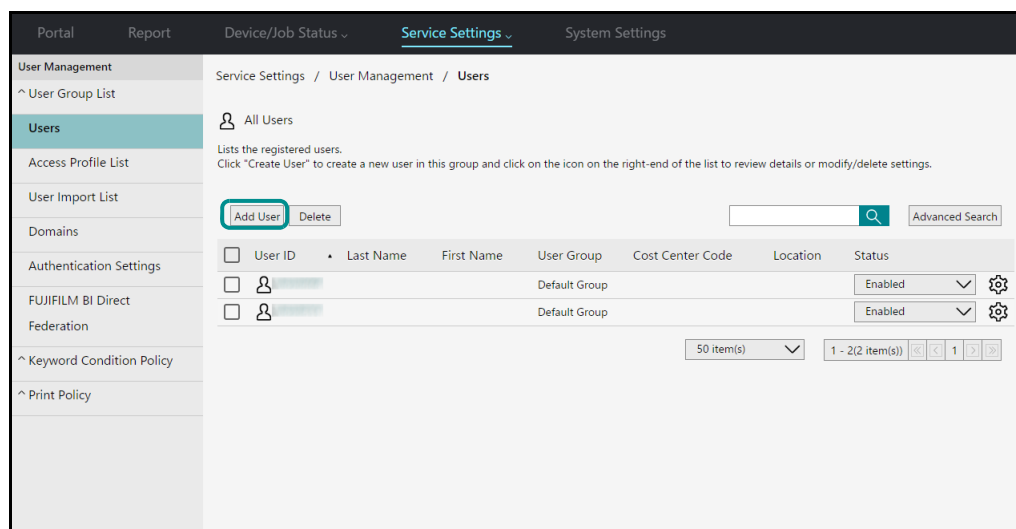


Refer

“Display Settings” (P.44)

Adding users

Click [Add User].



(1) User Settings

Specify the following item, and then click [Next].

[First Name]

Enter the first name of the user.

[Last Name]

Enter the last name of the user.

[Display Name]

Enter the display names of users.



Note

When you update added users to a device, set them with up to 16 double-byte characters and 32 single-byte characters. If you set the display name of users with more characters than these numbers, you cannot update them to a device.

[Furigana]

Enter the display names (furigana) of users.

[Index]

Enter the index characters used for the index search of recipient table. You can enter characters "A-Z". When nothing is entered, the leading character is automatically recognized according to the priority order from furigana, display name, and user ID, and the recognized character is entered automatically.

[Parent User Group]

Click [Edit] and select the user group to be affiliated with. In default settings, "Default Group" is set.

[E-mail Address]

Enter the e-mail address of users. Click  and you can set more than one. To set several, click [Set As Default] for the e-mail address as default.

E-mail addresses are not case-sensitive.



Note

Even when several e-mail addresses are set with a user, the e-mail is sent only to the e-mail address that is specified in "Set As Default".

[User ID]

Enter ID to identify users.

The User ID is not case sensitive.



Note

Make sure that to update user information to an actual device, the user ID has the character type and number of characters which are usable in the device. The users who do not follow the device restriction cannot be updated to the device.

[Alternate User ID]

For more than one setting of the user ID, enter the alternate user ID. Click  and you can set more than one.

If you set the alternate user ID, one user can log in, print the print job transmitted with several different user IDs at one time and display job lists.



Note

The alternate user ID is not available at the time of logging in to ApeosWare Management Suite and authentication with a device.



Refer

"Alternate User ID" in "Installation and Operation Guide"

[Password]

Enter a user password.

When a password or PIN is input at the time of authentication in a device, it is verified by this password.

Passwords are case sensitive.



Note

You can set the minimum character number of a password and the necessary character type in the [Authentication Settings] page.



Refer

"Set authentication features" (P.172)

[Alternate Authentication ID]

Specify the authentication ID that you use for authentication with the ID other than the user ID. Click  and you can set more than one.

- [Card ID (PAN)]

It is the "card ID" at the time of the card authentication by using the IC card reader.

You can manually enter the card ID (PAN) in the device where the authentication method is set to [Custom Authentication].

- [External ID]

It is the ID managed by the external user management system. It is available in the device where the authentication method is set to [Custom Authentication].

**Note**

- If you use a copy card for authentication, set only a single seven or less digit number for the card ID (PAN) (for use of a copy card for authentication, the setting in the device is necessary).
- When you use the alternate authentication ID, you need to set [Enter Authentication ID] in the [Authentication Settings] page.
- When you log in to ApeosWare Management Suite from a PC, the alternate authentication ID is not available.
- When you edit user information imported from Active Directory to ApeosWare Management Suite, delete the value of [Card ID/PAN] of [Attribute Mapping] in the [User Import] setting.

**Refer**

"Set authentication features" (P.172)

[External Accounting ID]

Enter the ID to use when working with the external accounting system. This ID is not available for authentication.

[User Account Expiration Date]

Set the user account expiration date in either one of the following methods.

- [End Date Settings]
Specify the date and time for the user account expiration date. If you set only date, the user becomes disabled from the next day on. If you specify date and time, when the date and time are past, the user becomes disabled.
When you select [End Date Settings] and leave the date text box blank, the indefinite period is set.
- [Valid Period Since Last Login {n} days]
If the setup validity period is past after the last ApeosWare Management Suite login, the user becomes disabled. You can set the validity period in [Valid Period Since Last Login by User] of the [Authentication Settings] page.

**Refer**

"Authentication Settings" (P.172)

[Status]

To make users valid, select a checkbox. You can switch the user status through the user list.

**Note**

When the user validity period is past and the user becomes disabled, [Status] cannot be changed. In that case, make [End Date Settings] of [User Account Expiration Date] blank or set the future date.

[Cost Center Code]

Set this only for cost management.

Enter the cost center code. You can create a report by tallying per "cost center code".

[Storage Location]

Enter the storage destination of documents (path name) in the UNC format when using the "scanner (my folder storage)" feature of the device.

Example: \\192.0.2.1\share\myfolder

[Location]

Enter information such as address and floor as necessary.

[Access Profile]

Specify access profile to apply to users. If you do not, the access profile set for the user group which the users are affiliated with is applied.

You can also click "Create Access Profile" under the drop-down list box to create an access profile.



Refer

"Adding access profile" (P.140)

[Description]

Enter descriptions for the access profile as necessary.

[Details]

Enter the personal information on users including link to pictures, phone numbers, and fax numbers. By clicking , you can set more than one fax numbers.

[FUJIFILM BI Direct Federation]

To enable single sign-on authentication for FUJIFILM BI Direct, configure the user ID (e-mail address) to be registered in FUJIFILM BI Direct.



Note

If the user ID is not configured, user information will not be updated in FUJIFILM BI Direct systems even after linking an access profile with a tenant.

[Approver]

Specify the user ID of the approver when Approval Print is enabled. Click [Settings] to display the [Approver Settings] screen and set the user. Click  and you can set more than one approver.

[Special Approver]

Specify the user ID of the user assigned to Special Approver.

When setting by importing the special approver, be sure to set the attribute values for Active Directory/LDAP so that the approver will be set as well.

If an import is performed without setting the approver (a user for which attributes associated with the approver are blank, and with values only for attributes associated with the special approver is imported), the approver and special approver of that user will be imported with blank values. In that case, if Approval Print is performed with that user, the print job will be canceled as the approver is not set.



Note

- When multiple approvers are registered, conduct approval operation in the registration order.
- When the user registered as an approver is deleted during the period from issuance of a print job to output of it, cancel the print job.
- Up to nine approvers can be specified.
- A special approver cannot be specified unless an approver is specified.

(2) Account Association

[Account Association]

Set this only for cost management. Specify the following item, and then click [Next].



Note

In the [Cost Management] menu too, you can associate accounts with users. The same settings are applied in either operation.

[On]

When you associate accounts with users, select [On] and associate the account according to the following procedure.

- (1) Click [Add] to display the [Add Account] dialog box.
- (2) Attach the check mark to the account name to be associated, and then click [Add].

**Note**

- The account can be added only when the account is enabled.
- To add all accounts, click [Add All].
- To narrow down from the accounts displayed in the list of accounts to associate with, enter a part of account name you want to search into ,  and then press the <Enter> key.

**Refer**

"[Enable Account]" (P.205)

- (3) If you have associated several accounts with user, use [Default Account] to select the default account.

The default account is used when you try to operate an account although it is not selectable.

**Note**

To delete the account association, click [Delete] or [Delete All].

[Off]

Select when you do not associate accounts with users.

**Note**

To use the device of [Custom Authentication] in the environment where the cost management feature is enabled, associate the user who use the device with the account. If the account is not set, the error "There is no available account" occurs when logging in to the device or accessing ApeosWare Management Suite from the device.

(3) Delegate Users settings

Specify the following item, and then click [Next].

[Delegate Users settings]

Set whether this user prints out a print job from other users as a delegate.

[On]

When enabling the user to print the job as a delegate, select [On] and add the delegate user according to the following procedure. This user as a delegate becomes able to print out a print job of [Delegate Users] added here.

It is available only in Print On Demand.

- (1) Click [Add] to display the [Add User] dialog box.
- (2) Attach the check mark to the user to be added, and then click [Add].

**Note**

- The user can be added only when the user is enabled.
- To add all users, click [Add All].
- To narrow down from the users displayed in the delegate users list, enter the user ID you want to search into  , and then press the <Enter> key.

[Off]

Select when you are not adding a user.

(4) Overview

After you check the configured setting, clicking [Save] will create the user.

You can click [Edit] for each item to change the settings.

Narrowing Down Users

To narrow down from the users displayed in the [User List] dialog box, enter the information of user you want to search into , and then press the <Enter> key.

You can also narrow down by clicking [Advanced Search], selecting conditions from the pull-down menu, and then entering information into the text box as needed.

Checking User Information

Click  of the user list and select [Properties].

Deleting users

Click  of the user list and select [Delete].

When the users are deleted, the following information is deleted too.

- User information set for the device, the folder whose owner is the user, and the document reserved in the folder
- Job flow whose owner is a user and which is set for a device

Switching validity and invalidity of users

Select [On] or [Off] from [Status] of the user list.

However, when [User Account Expiration Date] set for users expires and become disabled, [Status] cannot be changed. In that case, enable it according to the following procedure.

- When [End Date Settings] is set for [User Account Expiration Date] and the end date expires
In editing user property, leave blank [End Date Settings] set for [User Account Expiration Date] or set a future date.
- When [Valid Period Since Last Login {n} days] is set for [User Account Expiration Date] and login is not operated within the valid period.

In editing user property, select a checkbox for [Valid] set for [Status]. The validity period is extended, starting on the operation date.

Unlocking users who are locked out

[Lock Out] is selected for lockout users in [Status] of the user list. If you select [On], lockout is unlocked.

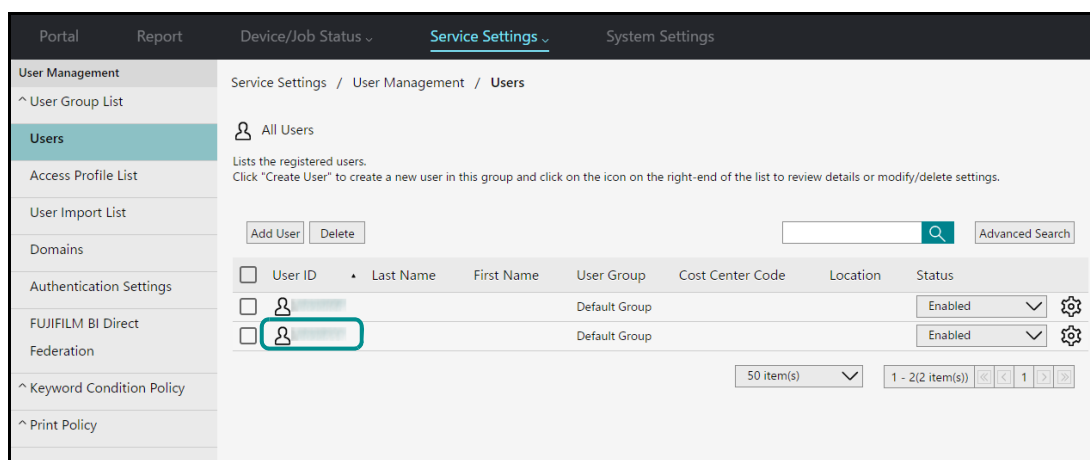


If [User Account Expiration Date] expires and become disabled after lockout, [Status] cannot be changed. In that case, in editing user property, set [User Account Expiration Date] to a future date.

User List (Details of Users)

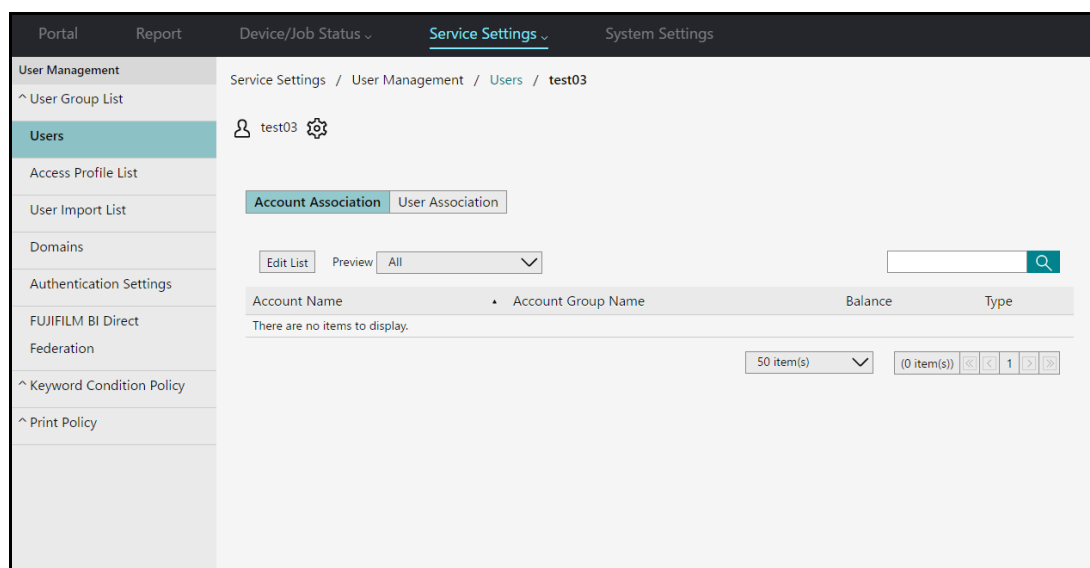
How to Display

Click the user name link in the user list.



Page Summary

Add association with an account and delegated users to the selected user.



Changing User Association

Display the [User Association] tab.

The information on the selected user is displayed. When you click [Edit List], the User Association page is displayed and you can add or delete users.

Changing Account Association

Display the [Associate Account] tab.

The list of accounts associated with the selected user is displayed. When you click [Edit List], the Account Association page is displayed and you can add or delete accounts.

Access Profile List

How to Display

Select [Service Settings] > [User Management] > [Access Profile List] from the menu on the administrator screen.

Page Summary

Set access profile for which access rights to usable devices and each feature are set. You can add access profile, edit, copy, and delete Properties.

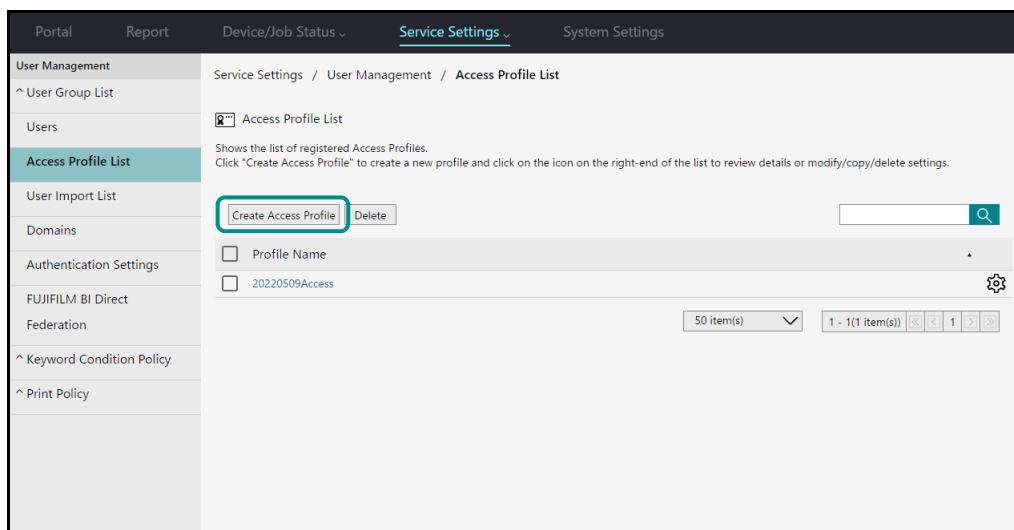


Refer

“What Is Access Profile?” in “Installation and Operation Guide”

Adding access profile

Click [Create Access Profile].



(1)Access Profile Settings

Specify the following item, and then click [Next].

[Access Profile Name]

Enter the access profile name.

[Description]

Enter descriptions for the access profile as necessary.

[Require PIN/Password Input]

This setting is valid only in the device where the authentication method is [Custom Authentication] or the mobile device.

Specify whether you use PIN or a password at the time of authentication of users.

- [On]
PIN or a password is used.
- [Yes (For Authentication ID Only)]
Password is not used when authenticating using the card.
When entering the authentication ID, use the password.

- [Off]
No PIN or password is used.
- [Follow Device Group Settings]
At the time of authentication with a device, follow the values of [Require PIN/Password Input] set for the device group.
At the time of authentication with a mobile device, follow the values of [Enforce PIN/password during device/mobile authentication] set in the [Authentication Settings] page.
- [Follow Authentication Common Settings]
Follow the values of [Enforce PIN/password during device/mobile authentication] set in the [Authentication Settings] page.

When [Yes] or [Yes (For Authentication ID Only)] is selected, specify the operation when the PIN or password is not set upon login in [When PIN/Password is not set].

There are the following two options for [When PIN/Password is not set].

- [Display Cancel screen]
The login screen is displayed.
If the PIN or password is not set, you cannot log in to ApeosWare Management Suite.
- [Display PIN/Password Setting screen]
The PIN/Password Setting screen is displayed.
When the PIN or password is not set, set the password in the PIN/Password Setting screen. When the password is set, even if it is expired, the PIN/Password Setting screen is not displayed.



Note

This setting is not applicable to the password with which you log in to ApeosWare Management Suite from a PC.



Refer

- "Add Device Group" (P.77)
- "Set authentication features" (P.172)

[Display screen at login]

This setting is valid only when the authentication method of the device is [Custom Authentication].

Select the first screen to display from the followings when you push the [ApeosWare Menu] button on the menu screen using the control panel of the device or when you log in to the device.

- Print On Demand
Display the operation screen of Print On Demand in ApeosWare Management Suite.
- ApeosWare Management Suite Menu
Display the portal screen of ApeosWare Management Suite. In the portal screen, the menu buttons of each feature are displayed. The menus to be displayed depend on the setting status of option license and the setting content of [Access to File Management Service] of access profile associated with users.
- Device Screen
Displays the home screen of a device.



Refer

- "ApeosWare Management Suite Portal Screen" (P.116)
- "Device Home Screen" (P.113)

[Print on demand if there is a job]

When the [Print on demand if there is a job] checkbox is selected, if there are any pending print jobs at the time of login, then regardless of the [Display screen at login] setting, the operation screen of Print On Demand will be displayed.

If there are no pending print jobs, the screen selected in [Display screen at login] will be displayed.

[Display screen when “Home” button is pressed]

Select the screen to display when you push the Home button () in the upper right of the operation screen of ApeosWare Management Suite using the control panel of the device.

- ApeosWare Management Suite Menu
Display the portal screen of ApeosWare Management Suite.
- Device Screen
Displays the home screen of a device.



Refer

- “ApeosWare Management Suite Portal Screen” (P.116)
- “Device Home Screen” (P.113)

[Allow Device Use]

Select a checkbox for operation to be allowed to use.

- Print operation (color/black and white)
- Color operation (color/black and white)
- Scan operation
- Fax operation

However, The settings in “(4) Device/Device Group Permission Settings” (P.148) is more prioritized than the values set here.



Note

Direct Fax is not a target for this setting.

[Access device that cannot connect to network]

This setting is applied only when for the settings of the device group that a device is affiliated with, the authentication method is set to [Custom Authentication] and [Access device that cannot connect to network] is set to [Allow].

Select the checkbox when you allow user’s operation even for the devices that cannot be connected to the ApeosWare Management Suite server.

When you select the checkbox for [Allow], user information is held in the device for a case that connection to the ApeosWare Management Suite server becomes impossible due to a network failure or some other reasons. Therefore, authentication is executed even in the offline device, and the user becomes able to use the features of the actual device. The card authentication and authentication by user ID input are available for an offline device.



Note

- For offline authentication, be sure to set [Card ID (PAN)] in the [Alternate Authentication ID] of user property.
- If you select a checkbox for [Stop] in the [Force stop when minimum balance is reached] of access profile, you cannot set this item to [Allow].

[Display Usage]

Specify the information type to be displayed when the  button on the ApeosWare Management Suite menu screen on the multifunction device is pushed.

When [Standard] is selected, the number of printed sheets of the user and CO2 emissions are displayed on a popup screen.

When [Detailed (With Cost Reduction Information)] is selected, the user's output impressions of copy/print and whether the actual cost reductions achieved the target are displayed on the usage status screen.

The following items are specified when [Detailed (With Cost Reduction Information)] is selected.

- [Display at Login]

This setting is valid only when the authentication method of the device is [Custom Authentication]. Also, you can set it only when [ApeosWare Management Suite Menu] is selected for [Display screen at login].

Specify whether to display the usage status screen forcibly after logging in the device. When displaying it, select [Always Display] or [Display If Likely Below Target].

If you select [Display If Likely Below Target], the usage status screen is displayed when [2 Sided Rate] or [Pages per Side Rate] fell below the target value by 10%, or [Color Rate] exceeded the target value by 10%.

- [Target]

Specify the cost reduction target value in percentage.



Refer

"ApeosWare Management Suite Portal Screen" (P.116)

[Force Print]

Specify whether to forcibly execute black & white print, 2 sided print, or 2 pages print.

If you select a checkbox, the print job of the user is forcibly executed with black and white, two-sided print, or 2 pages regardless of the settings of [Force Black & White], [Force 2 Sided], and [2 Pages] in the print rules.

If you remove the check mark, the settings of [Force Black & White], [Force 2 Sided], and [2 Pages] in the print rules are applied to the print job.

[Auto Print at Login]

Specify whether to allow "print without list" when executing Print On Demand.

- [On (Always)]

If there are pending print jobs, the list screen is not displayed after authentication, and the print job sent by the user to the server is sent and printed as-is.

If there are no pending jobs, the screen selected in [Display screen at login] will be displayed.

- [On (if there is only one job)]†

If there is one pending print job, this is printed as-is after authentication. If there are two or more jobs, and [Print on demand if there is a job] is enabled, the operation screen of Print On Demand is displayed. For other cases, the screen selected in [Display screen at login] will be displayed.

- [Select on confirmation screen]†

If there are pending print jobs, the print confirmation screen is displayed after authentication. If there are no pending print jobs, the screen selected in [Display screen at login] will be displayed.

- [Off]

If [Print on demand if there is a job] is enabled, and there are pending print jobs, the operation screen of Print On Demand is displayed. For other cases, the screen selected in [Display screen at login] will be displayed.

Options indicated with † are only enabled when using custom authentication. If other than custom authentication is used, the operations will follow the [Off] setting.



Refer

Print With a List and Print Without a List → “Installation and Operation Guide”

[Change Job Settings in Control Panel]

Specify on the control panel of the multifunction device whether to allow the change of print settings such as change from 1 sided print to 2 sided print.

[Access to File Management Service]

Select a checkbox for the file management service that access is allowed when working with the file management service.

[Mobile Settings]

When you allow control from the mobile device, select a checkbox for [Allow] and control to be allowed.

[Force stop when minimum balance is reached]

Set this only for cost management.

If you select a checkbox for [Stop], the users are restricted as follows.

- When the account balance that users are using falls below the value of the set [Minimum Balance], the service job is forcibly stopped (force stop operation depends on service).
- The user can log in the devices where the authentication methods are [Custom Authentication] and [Remote Authentication (ApeosWare Authentication Agent)]. If you try to log in to the device where the authentication method is [Local Authentication], an error occurs.
- User registration in the device of [Local Authentication] is not executed.
- In [Remote Authentication (ApeosWare Authentication Agent)], If a user whose specified account is not set tries to log in, an error occurs.
- When using serverless on-demand printing, set an existing account.
- If the user registered with ApeosWare Management Suite is using an Internet Service, please set an existing account.



Note

- If you select a checkbox for [Allow] in the [Access device that cannot connect to network] of access profile, you cannot set this item to [Stop].
- Fax is not for force stop when the minimum balance is reached.
- Some models do not correspond to the [Force stop when minimum balance is reached] feature. For details, please refer to “Readme”.
- This configuration can only be used by models that do not support custom authentication if the print method is set to [Direct Print] or printing is performed using the On Demand Print Terminal.
- The job is canceled only when the balance is insufficient at a timing the print server receives a printing job.

If the following conditions are satisfied, you can use [Force stop when minimum balance is reached] when printing with Print On Demand Without a List.

- IC Card Gate 2/IC Card Gate 3 and the printer are connected to the network.
- IC Card Gate 2/IC Card Gate 3 is authenticated directly to Active Directory.

However, there are the following notes.

- Available in Remote Authentication (Active Directory). (Unavailable in [Local Authentication] and [Remote Authentication (ApeosWare Authentication Agent)]).
- Available for the billing target printer.



Refer

Concerning balance → "Installation and Operation Guide"

[Using shared account that all users can use]

Set this only for cost management.

If you select a checkbox for [Allow], you can use the shared account where [Enable shared account for all users to use] is enabled.



Refer

"Installation and Operation Guide"

[Use without specifying account]

Set this only for cost management.

Normally specifying an account is necessary for the use of a device, but if you select a checkbox for [Allow], you become able to use a device just by entering your directions without specifying an account.

The job operated without specifying an account is recorded in [Non Account Associated Job List]. A user can replace the job cost with an appropriate account after operation.



Refer

"Installation and Operation Guide"

[Print Popup Settings]

Set the popup notification screen to be displayed on a client PC when you transmit a print job. Select a checkbox for the screen to be displayed.



Note

To display the popup notification screen, you need to install Popup Messenger on the client PC.



Refer

Install Popup Messenger → "Install Popup Messenger" (P.269)

- [Display Popup Screen]
Display the popup notification screen on a client PC transmitting print.
- [Display balance on screen]
Display the balance of cost management on the popup screen.
- [Allow Change Job Owner]
Display [User Name] on the popup notification screen. When [User Name] is displayed, you become able to execute print-out with a name different from the owner of the print job. If you want to separate a print transmitter from a person charged for print, select a checkbox.
- [Ignore Print Rule]
Display [Do Not Apply Print Rule] on the popup notification screen. If you allow print for which the print rules are ignored, select a checkbox.
- [Select Accounts]
Display the account selection screen on the popup notification screen. Users become able to execute print by changing an account for use.

[Notification Settings]

When you select the checkbox for [Display Print Job Status in Popup Screen], the popup notification screen appears on the client PC when the print job is canceled by the process of ApeosWare

Management Suite. On the notification screen, the name of the print job and the reason of the cancelation is described.



Note

To display the popup notification screen, you need to install Popup Messenger on the client PC.



Refer

- "Color Print Warning Notification" (P.276)
- Install Popup Messenger→"Install Popup Messenger" (P.269)

[Access to User Portal]

Specify whether to allow access to the user screen.

When you select the checkbox for [Allow], on the header of the operation screen in ApeosWare Management Suite, [User Portal], a link to the user screen, is displayed.

For [Allow], specify the following too.

- [Change E-mail Address]

If you select a checkbox, users themselves can change their e-mail address set for them.

- [Change Storage Location]

If you select a checkbox, users themselves can change the storage destination of documents when using the "scanner (my folder storage)" feature of the device.



Note

If you do not allow [Access to User Portal] for setting, the user screen cannot be displayed. In that case, users cannot change a password by themselves either.

[View and edit report]

Specify whether to allow users to view and edit a report.

- [Disallow]

The report menu is not displayed in the [Report] page on the administrator screen.

- Allow [Generate] only.

You can browse reports in the [Report] page on the administrator screen. You cannot customize reports and change conditions.

- [Allow]

You can create, display, and customize reports in the [Report] page on the administrator screen.

[Administrator Permission Settings]

Select a checkbox for the administrator permission to set for users. You can select more than one administrator permission. The first page to be displayed when logging in and the accessible pages depend on the administrator permission set here.

- System Management
- User Management
- Account/Balance Management
- Guest Job Management
- Device Management
- On Demand Print Terminal Management
- Image Log Control
- Image Log Search/Monitoring

- User group

**Note**

- [System Manager] and other administrator permissions are linked together. If you attach the check marks to all of [User Management], [Account/Balance Management], [Guest Job Management], [Device Management], and [On Demand Print Terminal Management], the check mark is attached automatically to [System Manager]. Moreover, if you remove any one of those permissions, the check mark for [System Manager] is removed too.
- The users with only [On Demand Print Terminal Management] permission cannot log in to the operation screen of ApeosWare Management Suite.
- Select the target group of [Image Log Search/Monitoring] from [User Group]. Select either [All] or [Select]. When you select [Select], you can select a user group to add in the [Select Additional User Group] dialog box.

**Refer**

"Access Permissions to the Operation Screen" (P.18)

[Change Scan to E-mail Sender]

Specify whether to allow the change of e-mail senders when Email.

If you select a checkbox, you can change the e-mail sender in the control screen when the user Email.

If you remove the check mark, the e-mail address of [Sender] set in [Service Settings] > [Scan Settings] > [Email Settings] is used as the Sender of Email that was executed by the user.

(2) Associate With Print Queue

Specify the following item, and then click [Next].

[Associate With Print Queue]

[On]

To associate print queues with a user, select [On] and add the print queue according to the following procedure.

With a checkbox selected for [Associate All Device Groups], the users using this access profile can use all the print queues.

The user using this access profile can use only the print queue added here.

(1) Click [Add] to display the [Print Queue] dialog box.

(2) Attach the check mark to the print queue you wish to add, and then click [Add].

**Note**

To add all print queues, click [Add All].

(3) Select [Default Print Queue].

**Note**

To delete the association with print queue, click [Delete] or [Delete All].

[Off]

Select when do not add the print queue.

(3) Associate With Devices/Device Groups

Specify the following item, and then click [Next].

[Associate With Device Groups]

[On]

When you associate the device group with the user, select [On].

With a checkbox selected for [Associate All Device Groups], the users using this access profile can use the devices affiliated with all device groups.

To restrict device groups for use, uncheck the checkbox for [Associate All Device Groups] and select the device groups you allow for use according to the following procedure.



Note

If you select a checkbox for [Associate All Device Groups], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Device Group] dialog box.

(2) Attach the check mark to the device group that you wish to add, and then click [Add].



Note

- To add all device groups, click [Add All].
- To delete the association with device groups, click [Delete] or [Delete All].

[Off]

Select when you do not add the device group.

[Associate With Devices]

[On]

When you associate devices with the user, select [On].

With a checkbox selected for [Associate All Devices], the users using this access profile can use all devices.

To restrict devices for use, uncheck the checkbox for [Associate All Device Groups] and select the devices you allow for use according to the following procedure.



Note

If you select a checkbox for [Associate All Devices], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Device] dialog box.

(2) Attach the check mark to the device that you wish to add, and then click [Add].



Note

- To add all devices, click [Add All].
- To delete the association with device, click [Delete] or [Delete All].

[Off]

Select when you are not adding a device.

(4) Device/Device Group Permission Settings

Specify the following item, and then click [Next].

The device and device groups selected in (3) are set to permissions set in [Allow Device Use] of “(1) Access Profile Settings” in default settings. Only if you change this setting separately, set the following.

[Set Permission to Device Group]

When you change permissions of device groups separately, select [Yes] and specify the device groups for the setting change and permissions. Click  and you can set more than one.

[Set Permission to Device]

When you change permissions of devices separately, select [Yes] and specify the devices for the setting change and permissions. Click  and you can set more than one.

If you set both devices and device groups to permissions, the devices is prioritized.

(5) Policy Settings

Associate the policy created in “Keyword Condition Policy” (P.176) and “Print Policy” (P.179) with the access profile.

When associating the print policy, select either “Add Forcibly” or “Select by User” for watermark. When you select “Select by User” and set “On” to the default value, the settings by the device are applied.

(6) Overview

After you check the configured setting, clicking [Save] will create the access profile.

You can click [Edit] for each item to change the settings.

Checking Access Profile Information

Click  in the access profile list and select [Properties].

You can display and edit the content configured for the access profile. You can edit the same items as in “Adding access profile” (P.140).

Copying Access Profile

Click  in the access profile list and select [Copy].

You can copy the settings of an access profile, and create a new access profile. When copying, you can edit the setting items. You can edit the same items as in “Adding access profile” (P.140).

Deleting access profile

Click  of the access profile list and select [Delete].

Changing Print Queue Association

Click the profile name link from the list to display the [Associate With Print Queue] tab on the page that appears.

A list of print queues associated with the selected access profile is displayed.

When you click [Edit List], the Associate With Print Queue page is displayed and you can edit the print queue association.

Changing Devices/Device Groups Association

Click the profile name link from the list to display the [Associate With Devices/Device Groups] tab on the page that appears.

A list of devices/device groups associated with the selected access profile is displayed.

When you click [Edit List], the Associate Devices/Device Groups page is displayed and you can edit the device/device group association.

User Import List [User Import] Tab

How to Display

Select [Service Settings] > [User Management] > [User Import List] from the menu on the administrator screen and display the [User Import] tab.

Page Summary

Automatically import user information managed by the remote authentication server and by the files into ApeosWare Management Suite by specifying a schedule.

You can specify one of the following for the inbound channel of user information.

- Active Directory/LDAP/Microsoft Entra Domain Services (Microsoft Entra ID DS)

Import user information from Active Directory, LDAP server, or Microsoft Entra ID server.

For details, refer to “Create an import schedule (Active Directory/LDAP/Microsoft Entra Domain Services (Microsoft Entra ID DS)) import)” (P.150)

- Import File

Import user information from the CSV file or the text file.

For details, refer to “Create an import schedule (Import file)” (P.159)

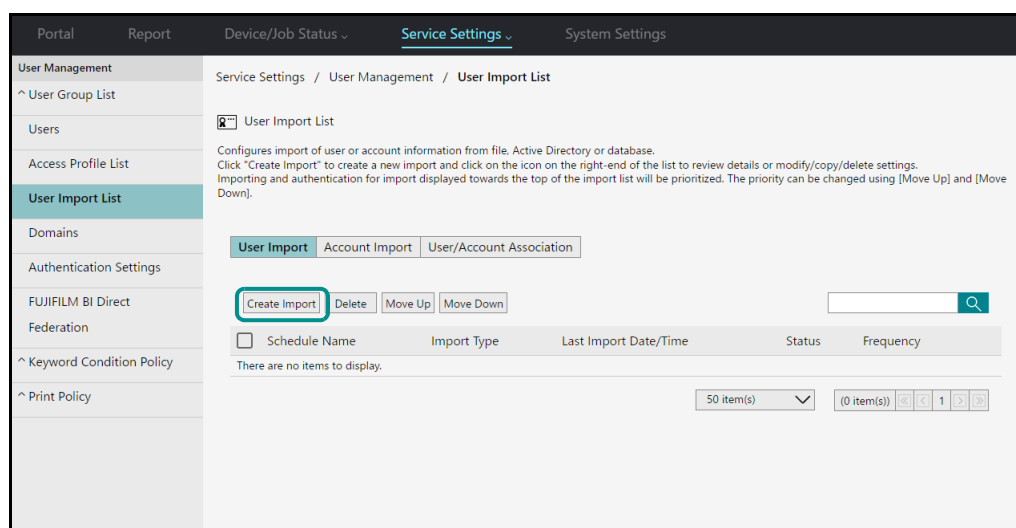
- Database

Import user information from external database.

For details, refer to “Create an import schedule (Database import)” (P.164)

Create an import schedule (Active Directory/LDAP/Microsoft Entra Domain Services (Microsoft Entra ID DS)) import)

Click [Create Import].



(1) Inbound channel selection

Select the inbound channel of user information, and then click [Next].

Hereafter, the items in the situation where you have selected [Active Directory/LDAP/Microsoft Entra Domain Services(Microsoft Entra ID DS)] are described.



Note

If [Microsoft Entra Domain Services (Microsoft Entra ID DS)] is selected as the import source, after importing the user information, check the imported user settings, paying attention to the following points.

- When authenticating with a user imported from Microsoft Entra Domain Services, it is necessary that the AWMS server can access the login URL of the Microsoft Entra ID.
- When the ApeosWare Management Suite server is connecting to the login URL (login.microsoftonline.com) of the Microsoft Entra ID, if a proxy connection is necessary, check the [Connect using a proxy] check box.

(2) Details of the inbound channel

Specify the following item, and then click [Next].

[Domain]

Select a domain for import from the domains added in the [Domains] page.

[Management Scope]

Specify the scope to be imported into ApeosWare Management Suite out of the users on the remote authentication server. Click [Select] and specify the target organization unit (OU) . The import targets are the user and the group affiliated in the hierarchy under the specified organization unit (OU).



Note

You cannot set the individual user unit to [Start OU].

[Filter]

To restrict import targets to the specified users, specify the LDAP filter.

[Import Processing Method]

Select how to process import user information.

- [Add]
Process the import target user not existing on ApeosWare Management Suite as the new user. When the user for import is already in ApeosWare Management Suite, no processing is performed.
- [Update]
The target for update depends on the type of the remote authentication server in the inbound channel.

Remote authentication server	Target for update
For Active Directory or Microsoft Entra Domain Services	Among the target users for import with the remote authentication server, respective attributes are updated for the users whose attributes (including the attributes yet to be associated) are updated.
For LDAP	All users for import are targets for update. Update all the attributes of relevant users.

If the user for import is not in ApeosWare Management Suite, no processing is performed.

- [Add/Update]
Process all users for import as addition or update targets. When the user for import is already in ApeosWare Management Suite, an update is performed. Add them if none is found.
- [Delete]
Delete the users not for import from ApeosWare Management Suite.
- [All]
Process all users for import as adding, updating or deleting targets.
When the user for import is already in ApeosWare Management Suite, an update is performed. Add them if none is found. Also, delete the users not for import from ApeosWare Management Suite.



Note

For [Update], [Add/Update], or [All], all attribute values with attribute association will be updated.

(3) Attributes correspondence

Specify the following item, and then click [Next].

[User Settings]

Set each user attribute of ApeosWare Management Suite.

Select the attributes on the remote authentication server to correspond to user attributes from the drop-down list box or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Note

In direct input, if you put it in {}, it is recognized as an attribute of the remote authentication server.
Example: {description}

Be careful about the following when making an attribute correspond.

- If Active Directory or Microsoft Entra Domain Services is selected as the import source server, associate the following attributes with [User ID].
SAM format: {sAMAccountName}
UPN format: {userPrincipalName}
- Make sure that the user ID and display name used in the remote authentication server has the character type and number of characters which are usable in the device. The users who do not follow the device restriction cannot be updated to the device.
- Give an index to the attribute of the remote authentication server used for the card ID (PAN), the external ID, and e-mail addresses. Otherwise, it does not perform well at the time of authentication and may take time for authentication.
- With more than one correspondence to values, you can specify more than one e-mail address. If a standard e-mail address is not set at the time of update, the system determines one at random. If it is already set, the setting is held.

[Associate User with User Group]

To specify user groups to affiliate the users for import with , select a checkbox and specify the following items.

If you remove a check, the imported user is affiliated with the default user group (Default Group).

[User Group to Associate]

To create a new user group that users are affiliated with, click [Create] and select [How to Create].

To affiliate users with the existing user group, select [Existing] and specify [Parent User Group].

[How to Create]

Specify this item when you select [Create] in [User Group to Associate].

Select the creation method of the user group from either one of the following.

- [Specify Attribute/Group Name]
Sort out the users after import by the user attribute on the remote authentication server or specify an arbitrary user name and affiliate all users after import with the user group.
For details, refer to [Attribute/Group Name].
- [Select OU]
Make the Organization Unit (OU) which users affiliate with in the remote authentication server a user group unit after import. Specify the OU of which hierarchy becomes a user group in [OU that creates the group].

For details, refer to [OU that creates the group].

[Attribute/Group Name]

Specify this item when selecting [Specify Attribute/Group Name] in [How to Create]. There are two ways of specification below.

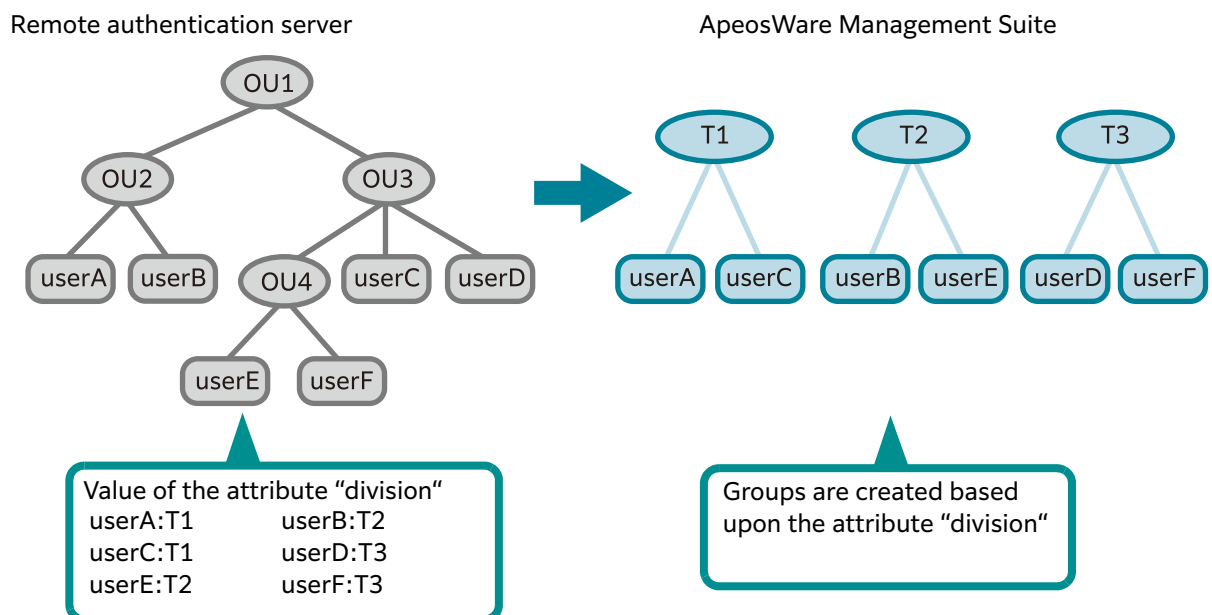
- When you sort out by the user attribute

Specify attributes on the remote authentication server to be used for the sort-out. You can select them from the drop-down list box.

If you input an attribute name directly, put it in {}. For example, if a user of the remote authentication server has the attribute of givenName, specify it with "{givenName}".

The users whose specified attribute values are identical are in the same groups. The name of the attribute is used for that of the user group. The user whose value is not set for the specified attribute is affiliated just under the user group specified in [Parent User Group].

Example: When you specify "{division}" in [Attribute/Group Name]



- When you create arbitrary user groups

Directly enter an arbitrary character string in [Attribute/Group Name]. One user group in which you have entered a name is created. All of the imported users are affiliated with this user group.

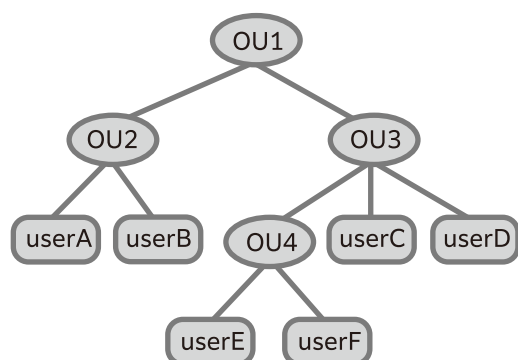


Note

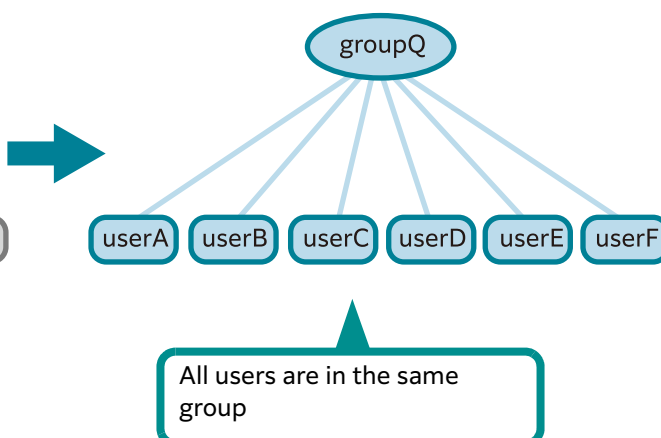
When creating an arbitrary user group, do not use "{}" for a user group name. Otherwise, it is recognized as an attribute name on the remote authentication server.

Example: When you specify "groupQ" in [Attribute/Group Name]

Remote authentication server



ApeosWare Management Suite



[OU that creates the group]

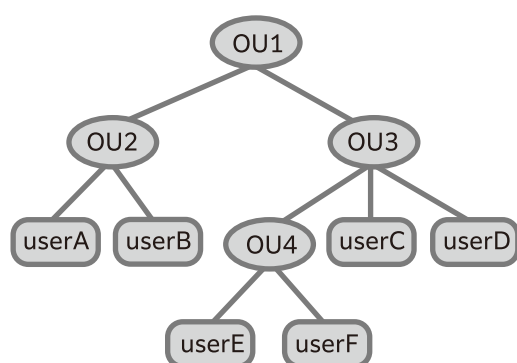
Specify this item when you select [Select OU] in [How to Create]. Specify the OU of which hierarchy becomes a user group from the following.

- All OU

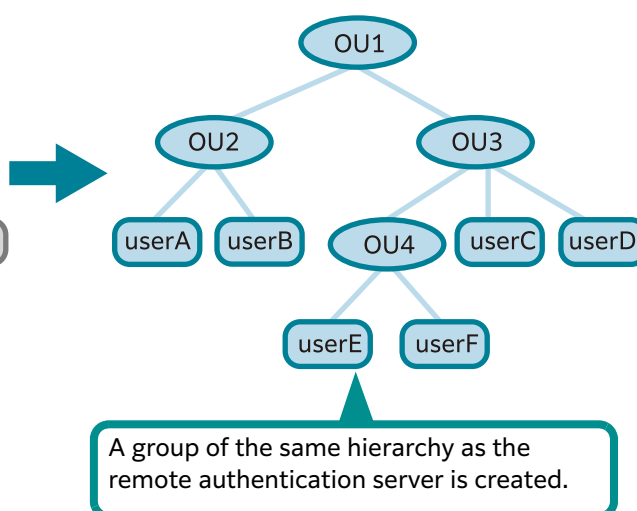
The OU on the remote authentication server becomes a user group after import with the hierarchy structure as it is. The OU name on the remote authentication server becomes a user group name.

Example:

Remote authentication server



ApeosWare Management Suite



- Specify a OU hierarchy

Specify a comparative hierarchy from import users in [No. of OU Hierarchy].

The OU in the specified hierarchy becomes a user group which users affiliate with after import. The OU name on the remote authentication server becomes a user group name.

[No. of OU Hierarchy]

Specify a hierarchy for user groups after import based on a relative position from users. Specify it with a positive number value of "0" or over.

0: Affiliated OU of user

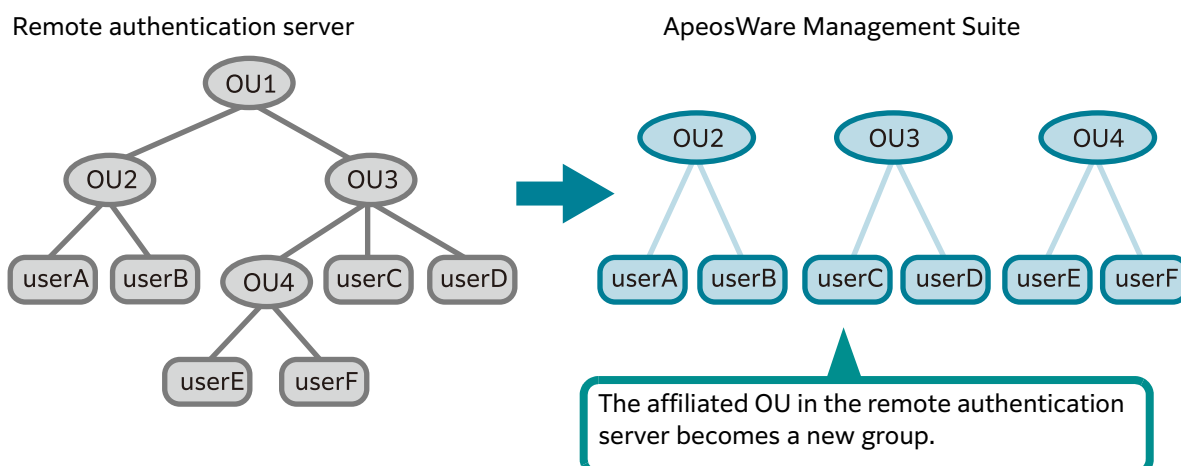
1: One hierarchy above the affiliated OU of user

2: Two hierarchies above the affiliated OU of user

Example:

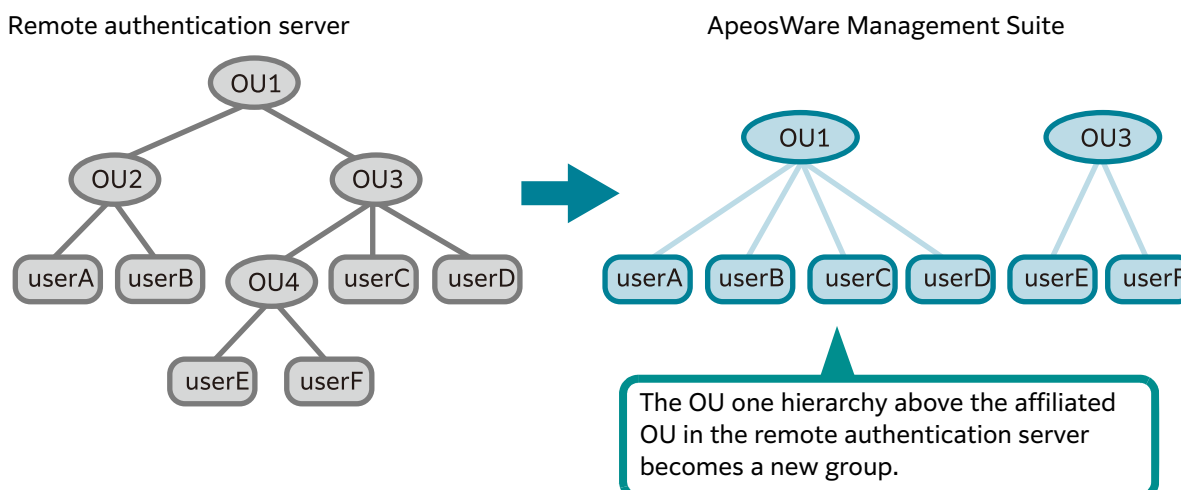
When you specify "0" for [No. of OU Hierarchy]

The OU that users were affiliated with in the remote authentication server becomes an affiliated user group after import.



When you specify "1" for [No. of OU Hierarchy]

The OU one hierarchy above the OU that users are affiliated with in the remote authentication server becomes an affiliated user group after import.



[Parent User Group]

Click [Change] and specify a user group.

When you select [Existing] in [User Group to Associate], the user group specified here becomes the user group that import users are affiliated with. When you select [Create] in [User Group to Associate], the user group becomes the parent user group of the user groups newly created.

[Update User Group]

This item is set when [Existing] is selected in [User Group to Associate], and the import type is set to [Active Directory/LDAP/Microsoft Entra Domain Services(Microsoft Entra ID DS)].

If you deselect the [Do not update when reimporting] check box, the parent user group is updated to the parent user group specified by the import schedule when updating users.

If you select the [Do not update when reimporting] check box, the parent user group will not be updated when updating users.



Note

For Active Directory/Microsoft Entra Domain Services, users are only updated if their attributes are updated on an external authentication server. Accordingly, user groups are also only updated when their attributes are updated on an external authentication server.

[Access Profile]

Set this item when you select [Create] in [User Group to Associate].

Select access profile from the top-down list box. The selected access profile is associated with a user group to be newly created.

If you specify [All OU] in [OU that creates the group], access profile is associated with the user group at the top of hierarchy.

(4) Confirm correspondence

If you select [Active Directory/LDAP], the content of correspondence is not displayed.

(5) Create New Account

Set this for cost management.

Specify the following item, and then click [Next].



Note

[Allotted Balance], [Top-Up Balance], and [Minimum Balance] of accounts are set only once when imported. When these values are already set, they are not updated even if you select [Update], [Add/Update], or [All] in [Import Processing Method].

[Create/Associate Personal Account]

If you associate import users with personal accounts, select a checkbox and specify each item of personal accounts.

Each item of personal accounts

Select attributes on the remote authentication server to correspond to user attributes from the drop-down list box or directly input the arbitrary character string. If you click and specify more than one, the values coupled with those are set.



Note

In direct input, if you put it in {}, it is recognized as an attribute of the remote authentication server.
Example: {description}



Refer

Each item of personal accounts→“Create an account” (P.204)

[Clear All]

Displayed when [Update] is set to [Import Processing Method]. If checked, all the associations of shared accounts currently set are released. If you create a shared account on [Create] of [Create/Associate Shared Account] in the situation that all associations are released, only the created shared account will be associated.

[Create/Associate Shared Account]

Select a checkbox when you associate shared accounts with import users.

[Shared Account]

To create a new shared account, select a checkbox for [Create] and select [Standard when creating the account]. To associate a shared account which has been already created, remove a check from [Create].

[Standard when creating the account]

Set this item if you select a checkbox for [Create] in [Shared Account]. Select the way to specify the account name of the shared account from either one of the following.

- [Specify Attribute/Account Name]
Make an attribute on the remote authentication server correspond to a shared account name or specify a shared account name with arbitrary character account.
- [Select OU]
Name a shared account after an OU name on the remote authentication server. Specify a target OU by the comparative number of hierarchy from the user.

[Account Name]

Set this item if you select [Specify Attribute/Account Name] in [Standard when creating the account]. Select attributes on the remote authentication server to correspond to shared account names from the drop-down list box or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Note

In direct input, if you put it in {}, it is recognized as an attribute of the remote authentication server.

Example: {description}

[No. of OU Hierarchy]

Set this item if you select [Select OU] in [Standard when creating the account].

Specify an OU to be used for a shared account name by a comparative location from users. Specify it with a positive number value of "0" or over.

- 0: Affiliated OU of user
- 1: One hierarchy above the affiliated OU of user
- 2: Two hierarchies above the affiliated OU of user

•
•
•

Example:

- When you specify "0" for [No. of OU Hierarchy]
The name of the OU the user is affiliated with in the remote authentication server is an account name of a shared account to be associated with the user after import.
- When you specify "1" for [No. of OU Hierarchy]
The OU one hierarchy above the OU that users are affiliated with in the remote authentication server becomes an account name of a shared account to be associated with the user after import.

Each item of shared accounts

Select attributes on the remote authentication server to correspond to shared account names from the drop-down list box or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Note

In direct input, if you put it in {}, it is recognized as an attribute of the remote authentication server.
Example: {description}



Refer

Each item of shared accounts → “Create an account” (P.204)

[Select Accounts]

To add a shared account which has been already created, click [Add] and select an account.

(6) Schedule Settings

Configure the following items, and then click [Save].



Note

Because any duplicate user ID is not permitted in the system, adjust the import schedule execution order so that any duplicate user ID does not occur when import is performed, such as by setting deletion schedule to be executed first when you have made a change with user domain or OU.

[Schedule Name]

Enter the schedule name.

[Description]

As needed, enter descriptions for the schedule.

[Schedule Settings]

Select an import schedule from the following.

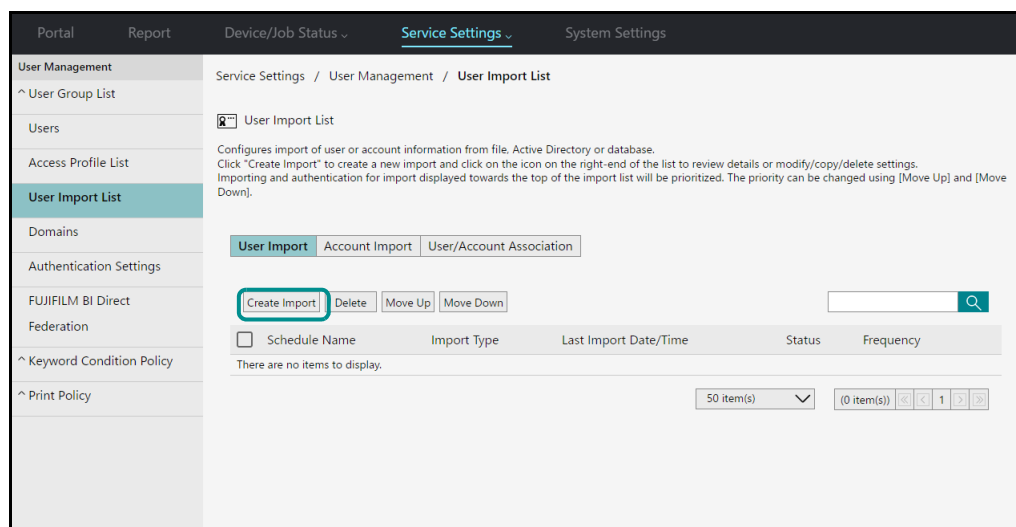
- [By Day]
Run import at the specified [Time] every day.
- [By Week]
Run import at the specified [Date/Time] (days of the week and hours) every week.
- [By Month]
Run import at the specified [Date > Time] every month. If you run import at the end of the month, select a checkbox for [Last Date].
- [By Minute]
Run import at the specified [minutes] intervals.
- [Specified Date & Time]
Run one-time-only import at the specified [Date] and [Time].
- [Manual Refresh]
Import gets started when you click [Run Import] in the user import list.

[Run Result Notification]

To notify the import run result, select a checkbox for [Notify by E-mail] and specify the notification destination name and the recipient e-mail address.

Create an import schedule (Import file)

Click [Create Import].



(1) Inbound channel selection

Select the inbound channel of user information, and then click [Next].

Hereafter, the items in the situation where you have selected [Import File] are described.

(2) Details of the inbound channel

Specify the following item, and then click [Next].

[File Type]

Select [Text File] or [CSV File].

[File]

Click [Browse] and select the target file for reading.

[Use the first row of the file as header]

If there is a heading line in the first row of the file, select a checkbox.

If you select a checkbox, the first row of the file is skipped in processing. You can refer to the heading when you select a field in “(3) Attribute correspondence”.

Remove a check if the data row is described from the first row of the file.

[Change file name after import]

After import processing, specify whether to change file names.

If you select a checkbox, the date and name are added to the end of the file name of the processed file in the following format.

“YYYYMMDDhhmmss” (year, month, day, hour, minute, second)

For example, if the file name is “userfile.csv”, it is “userfile20151031121546.csv” after processing.

[Import Processing Method]

Select either one of the following.

- [Handle according to the process type specified in the entire file.]

The entire file is processed as follows

Items	Descriptions
Add	All rows in the file are processed as a new row. When the user in the file is already in ApeosWare Management Suite, no processing is performed. You can select whether to register an attribute for which a duplicated value cannot be specified, such as the card ID/PAN, by disabling an existing user attribute.
Refresh	Process all rows in the file as refresh targets. Refresh all the values of the relevant rows. If the user in the file is not in ApeosWare Management Suite, no processing is performed. For the attributes in which you can specify more than one value such as e-mail addresses, you can select either to add or overwrite the attributes. You can select whether to register an attribute for which a duplicated value cannot be specified, such as the card ID/PAN, by disabling an existing user attribute.
Add/Update	Process all rows of the file as adding or refreshing targets. When the user in the file is already in ApeosWare Management Suite, refresh is performed. Add them if none is found. If the checkbox for [Delete User Not in File During Refresh] is selected, users who do not exist as the import target are deleted from ApeosWare Management Suite. For the attributes in which you can specify more than one value such as e-mail addresses, you can select either to add or overwrite the attributes. You can select whether to register an attribute for which a duplicated value cannot be specified, such as the card ID/PAN, by disabling an existing user attribute.
Delete	Delete all the users in the rows of the file from ApeosWare Management Suite.



Note

- For [Update] or [Add/Update], all attribute values with attribute association will be updated.
- In the case of account import, the [Delete] function is not available.
- [Handle according to process type specified in each row]
Process the target rows as follows according to the “processing type” specified in the file. For the rows whose “processing type” is not specified, skip processing and record them as a warning in the log file.

Items	Descriptions
Add ^{*1}	Create rows if the users are not in ApeosWare Management Suite. If there is already a user, no processing is performed.
Refresh ^{*1}	If the user is not in ApeosWare Management Suite, no processing is performed. If any user is found, refresh the rows with information set for each item of the relevant rows.
Delete ^{*1}	If the user is not in ApeosWare Management Suite, no processing is performed. If any user is found, delete the user.

^{*1} Specify the following in the file. (This is not case sensitive.)

To add: “a”
To refresh: “m”
To delete: “d”



Note

- For [Refresh], all attribute values with attribute association will be updated.
- In the case of account import, the [Delete] function is not available.



Refer

Process type→“User Import” (P.188)

[Delimiter]

For the text file, specify the characters to delimit each item value in the row.

[Encoding]

Select the file encoding.

(3) Attributes correspondence

Specify the following item, and then click [Next].

[Processing Type]

Set this item if you specify [Handle according to process type specified in each row.] in “(2) Details of the inbound channel”. Select the field of the inbound channel in which [Processing Type] is described.



Refer

Process type→“User Import” (P.188)

[Identifier to identify the user to be refreshed]

Set this item if you select [Refresh] or [Delete] of [Handle according to the process type specified in the entire file.] in “(2) Details of the inbound channel”.

Select one of the following as an identifier to identify users to refresh.

- User ID
- Card ID/PAN
- External ID
- E-mail address

[User Settings]

Set each user attribute of ApeosWare Management Suite.

Select the field of the inbound channel to correspond to user attributes from the drop-down list box or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.

- [Overwrite]

When you specify [Update] or [Add/Update] of [Handle According to Processing Type of Entire File], or [Refresh] of [Handle According to Process Type Specified in Each Row] in “(2) Details of the inbound channel”, [Overwrite] is displayed next to the attribute in which you can specify more than one value such as e-mail addresses. If you attach a check mark, the user attribute is replaced with a file value. If you remove a check mark, a file value is added to the existing user attribute.



Note

- To specify more than one value in a file, specify them by delimiting them with a semicolon (;).
- When you specify more than one e-mail address, the top e-mail address becomes a standard e-mail address.
- If you select a checkbox for [Use the first row of the file as header] in “(2) Details of the inbound channel”, you can select fields while referring to the heading.



Refer

- Details items of users→“Adding users” (P.133)
- Format of items in file→“Attribute Correspondence in Import” (P.188)

- [Overwrite Existing User]

When [Handle according to the process type specified in the entire file.] is set to [Add], [Update], or [Add/Update] under “(2) Details of the inbound channel,” or [Handle according to process type specified in each row.] has been checkmarked, [Overwrite Existing User] will be displayed next to those attributes for which duplicated values such as card ID/PAN cannot be set. If you place a check mark and an attribute that is already in use by an existing user is present, the duplicated attribute of the existing user is deleted and the file value is applied to the attributes of the imported user. If

you remove the check mark, an error occurs and the user cannot be imported.

[Associate User with User Group]

When you specify the user group to be affiliated with import users, select a checkbox and specify the following items.

If you remove a check, the imported user is affiliated with the default user group (Default Group).

- [User Group to Associate]

To create a new user group that users are affiliated with, click [Create] and select [Attribute/Group Name].

To affiliate users with the existing user group, select [Existing] and specify [Parent User Group].

- [Attribute/Group Name]

Specify this item when you select [Create] in [User Group to Associate].

Specify the name of a user group to be newly created. The group corresponding to the user group name set here is created and imported users are imported under that.

Select the field of the inbound channel to correspond to the name of a user group from the drop-down list box. or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.

- [Parent User Group]

Click [Change] and specify a user group.

When you select [Existing] in [User Group to Associate], the user group specified here becomes the user group that import users are affiliated with. When you select [Create] in [User Group to Associate], the user group becomes the parent user group of the user groups newly created.

- [Access Profile]

Specify this item when you select [Create] in [User Group to Associate].

Select access profile from the top-down list box. The selected access profile is associated with a user group to be newly created.

(4) Confirm correspondence

The content set in “(3) Attribute correspondence” is displayed. Confirm whether it corresponds properly, and then click [Next].

(5) Create New Account

Set this for cost management.

Specify the following item, and then click [Next].



Note

[Allotted Balance], [Top-Up Balance], and [Minimum Balance] of accounts are set only once when imported. When these values are already set, they are not updated even if you select [Update] or [Add/Update] in [Import Processing Method].

[Create/Associate Personal Account]

If you associate import users with personal accounts, select a checkbox and specify each item of personal accounts.

Each item of personal accounts

Select the field of the inbound channel to correspond to the items of personal accounts from the drop-down list box or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Refer

- Details of items of account→“Create an account” (P.204)
- Format of items in file→“Attribute Correspondence in Import” (P.188)

[Clear All]

Displayed when [Refresh] is set to [Import Processing Method]. If checked, all the associations of shared accounts currently set are released. If you create a shared account on [Create] of [Create/Associate Shared Account] in the situation that all associations are released, only the created shared account will be associated.

[Create/Associate Shared Account]

Select a checkbox when you associate shared accounts with import users.

[Shared Account]

To create a new shared account, select a checkbox for [Create] and set each item of shared accounts. To associate a shared account which has been already created, remove a check from [Create].

Each item of shared accounts

Select the field of the inbound channel to correspond to the items of shared accounts from the drop-down list box Or directly input the arbitrary character string. If you click and specify more than one, the values coupled with those are set.



Refer

- Details of items of account→“Create an account” (P.204)
- Format of items in file→“Attribute Correspondence in Import” (P.188)

[Select Accounts]

To add a shared account which has been already created, click [Add] and select an account.

(6) Schedule Settings

Specify the following item, and then click [Next].

[Schedule Name]

Enter the schedule name.

[Description]

Enter descriptions for the schedule as necessary.

[Schedule Settings]

Select an import schedule from the following.

- [By Day]

Run import at the specified [Time] every day.
- [By Week]

Run import at the specified [Date/Time] (days of the week and hours) every week.
- [By Month]

Run import at the specified [Date > Time] every month. If you run import at the end of the month, select a checkbox for [Last Date].
- [By Minute]

Run import at the specified [minutes] intervals.
- [Specified Date & Time]

Run one-time-only import at the specified [Date] and [Time].

- [During file update]

When the file on the constant watch is updated, import is executed.

- [Manual Refresh]

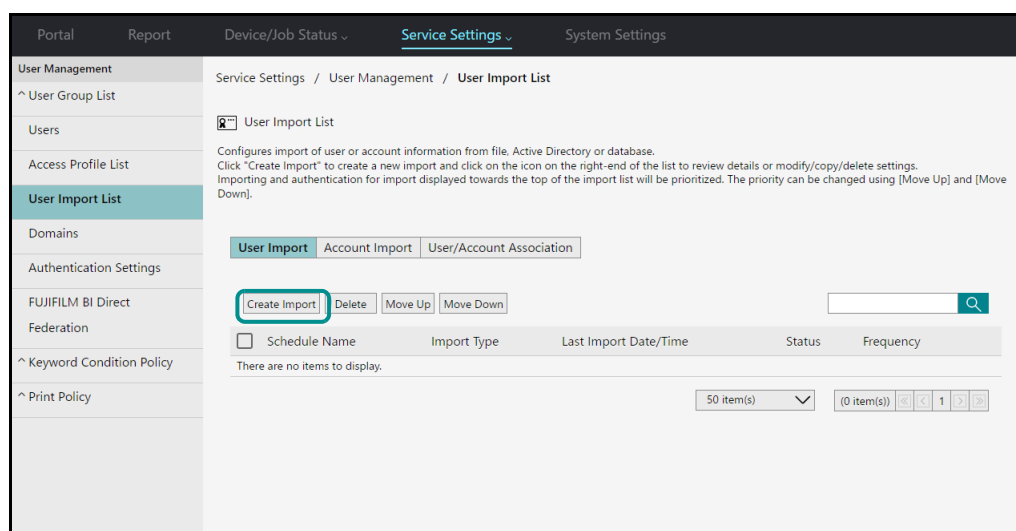
Import gets started when you click [Run Import] in the user import list.

[Run Result Notification]

To notify the import run result, select a checkbox for [Notify by E-mail] and specify the notification destination name and the recipient e-mail address.

Create an import schedule (Database import)

Click [Create Import].



(1) Inbound channel selection

Select the inbound channel of user information.

Hereafter, the items in the situation where you have selected [Database Import] are described.



Refer

User properties and formats available for import→“User Import” (P.188)

(2) Details of the inbound channel

Specify information on the inbound channel database.

In Import Processing Method, specify [Add/Refresh] or [Refresh].

Enter a query string in query to obtain the user information from the database of the import source.

(3) Attribute correspondence

Make the user attributes of ApeosWare Management Suite correspond to the column names of the database result set. [Overwrite] is displayed under the attributes in which you can specify more than one value such as e-mail addresses. If you attach a check mark, the user attribute is replaced with a database value. If you remove a check mark, a database value is added to the existing user attribute.

Moreover, [Overwrite Existing User] is displayed next to the attribute for which a duplicated value cannot be specified, such as the card ID/PAN. If you place a check mark and an attribute that is already in use by an existing user is present, the duplicated attribute of the existing user is deleted and the database value is applied to the attributes of the imported user. If you remove the check mark, an error occurs and the user cannot be imported.

For details, refer to "(3) Attribute correspondence" in "Create an import schedule (Import file)" (P.159) except the following.

- When [Create] is selected in [Associate User with User Group], user import of up to 10 hierarchies is available.
- In [Attribute/Group Name], you can specify the row name of the database results set in each hierarchy.
- [User groups with no users will be deleted after successful import]
Specify this item when you select [Create] in [User Group to Associate].
If you select the checkbox, all user groups below the parent user group that do not contain users will be deleted after import. However, if even one import has failed, deletion processing will be skipped.

(4) Confirm correspondence

The content set in "(3) Attribute correspondence" is displayed. Confirm whether it corresponds properly.

(5) Create New Account

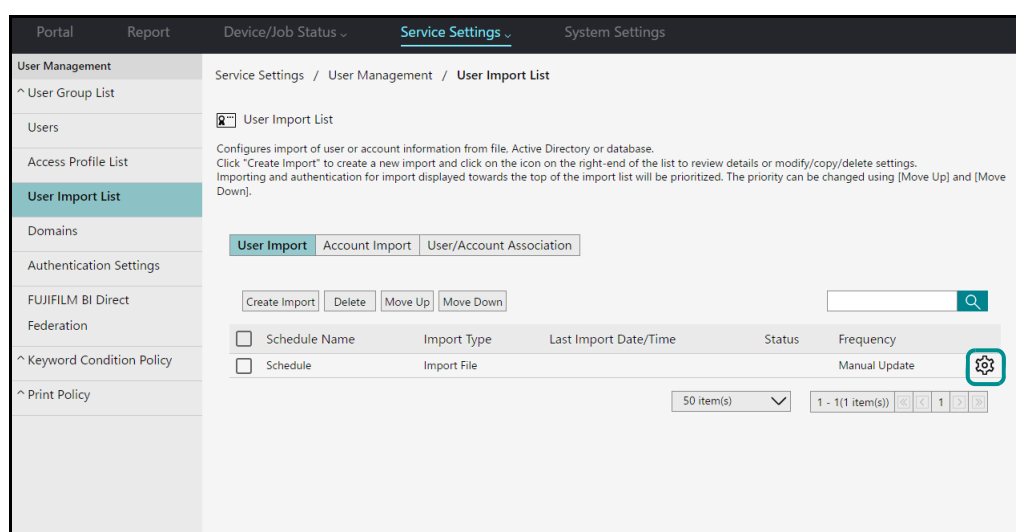
For details, refer to "(5) Create an account" in "Create an import schedule (Import file)" (P.159).

(6) Schedule Settings

For details, refer to "(6) Schedule Settings" in "Create an import schedule (Import file)" (P.159).

Executing an import schedule manually

For immediate start of a schedule, click  in the user import list and select [Run Import]. The import schedule is executed.



Checking Import Schedule Information

Click  in the user import list and select [Properties].

Making Duplicate of Import Schedule

Click  in the user import list and select [Copy].

Deleting an import schedule

Click  in the user import list and select [Delete].

Replace the order of connection to the remote authentication server at the time

of authentication

ApeosWare Management Suite is connected to the remote authentication server by the inbound channel following import information set for [Active Directory/LDAP] at the time of authentication of users and identifies them. Then, upper ones are connected first in terms of the import schedule of the user import list.

As for priority order, order can be replaced by clicking [Move Up] and [Move Down].

User Import List [Account Import] Tab

How to Display

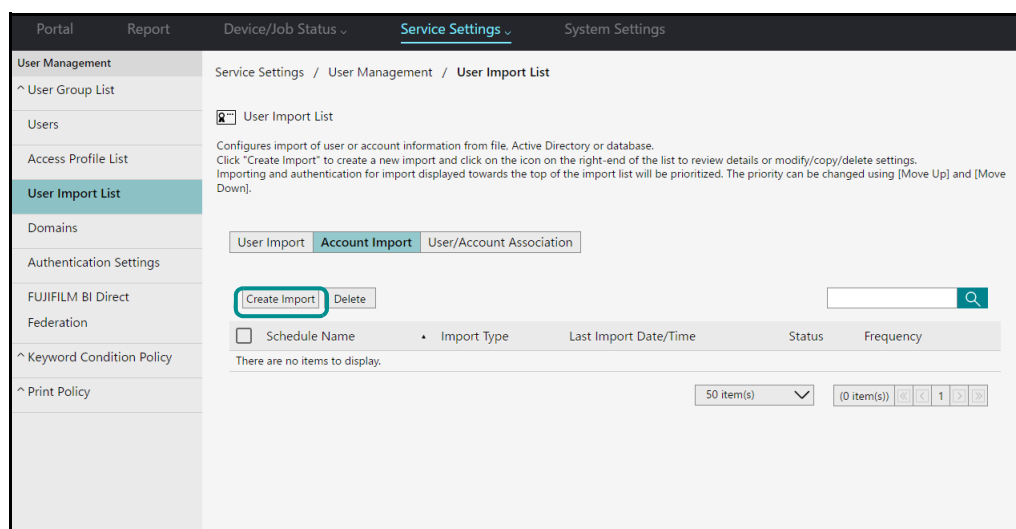
Select [Service Settings] > [User Management] > [User Import List] from the menu on the administrator screen and display the [Account Import] tab.

Page Summary

Automatically import account information managed by the files into ApeosWare Management Suite by specifying a schedule.

Create an import schedule (Import file)

Click [Create Import].



(1) Inbound channel selection

Specify the following item, and then click [Next].

Select the inbound channel of account information.

Hereafter, the items in the situation where you have selected [Import File] are described.

(2) Details of the inbound channel

For details, refer to “(2) Details of the inbound channel” in “Create an import schedule (Import file)” (P.159).

(3) Attributes correspondence

Specify the following item, and then click [Next].

[Account Details]

Select the field of the inbound channel to correspond to the items of accounts from the drop-down list box Or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Note

If you select a checkbox for [Use the first row of the file as header] in “(2) Details of the inbound channel”, you can select fields while referring to the heading.



Refer

- Details of items of account→“Create an account” (P.204)
- Format of items in file→“Attribute Correspondence in Import” (P.188)

[Set Account Balance]

When setting the balance for the import account, select a checkbox and set each item of the balance.

Each item of the balance

Select the field of the inbound channel to correspond to the items of the balance from the drop-down list box. Alternatively, directly input the numbers.



Note

[Allotted Balance] and [Top-Up Balance] of the account will become as follows by [Import Processing Method].

- If you select [Update] or [Add/Update], the specified values are added to the setup values or subtracted from them.
- If you select [Add], the specified value is set.



Refer

Details of items of account→“Create an account” (P.204)

(4) Confirm the details of the account

The content set in “(3) Attribute correspondence” is displayed. Confirm whether it corresponds properly.

(5) Schedule Settings

For details, refer to “(6) Schedule Settings” in “Create an import schedule (Import file)” (P.159).

User Import List [Associate User/Account] Tab

How to Display

Select [Service Settings] > [User Management] > [User Import List] from the menu on the administrator screen and

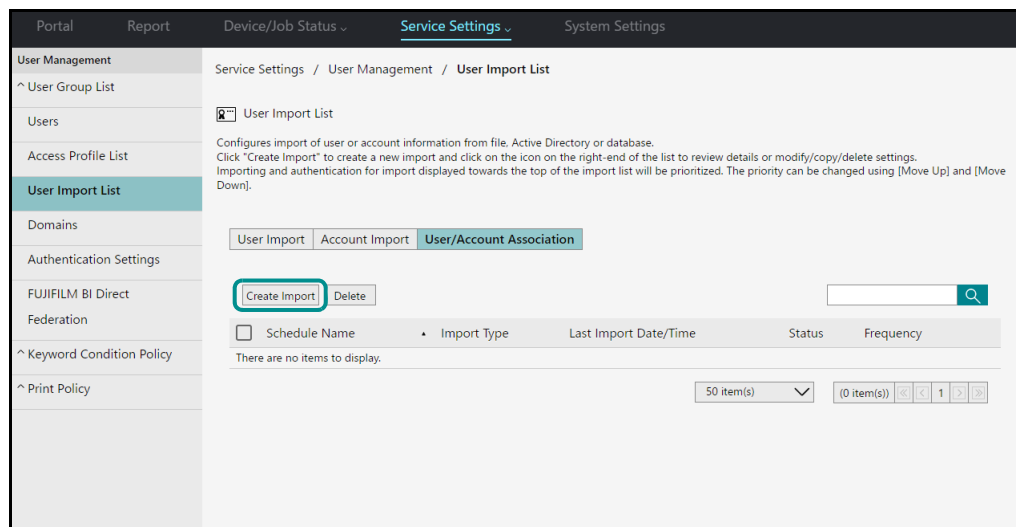
select the [Associate User/Account] tab.

Page Summary

Import the file to which the user ID and account corresponded. After setting a schedule, you can import it automatically.

Creating an import (Import File)

Click [Create Import].



(1) Inbound channel selection

Select the inbound channel of information on the association, and then click [Next].

Hereafter, the items in the situation where you have selected [Import File] are described.

(2) Details of the inbound channel

For details, refer to "(2) Details of the inbound channel" in "Create an import schedule (Import file)" (P.159).

(3) Attributes correspondence

Select targets to be associated with an account from [User] and [User Group], and then click [Next].

Select the field of the inbound channel to correspond to each item from the drop-down list box. Or directly input the arbitrary character string. If you click  and specify more than one, the values coupled with those are set.



Note

If you select a checkbox for [Use the first row of the file as header] in "(2) Details of the inbound channel", you can select fields while referring to the heading.



Refer

- Details of items of account→"Create an account" (P.204)
- Format of items in file→"Attribute Correspondence in Import" (P.188)

(4) Confirm the details of association

The content set in "(3) Attribute correspondence" is displayed. Confirm whether it corresponds properly.

(5) Schedule Settings

For details, refer to "(6) Schedule Settings" in "Create an import schedule (Import file)" (P.159).

Domain list

How to Display

Select [Service Settings] > [User Management] > [Domains] from the menu on the administrator screen.

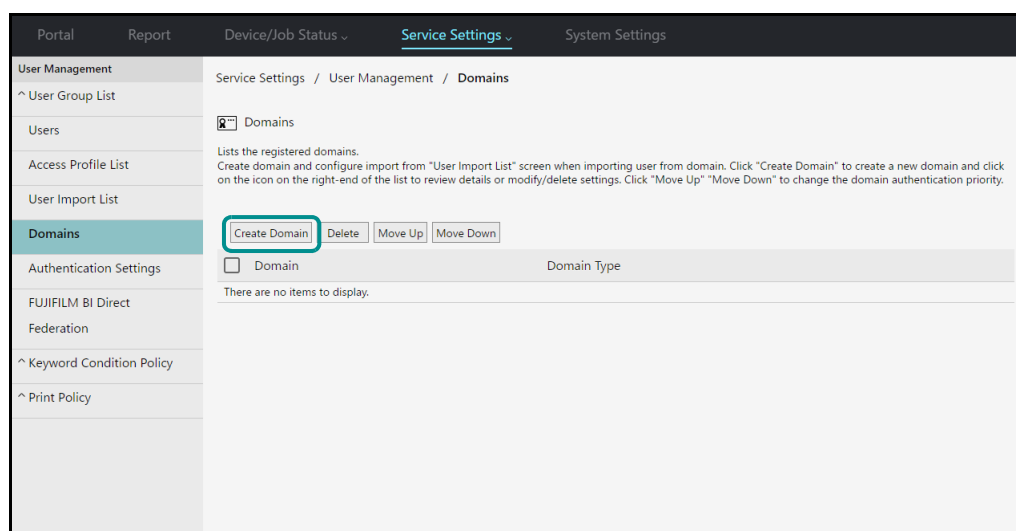
Page Summary

Set the domain information on the remote authentication server linking with ApeosWare Management Suite. You can add domains, edit and delete properties.

The domain search order at the time of user authentication is according to the domain list order.

Adding domains

Click [Create Domain] and configure the following items, and then click [Save].



[Select Inbound Channel]

Select the type of external authentication server from among [Active Directory], [LDAP], or [Microsoft Entra Domain Services (Microsoft Entra ID DS)].



Note

- If [Microsoft Entra Domain Services (Microsoft Entra ID DS)] is selected as the import source, after completing the settings, click [Check connection], and check that the information entered is correct. If it is not possible to connect well, check the following items.
 - Check whether the network can access Microsoft Entra Domain Services.
 - Check whether the LDAPS protocol on the Microsoft Entra ID DS domain service is enabled, and whether port 636 is released.
 - Check whether the certificate exported at "Installing Certificates for Secure LDAP" (P.69) has been imported into the ApeosWare Management Suite server, and that the server has been restarted.
 - Check whether the user of the domain to be created has been linked to the enterprise application.
 - For details, refer to "Set the enterprise application" (P.66) and "Creating Microsoft Entra Domain Services" (P.68).
- When using Microsoft Entra Domain Services, take note of the following points.
 - When logging in on the administrator screen and the user screen, authentication cannot be carried out with the email address set in the ApeosWare Management Suite user, even when the [Enable authentication with an email address] check box is checked in the [Authentication Mode] of [Authentication Settings].
 - When logging in on the screens other than the administrator screen and the user screen, if multifactor authentication is enabled in Microsoft Entra ID, authentication fails when logging in with a password.
 - External users of Microsoft Entra ID are not supported.

[Domain]

Set for Active Directory, or LDAP server.

Enter the Active Directory domain name or the authentication destination (realm name) of the LDAP server.

[Microsoft Entra Domain Services Domain]

Set only for Microsoft Entra Domain Services.

Enter the DNS domain name created at "Creating Microsoft Entra Domain Services" (P.68).

[User Name]/[Password]

Enter a user name and password for connection.

- For Active Directory

Enter a user name. You can enter it either in the SAM format or in the UPN format. You can skip a domain.

- For LDAP server

Specify the user name in the DN format (Domain Name). Connect the attribute name of RDN (Relative Identification Name) to the attribute value with equality (=). Delimit each RDN with a comma (,).

Example: cn=root, ou=ou1, dc=example, dc=local

- Microsoft Entra Domain Services

Enter the user name and password of the user associated with the application created at "Set the enterprise application" (P.66).



Note

In the case of a user in Microsoft Entra ID before being associated with Microsoft Entra Domain Services, the passwords are not synchronized. The user password used here must be changed after association with Microsoft Entra Domain Services.

After changing your password in Microsoft Entra ID, please wait a little while before adding your domain, as it may take up to 10 minutes for it to be synced to Microsoft Entra Domain Services.

[User ID Format]

Set for Active Directory or Microsoft Entra Domain Services.

- For Active Directory

Select the display format of the user ID from [SAM Format] and [UPN Format].

For [SAM Format], the user name is shown with the format of "{NetBIOS domain name} \ {User name}". For [UPN Format], the user name is shown with the format of "{User name} @ {FQDN domain name}".



Note

For [User ID Format], be sure to specify a format used for authentication on the remote authentication server. Without a correct format, users are not authenticated properly.

- For Microsoft Entra Domain Services

Select [SAM Format].

[Enable LDAPS Communication with Active Directory Server]

Set for Active Directory or Microsoft Entra Domain Services.

- For Active Directory

When you execute the LDAPS communication with the Active Directory server, select a checkbox. For the LDAPS communication, you need to install the server certificate and set it so that the

communication can be coded.

- For Microsoft Entra Domain Services
Apply a check mark.

[Domain Controller]

Set this only for Active Directory / Microsoft Entra Domain Services.

If there is more than one domain controller in the domain, set the priority order of the domain controller for authentication.

ApeosWare Management Suite confirms connection to the domain controller according to the set priority order and imports user information from the domain controller that it can communicate with first.



Note

If the domain controller is not prioritized, different domain controllers may be used by service. To use the same domain controller for each service, prioritization is recommended.

[Server]

Set this only for the LDAP server.

Enter the URL of the LDAP server in the "ldap://" or "ldaps://" format.

To specify the URL in the "ldaps://" format, you need to install the server certificate and set it so that the communication can be coded.

Example: ldap://192.0.2.1

[LDAP User Object Class]

Set this only for the LDAP server.

Input the object class name to be used for the user object class.

[LDAP Group Object Class]

Set this only for the LDAP server.

Input the object class name to be used for the group object class.

[Login URL]

Set only for Microsoft Entra Domain Services.

Enter the [Login URL] that you wrote down in the supplement to procedure 15. of "Set the enterprise application" (P.66).

[Identifier (Entity ID)]

Set only for Microsoft Entra Domain Services.

Enter the identifier (Entity ID) set in procedure 15. of "Set the enterprise application" (P.66).

[Application ID]

Set only for Microsoft Entra Domain Services.

Enter the application ID created at procedure 8. of "Set the enterprise application" (P.66).

Checking Domain Information

Click  of the domain list and select [Properties].

You can display and edit the content configured for the domain. You can edit the same items as in "Adding domains" (P.169). However, you cannot change the remote authentication server type.

Deleting domains

Click  of the domain list and select [Delete].

To delete a domain set in the inbound channel of the import schedule, you need to delete a domain after deleting the import schedule.

If you delete a domain, all users in the domain are deleted from ApeosWare Management Suite. However, the user group is left.

When the users are deleted, the following information is deleted too.

- User information set for the device, the folder whose owner is the user, and the document reserved in the folder
- Job flow whose owner is a user and which is set for a device

Changing domain search order

The domain search order at the time of user authentication is according to the domain list order. Click [Move Up] or [Move Down] and replace the domain search order.

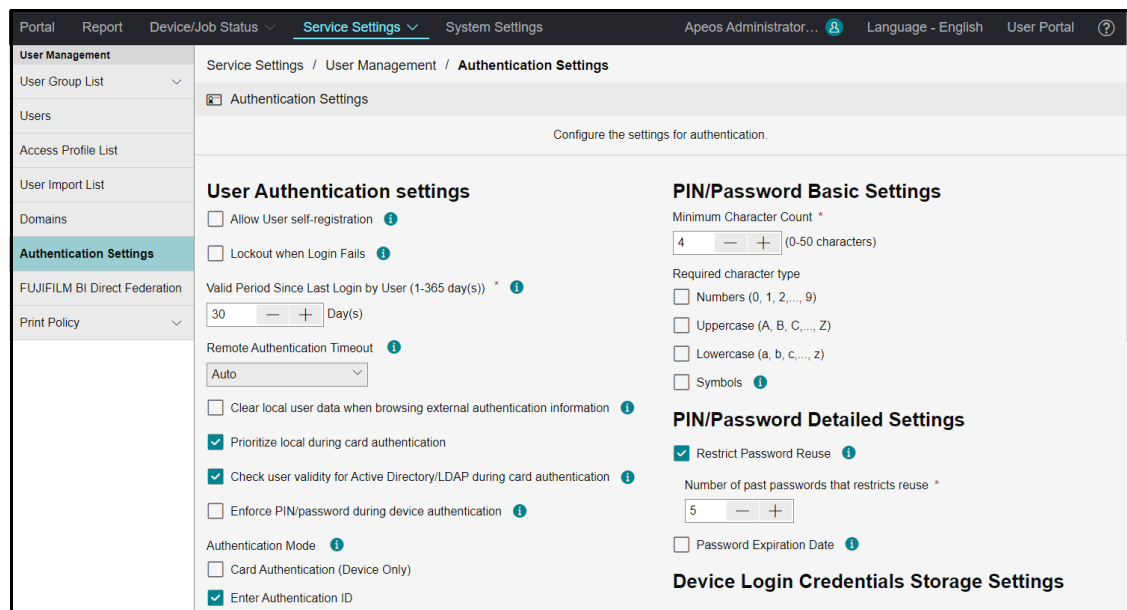
Authentication Settings

How to Display

Select [Service Settings] > [User Management] > [Authentication Settings] in the administrator screen menu.

Page Summary

Sets user authentication.



Set authentication features

[User Authentication settings]

- [Allow User self-registration]

Specify whether to allow users themselves to register user information.

With a check, by reading the IC card into the card reader connected to a device and a PC, users become able to register the card ID (PAN) by themselves. If the user reads the QR code for login using a mobile application, the user can register the external ID by himself/herself.



Refer

“User Information Registration by Users” (P.195)

- [Lockout when Login Fails]

Specify whether to lock out users when they input the wrong password and fail in log-in. When selecting a checkbox, specify the following item.

- [Number of allowed login retries]
Input the number of times within which failure in log-in is allowed before users get locked out. If users fail in log-in over the set number of times set here within [Time Until Failed Logins Reset], they are locked out. For example, if you input [5] times and users fail in log-in six times within the specified time, lockout is executed.
- [Time Until Failed Logins Reset]
Enter the time until you reset the number of times of users' failed log-in after their first failed log-in. If users fail in log-in over [Number of allowed login retries] within the time set here, they are locked out.
The administrator can unlock the users who are locked out in the [Service Settings] > [User Management] > [Users] page.



Note

Within the time frame of [Time Until Failed Logins Reset], the number of times for failed login attempts is not reset even when a login is successful.

For example, when [Number of Allowed Login Retries] is three times and [Time Until Failed Logins Reset] is one day, a user will be locked out if the user fails in login attempt two times consecutively and then succeeds to login but the user fails at the attempt two times consecutively again after a few hours elapse.

- [Valid Period Since Last Login by User]

This item is applied to the users for whom [User Account Expiration Date] is set to [Valid Period Since Last Login {n} days].

Enter the number of days of the user validity period. If this validity period is past after the last log-in, the users become disabled.

When you operate one of the following, valid status is extended for the valid days set here starting on the operation day.

- Access to ApeosWare Management Suite from the mobile device, PC, or device
- Log in to the device managed by ApeosWare Management Suite
- The job whose owner is the user is processed with the print service of ApeosWare Management Suite

- [Remote Authentication Timeout]

Specify the timeout value for the communication between the ApeosWare Management Suite server and the remote authentication server.

If the set timeout is over while you inquiring about authentication, authentication becomes unavailable. However, if you set more than one domain controller in the domain, timeout does not become unavailable immediately and moves to inquiry to the next server.

When you set [Auto] (default value), the timeout value determined in the OS of the ApeosWare Management Suite server will be set.

- [Clear local user data when browsing external authentication information]

Specify whether to update user information in ApeosWare Management Suite when inquiring of the user information to the remote authentication server.

User information is updated according to the import schedule. In addition to the settings according to the schedule, select a checkbox if you update user information at the time of authentication as well.

- [Prioritize local during card authentication]

Select the checkbox when you set to search for user information in the ApeosWare Management Suite server first.

- [Check user validity for ActiveDirectory/LDAP during card authentication]

In the case you have selected the checkbox for [Prioritize local during card authentication], put a check mark in the checkbox when you want to check whether the remote user found in the ApeosWare Management Suite server is also enabled in Active Directory/LDAP.

- [Enforce PIN/password during device/mobile authentication]

This setting is valid only in the device where the authentication method is [Custom Authentication] or the mobile device. Each setting is applicable to the following cases.

- The device where the authentication method is [Custom Authentication]
When you select [Follow Authentication Common Settings] in [Require PIN/Password Input] of access profile associated with users.
- Mobile Device
When you select [Follow Device Group Settings] or [Follow Authentication Common Settings] in [Require PIN/Password Input] of access profile associated with users.

Specify whether to use PIN or a password at the time of authentication of users. When using it, select a checkbox.



Note

This setting is not applicable to the password with which you log in to ApeosWare Management Suite from a PC.

- [Authentication Mode] > [Card Authentication (Device Only)]

This setting is applicable only when the authentication method of the device is [Custom Authentication]. Select a checkbox at the time of authentication with the IC card reader in the device.



Note

- Be sure to select a checkbox when using the IC card reader in the device of [Custom Authentication]. If you do not select a checkbox, the card authentication is not available.
- When an authentication method is [Local Authentication] or [Remote Authentication] in a device, if you set a card reader and enable it, card authentication becomes valid automatically.

- [Authentication Mode] > [Enter Authentication ID]

This setting is applicable only when the authentication method of the device is [Custom Authentication].

Select a checkbox for the type of the authentication ID to be used at the time of authentication in the device. You can select more than one authentication ID from the following.

- User ID
 - Allow Authentication by Email Address
To log in to a device using an e-mail address instead of a user ID, select the checkbox for [Allow Authentication by Email Address].
- Card ID (PAN) (manual input of the card ID)
- External ID



Note

- When an authentication method is [Local Authentication] or [Remote Authentication] in a device, authentication with the card ID (PAN), external ID, or e-mail address is not available.
- E-mail addresses that can be used are restricted to those not shared with other users. If it is shared, this will generate an error.

[User Import Settings]

- [Overwrite Duplicate Card ID on ActiveDirectory/LDAP]
Select this checkbox to overwrite card IDs when they are duplicated.

[QR Code Login Settings]

- [QR Code Timeout Value (1 to 60 sec.)]
This setting is applied when [On] is set to [Display Login QR Code]. Set the valid time for QR code to display.
- [Mobile App Settings]
This setting is used to set application specific information to use the login QR code of [ApeosWare MS Mobile 2], [Alipay], and [WeChat].



Refer

"Advance Setting When Using Login with a QR Code" (P.70)

[PIN/Password Basic Settings]

- [Minimum Character Count]
Enter the minimum number of the characters of a password to log in with.
If you do not set a password, specify "0". With "0" specified, users can log in without inputting a password.
- [Required character type]
Select a checkbox on the character type which you are sure to include in the password. You can select multiple templates.

[PIN/Password Detailed Settings]

- [Restrict Password Reuse]
Specify whether to inhibit the reuse of the password set for the present. If you select a checkbox, input the following item.
- [Number of past passwords that restricts reuse]
Reusing of password that was used previously is prohibited until the password will have been changed for the number of times that is set here.
For example, when the number of times is set to [5], any password used inside the past five times cannot be used when changing the password. The passwords before that are available.
- [Password Expiration Date]
Specify whether to set the expiration date of a password. When selecting a checkbox, specify the following item.
- [Validity Period of Password]
Specify the validity period of password of a user.
When the validity period set here is past after the password was changed for the last time, the password becomes disabled. However, the last password is usable for the number of times set in [Number of grace logins until password change].
 - [Number of grace logins until password change]
Enter the number of grace logins that is applied after the validity period of password is past.
With any user who logs in exceeding the number of times set here after the validity period expires, the password will be disabled and the user will be locked out. For example, when the number of times is set to [5], users can log in up to five times. However, if they try for the sixth time, they get locked out.

[Device Login Credentials Storage Settings]

- [Storage Method for Login Credentials to Use When Network Connection Fails]

Specify the method of saving the user who uses the offline mode of custom authentication.

- [Save allowed users when settings are reflected on device]
Save all users who can use in offline mode in the device at the time of updating the device.
Users who can use in offline mode mean the users with whom the following settings are enabled.
- [Access device that cannot connect to network] in Access Profile: Allow
- [Save users allowed to access device each time they log in]
At the timing that the user logs in to the device while online, the user information is saved to the device in question as cache.

The user information registered in the device is deleted when either of the followings occurs.

- If the device is updated without the check mark of [Access device that cannot connect to network] in Administrator Portal > Device Group Properties, all the user information saved in the device is deleted.
- Upper limit for the number of users that can be saved (10,000 users) is exceeded
User information is deleted starting from the information having the oldest login history.

Keyword Condition Policy



Note

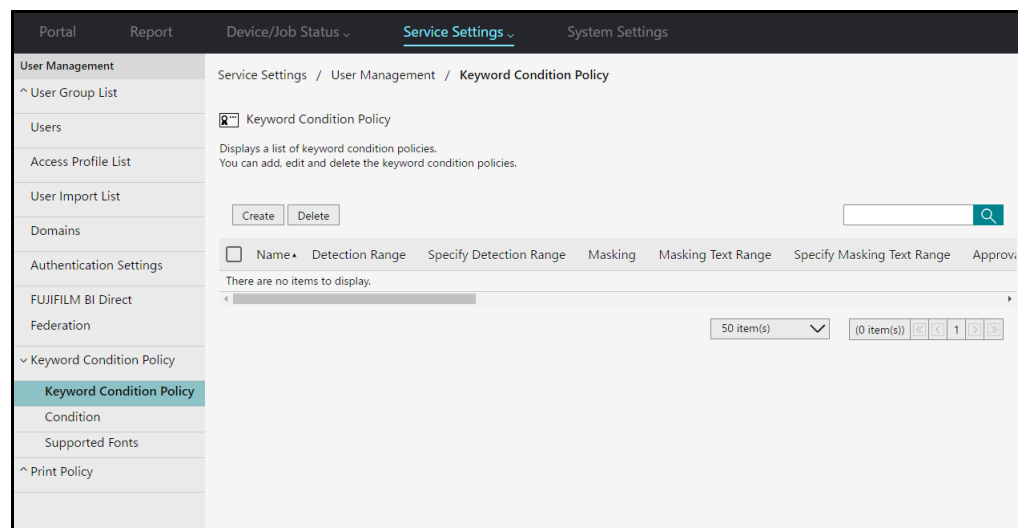
This feature is not available in some countries and regions.
For details, contact our dealers.

How to Display

Select [Service Settings] > [User Management] > [Keyword Condition Policy] in the administrator screen menu.

Page Summary

Displays the keyword condition policy.



Sets the keyword condition policy.

Click [Create] in the Keyword Condition Policy list.

The keyword condition policy creation dialog box is displayed.

[Name]

Enter the name of policy to create.

[Detection Range]

Specify the detection range.

[Masking]

Specify whether or not to mask the detected keyword with "*" when a specific keyword is detected. You can select the string to mask from the first letter, odd letters, even letters, and specified range.

[Approval Print]

Set whether to execute approval print.

When special approval is made when security information is searched more than the value specified in [Number of Detections], select a checkbox for [Require Special Approval] and set the number of detections.

- [Require Special Approval]
Select the checkbox when making special approval and set the number of detection of security information for special approval.
- [Auto Reject]
Select the checkbox when making auto rejection and set the number of detected security information for auto rejection of print jobs.
- [Allow Transfer]
Select a checkbox when you allow transfer. To select the requester for approval as the transfer destination, select the checkbox for [Select Requester for Approval as Transfer Destination].

[Cancel Job Containing Unsupported Fonts]

Specify whether or not to cancel the job when keyword detection is performed on a job containing unsupported fonts.

[Condition]

Select the detection condition.

Click [Add] and add a condition in the [Add Condition] dialog box.

Delete the keyword condition policy.

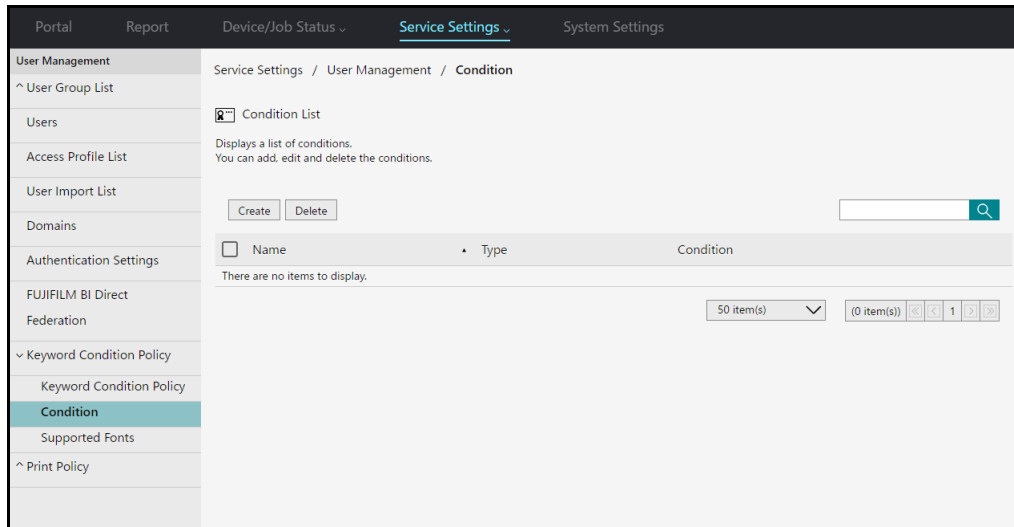
Select a checkbox for the keyword condition policy you wish to delete, and then click [Delete].

Condition**How to Display**

Select [Service Settings] > [User Management] > [Keyword Condition Policy] > [Condition] in the administrator screen menu.

Page Summary

Display a list of registered conditions.



Add conditions

Click [Create] and configure the following items, and then click [Save]. You can add up to 100 conditions.

[Name]

Enter a condition name.

Condition

Select either [Regular Expression] or [Keyword].

In the case of [Regular Expression], a regular expression is displayed, and in the case of [Keyword], a random string is displayed.

Delete conditions

Select a checkbox for the conditions you wish to delete, and then click [Delete].

Supported Fonts

How to Display

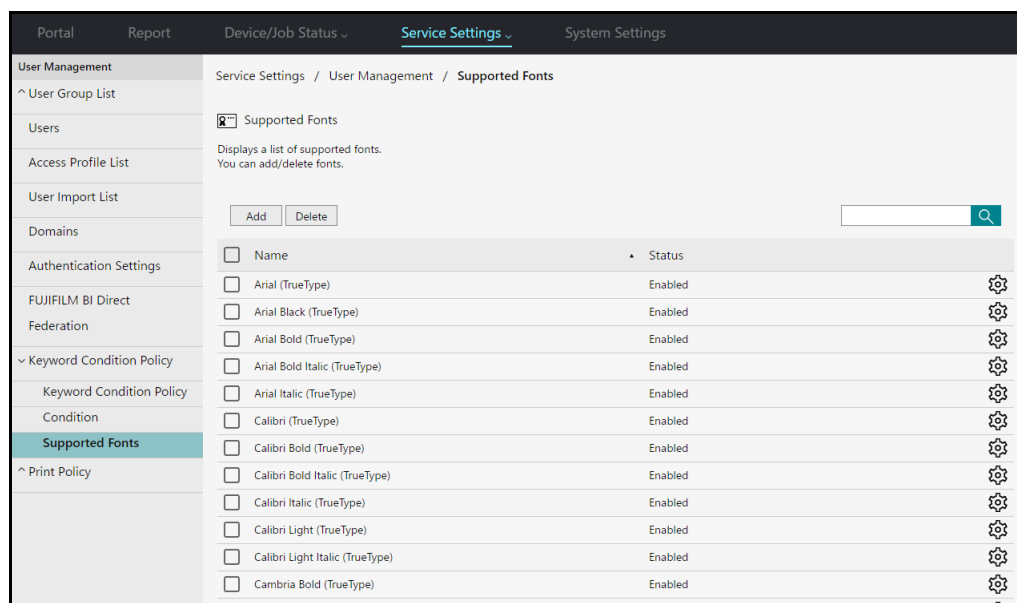
Select [Service Settings] > [User Management] > [Keyword Condition Policy] > [Supported Fonts] in the administrator screen menu.

Page Summary

Displays a list of supported fonts.

Adds supported fonts.

Click [Add], select fonts to add in the list of the fonts installed in the server, and click [Add].



Deletes supported fonts.

Select a checkbox for the supported fonts you wish to delete, and then click [Delete].

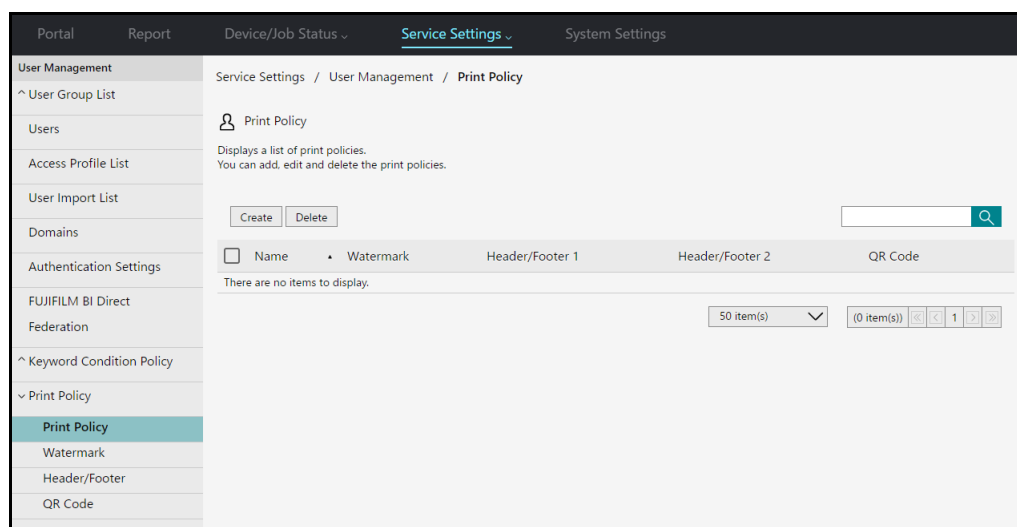
Print Policy

How to Display

Select [Service Settings] > [User Management] > [Print Policy] from the menu on the administrator screen.

Page Summary

Displays the print policy.



Sets the print policy

Click [Create] in the print policy list.

The print policy creation dialog box is displayed.

[Name]

Input the name of policy to be created in the range from 1 to 128 characters.

[Watermark]

Sets the watermark.

Click [Edit] and select a watermark in the [Add Watermark] dialog box.

[Header/Footer 1]

Set the header/footer.

Click [Edit] and select a header or footer in the [Add Header/Footer] dialog box.

[Header/Footer 2]

Set the header/footer.

Click [Edit] and select a header or footer in the [Add Header/Footer] dialog box.

[QR Code]

Sets the QR code.

Click [Edit] and select a QR code in the [Add QR Code] dialog box.

Deleting the print policy

Select a checkbox for the print policy you wish to delete, and then click [Delete].

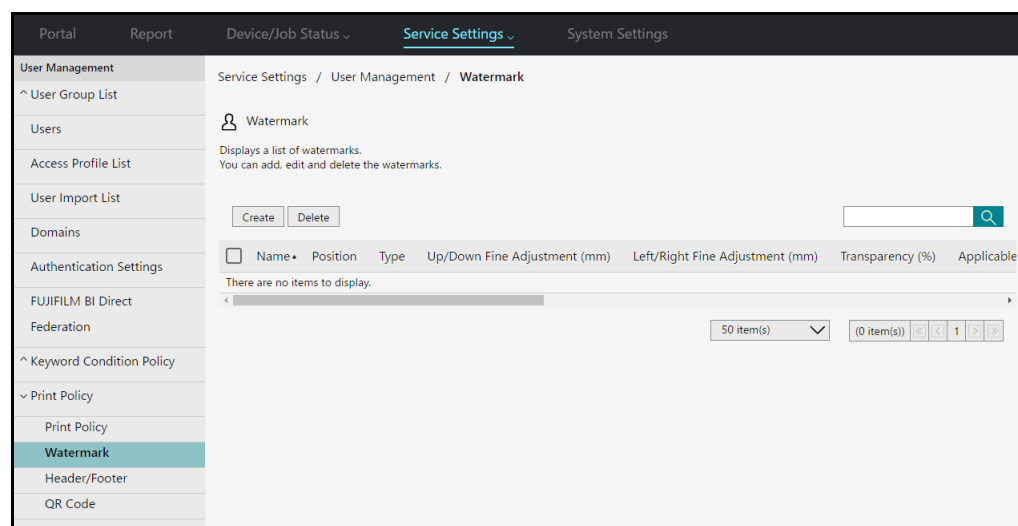
Watermark

How to Display

Select [Service Settings] > [User Management] > [Watermark] from the menu on the administrator screen.

Page Summary

Displays a list of registered watermarks.



Adding watermarks

Click [Create] and configure the following items, and then click [Save].

[Name]

Input the name of the watermark in the range from 1 to 128 characters.

[Type]

Select either [Image] or [Text].

The setting items vary according to the selection.

When [Image] is selected for [Type]**[Image File]**

Click [Browse] and select a watermark in the dialog box.

[Magnification/Reduction (%)]

Specify the magnification rate of the watermark in the range of 30 to 400% in increments of 10%.

[Repeat Image]

Select [On] or [Off] of repeat print of watermark.

[Position]

Select the watermark display position from "Upper Left," "Upper Center," "Upper Right," "Left Center," "Center," "Right Center," "Lower Left," "Lower Center," and "Lower Right."

[Fine Adjustment at Top and Bottom (mm)]

Specify the watermark display position in the range of -100 to 100 mm in increments of 10 mm when making fine adjustment in the top and bottom direction.

[Fine Adjustment at Left and Right (mm)]

Specify the watermark display position in the range of -100 to 100 mm in increments of 10 mm when making fine adjustment in the left and right direction.

[Rotation (deg)]

Specify rotation of the watermark in the range of -90 to 90 degrees in increments of 45 degrees.

[Transparency (%)]

Specify the transparency of the watermark in the range of 0 to 100 in increments of 10.

0 is the highest transparency.

[Scope of Application]

Select the pages to display the watermark from "First Page," "First and Last Pages," and "All Pages."

When [Text] is selected for [Type]**[Displayed Text]**

Select the text used as the watermark from "Time," "Print Document Name," "User ID," "IP Address," and "Specify Text."

[Specify Text]

When [Specify Text] is selected in [Displayed Text], enter a string in the range of 1 to 128 characters.

[Font Name]

Specify the font of the watermark text. Select the font from those installed in the server.

[Font Size (pt)]

Specify the font size of the watermark text from "50," "60," "70," "80," "90," and "100."

[Letter Color]

Click [Edit] and select the color of the watermark text in the dialog box.

[Bold]

Select the checkbox to use bold letters for the watermark text.

[Italic]

Select the checkbox to use italic letters for the watermark text.

[Masking]

When "IP Address" is selected in [Displayed Text], specify the range of masking.

Items	Descriptions
No	No masking
192.168.1.XXX	Mask the 4th octet of the IP address.
192.168.XXX.XXX	Mask the 3rd and 4th octets of the IP address.
192.XXX.XXX.XXX	Mask the 2nd to 4th octets of the IP address.

Others

[Fine Adjustment at Top and Bottom (mm)], [Fine Adjustment at Left and Right (mm)], [Rotation (deg)], [Transparency (%)], and [Scope of Application] are same as those when [Image] is selected for [Type].

Deleting watermarks

Select a checkbox for the watermarks you wish to delete, and then click [Delete].

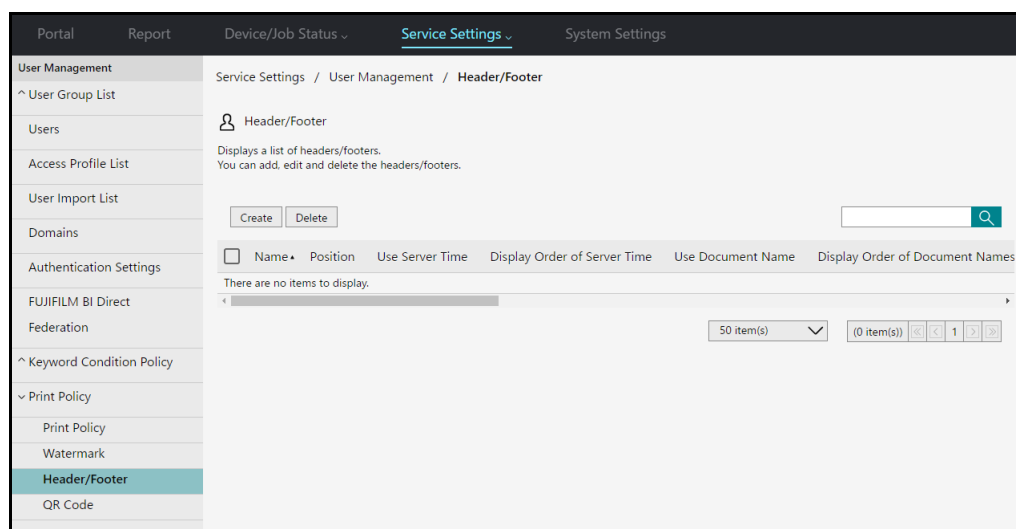
Header/Footer

How to Display

Select [Service Settings] > [User Management] > [Header/Footer] from the menu on the administrator screen.

Page Summary

Displays a list of registered headers/footers.



Adding header/footer

Click [Create] and configure the following items, and then click [Save].

[Name]

Input the name of the header or footer in the range from 1 to 128 characters.

[Position]

Select the header or footer display position from "Upper Left," "Upper Center," "Upper Right," "Lower Left," "Lower Center," and "Lower Right."

[Font Name]

Specify the font of the header or footer text. Select the font from those installed in the server.

[Font Size (pt)]

Specify the font size of the header or footer text in the range of 8 to 48 pt in increments of 1 pt.

[Letter Color]

Click [Edit] and select the color of the header or footer text in the dialog box.

[Display Items]

Set the items of the string to be displayed in the header or footer and the display order in the string. Select the checkbox of the items to be displayed in the string and specify the order in [Display Order] of each item.

When the checkbox of [User IP Address] is selected, specify the masking range of an IP address in [Masking].

When the checkbox of [Specified String] is selected, enter a string in [Specified String] in the range of 1 to 128 characters.



"[Masking]" (P.182)

[Display Delimiter]

Set whether to separate each display item with line breaks, or whether to separate using a single-character delimiter and print in one line.

If separating with line breaks, select the checkbox for [Line Break].

If separating with a delimiter, enter the delimiter in [Delimiter].

Deleting header/footer

Select a checkbox for the headers/footers you wish to delete, and then click [Delete].

QR Code

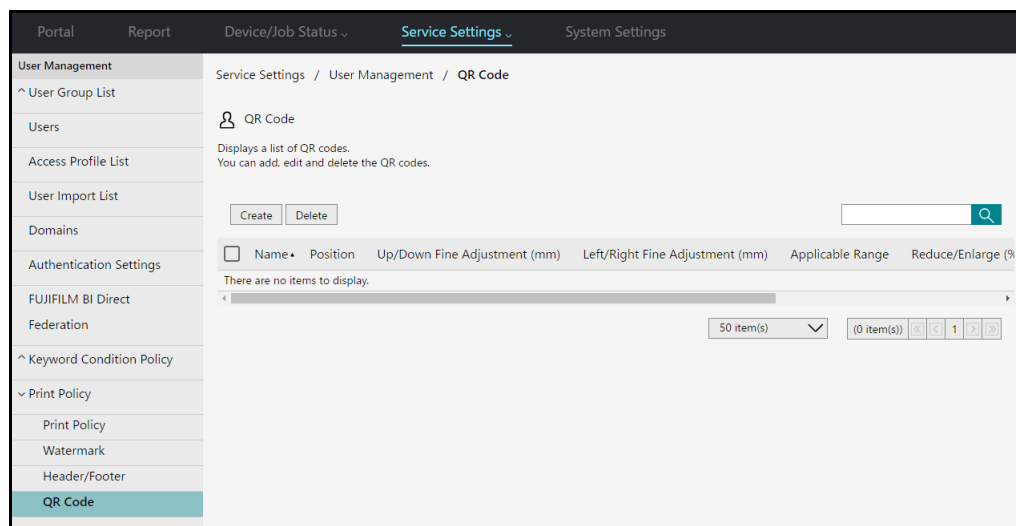
The information embedded by this QR code can be read by a general QR code reader. When personal information is embedded in a QR code, it can be read. When using this feature, obtain consent of the user or take other considerations.

How to Display

Select [Service Settings] > [User Management] > [QR Code] from the menu on the administrator screen.

Page Summary

Displays a list of registered QR codes.



Adding QR code

Click [Create] and configure the following items, and then click [Save].

[Name]

Input the name of the QR code in the range from 1 to 128 characters.

[Position]

Select the QR code display position from "Upper Left," "Upper Center," "Upper Right," "Left Center," "Center," "Right Center," "Lower Left," "Lower Center," and "Lower Right."

[Fine Adjustment at Top and Bottom (mm)]

Specify the QR code display position in the range of -100 to 100 mm in increments of 10 mm when making fine adjustment in the top and bottom direction.

[Fine Adjustment at Left and Right (mm)]

Specify the QR code display position in the range of -100 to 100 mm in increments of 10 mm when making fine adjustment in the left and right direction.

[Scope of Application]

Select the pages to display the QR code from "First Page," "First and Last Pages," and "All Pages."

[Type of String Embedded in QR Code]

Select the checkbox of the item of the string embedded in QR code.

When the checkbox of [Specify String] is selected, enter a string in [Specify String] in the range of 1 to 128 characters.

Deleting QR code

Select a checkbox for the QR code you wish to delete, and then click [Delete].

FUJIFILM BI Direct Federation



Note

This feature is only available in Japan.

How to Display

From the menu on the administrator screen, select [Service Settings] > [User Management] > [FUJIFILM BI Direct Federation].

Page Summary

Configure the settings to use single sign-on authentication for FUJIFILM BI Direct. Automated update schedules can be configured to add and delete tenants, confirm tenant information, and update user information.

Process to Enable and Use Single Sign-on Authentication

You must already have a valid subscription for FUJIFILM BI Direct services before you can configure single sign-on authentication. The process from service subscription to using single sign-on authentication is as follows.

- (1) Subscribe to the services you want to use together with ApeosWare Management Suite.



Note

Contact our representatives for more information on subscribing to services.

- (2) An email notification that services are available for use is sent to the email address provided when you subscribed for services. Set an initial password as necessary.



Note

The user registered when you subscribed for services becomes as the user who can access FUJIFILM BI Direct from ApeosWare Management Suite.

- (3) In ApeosWare Management Suite, display the [FUJIFILM BI Direct Federation] screen, add the single sign-on tenant, and set the required information.



Refer

"Add the single sign-on authentication tenant" (P.186)

- (4) User information will be updated in FUJIFILM BI Direct systems when sent by the device manually or by automated schedules.
- (5) Once user information is updated in FUJIFILM BI Direct systems, an email message is sent to provide some guidance on FUJIFILM BI Direct services.
The following procedure is performed by users.
- (6) Users must access the URL described in the email message before it expires and enter the "authentication code" provided by an administrator.



Note

- The URL becomes invalid if not accessed before it expires. If this happens, an invitation email message must be issued again.
- The “authentication code” is the “tenant ID” that appears when adding a tenant.

(7) If the user is not registered in FUJIFILM BI Direct systems, the user registration screen appears. Follow the on-screen instructions to register user information. If the user has already been registered, the login screen appears. Enter your credentials to log in.

Add the single sign-on authentication tenant

At the [FUJIFILM BI Direct Federation] screen, click [Add].

(1) Access User Settings

Users are authenticated so as to be able to access FUJIFILM BI Direct from ApeosWare Management Suite.

Click [FUJIFILM BI Direct Login] to display the FUJIFILM BI Direct Login screen. Log in as a user with tenant administrative privileges.



Note

The user registered when subscribing to FUJIFILM BI Direct services has tenant administrative privileges.

(2) Select Tenant

A list of tenants managed by the current login user appears. Select the tenant to be added, make a note of the “tenant ID”, and then click [Next].

The “tenant ID” is used as the “authentication code” when users agree to becoming a tenant. Notification is sent to the user associated with the tenant.



Note

Tenants already linked will not appear.

(3) Tenant Policy Settings

Set a tenant policy as necessary, and then click [Next].

Click [Open in New Window/Tab] in [Policy Settings] to display the screen to set tenant policies for FUJIFILM BI Direct.



Note

Close the FUJIFILM BI Direct window once you have finished setting a tenant policy. Continue to set the [FUJIFILM BI Direct Federation] settings.



Refer

Refer to FUJIFILM BI Direct reference material for more information on tenant policies.

(4) Select Access Profile

Select the Access Profile to apply to the tenant, and then click [Next].

Users are registered as tenants once an access profile is selected and applied.



Note

- [FUJIFILM BI Direct Federation] must be configured before users will be registered, regardless of whether an access profile has been applied.
- Access profiles applied to a user group affect all users in the group.
- If a different access profile is applied to the user and the user group to which the user belongs, the access profile applied to the user has priority.

(5) Schedule Settings

Set the schedule to automate updates of ApeosWare Management Suite user information in FUJIFILM BI Direct systems, and then click [Next].

[Schedule Settings]

Select a schedule from the drop-down menu and set the required information.

Select from the following.

- [By Day]
Runs an update at the specified time every day at the time configured with [Time].
- [By Week]
Runs an update on the specified day at the specified time every week configured with [Date/Time].
- [By Week]
Runs an update on the specified date at the specified time every month configured with [Date/Time].
- [Specified Date & Time]
Runs an update once on the specified date at the specified time configured with [Date] and [Time].
- [Off]
Turns off automated, scheduled updates. Information must be updated manually.

[Run Result Notification]

Enables/disables the sending of update results notifications.

Select the [Notify by E-mail] checkbox to enable notifications.

Results of user information updates are sent to the email address registered as the notification contact in the tenant settings.

(6) Overview

After you check the configured setting, clicking [Save] will add the tenant.

You can click [Edit] for each item to change the settings.

Update user information

Perform this operation to manually update user information.

Click  in the tenant list and then select [Start Sending User Information].

ApeosWare Management Suite user information is updated in FUJIFILM BI Direct systems.

Check the update status in the tenant list. To check detailed information, click  and then select [Confirm User Information Processing Status].

To cancel, select [Stop Sending User Information] while the [Status] is [In Progress].



Note

- When the linked tenant changes after changing the user group to which a user belongs or access profile, update the old tenant before updating the new tenant.
- To delete users registered in FUJIFILM BI Direct systems via single sign-on authentication or to delete tenants, delete the user information or remove the access profile in ApeosWare Management Suite and then run the update process in the software.

View tenant information

Click the tenant name link or  in the tenant list and then select [Properties]. Here you can view information configured when the tenant was added, such as the access user and access profile.

Delete tenants

Click  in the tenant list and then select [Delete].

The tenant link will be deleted.



Note

- User information in FUJIFILM BI Direct systems registered via single sign-on authentication will not be deleted. Once the link with ApeosWare Management Suite has been deleted, properties of FUJIFILM BI Direct users can be edited directly.
- Deleting a tenant also deletes single sign-on authentication configuration information stored in devices.

Attribute Correspondence in Import

This section describes the attribute that can correspond to imported information when you import user or account information from the file or the remote authentication server.

User Import

In user import, you can set the following attributes. For the items with “○” in “inbound channel import” in the table, you can import information from the inbound channel.

User Settings

Items	Description	Inbound channel import
Process type	The following character string (this is not case sensitive) • To add: “a” • To refresh: “m” • To delete: “d”	○
First Name	Arbitrary string	○
Last Name	Arbitrary string	○
Display name	Arbitrary string	○
Furigana	Arbitrary string	○
Index	Index characters used for the index search of recipient table. Characters “A-Z” can be entered.	○
E-mail address	Character string in the e-mail address format To specify more than one, perform as follows. • When you import from the remote authentication server With more than one correspondence to values, you can specify more than one e-mail address. If a standard e-mail address is not set at the time of update, the system determines one at random. If it is already set, the setting is held. • When you import from file/database With more than one, specify them by delimiting them with a semicolon (;). The top e-mail address becomes a standard e-mail address.	○

Items	Description	Inbound channel import
User ID	Arbitrary string (single-byte alphanumeric only)  Note Make sure that to update user information to an actual device, the user ID has the character type and number of characters which are usable in the device. The users who do not follow the device restriction cannot be updated to the device.	☐
Alternate User ID	Arbitrary string (single-byte alphanumeric only) To specify more than one, perform as follows. • When you import from the remote authentication server With more than one correspondence to values, you can specify more than one alternate user ID. • When you import from file/database Specify them by delimiting them with a semicolon (;).	☐
Password	Arbitrary string The minimum number of characters and the necessary character type follow the value set in the [Authentication Settings] page. This is case sensitive.	☐
Card ID/PAN	Arbitrary string (single-byte alphanumeric only) To specify more than one, perform as follows. • When you import from the remote authentication server With more than one correspondence to values, you can specify more than one card ID (PAN). • When you import from file/database Specify them by delimiting them with a semicolon (;).	☐
External ID	Arbitrary string (single-byte alphanumeric only) To specify more than one, perform as follows. • When you import from the remote authentication server With more than one correspondence to values, you can specify more than one external ID. • When you import from file/database Specify them by delimiting them with a semicolon (;).	☐
External Accounting ID	Arbitrary string (single-byte alphanumeric only)	☐
End Date/Time	Date and time string in the yyyy/mm/dd hh:mm format Either "2015/1/1 1:1" or "2015/01/0 01:01" can be specified.	☐
Status	Set this item only when importing from files or database. In the import settings, select either [On] or [Off] or specify the following character string from file/database (not case sensitive) • On: "active" • Off: "inactive"	☐ (file/ database only)
Cost Center Code	Arbitrary string	☐
Destination to save	Arbitrary string	☐
User Location	Arbitrary string	☐
Access Profile	Arbitrary string It must be a character string that corresponds with the name of the existing access profile.	☐
Descriptions	Arbitrary string	☐

Items	Description	Inbound channel import
Photo Location/Path	Arbitrary string	☐
Telephone Number	Arbitrary string	☐
Mobile Number	Arbitrary string	☐
Fax Number	Arbitrary string To specify more than one, perform as follows. - When you import from the remote authentication server With more than one correspondence to values, you can specify more than one fax number. - When you import from file/database Specify them by delimiting them with a semicolon (;).	☐
FUJIFILM BI Direct Federation	To enable single sign-on authentication for FUJIFILM BI Direct, configure the user ID (e-mail address) to be registered in FUJIFILM BI Direct.	☐

Associate User with User Group

Items	Description	Inbound channel import
Group Name	Arbitrary string	☐
Descriptions	Arbitrary string	☐
Parent User Group	When creating import, select from the existing user groups.	
Access Profile	When creating import, select from the existing access profiles.	

Create/Associate Personal Account

Items	Description	Inbound channel import
Account	Arbitrary string	☐
Account description	Arbitrary string	☐
First Name	When creating import, select from the existing account groups.	
Start date	Date and time string in the yyyy/mm/dd hh:mm format	☐
End date	Date and time string in the yyyy/mm/dd hh:mm format	☐

Items	Description	Inbound channel import
Account status	When creating import, select [On]/[Off] or the inbound channel field. When the inbound channel field is selected, the account is imported as On if the value is Active/Enabled/True/1/Activated/Yes, and as Off if the value is Inactive/Disabled/False/0/Deactivated/No. In the case of other values, the account status becomes as shown below according to the import method. [Import File] In the case of blank, single-byte space, and double-byte space, the account is imported as the account status is On. [Database] In the case of null or blank, the account is imported as the account status is On. In the case of single-byte space and double-byte space, import fails.	○
Price policy	When creating import, select from the existing price policies.	
Cost Center Code	Arbitrary string	○
External ID1	Arbitrary string	○
External ID2	Arbitrary string	○
Bill to client	When creating import, specify on/off.	
Allotted balance	Number ^{*1}	○
Top-up balance	Number ^{*1}	○
Display the balance of the multifunction device	When creating import, specify on/off.	
Minimum balance	Number ^{*1}	○
Replenishment schedule	When creating import, select from the existing replenishment schedules.	

*1 If the number of digits after decimal point exceeds [Currency Decimal Digits] set in [System Settings] > [Currency Settings], it is rounded down.

Create/Associate Shared Account

Items	Description	Inbound channel import
Account	Arbitrary string	○
Account description	Arbitrary string	○
Shared account that all users can use	When creating import, specify on/off.	
Parent account	When creating import, select from the existing accounts.	
Account group name	When creating import, select from the existing account groups.	
Start date	Date and time string in the yyyy/mm/dd hh:mm format	○
End date	Date and time string in the yyyy/mm/dd hh:mm format	○
Account status	When creating import, select [On] or [Off].	
Price policy	When creating import, select from the existing price policies.	

Items	Description	Inbound channel import
Cost Center Code	Arbitrary string	○
External ID1	Arbitrary string	○
External ID2	Arbitrary string	○
Bill to client	When creating import, specify on/off.	
Allotted balance	Number ^{*1}	○
Top-up balance	Number ^{*1}	○
Display the balance of the multifunction device	When creating import, specify on/off.	
Minimum balance	Number ^{*1}	○
Replenishment schedule	When creating import, select from the existing replenishment schedules.	

*1 If the number of digits after decimal point exceeds [Currency Decimal Digits] set in [System Settings] > [Currency Settings], it is rounded down.

Account Import

In account import, you can set the following attributes. For the items with “○” in “inbound channel import” in the table, you can import information from the inbound channel.

Account Details

Items	Description	Inbound channel import
Process type	The following character string (this is not case sensitive) • To add: “a” • To refresh: “m”	○
Account type	The following character string (this is not case sensitive) • For personal accounts: “personal” • For shared accounts: “shared”	○
Account	Arbitrary string	○
Account description	Arbitrary string	○
Shared account that all users can use	When creating import, specify on/off.	
Parent account	When creating import, select from the existing accounts.	
Account group name	When creating import, select from the existing account groups.	
Start date	Date and time string in the yyyy/mm/dd hh:mm format	○
End date	Date and time string in the yyyy/mm/dd hh:mm format	○
Cost Center Code	Arbitrary string	○
External ID1	Arbitrary string	○
External ID2	Arbitrary string	○
Account status	When creating import, select [On] or [Off].	
Bill to client	When creating import, specify on/off.	
Price policy	When creating import, select from the existing price policies.	

Balance Settings

Items	Description	Inbound channel import
Allotted balance	Number ^{*1}	☐
Top-up balance	Number ^{*1}	☐
Replenishment schedule	When creating import, select from the existing replenishment schedules.	
Display the balance of the multifunction device	When creating import, specify on/off.	
Minimum balance	Number ^{*1}	☐

*1 If the number of digits after decimal point exceeds [Currency Decimal Digits] set in [System Settings] > [Currency Settings], it is rounded down.

User/Account Association Import

In user/account association import, you can set the following attributes. For the items with “O” in “inbound channel import” in each table, you can import information from the inbound channel.

User

Items	Description	Inbound channel import
Process type	The following character string (this is not case sensitive) • To add: “a” • To delete: “d”	O
User identifier	When creating import, select the type of ID to identify users from the following. • User ID • Card ID (PAN) • External ID	
User ID/Card ID (PAN)/ External ID	Any one of the existing user ID, card ID (PAN) or external ID according to the type selected in [User Identifier]	O
Account name	Existing account name	O
Parent account name	Existing account name	O
External ID of account	Existing external ID of account	O
External ID of parent account	Existing external ID of account	O

User group

Items	Description	Inbound channel import
Process type	The following character string (this is not case sensitive) • To add: “a” • To delete: “d”	O
User group name	Existing user group name	O
External ID of user group	Existing external ID of user group	O
Parent user group name	Existing user group name	O
External ID of parent user group	Existing external ID of user group	O
Account name	Existing account name	O
External ID of account	Existing external ID of account	O
Parent account name	Existing account name	O
External ID of parent account	Existing external ID of account	O

User Information Registration by Users

Users are able to register the card ID (PAN) by themselves in either one of the following ways.

- Register the card ID using the card reader connected to a PC
- Register the card ID using the card reader connected to a device
- Read the login QR code displayed on the device and register the external ID.

Register the card ID using the card reader connected to a PC

Operate registration using a web browser by reading the card ID with the IC card reader connected to a PC.

Operation check

Check the following operating environment

Items	Descriptions
Target OS/Network	The same environment as the web client of ApeosWare Management Suite
Target Web browser	Microsoft Edge (use IE mode) Internet Explorer® 11 (use a web browser supported by the OS)
Target card reader	• PaSoRi RC-S320 • PaSoRi RC-S330 • PaSoRi RC-S340 • PaSoRi RC-S360 • PaSoRi RC-S370 • PaSoRi RC-S380 NFC port software supported by the above-mentioned IC Card Readers is required to be installed.



Note

- PaSoRi is the IC card made by Sony Corporation. For the installation and operation method, refer to the manual supplied with PaSoRi.
- If you use a card other than our IC card or Fuji Xerox's, separate settings are required. Please contact our sales representatives.



Refer

ApeosWare Management Suite operating environment → "Setup Guide"

Allowing users to register themselves

Set the following so that users can register the card ID (PAN).

Select [Service Settings] > [User Management] > [Authentication Settings] on the administrator screen, and check [Allow] on [Allow User self-registration].

Registering the card ID

Before operation, set the web browser of the PC as follows.

- Validate JavaScript
- Enable the download of the signed ActiveX control

1. Log in to the PC to which the IC card reader is connected and activate a web browser.

2. Enter the following URL in the address bar of a web browser.

http://{host name or IP address}/UDR/

For {host name or IP address}, specify the host name or IP address of the ApeosWare Management Suite server.



Note

For coded communication with SSL, enter "https://". If you have changed the port number for communication from the default settings (HTTP communication "80", HTTPS communication "443"), enter a colon ":" and the port number following the input of {host name or IP address}.

3. Hold a card over the IC card reader according to a message displayed in the screen.
4. The login screen is displayed, then input user information and log in.
The card ID read with the card reader is registered as properties of the user who has logged in.

Register the card ID using the card reader connected to a device

Read the card ID with the IC card reader connected to the device and register the read card information in ApeosWare Management Suite.

Operating environment

Check the following operating environment

Items	Descriptions
Target device	A target device for ApeosWare Management Suite meets either one of the following conditions • A device model whose authentication method is [Custom Authentication] and to which the custom service is available • A device model whose authentication method is [Remote Authentication] (authentication system: ApeosWare Authentication Agent) and to which the web applications feature is available
Target card reader	The card reader that the above device supports



Note

This feature is not available to the device whose authentication method is [Local Authentication].

Allowing users to register themselves

Set the following so that users can register the card ID (PAN).

Select [Service Settings] > [User Management] > [Authentication Settings] on the administrator screen, and check [Allow] on [Allow User self-registration].

Setting the card authentication

In the device where the authentication method is [Custom Authentication], set the following for the card authentication.

Select [Service Settings] > [User Management] > [Authentication Settings] on the administrator screen, and check [Card Authentication (Device Only)].



Note

For the device where the authentication method is [Remote Authentication], you do not need to set the above. If you put in the card reader to validity, the card authentication is automatically enabled.

Setting the destination of the device web applications

For the device where the authentication method is [Remote Authentication], use the web applications feature and access the self-registration feature of users. For that reason, set some such as the destination URL for use of web applications.



Note

For the device where the authentication method is [Custom Authentication], you do not need to set it.



Refer

Web applications service setup→“Using the Web Applications Features” (P.121)

Registering the card ID

The menu of the control panel depends on devices. This section describes a typical example.

1. Log in to a device by holding the IC card over the IC card reader connected to the device.
2. For the device where the authentication method is [Remote Authentication], operate the following.
 - (1) Display the destination list screen of web applications with the device control panel.
 - (2) Select the destination URL to the self-registration feature of users and then [Open].



Note

For the device where the authentication method is [Custom Authentication], it is automatically connected to the self-registration feature of users.

3. The login screen is displayed, then input user information and log in.
The card ID read with the card reader is registered as properties of the user who has logged in.

Read the login QR code displayed on the device and register the external ID.

Read the login QR code displayed on the device using a mobile application and register the external ID of the mobile application to ApeosWare Management Suite.



Refer

“Advance Setting When Using Login with a QR Code” (P.70)

Operating environment

Check the following operating environment

Items	Descriptions
Target device	A target device for ApeosWare Management Suite meets the following condition. • A device model whose authentication method is [Custom Authentication] and to which the custom service is available
Target mobile applications	• ApeosWare MS Mobile 2 • AliPay • WeChat



Note

This feature is not available to the device whose authentication method is [Local Authentication] or [Remote Authentication].

Allowing users to register themselves

Set the following so that users can register the application ID.

Select [Service Settings] > [User Management] > [Authentication Settings] on the administrator screen, and check [Allow] on [Allow User self-registration].

Enable the QR code for login.

In the device where the authentication method is [Custom Authentication], set the following for login by QR code.

Select the mobile application to use in [Service Settings] > [User Management] > [Authentication Settings] > [QR Code Login Settings] > [Mobile App Settings] and make settings specific to the mobile application.



Note

For AliPay and WeChat, registration and settings of an official account are required in the respective official sites in advance.

Registering the external ID

The menu of the control panel depends on devices. This section describes a typical example.

1. Read the login QR code displayed on the device using the target mobile application.
2. When authentication of the mobile application goes successful, and [Register User Information] is displayed on the device, enter the user ID and password of the user to associate with the external ID.

What if?

This section describes operation of user management.

Actions to take if the network is not connected or is unstable

Since it is necessary to communicate with the Microsoft Entra ID and Microsoft Entra Domain Services when authenticating with users imported from Microsoft Entra Domain Services, if the network is unstable, authentication may be delayed.

To reduce the effect on the network, configure the following settings:

- Disable [Clear local user data when browsing external authentication information]
- Enable [Prioritize local during card authentication]
- Disable [Check user validity for Active Directory/LDAP during card authentication]

If the problem occurs even after you have confirmed that there is no problem with the authentication settings in the operating environment, gradually increase the setting value of [Remote Authentication Timeout] (10 seconds max.).

Precautions at the Time of Updating User Information to the Device

For the user ID, display name, and a password, the number of characters and the character type that you can input are different between ApeosWare Management Suite and the device.

To register in a device the users registered in the remote authentication server and the users added in ApeosWare Management Suite as users for local authentication, you need to be careful about character restrictions in the device. If you ignore restrictions in the device and set the user ID and display name, you cannot update them to the device.

The following table shows the character type and the number of characters you can input.

Target	The character type and the number of characters you can input		
	User ID	Display name	Password
ApeosWare Management Suite	Within 64 characters of ASCII code	Within 128 double- or single-byte characters	Within 50 characters of ASCII code
Device	Depend on devices	Within 16 double-byte characters and 32 single-byte characters	4 to 12 characters of ASCII code



"Update to Device" in "Installation and Operation Guide"

Change a Password of Apeos_Admin Users from the Command

Normally, you can change a password of Apeos_Admin users in the [System Settings] > [Change Administrator Password] menu of the administrator screen. If you forget a password and cannot access the operation screen, you can also change a password by using the command.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Enter the following command, and then press the <Enter> key.

```
cd{Installation Folder}\Utils\ResetPassword
```

{Installation folder} is as follows if no change is made on the default settings.

"C:\Program Files\FUJIFILM\ApeosWare MS"

3. Enter the following command and push the <Enter> key.

```
AwmsResetPassword -u Apeos_Admin [-p {New password}]
```

A password is case sensitive.

If you skip -p {New password}, it becomes the default value (FujiFilm_11111) at the time of installation.

Changing a password and property by users themselves

Login users change their own passwords and properties for logging in to ApeosWare Management Suite by themselves.

1. Display the user screen.

If you click [User Portal] in the header menu during the display of the administrator screen, the user screen is displayed.



Note

The user may not be able to display the user screen depending on the contents of the access profile associated with the user. In this case, the user is not allowed changing the password and the properties by oneself.

2. Select [User/Service Settings] > [User Management] > [User Properties] in the user screen menu.

3. Change the password and other pieces of information, and then click [Apply].

The user may not be able to change the e-mail address and the storing location depending on the contents of the access profile associated with the user.

The screenshot shows the 'User Properties' page in the ApeosWare Management Suite. The top navigation bar includes 'Portal', 'Report', 'Print/Job', and 'User/Service Settings'. The left sidebar has 'User Management' and 'User Properties' (selected). The main content area is titled 'User Properties' and contains the following fields and buttons:

- E-mail Address:** A text input field with a '+' button to the right.
- Storage Location:** A text input field with an information icon (i) to the right.
- Change Password:** A section with an 'Edit' button.
- Apply:** A button at the bottom right of the form.

5 Cost Management

Settings and Confirmation in a Web Browser

You can set and check cost management in a web browser. This section describes what you can do with each page.

- [Service Settings] > [Cost Management]

Pages	Descriptions
Account Group List	Create and manage an account group that unifies accounts.  Refer "Account Group List" (P.201)
Account List	Create and manage an account that manages the balance.  Refer "Account List" (P.204)
Price Policy	Set a device charge list, and rules for a limited-time discount/an additional charge.  Refer "Price Policy" (P.211)
Replenishment Schedule	Set a schedule to replenish the account balance.  Refer "Replenishment Schedule" (P.216)
Settings	Set general settings for Cost Management including the charge calculation method and the notification settings.  Refer "Settings" (P.219)

Account Group List

How to Display

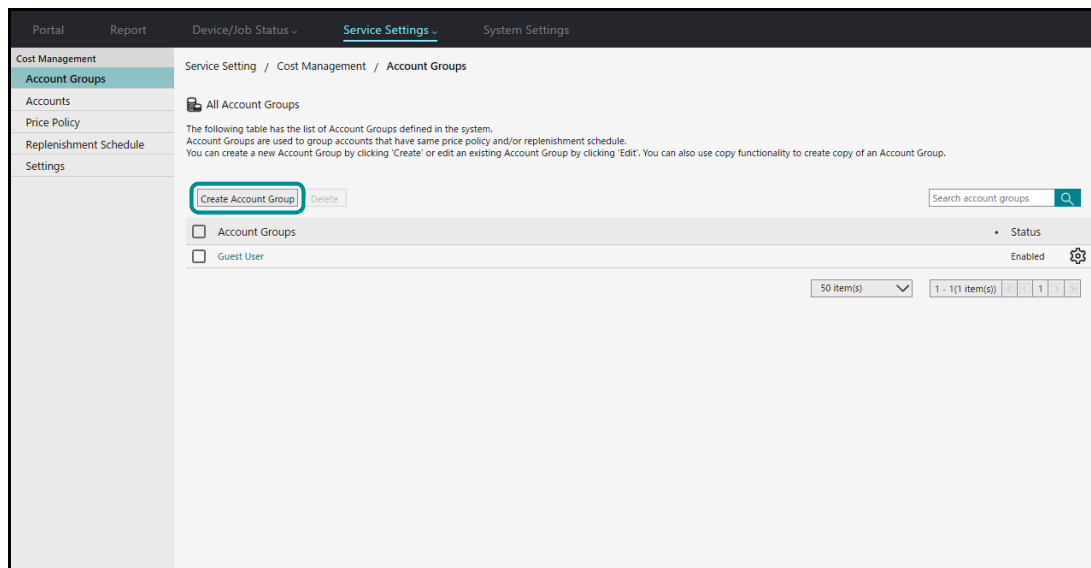
Select [Service Settings] > [Cost Management] > [Account Group List] in the administrator's screen menu.

Page Summary

Create and manage an account group that unifies accounts. You can add an account group, edit, copy, and delete property.

Creating an account group

Click [Create Account Group].



(1) Set an account group

Specify the following item, and then click [Next].

[Group Name]

Enter the account group name.

[Description]

As needed, enter descriptions for the account group.

[Enable Account Group]

Switch a valid and an invalid account group. If you make an account group valid (or invalid), all the accounts affiliated with the group become valid (or invalid).



Note

Even if the account group is enabled, the account out of [Start Date] and [End Date] is disabled.

[Replenishment Schedule]

Select a replenishment schedule used in an account group from the drop-down list. If a replenishment schedule is not set in the account affiliated with an account group, the replenishment schedule you have selected here is applied.

You can also click "Create new replenishment schedule" under the drop-down list box to create a replenishment schedule.



Refer

"Replenishment Schedule" (P.216)

[Price Policy]

Select a replenishment schedule that you use in an account group from the drop-down list. If the price policy is not set in a device, a device group, and an account, the price policy that you select here is applied to an account affiliated with an account group.

You can also click [Create Price Policy] under the drop-down list box to create a price policy.



Refer

"Price Policy" (P.211)

[Account price policy has priority over device/device group]

Normally, higher priority is put on the price policy set in a device or a device group than an account group, but if you select a checkbox for this item, higher priority is put on the price policy set in an account group than that set in a device and a device group.



Note

If the price policy is set in an account, that of the account, not of the account group, is applied.



Refer

"Priority order of the price policy" in "Installation and Operation Guide"

(2) Account Association

Specify the following item, and then click [Next].

[Account Association]

[On]

When you add accounts to account groups, select [On] and associate the account according to the following procedure.

(1) Click [Add] to display the [Add Account] dialog box.

(2) Select the checkbox for the account name to be associated, and then click [Add].



Note

- The account can be added only when the account is enabled.
- To add all accounts, click [Add All].
- To narrow down from the accounts displayed in the account association list, enter a part of account name you want to search into , and then press <Enter>.
- To delete the account association, click [Delete] or [Delete All].

[Off]

Select when you do not associate accounts.

(3) Overview

After you check the configured setting, clicking [Save] will create the account group.

You can click [Edit] for each item to change the settings.

Checking Account Group Information

Click  in the account group list and select [Properties].

You can display and edit the content configured for the account. You can edit the same items as the features configured in "Creating an account group" (P.202).

Copying Account Groups

Click  in the account group list and select [Copy].

You can copy the settings of an account group, and create a new account group. When copying, you can edit the setting items. You can edit the same items as the features configured in "Creating an account group" (P.202).

Delete an account group

Click  of the account group list and select [Delete].

If you delete an account group, the information on the association of an account affiliated with the group is deleted. The account is not deleted.

Account List

How to Display

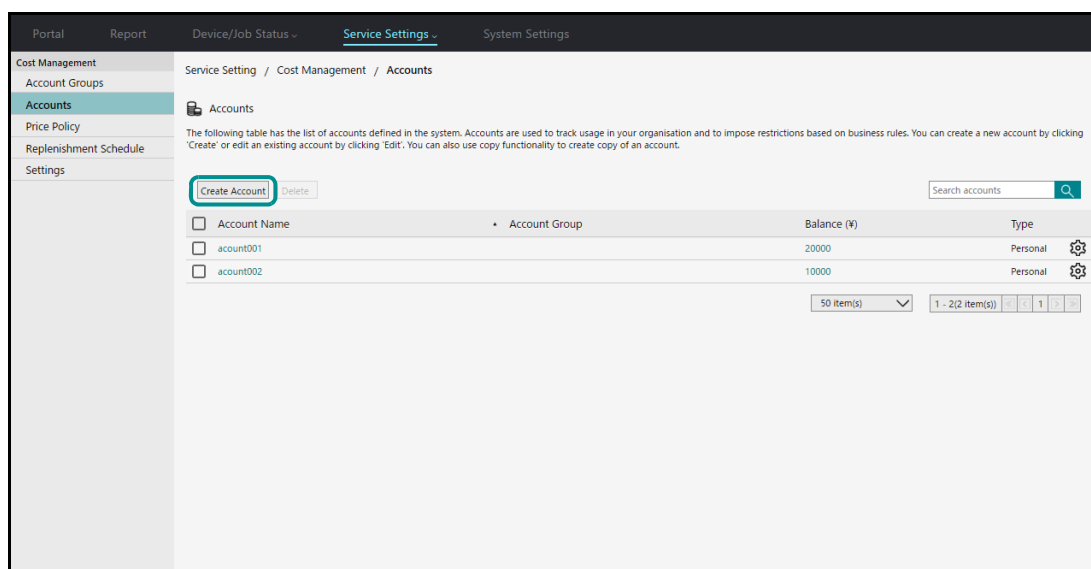
Select [Service Settings] > [Cost Management] > [Account List] in the administrator's screen menu.

Page Summary

Create and manage an account that manages the balance. You can add an account, edit, copy, and delete property.

Create an account

Click [Create Account].



(1) Account Settings

Specify the following item, and then click [Next].

[Account Type]

Select the type of account from the following.

- [Personal Account]
It is an exclusive account for one user. One or more than one personal account can be associated with one user.
- [Shared Account]
It is an account shared and used by more than one user. One shared account can be associated with more than one user.



Once you set the type of account, you cannot change it.

[Account Name]

Enter the account name.

[Description]

As needed, enter descriptions for the account.

[Enable shared account for all users to use]

You can set this item when you select [Shared Account] in [Account Type].

If the checkbox is checked, the users who are set to [Allow] on [Using shared account that all users can use] in the access profile will be able to use this account.

[Parent Account]

You can set this item when selecting [Shared Account] in [Account Type] and not setting [Account Group].

When you set the parental relation for an account, click [Associate Parent Account] and select an account to be a parent from the account list. The account for which the parent account has been set becomes "sub-account".

The relation between the parent account and sub-accounts, and restrictions are as follows.

- The user associated with the parent account can use sub-accounts.
- The user associated with sub-accounts cannot use the parent account.
- When [Enable shared account for all users to use] is set to the parent account, sub-accounts too take it over.
- Sub-accounts cannot be associated with an account group.
- For one account, you can create an sub-account only in one hierarchy.
- You cannot set any account for which the balance is set to a sub-account. You can set the balance for only either the parent account or sub-accounts.

[Account Group]

You can set this item when you do not specify [Parent Account].

Select an account group to be affiliated with an account from the drop-down list box.



Note

You cannot share the balance inside an account group.

[Start Date]/[End Date]

Specify the start date and the end date of an account. You can use an account only between the start date and the end date.

[Enable Account]

Switch a valid and an invalid account.



Note

- When you affiliate an account with an account group, the setting of a valid and an invalid account is overwritten in the setting of a valid and an invalid account group.
- Even when the setting of an account is valid, if the account is not between [Start Date] and [End Date], it is invalid.

[Price Policy]

Select the price policy to use in an account from the drop-down list box.

You can also click [Create Price Policy] under the drop-down list box to create a price policy.

[Account price policy has priority over device/device group]

Normally, higher priority is put on the price policy set in a device or a device group than an account, but if you select a checkbox for this item, higher priority is put on the price policy set in an account than that set in a device and a device group.



Refer

“Priority order of the price policy” in “Installation and Operation Guide”

[Cost Center Code]

Enter the cost center code. You can create a report by tallying per “cost center code”.

[External ID1]/[External ID2]

This is ID managed with the external system. Specify it to work with the external system.

[Enable Client Billing]

You can set this item when putting a check on [Enable shared account for all users to use].

This setting is to create bills to charge your clients (customers). When this item is checked, the [Client Billable] checkbox is displayed on the control panel of the device or the screen for selecting the Popup Messenger account to use the device.

With the report feature, usage reports of the only jobs executed with the [Client Billable] checked can be created.

You cannot set this item in sub-accounts. Sub-accounts take over the setting of [Enable Client Billing] of the parent account.

(2) Set Account Balance

Specify the following item, and then click [Next].

[Set balance for account]

When you set the balance, click [Yes] and specify the following items.

[Set Account Balance]

- [Allotted Balance]

First enter your allotted balance. If you use a device, the charge of a device is first deducted from this balance.

When the parental relation is set in an account, you can set [Allotted Balance] to either of the parent account or sub-accounts.



Refer

Allotted balance → “Balance Types” in “Installation and Operation Guide”

- [Top-Up Balance]

Enter the balance to be allotted to an account in addition. With the increased use of a device and [Allotted Balance] becomes zero (0), the charge of a device is deducted from this [Top-Up Balance].

When the parental relation is set in an account, you can set [Top-Up Balance] to either of the parent account or sub-account.



Refer

Top-up balance → “Balance Types” in “Installation and Operation Guide”

- [Prohibit Top-Up balance charge by general user]

Specify whether you allow users to charge additionally to [Top-Up Balance]. If unchecked, users can

charge the top up balance through an external account management system.

- [Display balance in Device]

When you display a user's status of usage in the control panel of a device, specify whether you display the balance of the account.



Refer

"The (Display your status of usage) Button" (P.116)

Set Minimum Account Balance

- [Minimum Balance]

When you stop the use of a device forcibly, specify the minimum value of the balance as a standard. You can set the values of plus, minus, and zero (0).

For the user whose [Force stop when minimum balance is reached] is set to [Stop] in access profile, if the balance of the account falls below this value, the use of the device is banned.



Note

- The [Force stop when minimum balance is reached] feature is available when the authentication method of a device is [Custom Authentication] and [Remote Authentication (ApeosWare Authentication Agent)].
- Fax does not correspond to [Force stop when minimum balance is reached].
- For [Remote Authentication (ApeosWare Authentication Agent)], copy operation cannot be performed on a device if the account balance is lower than [Minimum Balance] when logging in.



Refer

Details on balance → "Installation and Operation Guide"

- [Amount Limit Settings]

You can set this item in the sub-accounts for which the parental relation is set only when the balance is set for the parent account.

Specify the amount limit available to users. For the user whose [Force stop when minimum balance is reached] is set to [Stop] in the access profile, the device is available up to the lower value of either of the following.

- The difference between [Amount Limit] and the usage record
- The current balance of the parent account



Note

When you do not set [Force stop when minimum balance is reached] in the access profile, the setting of [Amount Limit] is ignored.



Refer

Details on amount limit → "Installation and Operation Guide"

- [Reset current Usage]

You can set this item in the sub-accounts for which the parental relation is set only when the balance is set for the parent account.

Turn the current usage record of this account to zero (0) manually. To reset it, you need to enter your comment.

[Replenishment Schedule Settings]

When you set a replenishment schedule for the balance of an account, click [Yes].

If you select [No], the replenishment schedule of the account group that this account is affiliated with is applied. If The replenishment schedule is not set to the account group or the account is not affiliated with any account group, the update process of the balance is not performed.



Refer

Priority order of replenishment schedule → “Installation and Operation Guide”

- [Set Schedule]

When you have selected [Replenishment Schedule Settings] to [Yes], select the replenishment schedule from the drop-down list box.

You can also click “Create new replenishment schedule” located next to the drop-down list box to create a replenishment schedule.

(3) Associate Users/User Groups

Specify the following item, and then click [Next].

[User Group Association]

You can set this item only when selecting [Shared Account] for [Account Type].



Note

In the [User Management] menu too, you can associate an account with a user group. The same settings are applied in either operation.

[On]

When you add a user group that can use an account, click [On], and then add a user group according to the following procedure.

Selecting the checkbox for [Associate All User Groups] enables all user groups to use the account.

(1) Click [Add] to display the [Add User Groups] dialog box.

(2) Select the checkbox for the user group you wish to add and then click [Add].



Note

- To add all users, click [Add All] in the [Add User Groups] dialog box.
- To narrow down from the user groups displayed in the associated user groups list, enter a part of user group name you want to search into , and then press <Enter>.
- To delete the user group association, click [Delete] or [Delete All] for the associated user group.

[Off]

Select when you are not adding a user.

[User Association]



Note

In the [User Management] menu too, you can associate an account with a user. The same settings are applied in either operation.

[On]

When you add users to an account, select [On] and add the users according to the following procedure.

Selecting the checkbox for [Associate All Users] enables all user groups to use the account.

(1) Click [Add] to display the [Add Users] dialog box.

(2) Select a check mark for the user to be added, and then click [Add].



Note

- The user can be added only when the user is enabled.
- To add all users, click [Add All].
- To narrow down from the users displayed in the associated users list, enter the user ID or a part of user name you want to search into , and then press <Enter>.

- To delete the user association, click [Delete] or [Delete All] for the associated user.

[Off]

Select when you are not adding a user.

(4) Associate Devices/Device Groups

Specify the following item, and then click [Next].

[Associate Device Groups]

In default settings, an account is associated with all device groups. If you want to restrict a device that uses an account, delete the check of [Associate All Device Groups] and select only the device group that you allow to use an account.

[On]

To restrict devices that use the account, select the devices according to the following procedure.



Note

If you select a checkbox for [Associate All Device Groups], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Device Group] dialog box.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all device groups, click [Add All].
- To delete the association with device groups, click [Delete] or [Delete All].

[Off]

Select when you do not associate device groups.

[Associate Devices]

In default settings, an account is associated with all device groups. If you want to restrict a device that uses an account, delete the check of [Associate All Devices] and select only the device that you allow to use an account.

[On]

To restrict devices that use the account, select the devices according to the following procedure.



Note

If you select a checkbox for [Associate All Devices], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Add Device] dialog box.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all devices, click [Add All] in the [Add Device] dialog box.
- To delete the association with device, click [Delete] or [Delete All].

[Off]

Select when you do not associate devices/device groups.

(5) Overview

After you check the configured setting, clicking [Save] will create the account.

You can click [Edit] for each item to change the settings.

Checking Account Information

Click  in the account list and select [Properties].

You can display and edit the content configured for the account. You can edit the same items as the features configured in “Create an account” (P.204).

Copying Account

Click  in the account list and select [Copy].

You can copy the settings of an account, and create a new account. When copying, you can edit the setting items. You can edit the same items as the features configured in “Create an account” (P.204).

Delete an account

Click  in the account list and select [Delete].



Note

If the account usage history is remaining, the account cannot be deleted. Check whether or not the history is remaining according to the procedure below.

- (1) Create a report for [Account Usage & Replenishment History (Cost Management Report)] according to the settings below. If contents are displayed, the history is remaining in the target account.
 - Under [Time Period], select [Custom data range] and specify the period including the job log retention period.
 - Turn ON all [Transaction Type].
 - Turn ON [Service Usage], [Include Canceled], and [Balance Replenishment] under [History Type].
 - Under [Accounts], specify the account to investigate.
- (2) The retention period of the history is the period specified in [Job Log Retention Period]. For details, see the “[Job Log Retention Period] Tab” (P.47).
- (3) If an account cannot be deleted, disable the accounts that need not be used. You can disable an account from the dialog box displayed at the time of selecting deletion. Alternatively, see “[Enable Account]” (P.205).

Creating Sub-Accounts

Click the account link, and click [Create Sub-Account] in the [Create Sub-Account] tab.

The operation is the same as that in “Create an account” (P.204).



Note

When a sub-account is set from the screen that appears when the account name link is clicked, the account you clicked becomes as the parent account. From the account whose type is the same as with the clicked account, you can also select the parent account to modify the association. You cannot change the account type.

Displaying Associated Users and Groups

Click the account link to display the [Associated Devices and Groups] tab.

The associated devices and account groups are shown in the account list.

You can click [Edit] to change the device/group association settings.

The operation is the same as that in “(3) Associate Users/User Groups” (P.208).

Displaying Associated Devices and Groups

Click the account link to display the [Associated Devices and Groups] tab.

The associated devices and account groups are shown in the account list.

You can click [Edit] to change the device/group association settings.

The operation is the same as that in “(4) Associate Devices/Device Groups” (P.209).

Checking Sub-Account Information

Click  in the sub-account list and select [Properties].

You can display and edit the content configured for the sub-account. You can edit the same items as the features configured in "Create an account" (P.204).

By clicking the sub-account link and selecting [Edit], you can also display and edit the content configured for the sub-account.

Price Policy

How to Display

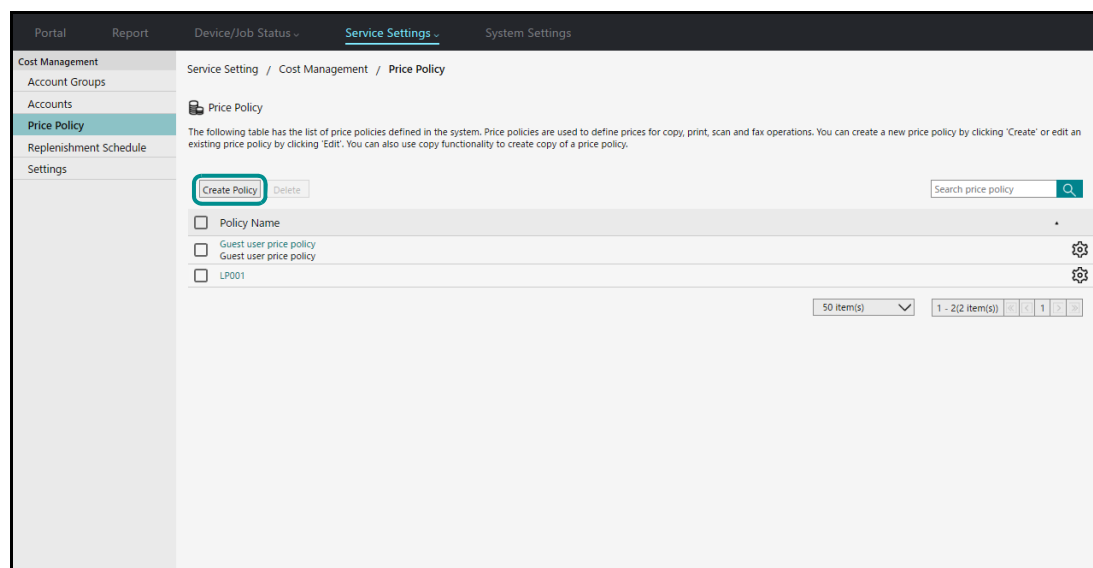
Select [Service Settings] > [Cost Management] > [Price Policy] in the administrator screen menu.

Page Summary

You can set the price policy with rules such as the charge list of the copy, print, scan, and fax by service, and a time-limited discount included. You can add the price policy, edit, copy, and delete property.

Create the price policy

Click [Create Policy].



The screenshot shows the 'Service Settings' section with 'Price Policy' selected. The breadcrumb trail is 'Service Setting / Cost Management / Price Policy'. A sidebar on the left lists 'Cost Management', 'Account Groups', 'Accounts', 'Price Policy' (highlighted), 'Replenishment Schedule', and 'Settings'. The main content area has a title 'Price Policy' and a description: 'The following table has the list of price policies defined in the system. Price policies are used to define prices for copy, print, scan and fax operations. You can create a new price policy by clicking 'Create' or edit an existing price policy by clicking 'Edit'. You can also use copy functionality to create copy of a price policy.' Below this is a 'Create Policy' button (highlighted with a red box) and a 'Delete' button. A search bar 'Search price policy' is on the right. A table lists price policies with columns for 'Policy Name', 'Guest user price policy', and 'LP001'. The table has a '50 Item(s)' dropdown and a '1 - 2(2 Item(s))' pagination control.

(1) Price Policy Details

Specify the following item, and then click [Next].

[Price policy name]

Enter the price policy name.

[Description]

As needed, enter descriptions for the price policy.

[Print]/[Copy]

- [All]
Select it when you set the print and copy charge across the board. Enter the charge per one side.
- [Paper Size]
Select it when you set the charge separately.
Select paper size from the drop-down list box of [Select Paper Size] and enter the charge per 1

sided/2 sided and output color. For the charge to which none of the setup paper is applied, enter the charge in [Default].



Note

When you output a job of odd pages in 2 side with color and black and white paper alternately included, the last page too is calculated as the 2 sided charge.

[Set Price]

- [Scan]

Enter the scan charge per 1 side.

- [Fax]

- [All]

Select it when you set the fax charge across the board. Enter the charge per one side.

- [Detailed Settings]

Select it when you set the charge per fax number.

Click [Add New Pattern] and enter the fax number and charge to compare. The number you have entered is compared with the top number of the fax number. For example, if you specify "02", it applies to "0234567", but not to "0123456".

For the charge to which no set patterns are applied, enter the charge in [Default].

(2) Variance Rules

Specify the following item, and then click [Next].

[Variance Rules]

When you give a discount or an additional charge to the charges set in "(1) Price policy settings", select [Yes] and specify the following items.

[Schedule Settings]

- [Duration and Time Period]

Specify the duration, time period, and days to apply discount or additional charge.

During the time period specified as [Start Date] until [End Date], on the specified [Days], and from [Start Time] until [End Time], the charge is counted by the value set in [Discount/Additional Charge Ratio].

- [Time Period]

Specify the time period and days to apply discount or additional charge.

In each week, on the specified [Days] from [Start Time] until [End Time], the charge is counted by the value set in [Discount/Additional Charge Ratio].

If you set other schedule patterns, click [Add Variance Rule].

[Discount/Additional Charge Ratio]

Enter the ratio with percent (%) to change in the charges set in "(1) Price policy settings". Enter the negative value for a discount and the positive value for an additional charge.

For example, if you set "80 yen" for the print charge and "100 yen" for the copy charge, [Discount/Additional Charge Ratio] and the charges during the period are as follows.

Items	[Discount/Additional Charge Ratio]	Charges During the Period	
		Print "80 yen"	Copy "100 yen"
Discount 5%	-5	76 yen	95 yen
Discount 90%	-90	8 yen	10 yen

Items	[Discount/Additional Charge Ratio]	Charges During the Period	
		Print "80 yen"	Copy "100 yen"
Additional charge 5%	5	84 yen	105 yen
Double	100	160 yen	200 yen
Free of charge	-100	0 yen	0 yen

(3) Account/Group Association

Specify the following item, and then click [Next].

[Associate with Account Group]

[On]

When you associate this price policy with an account group, select [On] and associate the account group according to the following procedure.



Note

If you associate the price policy with both an account group and a device, priority is placed on the price policy of the device. For details, refer to "Priority order of the price policy" in "Installation and Operation Guide".

(1) Click [Add] to display the [Add Account Group] dialog box.

(2) Select the checkbox for the account group name you wish to associate and then click [Add].



Note

- The account group can be added only when it is enabled.
- To add all account groups, click [Add All].
- To narrow down from the account groups displayed in the list of associated accounts, enter a part of account group name you want to search into , and then press <Enter>.
- To delete the account group association, click [Delete] or [Delete All].

[Off]

Select when you do not associate account groups with the user group.

[Account Association]



Note

If you associate the price policy with both an account and a device, priority is put on the price policy of the device. For details, refer to "Priority order of the price policy" in "Installation and Operation Guide".

[On]

When you associate this price policy with an account, select [On] and associate the account according to the following procedure.



Note

If you associate the price policy with both an account and a device, priority is put on the price policy of the device. For details, refer to "Priority order of the price policy" in "Installation and Operation Guide".

(1) Click [Add] to display the [Add Account] dialog box.

(2) Select the checkbox for the account name to be associated, and then click [Add].



Note

- The account can be added only when the account is enabled.
- To add all accounts, click [Add All].
- To narrow down from the accounts displayed in the list of associated accounts, enter a part of account name you want to search into , and then press <Enter>.

- To delete the account association, click [Delete] or [Delete All].

[Off]

Select when you do not associate accounts with the price policy.

(4) Associate Devices/Device Groups

[Do you want to associate the price policy to the device group?]



Note

In the [Device Management] menu too, you can associate the price policy with a device group. The same settings are applied in either operation.

[On]

When you associate this price policy with a device group, select [On] and add the device group according to the following procedure.

When the checkbox for [Associate All Device Groups] is selected, the price policy will be associated with all device groups.



Note

If you select a checkbox for [Associate All Device Groups], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Device Group] dialog box.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all device groups, click [Add All].
- To delete the association with device groups, click [Delete] or [Delete All].

[Off]

Select when you do not associate the price policy with device groups.

[Do you want to associate this price policy with the device?]



Note

In the [Device Management] menu too, you can associate the price policy with a device. The same settings are applied in either operation.

[On]

When you associate this price policy with a device, select [On] and add the device according to the following procedure.

When the checkbox for [Associate All Devices] is selected, the price policy will be associated with all device groups.



Note

If you select a checkbox for [Associate All Devices], the devices registered after this setting are also automatically set for it.

(1) Click [Add] to display the [Device] dialog box.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all devices, click [Add All].

- To delete the association with device, click [Delete] or [Delete All].

[Off]

Select when you do not associate the price policy with devices.

(5) Overview

After you check the configured setting, clicking [Apply] will set the price policy.

You can click [Edit] for each item to change the settings.

Checking Price Policy Information

Click the price policy name link or  in the price policy list, and then select [Properties].

You can display and edit the content configured for the price policy. You can edit the same items as the features configured in “Create the price policy” (P.211).



Note

When you have displayed the price policy information by clicking the price policy name link, click [Edit] when you wish to edit the settings.

Copying Price Policy

Click  in the price policy list and select [Copy].

You can copy the settings of a price policy, and create a new price policy. When copying, you can edit the setting items. You can edit the same items as the features configured in “Create the price policy” (P.211).

Delete the price policy

Click  in the price policy list and select [Delete].

Price Policy List (Price Policy Details)

How to Display

In the price policy list, click on a price policy name.

Page Summary

Add Associated Account & Groups and Associated Devices & Groups to the selected price policy

Displaying Associated Accounts and Groups

Display the [Associated Accounts and Groups] tab.

The accounts and account groups that are associated with price policy are displayed.

By clicking [Edit], you can change the association of account groups/accounts.

The operation is the same as that in “(3) Account/Group Association” (P.213).

Displaying Associated Devices and Groups

Display the [Associated Devices and Groups] tab.

The account groups that are associated with price policy are displayed.

You can click [Edit] to change the device/group association settings.

The operation is the same as that in “(4) Associate Devices/Device Groups” (P.214).

Replenishment Schedule

If setting and executing a replenishment schedule, note the following so that the balance of the account will be replenished after the job log collection of the device is executed.

- Set the schedule so that the replenishment will be executed during the time period when the amount of use of the devices is small.
- Before the replenishment is executed, turn on the powers of all the devices.

Even in the case of a job before the execution of the replenishment schedule, if job logs are collected from devices after the replenishment schedule execution, they are subtracted from the account balance after the replenishment.

How to Display

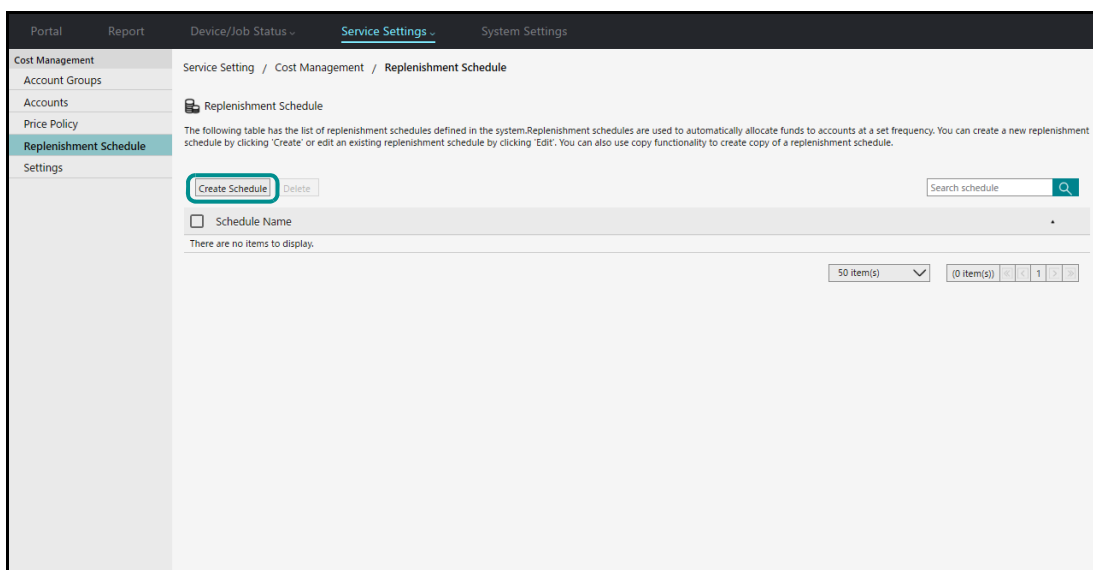
Select [Service Settings] > [Cost Management] > [Replenishment Schedule] from the menu on the administrator screen.

Page Summary

Set a schedule to replenish the account balance. You can add a replenishment schedule, edit, copy, and delete property.

Create a replenishment schedule

When you click [Create Schedule] and set each item, clicking [Apply] will create the replenishment schedule.



[Reset Schedule Name]

Enter the replenishment schedule name.

[Description]

As needed, enter descriptions for the replenishment schedule.

[Frequency]

Select frequency in which you replenish the balance.

- By Day
- By Week
- Fortnightly

- By Month
- Quarterly
- Half Yearly
- Yearly

Set the start date for the replenishment schedule by [Start Date]/[End Date].

The update date for the balance and the update time follow the settings of [Start Date] and [End Date].

For example, if you set the start date to 10 AM, July 1st, 2021 and the end date to 10 PM, December 31st, 2021, the update date for the balance is as follows.

Frequency	Update date	Update time
By Week	Every Wednesday from July 1st until December 31st, 2021	AM10:00
By Month	July 1st, August 1st, September 1st, October 1st, November 1st, December 1st, 2021	AM10:00
Quarterly	July 1st, October 1st, 2021	AM10:00
Half Yearly	July 1st, 2021	AM10:00

[End Date]

Set the end date for your replenishment schedule. After [End Date] is past, the account balance is not replenished. Set [End Date] as necessary.

[Amount]

Enter the amount you replenish in the allotted balance on the replenishment date.

[Balance Update Method]

When [Accumulate] is selected, the amount entered in [Amount] is added to the current balance.

When [Reset] is selected, the current balance is cleared and the amount becomes as entered in [Amount].

For example, if the current amount is 1,000 yen and the replenishment amount is 5,000 yen, the balance after update is as follows depending on when you aggregate or reset it.

Mode	Allotted balance after update
Accumulate	6,000 yen ^{*1}
Reset	5,000 yen

^{*1} Depending on the settings of [Max Balance], and [Replenish to Allotted Balance]/[Replenish to Total Balance], the balance to be carried forward changes.

• [Max Balance]

When you have selected [Accumulate] as the balance update method, specify the maximum balance in order to limit the amount accumulated in the balance. If the result obtained by adding the replenishment amount to the balance is over [Max Balance] set here, the allotted balance is adjusted so that it will not exceed the max value.

- Check against Allotted Balance
Limit the allotted balance so that the allotted balance set for the account does not exceed the maximum balance.

- Check against Total Balance

Limit the total balance so that the total balance set for the account (Allotted balance + Top-up balance) does not exceed the maximum balance.

For example, if the current allotted balance is 200 yen, the current top-up balance is 500 yen, the replenishment amount is 5,000 yen, and the max balance is 5,500 yen, the balance after update becomes as follows.

	Total balance after update	Allotted balance after update	Top-up balance after update
Check against Allotted Balance	Allotted balance 200 yen + Top-up balance 500 yen + Replenishment amount 5,000 yen = 5,700 yen	5,700 yen	500 yen
Check against Total Balance	Total balance 700 yen + Replenishment amount 5,000 yen = 5,700 yen	5,500 yen The replenishment result is 5,700 yen and exceeds the max value 5,500 yen, so the allotted balance is adjusted to the max value of 5,500 yen.	500 yen

When the current allotted balance is 200 yen, the current top-up balance is 500 yen, the replenishment amount is 5,000 yen, and the max balance is not set, the same balance is reached after "Check against Allotted Balance" and "Check against Total Balance" as shown below.

	Total balance after update	Allotted balance after update	Top-up balance after update
Check against Allotted Balance Check against Total Balance	Allotted balance 200 yen + Top-up balance 500 yen + Replenishment amount 5,000 yen = 5,700 yen	Allotted balance 200 yen + Replenishment amount 5,000 yen = 5,200 yen	500 yen

Checking Replenishment Schedule Information

Click the replenishment schedule list name link or  in the replenishment schedule list, and then select [Properties].

You can display and edit the content configured for the replenishment schedule. You can edit the same items as the features configured in "Create a replenishment schedule" (P.216). You can also delete the association of replenishment schedule with the accounts or with the account groups.

Copying Replenishment Schedule

Click  in the replenishment schedule list and select [Copy].

You can copy the settings of replenishment schedule list, and create a new replenishment schedule list. When copying, you can edit the setting items. You can edit the same items as the features configured in "Create a replenishment schedule" (P.216).

Delete the replenishment schedule

Click  in the replenishment schedule list and select [Delete].

Settings

How to Display

Select [Service Settings] > [Cost Management] > [Settings] from the menu on the administrator screen.

Page Summary

Set general cost management. Set each item, and then click [Apply].

The screenshot shows the 'Service Settings' page with a sidebar menu on the left containing: Portal, Report, Device/Job Status, Service Settings (selected), and System Settings. The main content area is titled 'Service Setting / Cost Management / Settings' and includes a 'Settings' icon. Under 'Charge Calculation Settings', it states 'Configures the charge calculation method for billing.' and shows two radio button options: 'Output Count' (unselected) and 'Smaller Value of Estimated and Output Count' (selected). Below this is the 'Notification Settings' section, which includes 'E-mail Notification' (radio buttons for 'Notify' and 'No', with 'No' selected) and 'Error Email Notification' (radio buttons for 'Yes' and 'No', with 'No' selected). The 'Account Label Settings' section includes a description and two radio button options: 'Personal' and 'Shared'.

[Charge Calculation Settings]

When printing, the charge is calculated based on the predicted value obtained from the print job and subtracted from the balance, but this predicted value can differ from the actual output count of actual printing. To adjust such a difference, you can select the charge calculation method from the followings.

- [Output Count]

The charge is calculated based on the actual value of printing,

When the actual value exceeds the predicted value, the difference is subtracted from the account balance after the job log is collected. When the actual value is less than the predicted value, the difference is returned to the account balance.

- [Smaller Value of Estimated and Output Count]

The charge is calculated with the smaller value after comparing the actual value and the predicted value.

When the actual value is less than the predicted value, the difference is returned to the account balance after the job logs is collected.



Note

- When print is made via print management, for the users whose setting of [Force stop when minimum balance is reached] is not enabled, the charge is calculated with [Output Count].
- [Charge Calculation Settings] will be applied only after the setting is made. It does not affect the past operation record.

[Notification Settings]

- E-mail Notification

[Notify]

When the lower limit value specified in [Notify When Value Falls Below] falls below, e-mail notification is sent to the users specified in [Add the following email address to the Notification Address].

You can specify more than one notification address by clicking .

When you select the checkbox for [Notify when account reached minimum balance], notification e-mail is sent again when the value falls below the minimum balance.

[Off]

Notification e-mail is not sent when the balance decreases.

The default format of the e-mail is as follows.

Items	Descriptions
Subject	<ApeosWare Management Suite> Balance is getting low.
Sender	Sender's e-mail address set in [System Settings] > [Network Settings] > [SMTP/POP3]
Address	User's standard e-mail address
Message body	Account Name, User Name, User ID, and the balance

You can change the format of the notification e-mail by directly editing the template file.

The changed format is applied from the next notification e-mail.

File storage location:

- {Folder of data storage directory} ¥Data¥Conf¥CR¥Mail
In default setting, {Folder of data storage directory} is "C:¥FUJIFILM¥ApeosWare MS".

File name:

Edit the file for subject and the file for message body separately. Edit the following files using the language that was set during the ApeosWare Management Suite installation. The text encoding is UTF-8.

File for subject

MailSender_BalanceThreshold_Subject_ja.txt (Japanese)

MailSender_BalanceThreshold_Subject_en.txt (for languages other than Japanese)

MailSender_BalanceThreshold_Subject2_ja.txt (Japanese)

MailSender_BalanceThreshold_Subject2_en.txt (Language other than Japanese)

File for message body

MailSender_BalanceThreshold_Body_ja.txt (Japanese)

MailSender_BalanceThreshold_Body_en.txt (for languages other than Japanese)

MailSender_BalanceThreshold_Body2_ja.txt (Japanese)

MailSender_BalanceThreshold_Body2_en.txt (Language other than Japanese)

- Variables

The following variables are available.

Variables	Description
%ACCOUNTNAME%	Account Name that fell below the minimum value (threshold)
%DISPLAYNAME%	Display Name of the notification target user
%USERID%	User ID of the notification target user
%CURRENTBALANCE%	Current account balance (Displays the total balance)
%THRESHOLD%	Minimum value (threshold)

Example of the text settings

The balance of %ACCOUNTNAME% fell below the threshold %THRESHOLD%.

User name: %DISPLAYNAME%

User ID: %USERID%

The current balance of the parent account: %CURRENTBALANCE%

- Error e-mail notification

Specify whether to send an e-mail notification to the administrator when an unanticipated job is received, such as closed job and canceled job.

[On]

When an error is detected, notification e-mail is sent to the specified users.

You can specify more than one notification address by clicking .

By clicking [Advanced], you can select the details of error to detect.

[Off]

Error detection e-mail is not sent.



Note

In [Occurrence of a job where the difference between the output estimation and output result is the same as the threshold value or more] of [Advanced], the value given from the following calculation formula by percentage (%) is specified and the error is determined when the plus/minus difference exceeds the specified value.

Specified value = Predicted output ÷ Actual output x 100

[Account Label Settings]

The account label displayed on the user screen or the control panel of the device can be changed for easy recognition. The settings are common in all languages.

[Account List Display Settings]

Set the display order of the account list displayed on the account control screen. When you select the checkbox for [Ascending Order of Account Names], the names are displayed in the ascending order.

[Account Selection Settings on Multifunction Device]

Customize [Select Accounts] displayed after authenticated on the control panel of the device in [Default Settings].

This setting is valid only for the device that [Authentication/Accounting Mode] is set to [Custom Authentication] and is affiliated with the group device.

When you select the checkbox for [Always Show [Select Accounts] After Authentication], [Select Accounts] is displayed under the specific conditions.



Refer

"Select Accounts screen of ApeosWare Management Suite" (P.114)

[Print Server Linkage Settings]

In [Price Policy], select a created price policy.

[Refund if not printed] sets the amount of time until refunds are made for unprinted prints from the GX Printer Server.

Setting and Check from Command Line Tools

The update and check of an account balance can be performed from the command line tools. The overview and operation method of the command line tools are explained.

Overview of command line tools

There are three tools as command line tools for cost management as shown in the following.

- Account balance update tool (AWMSUpdateBalance)
Using the file for account balance update, update the allotted balance or top-up balance for each account. After the update, automatically create a recovery file to understand error situations.
- Account balance acquisition tool (AWMSGetBalance)
Check the allotted balance or top-up balance.
- Recovery file repair tool (AWMSRepairRecoveryFile)
Repair the recovery file in which error situations are written so that it can be used with the account balance update tool.

Update of account balance

The method of updating the allotted balance or top-up balance of an account using the command line tool is as follows. After the update of account balance, the result of update is indicated with Exit code. The update of an account balance is available only with the accounts to which the balance is set.

1. Create a file for account balance update.



Refer

"Creation of file for account balance update" (P.222)

2. Specify the file created in procedure 1 to execute the account balance update tool.



Refer

"Update of allotted balance or top-up balance for each account" (P.224)

3. Check the Exit code of the account balance update tool to execute the operation for each Exit code.



Refer

"Checking and handling of Exit code" (P.227)

Creation of file for account balance update

Create a file in which the account name, allotted balance or top-up balance are written used for the account balance update tool. Depending on options designated to the file (→P.225), you can use an arbitrary CSV file.

Character code of file for account balance update

A character code when a file for account balance update is saved varies depending on the option specified with the account balance update tool.

- When not specifying the -sh option
UTF-8 (no BOM)

- If `-sh` option is specified

Shift-JIS



Note

When specifying an arbitrary format, refer to “-ls options of account balance update tool” (P.226).

Format of file for account balance update

Create a file for account balance update, with a comma separated CSV format text file. An entry item varies depending on the option specified with the account balance update tool.

- If `-s` option is not specified

```
{Account name}, {Amount added or subtracted}
{Account name}, {Amount added or subtracted}
.
.
.
```

Entry description	Description
Account name	Account name for updating allotted balance or top-up balance. Specify it with two-byte or one-byte characters. The number of characters is 250 or less.  Note If a comma is included in an account name, the entire name should be surrounded by double quotes (" ").
Amount added or subtracted	If adding to the current account balance, specify the added amount with a positive integer. If subtracting from the current account balance, specify the subtracted amount with a negative integer. Specify the amount with one-byte numbers. An amount which can be specified is in the following range. -99999999999999 to 99999999999999 (14 digits)  Note Specify the identification of an allotted balance and top-up balance with the option of the account balance acquisition tool.

- If `-s` option is specified

```
{Account name}, {Parent account name}, {Amount added or subtracted}
{Account name}, {Parent account name}, {Amount added or subtracted}
.
.
.
```

Entry description	Description
Account name	Account name for updating allotted balance or top-up balance. Specify it with two-byte or one-byte characters. The number of characters is 250 or less.  Note If a comma is included in an account name, the entire name should be surrounded by double quotes (" ").

Entry description	Description
Parent account name	If an account to update a balance is a sub account, specify a parent account name. If this item is not specified, the non-sub account (first hierarchy account) is the update target. Specify it with two-byte or one-byte characters. The number of characters is 250 or less.  Note If a comma is included in an account name, the entire name should be surrounded by double quotes (" ").
Amount added or subtracted	If adding to the current account balance, specify the added amount with a positive integer. If subtracting from the current account balance, specify the subtracted amount with a negative integer. Specify the amount with one-byte numbers. An amount which can be specified is in the following range. -99999999999999 to 99999999999999 (14 digits)  Note Specify the identification of an allotted balance and top-up balance with the option of the account balance acquisition tool.

Update of allotted balance or top-up balance for each account

The method to update an account balance is as shown in the following.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Enter the following command and press the <Enter> key.

```
AWMSUpdateBalance -f {Balance update input file path} -o {Output destination root folder path} (-a|-t) [-s|-ls|-sh] [-Xn]
```

For (-a|-t), specify "-a" or "-t".

For [-s|-ls|-sh], specify "-s", "-ls", and "-sh".

If "-a" and "-s" are specified, describe as shown in the following.

```
AWMSUpdateBalance -f {Input file path for balance update} -o {Output destination root folder path} -a -s [-Xn]
```

Specify the "-b" option when the balance update input file is a recovery file which is designated for the "-f" option.

- When the input file is not a recovery file

```
AWMSUpdateBalance -f {Balance update input file path} -o {Output destination root folder path} (-a|-t) [-s] [-ls spec] [-sh] [-Xn]
```

- When the input file is a recovery file

```
AWMSUpdateBalance -f {Recovery file path} -b {Backup file path for error occurrence} -o {Output destination root folder path} (-a|-t) [-s] [-ls spec] [-sh] [-Xn]
```


When performing an operation with the recovery file designated, specify the same options, other than “-b”, as with the command that was run initially.



Note

- Execute the update of an account balance by specifying the account in the file for account balance update or recovery file.
- Specify the items of an allotted balance, top-up balance, etc. for each account with the option of the account balance update tool.

Account balance update tool options

The options of the account balance update tool are as shown in the following.

○: Required

-: May be skipped

Options	Required	Option name	Descriptions
-f	○	Input file path for balance update	Specify a file for created account balance update and recovery file automatically created or repaired. If a recovery file has been specified, skip the account which has been processed. As for a judgment of whether it has been processed, make a judgment by whether “1” is output to the balance update completion flag.
-b	-	Backup file path for error occurrence	When specifying the recovery file for -f, this option must be set. If not designating the recovery file for -f, setting of this option is not necessary. Designate the backup file path at the time of error occurrence.
-o	○	Output destination root folder path	Specify the root folder paths that become as the designated output destinations for the balance update input file and recovery file. The output destinations for files are as follows. • Output destination for the balance update input file {Output destination folder path} %backup • Output destination for the recovery file {Output destination folder path} %recovery Before executing the account balance update processing, rename the input file, and move the file to the output destination path for the balance update input file. When the account balance update processing is started, a recovery file is created in the recovery file output destination.

Options	Required	Option name	Descriptions
-a	○	Update of allotted balance	Specify it if updating the allotted balance of an account.  Note It cannot be specified with -t at the same time.
-t		Update of top-up balance	Specify it if updating the top-up balance of an account.  Note It cannot be specified with -a at the same time.
-s	-	Balance update of shared account and global account	Specify it if updating the balance of a shared account or global account.  Note • If a balance has been specified to a shared account or global account, the balance update of a sub account cannot be performed. • The top-up balance of a shared account or global account cannot be updated. • If specifying this option, create a file for account balance update with a dedicated format. • If specifying this option, the balance update of an individual account cannot be performed.
-ls {Column specifier}	-	Column specification of input file	Specify it if using any format CSV file as a file for account balance update.  Refer “-ls options of account balance update tool” (P.226)
-sh	-	Read an input file with Shift-JIS.	Specify it if reading a file for created account balance update and recovery file automatically created or repaired with the Shift-JIS format. If this option is specified, also the recovery file automatically created becomes the Shift-JIS format.
-Xn	-	Not updating the balance (Simulation feature)	Check whether the account update tool can be run by any other option that is specified. When this option is specified, the followings are not performed: retrieval of pre-update balance, balance update, and retrieval of post-update balance.
-h	-	Display help	Display help

-ls options of account balance update tool

When the -ls option is specified to the account balance updating tool, a CSV file of arbitrary format becomes available as the account balance update file. With the -ls option, specify arbitrary lines in the CSV file to set the account name, parent account name, and amount to be added/subtracted. Specify each item by arranging the line specifiers in a comma delimited format. When the lines you specify are

distant from each other, use integers to specify the number of lines to be skipped. Specify the line specifier using uppercase letters.

Column specifier	Whether there is necessity	Column specifier name	Descriptions
AN	○	Account name	Specify a column in which an account name is written.
PAN	○	Parent account name	If the -s option is specified, specify a column in which a parent account name is written.
B	○	Amount added or subtracted	Specify a column in which the amount added or subtracted is written.
{Positive number}	-	-	Specify the number of interval columns of columns specified to the column specifier with an integer from 1 to 256.

- Example in which account name is written in first column and amount added or subtracted is written in fourth column
-ls AN,2,B
- Example in which parent account name is written in first column, account name is written in second column and amount added or subtracted is written in sixth column
-ls PAN,AN,3,B

Checking and handling of Exit code

The details of Exit codes are as shown in the following.

Exit code	Description	Detail
0	Normal finish	-
1	Error which can be recovered by retry	• It is a communication error before a balance is updated.

Exit code	Description	Detail
2	Error which cannot be recovered even by retry	• Unable to create “Output destination for the account balance updating input file” or “Recovery file output destination” folder. • A file having the same name exists in the output destination for the account balance update input file. Or there is no access right of a specified output destination. • There is no specified account. • No balance has been set in a specified account. • The update of the top-up balance of a specified account is prohibited. • A balance has been set to a parent account, so the balance update of a specified account cannot be performed. • The format of a file for account balance update or recovery file is illegal. • The number of elements excluding header and footer of entered recovery file does not match with the number of backup file elements at the time of error occurrence. (Only when the recovery file is specified to -f and the backup file at the time of error occurrence is specified to -b) • A backup file at the time of error occurrence is specified which is not linked with entered recovery file. (Only when the recovery file is specified to -f and the backup file at the time of error occurrence is specified to -b) • The license of the Cost Recovery Option does not exist. • Database error.
3	Communication error or recovery file cannot be written	• The creation of a recovery file failed. • Communication error. • The reading of a file for account balance update or recovery file failed.
4	Wrong parameter	• The necessary option of the account balance update tool has not been set. • The -a and -t options of the account balance update tool were specified at the same time. • The -b option of account balance updating tool is not specified. • Path does not exist which was specified by -f, -b, or -o option of account balance updating tool.  Note Any symptom relevant to -b option occurs only when the recovery file is specified with the -f option.
5	There is no administrator authority	• There is no administrator authority in a user who performed the account balance update tool.
6	Multiple activation	• The account balance update tool has already been executed.
7	Normal finish with warning	• The update processing of an account balance succeeded but an error occurred in balance acquisition for a log output.

Recovery file

In the case of an error finish, check whether a file has been created to the output destination of a recovery file. If it has been created, the file becomes a recovery file. The handling for each Exit code varies depending on whether there is a recovery file and description written in the file.



Note

If the account specified as the operation target does not exist, processing up until that point is performed, but processing after the account that does not exist is not performed.
If the value to update is 0, processing of that account is not performed, processing of the next account continues.



Refer

For details on the output destination for recovery file and the description written in the file, refer to "Recovery file" (P.230).

Handling in case where Exit code is 0 or 7

The update of an account balance succeeded, so there is no additional work.

Handling in case where Exit code is 1

The operation varies depending on the status of the recovery file.

- If no recovery file is created
Perform Step 2 of "Update of account balance" (P.222) again.
- If recovery file has been created
Specify the automatically created recovery file, and perform Step 2 of "Update of account balance" (P.222).

Handling in case where Exit code is 2

Check which symptom in the following applies by the standard output or log and perform processing corresponding to each symptom.

- There is a file with the same name in the output destination of a file for account balance update specified in the -o option of the account balance update tool. Or there is no access right of a specified output destination.
- There is no specified account.
- No balance has been set in a specified account.
- The update of the top-up balance of a specified account is prohibited.
- A balance has been set to a parent account, so the balance update of a specified account cannot be performed.
- The format of a file for account balance update or recovery file is illegal.
- The license of the Cost Recovery Option does not exist.
- Database error.

Handling in case where Exit code is 3

The operation varies depending on the status of the recovery file.

- If no recovery file is created
Perform Step 2 of "Update of account balance" (P.222) again.
- If content of recovery file is empty or there is only header row

- 1 Repair the recovery file with the recovery file repair tool.



"Repair of recovery file" (P.233)

- 2 Specify the repaired recovery file, and perform Step 2 of "Update of account balance" (P.222).
- If content is written in recovery file
 - 1 Specify an account in which "Balance update start flag" is "1" and "Balance update completion flag" is not written with a recovery file.



"Recovery file" (P.230)

- 2 Check that the balance of the account specified in the above has been updated correctly with the account balance acquisition tool or WebUI.



- "Check of account balance" (P.230)
- "Account List" (P.204)

- 3 For an account in which the balance has not been updated correctly, repair the recovery file with the recovery file repair tool.



"Repair of recovery file" (P.233)

- 4 Specify the repaired recovery file, and perform Step 2 of "Update of account balance" (P.222).

Handling in case where Exit code is not 0, 1, 2, 3 and 7

Perform Step 2 of "Update of account balance" (P.222) again.

Recovery file

If the account balance update tool is executed, the CSV format recovery file is created automatically. The update result of an account balance is output to the recovery file. Use it as an input file when the account balance update tool is re-executed if an error occurs.

Output destination and file name of recovery file

The output file name of a created recovery file varies depending on the case where the update of the account balance has been completed normally and the case where an error has occurred.

- Case of normal completion
{Input file name}_r_yyyyMMddHHmmssSSS.csv
- Output destination in case of error completion
E_{Input file name}_r_yyyyMMddHHmmssSSS.csv

The output destination of a recovery file is under a folder specified with the -o option.

{Output folder path}\recovery

Check of account balance

The method to check an account balance with the command line tool is as shown in the following. After the check operation of the account balance, the operation result is shown with an Exit code. Also the check result is output with a log file.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Enter any of the following commands, and then press the <Enter> key.
 - When retrieving specific account

```
AWMSGetBalance -n {Account name} (-a|-s) [-p {Parent account name}] [-Of {Output file name}] [-Ow] [-Ts]
```

- When retrieving all accounts nested in specific group

```
AWMSGetBalance -n {Account Group Name} -Ag [-Of {Output file name}] [-Ow] [-Ts]
```

- When retrieving all accounts

```
AWMSGetBalance -Aa [-Of {Output file name}] [-Ow] [-Ts]
```



Note

- As for an account balance, the total balance of the allotted balance and top-up balance is displayed to the standard output.
- If a display target account is a sub account, specify a parent account.
- If there is no parent account specification, the balance of a shared account matching with the specified account name is displayed.
- If the specified account does not exist, an error is displayed.

Options of account balance acquisition tool

The options of the account balance acquisition tool are as shown in the following.

○: Required

-: May be skipped

Options	Required	Option name	Descriptions
-n	○	Account name	Specify an account name for checking an account balance.
-a	○	Personal Account	Specify it if setting a check target to an individual account.  Note It cannot be specified with -s at the same time.
-s		Shared Account	Specify it if setting a check target to a shared account.  Note It cannot be specified with -a at the same time.

Options	Required	Option name	Descriptions
-p	-	Parent account name	Specify it if displaying the balance of a sub account. If a parent account name is specified, the balance of a sub account corresponding to the account name specified with the -n option is displayed.  Note Specify the -p option if the -s option is specified.
-Ag	-	Designating retrieval target as all accounts nested in Account Group	It is an option to set the retrieval target as all accounts (including personal and shared) nested in Account Group. Specify the name of Account Group by the -n option.
-Aa	-	Designating retrieval target as all accounts	It is an option to set the retrieval target as all accounts (including personal and shared).
-Of [filename]	○ ^{*1}	Name of retrieval result output file	Specify the name of output file by enclosing with double quotation (") mark (can also be specified using the full file path). When only the file name is specified, the file is created in the current directory. You need to include the following extension in the file name. • Include ".csv" when the -Ts option is not specified • Include ".tsv" when the -Ts option is specified  Note If no extension is specified or if any extension other than the above is contained, an error occurs.
-Ow	-	Save by overwriting when outputting the file	When the file name specified for the file output is the same as that of an existing file, the result of output will overwrite the existing file. When not specified, the overwrite save is not performed.  Note If there is already an existing file, an error occurs.
-Ts	-	Retrieval result output file format	Specify when outputting the file in the TSV format. When not specified, the file is output in the CSV format. The setting of this option is effective with both the standard output and file output.
-h	-	Display help	Display help

*1 It is required when the -Ow option is specified.

Detail of Exit codes

The details of Exit codes are as shown in the following.

Exit code	Description	Detail
0	Normal finish	-
1	Processing error	• Communication error. • There is no specified account. • No balance has been set in a specified account. • The license of the Cost Recovery Option does not exist. • Database error.
2	User operation error	• The necessary option of the account balance acquisition tool has not been set. • The -p option has been specified but no parent account name has been specified. • The -a and -s options of the account balance acquisition tool were specified at the same time. • There is no administrator authority in a user who performed the account balance acquisition tool.

Repair of recovery file

If the result of the execution of the account balance update tool is Exit code 3, repair and use the output recovery file.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Enter the following command and press the <Enter> key.

```
AWMSRepairRecoveryFile -i {Backup file path for error occurrence} -r {Path of recovery file to be repaired} -o {Output destination of recovery file after repair} (-n|-d) [-s|-ls|-sh]
```

For (-n|-d), specify "-n" or "-d".

For [-s|-ls|-sh], specify "-s", "-ls", and "-sh".

If "-n" and "-s" are specified, describe as shown in the following.

```
AWMSRepairRecoveryFile -i {Backup file path for error occurrence} -r {Path of recovery file to be repaired} -o {Output destination of recovery file after repair} -n -s
```



Note

A recovery file after a repair is output to a path specified with the -o option.

Options of recovery file repair tool

The options of the recovery file repair tool are as shown in the following.

○: Required

-: May be skipped

Options	Required	Option name	Descriptions
-i	○	Backup file path for error occurrence	Specify the path of balance update input file for when an error occurs.  Refer "Output destination and file name of recovery file" (P.230)
-r	○	Path for recovery file of repair target	Specify a path for the recovery file of a repair target.  Refer "Output destination and file name of recovery file" (P.230)
-o	○	Output destination of recovery file after repair	Specify the output destination of a recovery file after a repair.
-n	○	Specified account is included in balance update target	Set [Balance update completion flag] in the error occurrence account row to "0" for a repair target recovery file.  Note It cannot be specified with -d at the same time.
-d		Include error occurring account for update of balance	Set [Balance update completion flag] in the error occurrence account row to "1" for a repair target recovery file.  Note It cannot be specified with -n at the same time.
-s	-	Exclude error occurring account for update of balance	By specifying this option, the recovery file is considered as an input file for the account balance update of a shared account or global account.  Note If this option is not specified, the column of the parent account name is not output into the recovery file after a repair.
-ls [spec]	-	Column specification of input file for balance update	Specify it if using any format CSV file as a file for account balance update.  Refer "-ls options of account balance update tool" (P.226)

Options	Required	Option name	Descriptions
-sh	-	Read an input file with Shift-JIS.	Specify it if reading a file for created account balance update and recovery file automatically created or repaired with the Shift-JIS format. If this option is specified, also the recovery file repaired is output with the Shift-JIS format.  Note If this option is not specified, the recovery file repaired is output with UTF-8 (without BOM).
-h	-	Display help	Display help

Cost Management Operation

Start Cost Management

For cost management, you need to set the following.

- Add User
- Create New Account
- User/Account Association
- Create Price Policy
- Supplement Schedule Settings

When you have set these and a user selects an account and uses the device service, cost management starts.

Devices For Cost Management

For cost management, set [Authentication/Accounting Mode] of the device group that a device is affiliated with to either of the followings.

- Local Authentication/Local Accounting (Local Authentication)
- Local Authentication/Network Accounting (Network Authentication)
- Remote Authentication (select ApeosWare Authentication Agent for the authentication system)
- Custom Authentication

For details of each mode, refer to “Authentication/Accounting Settings Type” in “Installation and Operation Guide”.

When You Select an Account

When you operate with the device control panel

Performance varies depending on the authentication method of a device.

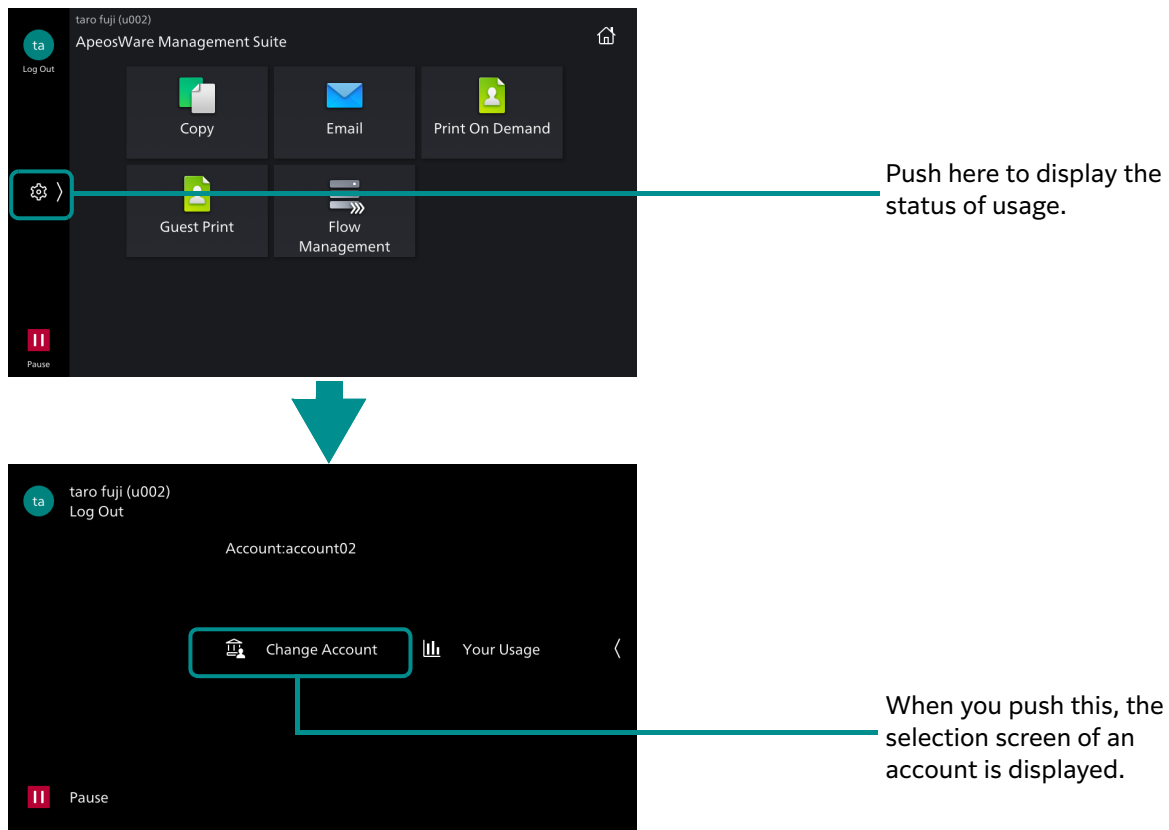
The authentication method of a device is [Custom Authentication]

If authentication by a device succeeds when there is more than one account associated with a user, the selection screen of an account is displayed in the control panel. Select one account to use.

On the [Favourite Account] tab, the user-set favourite account is displayed. For the setting method, refer to “Add Favourite Accounts” (P.237).

On the [Recently Used Account] tab, accounts that recently executed jobs are displayed up to 10 accounts.

When you set [Force stop when minimum balance is reached] of access profile to [No stop], even after the screen transitions to ApeosWare Management Suite screen, you can change an account.



Note

When you set [Force stop when minimum balance is reached] of access profile to [Stop], after the screen transitions to ApeosWare Management Suite screen, you cannot change an account.

When there is only one account associated with a user, the selection screen of an account is not displayed. The associated account is used.

The authentication method of a device is [Local Authentication] or [Remote Authentication]

You cannot select an account during the device operation. The default account set to the user is automatically selected.

When you print

When the setting is that the popup notification screen is displayed in your client PC, after you transmit a print job, print is available by changing the account in the displayed popup screen.

To display the popup notification screen, set the following.

- Install Popup Messenger in the client PC
- Select a checkbox for [Display Popup Screen] and [Select Account] in [Print Popup Settings] of the access profile



"Install Popup Messenger" (P.269)

Associate an account with a job without account specification

The user set to [Allow] in [Use without specifying account] in the access profile can use a device without specifying an account.

In operation without specifying an account, users can replace the job cost for an appropriate account after operation.

1. Select [Print/Job] > [Cost Management] > [Non Account Associated Job List] from the user screen menu.
2. Select your job and click [Associate].

Add Favourite Accounts

From the accounts the users can use, frequently used accounts can be set.

This setting enables the screen for selecting an account to display only favourite accounts so that the users can save the effort of searching or selecting the account from among many accounts.

A maximum of 10 favourite accounts can be added.



Note

The favourite accounts can be added from the account selection screen of the device.

1. Select [User/Service Settings] > [Cost Management] > [Favourite Account] from the menu on the user screen.
2. Click [Add].
3. Select the account you want to set as the favourite, and click [Apply].

Precautions for Cost Management Operation

When performing cost management by ApeosWare Management Suite, note the following.

- The cost management feature of ApeosWare Management Suite is a billing system based on the job log. The job log differs from the billing meter of the multifunction machine. Therefore, the amount billed by billing meter may be different from the amount that is processed for billing by ApeosWare Management Suite based on the job log.
- Implement settings that ApeosWare Management Suite can collect job logs appropriately from a device.
- If the job log collection process and the billing process based on the job log have stopped, it is recommended to set e-mail notification. Use the following procedure to configure the settings:
 - (1) Log in to the Management screen as an administrator.
 - (2) Select the menu on the Administrator screen in the order of [Service Settings] > [Server Monitoring Settings] > [Monitoring Settings] > [Service Settings].
Make sure that a check mark is placed for monitoring the services below.
 - ApeosWare Management Suite Core Service
 - ApeosWare Management Suite Multi Task Service
 - (3) Select the menu on the Administrator screen in the order of [Service Settings] > [Server Monitoring Settings] > [Notification Settings].

(4) Set [E-mail Notification] to [On].

(5) Set the notification e-mail address in [Add the following e-mail address to the Notification Address].

- When collecting job logs from a device, do not set “All job logs recorded in device” as collection targets. Job logs in a device are collected double and billing processing may be performed double.
- The cost management of ApeosWare Management Suite is not available with any unsupported devices as well as devices without hard disk drive (including the SSD).
For the models supporting the cost management feature, refer to our official website. (Refer to the first page of this guide for URL.)
- Perform the operation while preventing any “omission” of job log occurring depending on the device state.



Refer

Concerning omission → “Installation and Operation Guide”)

- Implement redundancy and periodic backup of the hard disks (including the SSD) of the ApeosWare Management Suite server and on-demand terminal. If a failure occurs in job log information, it can be recovered from the backup.
- If the hard disk (including the SSD) of a device fails, ApeosWare Management Suite cannot acquire job logs of the device, so they are not made as billing targets.
- If the board or hard disk drive (including the SSD) of a device is replaced, ApeosWare Management Suite cannot acquire job logs of the device, so they are not made as billing targets.
- If the power of a device is turned off while jobs are executed, ApeosWare Management Suite cannot acquire job logs of the device, so they are not made as billing targets.
- When different paper sizes or color and black & white are mixed in a job, the actual value of job cost can differ from the predicted value that is displayed prior to the execution of job.
- When [Force Stop When Minimum Balance is Reached] function is being used, the job cost estimated value displayed before the job execution may go under the value of [Minimum Balance] that was set.
- When [Force Stop When Minimum Balance is Reached] function is being used, printing may not be possible even when there is a balance sufficient for the job to be executed.



Note

In [Charge Calculation Settings] of cost management, when [Smaller Value of Estimated and Output Count] is set, printing is executed as long as balance is remaining.

- If the device and ApeosWare Management Suite server cannot communicate normally after a job execution, a delay may occur in balance confirmation processing.



Note

The final confirmation processing for the balance is performed at intervals set with [Collection Interval] of job log collection settings (item in device group settings).

- When [Force Stop When Minimum Balance is Reached] function is being used, the value may go under the value set in [Minimum Balance] if the device cannot communicate normally with ApeosWare Management Suite server after the job execution.

**Note**

After Print On Demand is canceled, it will take some time until the canceled charge is returned to the account in use.

As a result, if printing is attempted in succession while the [Force Stop When Minimum Balance is Reached] function is being used, you may not be able to print because of an insufficient balance.

When you wish to continue with printing, log in again to the device you are using and then execute printing.

By logging in again, the balance is updated to the balance before a print job was canceled.

- In “On demand print terminal + Billing system”, a job cost may be withdrawn at a predicted value from the billing system. If there is a difference between a predicted value and actual value, refund processing with cash cannot be performed.
- When a refund is generated such as when a job is canceled, the refund is made to either the [Allotted Balance] or [Top-Up Balance], whichever was used.
Refund processing is a process that starts when processing on the device is complete. For example, if the [Allotted Balance] becomes zero (0) when printing multiple print jobs at once, the charge of a device is deducted from the [Top-Up Balance]. If some jobs are canceled, the charge is deducted from [Top-Up Balance] even if [Allotted Balance] is not zero (0) as the canceled jobs are refunded to the [Allotted Balance].
- If you are using the card ID customization function for external authentication that is provided only in some countries, you cannot use cost management of ApeosWare Management Suite.

Confirming the Accounting Result

You can use the report function to view the result of setting and executing the process of accounting, such as replenishing the balance and doing accounting based on a prediction and then correcting it with actual usage, in order to check whether there is a difference in accounting and how much the difference is.

Viewing the cost management report

You can confirm the accounting result from the following report:

- In the administrator screen, go to [Report] > [Users / User Groups] > [Account Usage & Replenishment History (Cost Management Report)]
- In the user screen, go to [Report] > [Account Usage & Replenishment History]

**Refer**

“11 Job Log Accounting/Report”

Confirming the cost management report

This section provides an example of the cost management report. The following report is an example where print data is sent to device and then canceled in the device.

ApeosWare Management Suite **FUJIFILM**

Account Usage & Replenishment History (Cost Management Report)

Date Range: 29/04/2021 12:00 PM - 29/04/2021 12:35 PM
 Transaction Type: Copy, Print
 History Type: Service Usage (Exclude Canceled), Balance Replenishment

Transaction Date/Time	User ID	Account Name	Transaction Type	Performed By	Transaction Remarks	File name	Cost (¥)	Balance (¥)	Confirmed	ID
29/04/2021 12:33 PM		a2	Balance Replenishment	u1	Added balance is set in account creation		6000	6000	Confirmed	1
29/04/2021 12:33 PM		a2	Balance Replenishment	u1	Added balance is set in account creation		6000	6000	Confirmed	2

FUJIFILM Business Innovation Corp. 1/1 29/04/2021 6:02 PM

Check the following things.

- (1) Check that "Confirmed" is shown in the "Confirmed" column.
 If "Confirmed" is not shown even though a print process is finished (output is completed) in the device, there may be a problem in the ApeosWare Management Suite server or the device.
- (2) One process can be shown in two rows due to repayment, additional collection, etc. Check the association from the ID number in the Remarks column and the number in the ID column.
- (3) Check that charges for processes are correctly reflected in the account balance.
- (4) Check the result outputted from the device to see the paper size, whether it is printed in color or in black and white, and whether it is printed in one side or in both sides. On the basis of it, check the unit price with the administrator and confirm that a calculation is made with the correct price.
 Note that the unit price cannot be checked in a report.

If, as a result of checking, there is a problem, ask the administrator.

6 Download Management

Settings from a Web Browser

You can set the settings for the user and confirm them with a web browser. This section describes what you can do with each page.



Note

- Download Management is available only for devices used in Japan.
- The downloaded printer drivers is supported by only Japanese OS.
- Job Owner Setup is supported by only Japanese x86/x64 OS.

Pages	Descriptions
Files	Manages files and folders to be distributed to users.  Refer "Files" (P.241)
Printers	Manages print settings (Output Color, 2-Sided, etc.) of the printer to be distributed to users.  Refer "Printers" (P.243)
Settings	
Administrator Information	Sets the information of the administrator who installs printer drivers or software in place of the users who do not have the administrator permission.  Refer "Administrator Information" (P.245)
Print Settings Default Value	Sets default values of printing settings (Output color, 2-sided, etc.) for printers to add.  Refer "Print Settings Default Value" (P.246)
Header/Footer Default Value	Sets default values of the header and footer for printers to add.  Refer "Header/Footer Default Value" (P.247)

Files

How to Display

Select [Service Settings] > [Download Management] > [Files] from the menu on the administrator screen.

Page Summary

Manages files and folders to be distributed to users. Other than files, folders can be added.

The maximum capacity of the file/folder can be added is 4 GB.

The file/folder to be added needs to be located directly under the following folder.

{Folder of data storage directory}¥Data¥karaf¥etc¥Download¥DLFiles



Note

In default setting, {Folder of data storage directory} is "C:¥FUJIFILM¥ApeosWare MS".

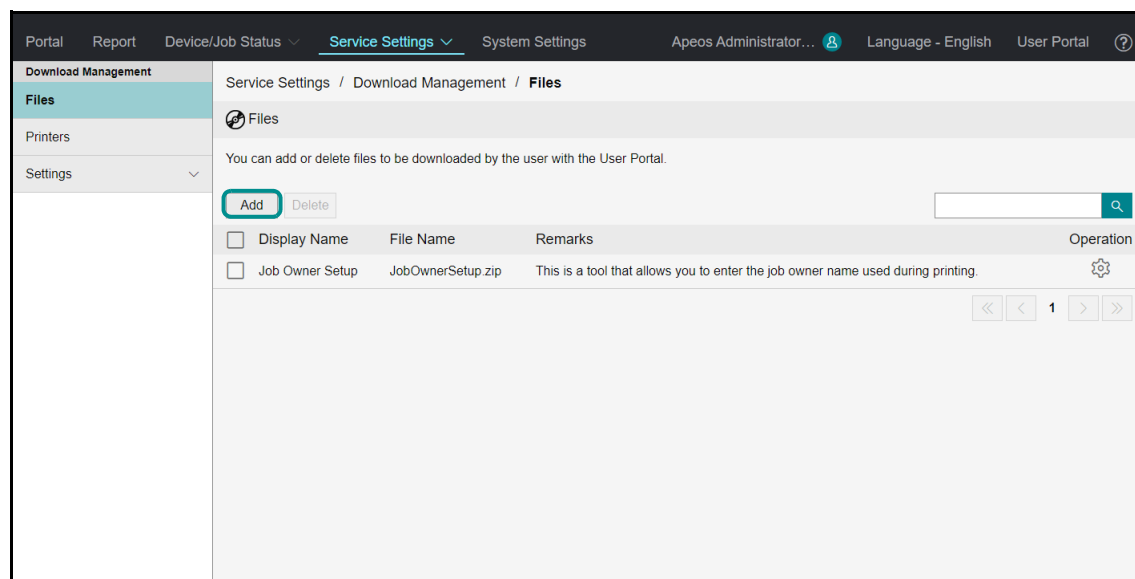
Following tools are registered by default.

- Job Owner Setup

Enables you to enter a job owner name when printing.

Adding Files

Click [Add].



[Display Name]

Enter the file name. Entered contents will be shown on the [File Download] page.

[File Name]

Enter the name of the file or the folder that stored directly under "DLFiles".



Note

Place the file or folder you wish to add to directly under the following folder.

{Folder of data storage directory}¥Data¥karaf¥etc¥Download¥DLFiles

In default setting, {Folder of data storage directory} is "C:¥FUJIFILM¥ApeosWare MS".

[Remarks]

As needed, enter the remarks.

[Executable File]

To execute the downloaded file automatically, specify the path of the file to execute and the argument of the command line.

Enter the path of the executable file which is relative to the stored location (DLFiles folder).

Example 1: To execute "SoftA.exe" stored directly under "DLFiles", specify as following.

File name	SoftA.exe
Executable file name	SoftA.exe

Example 2: To execute "SoftB.exe" stored in the "SubFolder" folder that is located under "DLFiles", specify as following.

File name	SubFolder
Executable file name	SubFolder\SoftB.exe

Example 3: To execute "SoftA.exe" located directly under "DLFiles" by specifying the argument "-a", specify as following.

File name	SoftA.exe
Executable file name	SoftA.exe -a

Be sure to enter this item when [Run with Administrator Permissions] is checked.

[Runtime Setting]

Specifies whose permission is used to execute the downloaded file automatically.

If you check [Run with Administrator Permissions], the permission of the user on the [Settings] > [Administrator Information] is used to execute the file.

Uncheck the mark to execute the file with the permission of the user who downloaded the file.

Checking File Information

Click  in the file list and select [Properties].

You can display and edit the content configured for the file. You can edit the same items as the features configured in "Adding Files" (P.242).

Deleting files

Click  in the file list and select [Delete].

This operation deletes the file from the list of files, but the file still remains the stored location. Delete the file in the "DLFiles" folder as well when necessary.

Printers

How to Display

Select [Service Settings] > [Download Management] > [Printers] from the menu on the administrator screen.

Page Summary

Manages print settings of the printer to be distributed to users.

The information of the device registered on ApeosWare Management Suite is used. Therefore add devices to [Service Settings] > [Device Management] > [Device List] in advance.

Also, printer drivers are set or updated by Update Service. Add the printer driver that is supported by the printer with Update Service in advance.

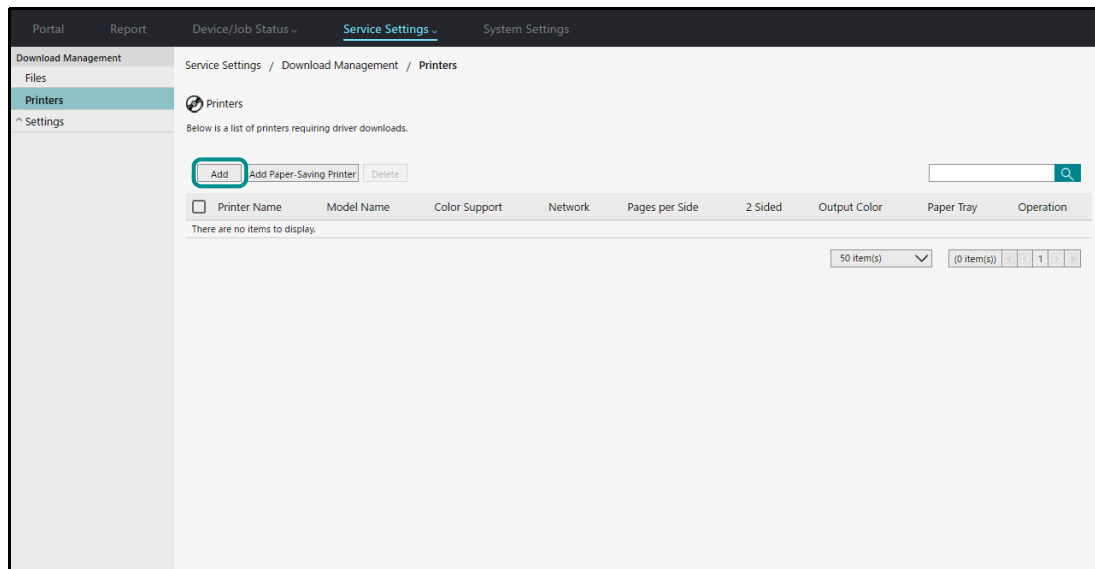


Note

Printer drivers cannot be distributed by solely adding printers. Make sure to add the drivers to Update Service.

Add a Printer

Click [Add].



(1) Select a device

Click one printer you wish to add, and then click [Next].

(2) Basic settings

Configure basic settings for the printer such as the printer name and the driver type, and then click [Next].

(3) Print settings

Set [Pages per Side], [2 Sided], [Output Color], and [Paper Tray] individually, and then click [Next]. When [Default] is selected, the value set on the [Print Settings Default Value] page is set on the printer.

(4) Header/footer settings

Set the contents for headers and footers to be printed, and then click [Next]. When [Default] is selected, the value set on the [Header/Footer Default Value] page is set on the printer.

(5) Overview

After you check the configured settings, clicking [Save] will add the printer.

You can click [Edit] for each item to change the settings.

Add printers for saving paper

Click [Add Paper-Saving Printer]. The following three types of printers whose settings include the paper saving settings are automatically added.

[Printer Name]	Setting value of [Pages per Side]	Setting value of [2 Sided]
2 up - {IP address/Host name}	2 Pages (Right or Down)	Default
2-Sided - {IP address/Host name}	Default	2 Sided, Flip on Long Edge
2 up 2-Sided - {IP address/Host name}	2 Pages (Right or Down)	2 Sided, Flip on Long Edge

Checking User Information

Click the printer name link or  in the printer list, and then select [Properties].

You can display and edit the content configured for the printer. You can edit the same items as the features configured in "Add a Printer" (P.244).

Delete printers

Click  in the printer list and select [Delete].

Administrator Information

How to Display

Select [Service Settings] > [Download Management] > [Settings] > [Administrator Information] from the menu on the administrator screen.

Page Summary

Sets information of the administrator to execute installation by proxy. This information is used when the user without the administrator permission installs software or printer drivers.

When downloading the files include an executable file, and if the settings of [Run with Administrator Permissions] is enabled, the administrator permission set here is used for the installation.

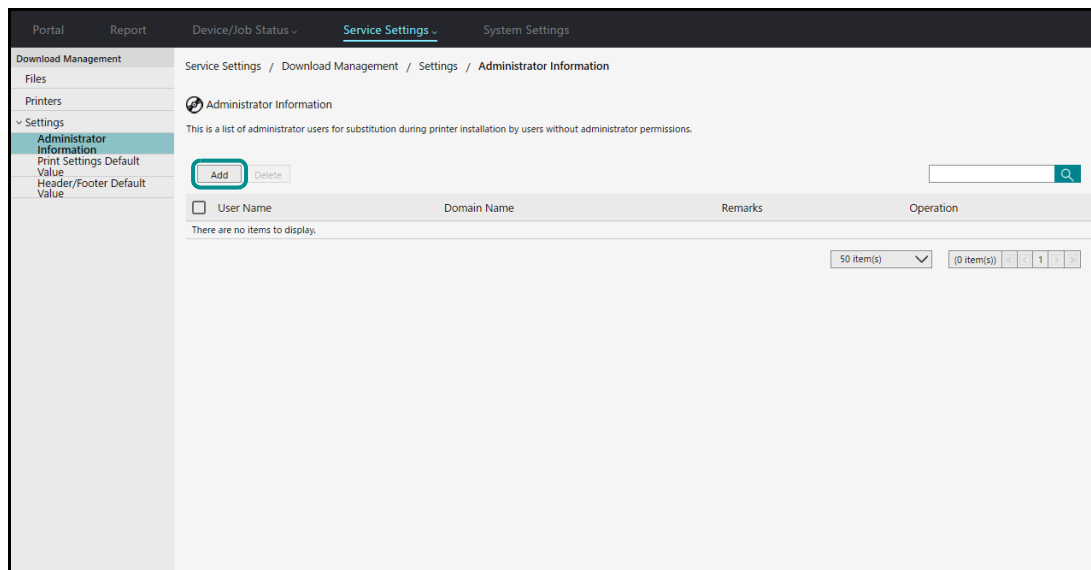
When downloading printer drivers, if the operating user does not have an administrator permission, the administrator permission set here is used to install the drivers.

Multiple administrator information can be registered.

When two or more administrator information are registered, install the software and printer driver by selecting the administrator information having the administrator authority for the distribution target client PC.

Add Administrators

Click [Add] and configure the following items, and then click [OK].



[User Name]

- When the PC of distribution target is joined the same domain, specify a user joined the same domain and having the administrator permission.
- When the PC of distribution target is not joined the same domain, specify a user registered on the client PC and having the administrator permission.

[Domain Name or Computer Name]

- When the PC of the distribution target is joined the domain, specify the domain name.
- When the PC of the distribution target is not joined the domain, specify the computer name of the client PC.

[Password]

Specify the password of the user specified on [User Name].

[Remarks]

As needed, enter the remarks.

Checking Administrator Information

Click  in the administrator list and select [Properties].

You can display and edit the content configured for the administrator. You can edit the same items as the features configured in “Add Administrators” (P.246).

Delete Administrators

Click  in the administrator list and select [Delete].

Print Settings Default Value

How to Display

Select [Service Settings] > [Download Management] > [Settings] > [Print Settings Default Value] from the menu on the administrator screen.

Page Summary

Configure the default values for printer settings, and then click [Save]. The values set here are applied as default when you select [Default] on [Basic Settings] on the [Add Printer] screen.

However, the following items cannot be set when printers are added. Values set here are applied to all printers.

[Job Owner Name]

Selects how to specify job owner names.

[Alternate Name of Job Owner Name]

Set the message shown on the screen when a job owner name is needed to enter during the download process of the printer.

Example

When [Alternate Name of Job Owner Name] is set to "Project Code", the following message is shown on the screen to enter the job owner name.

For Job Owner Name, display the value that is to be used as <Project Code>.



Note

In the operation of downloading printers, enter the job owner name in the following cases.

- [Enter Job Owner Name] is specified on [Job Owner Name].
- [Use User Organization] is specified on [Job Owner Name] but the organization information is not set for the user. Or the organization information exceeds the number of characters of the entry rule for job owner names.
- [Use User ID] is specified on [Job Owner Name] but the value of the user ID exceeds the number of characters of the entry rule for job owner names.

Header/Footer Default Value

How to Display

Select [Service Settings] > [Download Management] > [Settings] > [Header/Footer Default Value] from the menu on the administrator screen.

Page Summary

Set the default value for the header and the footer, and then click [Save]. The value set here is applied as default when you select [Default] on [Header/Footer Settings] on the [Add Printer] screen.

Portal Report Device/Job Status Service Settings System Settings

Download Management / Settings / Header/Footer Default Value

Header/Footer Default Value

You can set the header/footer default value. It will become the default value for all registered printers.

Item	Font
Login Name	Font Name
Job Owner Name/User ID	Size
Document Name	Color
Page Number	Bold
Date	Italic
Time	

Save Cancel

Download of File/Printer

Describes the procedure for downloading of the software and the printer drivers for distribution from the server.



Note

- Download Management is available only for devices used in Japan.
- The downloaded printer drivers is supported by only Japanese OS.
- Job Owner Setup is supported by only Japanese x86/x64 OS.

Download files

Download the file for distribution on the client PC.



Note

When using a web browser other than Internet Explorer, the file names that contain semicolons (;) or double-byte characters are displayed as "DVPUSerDownloadFile" on the [File Download] screen. Also if the extensions contain semicolons (;) or double-byte characters, the file names are displayed without extension.

1. Access ApeosWare Management Suite with a web browser and log in.
When administrator permission is set to the user, logging in will cause the administrator screen to appear. Select [User Portal] on the header and display the user screen.
2. Select [User/Service Settings] > [Download Management] > [File Download] from the menu on the user screen.
3. Click of the file to be downloaded, and select [Download].
Downloading of the file starts.
4. When the downloaded file is set as [Executable File], the message to confirm the execution is

displayed. Execute the file by following the message.

Installation of printer drivers

Install the printer driver for distribution on the client PC.

1. Access ApeosWare Management Suite with a web browser and log in.
 2. When administrator permission is set to the user, logging in will cause the administrator screen to appear. Select [User Portal] on the header and display the user screen.
 3. Select [User/Service Settings] > [Download Management] > [Printer Download] from the menu on the user screen.
 4. Check the printer driver you want to download and click [Download].
The [Download Setup File] page is displayed.
 5. Set the following items.
 - [Client Operating System]
Select OS to be downloaded.
 - [Job Owner Name]
This may be displayed or not displayed depending on the settings. When displayed, enter the job owner name.
-  **Refer**
"Print Settings Default Value" (P.246)
6. Click [Download].
Downloading of the setup file starts.
 7. Execute the downloaded setup file. When the message to confirm the execution is displayed, execute the file by following the message.

7 Print Management and Operations

Settings and Operation from Web Browser

You can set print settings and confirm and execute a print job from web browser.
This section describes what you can do with each page.

Types of Pages	Descriptions
Print Queue List	Displays the print queue list registered in the print server. Register and set the print queue.  Refer "Print Queue List" (P.253)
Print Job List	Displays print job lists. You can confirm the print job properties, remove the hold and cancel the job, etc.  Refer "Print Job List" (P.260)
Print Rule List	Displays the print rule list already created. You can create and change print rules.  Refer "Print Rule List" (P.258)
Print Settings	You can set print settings.  Refer "Print Settings" (P.261)
Print Server List	The print server list already created is displayed. You can create, edit and delete print servers.  Refer "Print Server List" (P.252)
Mode Schedule List	Displays the list of print mode schedules. You can create, edit, and delete the print mode schedule.  Refer "Mode Schedule List" (P.266)

Side Menu Configuration

A side menu configuration varies depending on the print server configuration.

- All-in-One Configuration

The same configuration as the list above because there is only one print server.

- Distributed Configuration with the Print Application Server Separated

The print queue list, the print job list, the print rule list and the print settings in each print sever are displayed.

- Distributed Configuration with the Print Input/Output Server Separated

The print queue list in each print server is displayed. The print job list, the print rule list and the print settings are in common in all the servers.

Preparations

Device Settings and Registration

Confirm the LPD port is enabled on the device associated with the print queue.

To create a print queue associated with the device already registered to ApeosWare Management Suite, register the device information in advance.



Refer

"3 Device Management" (P.75)

User Registration

To ApeosWare Management Suite, register the user who uses the printing features, and set the access profile.

To use Guest Print, attaching the user to the user group for Guest Print, create the user for Guest Print. Among the users of guest print, you can select users and permit Web Print only.

To manage the cost, creating the account, associate it with the user or the user group. Moreover, creating the price list, associate it with the device or the account.



Note

A user group of guest print "Guest User Group" is automatically created when ApeosWare Management Suite is installed. The group name may be changed.



Refer

- "4 User Management" (P.126)
- "User Screen" (P.33)
- "5 Cost Management" (P.201)

Disabling User Account Control

When a print input/output server is installed, to specify a local user other than the built-in account (Administrator) for [User Name] and [Password] specified in "Creating a Print Server" (P.252) to be described later, user account control must be disabled.

To disable the user account control, perform following steps on the PC of print input/output server.



Note

The following process is to be operated on Windows. For the details, refer to the manual or help of Windows.

- (1) Display [Local Security Policy] from Server Manager.
- (2) Select [Security Settings] > [Local Policies] > [Security Options].
- (3) Double-click [User Account Control: Run all administrators in Admin Approval Mode] displayed in the list on the right side of the [Security Options] screen.
- (4) Select [Disabled] displayed on the [Local Security Setting] tab, and then click [OK].
- (5) Reboot the PC.

Print Server List

How to Display

Select [Service Settings] > [Print Management] > [Print Server List] on the administrator screen.

Page Summary

The print server list already created is displayed. You can create and delete a print servers, and edit the properties.



Note

- In the case of the All-in-One Configuration and Distributed Configuration with the Print Input/Output Server Separated, first add the main server. Note that you cannot delete the added main server. When using the Distributed Configuration with the Print Input/Output Server Separated, register the print server in the list of print servers even if you are not using the main server as the Print Input/Output Server.
- Create the print queue to the print server.

Creating a Print Server

Click [Add Server].

[Display Name]

Set the display name of the print server.

[IP Address/Host Name]

Select the IP address of the print server or the FQDN host name.

[User Name], [Password]

Enter the license activation information to access the print server.



Note

- Enter the information of the user who belongs to the administrator group of the print server.
- In case a print input/output server is installed, when specifying a local user other than built-in account (Administrator) as the user to access the server, the user account control is required to be disabled. For details, refer to "Disabling User Account Control" (P.251).

[Domain]

Enter the domain name to which the user entered on [User Name] belongs.

[Backup Server]

Set the IP address of the backup server.



Note

- The backup server can be set only by the print input/output configuration.
- Between two servers, a mutual server cannot be specified as a backup server.
- In the following cases, no job is copied to a backup server.
- If server is down during execution of backup processing
- If backup server cannot be communicated
- To a print server set to a backup server, a job requested to the print server set in [IP Address/Host Name] is copied. Even if the print server of the copy source is down, the job remains in the backup server, so print processing is executed.

Checking Print Server Information

Click the print server name link or  in the print server list, and then select [Properties].

You can display and edit the content configured for the print server. You can edit the same items as with the content configured in “Creating a Print Server” (P.252).

Deleting a Print Server

Select a checkbox for the print server you wish to delete, and then click [Delete].



Note

In the case with All-in-one Configuration Setup, the print server cannot be deleted.

Print Queue List

How to Display

Select [Service Settings] > [Print Management] > [Print Server List] on the administrator screen, and then select [Print Queue List] from the side menu.

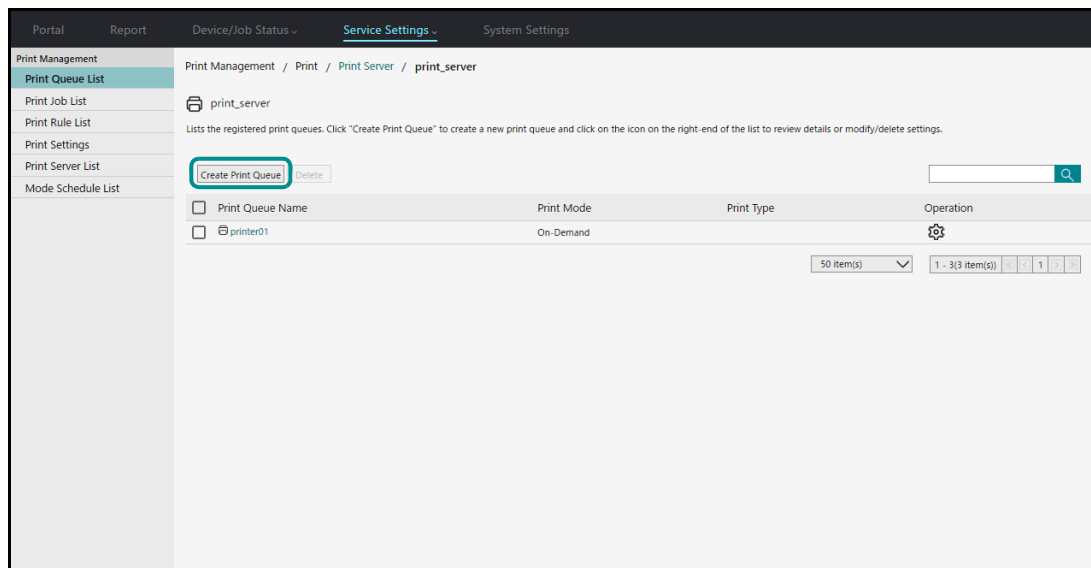
Page Summary

The print queue list already created in the print server is displayed. You can confirm the print mode and the print type of the print queue.

You can create a new print queue and change the settings of the print queue already created.

Creating a Print Queue

Click [Create Print Queue].



(1) Details of Print Queue

Specify the following item, and then click [Next].

[Print Queue]

Select one from the Windows shared printers set to the print server, or select [Create New Print Queue].

When selecting [Create New Print Queue], enter the new print queue name.



Note

The Windows shared printer already used in another print queue is not displayed on the list.

[Print Mode]

Select the print mode to set to the print queue.

When setting a print mode schedule, the time period that is not defined in the schedule is set to the print mode selected here.



Refer

About print mode→“Installation and Operation Guide”

[Schedule]

Select the print mode schedule for the printer queue from the drop-down list box. If you do not specify the print mode schedule, select [Always Default Print Mode].

[Print Type]

Select a print type. You can select multiple print types.

- [Print E-mail]

You can set [Print E-mail] to only one print queue. If [Print E-mail] has been already set to another print queue, you cannot select it.

When selecting this, set the email address to print the email received, and the user ID and the password to access the POP3 server.

When using e-mail printing, if [Modern Authentication] is set to [On] in [System Settings] >

[Common Settings] > [Network Settings], [Modern Authentication] will be displayed in addition to the e-mail address and user name.

In these cases, enter the user that matches the "Exchange Online" or "Gmail" setting selected in "Network Settings" for the e-mail address and user name, then click [Modern Authentication].

If authentication processing has been performed, this will change from [Authentication Required] to [Authenticated].

Furthermore, if the receiving e-mail address or user name has been changed, performing authentication again will be required.

If this is not authenticated, creation of a logical printer will fail.



"[Modern Authentication]" (P.41)

- [Web Print]
- [Mobile Print]

When selecting this, you can set [Direct Print with IP Address/Host Name Specification]. This settings are enabled only when the following both the requirements are satisfied.

- The print mode is [Direct Print].
- This feature is not enabled in another print queue.

The print queue whose [Direct Print with IP Address/Host Name Specification] is checked is associated with all the devices.



Note

When the print mode is [Direct Print] and you are issuing a printing command to a print queue that is associated with multiple devices, you cannot specify the device that performs printing. In order to specify a device for printing, follow the method below.

- Prepare a print queue that is associated beforehand with the device used for printing whose print mode is on-demand printing. Then, issue a printing command to this print queue when printing, and output the print job by selecting the job on the screen of the device in question.
- When using ApeosWare MS Mobile 2, output the print job by reading the QR code of the device or by specifying the device group or device.

[Limit to IP Address]

Check this when the destination to notify the popup message is limited to the IP address issued the print job.

[Windows Port Name]

When specifying Window port name, check [Specify] and enter the port name.

[Receiving LPR Queue Name]

When using the print queue as a LPR queue, check [On] and set the queue name and the character set used. When setting multiple print queues, click the  icon, and then add the LPR queue.



Note

Creating multiple LPR queues with different character sets in one print queue allows receiving the print jobs sent from various language environments in the same print queue.

Standard settings for each client OS is as the followings.

- Japanese Windows: Japanese (Shift JIS/CP932)
- Simplified Chinese Windows: Simplified Chinese (GB18030)
- Traditional Chinese Windows: Traditional Chinese (CP950)
- Korean Windows: Korean (CP949)

- English Windows: English (ISO8859-1/CP1252)
- For Mac OS, Fedora, Vine Linux, and Red Hat Enterprise Linux: Unicode (UTF-8)

[Sending LPR Queue Name]

When specifying a name of the LPR queue of the device that sends print jobs, check [On] and enter the queue name.

When it is not enabled, the job is sent to the queue named "AUTO".

[IPP Port]

Select this checkbox to receive jobs on the logical printer with the IPP/IPPS protocol.

When using IPPS, select the checkbox for [Enable] of [IPP Communication Encryption].

- [BASIC Authentication]

Only displayed if the [Enable] check box for [IPP Port] and the [Enable] check box for [IPP Communication Encryption] are selected.

When using IPPS protocol, user authentication is performed.

- [Print from iOS Device]

Only displayed if the [Enable] check box for [IPP Port], the [Enable] check box and the [BASIC Authentication] check box for [IPP Communication Encryption] are selected.

Select when printing from an iOS terminal.



Note

- IPP printers are shown as selectable printers when printing from iOS. For this to occur, the customer's network infrastructure must support mDNS.
- IPP printers perform user authentication when printing from iOS, and print jobs are issued for authorized ApeosWare Management Suite users. Operations after print jobs are issued are the same as for other print jobs.
- When Direct Print is specified in Print Mode, IPP printers will print directly.
- When On Demand Print is specified in Print Mode, IPP printers will store the job, and print when it is released.
- If the [Print from iOS Device] check box is selected, the [Page Description Language Default Value] is set to [Do Not Detect], and the setting cannot be changed. Note that you will be unable to use some functions.

[Page Description Language Default Value]

Select from the following options whether to recognize page description language for a job received with the logical printer.

- Auto Recognize

Automatically analyzes the content of print jobs to determine the page description language.

The job is printed provided that the determined page description language is supported by ApeosWare Management Suite.

- Do Not Detect

Does not determine the page description language. Print jobs in page description languages not supported by ApeosWare Management Suite can also be printed.

However, when [Do Not Detect] is selected, no information can be acquired from print jobs, and thus costs will be displayed in accordance with the values set in [Job Information Complementary Paramete]. Additionally, when you display a job on the panel of a multi-function printer using on-demand printing, a warning mark will be displayed. Several features are also unavailable. For details on unavailable features, refer to "Auto Judgment Page Language Description" (P.282).

[Job Analysis Method]

When the license of “Additional OS Parser Option” is activated, methods of analyzing print jobs can be selectable.

Using Additional OS Parser Option enables to change the settings of Output Color, 1 Sided/2 Sided, and Paper Size for PostScript print jobs sent from clients whose OS is Linux or Mac OS.

When the option is not used for analyzing print jobs, select [Standard Feature].



Note

Additional OS Parser Option is available only in Japan.

[Print Server Linkage]

Select the checkbox for [Enabled] to link with the GX Print Server.

If you enable print server linkage, [Page Description Language Default Value] will be set to [Do Not Detect] and cannot be changed. Additionally, setting of the Sending LPR Queue Name will not be possible, and the Sending LPR Queue Name set in the device will be used.

(2) Associate With Devices/Device Groups

For the print queue to be created, set the association with the device or the device group, and then click [Next]. You need to make an association with either the device or the device group.

[Associate With Device Groups]

[On]

When you associate the print queue with the device group, select [On].

With the checkbox for [Associate All Device Groups] is selected, the print queue can use all the devices affiliated with device groups.

To associate the print queue with a specific device group, uncheck the checkbox for [Associate All Device Groups], and then select the device group according to the following procedure.



Note

When you have selected the checkbox for [Associate All Device Groups], the setting is also applied to devices registered thereafter.

(1) Click [Add] to display the [Device Group] dialog box.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all device groups, click [Add All].
- To narrow down from the device groups displayed in [Associate with Device Groups], enter a part of group name you want to search into , and then press <Enter>.
- To delete an association with a specific device group, from [Associate with Devices], click [Delete] or [Delete All].

[Off]

Select when you do not associate device groups.

[Associate With Devices]

[On]

When you associate the print queue with devices, select [On].

When the checkbox for [Associate All Devices] is selected, the print queue can use all the devices.

To associate the print queue with a specific device, uncheck the checkbox for [Associate All Devices], and then select the device according to the following procedure.



Note

When you have selected the checkbox for [Associate All Device Groups], the setting is also applied to devices registered thereafter.

(1) Click [Add] to display the [Device] dialog box.



Note

Clicking [Add] displays the list of devices registered in ApeosWare Management Suite.

(2) Select the checkbox for the device that you wish to add, and then click [Add].



Note

- To add all devices, click [Add All].
- To delete an association with a specific device, from [Associate with Devices], click [Delete] or [Delete All].

[Off]

Select when you do not associate devices.

(3) Confirm settings

After you check the configured settings, clicking [Save] will add the print queue.

You can click [Edit] for each item to change the settings.

Checking Associated Devices/Device Groups

Clicking the print queue name link displays the list of devices/device groups associated with the print queue.

By clicking [Edit], you can display and edit the content configured for the print queue. You can edit the same items as with the function configured in “Creating a Print Queue” (P.254) except for the print queue name.

Checking Print Queue Information

Click  in the print queue list and select [Properties].

You can display and edit the content configured for the print queue. You can edit the same items as the features configured in “Creating a Print Queue” (P.254).

Checking Print Queue Job

Click  in the print queue list and select [Display Job].

You can display the print job list of the print queue. The same items as in “Print Job List” (P.260) are displayed.

Deleting a Print Queue

Click  in the print queue list and select [Delete].

Print Rule List

How to Display

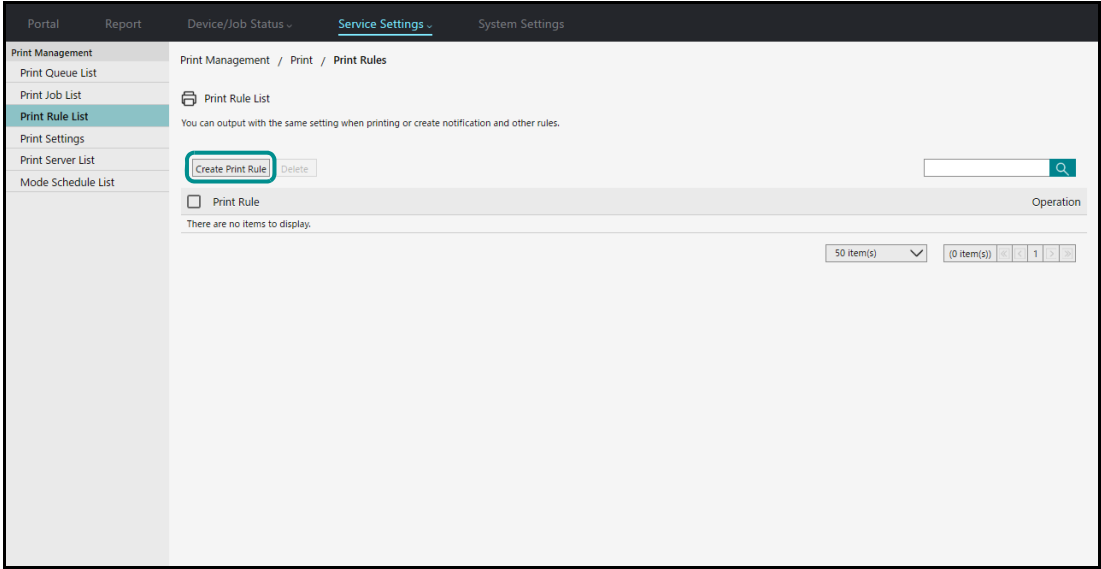
Select [Service Settings] > [Print Management] > [Print Rule List] on the administrator screen.

Page Summary

The print rule list is displayed.
You can create a new print queue and change the settings of the print queue already created.

Creating Print Rule

Click [Create Print Rule]. The main settings are as shown below.



[Rule Name], [Print Rule Description]

Set the rule name and the descriptions.

[Print Queue]

Select the print queue to be associated with the rule. You can associate multiple print queue with to one rule.

Click [Edit], and [Associate With Print Queue] is displayed.

Check [Associate With All Print Queues] or select one from the print queue displayed by clicking [Add].

[Delete Duplicate Job]

Select this to cancel the received job that is duplicate.

[Specify Process Conditions]

Select this when specifying the condition and process. When selected, set the condition and process to apply on [Rule Condition Settings].

[Rule Condition Settings]

Select [Properties], [Condition], and [Value]. When adding a condition, click  and select [And], [Or], or [And Not] on [Operator].

[Rule Action Settings]

Select how the print job satisfying the requirements will be processed.

When [Specify Print Settings] is selected, select the process to apply from [Force Black & White], [Force 2 Sided], and [Print Header/Footer].

When [Move to Print Queue] is selected, click [Edit], and then select the print queue to which the print job is transferred.

Checking Print Rule Information

Click the print rule name link or  in the print rule list, and then select [Properties].

You can display and edit the content configured for the print rule. You can edit the same items as the features configured in “Creating Print Rule” (P.259).

Copying Print Rule

Click  in the print rule list and select [Copy].

You can copy the settings of a print rule, and create a new print rule. When copying, you can edit the setting items. You can edit the same items as the features configured in “Creating Print Rule” (P.259).

Deleting Print Rule

Click  in the print rule list and select [Delete].

Print Job List

How to Display

Select [Device/Job Status] > [Print Job Status] > [Print Job Status] from the menu on the administrator screen.



Note

The following ways enable you to display the list.

- Select the menu displayed on [Service Settings] > [Print Management] on the administrator screen, and then select [Print Job List] from the side menu.
- Select [Print/Job] > [My Jobs] > [Print Job List] on the user screen.

Page Summary

Displays print job lists.

On the administrator screen, the print jobs executed by all the users display.

On the administrator screen, the following print jobs are displayed.

- The print job submitted by the login user
- The print job executed with the alternate user ID for the login user
- The print job submitted by [Delegate Users] set to the login user

On Print Job List, you can perform the following operations to the print job.

- [Remove On Hold]

Removes the hold of the print job being held in Guest Print or waiting for the process in Popup Notification.

- [Cancel]

Cancels the print job.



Note

On Print On Demand, when the user cancels printing, the print job return to on-hold status. To resume printing, remove the hold.

You can remove the hold of the print job or cancel the job.

Select the job type to be displayed.

Select the job status to be displayed.

The screenshot shows the 'Print Job List' page in a web application. The top navigation bar includes 'Portal', 'Report', 'Device/Job Status', 'Service Settings', and 'System Settings'. The left sidebar lists 'Print Management', 'Print Queue List', 'Print Job List' (highlighted), 'Print Rule List', 'Print Settings', 'Print Server List', and 'Mode Schedule List'. The main content area shows the breadcrumb 'Print Management / Print / Print Job' and a sub-header 'Print Job List' with the description 'Display print job status. Release or cancel print job.' Below this are three buttons: 'Remove On Hold', 'Cancel', and 'View'. To the right of these buttons are two dropdown menus: 'Job Type' set to 'All' and 'Job Status' set to 'Receiving in Progress'. A search bar with a magnifying glass icon and an 'Advanced Search' button is also present. Below the search bar is a table header with columns: 'Job Name', 'Job Type', 'Guest Print ID', 'User Name', 'Charge (¥)', 'Date/Time Created', 'Job Status', 'Output Device', and 'Operation'. The table body is empty, displaying 'There are no items to display.' At the bottom right, there are pagination controls showing '50 item(s)' and a page indicator '1'.

[Guest Print ID]

The ID issued when the user executes Guest Print is displayed.



Note

If administrator's permissions are required on Guest Print, removing the hold on the job list by the administrator enables the user to print. Search the print job whose on-hold status is removed by Guest Print ID.

Confirm Print Job Properties

Click  and select [Properties] or click the job name link.

Search Print Job

Enter the character string in the search box and click . The print job which matches partially the character strings entered with the job name is searched.

To search the job setting detailed requirements, click [Advanced Search].

You can search the print job with the user name and the job type as a requirement. To specify multiple requirements, select any of [And], [Or] and [And Not] on [Operator].

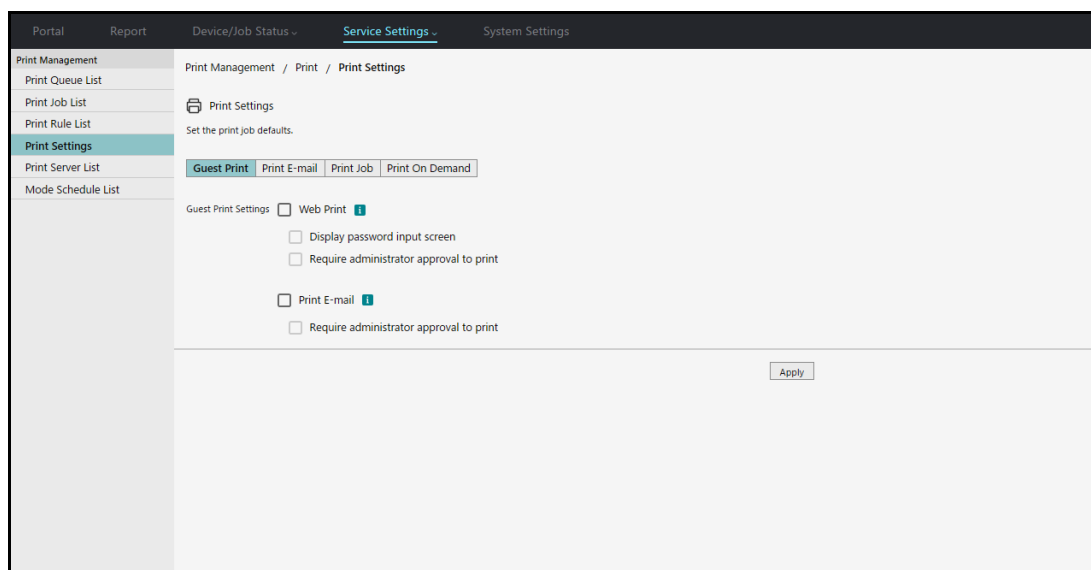
Print Settings

How to Display

Select [Service Settings] > [Print Management] > [Print Settings] on the administrator screen.

Page Summary

You can set print settings.



[Guest Print] tab

[Web Print]

To use Guest Print feature using a web browser, check here.

- Display password input screen

If you require the user executing the print job to enter the password, check here.

- Require administrator approval to print

In order to make an administrator's approval to be required prior to printing, select the checkbox.

When set, the user will be required to obtain an administrator's approval before removing the hold of a print job.



Note

- The approval of administrator is necessary when you wish to manage the guest print cost.
- Among the users of guest print, you can select users and permit Web Print only.

[Print E-mail]

To print the email you sent with Guest Print, check here.

Set whether administrator's permissions are required, as well as Web Print.

[Print E-mail] tab



Refer

Settings for sending email → "Network Settings" (P.40)

[Print Attachment Only]

To print only the attached file without printing the mail body, check [Enabled].

[E-mail Address of Sender]

Set the sender's email address of the result mail.

[Polling Interval]

Set the interval to receive an email from the POP3 server in minutes.

[Message Language]

Select the language of the subject or the body of the result mail.



Note

The default is the language selected on ApeosWare Management Suite. You can change only the language of the result mail to another language.

[E-mail Address of Spam Mail]

Enter the email address judged to be spam. To specify multiple email addresses, click and add them.

If the sender's address of email to be printed partially matches the character string specified here, it is judged to be a spam. Not case sensitive.

For example, when you specify "sample.com" in [E-mail Address of Spam Mail], all the email addresses including "sample.com" are judged to be spam.

[Guest Print User]

To execute Guest Print using Print E-mail, set a user ID to be the print job owner. You can set only one user ID.

It can be set only if a check mark is attached to [Print E-mail] in the [Guest Print] tab.

[Print Job] tab

[Job Validity Period]

You can set the validity period for the print job.



Note

The validity period of print jobs is the maximum time that the job can remain in the "On Hold" and "Standby" status. If the period in "On Hold" and "Standby" gets longer than the validity period, the print job is canceled.

[Job History Retention Period]

Specify the period until the print job history is automatically deleted after the print job is completed or canceled.

[Print Job Timeout]

When the print job receiving process is not completed, specify after how long time the job will be automatically canceled.

[Select User Print Job]

Select information to determine which user's print job is accepted by the logical printer.

In on-demand printing, print jobs sent by users are retrieved and displayed in a list.

Information	Descriptions
User name	Is the user name used when the user executing the print job logs on to the client PC. When a Windows shared printer is used to print, it is the user name accessing the printer.
Job Owner Name	Specify this with a printer driver etc. in executing a print job.

When [Job Owner Name or User Name (By Job Owner Name)] is selected, the job is searched by the job owner name. If the job owner name is not set, it is searched by the user name.

To search by the user name, it is required that the ApeosWare Management Suite user ID match with the logon name of the PC which is used to execute the print job.

When [BASIC Authentication] is selected in the logical printer, print jobs for which the user name and job owner name have not been set use the BASIC Authentication user ID.



Note

When printing from an iOS terminal, the user ID must be specified in BASIC Authentication.



Refer

[IPP Port] in "Create Logical Printer" > [BASIC Authentication](P.256)

[Save Print Data to File]

You can output the print data to a file as necessary, such as when you resolve the problem occurring during printing with ApeosWare Management Suite.

When [Allow] is specified, the print data is output to the following folders on the print server.

{Data Storage Folder}\Data\Temp\Spool\OutputPDLFile

Specify the data storage folder when installing the program. If default setting is not changed, "C:\FUJIFILM\ApeosWare MS" is applied.



Note

If you continue using it while the setting remains set to [Allow], the print data is continued outputting. We recommend that you reset the output file to [Disallow] after retrieving the printing data you need.

[Action When No Paper Supplied]

Set whether to continue Instruct To Print even if there is no remaining paper of the device.

[Display Details/Hide Details]

Clicking [Display Details] will display [Unregistered User ID Print], [Job Handling in Print Application Server (Distributed Configuration)] and [Job Information Complementary Parameter].

[Unregistered User ID Print]

Select whether to permit a print by a user not registered. When permitted, Print On Demand is available without the user registered.

If [Yes] is selected, the print is permitted under predetermined conditions.

If [No] is selected, an error message is displayed and the print is not permitted.



Note

When [Yes] is selected, you can output the job from the distributed server even if the main server goes down in the distributed configuration.

[Job Handling in Print Application Server (Distributed Configuration)]

With the print application server in a distributed configuration, select whether to print all jobs or pause when the main server is down.



Note

If pause is not selected, when the main server goes down in a distributed configuration, jobs may be printed without approval or masking.

[Job Information Complementary Parameter]

If a paper size and page information per copy cannot be detected, set a parameter applied to the print job.

- [Paper Size]
Select a paper size.
- [Color Delivered per Set]

Set the number of color sheets per set.

- [Color Impressions per Set]

Set the total impressions of color domains per set.

- [Black Delivered per Set]

Set the number of monochrome sheets per set.

- [Black Impressions per Set]

Set the total impressions of monochrome domains per set.

- [Quantity]

Set a print quantity.

[Print On Demand] tab

Set Print On Demand settings.

[Job Timeout]

When the print job is not executed even after removing the hold of the print job, specify after how long time the job will be automatically canceled.

[Check Balance When Job Received]

Select whether to check the balance when [Print] is clicked in the Print On Demand popup screen.

- [Off]

If the [Display Popup Screen] checkbox is selected in the access profile, [Print Details] will be displayed, and pressing [Print] will put this on hold.

- [On]

If the [Display Popup Screen] checkbox is selected in the access profile, [Print Details] will be displayed, with a warning message displayed with printing not being possible. Change to an account with sufficient balance, and press [Print] to hold.



Note

- To display the popup notification screen, you need to install Popup Messenger on the client PC.
- If the [Display Popup Screen] checkbox is not selected in the access profile settings, this will be held regardless of the [Check Balance When Job Received] setting.



Refer

- Installation of Popup Messenger → "Install Popup Messenger" (P.269)
- Access Profile Settings → "[Print Popup Settings]" (P.145)

[Print With List Settings]

- [Information to be used for the Job Display Name]

When the display name for Print On Demand is generated, select what information is used.

- [Header Text to be Deleted]

When the display name for Print On Demand is generated, set the character string to be deleted. If the character string set here is included in the beginnings of the print job, it is deleted and the display name is generated.



Note

For example, if the application name executing the print is put on the beginning of the print job name, specify the application. Deleting the application name allows being generated a display name identified easily on the control panel.

- [Job Display Order (Date/Time Received)]

Select the order displayed on the print job list.

- [Maximum Jobs Displayed]

Select the maximum number of jobs displayed on the print job list.

[Print Without List Settings]

- [Delete Canceled Print Job]

When the print job canceled, select whether to delete the front job (on printing job). When the job is not deleted, it becomes on hold status that you can resume the print job.

- [Print Job With Restrictions]

“Job With Restrictions” is a print job sent to the device not supporting the feature specified. (e.g., when the print job specified Folding or Punch Hole is sent to the device without a finisher.)

When printing, the feature not supported is ignored.

- [Max Number of Jobs for Printing]

Set the maximum number of jobs to print by one operation.

[Recommended Print Settings]

The following print settings can be set as the initial setting or the recommended setting.

- [Pages per Side]

Only recommended value can be set.

- [2 Sided Print]

- [Black & White Print]

[Job Display Target Server]

Sets the target server to display jobs. Enabled only for displaying Print On Demand jobs.



Note

You can perform this only with the print application server configuration.

[Communication Settings] Tab

Configure IPP/IPPS communication settings.

[IPP Port Number/IPPS Port Number]

Set the port number to use for IPP reception or for IPPS reception.

Mode Schedule List

How to Display

Select [Service Settings] > [Print Management] > [Mode Schedule List] on the administrator screen.

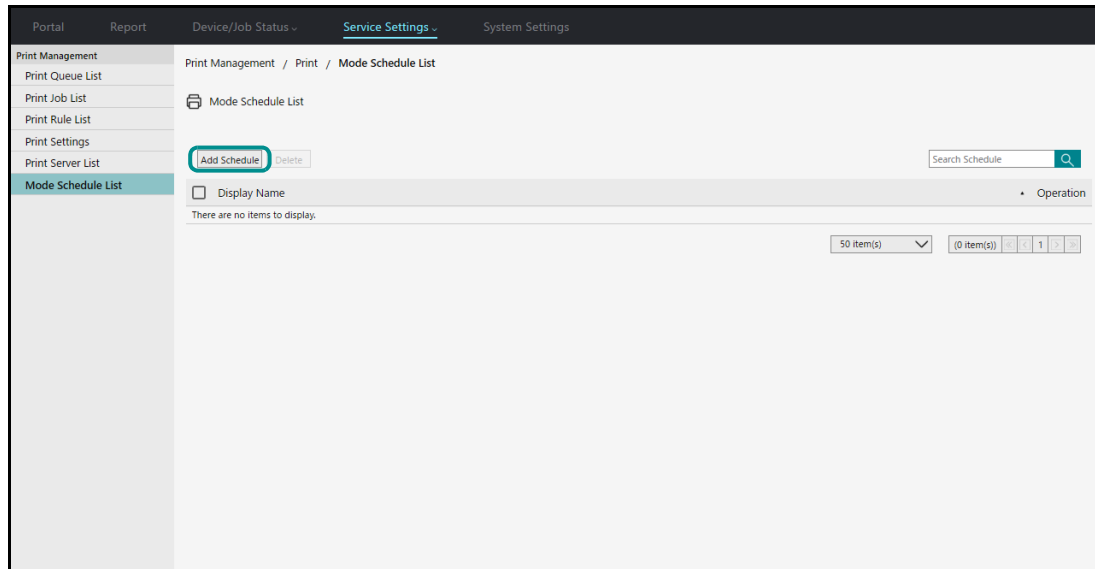
Page Summary

Displays the list of print mode schedules.

You can create new print mode schedules, or edit the print mode schedules that created previously.

Adding Schedules

Click [Add Schedule]. Up to 300 schedules can be created.



(1) Schedule Basic Information

Specify the following item, and then click [Next].

[Schedule Name]

Enter the name of the print rule schedule.

[Description]

Enter the description of the print schedule.

(2) Schedule Settings

Specify the following item, and then click [Next].

[Applicable Period]

Select the period to apply the schedule from the drop-down list box.

- [Duration and Time Period]
Specify the specific time and the time period for each day of the week during the time.
- [Time Period]
Specify the time period for each day of the week.

[Start Date], [End Date]

Specify these items when [Applicable Period] is set to [Duration and Time Period]. Enter the start date and end date of the schedule, or select using the calendar.

[Start Time], [End Time]

Specify the time applied to the schedule (hour, minute, a.m./p.m.).

[Day]

Select the day of the week applied to the schedule.

[Print Mode]

Select the print mode to apply from the drop-down list box.

[Add Schedule]

Add another schedule specified the duration and time period. Up to 100 items can be added to a schedule.

(3) Associate With Print Queue

Specify the following item, and then click [Next].

[Associate With Print Queue]

Select whether to associate the created schedule with a printer queue.

[Associate Print Queue]

Select a printer to associate with the created schedule. Click [Add] to display the list of printer queues.

(4) Overview

After you check the configured settings, clicking [Save] will create the print mode schedule.

You can click [Edit] for each item to change the settings.

Checking Mode Schedule Information

Click  in the mode schedule list and select [Properties].

You can display and edit the content configured for the mode schedule. You can edit the same items as the features configured in “Adding Schedules” (P.267).

Deleting Mode Schedule

Click  in the mode schedule list and select [Delete].

Print Operations

On ApeosWare Management Suite, the administrator sets the print environments.

The user who submits the print job selects a print queue on ApeosWare Management Suite by following the administrator instructions, and performs printing.

Overview of Print Operations

The print queue to be used determines which method is used, “Print On Demand” or “Direct Print”.

Direct Print makes the print job to be printed directly.

On Print On Demand, authentication by the user on the device allows printing. On Print Without a List, all the print jobs sent are printed. Print With a List displaying the print job list, you can select a job from the list and print it. You can change the print job settings and cancel the job.

When the access profile of the user submitting the print job is set so as to display the popup notification window, the print job information is notified to the PC executing the print job with a popup screen. The user, receiving the notification, authenticate it on the device and can operate the print job.



Note

Popup Messenger is required to receive a popup notification.

Preparation for Print

Add a Printer

To submit the print job from an application, you are required to add a print queue on ApeosWare Management Suite as the printer. Confirming the following information to the administrator, add a printer.

Print Queue Types	Required Information
Windows shared printer	Shared printer name
LPR queue	• Print server host name or IP address • LPR Queue Name

If necessary, install the required printer driver, open the Properties dialog, and set the following information.

- (1) Click the [Detailed Settings] tab.
- (2) Select [Spool print documents so program finishes printing faster].
- (3) Select [Start printing after last page is spooled].
- (4) Select the [Print spooled documents first] checkbox.
- (5) Remove the check mark on [Keep printed documents].



Note

Deselect the [Print spooled documents first] checkbox if print jobs are large and delay the processing of subsequent print jobs. Note that the print sequence may change afterwards.

Confirm the Device to be the output destination

Confirm the print mode of the print queue to be used, the device associated and the device authentication method.

To use the external access feature of the device, confirm the URL to access ApeosWare Management Suite from the device.

Install Popup Messenger

To receive a notification with Popup Messenger, install Popup Messenger on the client PC executing the print job.

Start the installer by the method corresponding to the OS in the installation environment, and install it following the message displayed.

In Windows Environment



Note

When installing Popup Messenger in Windows PC where firewall is enabled, add the following port as an exceptional setting before installation.

- Outbound:80/TCP, 443/TCP, 8181/TCP, 8183/TCP
- Inbound:8088/TCP

- (1) Log on to the PC to be installed as a user in the Administrators group.
- (2) Display the tool list on the installation screen of ApeosWare Management Suite.



Refer

How to start the installation screen → "Setup Guide"

- (3) Select Popup Messenger and install it.

In MacOS Environment

- (1) To the desktop, copy "Popup Messenger.pkg" contained in the DVD-ROM included in the ApeosWare Management Suite product package or found in the file you have downloaded.
- (2) Double-click the file you copied.



Note

If you are requested to enter the authentication information, enter the information of the user who has administrator permission for the environment to be installed.

In Linux Environment

- (1) Logon to the PC to be installed as root in the Administrators group.
- (2) Start the terminal.
- (3) Execute "Popup_Messenger.bin" contained in the DVD-ROM included in the ApeosWare Management Suite product package or found in the file you have downloaded.



Note

Input values are not case-sensitive.

Default Settings

After installation, activate Popup Messenger and perform initial setup.

For the settings required, refer to "Flow of Initial Settings" in "Popup Messenger Help".

Perform Print Job

The following describes how to perform print job.

Perform Direct Print

Select the printer whose print mode is set to [Direct Print] or [Direct Print - Non-Billed], and perform the print job.

You can perform print jobs by the operations as below.

- To submit the print job from an application
- Perform Web Print
- Perform Print E-mail
- To submit the print job from a mobile device



Refer

- "Perform Web Print" (P.272)
- "Perform Print E-mail" (P.273)
- "9 Mobile Device Settings and Operations" (P.309)

If you can receive a popup notification, you are notified of the print job status and the device to be the output destination.

The printings are collected in the device to be the output destination.



Refer

- "Receive Notification with Popup Messenger" (P.274)

Perform Print On Demand

The following describes how to operate Print On Demand.

1. Select the printer whose print mode is set to [On-Demand] or [On-Demand - Non-Billed] and execute the print.
 How perform the print job is the same operations as those on Direct Print.
 If you can receive a popup notification, you are notified that the job has been stored in the print server.
 You can change the print job attribute and the account to be used on the popup notification screen.
 For details, refer to "Receive Notification with Popup Messenger" (P.274).
2. On the device to be the output destination, following the settings, perform authentication.
3. Perform the following steps.
 - To Use Custom Service
 - (1) Push the ApeosWare Management Suite menu button displayed on the control panel.
 - (2) Select [Print On Demand].
 - To Use External Access Feature of the Device

The screen displayed and the features you can use vary deepening on the version of the external access feature of the device.

 - (1) Push the <Menu> button on the control panel.
 - (2) Press [Web Applications].
 - (3) Select the print server's URL from the connection destination list.
 - (4) Select [Open] on the popup menu.
 - (5) If the [Multifunction Device Settings] screen appears, press [Continue].
4. Perform the following steps.
 - On Print Without a List

The on-hold status of the print job executed by the user is removed, the print job resume.
 - On Print With a List

Selecting the target job from the print job list, perform it.

Operations Available on Print With a List

You can perform not only performing print job but the following operations on the print job list.

- To cancel the print job
 Select the print job, and then press [Delete].
- To check the estimated cost
 In cost management, you can see the cost needed to print.

Performing Print On Demand on another manufacturer's device

- From [Others] of the device list properties, link the external terminal to use.
- From [Communication Settings] of the device list properties, set "Retrieve Device Status" and "Retrieve Device Job Status" of Print Settings to [Off].
- The port specified in [System Settings] > [External Terminal Settings] must be opened in advance.
- The cost management feature cannot be used.
- Configuration of the network settings of the external terminal is required in advance.



Note

Use of this setting requires an option license.



Refer

- "Checking and Changing Device Information" (P.97)
- "External Terminal Settings" (P.54)

To change and confirm the print job attribute

You can confirm print job names, received dates, attribute of the print on the list of print jobs.

When you want to confirm the detailed information, push the job name in the print job list or push the Properties button to display the properties screen of the print job. On the properties screen, you can change the settings and print the job.



Note

- When the external access feature of the device is used, the settings you can change vary depending on the version of the external access.
- Depending on Page Description Language, the value of attribute that is different from the recommended value is shown in red characters.
- To change the print job to be displayed on the list

You can change the settings so as to be displayed only the job to be printed or not to be printed on the print job list.

Select the job you want to display from [Jobs to Display] on the [Print Settings] screen.

Perform Web Print

Access ApeosWare Management Suite with a web browser, and upload and print the file.

You can use Guest Print on Web Print.

In the Usual Web Print

1. Access ApeosWare Management Suite with a web browser and log in.
2. Select [Print/Job] > [Web Print] > [Web Print (Upload Print)] on the user screen.
When administrator permission is set to the user, logging in will cause the administrator screen to appear. Select [User Portal] on the header and display the user screen.
3. Select the file to be printed and the print queue, and set the print settings on the [Web Print] screen.
The print queue and the feature available are restricted depending on the access profile of the login user.
4. Click [Print].
 - When the print mode is [Direct Print]
The print job is sent to the device associated with the print queue.
 - When the print mode is [On-Demand], not Guest Print,
The print job is stored in the server.
The job is authenticated on the device and printed in the same way as in the usual Print On Demand.



Refer

"Perform Print On Demand" (P.270)

On Guest Print

When you perform Guest Print, confirm the following information to the administrator.

- The user ID and the password for Guest Print

- Whether administrator approval is required or not
- The print queue to be used

1. Access ApeosWare Management Suite with a web browser and log in.
To log in, use the user ID for Guest Print.
2. Select [Print/Job] > [Web Print] > [Web Print (Upload Print)] on the user screen.
3. Select the file to be printed and the print queue, and set the print settings on the [Web Print] screen.
The print queue and the feature available are restricted depending on the access profile set.
4. Click [Print].
When a password input area appearing, set the password you will enter in printing.
The print job sent, the guest print ID is displayed on the web browser.
5. If administrator approval is required, the administrator is notified of the guest print ID.
The administrator will search the job corresponding to the guest print ID on the print job list.
When the print is allowed, the administrator will remove the hold of the print job.
In Cost Management, the price for the process is displayed on the print job list. Determine how to impose the guest print cost in the operation policy.
6. Select the guest print menu on the device associated with the print queue.
7. Enter the guest print ID to perform the print job.
When you are required to enter a password, enter the password set in the step 4.
How perform the print job is the same operations as those on Print On Demand.

Perform Print E-mail

Print E-mail allows printing the mail body and the attached file sent to the specific email address or only the attached file. The administrator sets the email address for Print E-mail.

On Print E-mail, the print job is generated for the sender or the email address user set in CC.

When the print server receives an e-mail and accepts the print job, the result e-mail is sent to each mail address.

The name of the print queue which has sent the print job is described in the result mail.

The job status is confirmed on the job list, and the job is printed in the same way as on Web Print.

On Guest Print

When the mail sender or the CC address is not registered in the ApeosWare Management Suite user information, it will be processed as Guest Print.

In this case, the guest print ID is described in the result mail.

If administrator approval is required, notifying the administrator of the guest print ID, request to remove the hold of the print job.

After that, print it using the guest print ID with the device associated with the print queue.

Receive Notification with Popup Messenger

By installing Popup Messenger on the client PC that executes print jobs, you can receive print details and cancel print job notifications from ApeosWare Management Suite.



Note

- The features available vary depending on the user access profile and the print rule settings.
- For Web Print, Print E-mail, File Management Service Print or Mobile Print, a popup notification window is not displayed.



Refer

Details on features and operations → “Help for Accessory Tools”

Notification of print details

When Popup Notification is set in the access profile of the user who has executed printing, the [Print Details] screen is shown by the popup when print job is executed by using ApeosWare Management Suite.

[Print Details] window enables you to confirm the cost of the process and change the print job settings.

The print job remains on-hold until you click [Print].

The following are the items displayed on the [Print Details] window.

Items	Descriptions
Job Name	The print job name is displayed. Clicking the right icon allows changing the print job name.
User	The user name corresponding to the job owner name of the print job is displayed. If an alternate user ID is set, you can select it from the dropdown list box. Clicking the right icon allows specifying the temporal user ID.  Note The job owner name at the time when the print job is performed is changed to the user ID specified here. Therefore, the user ID specified here is recorded in the job log.

Items	Descriptions
Account	Select an account.  Note • Each account can be selected when a check mark is attached to [Select Account] in the access profile. • When a check mark is attached to [Ascending Order of Account Names] in [Account List Display Settings] in [Service Settings] > [Cost Management] > [Settings] on the administrator screen, the accounts are sorted and displayed in ascending order.
Personal/Shared Account	The account associated with the user and the balance or the amount limit are displayed. If multiple accounts are associated with the user, you can select one from the dropdown list box.  Note • If a parent account is associated, the sub account is displayed. The parent account is not displayed. • When the check mark is removed from [Display balance on screen] in [Print Popup Settings] in the access profile, the balance and amount limit are not displayed.
All User Accounts	To use [Shared account that all users can use], select an account from here.
Client Billable	When charging the account selected in [Shared Global], select the checkbox.  Note • [Client Billable] is displayed when other than [Off] is selected in [Shared Global]. • When a check mark is attached to [Enable Client Billing] in [Service Settings] > [Cost Management] > [Account List] > [Create Account] on the administrator screen, [Client Billable] is enabled.

Items	Descriptions
Account (Continued)	
Recently Used Account	To select an account from the recently used accounts, select an account from here.  Note [Recently Used Account] is displayed when one or more recently used accounts exist.
Favourite Account	To select an account from the favourite accounts, select an account from here.  Note • [Favourite Account] is displayed when one or more favourite accounts exist. • Favourite Account can be set on a Web browser or the operation panel of a device. They cannot be set in the popup screen of Popup Messenger.
Use without specifying account	When there is no relevant account or when the balance is insufficient, you can perform print job without specifying an account. Select this option in these cases.  Note [Use without specifying account] can be selected when a check mark is attached to [Using shared account that all users can use] in the user access profile and a check mark is also attached to [Use without specifying account].
Enter reason	Enter the reason to use it without specifying an account. When [Use without specifying account] is selected, this field is required.
Job Cost	The estimated cost of printing is displayed. If the print settings are changed on the popup notification window, the cost will be changed as well.  Note If ApeosWare Management Suite fails to analyze the print job, "Unknown" may appear.
Paper size	You can change the print settings.
Output Color	
2 sided	
Number of Copies	

Color Print Warning Notification

The confirmation message "Settings are configured to perform color print. Is it OK to print?" can be displayed when [Print] is clicked with Output Color set to color.

Configure the setting to display the warning using the following procedure.

1. Log on to a PC on the print server with the Administrator permission.
2. Open a command prompt window as an administrator.
3. Enter the following command and press the <Enter> key.

```
cd /d c: \{Installation destination of ApeosWare Management Suite}\Utils\Print pumConfCustomize
popupColorUsedWarning true
```

**Note**

To set the warning display to off, enter the following command in Step 3.

```
cd /d c: \{\Installation destination of ApeosWare Management Suite\}\Utils\Print pumConfCustomize
popupColorUsedWarning false
```

Cancel Notification of Print Jobs

When the popup screen is set to display the status of a print job in the access profile of the user who has executed printing, the notification can be received if the print job is canceled by the ApeosWare Management Suite processing.

On the cancel notification, the name of the print job and the reason of the cancelation is described.

The notification is provided when the reason of the print cancelation is either of the followings.

- The user who executed the print job is not associated with the printer queue.
- The user who executed the print job does not have a permission to use the device for the printing.

**Note**

The notification is given only when using the direct print.

- There is no account that the user who executed the print job can use.
- The balance of the account is insufficient relative to the print charge.
- The setting of "Cancel" in Print Rule is applied.

**Note**

If [Display Popup Screen] is activated in the access profile, the print job cancellation is notified at the same time of the print details notification.

- Printing is executed specifying the print queue with which Print Mode is set to [Disable Use].

The notification is not provide when the user cancels the print job him/herself from a web browser or the print job is canceled after the validation period expired.

Perform Approval Print Job

**Note**

- This feature is not available in some countries and regions.
For details, contact our dealers.
- Detection of specific information used in Approval Print/Alert of ApeosWare Management Suite 2 does not guarantee 100% accuracy.

With Approval Print, a document that a printing user (hereinafter referred to as "Approval Requester") attempts to print (hereinafter referred to as "Document Pending Approval") can be output subject to viewing and approval by an approving user (hereinafter referred to as "Approver").

Preparation for Approval Print

1. Select [Service Settings] > [User Management] > [Keyword Condition Policy] and set Approval Print to [On].

**Refer**

"Keyword Condition Policy" (P.176)

2. In [Add User], set the Approver for each user.



Refer

"Adding users" (P.133)

Operation by Approval Requester

1. Access ApeosWare Management Suite with a web browser and login.
2. On the user screen, select [Print/Job] > [Documents Requiring Approval] > [List of Documents Pending Approval].
Jobs with a user set as the Approver and pending approval are listed.
 - Canceling request for Documents Pending Approval
Select the checkbox for the document for which the request is to be canceled and click [Cancel Request], or click  under Operation and select [Cancel Request] from the menu displayed.
A dialog box to confirm Cancel Request is displayed. Enter comments as required and click [OK].
 - Resending request for Documents Pending Approval
Select the checkbox for the document for which a request is to resent and click [Resend Request], or click  under Operation and select [Resend Request] from the menu displayed.
A dialog box to confirm Resend Request is displayed. Enter comments as required and click [OK].
 - Canceling Documents Pending Approval
Select the checkbox for the document to cancel and click [Cancel], or click  under Operation and select [Cancel] from the menu displayed.
A dialog box to confirm Cancel is displayed. Enter comments as required and click [OK].
 - Checking the content of Documents Pending Approval
Select the checkbox for the document to confirm and click [View], or click  under Operation and select [View] from the menu displayed.
 - Searching for a job
If you Select [Advanced Search], the [Advanced Search] dialog box is displayed.
If you enter an operator, search attribute, condition and setting content and click [Search], jobs can be narrowed down with the specified conditions.

Operation by Approver

Approving, viewing or rejecting Documents Pending Approval

1. Access ApeosWare Management Suite with a web browser and login.
2. On the user screen, select [Print/Job] > [Documents Requiring Approval] > [List of Documents Requiring Approval].
A list of jobs currently requiring user approval appears.
A list of all jobs requiring approval is displayed when logged in as a system administrator.
 - Approving Documents Requiring Approval
Select the checkbox for the document to confirm and click [Approve], or click  under Operation and select [Approve] from the menu displayed.
A dialog box to confirm Approve is displayed. Enter comments as required and click [OK].
 - Checking the content of Documents Requiring Approval
Select the checkbox for the document to confirm and click [View], or click  under Operation and select [View] from the menu displayed.

■ Rejecting the content of Documents Requiring Approval

Select the checkbox for the document to confirm and click [Reject], or click  under Operation and select [Reject] from the menu displayed.

A dialog box to confirm Reject is displayed. Enter comments as required and click [OK].

Checking the history of Documents Pending Approval

1. Access ApeosWare Management Suite with a web browser and login.
2. On the user screen, select [Print/Job] > [Documents Requiring Approval] > [History of Documents Pending Approval].
Jobs with a user set as the Approval Requester and pending approval are listed.

Narrowing Down Jobs

If you Select [Advanced Search] in List of Documents Requiring Approval or History of Documents Pending Approval, the [Advanced Search] dialog box is displayed.

If you enter an operator, search attribute, condition and setting content and click [Search], jobs can be narrowed down with the specified conditions.

Precautions for Approval Print and Auto Masking

- Approval print and auto masking can be used only when prints are made from the common driver (Multi-model Print Driver 2).
- Approval print and auto masking are not available for printing from Flow Management Option. In the case of printing from Flow Management Option, keyword detection is not performed, and a job is printed as it is.
- Approval print and auto masking are not available for printing from USB. In the case of printing from USB, keyword detection is not performed, and a job is printed as it is.
- Approval print and auto masking are not available for USB printing from an on-demand terminal. In the case of USB printing from an on-demand terminal, keyword detection is not performed, and a job is printed as it is.
- Approval print and auto masking do not support printing from a mobile device. When a user for whom approval print or auto masking is enabled makes a print from a mobile device, the job is canceled regardless of whether a keyword is specified or not.
- In the keyword detection performed by approval print and auto masking, only the letters that contain font information can be detected. When letters are expressed with images or drawing commands or when letters are converted into images by applications such as PDF or by a printer driver during print process, they are ignored during detection.
- In the keyword detection performed by approval print and auto masking, string detection is performed for each line. If a string spans multiple pages or multiple lines, it is ignored during detection.
- In the keyword detection performed by approval print and auto masking, when a same area is detected by multiple conditions (keyword/regular expression), the condition defined later is not detected and is ignored.
- Approval print does not support direct print. If it is determined that approval is required for direct print, the job is canceled.
- If the "ApeosWare Management Suite 2 Feature Extension Option (b)" license that enables approval print and auto masking has been enabled or disabled, all servers, including distributed servers, must be rebooted. If these are not rebooted, they will fail to detect the target font, and thus may prevent correct usage of the approval print and auto masking functions.

Notes and Restrictions on Printing

GX Server Restrictions

Items	Description
Billing operations are not supported	Job charges are always calculated from their actual values. Estimates are made based on job information complementary parameters at the time of a printing command, but are adjusted after printing. If job logs are not collected within a defined period of time after sending jobs from the ApeosWare Management Suite to the print server, then the estimate will be refunded.
Available functions	If the [Print Server Linkage] checkbox is selected in the logical printer, [Page Description Language Default Value] will be set to [Do Not Detect]. Printing to the GX Server is processed as device-specific (Bypass), so available functions are limited.
Printer driver	Sending a job to the print server requires that printing is done via a PPSP-compatible PS printer driver.
Jobs on device	The GX Server job status is not monitored. After sending jobs to the print server, the job is completed in ApeosWare Management Suite. Furthermore, the job cannot be stopped from ApeosWare Management Suite.
Guaranteed print order	The print order of jobs printed via the print server relies on the processing order of the print server, so this cannot be guaranteed in ApeosWare Management Suite. Also, if a job via the print server and an on-demand print job are released at the same time, the print order is not guaranteed.
Device registration	Both the print server and the device need to be registered with a fixed IP address (DHCP not allowed). Before operation, perform a test print on the device registration screen to confirm that the output is from the intended device. Test printing is not subject to billing, and the print user ID will be "Apeos_Admin". At print server linkage, only LPR can be specified for the send protocol.
LPR queue name	When print server linkage is enabled, the Send LPR Queue Name cannot be specified on the logical printer, and the Send LPR Queue Name specified on the device will be used.
Status monitoring	Print server monitoring is not performed. When the device power is ON and the print server power is OFF, the device status will be displayed as "Normal", however, job sending will be canceled after a retry.
Job operation by another user on GX Print Server	With GX Print Server linkage, even if another user operates a job pending on the GX Print Server, it will be recorded as an operation by the user who sent the job.

Restrictions on Printing from iOS Devices

Items	Description
Available functions	If the [Print from iOS Device] checkbox is selected in the logical printer, [Page Description Language Default Value] will be set to [Do Not Detect]. Printing to the device is processed as device-specific (Bypass), so available functions are limited.
Print attribute specification	Numbers of prints and double-sided printing settings specified on the iOS device are not reflected in print attributes. Furthermore, print attributes displayed in ApeosWare Management Suite are values set in the job information complementary parameters, and cannot be changed.
Target devices	Devices that can print from an iOS device are only those that can print from iOS devices without using ApeosWare Management Suite.

Items	Description
Billing operations are not supported	Estimation at the time of a printing command is implemented from job information complementary parameters, but after printing completes, it will be adjusted in accordance with ApeosWare Management Suite settings.

Print Application Server Configuration Restrictions

With the print application server configuration, if connection to the main server is not possible or if the main server stops, some of the following functions may not be available.

- **Accept Print Job**
Printing from the printer driver as well as the print jobs other than e-mail print cannot be accepted. In the case of e-mail print, the notification e-mail is not sent when a print job is accepted.
- **Print rule**
 - When a print rule by user name is set, the print rule is ignored.
 - When a print rule by user group name is set, the print job becomes canceled.
- **Access Profile**
The default setting is applied for the access profile settings.

What if?

FAQ

Below are some frequently asked questions and the answers about printing.

To automatically delete the print jobs accumulated in the server

The print jobs on “Standby” and “On Hold” are automatically deleted after the period set on [Job Validity Period] has been expired.

Specify the validity period depending on the operation.

The validity period for the print job is also applied to the print jobs received before a change in the settings.

To request to analyze the print data with error

If an error has occurred during printing and solving of the error is difficult, contact our sales representatives. The sales representatives may ask to hand in the print data. When you are requested to hand in the print data, set [Save Print Data to File] to [Allow] on the [Print Job] tab on [Print Settings].



Note

Before retrieving the print data, make sure there aren't any problems if you provide the print data. After retrieving the data required, reset it not to output.

The print cost is not calculated correctly

The print cost, using the information retrieved by prescanning the print job, such as the number of sheets, the number of pages and Color Mode, determines the cost of processing. Therefore, the cost displayed may be different from the actual printing result depending on the page description language of the print job or the printing timing.

What is Page Description Language?

We describe Page Description Language and the features available as bellow.

Auto Judgment Page Language Description

If [Page Description Language Default Value] is set to [Auto Recognize] on the Print Queue

If [Page Description Language Default Value] is set to [Auto Recognize] on the Print Queue, print jobs are analyzed to determine the page description language.

If [Page Description Language Default Value] is set to [Do Not Detect]

Page description languages are not determined if [Page Description Language Default Value] is set to [Do Not Detect]. This enables print jobs in page description languages not supported by ApeosWare Management Suite to be printed instead of being canceled. The following features will be unavailable when this auto detection is turned off.

- Prescan
- Application of print rules
- Adding job client IDs and job access tickets
- Color mode changes, 2-sided/1-sided changes, monochrome only printing, 2-sided only printing, page number changes, and paper size changes

When job details or a list of print jobs are displayed on the panel of a multi-function printer during on-demand printing, a warning mark is displayed.

Additionally, the fees displayed may differ from actual fees in some cases.

Page Description Language and the Features Available

The relationship between the ApeosWare Management Suite features and the page description languages is as shown below.

○: Available

-: Not Available

Features	Page Description Language						
	ART-EX/PLW	PostScript	XPS ^{*1}	PCL	PDF	XDW	The Others
Auto Judgment Page Language Description	○	○	○	○	○	○	-
Prescan ^{*2}	○	○	○	○	○	○	○
Change Output Color Change 2 Sided Force Black & White Print Force 2 Sided Print	○	○	○	○ ^{*4}	○	○	-
Print Force 2 Pages Print Add watermark Add header/footer Add QR code	-	-	-	○	-	-	-
Change Paper Size ^{*3}	○	○	○	○ ^{*4}	○	○	-
Calculate Cost for Processing Job	○	○	○	○	○	-	-

^{*1} XPS is an abbreviation for "XML Paper Specification".

^{*2} The contents to be prescanned vary depending on the page description language. For details, refer to "Information Retrieved by Prescanning" (P.284).

^{*3} You may not be able to change the print job sent from ContentsBridge Utility.

^{*4} This can be judged only when our printer driver or Fuji Xerox's is used.

Print On Demand Features and Page Description Languages

The relationship between the Print On Demand features and the page description languages is shown as below.

○: Available

-: Not Available

Features	Page Description Language						
	ART EX	PostScript	XPS ^{*1}	PCL	PDF	XDW	The Others
Judge whether Print Job With Restrictions ^{*2}	○	○ ^{*3}	-	○	○	-	-
Change the Number of Copies ^{*4}	○	○	○	○	○	○	-
Change Output Color and Change 2-Sided	○	○	○	○	○	○	-

Features	Page Description Language						
	ART EX	PostScript	XPS*1	PCL	PDF	XDW	The Others
Cost Estimation	○	○*3	○*5	○	○	○	-
Create Display Name of Print On Demand	○	○*6	○*6	○*6	○*6	○*6	○*7

*1 XPS is an abbreviation for "XML Paper Specification".

*2 Determines whether it is applied for [Print Without List Settings] > [Print Job With Restrictions] on [Print Settings] > [Print On Demand] tab. The page description language with "-" processes all the print jobs received as a print job which can be print without restriction.

*3 Some printers may not be able to judge correctly.

*4 Available only for the device with a hard disk (including the SSD).

*5 Is judged only when the print job is sent from ContentsBridge Utility.

*6 Is created only when Charge Print Stored Document Name (ACNA) is set on XPJL.

*7 The print job name retrieved from Charge Print Stored Document Name (ACNA) cannot be used.

Information Retrieved by Prescanning

The information retrieved by prescanning by page description language is as below.



Note

- If the paper size is not specified, prescanning is performed on all pages of the print job when the page description language of data is XPS, PDF, or XDW.
- If the paper size is not specified, prescanning is performed on only the first page of print job to retrieve the size information only regarding the page description language of data not applicable to the full page scan.
- The values of "Number of Color Pages per Copy", "Total Number of Black & White per Copy", "Color Delivered per Set", and "Number of Black & White per Copy" are estimated values, so they may be different from the actual print results.

○: Possible to be retrieved

-: Impossible to be retrieved

Information which can be retrieved	Page Description Language						
	ART EX	PostScript*1	XPS*2	PCL	PDF	XDW	The Others
Job Owner Name	○	○	○*6	○	○	○	○*9
Paper size	○	○	○*7	○	○	○	-
The Number of Color Pages per Copy	○	○	○*8	○	○	○	-
The Total Number of Black & White per Copy	○	○	○*8	○	○	○	-
Color Delivered per Set*3	○	○	○*8	○	○	○	-
The Number of Black & White per Copy	○	○	○*8	○	○	○	-
Specify 2 sided	○	○	○*7	○	○	○	-

Information which can be retrieved	Page Description Language						
	ART EX	PostScript ^{*1}	XPS ^{*2}	PCL	PDF	XDW	The Others
Specify Finisher ^{*4}	○ ^{*9}	○ ^{*9}	○ ^{*9}	○ ^{*9}	○ ^{*9}	○ ^{*9}	-
Number of Copies ^{*5}	○	○	○ ^{*6}	○	○	○	-
Alternate Job Name	○	-	-	○	○ ^{*9}	○	○ ^{*9}
N Up	○	○	○ ^{*7}	○	○	-	-

*1 The attribute can be retrieved correctly when the print job is sent with our PostScript printer driver or Fuji Xerox's.

For the print job sent from the client whose OS is Linux or Mac OS, the Output Color, Impressions/Sheets, the Number of Copies, and Paper Size can be retrieved correctly by using Additional OS Parser Option.

*2 XPS is an abbreviation for "XML Paper Specification".

*3 If either of the two sides is Color, it is judged as Color.

*4 Retrieves the settings such as Staple, Punch and Folding etc.

*5 On the device with a hard disk (including the SSD), you can retrieve the accurate number of copies.

*6 Is retrieved only when the job is sent from ContentsBridge Utility.

*7 If [Use Printer Job Language] has been specified on the print settings in ContentsBridge Utility, the document size, 2 Sided, the number of copies and N-up specified on XPJL are given priorities.

*8 If 2 Sided and N-up settings specified on XPJL are different from the data values of XPS(XML Paper Specification), the values retrieved by prescanning may be different from the actual output results.

*9 This is retrieved only when you specify it in printing.

Print Job Status

The print job status is as shown below.

Job Status	Descriptions
Receiving in Progress	Analyzing the print job received and changing the attribute.
Waiting for Administrator Approval	The guest job is waiting for the administrator approval. Removing the hold by the administrator will allow printing.
On Hold	The job is on-hold by Print On Demand
On Hold (During PC Operation)	Either of the following. • The attribute of the print job that is [On Hold] is being changed. • Popup screen is displayed
Printing in Progress	The job is being preprocessed to send the print job to a device.
Standby	The job has been completed, and is waiting for being sent to the device.
Transferring	The print job is now being sending to the device.
Printing	Under printing by the device.
Printing Completed	Printing has been completed.
Cancel	Printing has been canceled.

- Some devices may reach "Printing Completed" status at the end of data transfer.
- If an error occurs during printing or data transfer, the status becomes "Standby". It will restore to its former status. However, if the status of not being processed persists, it will be canceled.

- On the print job on Print On Demand and the one that the Popup screen is displayed, the status turns "Receiving in Progress" to "On Hold". After removing the hold by the user, it turns to [Standby].

Uninstall Popup Messenger

When Popup Messenger is no longer needed, uninstall it following the steps blow.



Note

You are required to perform it as a user with administrator permission as well as in installation.

In Windows Environment

Displaying Windows program and the feature window, select Popup Messenger and uninstall it.

In MacOS Environment

Activating the terminal, and perform the shell script to uninstall the program.

Execution location: /usr/local/FUJIFILM/ApeosWare MS/Popup Messenger

Shell Script: `uninst_Popup_Messenger.sh`

In Linux Environment

Perform "UNINSTALL", the installation directory of Popup Messenger.

Printing from Chromebook

When printing from Chromebook, use of a Google Workspace environment is required. Set the following.

Policy settings

When printing from Chromebook to ApeosWare Management Suite 2 using IPP, use of a Google Workspace environment is necessary in order that ApeosWare Management Suite 2 is notified of the name of the user logged in with IPP.

1. On the Admin console Home page, select [Devices] > [Chrome] > [Settings] > [Users & browsers].
2. Select the organizational unit that created the user.
3. From [Print] > [CUPS print job information], select [Include user account and filename in print job].

Adding a printer

Use the procedure below to add a printer in Google Workspace.

1. On the Admin console Home page, select [Devices] > [Chrome] > [Settings] > [Printers] > [Printers].
2. Select the organizational unit that created the user.
3. Select the yellow [+] icon > press the [Add a printer] icon.
4. On the printer adding screen, enter the printer details, and press [Add Printer].
 - Printer name: Arbitrary name
 - Use driverless configuration: Deselected
 - Select manufacturer: Select the manufacturer of the actual printing device
 - Select model: Select the model of the device that will actually print
 - Protocol: Select https or ipp^{*1}

Host: ApeosWare Management Suite IP and host name^{*1}

Port: IPPS port number set in ApeosWare Management Suite^{*1}

Path: IPP printer name set in ApeosWare Management Suite^{*1}

^{*1} In order to print with the user name logged in to the Chromebook, creation of an IPPS logical printer is required in ApeosWare Management Suite 2.

Set the protocol, host, port, and path to match the ApeosWare Management Suite 2 IPP settings.

5. Select the added printer, enable [Allow for users in this organization], and press [Save].

8 Setting Scan and File Management Service

Settings from a Web Browser

The user with [System Manager] permission can set scan settings from a web browser and settings to link with the file management service. S/he, moreover, can confirm the scan job the user has executed. The file management service user can set the authentication information to the file management service.

We describe the settings and management available on each page.



Note

The user with [System Manager] permission includes an Apeos_Admin user.

- For the user with [System Manager] Permission

Pages	Descriptions
Scan Settings	Sets the scan settings to be required to use the simple flow feature.
Email Settings	Sets the initial settings of the mail subject and the body to email a scanned document.  Refer "Email Settings" (P.290)
Common Settings	Sets the scan setting values and how to process a scanned document. These settings are in common with [Email] and [Scan to {File Management Service}].  Refer "Common Settings" (P.290)
File Management Service Settings	Sets the settings to link with a file management service.  Note You are required to contract to use the file management service and to retrieve the account required in advance. Refer to the guide provided by the file management service about the settings required and how to operate the file management service.
Shared Folder Settings	Sets the settings to link with a shared folder.  Refer "Shared Folder Settings" (P.292)
Google Drive Settings	Configures to link with Google Drive.  Refer "Google Drive Settings" (P.295)

Pages	Descriptions
File Management Service Settings (Continued)	
SharePoint Settings ^{*1}	Configures to link with SharePoint.  Refer "SharePoint Settings" (P.293)
DocuShare Settings ^{*1}	Configures to link with DocuShare.  Refer "DocuShare Settings" (P.293)
Salesforce Settings ^{*1}	Configures to link with Salesforce.  Refer "Salesforce Settings" (P.294)
OneDrive Settings ^{*1}	Configures to link with OneDrive.  Refer "OneDrive Settings" (P.297)
SharePoint Online Settings ^{*1}	Configures to link with SharePoint Online.  Refer "SharePoint Online Settings" (P.297)
ABBYY FlexiCapture Settings ^{*1}  Note This feature is not available in some countries and regions. For details, contact our dealers.	Configures to link with ABBYY FlexiCapture.  Refer "ABBYY FlexiCapture Settings" (P.295)
Scan Job Status	
Scan Job Status	The list of scan jobs executed by all users is displayed.  Refer "Scan Job Status" (P.299)

^{*1} Displayed only when the option license is required.

- For the file management service user

Pages	Descriptions
Setting {File Management Service}	Sets the authentication information of the file management service. File management services allowed to access are displayed.  Refer "Set Authentication Information to File Management Service" (P.300)
Scan Job List	Displays the list of the scan job that the user executed him/herself. The user can cancel or resume jobs.  Refer "Confirm Scan Job Status" (P.301)

Setting Items by the User with [System Manager] permission

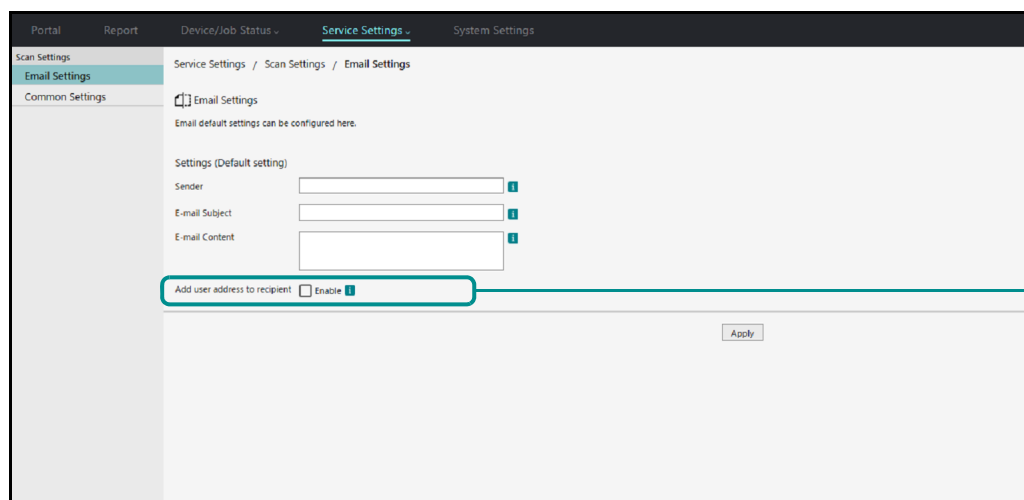
Email Settings

How to Display

Select [Service Settings] > [Scan Settings] > [Email Settings] on the administrator screen.

Page Summary

You can set sender's email address, the subject and the body emailed by [Email]. The items that have been set are displayed as default values when [Email] is executed, and you can modify the values as needed.



Check the box, and the mail address of the user performing scanning will be added to the recipients.

You can enter the following variables to the sender's mail address and the subject. Not case sensitive. The variable can be replaced with the information retrieved in emailing.

Items	Variables	Information	Information Sources
Sender	{LoggedInUser}	Normal email address of the user performing scanning	ApeosWare Management Suite
Subject	{Location}	Installation Location	Device
	{Name}	Name	
	{IPAddress}	IP Address	



Note

To send email with ApeosWare Management Suite, you are required to set the SMTP server or the POP3 server information on [System Settings] > [Network Settings] on the administrator screen.



Refer

Settings for sending emails→“Network Settings” (P.40)

Common Settings

How to Display

Select [Service Settings] > [Scan Settings] > [Common Settings] on the administrator screen.

Page Summary

You can set the scan settings and how to process a scanned document. These settings are in common to the following features.

- To email a scanned document as an attachment

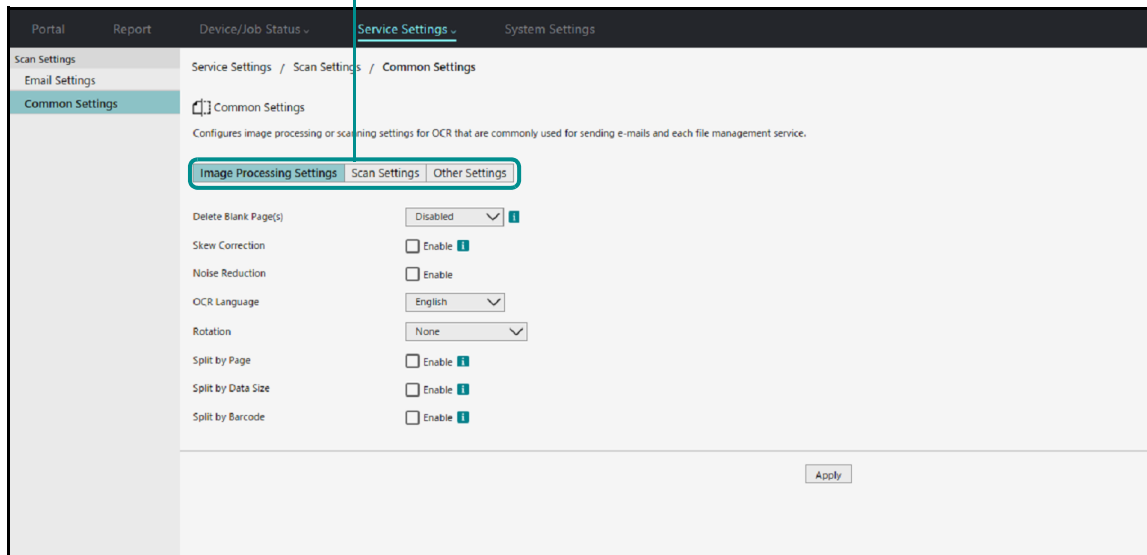
- To send a scanned document to a file management service



Note

These settings are available to submit a scan job with a mobile device.

You can switch the setting screen here.



[Image Processing Settings] tab

This enables you to set how to process the scanned image. The following settings are available.

- Delete Blank Page(s)
- Skew Correction
- Noise Reduction
- OCR Languages

Select a language to perform OCR Processing.

- Rotate

Selecting [Auto Rotation] allows being Auto Rotation using the OCR processing result.

- The settings to split a document

Select something from Delimit by File Page Count, Delimit by File Size or Delimit the page with barcode and split the document. You can select multiple options.



Note

- When splitting is performed based on the number of pages, or splitting is performed based on pages with barcodes, use the following formats:
PDF, PDF (OCR Convert), PDF/A, Word, Excel, PowerPoint, TIFF (Multi-Pages), XML Paper Specification(XPS)
- When splitting is performed based on the file size, use the following formats:
PDF (OCR Convert), PDF/A, Word, Excel, PowerPoint
- To split a document by a barcode, OmniPage Barcode Reader Option is required.
- When you split a document, the file name will become the name with the data and the time (YYYYMMDDhhmmsssss) attached to the original file name.
- Image processing of DocuWorks documents cannot be performed. It will be skipped if it is set.
- If Thai is selected as the OCR language, conversion to MS-Office (Word), MS-Office (Excel), or MS-Office (PowerPoint) is not available.
- You cannot convert high compression for some scanning resolutions, scanning magnifications, color modes, and output file formats.

[Scan Settings] tab

This enables you to set the initial values displayed on the scan executing screen. By applying a check mark in the [Prohibit Change] checkbox on the right side of the setting item, the settings will be fixed and not allowed to be modified in performing scanning on the device. Note that the scan job is executed selecting from the usable values on the model not supporting the fixed value.

For example, when the feeder is set to 2 side, the model not available for 2 side scanning performs the scan job selecting [1 Sided] on the scan executing screen.

The reserved character strings that can be used are as follows. They are respectively replaced with the year, month, day, hour, minute and second when the scan job was executed.

[\$YYYY]: Replaced with a year in 4 digits.

[\$MM]: Replaced with a month in 2 digits.

[\$DD]: Replaced with a date in 2 digits.

[\$H]: Replaced with an hour in 24-hour format.

[\$mm]: Replaced with minutes in 2 digits.

[\$ss]: Replaced with seconds in 2 digits.



Note

For some devices, you cannot convert to XML Paper Specification (XPS).

[Other Settings] tab

This enables you to set whether to display the following windows on the control panel after operating on the device.

This tab is displayed only when the license of Cost Recovery Option is activated.

- Display charge confirmation screen

Check the box to display the window to confirm the cost of processing.



Note

For the user with [Force stop when minimum balance is reached] set to [Stop] in the access profile, the cost confirmation window is necessarily displayed regardless of this setting.

Shared Folder Settings

Preparations

Sets the access permission for the require user creating the shared folder.



Note

The required user means the user who uses the feature to store the scanned document in the shared folder.

How to Display

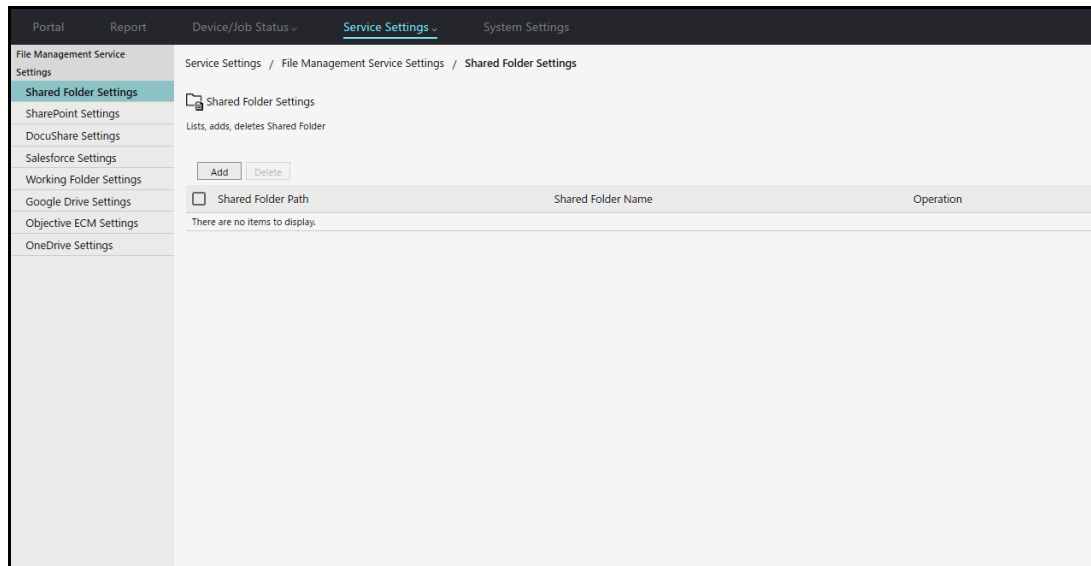
Select [Service Settings] > [File Management Service Settings] > [Shared Folder Settings] on the administrator screen.

Page Summary

The storing destination list is displayed.

To add a storage location, clicking [Add], set the path of the shared folder and the shared folder name. Specify the path by either of the following.

How to specify the path	Cooperating Folder
The path beginning with “\\”	Windows Shared Folder
The path beginning with “ftp://”	The folder on the FTP server



SharePoint Settings

Preparations

Confirm the URL of the SharePoint server and the path for the private site.

How to Display

Select [Service Settings] > [File Management Service Settings] > [SharePoint Settings] on the administrator screen.

Page Descriptions

The SharePoint server list already set is displayed.

To add a server, clicking [Add], set the SharePoint server URL, the display name and the path for the private site.



Note

The private site is displayed on the personal tab in accessing SharePoint.

DocuShare Settings

Preparations

The server common software DocuShare cooperation option is required to install in the DocuShare server.

How to Display

Select [Service Settings] > [File Management Service Settings] > [DocuShare Settings] on the administrator screen.

Page Descriptions

The DocuShare server list already set is displayed.

To add a server, click [Add] and specify the DocuShare server URL and the DocuShare server name (displayed name). When the ApeosWare Management Suite server requires proxy connection to connect DocuShare, select the checkbox for [Use proxy to connect].



Note

- For the DocuShare server URL, enter up to before "dsweb".
Example: When the URL is "http://serverA/docushare/dsweb", enter as "http://serverA/docushare/".
- To use a proxy server, HTTP proxy server information is required to be set on [System Settings] > [Network Settings] on the administrator screen. These settings are in common to the whole system of ApeosWare Management Suite. When you change the setting, verify that it will not affect any other functions.

Salesforce Settings

Preparations

Register ApeosWare Management Suite as connection application, accessing Salesforce by administrator permission. The steps are as follows:

- (1) Click [New] on the connection application.
- (2) Set the basic information. The recommended values for connecting to ApeosWare Management Suite are as shown below.
- (3) The set values are displayed on the authentication screen when accessing Salesforce from ApeosWare Management Suite.

Items	Descriptions	Recommended Values
Connection application name	Display name of the application	FUJIFILM ApeosWare Management Suite
API reference name	ID information to specify the connection application	awms
Merchant manager email	Email address of the contact for general users	Email address of the Salesforce administrator
Merchant manager telephone	Telephone number of the contact for general users	None Set any value as necessary.
Logo image URL	The URL of the logo image displayed on the authentication window	
Icon URL	The URL of the icon displayed on the authentication window	
Information URL	The URL displayed on the authentication window	
Descriptions	The description displayed on the authentication window	

- (4) Check [Enable OAuth Settings], and set [Callback URL] and [Selected OAuth Scopes].

Items	Setting Value
Callback URL	Enter the following URL. https://{Host name or IP address}/user/connector/generic/redirectoauth For {Host name or IP address}, enter the host name or IP address specified when ApeosWare Management Suite was installed.

Items	Setting Value
Selected OAuth scope	Select the following items from [Available OAuth Scopes] and add them. • Access Connect REST API resources (chatter_api) • Perform requests any time (refresh_token, offline_access) • Allow access to unique user identifier (openid) • Access custom permissions (custom_permissions) • Use API to manage user data (api)

(5) Once you have registered the connection application, confirm [Consumer Key] and [Consumer Secret].

How to Display

Select [Service Settings] > [File Management Service Settings] > [Salesforce Settings] on the administrator screen.

Page Descriptions

Set Consumer Key, Consumer Secret and the server name specified in the preparations. In addition, when the ApeosWare Management Suite server requires proxy connection to connect Salesforce, select the checkbox for [Use proxy to connect].



Note

To use a proxy server, HTTP proxy server information is required to be set on [System Settings] > [Network Settings] on the administrator screen. These settings are in common to the whole system of ApeosWare Management Suite. When you change the setting, verify that it will not affect any other functions.

ABBYY FlexiCapture Settings

Preparations

Check the path to the server of ABBYY FlexiCapture.

How to Display

Select [Service Settings] > [File Management Service Settings] > [ABBYY FlexiCapture Settings] on the administrator screen.

Page Descriptions

The ABBYY FlexiCapture server list already set is displayed.

To add a server, click [Add] and specify the ABBYY FlexiCapture server URL and the ABBYY FlexiCapture server name (displayed name).

Google Drive Settings

Preparations

Confirm that you can access Google Drive on the Internet from the ApeosWare Management Suite server.

Additionally, Google Workspace users are required to register applications in the Google Cloud Platform (<https://console.cloud.google.com/>), and obtain an application ID and client secret. Furthermore, being able to use a web browser to make an FQDN format HTTPS connection on the ApeosWare Management Suite 2 administrator screen is required.

1. Access the Google Cloud Platform (<https://console.cloud.google.com/>).
2. Either select a project, or create a new project.
3. Click [Library] under [APIs & Services], and enable [Google Drive API].
4. Click [OAuth consent screen] under [APIs & Services].
5. For [User Type], select [Internal] and click [CREATE].
6. Set the [App name], [User support email], and [Developer contact information].
For [App name], "FUJIFILM ApeosWare Management Suite" is recommended.
7. Click [SAVE AND CONTINUE].
8. Click [ADD OR REMOVE SCOPES], and select the following.
API: Google Drive API
Scope: .../auth/drive
Click [UPDATE].
9. Click [SAVE AND CONTINUE] and check the details.
10. Click [Credentials] under [APIs & Services].
11. Click [Create credentials], and select [OAuth client ID].
12. For [Application type], select [Web application].
13. Set the [Name] and [Authorized redirect URIs], and click [CREATE].
Set [Authorized redirect URIs] to "https://{Server name}/user/connector/generic/redirecttoauth".
For "{Server name}", set the ApeosWare Management Suite 2 main server host name. The IP address cannot be set. The host name to set must be in a format that can be accessed from client PCs and multifunction devices.
14. Record the client ID and client secret.
15. From the ApeosWare Management Suite 2 administrator screen, access [Service Settings] > [File Management Service Settings] > [Google Drive Settings].
16. Enter the application ID and client secret acquired when the application was registered to the Google Cloud Platform into [Your Client ID] and [Your Client Secret]. As necessary, select the checkbox for [Use proxy to connect].
If the [Your Client ID] and [Your Client Secret] is set, reconfiguration of credentials for all users on the ApeosWare Management Suite 2 user screen is necessary.

How to Display

Select [Service Settings] > [File Management Service Settings] > [Google Drive Settings] on the administrator screen.

Page Descriptions

When the ApeosWare Management Suite server requires proxy connection to connect Google Drive, select the checkbox for [Use proxy to connect].



Note

To use a proxy server, HTTP proxy server information is required to be set on [System Settings] > [Network Settings] on the administrator screen. These settings are in common to the whole system of ApeosWare Management Suite. When you change the setting, verify that it will not affect any other functions.

OneDrive Settings

Preparations

In the Microsoft Azure Portal, it is necessary to register the application and acquire the application ID and client secret.

1. From the Microsoft Azure Portal (<https://portal.azure.com/>), access [Application registration] of [Microsoft Entra ID], and click [New registration].
2. Set the name, supported account type, and redirect URL and click [Register].
For the name, "FUJIFILM ApeosWare Management Suite" is recommended.
For the supported account type, select [Directory for any organization (any Microsoft Entra directory - multi-tenant)].



Note

For the redirect URL, select [Web] and enter "https://{Server Name}/user/connector/generic/redirecttoauth". In "{Server Name}", set the host name or the IP address of ApeosWare Management Suite. The host name and IP address you set need to be in the format that enables access from the client PC and the multifunction device.

3. Click [Overview].
4. Record Application ID.



Note

The application ID is generated automatically.

5. Click [Certificate and Secret].
6. Click [New Client Secret], and record the Value of the client secret.
7. Click [API Access Permission].
8. Click [Add Access Permission], and add the Sites.ReadWrite.All authority of Microsoft Graph by [Delegated Access Permission].

How to Display

Select [Service Settings] > [File Management Service Settings] > [OneDrive Settings] on the administrator screen.

Page Descriptions

The connection setting screen to Microsoft OneDrive for Business is displayed.

Enter the application ID and client secret acquired when the application was registered to the Microsoft application registration portal into [Application ID] and [Application Secret]. Select the checkbox for [Use proxy to connect].

SharePoint Online Settings

Preparations

In the SharePoint Application Registration Portal, it is necessary to register ApeosWare Management Suite as a connection application and acquire the client ID and client secret.

The settings need to be made per site to be registered. The URL of a sub site can be specified, but the upstream sites and sub site cannot be accessed. The steps are as follows:

1. SharePoint Application Registration Portal
Access (https://{URL of site to register}/_layouts/15/AppRegNew.aspx).
Example: When using <https://test.sharepoint.com/sites/TestSite>, access https://test.sharepoint.com/sites/TestSite/_layouts/15/AppRegNew.aspx.
The application registration screen is displayed.
2. Click [Generate] of [Client Id].
[Client ID] is generated automatically.
3. Make a note of the generated [Client Id].
You will need [Client ID] in the subsequent work.
4. Click [Generate] of [Client Secret].
[Client Secret] is generated automatically.
5. Make a note of the generated [Client Secret].
You will need [Client Secret] in the subsequent work.
6. Enter the application name in [Title].
For the application name, "FUJIFILM ApeosWare Management Suite" is recommended.
7. Enter the domain name of the ApeosWare Management Suite server in [Application Domain].



Note

You can enter "WORKGROUP".

8. Enter the following URL in [Redirect URL].
<https://{ApeosWare Management Suite host name}/user/connector/generic/redirecttoauth>
9. Click [Create].
ApeosWare Management Suite is registered as the connection application.

After registration of the application, make shared registration of SharePoint Online data.

The settings need to be made per site to be registered. The URL of a sub site can be specified, but the upstream sites and sub site cannot be accessed. The steps are as follows:

10. Access "https://{URL of site to register}/_layouts/15/appinv.aspx".
Example: When using <https://test.sharepoint.com/sites/TestSite>, access https://test.sharepoint.com/sites/TestSite/_layouts/15/appinv.aspx.
The shared registration screen for SharePoint Online data is displayed.
11. Enter the client ID generated by the SharePoint Application Registration Portal in [App Id] and click [Lookup].
The application name, domain name, and URL you entered in SharePoint Application Registration Portal are displayed in [Title], [Application Domain], and [Redirect URL].
12. In [Permission Request (XML)], set the access rights to the site to register in the XML format as shown below:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">  
<AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="Write" />  
</AppPermissionRequests>
```

13. Click [Create].
The message "Do you trust FUJIFILM ApeosWare Management Suite?" is displayed.

14. Click [Trust It].

The data share registration of SharePoint Online is completed.

How to Display

Select [Service Settings] > [File Management Service Settings] > [SharePoint Online Settings] on the administrator screen.

Page Descriptions

A list of the registered SharePoint Online sites is displayed.

During preparations, if you want to additionally register a site for which application registration and data sharing registration are completed, click [Add] and set the site URL, site name, and client ID and client secret acquired upon application registration. When the ApeosWare Management Suite server needs a proxy connection to connect to the SharePoint Online site, select the checkbox for [Use proxy to connect].



Note

- To use the proxy server, the information of the HTTP proxy server needs to be set in [System Settings] > [Network Settings] on the administrator screen. These settings are in common to the whole system of ApeosWare Management Suite. When you change the setting, verify that it will not affect any other functions.
- Up to 300 SharePoint Online sites or sub sites that can be added.

Scan Job Status

How to Display

Select [Device/Job Status] > [Scan Job Status] > [Scan Job Status] on the administrator screen.

Page Descriptions

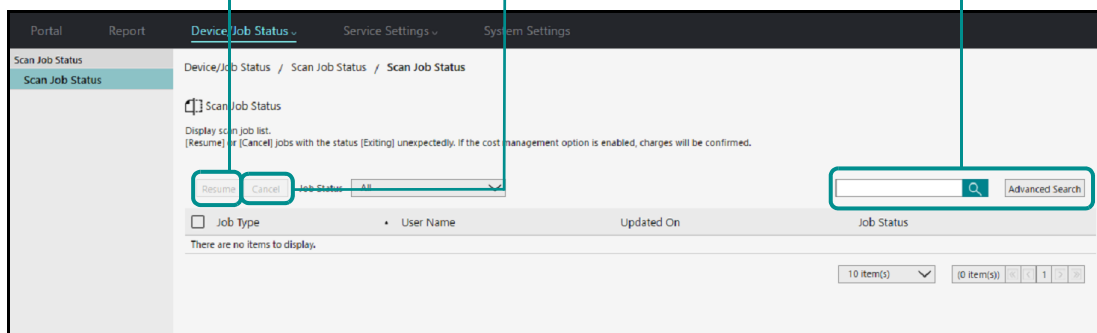
This enables you to confirm the job generated when the user uses the following features.

- To email a scanned document as an attachment
- To send a scanned document to a file management service

Resumes the job completed with an errors from the location the error has occurred.

Cancels the job running.

Narrows the jobs to be displayed.



The job record completed is automatically deleted after expiring the retention period.



Note

- The job submitted with a mobile device is also displayed.
- If the job has been completed with errors, the scanned document cannot be retrieved. When the error is not solved even the job is resumed, resume scanning.

- The job that the document stored in the file management service is printed is displayed on [Service Settings] > [Print Management] > [Print Job List].

What the users of File Management Service can do

The user using a file management service can set the authentication information in advance. Setting it previously enables the user to omit entering the authentication information in accessing the file management service from the device.

In addition, the user can confirm the status of the scan job executed by the user or cancel the job.



Note

- To set the authentication information of the file management service, it is required that the access to the user's portal be allowed in the access profile.
- To link with Google Drive, Salesforce, OneDrive, or SharePoint Online, it is required to set the authentication information in advance. When operating by the device, the authentication information cannot be entered.

Set Authentication Information to File Management Service

Preparations

Retrieve the information to access the linking file management service.

To set the authentication information of Google Drive, Salesforce, OneDrive, or SharePoint Online, confirm that HTTPS connection is available.

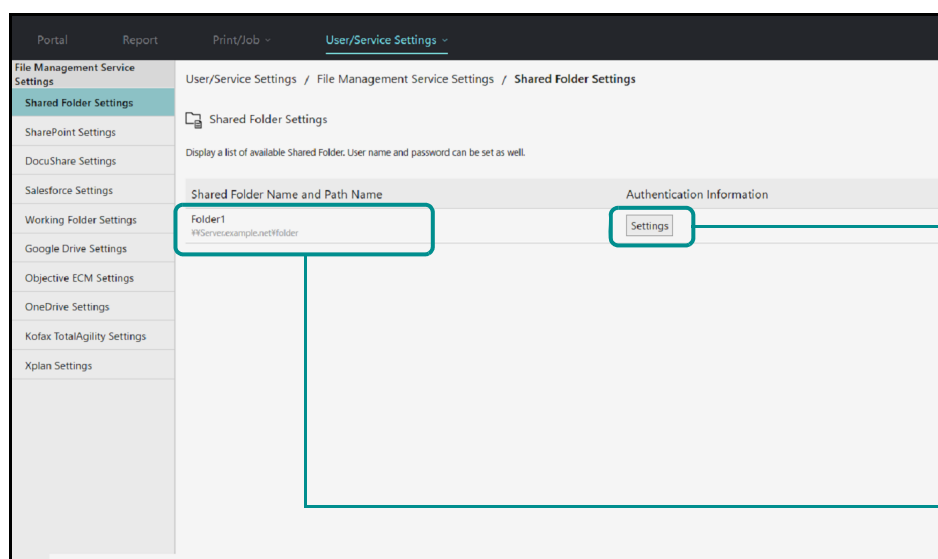
How to Display

Select the menu under [File Management Service Settings] of [User/Service Settings] on the user screen.

Page Descriptions

This part describes how to set a file management service taking [Shared Folder Settings] as an example. How to set the file management service other than Google Drive, OneDrive, Salesforce, SharePoint Online and ABBYY FlexiCapture is basically the same.

Click [Settings] or [Edit], and set the authentication information.



[Settings] is displayed when you are setting new authentication information, and [Edit] is displayed when information is already set.

The connection destination list the administrator registered is displayed.

Setting the authentication information with ApeosWare Management Suite enables you to check whether the access to the file management service is possible.

For Google Drive, Salesforce, and SharePoint Online, perform the following steps.

For Google Drive

Access the [User/Service Settings] menu of ApeosWare Management Suite via HTTPS connection. Clicking [Authenticate] displayed on the setting window of Google Drive displays the authentication window of Google Drive.

Enter the authentication information of Google Drive, and approve the operation from ApeosWare Management Suite.

For OneDrive

Access the [User/Service Settings] menu of ApeosWare Management Suite via HTTPS connection.

Clicking [Authenticate] displayed on the setting window of OneDrive causes the authentication screen of OneDrive to appear.

Enter the authentication information of OneDrive account, and approve the operation from ApeosWare Management Suite.

For Salesforce

Access the [User/Service Settings] menu of ApeosWare Management Suite via HTTPS connection.

Clicking [Authenticate] displayed on the setting window of Salesforce displays the authentication window of Salesforce.

Enter the authentication information of Salesforce account, and approve the operation from ApeosWare Management Suite.



Note

When setting the authentication information of Salesforce, access the [User/Service Settings] menu of ApeosWare Management Suite via HTTPS. If accessed through HTTP, the authentication information cannot be set.

For SharePoint Online

Access the [User/Service Settings] menu of ApeosWare Management Suite via HTTPS connection.

When [Authenticate] or [Edit Recipient] in the Settings screen of SharePoint Online is clicked, [Set Authentication Information] that requires a token of SharePoint Online is displayed.

When [Get] is clicked, the message of "Do you trust ApeosWare Management Suite?" of SharePoint Online is displayed.

Click [Trust It] to retrieve a token.

Click [Save] in [Set Authentication Information] of ApeosWare Management Suite.



Note

- To set the authentication information of SharePoint Online, access the user screen of ApeosWare Management Suite via HTTPS. If you access via HTTP, you cannot set the authentication information.
- The authentication information needs to be set per site to be registered.

Confirm Scan Job Status

How to Display

Select [Print/Job] > [My Scan Jobs] > [Scan Job List] on the user screen.

Page Descriptions

It is the same as with [Scan Job Status] of the administrator screen.

For details, refer to "Scan Job Status" (P.299)

Other Settings

We describe the other settings to use the simple flow feature.

Device and Device Group Settings

The device you use is required to be registered in ApeosWare Management Suite. Set [Authentication/Accounting Mode] of the device group to which the registered device belongs to one of the following.

- Local Authentication/Local Accounting (Local Authentication)
- Local Authentication/Network Accounting (Network Authentication)
- Remote Authentication

Select [ApeosWare Authentication Agent] in the authentication system.

- Custom Authentication

In addition, set the device group properties so as to display the ApeosWare Management Suite menu on the control panel of the device.



Refer

Details of device settings→“Device Group List (Details of Device Group/Sub-Device Group)” (P.90)

Device Body Settings

Refer to “Using Custom Service” (P.120), and configure the necessary settings with the device.

Temporary Folder Settings

Set the temporary folder on [System Settings] > [Temporary Folder Settings] in ApeosWare Management Suite. This folder will be used to send and receive data to and from the device.



Note

When operating the ApeosWare Management Suite server with the WORKGROUP environment, you are required to create the temporary folder on the ApeosWare Management Suite server and to set the access permission to Network Service.



Refer

“Temporary Folder Settings” (P.48)

Setting File Management Service

Set so as to enable access to the file management service from the ApeosWare Management Suite operation environment. Setting a firewall or a proxy server is required depending on the linking file management service.

In addition, registering the user using the simple flow feature in the linking file management service, retrieve the authentication information.



Note

When accessing the file management service provided as a cloud service by HTTP proxy, specify the server name and the port number of the proxy server in both settings of the web browser and ApeosWare Management Suite.

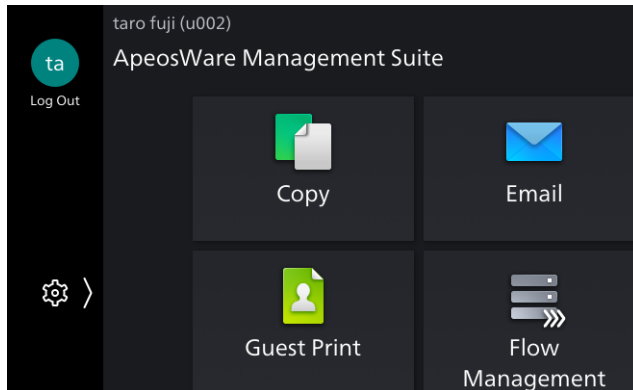
How to Operate the Device

How to operate a simple flow feature is described as below.

Menu Window

Configuring the required settings on the device causes the device control panel to display the ApeosWare Management Suite menu.

Selecting the ApeosWare Management Suite menu displays the features available for the users who are authenticated with the device.



We describe here the following menus.

- [Email]
This is the menu to send an email with a scanned document attached.
- Icon with File Management Service Name
This is the menu to access the file management service. The menu is displayed by each file management service set already.

The user, setting previously the authentication information with a web browser, is not required to enter the authentication information on the control panel of the device. Note that if the period of the authentication information has been expired or changed, the user may be requested to enter it. In such a case, enter the authentication information.

When linking with Salesforce or Google Drive, you are required to access each setting window from the user window of ApeosWare Management Suite, and then re-set the authentication information.



Refer

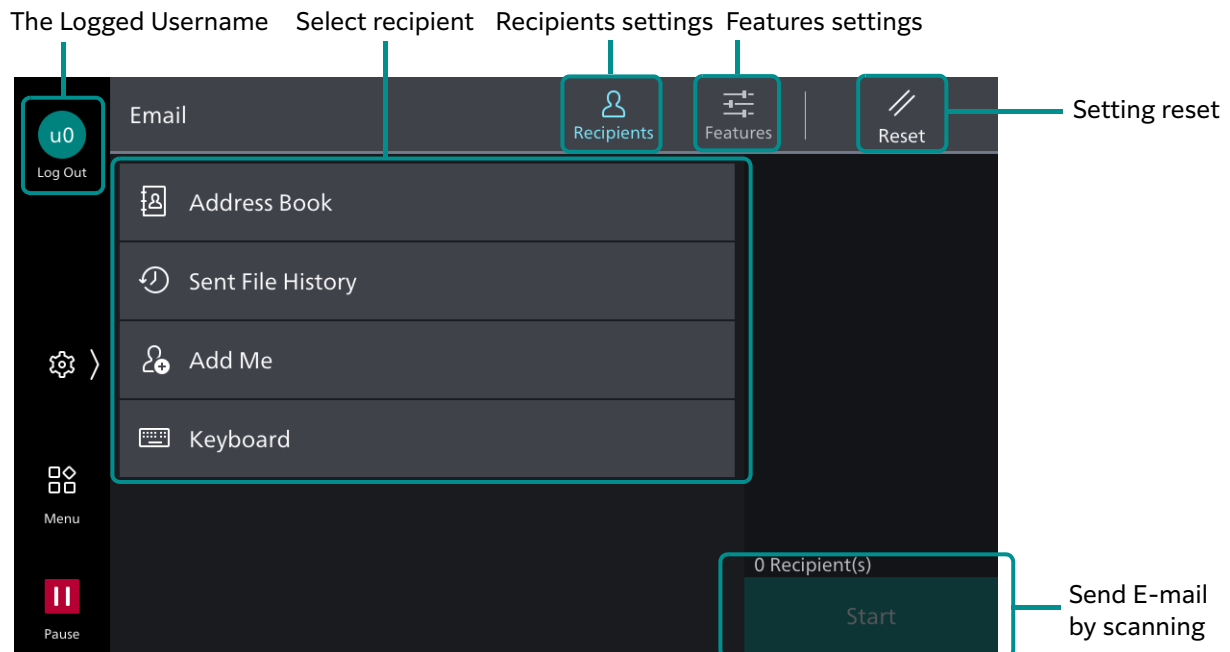
"Set Authentication Information to File Management Service" (P.300)

Restrictions in Scanning

Some models may not start scanning even if you use [Next Original] in scanning. In this case, return to the menu window, and resume scanning.

Email a Scanned Document

1. Following the settings, perform the authentication.
2. Push [Email] on the menu window.
[Email] is displayed.



- Select recipient
A user added first is added to To. Then if you want to change a recipient, by selecting the recipient, it is possible to switch to Cc or Bcc. A recipient can be added using the following three methods.
 - Push the Address Book button, and add the recipient from the list of users registered in ApeosWare Management Suite.
 - Select the recipient from the sent history.
 - Push Keyboard to display the keyboard, and enter the email address in the text box.
- Clicking "Add yourself" adds the standard email address of the logged in user to the recipient.
- Recipients settings
The recipients of the email to be sent can be edited. The sender's email address is enables to change only when it is allowed by the access profile.
- Features settings
The content of the email to be sent and the scan read settings can be changed.

3. Set the document on the device, and push [Start].



Note

When the preview setting is enabled, the label changes from [Send] to [Preview].

Link with File Management Service

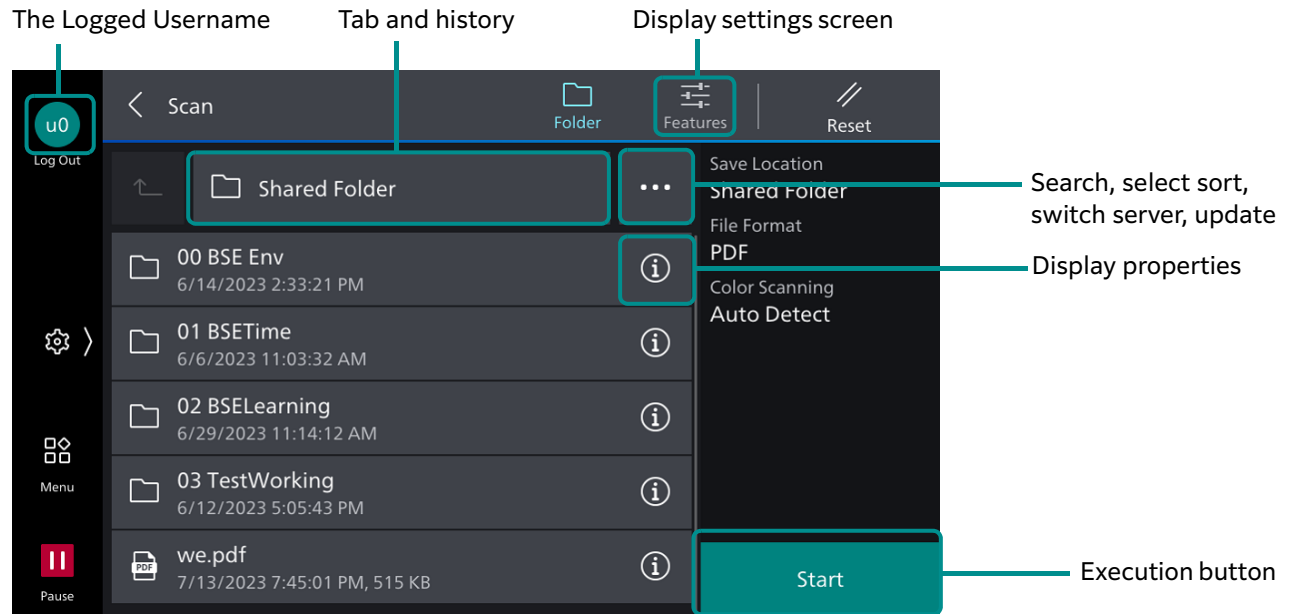
Access File Management Service

1. Following the settings, perform the authentication.

2. Perform the following procedure.

Select [Print] or [Scan].

The file management service folder and the file list are displayed.



• Tab

The sharing tab and the private tab are displayed. The tab name is assigned following the specifications on the file management service.

The list of the folder and the folder file the login user has the access permissions is displayed on each tab. In the case of FUJI XEROX ApeosPort-VII or later, also the history of operations is displayed.



Note

- The private tab may be displayed depending on the settings.
- When a shared folder is connected, the folder specified as [Storage Location] set on [User Properties] of the logged in user is displayed on the [My Folder] tab. Only UNC format of folder path can be set to [Storage Location].
- When connecting to DocuShare, ApeosWare Management Suite will be displayed in English even when the display language is set to Thai.
- In the initial state, [Sharing Tab] is shown first.
By overwriting the configuration file, you can select the initially appearing tab for each file management service.

Location of configuration file: {InstallFolder}\WebApp\MFD\ScanAndConnector.config

Setting method: <add key="ChangeRootLocationTab" value="{File management service ID}"/>

The file management service IDs are as shown below.

Shared Folder	1011
SharePoint	1012
DocuShare	1013
Salesforce	1014
Google Drive	1016
OneDrive	1020

SharePoint Online	1021
ABBYY FlexiCapture	1022

Example: When switching the display order of Sharing Tab and Private Tab for Shared Folder and OneDrive

```
<add key="ChangeRootLocationTab" value="1011,1020" />
```

- By overwriting the configuration file, you can skip the selection of [Print] or [Scan] for each file management service.

Location of configuration file: {InstallFolder}\WebApp\MFD\ScanAndConnector.config

Setting method:

1. When using Scan only: <add key="ScanOnly" value="{File management service ID}" />

2. When using Print only: <add key="PrintOnly" value="{File management service ID}" />

The file management service IDs are same as in the table above.

Example: When using Scan only with Shared Folder and OneDrive

```
<add key="ScanOnly" value="1011,1020" />
```

- Switch server

When multiple servers are registered, switch the server to access. When "Switch server" is selected from the menu that appears when the  icon is clicked, a list is displayed showing the servers that the logged in user can access.

- Select sort

From the menu that appears when the  icon is clicked, you can select "Select sort", and choose a different sorting method from name, update date/time, and size by selecting from the displayed button.

- Search

From the menu that appears when the  icon is clicked, selecting "Search" displays the search screen.

You can search by entering the character string included in the file name or the folder name. Pushing [Advanced Search] enables you to search specifying multiple conditions, such as the file title and the owner. Advanced Search searches the folder and the subfolder displaying. Search conditions you can specify vary depending on the file management service.

- Property Button

The property window of the file is displayed.



"Confirm File Properties" (P.308)

- Execution button

This executes a process.



- [New Scan], [Update Scan]→"Store Scanned Document in File Management Service" (P.307)
- [Print]→"Print a File in File Management Service" (P.307)
- [OK]→When [Scan] has been selected in Step 2 in "Access File Management Service" (P.305), refer to "Store Scanned Document in File Management Service" (P.307). When [Print] has been selected, refer to "Print a File in File Management Service" (P.307).

Store Scanned Document in File Management Service

1. Select [Scan] in Step 2 in "Access File Management Service" (P.305) and then push [OK] on the file list screen.



Note

- To perform [Update Scan], simply select the file on the list. The file selected is overwritten on the scanned document. To confirm the file contents before overwriting, perform the check on the property window. For [New Scan], the scanned document is stored in the folder being displayed. How to treat the original file varies depending on the linking file management service, such as delete, stored in trash box and being an old version file.
- You can use the following reserved character strings for [Document Name] of [New Scan].
 - [\$YYYY] (Year data of the time to start uploading to file management service (4 digits))
 - [\$MM] (Month data of the time to start uploading to file management service (2 digits))
 - [\$DD] (Day data of the time to start uploading to file management service (2 digits))
- With FUJI XEROX ApeosPort-VII or later, a new scan is performed when you have selected the folder then pushed [OK], and a update scan is performed when you have selected the file then pushed [OK].



Refer

"Confirm File Properties" (P.308)

2. Change the setting values if necessary.
You may not be able to change the value depending on the settings.
3. Set the document on the device, and push [scan].
The cost confirmation display may be displayed depending on the settings after finishing the process.



Note

- When there is a document whose name is the same as the scanned document in the storing location, the storage methods vary depending on the file management service.
- When it is connected with DocuShare, if you select the file locked, you cannot resume to scan it.

Print a File in File Management Service

1. Select [Print] in Step 2 in "Access File Management Service" (P.305), select a file on the file list screen, and then push [OK].
You can select multiple files.
To confirm the file contents before printing, confirm it on the property window.



Refer

"Confirm File Properties" (P.308)

2. Change the print settings as necessary, and push [Print].
The cost confirmation display may be displayed depending on the settings after finishing the process.



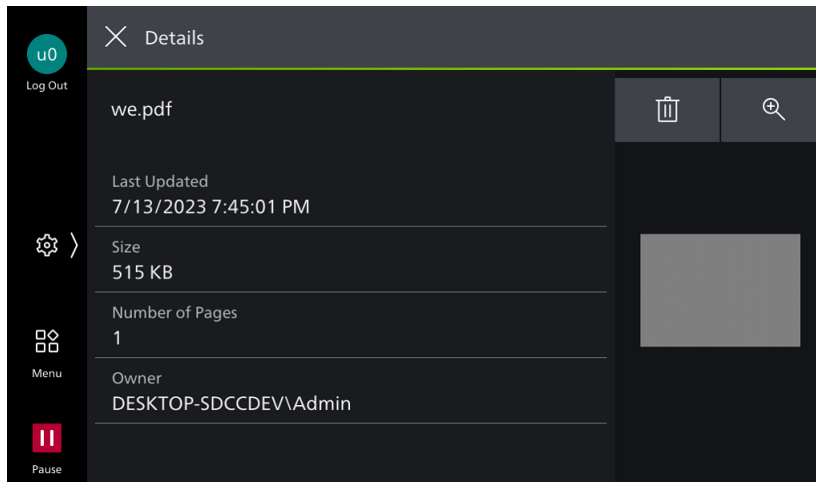
Note

To print a DocuWorks document, the paper tray is fixed to [Auto] and cannot be changed.

Confirm File Properties

You can confirm the file properties before printing or resuming scanning.

1. Push the property button of the file you want to confirm on the file management service window.
2. The properties, such as an updated date and the size of the file, are displayed.
A preview screen appears depending on the file format, and you can check the content.



3. Perform the process as necessary.
You can perform either [Delete] or [Print].



Note

Once you execute [Delete], the file stored in the file management service will be deleted. The deleted file is moved to the trash box depending on the file management service, but you cannot access the trash box from ApeosWare Management Suite. To restore the file moved to the trash box, access directly the file management service and perform it.

9 Mobile Device Settings and Operations

Preparations

ApeosWare Management Suite Settings

Access ApeosWare Management Suite with administrator permission, and register the device to be used and the user information. Create a print queue if necessary.

Install Application for a Mobile Device

Download the Mobility application corresponding to the mobile device you use, and install it.
Application name: ApeosWare MS Mobile 2

Preparation for using an NFC tag

To use an NFC tag to associate the device with the mobile device, set the following settings.

Mobile Device Settings

Enable NFC features on wireless network setup on the mobile device to be used.

NFC Tag Settings

Write the identification information of the device to the NFC tag.

Put an NFC tag seal which is sold separately to the device to be used previously.



Note

Once information has been written in an NFC tag, you cannot change it.

1. Start ApeosWare MS Mobile 2, and then log in with System Manager permissions for ApeosWare Management Suite or by the user with management permissions for the device.



Refer

"Login" (P.310)

2. Hold the mobile device over the NFC tag seal of the target device.
The list of devices associated with the login user is displayed on the ApeosWare MS Mobile 2 screen.
3. Select the target device from the dropdown list box.
4. Write the device information.

Prepare QR Code

You are not enabled to display a QR code on the control panel of the device for the following devices.

- The device whose [Authentication/Accounting Mode] is set to other than [Custom Authentication]
- The device without a control panel

For those devices as mentioned, print the QR code previously. You can create the QR code following the steps as below.

1. Select [Service Settings] > [Device Management] > [Device List] on the administrator screen of ApeosWare Management Suite.
2. Displaying the properties of the target device, confirm [Model Code] and [Serial Number].
3. Using any QR code creation tool, create the QR code for "{Model Code} _ {Serial Number}".
For example, when the model code is "AB123456" and the serial number is "111111", create the QR code, "AB123456_111111".
4. Print the QR code you have created.



Note

We recommend you to put the QR code created to the device in order to read it with the mobile device.



Refer

- Device Registration and Settings→"3 Device Management" (P.75)
- Creation of a Print Queue→"7 Print Management and Operations" (P.250)

Install Application to Display a File

For the mobile device with Android OS, when displaying the file contents, install the preview application corresponding to the file format.

Operating Mobile Device

This section describes the outline of the operation to use ApeosWare Management Suite features from a mobile device.

Login

Tapping the icon of ApeosWare MS Mobile 2 displays the login window to ApeosWare Management Suite.



Note

- When activating ApeosWare MS Mobile 2, if a window appears requesting for the permission of notification from the ApeosWare Management Suite server, allow the notification.
- When logging in with ApeosWare MS Mobile 2, if an alert message "Communication is not protected. Do you want to connect?" appears, you are required to take measures by, for example, installing a certificate on the mobile device. Take measures by referring to the support page.

[User Name]

Enter the "User ID" registered in ApeosWare Management Suite.

Select a Server

The ApeosWare Management Suite server information searched on the network is displayed. If multiple servers are displayed, select the server you want to log in. If any server could not be found by the search, manually enter the IP address of the ApeosWare Management Suite server.



Note

The number of users who can log in to ApeosWare Management Suite at the same time is controlled by Mobile User License.

Menu Window

Logging in, and the menu window is displayed.

Menu Names	Descriptions
General feature	The menu to operate the file and the camera feature in the mobile device is displayed. The following menus will be displayed. • Album • My Document • Camera
Service feature	The menus to access ApeosWare Management Suite features are displayed.
File Management Service	The menus to access a file management service are displayed.



Note

The feature and the file management service allowed by the access profile only are displayed.

Property Window

Tapping  on the menu window causes the property window to appear.

We describe here the items to be displayed on the property window.

Items	Descriptions
User	The login user name and the mail address are displayed.
Account	This is displayed when it is on Cost Management. The account the user can use is displayed.
Use mobile data communication	Set whether to restrict sending a print job and uploading to or downloading from the file management service. In the default settings, they are restricted.  Note When the mobile device connects to a network by Wi-Fi, even if the settings restrict data forwarding, it is not applied.
SSL verification during communication	When set, the certificate is verified in a communication.  Note If not set, you can change the setting so as to verify the certificate.
OSSLicense	OSSLicense is displayed.
Log out	The user is logged out from ApeosWare Management Suite.

[General Feature]

You can operate the file and the picture in the mobile device and the picture taken by the OS's camera feature.

The features available are the following.

- Printing
- Upload
Is available when it links with a file management service.
- Delete

The file that can be operated and the feature available vary depending on the OS of the mobile device.

[Album]

You can operate the file and the picture in the mobile device and the picture taken by the OS's camera feature.



Note

If a window appears requesting the access permission to the album feature from ApeosWare MS Mobile 2, allow the access.

[My Document]

You can operate the following files.

OS	Files that Can Be Operated
Android	All the files to be stored in the mobile device
iOS	All the files to be downloaded from the stored in the file management service

[App Storage]

You can operate the following files.

OS	Files that Can Be Operated
Android	• All the files to be downloaded from the stored in the file management service • Files taken with the camera in the app

[Camera]

The camera feature in the mobile device starts. You can print and upload the picture you have taken.



Note

If a window appears requesting the access permission to the camera feature from ApeosWare MS Mobile 2, allow the access.

[Service Feature]

You can operate the features of ApeosWare Management Suite.

[Log in with QR code]

Shows the window of log-in QR code reader screen. Read the log-in QR code to log in to the device. Log-in QR code requires mobile app setting by selecting [Service Settings] > [User Management] > [Authentication Settings].



Refer

"Read the login QR code displayed on the device and register the external ID." (P.197)

[Print On Demand]

The print job list sent by the login user with Print On Demand is displayed. Selecting one or multiple jobs enables you to execute "Print On Demand".

For details on Print On Demand, refer to "Details of Print On Demand" in "Installation and Operation Guide".

[Email]

Emails a scanned document.



Refer

For items other than the email settings, refer to "[Scan Settings] tab" (P.292).

[Email Settings]

Set here the address, the subject and the body of the email attaching a scanned document.

- Address

When [Add user address to recipient] in [Email Settings] of ApeosWare Management Suite is enabled, the email address set to the user information of the login user is displayed.

To specify the recipient, enter the email address directly. You can enter multiple email addresses with semicolon (;) separated.

- Subject and Body

[Email Subject] and [Email Content] set in [Email Settings] of ApeosWare Management Suite by the administrator are displayed.

You can change it to any character string as necessary.

[File Management Service]

The menus to access a file management service are displayed.

Only the menu of the file management service allowed by the access profile is displayed.

When you have set the authentication information previously by [File Management Service Settings] on the ApeosWare Management Suite user screen, you can log in to the file management service by selecting the menu. If you have not, the log in window appearing, enter the authentication information of the file management service and log in.

The entered authentication information stored, you can omit it from the next time.



Note

To link with Google Drive, Salesforce, OneDrive, or SharePoint Online, it is required to set the authentication information in advance. If an error messages appears when selecting the menu, access ApeosWare Management Suite with a web browser and set the login information.

The operations available are as follows.

- Printing

You can print the file selected.

- Upload or Revise

When the file has not been selected, [Upload] is displayed. When it has been selected, [Revise] is displayed.

The file selected is overwritten by the file to be uploaded by performing [Revise].

You can upload pictures taken by the camera feature and scanned documents as well as files in the mobile device.

When the file with the name which is the same as the name of the file to be uploaded exists in the uploading location, the operation will follow the specifications of the file management service connected.

- Download

When the file with the name which is the same as the name of the file to be downloaded exists in the downloading location, “-{YYYYMMDD}_{HHMMSS}” is added at the end of the file name, and it is stored as another file.



Refer

“Set Authentication Information to File Management Service” in “Installation and Operation Guide”

Select a Device

In executing a print job or a scan job from each feature, the setting window is display.

Select the device you use on the setting window. You can select one by any of the following.

- Use QR code

Tapping [Scan QR] causes the window of QR code reader to appear. Reading the QR code displayed on the control panel of the device enables you to select the device.



Note

When the device doesn't have a control panel, create the QR code and print it.



Refer

“Preparations” (P.309)

- Use NFC Tag

When the OS of the mobile device is Android, you can select the device by this procedure.

For the mobile device available to use the NFC feature, the icon showing the NFC tag reading feature on the setting window is displayed. While this icon remains been displayed, hold the mobile device over the NFC tag seal put on the device.



Note

It is required that the NFC tag seal on which the identification information has been written be put on the device previously.



Refer

“Preparations” (P.309)

- Select from the devices that are registered in ApeosWare Management Suite.

When performing a print job, you can select the device by this procedure.

Tapping [Print] on the print setting window causes the [Select Queue/Device] window to appear. Determine whether to select the print queue on the device belonging to the device group you specify.



Note

When selecting the device not belonging to the device group, select “Unaffiliated” on the device group.

Use ApeosWare MS Mobile 2 from Mobile App

From the following mobile apps, you can start ApeosWare MS Mobile 2 and perform printing/upload.

iOS

- Long-push the file attached to the email, and then select ApeosWare MS Mobile 2.
- Push the share button of the web page displayed in Safari, and then select ApeosWare MS Mobile 2.

For Android

- Select a file (extension: png, jpeg, jpg, bmp, gif) in the Photo app, and then push "Send File" and select ApeosWare MS Mobile 2.
- From the share menu of the web page that is displayed in Chrome, select ApeosWare MS Mobile 2.

A document containing any of the characters "¥ / : * ? " < > | ' &" in the name cannot be printed.

Also, a correct operation is not guaranteed when print/upload is attempted using a mobile app other than described above.

10 Image Log Control

Settings and Confirmation in a Web Browser

You can set the settings for the image log and confirm them with a web browser. This section describes what you can do with each page.

- [Service Settings] > [Image Log Control]

Types of Pages	Descriptions
Extract/Save Settings	Displays the setting items regarding extraction processing and save.  Refer "Extract/Save Settings" (P.317)
Archive/Delete Settings	Displays the setting items regarding archive/delete settings.  Refer "Archive/Delete Settings" (P.320)
Restore Archive	Displays the items regarding restoration of archive.  Refer "Archive/Delete Settings" (P.320)
Image Log Monitoring Setting	
Monitoring Start Time	Sets the time to start image log monitoring.  Refer "Monitoring Start Time" (P.323)
Monitoring Pattern	Sets the filter pattern used for image log monitoring.  Refer "Monitoring Pattern" (P.324)
Monitor Settings	Creates and manages monitor settings.  Refer "Monitoring Settings" (P.324)
Common Settings	Sets the password of an image log storage access user.  Refer "Common Settings" (P.329)

- [Device/Job Status] > [Image Log Status]

Types of Pages	Descriptions
Image Log Receiving Status	Displays the reception status of image logs.  Refer "Image Log Receiving Status" (P.330)

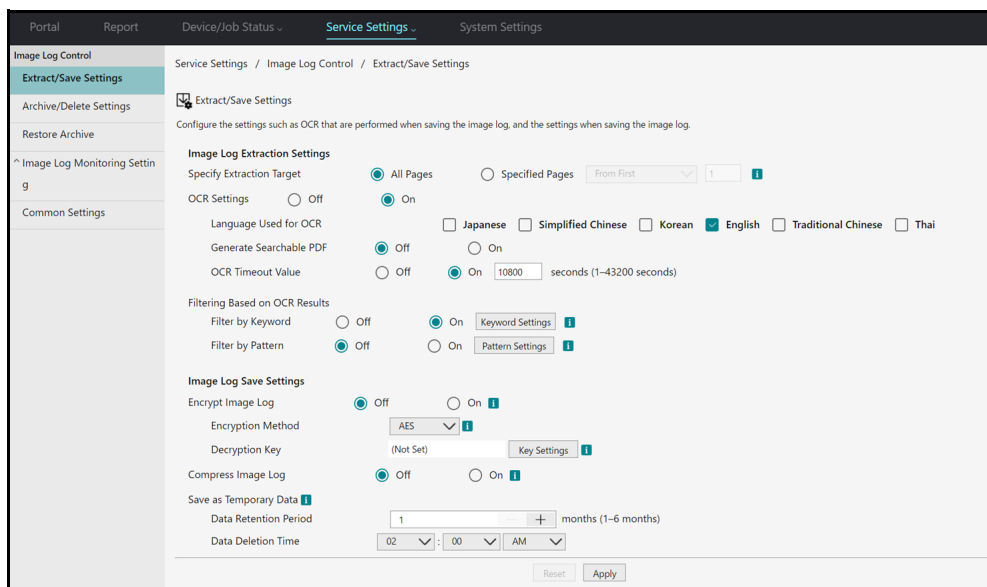
Extract/Save Settings

How to Display

Select [Service Settings] > [Image Log Control] > [Extract/Save Settings] from the menu on the administrator screen.

Page Summary

Makes settings regarding extraction processing and save.



[Specify Extraction Target]

Select the extraction pages from [All Pages] or [Specified Pages].

When selecting [Specified Pages], select any of the following items and specify the pages for extraction processing.

- [From First]
When selecting [From First], specify the number of pages from the first page as the pages for extraction processing.
- [From Last]
When selecting [From Last], specify the number of pages from the last page as the pages for extraction processing.
- [Specify Range]
When selecting [Specify Range], specify the range of extraction processing with the page numbers.



- The following settings are available only for the extraction target pages specified with this item.
- Regardless of the method of specifying pages, the specifiable page numbers are integers from 1 to 1000.

[Extract Text Information by OCR]

Select [Yes] or [No] for whether or not to extract text information by OCR. When selecting [Yes], you can set [Language], [Generate Searchable PDF], and [Timeout Value].

[No] is selected in the default settings.

This setting is enabled from the first job after change is made.

[Language]

Select the language used for OCR processing from the following options. You can select multiple options.

- Japanese
- Simplified Chinese
- Korean
- English
- Traditional Chinese
- Thai

Japanese is selected in the default settings.

This setting is enabled from the first job after change is made.



Note

- If too many languages are selected, there are cases where the processing accuracy is lowered and/or processing takes time.
- When using OCR Option of OmniPage, only one language can be selected.
- When using the OCR feature on an image log receiving server with distributed configuration, an ABBYY OCR license or Scan OCR Option license is required.
- When using ABBYY OCR in all-in-one configuration, an ABBYY OCR license is required.
- When using OmniPage OCR in all-in-one configuration, a Scan OCR Option license is not required.
- For the registration destination of an ABBYY OCR license and Scan OCR Option license, refer to "Setup Guide."

[Generate Searchable PDF]

Select [Yes] or [No] for whether or not to enable string search when saving an image of image log as PDF.

[Yes] is selected in the default settings.

This setting is enabled from the first job after change is made.



Note

When [Yes] is selected, processing may take time.

[Timeout Value]

Select [Off] or [On] for whether or not to timeout OCR processing. When selecting [On], enter the timeout value in seconds. The specifiable range is 1 to 43200 seconds (12 hours). When this value is exceeded, OCR processing is stopped. The default value is [10800 seconds] seconds (3 hours).

This setting is enabled from the first job after change is made.

[Filtering by Keyword]

Select [Off] or [On] for whether or not to conduct filtering by keyword on OCR processed image log images. When selecting [On], only the image logs containing any of the keywords specified in [Keyword Settings] are saved. Whether the strings of OCR results contain the keywords is judged. The image logs that do not contain the keywords become targets of temporary data and will be deleted after the period specified in [Save as Temporary Data] passes.

Click [Add Keyword] in the [Filter Keyword List] screen and enter keywords. When you finish entering keywords, click [OK].

When you finish adding keywords, click [Close] to return to the [Extract/Save Settings] screen.



Note

- Up to 100 keywords can be registered.
- One keyword can contain up to 256 characters in double-byte or single-byte characters.
- You can search the registered keywords with keywords and update date using .
- To edit keywords, click  and select [Edit].
- When deleting a keyword from the list, place a check mark in the checkbox on the list, and then click [Delete]. Or click  and select [Delete].
- When using both [Filtering by Keyword] and [Filtering by Pattern], only the image logs that become save targets of the both settings are saved. The image logs that do not become save targets of either setting and those that do not become save targets of neither settings become temporary save targets.
- Filtering by keyword does not guarantee 100% accuracy.

[Filtering by Pattern]

Select [Off] or [On] for whether or not to conduct filtering by pattern (regular expression) on OCR processed image log images. When selecting [On], only the image logs containing any of the patterns specified in [Pattern Settings] are saved. Whether the strings of OCR results contain the patterns is judged. The image logs that do not contain the patterns become targets of temporary data and will be deleted after the period specified in [Save as Temporary Data] passes.

Click [Add Pattern] in the [Filter Pattern List] screen and enter [Pattern Name] and [Filter Pattern]. When you finish entering, click [OK].

When you finish adding patterns, click [Close] to return to the [Extract/Save Settings] screen.



Note

- Up to 100 patterns can be registered.
- One pattern name can contain up to 40 characters in double-byte or single-byte characters.
- One filter pattern can contain up to 256 characters in double-byte or single-byte characters.
- You can search the registered patterns with a pattern name, filter patterns and update date using .
- To edit patterns, click  and select [Edit].
- When deleting a pattern from the list, place a check mark in the checkbox on the list, and then click [Delete]. Or click  and select [Delete].
- When using both [Filtering by Keyword] and [Filtering by Pattern], only the image logs that become save targets of the both settings are saved. The image logs that do not become save targets of either setting and those that do not become save targets of neither settings become temporary save targets.
- Filtering by pattern does not guarantee 100% accuracy.

[Encrypt Image Log]

If you encrypt and save image logs, select [Yes].

When selecting [Yes], select the encryption method and enter a key to [Encryption/Decryption Key].

Enter the same key to the re-entry field.

When selecting [No], click [Key Settings] according to need and enter [Decryption Key]. (For instance, when encrypted data is already saved, etc.)



Note

- A key can contain 8 to 63 characters in single-byte alphanumeric characters.
- When [No] is selected or [Encryption/Decryption Key] has been set, enter a key in the Key Settings/Change dialog box.
- When the decryption key is changed, the image log encrypted by the setting before change is made cannot be decrypted. Change the decryption key only if it is all right.
- Even when [No] is selected, select the encryption method according to need.

[Compress Image Log]

If you compress and save image logs, select [Yes].

When the image log compression feature is enabled, there are cases where image quality is partially deteriorated or color hue is changed in comparison with those before compression. For this reason, disable the image log compression feature when you place importance on the reproductivity of image quality and color hue.

[Save as Temporary Data]

Temporarily save the data that become deletion targets as a result of filtering by keyword and pattern. You can check and save temporarily saved data by Search Image Log.

You can set the save period and deletion time. The specifiable range of the save period is 1 to 6 months.

The specifiable range of the data deletion time is 1:00 to 12:59 am or pm. The default value is [02] hour [00] minute [AM].

The deletion timing is shown below.

- Date when the setting time comes for the first time after the deletion time setting is changed
- Date when the setting time comes for the first time after Log Management Core Service is started



Note

In the case of distributed configuration, the date when the setting time comes after the relevant service in the image log core server is started

- 2nd of each month



Note

Regarding the processing execution date, the “date when the setting time comes for the first time” refers to that day if the setting time is after the time of the change and the next day if it is before the time of the change.

Archive/Delete Settings

How to Display

Select [Service Settings] > [Image Log Control] > [Archive/Delete Settings] from the menu on the administrator screen.

Page Summary

Configures the save period of image logs and image log processing method after the save period is ended.

The screenshot shows the 'Archive/Delete Settings' page within the 'Service Settings' section. The breadcrumb trail is 'Service Settings / Image Log Control / Archive/Delete Settings'. The page title is 'Archive/Delete Settings'. Below the title, there is a description: 'Sets the image log retention period, and the image log processing method after the retention period.' The 'Image Log Retention Period' is set to '12' months (range 1-60 months). The 'Archive/Delete' method is set to 'Archive' (radio button selected). The 'Archived/Deleted On' time is set to '02' hours, '00' minutes, and 'AM'. There are 'Reset' and 'Apply' buttons at the bottom right.

[Image Log Retention Period]

Specify the image log retention period in months. The specifiable range is 1 to 60 months. The default value is [12] months.

The value specified in this field is enabled at the first archive or deletion after the setting is done.

[Archive/Delete]

Select processing on the image logs of which [Image Log Retention Period] passes from the followings.

- Archive
Move the logs from the database to specified folder.
- Delete
Delete the logs from the database.

[Archive] is selected in the default settings.

[Archived/Deleted On]

Specify the time to start archive or deletion of the image logs of which [Image Log Retention Period] passes in the range of 1:00 to 12:59 am or pm. The default value is [02] hour [00] minute [AM].

The execution dates of processing are as follows:

- Date when the setting time comes for the first time after the [Archived/Deleted On] setting is changed
- Date when the setting time comes for the first time after ApeosWare Management Suite Image Log Management Core Service is started
- 1st of each month

The path of the folder to which archived data is moved is as follows:

{Image Log Save Folder}\exported

{Image Log Save Folder} is specified upon setup. For details, refer to "Setup Guide."



Note

- In the destination of archived data, a folder with the date is created, and the archived data is stored in it. This date folder can be moved to any storage. To restore the archived data, however, it is necessary to return the data to the original folder.
- Regarding the processing execution date, the "date when the setting time comes for the first time" refers to that day if the setting time is after the time of the change and the next day if it is before the time of the change.

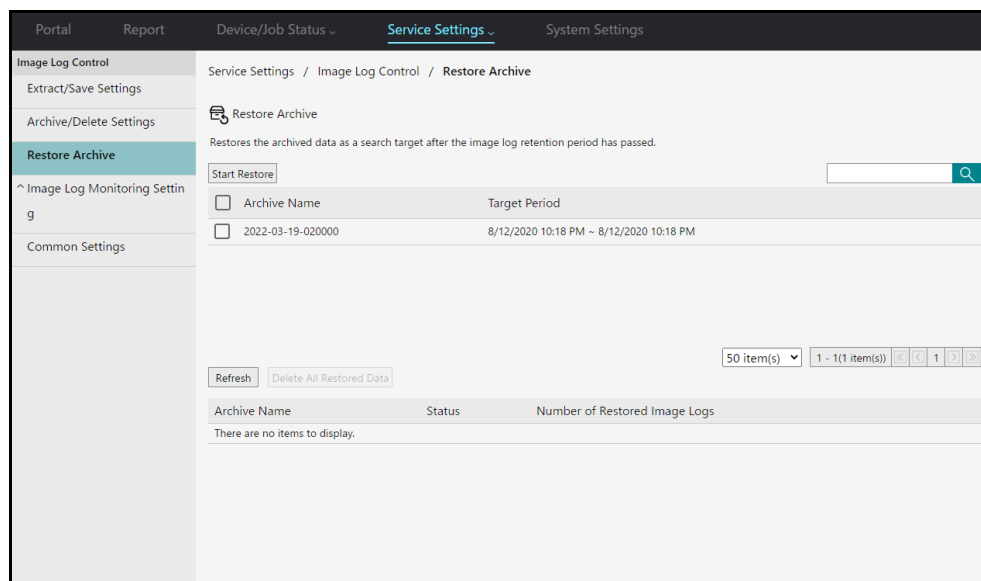
Restore Archive

How to Display

Select [Service Settings] > [Image Log Control] > [Restore Archive] from the menu on the administrator screen.

Page Summary

Restores data archived after the image log retention period is expired as search targets.



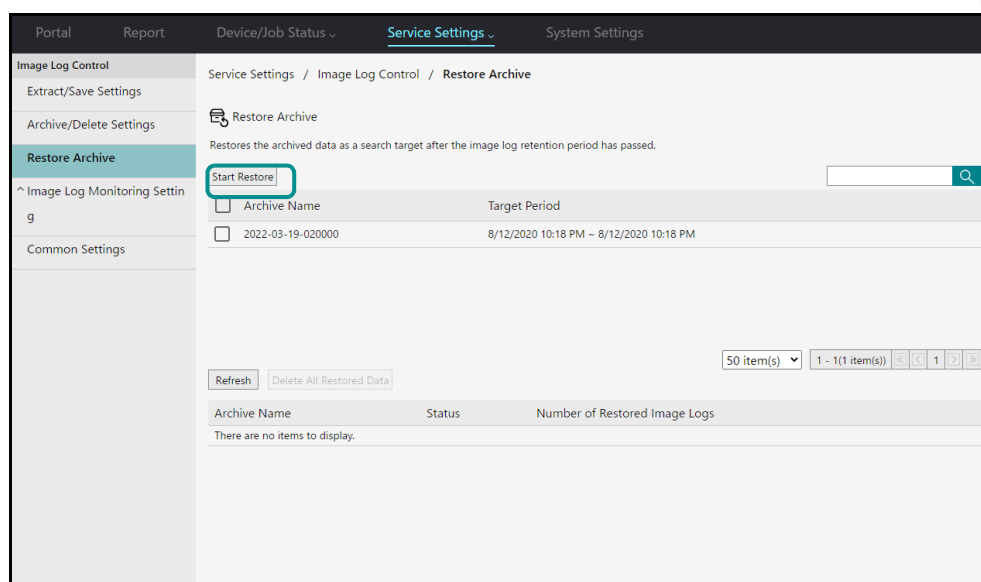
Restoring Archive

1. Select the checkbox of the archived data to restore and click [Start Restore].



Note

- If other user is conducting restoration, the archived data cannot be restored.
- It may take time for restoration processing. Even if you log out from Apeosware Management Suite during restoration processing, you can check the latest information of restoration processing next time you log in.
- You can select up to 12 files at a time.
- You can search archived data with the archive name and target period using



Data restoration starts.

2. Click [Refresh] and check the status of restoration processing.

Portal Report Device/Job Status Service Settings System Settings

Image Log Control

Service Settings / Image Log Control / Restore Archive

Restore Archive

Restores the archived data as a search target after the image log retention period has passed.

Start Restore

Archive Name	Target Period
2022-03-19-020000	8/12/2020 10:18 PM ~ 8/12/2020 10:18 PM

50 item(s) 1 - 1(1 item(s))

Refresh Delete All Restored Data

Archive Name	Status	Number of Restored Image Logs
There are no items to display.		

When processing is not finished, click [Refresh] again after a while. Confirm that all the archived data is restored.

When restored data becomes unnecessary, click [Delete All Restored Data].



Note

- Restored data cannot be deleted unless [Delete All Restored Data] is executed. Other archived data cannot be restored if restored data remains. Delete restored data periodically so that restored data will not remain.
- Even if a restored image log is deleted, the archived data before restoration is not deleted, and therefore it can be restored again.
- You can search restored data with the archive name and status using at the bottom.

Monitoring Start Time

How to Display

Select [Service Settings] > [Image Log Control] > [Image Log Monitoring Setting] > [Monitoring Start Time] from the menu on the administrator screen.

Page Summary

Sets the time to start image log monitoring when Severity B or Severity C is set.

Portal Report Device/Job Status Service Settings System Settings

Image Log Control

Service Settings / Image Log Control / Image Log Monitoring Setting / Monitoring Start Time

Monitoring Start Time

Sets the time to start monitoring the image log according to the monitoring setting for Severity B or C.

Image Log Monitoring Time Daily 12 : 00 AM

Reset Apply

[Image Log Monitoring Time]

Set the monitoring start time in the range of 1:00 to 12:59 am or pm. The default value is [12] hour [00] minute [AM].

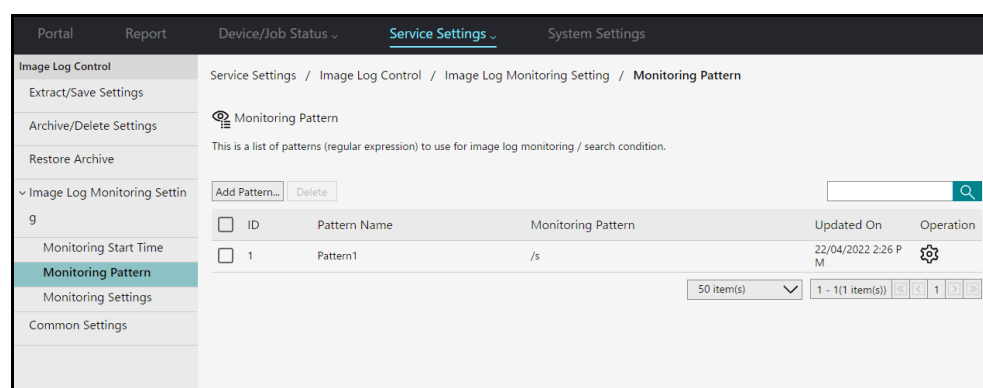
Monitoring Pattern

How to Display

Select [Service Settings] > [Image Log Control] > [Image Log Monitoring Setting] > [Monitoring Pattern] from the menu on the administrator screen.

Page Summary

A list of the created monitoring patterns is displayed. You can add, edit, and delete monitoring patterns.



Adding monitoring pattern

1. Click [Add Pattern].
2. Enter [Pattern Name] and monitoring pattern (regular expression) used for image log monitoring and click [OK].



Note

- Up to 100 monitoring patterns can be registered.
- One pattern name can contain up to 40 characters in double-byte or single-byte characters.
- One monitoring pattern name can contain up to 256 characters in double-byte or single-byte characters.
- You can search the registered monitoring patterns with a pattern name, monitoring patterns and update date using
- When deleting a monitoring pattern from the list, place a check mark in the checkbox on the list, and then click [Delete]. Or click and select [Delete].

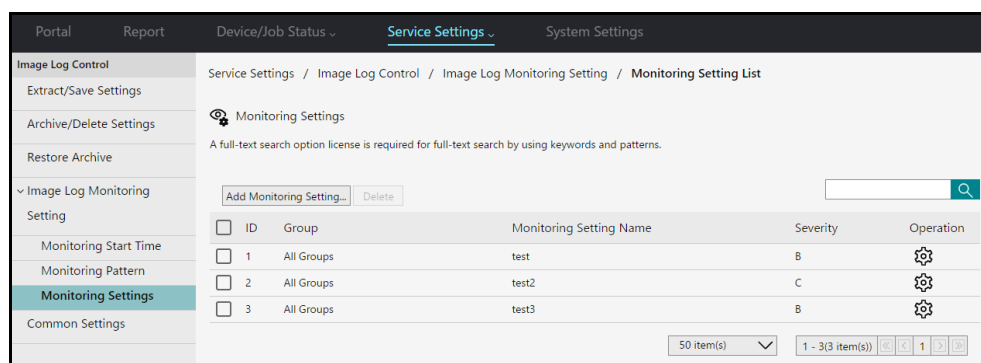
Monitoring Settings

How to Display

Select [Service Settings] > [Image Log Control] > [Image Log Monitoring Setting] > [Monitoring Settings] from the menu on the administrator screen.

Page Summary

A list of the created monitor settings is displayed. You can add, edit, and delete monitor settings.

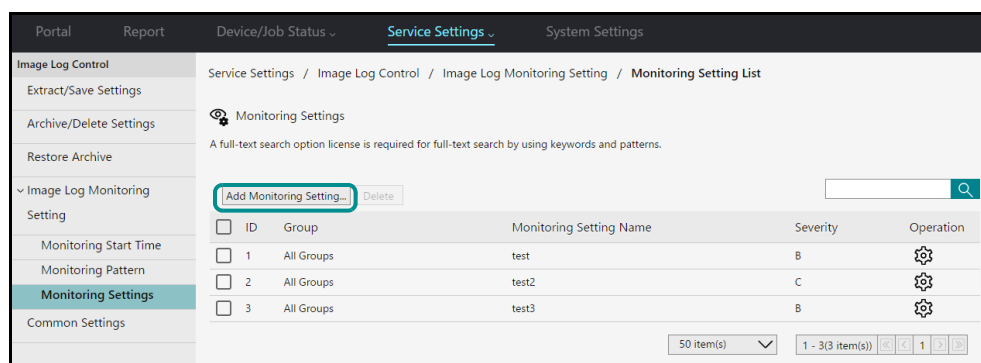


Note

Up to 500 monitoring settings can be set.

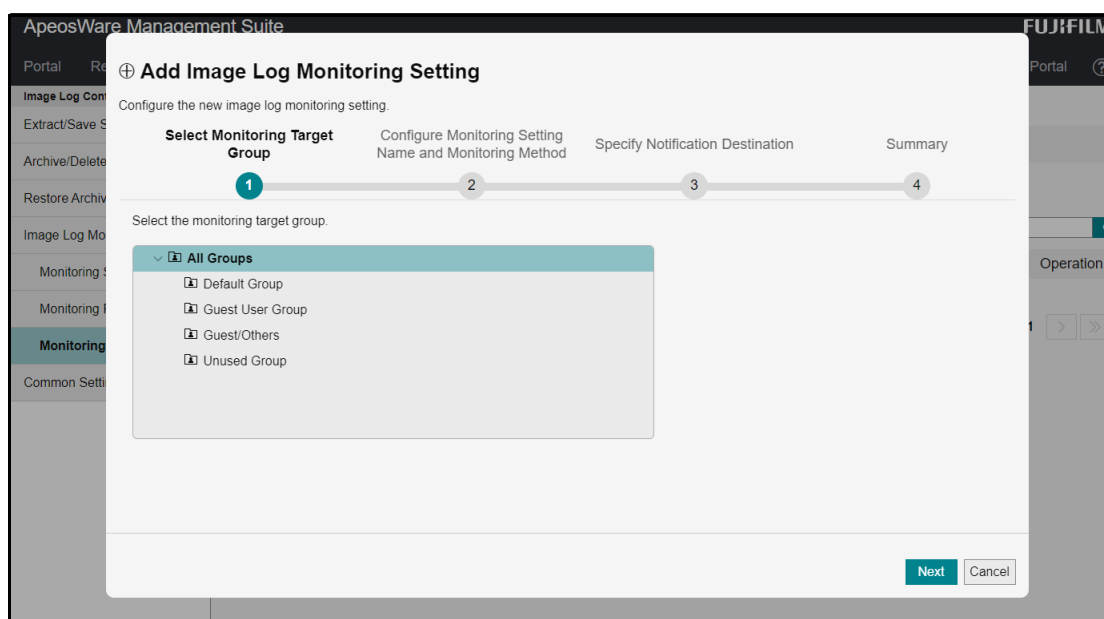
Adding monitoring settings

Click [Add Monitoring Setting].



(1) Selecting monitor target groups

Select monitor target groups and click [Next]. When users are not managed by group, select [All Groups].



(2) Configure monitoring setting name and monitoring method

Specify the following item, and then click [Next].

⊕ Add Image Log Monitoring Setting
Configure the new image log monitoring setting.

Select Monitoring Target Group **Configure Monitoring Setting Name and Monitoring Method** Specify Notification Destination Summary

Enter or select the monitoring setting and keyword/pattern.

Monitoring Target Group: Default Group

Monitoring Setting Name: *Required

Monitoring Method: ☐ Keyword ☒ Pattern (The one that matches any of the selected patterns will be the target)

Contains all of the following phrases: *Required

AND

Back **Next** Cancel

[Monitoring Setting Name]

Enter the monitoring setting name.

[Monitoring Method]

Select one or all of Keyword, Pattern, or Attribute conditions.

- **Keyword**
To use keywords, select the checkbox of [Keyword].
Enter the keywords that are included in image logs.
To specify multiple keywords, separate them with double-byte or single-byte space. You can use multiple languages specified in [Language Used for OCR].
Up to 256 character in double-byte or single-byte characters can be entered.
- **Contains all of the following phrases/Contains any of the following phrases**
When multiple keywords have been specified, select the join condition for the keywords between [Contains all of the following phrases] (AND condition) and [Contains any of the following phrases] (OR condition). In the default settings, [Contains all of the following phrases] is selected.
- **Pattern**
To use patterns, select the checkbox of [Pattern]. Select the checkbox of the pattern name to use. Patterns need to be registered in advance.
- **Attribute conditions**
Set the attribute and value of search conditions. Use or to add or delete attributes to be searched.



Refer

"Adding monitoring pattern" (P.324)

"Attribute conditions" (P.345)

(3) Specifying notification destination

Specify the following item, and then click [Next].

[Severity]

Select the severity of monitor settings from the followings.

- A (Monitor every 5 minutes and make notification)
Monitor every 5 minutes. When an image log that satisfies the condition is detected, it is notified by email immediately.
- B (Monitor once a day and make notification)
Monitor once a day at the specified time. When an image log that satisfies the condition is detected, it is notified by email immediately.
- C (Monitor once a day and not make notification)
Monitor once a day at the specified time. No notification is made by email.

In the default settings, [B (Monitor once a day and make notification)] is selected.

The execution time in the case of monitoring once a day is specified in "Monitoring Start Time" (P.323).

[Notification Email Address]

- Add the following email address to the Notification Address.
Enter the email address to which notification is sent when an image log contains the keywords. Up to 256 character in single-byte characters can be entered. This field cannot be entered in the case of Severity C.
- Add
Add the entered email address to [Notification Email Address]. Add the email address one by one.
- Notification Email Address
Email address to which notification is sent when an image log contains the keywords Up to 10 email addresses can be added. Up to 256 character in single-byte characters can be entered.



Note

Specify the email address of the image log administrator or user with the image log group administrator permission to the notification destination.

- Delete
Delete the email addresses selected in [Notification Email Address]. Multiple email addresses can be selected.

(4) Overview

After you check the configured setting, clicking [Save] will create the monitoring settings. You can click [Edit] for each item to change the settings.

⊕ Add Image Log Monitoring Setting
Configure the new image log monitoring setting.

Select Monitoring Target Group Configure Monitoring Setting Name and Monitoring Method Specify Notification Destination **Summary**

Select Monitoring Target Group Edit

Monitoring Target Group	Default Group

Configure Monitoring Setting Name and Monitoring Method Edit

Monitoring Setting Name	Monitoring Method	Monitoring Pattern	Monitoring Method
sample	Keyword	sample	Contains all of the following phrases
	No	Attribute	No

Specify Notification Destination Edit

Severity	Notification
B (Monitor and notify once a day)	example@example.com

Back **Save** Cancel

Searching monitor settings

You can search monitor settings with an entered string using .

Checking content of monitor settings

Click  of the monitor settings for check and select [Details].

You can check the content of monitor settings.

Changing content of monitor settings

Click  of the monitor settings for edit and select [Change].

You can edit the content of monitor settings.

Deleting monitor settings

When deleting monitoring settings from the list, place a check mark in the checkbox on the list, and then click [Delete]. Click  of the monitor settings for deletion and select [Delete].

You can delete the monitor settings.

Checking monitoring results

You can check the monitoring results with notification email or monitoring history.



"Monitoring History search" (P.350)

Checking with notification email

When an image log that satisfies the monitoring condition of Severity A or Severity B, notification email is sent to the specified email addresses.

Notification email is sent based on each monitoring condition. When UUID that satisfies the monitoring condition exceeds 100,

multiple emails are sent in the unit of 100.

An example of notification email is shown below.

You can change the subject and message body of email by editing the template file.



Note

The language of notification email is based on the OS language.

Subject:

An image log of <Image Log Management> monitoring target is registered.

Message body:

```
*****
This email is automatically sent by ApeosWare Management Suite.
You cannot reply to this email.
*****

An image log that satisfies the following monitor settings is registered.
[Monitoring Setting Name]

URL of monitoring history screen:
{Link to Monitoring History Screen}

The UUID of the registered image log is as shown below.
{UUID list of jobs that satisfy monitoring condition}
```

You can check the monitoring results with either of the following methods.

- Access the URL of the monitoring history screen provided in the email and check the results in the [Monitoring History] page.



Note

The content displayed in Monitoring History is the same as the search results of the image log.



Refer

"Monitoring History search" (P.350)

- Display the [Search Image Log] page and search the relevant image log using the UUID provided in the email as a search key.



Refer

"Search Image Log" (P.344)

Common Settings

How to Display

Select [Service Settings] > [Image Log Control] > [Common Settings] from the menu on the administrator screen.

Page Summary

Sets the password of an image log storage access user.

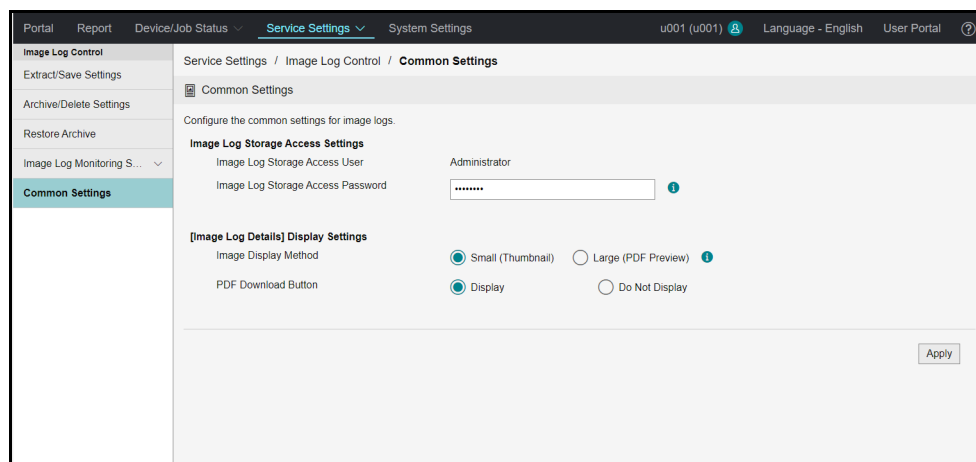


Image Log Storage Access Settings

[Image Log Storage Access User]

The user name of the image log storage access user is displayed based on the login destination.
In the case of domain, "domain¥user" is displayed. This item cannot be changed.

[Image Log Storage Access Password]

Set the password of a user who accesses to the image log/storage.
You can enter a string in the range of 1 to 128 characters in ASCII code.

Display settings of [Image Log Details]

[Image Display Method]

When displaying the details of the image log, set the display method of the image log to be displayed.

[PDF Download Button]

Set whether or not to display a button for downloading the image log in PDF format.

Image Log Receiving Status

How to Display

Select [Device/Job Status] > [Image Log Status] > [Image Log Receiving Status] in the administrator screen menu.

Page Summary

Displays the reception status of image logs by device.

Click [Edit] to change the device group for display.



Note

You can search the device group with the device name, installation location, model name, network, reception server, and last receiving date of image log using .

11 Job Log Accounting/Report

Settings and Confirmation in a Web Browser

You can set and confirm accounting in a web browser.



Note

When Cost Recovery Option is being used, the following report types are available on the User Portal screen.

- Account Usage & Replenishment History
- Account Usage
- Search Job Log

This section describes what you can do with each page.

Pages	Descriptions
Report Name List	You can create each type of report by accounting for job logs collected from a device in different ways. The conditions of consumables can also be displayed.
Accounting/Analysis Report	You can create a report by setting accounting conditions and display items for Accounting List Report, Accounting Graph Report, and Analysis List Report.
Custom Report List	The custom setting list you have created is displayed. It edits and deletes the content of custom settings.
Search Job Log	Searches job logs by specifying search conditions such as device, user, and date and time.
Search Image Log	Searches image logs by specifying conditions such as device, user, and date and time.
Monitoring History	Searches for image logs that match Monitor Settings.

Report Name List

How to Display

Select [Report] from the menu on the administrator screen. Select the type of report you want to create from the side menu.

Page Summary

You can create standard and custom reports by accounting in different ways for job logs or image log monitoring results collected from a device. The conditions of consumables can also be displayed. For the report created, you can specify a format and save it in a file.



Note

To report on image log monitoring, the core server license and OCR license must be valid.

Creating a standard report

Set the conditions, and click [Generate] of the report you wish to create.

Portal **Report** Device/Job Status Service Settings System Settings

Reports

Users / User Groups Users / User Groups

Account Reports Users / User Groups

Devices / Device Groups When creation takes a long time, it can be shortened by reducing the report items or range in [Custom Settings].

Sustainability Reports

Print Reports

Fax Report

Approval Print History

Accounting/Analysis Report

Supplies Report

Custom Reports

Saved / Scheduled Reports

Extended Report

Search Job Log

Transaction Type ☒ Copy ☒ Print ☐ Scan ☐ Fax Time Period Last month Report Format On Screen

Reports	Options
User - usage summary - with usage cost	Generate Set Filter / Schedule
Transaction details report - with usage cost	Generate Set Filter / Schedule
Transaction details	Generate Set Filter / Schedule
User group - usage summary - with usage cost	Generate Set Filter / Schedule
User - account usage summary - with usage cost	Generate Set Filter / Schedule
User - transaction at account level - with usage cost	Generate Set Filter / Schedule
User group - usage by transaction type - with usage cost	Generate Set Filter / Schedule
User - usage summary	Generate Set Filter / Schedule
User - usage by transaction type - with usage cost	Generate Set Filter / Schedule
User list report	Generate Set Filter / Schedule
User - usage by transaction type	Generate Set Filter / Schedule
User group - usage summary	Generate Set Filter / Schedule
User group - usage by transaction type	Generate Set Filter / Schedule
Account Usage & Replenishment History (Cost Management Report)	Generate Set Filter / Schedule

Specify conditions

[Transaction Type]

Select a checkbox for the service of accounting targets.

[Time Period]

Select a period for accounting targets.

[Report Format]

Select an output format of report results.

When you select [Screen Display], report results are displayed on the report results window. When you select [PDF], [Word] or [Excel], report results are saved in the files of each format.



Note

For some type of report, [CSV] can be selected.

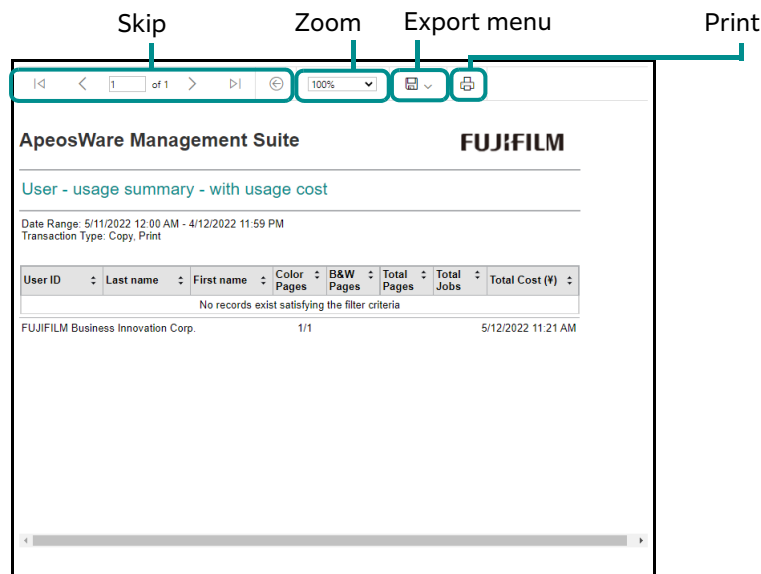


Refer

"Report Results Window" (P.334)

Report Results Window

When you select [Screen Display] in [Report Format] and create a report, the report results window is displayed.



Skip

When there are multiple pages in report results, you can change pages to display.

[Zoom]

You can zoom in/out the display of the report.

[Print]

You can print the report.

Export menu

Saves the report results to a file. Click  and from the menu that appears, select the saving format. You can select any one of PDF, Microsoft Word or Microsoft Excel.

Sorting

It sorts table data. Click  on the right side of the item title to sort data in ascending or descending order based on the value of the item. The current order is based on the column where the figures of icons are  or .

Configure Custom Settings

Click [Custom Settings] of a report you want to create and set each item with a dialog box displayed. The items you can set depend on the type of report you have selected.



Note

- [Custom Settings] is displayed when [View and edit report] is set to [Allow] in [Access Profile Settings] of [User Management].
The custom settings are not available to [Overview Report of Report] of [Environment Related Report].
- When specifying the following items in custom settings, the maximum numbers that can be specified are as follows.
 - Device groups: 100 max.
 - Devices: 100 max.
 - Accounts: 100 max.
 - User groups: 50 max.
 - Users: 50 max.

- Cost center code: 1,500 bytes max.
For example, if entering 10 characters for the cost center code, up to a maximum of 30 can be selected. (When 1 character is 4 bytes)
- Model name: 50 max.
- Serial number: 50 max.



Refer

"Access Profile List" (P.140)

[Transaction Type]

Select a checkbox for the service of accounting targets.

[Time Period]

Select a period for accounting targets. Reports for the specified period are created starting from the execution date. With [Custom] selected, you can specify start date and end date for accounting targets with arbitrary date.

[Report Format]

Select an output format of report results.

When you select [Screen Display], report results are displayed on the report results window. When you select [PDF], [Word] or [Excel], report results are saved in the files of each format.



Refer

"Report Results Window" (P.334)

[Graph Style]

Set this item when creating graph reports.

Select either [Line Graph] or [Bar Graph].

[Output Format]

Set this item when creating [Graph display of usage by service charge] reports.

Select the items for accounting from [Charge] and [Pages].

[By Group]

Select whether to have the user group or the device as the accounting target.

[Device Group]

Select whether to have all device groups as an accounting target or to specify device groups of accounting targets. If you select [Select], select target device groups.

For some type of report, specify the following items.

- [Contains device in sub device group]

If you select a checkbox, all devices, inclusive of groups under the specified device groups, become accounting targets. If you remove a checkbox, only groups just under the specified device groups become accounting targets.

- [Show by Device Group]

With a checkbox selected, accounting results are displayed per device group.



Note

When you cannot select the items of [Contains device in sub device group], only groups just under the specified device groups become accounting targets.

[Device]

Select whether to have all devices as accounting targets or to specify devices of accounting targets. If you select [Select], select target devices.

[Account Type]

Select the type of account for accounting targets.

- All
- Personal Account
- Shared Account
- All User Accounts

Accounts for which [Shared account that all users can use] is set in the account settings.

[Cost Center Code]

Select whether to have all cost centers as an accounting target or to specify cost centers of accounting targets. If you select [Select], select the target cost center code.

[Client Billable]

When checked, usage reports of only the jobs executed with the [Client Billable] are created.



Note

[Client Billable] is a function enabled only when an account for which [Enable shared account for all users to use] and [Enable Client Billing] are enabled is selected. For details on how to create an account, refer to "Create an account" (P.204).

[Accounts Filtering]

To create reports by each account, select the checkbox for [Split By Account]. To create reports by each sub account, select the checkbox for [Split by Sub-Accounts].

[Account]

Select whether to have all accounts as an accounting target or to specify accounts of accounting targets. If you select [Select], select target accounts.

To create reports by each sub account, select the checkbox for [Split by Sub-Accounts].

[Sub Account Display Conditions]

Set the display conditions for the sub account. It is enabled when parental relation is set for accounts.

- [Includes Sub Account]

With a checkbox selected, accounting targets are included in sub-accounts.

- [Show by Sub Account]

With a checkbox selected, accounting results are displayed by the sub-account.

[Include Account/User Group Association]

When creating a report containing the information of user group associated with the account, select the checkbox.

[Display Balance]

To include the balance as a target of the report, select the checkbox. When creating reports by each balance type, select the checkbox for [Split by Balance Type].

[Include Credit Transactions]

When recording the credit operation history of a user into the report, select the checkbox.

[User Group]

Select whether to have all user groups as an accounting target or to specify user groups of accounting targets. If you select [Select], select target user groups.

For some type of report, specify the following items.

- [Contains user in sub user group]

If you select a checkbox, all users, inclusive of groups under the specified user groups, become accounting targets. If you remove a checkbox, only users just under the specified user groups become accounting targets.

- [Show by Sub User Group]

With a checkbox selected, accounting results are displayed by the sub-user group.



Note

When you cannot select the items of [Contains user in sub user group], only users just under the specified user groups become accounting targets.

[User]

Select whether to have all users as accounting targets or to specify users of accounting targets. If you select [Select], select target users.

When performing accounting of operations by unregistered user only, select the checkbox for [Unregistered User Only].

[Include Inactive Users]

To include inactive users also as a target of the report, select the checkbox.

[Display for Each Color Mode]

Set this item when creating graph reports.

Select the checkbox when making distinctions between the color pages and B&W pages.

[Paper Reduction Calculation Method]

Set it at the time of the creation of [Analysis Report on Usage].

Select a parameter to calculate sheets of paper for reduction.

- N Up

It calculates the number of sheets of paper that could have been reduced with two pages per side print, though you printed the job with one page per side print.

- 2 sided

It calculates the number of sheets of paper that could have been reduced with two sided print, though you printed the job with one sided print.

- Pages per side (two sided)

It calculates the number of sheets of paper that could have been reduced with two pages per side and two sided print, though you printed the job with one page per side and one sided print, one page per side and two sided print, and two pages per side and one sided print.



Refer

"Calculation of Paper Reduction" (P.356)

[Model Name]

The report target can be specified with the device model name.

[Serial Number]

The report target can be specified with the device model name and serial number.

[Includes display conditions in report output result]

Select a checkbox to display the conditions of report creation, such as periods for accounting targets and the service type, in report results

[Show UPN]

When the UPN (User Principle Name) is set, check to show the user ID and the value.

Save as Custom Report/Schedule

In the [Custom Settings] dialog box, click [Save as Custom Report/Schedule] and set each item in the dialogged box that appears. You can set a report name and register custom settings as a custom report or configure auto report settings for creating reports on a periodic basis.



Note

- You can confirm and edit the custom settings saved in the custom report list.
- When creating a report with the auto report function, the report is created in the language of the OS on which the ApeosWare Management Suite is installed.
- If the job log of the device is not collected on the date specified in the auto report, information will not be accounted correctly. To enable accounting after completing the job log collection of the device, perform accounting after a sufficient amount of time has passed since the closing date. According to the default settings, job log collection is performed once a day at 0:00.
For example, if an automatic report is used to perform accounting at the end of the month, set the second day of the month in [Monthly] and create a report for the previous month on the second day of the following month to allow time for collection of the job log.



Refer

- "Concerning Authentication/Accounting Settings" in "Installation and Operation Guide"
- "Custom Report List" (P.341)

[Report Name]

Input the name of custom settings to save.

[Description]

As needed, enter descriptions for the custom settings.

[Auto Report Settings]

Specify a schedule to execute auto report settings.

- No
Auto report settings are not executed.
- Only once
Auto report settings are executed at specified time only once.
- By Hour
Auto report settings are executed at intervals of specified hours.
- By Day
Auto report settings are executed at intervals of specified days.
- By Week
Auto report settings are executed at intervals of specified weeks.
- By Month

Auto report settings are executed at intervals of specified months.



Note

The first execution date for the auto report settings registered is the relevant date of the schedule of the following day and after.

[Interval]

Specify the interval to execute auto report settings. Also, specify the day of the week when set to By Week, and the date of month when set to By Month.

[Start Date]

Specify the start date to execute auto report settings.

[Time]

Specify the time to execute auto report settings.

[Send Email of Report]

Enter the notification destination address, subject, and message for the email notification of processing results of auto report settings. Clicking  enables you to set multiple email addresses.

[Save Report to Folder]

Specify a folder to save a report created in auto report settings.

- [Network Path]

Specify the path of the storage destination of reports in the UNC format.

Example:

\\192.0.2.1\share\myfolder

\\servername\share\myfolder

- [User ID]/[Password]

Input the user ID and password to access the path of the storage destination with.



Note

Make sure that the drive specified for storage folders has enough capacity.

Accounting/Analysis Report

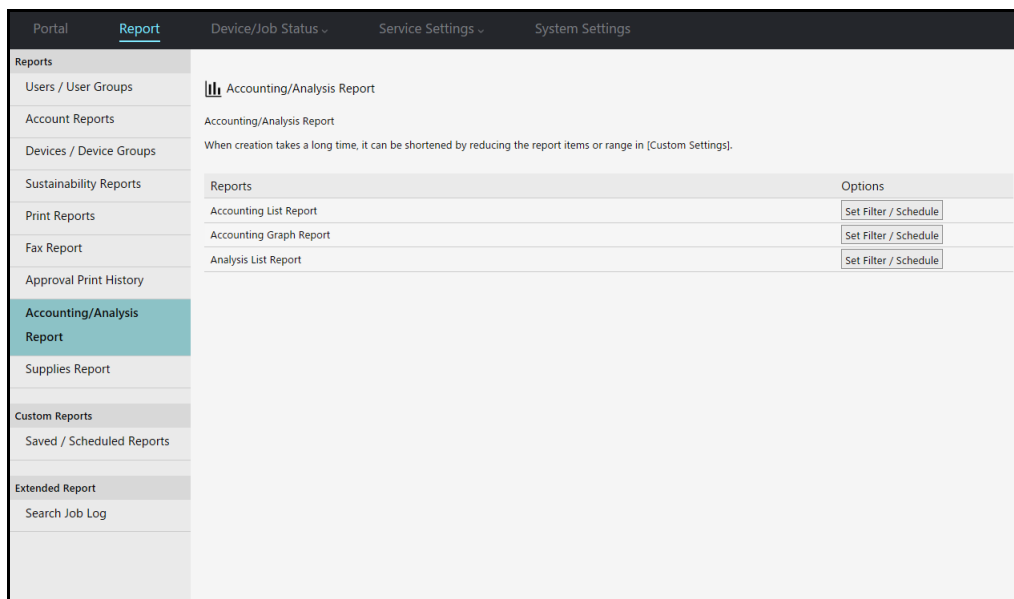
How to Display

Select [Report] > [Accounting/Analysis Report] from the menu on the administrator screen.

Page Summary

The following reports are created.

- Accounting List Report
Creates a list by tallying items such as impressions, sheets, and the number of jobs by department, user, device, etc.
- Accounting Graph Report
Creates a graph by tallying the impressions or sheets by department, user, device, etc.
- Analysis List Report
Creates a list of the sheets that can be reduced by using 2 sided printing and pages per side printing and the sheets that have been reduced by such 2 sided printing and pages per side printing.



[Custom Settings]

You can create a report by setting accounting conditions and display items for Accounting List Report, Accounting Graph Report, and Analysis List Report.

Setting items on the Custom Settings screen

[Transaction Type]

Select a checkbox for the service of accounting targets.

[Time Period]

Select a period for accounting targets.

[Report Format]

Select an output format of report results.

When you click [Screen Display], report results are displayed on the report results window. When you select [PDF], [Word], [Excel] or [CSV], report results are saved in the files of each format.

[User Group]

Set all user groups as the target or select a user group.

[Device]

Set all devices as the target or select a device.



Note

When selecting the device in custom settings, up to a maximum of 100 can be specified.

[Document Type]

Can be set in Classification List Report. Select the document type.

[Accounting Key]

Can be set in Accounting List Report and Classification List Report. Set the priority order of keys.

[Display Items]

Can be set in Accounting List Report and Classification List Report. Select the checkbox for relevant display items.

[Table Format]

Click [Preview] to display a sample. Displayed in Accounting List Report and Classification List Report.

[Target]

Can be set in Accounting Graph Report. Select either "By user", "By department", "By device", "By model" and "By account".

[Classification]

Can be set in Accounting Graph Report. Select either "Do not classify", "By output color", or "By service".

[Counting Unit]

Can be set in Accounting Graph Report. Select either [Impressions] or [Sheets].

[Graph Format]

Click [Preview] to display a sample. Can be displayed in Accounting Graph Report.

[Includes display conditions in report output result]

Select a checkbox to display the conditions of report creation, such as periods for accounting targets and the service type, in report results

[Save as Custom Report/Schedule]

Display the [Custom Settings] dialog box. You can set a report name and register custom settings as a custom report or configure auto report settings for creating reports on a periodic basis.



Refer

"Save as Custom Report/Schedule" (P.338)

[Generate]

Creates a report using the format specified in [Report Format].

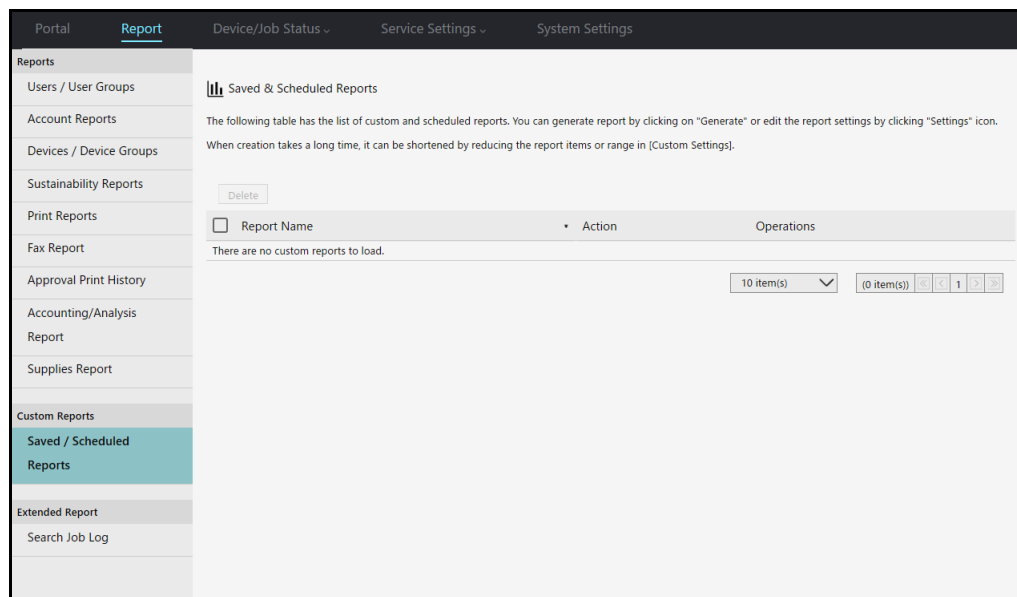
Custom Report List

How to Display

Select [Report] > [Custom Report List] from the menu on the administrator screen.

Page Summary

The custom setting list you have created is displayed. It edits and deletes the content of custom settings.



Creating custom reports

Click [Generate] of the report you wish to create.
A report is created according to the setup content.



Refer

“Report Results Window” (P.334)

Deleting custom settings

Click  of the custom settings to delete in the custom report list and select [Delete].

Changing custom settings

Click  of the custom settings to change in the custom report list and select [Properties].



Refer

“Configure Custom Settings” (P.334)

Search Job Log

How to Display

Select [Report] from the menu on the administrator screen. From the side menu, select [Search Job Log].

Page Summary

You can search job logs by specifying search conditions such as device, user, and date and time.



Note

Job logs can be searched on the user portal as well, which only searches jobs of the logged-in user.

Searching for Job Logs

Set the search conditions and click [Search].

Portal **Report** Device/Job Status Service Settings System Settings

Reports

Users / User Groups

Account Reports

Devices / Device Groups

Sustainability Reports

Print Reports

Fax Report

Approval Print History

Accounting/Analysis Report

Supplies Report

Custom Reports

Saved / Scheduled Reports

Extended Report

Search Job Log

Search Job Log

Search job log. Enter a search keyword.

☒ Match All Conditions ☐ Match Any Condition [Search Attribute Settings](#)

Device Name Contains [+](#)

[Search](#) [Reset](#) [Download Search Results](#) [Table Settings](#)

(0 item(s)) [1](#)

Device Name	Model	Model Code	Identification ID	Job ID	Service Type	User Name	Document Name	Sheets	Job End Date/Time
No item to display.									

50 item(s) (0 item(s)) [1](#)

From the left menu, select attributes you want to target in the search.

From the second menu from the left, select the search computation method.

The computation methods shown in the menu change depending on the type of the search item.

To add a search condition, click [+]. You can add up to five search conditions.

When you have set multiple search conditions, select either [Match All Conditions] or [Match Any Condition].

Display Search Result

Clicking [Search] displays the result of job log search.



Note

- If the number of search results exceeds 1,000, the first 1,000 results are displayed.
- You can change the items in the search results list by clicking [Table Settings].

Skip

When there are multiple pages in report results, you can change pages to display.

Download Search Results

Saves the list of search results as a CSV format text file.

Adding/Deleting Search Attributes

On the [Search Job Log] page, clicking [Search Attribute Settings] displays the [Search Attribute Settings] page.

In [Search Attribute List] shown in the left, select the checkbox for the attribute you wish to add, and then click [Add].

To delete an attribute, select the checkbox for the attribute you wish to delete in [Search Attribute] shown in the right, and then click [Remove].

Search Image Log

How to Display

Select [Report] from the menu on the administrator screen. From the side menu, select [Search Image Log].

Page Summary

Image logs can be searched by specifying search conditions such as device, user, and date and time.

Search Image Log

Set the search conditions and click [Search].

[Service Type]

Select the checkboxes for the service types to set as the searching target.

[Start Date/Time, End Date/Time]

Specify the range of the time when the job was completed by specifying the start and end date/time of the range.

 Click the calendar icon to display the calendar, on which the start date and end date can be selected.

The default value of the Start Date/Time is [0:00] on the day 7 days earlier than when the [Search Image Log] page was displayed.

The default value of the End Date/Time is [23:59] on the day when the [Search Image Log] page was displayed.

[Match All Conditions]/[Match Any Condition]

Select either AND search ([Match All Conditions]) or OR search ([Match Any Condition]) for the search conditions other than Service Type, Date and Group ID.

[Keyword]

Enter the keywords that are included in image logs. To enter multiple keywords, separate them with a double-byte or single-byte space character. When multiple keywords have been specified, select the join condition for the keywords between [Contains all of the following phrases] (AND condition) and [Contains any of the following phrases] (OR condition). In the default settings, [Contains all of the following phrases] is selected.

Languages set as [Language Used for OCR] can be mixed for entry. Up to 256 character in double-byte or single-byte characters can be entered.



Note

To use keywords as search conditions, the OCR license must be valid.

[Pattern]

Filter patterns registered for setting of languages used for OCR processing can be used for search.

Use [+] or [-] to increase or decrease the filter patterns used for search.



Note

To use patterns as search conditions, the OCR license must be valid.

Attribute conditions

Set the attribute and value of search conditions. Use  or  to add or delete attributes to be searched.

When a character string is entered, jobs with an attribute that matches or partially matches the character string entered are output as search results. Searches for a partial match is not case sensitive. When multiple character strings are entered, jobs with an attribute that matches or partially matches any of the character strings entered are output as search results (OR condition). When [Contains the following string (spaces included)] or [Matches the following string (spaces included)] is selected, the results of search with the entire text including spaces are output.

Available attributes are as follows.

Attribute	Items to be set	Specify method/ Search method
Job ID	Enter an ID assigned for each job by the device. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Complete match
UUID	Enter an UUID assigned for each job by the device. Up to 256 double-byte or single-byte characters can be entered.	
Job Complete Status	Select the job status from the following. • All • Completed Only • Other than Completed [Completed] refers to a job with the status of "completed".	Item selection
Job Name	Enter the name of the job. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Partial match
Device Host Name	Enter the Internet host name of the device that executed the job. Up to 256 single-byte alphanumeric characters and hyphens (-) can be entered.	Character string entry/ Partial match
IP address of device	Enter the IP address (IPv4) of the device that executed the job. Up to 256 single-byte numeric characters and periods (.) can be entered.	Character string entry/ Complete match
Device Name	Enter the device name of the device that executed the job. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Partial match
Job Owner Name	Enter the user ID of the user that executed the job. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Partial match
User name	Enter the user name of the user that executed the job. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Partial match
Impressions	Select the relation condition from the following. • Less Than • More Than Enter the impressions processed as an integer from 1 to 999. The "impressions" specified here refers to the following values respectively. • Copy, Print: Impressions printed • Send Fax: Number of pages sent • Receive Fax: Number of pages received • Scan: Number of sheets input	Relation condition and integer entry
Number of Copies	Select the relation condition from the following. • Less Than • More Than Enter the number of copies as an integer from 1 to 999.	Relation condition and integer entry

Attribute	Items to be set	Specify method/ Search method
Print Impression Output Color	Select the output color of print from the following. • Full Color • Dual Color • Single Color • Specific Color • Low-Price Output Color • Others	Item selection
Pages per Side	Select the layout of print from the following. • 1 Page • 2 Page • 4 Page • 8 Page • 16 Page • 32 Page • Auto • Others	Item selection
Client Host Name	Enter the Internet host name of the client that instructed the print processing. Up to 256 single-byte alphanumeric characters and hyphens (-) can be entered.	Character string entry/ Partial match
Client IP Address	Enter the IP address (IPv4) of the client that instructed the print processing.	Character string entry/ Complete match

Attribute	Items to be set	Specify method/ Search method
Port	Select one from the following. • Parallel • Serial • Ethertalk • lpd • NetWare:PServer • NetWare:RPrinter • Salutation • IPP • SMB • SMTP • POP3 • Port9100 • USB • HTTP • BMLinkS • WSD Print • ThinPrint • FTP • Report/List • PS Initalize • HDD • G3 • G4 • Netware • OEMHTTP • Media • WebDAV • Report/List • PS Initalize • HDD • G3 • G4 • Netware • OEMHTTP • Media • WebDAV • Others	Item selection
Document Name	Enter the file name given to the job. Up to 256 double-byte or single-byte characters can be entered.	Character string entry/ Partial match
Recipient Fax Number	Enter the phone number of the party at the end of the fax line (recipient/sender). Up to 256 single-byte numeric characters can be entered.	Character string entry/ Partial match
F Code	Enter the F code of the fax recipient/sender. Up to 256 ASCII code characters can be entered.	Character string entry/ Partial match

Attribute	Items to be set	Specify method/ Search method
Data Type	Select the type of the data to search from the following. • Active Data Searches active image logs. • Archived Data Searches image logs past the storage period (archived data). • Temporary Data Searches files marked to be deleted by the keyword or pattern filtering function and temporarily stored.	Item selection

[Table Settings]

When the display format is list view, change the items shown on the list of search results.

In [Available Items] shown in the left, select the checkbox for the attribute you wish to add, and then click [Add].

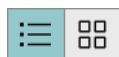
To delete an attribute, select the checkbox for the attribute you wish to delete in [Displayed Items] shown in the right, and then click [Remove].

Showing search results

Clicking [Search] displays in the lower part the results of image log search that satisfy all search conditions.

Hiding search conditions

Click  to collapse the search conditions. Click  to expand the collapsed search conditions.



(List view icon/Thumbnail view icon)

Switch the view of search results between list view and thumbnail view.

Skip

Changes the page to display when there are multiple pages of search results.

[Download Search Results]

Saves the list of search results as a CSV format text file.

Showing image log details

In the list of image log search results, click  and click [Details], or click [Details] to show the image log details. The detailed image of the image log to be displayed is displayed according to the display method set in [Image Display Method] in “Display settings of [Image Log Details]” (P.330).

[Download]

Saves the image log image content as a PDF file.

If the [PDF Download Button] is set to [Do Not Display] in “Display settings of [Image Log Details]” (P.330), this item will not be displayed.

[Change to Active Data]

When the Data Type is “Temporary Data,” converts the data to Active Data.

PDF Preview

This displays a preview of the contents of the PDF file. The method of using the Preview screen is as follows.

- : Displays a thumbnail of each page of the PDF file. If a thumbnail is clicked, that page is displayed.
- : Searches the PDF file for specified keyword(s).
- : Specify a page number, and that page is displayed.
- : Displays the PDF file enlarged or reduced.
- : Enables other functions to be used. (Rotates the page display, switches the method of scrolling pages)

Monitoring History search

How to Display

Select [Report] from the menu on the administrator screen. From the side menu, select [Monitoring History].



Note

This feature is displayed only when the core server license and OCR license are valid.

Page Summary

Allows searching for image logs that match Monitor Settings.

Searching Monitoring History

Set the search conditions and click [Update Monitoring History].

[Monitoring Settings]

Select monitor settings.

[Display Range]

Specify the range of date and time of image logs to display as the monitoring history results.

To show the entire range, select [All]. To specify the date and time, select [Specify]. Click to display the calendar, on which the start date and end date can be selected.

[Update Monitoring History]

Update the list of monitoring results using the monitor settings and monitoring range as the conditions.

[Details]

Shown when there are three or more patterns of monitor settings. Click to show the [Monitoring History Pattern Details] page.

[Table Settings]

When the display format is list view, change the items shown on the list of search results.

In [Available Items] shown in the left, select the checkbox for the attribute you wish to add, and then click [Add].

To delete an attribute, select the checkbox for the attribute you wish to delete in [Displayed Items] shown in the right, and then click [Remove].

Showing search results

Clicking [Update Monitoring History] displays in the lower part the results of image log search based on the monitor settings.

Portal

Report

Device/Job Status

Service Settings

System Settings

Apeos Administrator...

Language - English

User Portal

Users / User Groups

Account Reports

Devices / Device Groups

Sustainability Reports

Print Reports

Fax Report

Image Log Monitoring Report

Approval Print History

Accounting/Analysis Report

Supplies Report

Custom Reports

Saved / Scheduled Reports

Extended Report

Search Job Log

Search Image Log

Monitoring History

Monitoring History

Monitoring Settings

Display Range

Update Monitoring History

Group :

Keyword :

Pattern :

Attribute :

Table Settings

User Name

Group Name

Date/Time Completed

Service Type

Device IP Address

Operation

No items to display.

50 items

1

  (List view icon/Thumbnail view icon)

Switch the view of search results between list view and thumbnail view.

Skip

Changes the page to display when there are multiple pages of search results.

Download Search Results

Saves the list of search results as a CSV format text file.

Output items of search results

For the downloaded file of search results, output the attribute names and attribute values of jobs. For the list of image log search results and the [Image Log Details] dialog box, output the item names corresponding to the attribute names and attribute values. The list below shows the content output to the downloaded file of search results and the content output to the [Image Log Details] dialog box. Attributes with attribute values are all output regardless of Service Type.

- Common attributes

Downloaded file		Image Log Details	
Attribute name	Attribute	Item name*1	Item value
UUID		UUID	
Job ID		Job ID	
Service Type	Copy	Service types	Copy
	Print		Print
	FAX_Send		Send Fax
	FAX_Receive		Receive Fax
	Scan		Scan
	System Sheet		System Sheet

Downloaded file		Image Log Details	
Attribute name	Attribute	Item name *1	Item value
	File Transfer		File Transfer
	Email Transfer		Email Transfer
	Job Flow		Job Flow
Job Name		Job Name	
Start Time		Job Start Date/Time	
Complete Time		Job End Date/Time	
Receive Time		Job Received Date/Time	
Device Host Name		Device Host Name	
Device IP Address		IP address of device	
Printer Name		Device Name	
Job Owner Name		Job Owner Name	
User Name		User name	
Group ID		Group ID	
Group Name		Group Name	
Job Status	other	Job Complete Status	Others
	unknown		Unknown
	created		Uncompleted
	pending		
	processing		
	interrupted		
	retained		
	held		
	paused		
	terminating		
	completed		Completed
	completedWithError		Completed with Warning
	completedWithWarning		
	canceledByUser		Canceled
	canceledBySystem		Completed With Error
Document Name		Document Name	
Impressions		Impressions	
Copies		Number of Copies	
Print Color Mode	4 colors	Print Impression Output Color	Full Color
	3 colors		
	2 colors		Dual Color
	1 color		Single Color
	monochrome		Black & white
	unspecified		Others
	auto		Others

Downloaded file		Image Log Details	
Attribute name	Attribute	Item name *1	Item value
	few colors		Specific Color
	for low price mode		Low-Price Output Color
	mixed		Others
N Up	off	Pages per Side	1 Page
	1-up		
	2-up		2 Page
	3-up		4 Page
	4-up		
	5-up		8 Page
	6-up		
	7-up		
	8-up		
	16-up		16 Page
	32-up		32 Page
	auto		Auto
	unspecified		Others
	9-up		
Host Name		Client Host Name	
IP Address		Client IP Address	

Downloaded file		Image Log Details	
Attribute name	Attribute	Item name *1	Item value
Port	IEEE1284	Port	Parallel
	extended IEEE 1284		
	Serial		Serial
	Netware Pserver		Netware Pserver
	Netware Rprinter		Netware Rprinter
	USB		USB
	USB2		
	Ethertalk		Ethertalk
	lpd		lpd
	Salutation		Salutation
	IPP		IPP
	SMB		SMB
	SMTP		SMTP
	POP		POP
	Port9100		Port9100
	HTTP		HTTP
	BMLinks		BMLinks
	WSD Print		WSD Print
	ThinPrint		ThinPrint
	FTP		FTP
	Report/List		Report/List
	PS Initalize		PS Initalize
	WebDAV		WebDAV
	HDD		HDD
	NetWare		NetWare
	OEMHTTP		OEMHTTP
	Media		Media
	G3		G3
	super_G3		
	G3 without ECM		
	G4		G4
	forced_4800		Others
	forced 4800 without ECM		
	none		
	unspecified		
Destination		Recipient Information	
Phone Number		Recipient Fax Number	
F Code		F Code	
Remote ID		Remote ID	

Downloaded file		Image Log Details	
Attribute name	Attribute	Item name *1	Item value
Fax Communication Result	GOOD	Fax Communication Result	Good
	BUSY		Busy
	BUSYWITHRETRY		Busy (Auto Retry)
	FAILUREWITHRETRY		Auto Retry
	TERMINATED		Terminated
	COMMFAILURE		Resend Required
	FAILURE		Error
	{Other than above}		Others
Security	ForcedWMCcancel	Security	Allow Force Print Suspension
	AnalogWaterMark		Watermark
	TrustMarking		Watermark
	HybridWaterMark		Secure Watermark
	UUID		Print Universal Unique ID
	LoginID		Print User ID

*1 Show all for attributes with attribute values regardless of Service Type.

Calculation of Paper Reduction

This section describes the calculation of paper reduction.



Note

The calculation of paper reduction described here is used both for accounting for [Report] in an administrator's screen and Job Log Analyzer.

What are “actual paper reduction” and “possible paper reduction”?

“Actual Paper Reduction” is the value for actual paper reduction by 2 sided printing or pages per side printing compared to printing only 1 image on only 1 side per sheet of paper.

“Possible Paper Reduction” is the value for possible paper reduction by 2 sided with pages per side printing, pages per side printing, or 2 sided printing referencing the number of sheets actually printed.

Paper Reduction Calculation Method

You can select a parameter to calculate sheets of paper for reduction from [2 Sided/Pages per Side], [Pages per Side] or [2 Sided]. These can be set in the following menu.

- For [Report] on administrator screen:
[Paper Reduction Calculation Method] in custom settings



Refer

“Configure Custom Settings” (P.334)

- For Job Log Analyzer:
[Paper Reduction Calculation Parameter] in [Settings] sheet



Refer

"Help for Job Log Analyzer"

How Are Actual Paper Reduction and Possible Paper Reduction Calculated?

This section describes two examples of basic methods of calculating actual paper reduction and possible paper reduction.

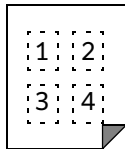


Note

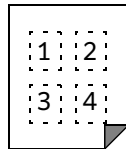
More information on calculation formula→"Calculation of Actual Paper Reduction" (P.360), "Calculation of Possible Paper Reduction" (P.362)

Example 1: When 1 set is printed of a document printed with 4 pages printing on three sides of 2 sheets of paper

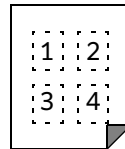
Side 1
= Front of Sheet 1



Side 2
= Rear of Sheet 1

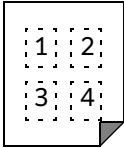
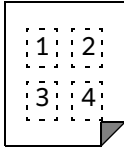
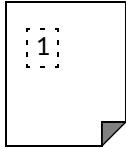
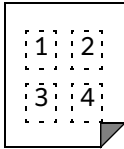
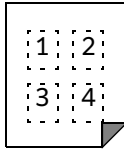
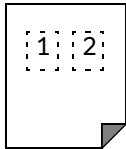
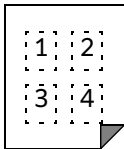
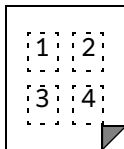
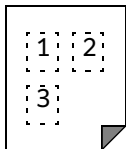
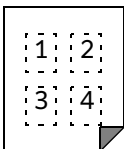
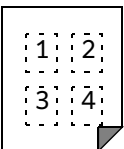
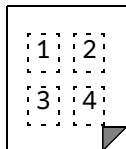


Side 3
= Front of Sheet 2



To calculate actual paper reduction and possible paper reduction, information of the number of original sheets of the job is required. However, information of the number of original sheets of the job is not included in the job log. Thus, an assumed number of original sheets is calculated from the impressions and the pages per side number.

In this example, since three sides are printed with 4 pages printing, the number of original sheets is 9, 10, 11, or 12 sheets.

Side 1 = Front of Sheet 1	Side 2 = Rear of Sheet 1	Side 3 = Front of Sheet 2	
			Possibility 1 Original sheets of Side 3 = 1 Total original sheets = 4 + 4 + 1 = 9
			Possibility 2 Original sheets of Side 3 = 2 Total original sheets = 4 + 4 + 2 = 10
			Possibility 3 Original sheets of Side 3 = 3 Total original sheets = 4 + 4 + 3 = 11
			Possibility 4 Original sheets of Side 3 = 4 Total original sheets = 4 + 4 + 4 = 12

The assumed number of original sheets is calculated as the mean of the smallest possible number and the largest possible number.

Assumed number of original sheets = (Smallest possible number + Largest possible number) / 2
= (9 + 12) / 2
= 10.5

Actual paper reduction is calculated with "number of sheets necessary for printing only 1 image on only 1 side per sheet of paper" as the assumed number of original sheets.

Actual paper reduction

The following is an example when you select [Pages per Side/2 Sided] in [Paper Reduction Calculation Method]. Actual paper reduction is calculated by the following formula.

Actual Paper Reduction = Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper - Number of sheets of paper printed
= 10.5 - 2
= 8.5

Accordingly, actual paper reduction is 8.5 sheets.

Possible paper reduction

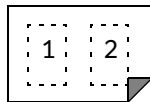
Possible paper reduction is calculated any of the following formulas. Which formula to be used is determined by [Paper Reduction Calculation Method].

- Sheets of paper printed - Sheets of paper required for 2 sided printing with 2 pages per side printing
- Sheets of paper printed - Sheets of paper required for 1 sided printing with 2 pages per side printing
- Sheets of paper printed - Sheets of paper required for 2 sided printing

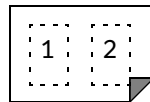
In example 1, since you are printing 2 sided with 4 pages printing, and since no sheets can be reduced in any of the above-described cases, possible paper reduction is 0.

Example 2: When 1 set is printed of a document printed with 2 pages per side printing on only 1 side each of 2 sheets of paper

Side 1
= Front of Sheet 1



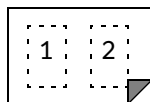
Side 2
= Front of Sheet 2



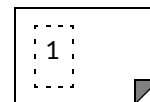
Identically to example 1, the assumed number of original sheets is calculated.

Since 2 sides are printed with 2 pages per side printing, the number of original sheets becomes 3 or 4.

Side 1
= Front of Sheet 1



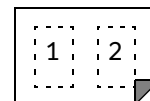
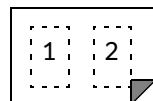
Side 2
= Front of Sheet 2



Possibility 1

Original sheets of Side 2 = 1

Total original sheets = 2 + 1 = 3



Possibility 2

Original sheets of Side 2 = 2

Total original sheets = 2 + 2 = 4

The assumed number of original sheets is calculated as the mean of the smallest possible number and the largest possible number.

Assumed number of original sheets = (Smallest possible number + Largest possible number) / 2

= (3 + 4) / 2

= 3.5

Actual paper reduction

"Actual paper reduction" is calculated by the following formula with "number of sheets necessary for printing only 1 image on only 1 side per sheet of paper" as the assumed number of original sheets.

Actual Paper Reduction = Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper - Number of sheets of paper printed

= 3.5 - 2

= 1.5

Accordingly, actual paper reduction is 1.5 sheets.

Possible paper reduction

Possible paper reduction is calculated any of the following formulas.

- Sheets of paper printed - Sheets of paper required for 2 sided printing with 2 pages per side printing
- Sheets of paper printed - Sheets of paper required for 1 sided printing with 2 pages per side printing
- Sheets of paper printed - Sheets of paper required for 2 sided printing

This is an example of possible paper reduction for 2 sided printing with 2 pages per side printing.

The number of sheets actually printed is 2 sheets. Since the original job is printed 1 sided with 2 pages per side printing, 1 sheet of paper is used if you print 2 sided with 2 pages per side printing.

Possible paper reduction = Sheets of paper printed - Sheets of paper required for 2 sided printing with 2 pages per side printing

= 2-1

= 1

Accordingly, possible paper reduction is 1 sheet.



Note

The value calculated with the calculation formula is a real number. However, since the accounting reports of Job Log Analyzer uses the defaults of the cell format of Excel, the values of integers rounded off below decimal points are displayed on the reports. To confirm the calculated values as actual numbers, change the setting of the cell format of Excel to display the digit numbers below decimal points.

Calculation of Actual Paper Reduction

This section describes how to calculate actual paper reduction in more detail.

The values used in calculation formula are as follows.

Value	Descriptions
Pages per side number	N value of pages per side set in "Pages per Side"
Sheets used	Sheets of paper printed
Number of sheets	Same value as for sheets used in accounting report. Sheets calculated at A4 size in analysis report
Impressions used	Impressions printed
Impressions	Same value as for impressions used in accounting report. Impressions calculated at A4 size in analysis report
Number of Copies	Copies printed

For calculating paper reduction when either 2 sided/pages per side, pages per side, or 2 sided printing is used, select it with [Paper Reduction Calculation Method].



Refer

"Paper Reduction Calculation Method" (P.356)

Formula when reduction calculation parameter is [2 Sided/Pages per Side]

The sheets reduced with 2 sided printing and pages per side printing are calculated as "Actual Paper Reduction".



Note

The numbers of the table indicate the calculation procedure executed by the program. They do not indicate operations by users.

1.	Since total values of multiple sets are recorded in impressions of the job log, "Impressions of 1 set unit" is calculated. Impressions of 1 set unit = Impressions / Copies
----	--

2.	Calculates the sheets required to print on 1 side with 1 page printing from the pages per side number and the impressions of 1 set unit. To calculate the sheets required to print on 1 side with 1 page printing, information of the number of original sheets of the job is required. However, information of the number of original sheets of the job is not included in the job log. Thus, an assumed number of original sheets is calculated from the impressions and the pages per side number. The assumed number of original sheets is calculated as the mean between the smallest possible number of sheets and the largest possible number of sheets. Example: For 4 pages printing on three sides, the page quantity printed on Side 1 and Side 2 is $4 \times 2 = 8$. Since the page quantity printed on Side 3 can be 1, 2, 3, or 4, the smallest number of sheets is 9 and the largest number of sheets is 12. Assumed number of original sheets = (Smallest possible number + Largest possible number) / 2 The assumed number of original sheets becomes the number of sheets required to print on only 1 side of each sheet with 1 page printing.
3.	Multiplies the sheets required for printing on only 1 side of each sheet with 1 page printing by the number of copies and calculates "Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper" Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper = Sheets required to print 1 sided with 1 page printing x Copies
4.	"Actual Paper Reduction" is the value when sheets used (sheets of paper actually printed) is subtracted from "Number of sheets required for printing only 1 image on only 1 side per sheet of paper" Actual Paper Reduction = Number of sheets required for printing only 1 image on only 1 side per sheet of paper - Sheets used

Formula when paper reduction calculation parameter is [Pages per Side]

Only the sheets reduced with pages per side printing are calculated as Actual Paper Reduction. The sheets reduced with 2 sided printing are not considered.



Note

- The numbers of the table indicate the calculation procedure executed by the program. They do not indicate operations by users.
- Calculation Steps 1 to 3 are the same as a formula when reduction calculation parameter is [2 Sided/Pages per Side].

1.	Since total values of multiple sets are recorded in impressions of the job log, "Impressions of 1 set unit" is calculated. Impressions of 1 set unit = Impressions / Copies
----	---

2.	Calculates the sheets required to print on 1 side with 1 page printing from the pages per side number and the impressions of 1 set unit. To calculate the sheets required to print on 1 side with 1 page printing, information of the number of original sheets of the job is required. However, information of the number of original sheets of the job is not included in the job log. Thus, an assumed number of original sheets is calculated from the impressions and the pages per side number. The assumed number of original sheets is calculated as the mean between the smallest possible number of sheets and the largest possible number of sheets. Example: For 4 pages printing on three sides, the page quantity printed on Side 1 and Side 2 is $4 \times 2 = 8$. Since the page quantity printed on Side 3 can be 1, 2, 3, or 4, the smallest number of sheets is 9 and the largest number of sheets is 12. Assumed number of original sheets = (Smallest possible number + Largest possible number) / 2 The assumed number of original sheets becomes the number of sheets required to print on only 1 side of each sheet with 1 page printing.
3.	Multiplies the sheets required for printing on only 1 side of each sheet with 1 page printing by the number of copies and calculates "Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper" Number of sheets necessary for printing only 1 image on only 1 side per sheet of paper = Sheets required to print 1 sided with 1 page printing x Copies
4.	"Actual Paper Reduction" is the value when "Impressions used" is subtracted from "Number of sheets required for printing only 1 image on only 1 side per sheet of paper" Actual Paper Reduction = Number of sheets required for printing only 1 image on only 1 side per sheet of paper - Impressions used "Impressions used" are subtracted because the sheets reduced by 2 sided printing are not considered. If 2 sided printing is considered, "Sheets used" are subtracted since two sides of one sheet of paper can be printed on. However, here "Impressions used" are subtracted because only impressions are considered when 2 sided printing is ignored.

Formula when paper reduction calculation parameter is [2 Sided]

Only the sheets reduced with 2 sided printing are calculated as "Actual Paper Reduction". The sheets reduced with pages per side printing are not considered.

Actual Paper Reduction is the value calculated by subtracting "Sheets used" from "Impressions used".

Actual Paper Reduction = Impressions used - Sheets used

Example: If you print with 2 sided printing on 2 sides of 1 sheet of paper, the actual paper reduction = $2 - 1 = 1$.

Calculation of Possible Paper Reduction

This section describes how to calculate possible paper reduction in detail.



Note

When "Side 2" or "Transparency" is the paper type used, it is determined that paper cannot be reduced

because they do not support 2 sided printing, and thus "Actual Paper Reduction" is calculated as 0.

The values used with the formula are described below.

Value	Descriptions
Pages per side number	N value of pages per side set in "Pages per Side"
Sheets used	Sheets of paper printed
Number of sheets	Same value as for sheets used in accounting report. Sheets calculated at A4 size in analysis report
Impressions used	Impressions printed
Impressions	Same value as for impressions used in accounting report. Impressions calculated at A4 size in analysis report
Number of Copies	Copies printed

For calculating paper reduction when either 2 sided/pages per side, pages per side, or 2 sided is used, set it with [Paper Reduction Calculation Method].



Refer

"Paper Reduction Calculation Method" (P.356)

Formula when reduction calculation parameter is [2 Sided/Pages per Side]

The sheets reduced with only 1 page/1 sided printing, 1 page/2 sided printing, and 2 pages per side/1 sided printing are calculated as Possible Paper Reduction. The calculation method is as follows.



Note

The numbers of the table indicate the calculation procedure executed by the program. They do not indicate operations by users.

1.	Since total values of multiple sets are recorded in impressions of the job log, "Impressions of 1 set unit" is calculated. Impressions of 1 set unit = Impressions / Copies
2.	Since information of original impressions is not included in the job log, "Assumed original impressions" is calculated by multiplying "Impressions of 1 copy unit" by the pages per side number. Assumed original impressions = Impressions of 1 copy unit x Pages per side number
3.	Divides "Assumed original impressions" by "Original impressions for 2 sided/2 pages per side printing" = 4, and calculates "Sheets required to print 1 set in 2 pages per side/2 sided printing". Sheets required to print 1 set in 2 pages per side/2 sided printing = Assumed original impressions / 4 (decimal points are rounded out)
4.	Multiplies "Sheets required to print 1 set in 2 pages per side/2 sided printing" by the number of copies to calculate "Total sheets required for 2 pages per side/2 sided printing". Total sheets required for 2 pages per side/2 sided printing = Sheets required to print 1 set in 2 pages per side/2 sided printing x Copies
5.	When the value reached by subtracting "Total sheets required for 2 pages per side/2 sided printing" from "Sheets used" exceeds 1, this determines reduction to be possible, and calculates "Possible Paper Reduction". Possible Paper Reduction = Actual output sheets - Total sheets required for 2 pages per side/2 sided printing

Formula when paper reduction calculation parameter is [Pages per Side]

The sheets reduced with only pages per side printing are calculated as Possible Paper Reduction. The calculation method is as follows.



Note

The numbers of the table indicate the calculation procedure executed by the program. They do not indicate operations by users.

1.	Since total values of multiple sets are recorded in impressions of the job log, "Impressions of 1 set unit" is calculated. Impressions of 1 set unit = Impressions / Copies
2.	Divides "1 set unit of impressions" by "Original impressions for 1 sided/2 pages per side printing" = 2, and calculates "Sheets required to print 1 set in 2 pages per side/1 sided printing". Sheets required to print 1 set in 2 pages per side/1 sided printing = 1 set unit of impressions / 2 (decimal points are rounded out)
3.	Multiplies "Sheets required to print 1 set in 2 pages per side/1 sided printing" by the number of copies to calculate "Total sheets required for 2 pages per side/1 sided printing". "Total sheets required for 2 pages per side/1 sided printing" = Sheets required to print 1 set in 2 pages per side/1 sided printing x Copies
4.	When the paper reduction calculation parameter is set to [Pages per Side], this considers "Impressions used" as sheets output. When the value reached by subtracting "Total sheets required for 2 pages per side/1 sided printing" from "Sheets used" exceeds 1, this determines reduction to be possible, and calculates "Possible Paper Reduction". Possible Paper Reduction = Impressions used - Total sheets required for 2 pages per side/1 sided printing

Formula when paper reduction calculation parameter is [2 Sided]

The sheets reduced with only 1 sided printing are calculated as Possible Paper Reduction. The calculation method is as follows.



Note

The numbers of the table indicate the calculation procedure executed by the program. They do not indicate operations by users.

1.	Since total values of multiple sets are recorded in impressions of the job log, "Impressions of 1 set unit" is calculated. Impressions of 1 set unit = Impressions / Copies
2.	Divides "1 set unit of impressions" by "Original impressions for 2 sided/1 page printing" = 2, and calculates "Sheets required to print 1 set in 2 sided/1 page printing". Sheets required to print 1 set in 2 sided/1 page printing = 1 set unit of impressions / 2 (decimal points are rounded out)

3.	Multiplies "Sheets required to print 1 set in 2 sided/1 page printing" by the number of copies to calculate "Total sheets required for 2 sided/1 page printing". Total sheets required for 2 sided/1 page printing = Sheets required to print 1 set in 2 sided/1 page printing x Copies
4.	When the value reached by subtracting "Total sheets required for 2 sided/1 page printing" from "Sheets used" exceeds 1, this determines reduction to be possible, and calculates "Possible Paper Reduction". Possible Paper Reduction = Sheets used - Total sheets required for 2 sided/1 page printing

Converting an Account ID Value

You can change the value in [Account ID] to an account managed by ApeosWare Management Suite when outputting a job log file.

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Open the following file with a text editor.
Folders: {Folder of data storage directory}\Data\karaf\etc
File name: joblogexport.properties
{Folder of data storage directory} is as follows if the default settings are not changed.
C:\FUJIFILM\ApeosWare MS
3. Change the setting value in Properties below and overwrite it.

Properties	Descriptions
com.fujifilm.fb.apeosware.joblog.export.accountmapping	Sets whether to convert the value in the job log file item "Account ID" into an account name managed by ApeosWare Management Suite. true: Converts the value recorded in the job log to the corresponding account name. false or no properties: The values collected from the device remain the same without being converted. Changing this property does not affect job log files already output. If the account name is changed when the setting value of this property is true, the account name in job log files already output does not change.



Note

If property "com.fujifilm.fb.apeosware.joblog.export.accountmapping" does not exist, com.fujifilm.fb.apeosware.joblog.export.accountmapping=true is added as a line.

4. Reboot the PC.

12 Maintenance

Backup and Restoration

This section describes the backup and restoration of ApeosWare Management Suite. Execute backup on a regular basis to reduce the risk of losing important information.

Overview

Backup and restoration are executed for the following purpose.

- Execute backup in case that some faults should happen to the ApeosWare Management Suite server. If that should happen, restore information and get back to the status at the time of backup.
- To operate the ApeosWare Management Suite server in a multiplexing or distributed configuration, restore information backed up from the duplicate source to the duplicate destination so as to duplicate the server.



Note

Moreover, when Flow Management Option is already installed, service in Flow Management Option needs to be stopped before settings in Windows. For procedures, refer to “Start or Stop Flow Management Service” in “Features Guide Flow Management Option”.

Command

When making a backup, use the command “backup.exe”.

To restore, use the command “restore.exe”.

Both “backup.exe” and “restore.exe” are copied to the following directory when ApeosWare Management Suite is installed.

{ApeosWare Management Suite installation folder}\Utils\BackupTool

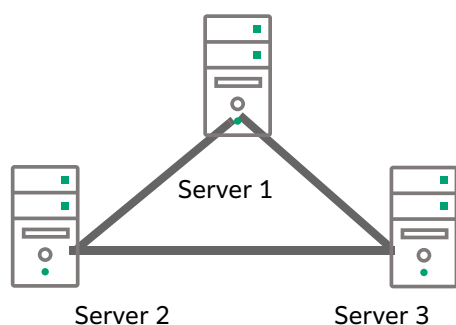


Note

- Copy files to the following folder on flow servers.
{ApeosWare Management Suite installation folder}\FM\tools\BackupTool
- By default, the ApeosWare Management Suite installation folder is “C:\Program Files\FUJIFILM\ApeosWare MS”.

Target for backup and restoration

The target for backup and restoration is a PC that has “backup.exe” and “restore.exe”. Therefore, in operation with the server being a multiplexing or distributed configuration, you need to back up and restore the whole server.



In each of Server 1 to Server 3, backup and restoration must be executed on all servers
Also, backup and restoration must be executed at all sites.

Backup target specification options	ApeosWare Management Suite Main Unit, Flow Management Option, Etc.		Image Log Management Option						Others
	Setting	Log	Setting	Log	Image log data			DB	
					Receiving spool	Storage	Archive		
(Default)	○	○	○	○	×	×	×	○	
Exclude log folder (-sl)	○	×	○	×	×	×	×	○	
Add receiving spool (-y_ilmRspool)	○	○	○	○	○	×	×	○	
Combination (-sl -y_ilmRspool)	○	×	○	×	○	×	×	○	
Storage backup (-only_ilmStorage) * Cannot be combined with other options	×	×	×	×	×	○	×	×	

When backup is performed, all the following settings data items are backed up.

Backup of individual data is not available. License is not confirmed at the time of backup.

- Device Management
- User Management
- Print Management



Note

Print jobs and documents in temporary folder are initialized (deleted).

- Cost Management
- Download Management (Supported by devices only used in Japan)
- Mobile Settings

- Scan Settings



Note

Scan jobs and documents in temporary folder are initialized (deleted).

- File Management Service Settings
- Server Monitoring Settings
- Flow Management Option settings



Note

The restoration only restores the flow and settings information, and all the “jobs” and “documents” are initialized (deleted).

- Paper Form Management settings

Independent restoration is not available. License is not confirmed at the time of restoration.

When restoring the backup data after making any additional installation of Flow Management Option feature, perform the restoration of Flow Management Option having all the added features.

Any subsequent installation attempt will fail if you try to install an additional feature after you perform restoration of Flow Management Option that did not have the added feature in question.

If such a case occurs, re-install Flow Management Option, install all of the features existed in the backed up environment, and then execute the restoration.

- Image Log Management settings
- Image log data



Note

- Only the image log data stored in Image Log Management is backed up (when -only_ilmStorage is specified in the command option of backup described later). Backup is not performed unless the option is specified.
- The upper limit of the number of image log data that can be backed up and restored is 600,000 jobs.
- The archive data of Image Log Management does not qualify as image log data that can be backed up and restored. If archive data is required, move the folder below to an arbitrary storage.
{Folder for saving image log}\exported

Conditions for Backup and Restoration

Backup and restoration need to be operated on the following conditions.

- “backup.exe” and “restore.exe” are not being run.
- Backup target data is not modified while the backup process is active.
- Execute operation as a user of the Administrators group.
- Users are able to log in to SQL Server with Integrated Windows Authentication and given the permission of the backup and restoration.
- Users are given write permissions to the backup file output folder, as well as read permissions for the folder containing backup files. Additionally, a different account can be specified with write permissions to the backup file output folder and read permissions for folders containing backup files.
- The software versions of data back upped and data to be restored correspond.
- The version of the SQL Server in the restoration resource is identical or upward compatible with that of the SQL Server in the backup destination .
- The Edition of the SQL Server in the restoration resource is identical or upward compatible with that of the SQL Server in the backup destination.

**Note**

- When executing backup and restoration on the Image Log Management core server, execute backup and restoration on the Image Log Management core server before executing backup and restoration of the incoming server.
- When executing backup on the Image Log Management core server, ApeosWare Management Suite Image Log Management Core Service must be stopped on the incoming server. After completion of backup, start the service stopped.

Options

This section describes the options of “backup.exe” and “restore.exe”.

Options	Descriptions
-e	Connect to the SQL Server using Integrated Windows Authentication. If you do not use either this option or -u, you are considered to have used this option. Options -u and -p cannot be used concurrently. Simultaneous usage will result in an error.
-u {User name of an account to connect to the SQL Server}	Use it to execute backup or restoration by connecting to the SQL Server with an account user name different from the user who logged on to Windows. This option is used along with -p.
-p {Account password to connect to SQL Server with}	Use it to execute backup or restoration by connecting to the SQL Server with an account password of the user different from the user who logged on to Windows. This option is used along with -u.
-o {Folder path of the backup destination or the restoration source}	Set the path for the backup file output folder, and for folders containing backup files, and perform backup or restore. An error will occur if this option is not specified.
For backup -rdb {Path to backup file output folder} For restore -rdb {Path to the folder containing backup files}/{Backup date}	Specify the backup destination or restoration resource of the database when the database server is separately configured. • To back up Specify the path to backup file output folder. The data is backed up in the specified folder on the node on SQL Server. • To restore Specify the path to folders containing backup files, as well as the date of backup, linked with a slash (/). The date format is “yyyyMMdd-HH:mm:ss”. Example: -rdb backfolder/20200514-103005 From the specified folder on node of SQL Server, search a backup file by the specified date, and restore it.  Note • For the folder, specify a folder readable/writable from SQL Server Service. Also specify a folder on the node of SQL Server. • When the database server is separately configured, it is required to specify both -o option and -rdb option. Specify the backup destination or restoration source for the database with -rdb option, and specify those for other than the database with -o option.

Options	Descriptions
-ou {Account user name to access the folder of the backup destination or the restoration source with}	For backup: Used when connecting and backing up with an account with write permissions for the backup file output folder, separate to the user logged in to Windows. This option is used along with -op.
	For restoration: Used when connecting and backing up with an account with read permissions for folders containing backup files, separate to the user logged in to Windows. This option is used along with -op.
-op {Account password to access folder in backup destination or in restoration source}	For backup: Used when connecting and backing up with the password for an account with write permissions for the backup file output folder, separate to the user logged in to Windows. This option is used along with -ou.
	For restoration: Used when connecting and backing up with the password for an account with read permissions for folders containing backup files, separate to the user logged in to Windows. This option is used along with -ou.
-nr	The target command is "restore.exe". The "restore.exe" stops the service before restoring and starts the service after restoration. Use this option when you do not start the service after restoration.
-sl	For backup: Use this option when a type does not back up the backup target of a log folder.
-y_ilmRspool	The target command is "backup.exe". Backs up the Image Log Reception spooled data.  Note • At the time of backup, stops ApeosWare Management Suite Image Log Management Receive Service and backs up the Image Log Reception spooled data. After completion of backup, start ApeosWare Management Suite Image Log Management Receive Service. • The ApeosWare Management Suite 2 Image Log Management backup tool is not used with this option.
-only_ilmStorage	The target command is "backup.exe". Uses the backup tool of ApeosWare Management Suite 2 Image Log Management to back up only the storage data of the image log. Other data such as the settings and receiving spool data of ApeosWare Management Suite 2 and ApeosWare Management Suite 2 Image Log Management cannot be backed up simultaneously. Note that -only_ilmStorage cannot be used together with another option (such as -sl).  Note • This option can only be specified on a node where the Image Log Core Server is installed. • At the time of backup, stops ApeosWare Management Suite Image Log Management Core Service and starts the service after receiving a notice of ApeosWare Management Suite 2 Image Log Management backup tool. • The Windows Server backup included with the OS is required for the ApeosWare Management Suite 2 Image Log Management backup tool used with this option. • The backup destination drive cannot be the same drive as the install folder and image log data folder.

Storage location of the backup file of image log storage data

The backup file of the image log storage data is stored by creating WindowsImageBackup directly under the drive where the root folder of the backup destination specified by the tool exists.

Storage Destination of Backup File and Path to Be Specified for Restoration

The paths for the backup file destination when the backup command is executed and for the folder containing backup files specified by the restore command are as follows.

When the data is not configured separately

- Storage location of the backup file

Backup is made in the following location.

{Folder path specified with -o option}%{Computer name of the server}%{Backup date}-{Hour, minute, and second of backup}

Example:

When specifying "C: %backfolder" with -o option, and when the backup is executed with the computer name "hostname" on May 14, 2020 at 5 seconds past 10:30, the backup is created in the following folder.

C:backfolder%hostname%20200514-103005

- Path to be specified for restoration

For the example noted above, specify the restoration command as follows.

```
restore -o C:%backfolder%hostname%20200514-103005
```

When the database is not separately configured.

When the database server is separately configured, specify both -o option and -rdb option. Specify the backup destination or restoration source for other than the database with -o option, and specify those for the database with -rdb option.

- Storage location of backup file for other than database

It is the same as with the case for "When the data is not configured separately".

- Storage location of the backup file for database and the file name

The backup is made in the following location with the following name.

{Folder path specified with -rdb option}%{Database name}_{Backup date}-{Hour, minute, and second of backup}.bak

Example:

When specifying "C:%db_backfolder" with -rdb option, and when the backup is executed with the database name "db_name" on May 14, 2020 at 5 seconds past 10:30, the following file is backed up.

C:%db_backfolder%db_name_20200514-103005.bak on the SQL Server node

- Path to be specified for restoration

For -rdb option, specify the path that is specified when the backing up with -rdp option and the backup date by combining them with slash (/). For the example noted above, specify the restoration command as follows.

```
awms2restore -o C:%backfolder%hostname%20200514-103005 -rdb C:%db_backfolder/20160514-103005
```

Back up

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Take necessary measures if the conditions described in “Conditions for Backup and Restoration” (P.368) are not satisfied.
3. Open a command prompt window as an administrator.
4. Enter the following command and press the <Enter> key.

```
cd {Installation Folder}\Utils\BackupTool
```

5. Enter the following command and press the <Enter> key.

- When the logged-in user has permissions to back up the database and write permissions to the backup file output folder

Each function of the ApeosWare Management Suite installed on the logged-on server, the Flow Management Option settings, and the Image Log Management Option settings are backed up. Since the storage of the image log is out of scope, execute the process separately with an option for backing up only the storage.

```
backup -e -o {Path to backup file output folder}
```

If the image log receiving spool is included, perform backup by adding the following options.

```
backup -e -o {Path to backup file output folder} -y_ilmRspool
```

The same usage method is used for subsequent cases of each user.

- When the log-on user is not given the authority to back up a database

Execute backup by connecting to the SQL Server with a user account which has authority over backup different from the log-on user.

```
backup -u {Account user name to connect to the SQL Server with} -p {Account password to connect to the SQL Server with} -o {Path to backup file output folder}
```

- When the logged-in user does not have write permissions to the backup file output folder

Backs up using a user account with write permissions to the backup file output folder, separate to the user logged in.

```
backup -e -o {Path to backup file output folder} -ou {Account user name to access a backup file output folder with} -op {Account password to access a backup file output folder with}
```

- When the log-on user is not given the authority to back up a database and write in a backup file output folder

Execute backup with a user account which has the authority to back it up and write in a backup file output folder different from the log-on user.

```
backup -u {Account user name to connect to the SQL Server with} -p {Account password to connect to the SQL Server with} -o {Path to backup file output folder} -ou {User name for account accessing the backup file output folder} -op {Password for account accessing the backup file output folder}
```

The set information is backed up in the specified folder. The backup data is stored in a folder "{Backup date} - {Hour, minute, and second of backup}". If the backup fails, refer to "Description and Handling of the Exit Code" (P.374), and take necessary measures.

■ When a backup of storage data of Image Log Management is to be taken

```
backup -e -o {Path to backup file output folder} -only_ilmStorage
```

When "-only_ilmStorage" is specified, only the storage of the image log is backed up. Execute the process separately without "-only_ilmStorage."



Note

- The size is large in a lot of cases, and therefore, it is expected that some time would be taken.
- When "-only_ilmStorage" is used, use different drives for image log storage and the backup file output folder.
- Specify the same storage path for the backup file output folder when "-only_ilmStorage" is specified and when it is not.

Restore

When restoring the main server and separate servers in distributed configurations, the main server must be restored first before updating the main server information configured in separate servers. Neglecting to perform this procedure will cause communication between the main server and the separation server to fail. On each of the separate servers, execute the "HostnameSetup.exe" command with the "-NM" option specified.

For details on the command, refer to "Changing Server Information" (P.376).

1. Log on to the PC in which ApeosWare Management Suite is installed with the user in the Administrators group.
2. Take necessary measures if the conditions described in "Conditions for Backup and Restoration" (P.368) are not satisfied.
3. Open a command prompt window as an administrator.
4. Enter the following command and press the <Enter> key.

```
cd {Installation Folder}\Utils\BackupTool
```

5. Enter the following command and press the <Enter> key.



Note

To the {Path to the folder containing backup files}, specify the storage location of the backup file. Refer to "Storage Destination of Backup File and Path to Be Specified for Restoration" (P.371).

■ When the log-on user is given the authority to restore a database and read a folder containing backup files

Each function of the ApeosWare Management Suite included in the folder containing backup files, the Flow Management Option settings, and the Image Log Management Option settings are restored.

If the storage of the image log (WindowsImageBackup folder) is included at the specified destination, it is also included as a restore target.

```
restore -e -o {Path to the folder containing backup files}
```

■ When the log-on user is not given the authority to restore a database

Execute restoration by connecting to the SQL Server with a user account which has authority over restoration different from the log-on user.

```
restore -u {Account user name to connect to the SQL Server with} -p {Account password to connect to the SQL Server with} -o {Path to the folder containing backup files}
```

■ When the log-on user is not given the authority to read a folder containing backup files

Execute restoration with a user account which has authority to read a folder containing backup files.

```
restore -e -o {Path to the folder containing backup files} -ou {Account user name to access the folder containing backup files with} -op {Account password to access the folder containing backup files with}
```

■ When the log-on user is not given the authority to restore a database and read a folder containing backup files

Execute restoration with a user account which has authority to read a folder containing backup files.

```
restore -u {User name to access SQL Server} -p {Account password to access SQL Server} -o {Path to the folder containing backup files} -ou {User name to access the folder containing backup files with} -op {Account password to access the folder containing backup files with}
```

■ When service is not started after restoration

```
restore -nr
```

Backup information is restored. If the restoration fails, refer to “Description and Handling of the Exit Code” (P.374), and take necessary measures.

6. If you use the -nr option in the procedure 5, service is started.

Description and Handling of the Exit Code

If the message of solution is displayed, follow it.

Exit code	Description and solution
0	Backup or restoration is normally finished.
2	The backup completed but the database or some files were not backed up.
4	Backup or restoration is being executed. Execute it after the job is finished.
6	There is no data suitable for backup or restoring.
8	Your option is wrong.
10	No permission to reference the registry. Execute it as a user of the Administrators group.
12	Target data cannot be referenced because you are accessing target data for other processes to back up such as anti-virus software or you have no access rights.
14	Could not log on to the PC containing the specified backup file output folder or the folder containing backup files. Input the correct user name and password.
16	For backup: No [Write] permissions for the specified backup file output folder. Execute it in a permitted account. For restoration: No [Read & execute] permissions for the specified folder containing backup files. Specify the correct folder. Execute it in a permitted account.
18	Free space is short in the specified backup file output folder. Specify another folder.

Exit code	Description and solution
20	For backup: There is already backed-up data present in the backup file output folder. To leave it, transfer it to another folder.
	For restoration: There is no folder containing backup files. Specify the correct folder.
22	The SQL Server is not installed.
24	You cannot log in to the SQL Server with the specified account. Input the correct user name and password.
26	You have failed in backing up or restoring a database.
28	For backup: Failed to write to the backup file output folder. If you do not have permissions, execute with a user that does have permissions. When another application is using the backup file output folder, close that application. If a network failure is occurring, please work it out.
28	For restoration: Failed to write to the folder containing backup files. If you do not have permissions, execute with a user that does have permissions. When another application is using the folder containing backup files, close that application. If a network failure is occurring, please work it out.
30	You have failed in referencing a list file for backup targets.
40	Database in the restoration source is not found in the database instance.
42	The database is not backed-up to the folder containing backup files. Confirm whether the specified folder is correct.
44	There is no data backed up to the folder containing backup files. Confirm whether the specified folder is correct.
50	You have failed in service stop.
52	You have failed in start of service.
54	You have failed in processing after restoration.
56	
58	

Changing Server Information

Overview

This section describes how to change the following information on the server.

- Host name or IP address
- Validity and invalidity of SSL
- Port number



Note

- Targets for host names, IP addresses, SSL settings, and port numbers are the ones set on the IIS website at the time of installing ApeosWare Management Suite.
- This section describes the procedure after setting host names, IP addresses, SSL settings, and port numbers in Windows. Perform the procedure of this section after settings in Windows. Moreover, when Flow Management Option is already installed, service in Flow Management Option needs to be stopped before settings in Windows. For procedures, refer to “Start or Stop Flow Management Service” in “Features Guide Flow Management Option”.

Change host names, etc. by using the command “HostnameSetup.exe”. It is necessary to restart the server after change.

After that, it may be necessary to change ApeosWare Management Suite settings.

Location of the command

“HostnameSetup.exe” is copied to the location shown below when ApeosWare Management Suite is been installed.

- In case of the Main Server or Image Log server, or the OCR server, print server or mobile server in a distributed configuration, the command is copied in the following location.

{Installation destination of ApeosWare Management Suite*1}\Utils\Hostname Setting

- In case of the flow server, the copy destination is as below.

{Installation destination of ApeosWare Management Suite*1}\FM\tools\Hostname Setting

*1 The default value is “C:\Program Files\FUJIFILM\ApeosWare MS”.



Note

HostnameSetup.exe is not available for the report server. When changing the report server information, refer to “When changing the report server information” (P.388).

Options

Option to change performing server settings

Options	Descriptions
-N {Host name or IP address}	Change the host name or IP address of the server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN

Options	Descriptions
-S {http or https}	Change the SSL settings of the web service provided by the server. Enter "http" to unset the SSL settings. Enter "https" to set the SSL settings.
-P {Port number}	Change a port number to provide the web service. Available port numbers are 0 - 65535.
-PSSL {Port number}	Change a port number for SSL. Available port numbers are 0 - 65535.  Note When -S https is specified, the following value is applied. • When -S http is specified but -P is not specified, the registry (Port) value is applied. • When -S https and -P XXX are specified, the value of -P (XXX) is applied to -PSSL. • When -S https, -P XXX, and -PSSL YYY are specified, an error occurs if the values of XXX and YYY do not match.



Refer

Execution example→"When you change the host name or the IP address of the server in all-in-one structure" (P.380)

Options to change information on another server set on servers with multiplexing structure

If changing information on another server set on servers with a multiplexing structure, change the host name or IP address.



Refer

Execution example→"When the host name or IP address is changed with the server of multiplexing configuration" (P.387)

Option to change the destination of database server

Option list

Options	Descriptions
-D {Host name of the database}	Change the database to the specified destination. When -D is specifier, either of -DE or the combination of -DU/-DP is required to be specified.  Note If there is a database in a server to execute a command, it is not necessary to specify the -D option.
-DE	Windows Authentication is used to connect the database server.
-DU {User name}	SQL Server Authentication is used to connect the database server. Specify the user name to be connect.
-DP {Password}	SQL Server Authentication is used to connect the database server. Specify the password of the user name to be connect.
-DN {Port number}	Change the port number of the database server. It can be done only on the main server and the flow server. Example of Port Number: "1433"

Options to change information on the main server set on the print server

You can perform this on the print server.

Option list

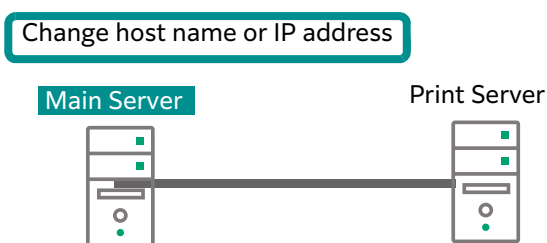
Options	Descriptions
-NM {Host name or IP address}	Change the host name or IP address of the main server set on the print server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN
-SM {http or https}	Change the SSL setting on the main server set on the print server. Enter "http" to unset the SSL settings. Enter "https" to set the SSL settings.
-PM {Port number}	Change a port number on the main server set on the print server. Available port numbers are 0 - 65535.



Refer

Execution example→"When the host name and IP address are changed with the main server and print server of a distributed configuration" (P.384)

How to use the -NM option



Execute a command by specifying the main server for the -NM option as follows.

```
HostnameSetup.exe -NM {Host name or IP address of main server after change}
```

Option to change information on the report server set on the main server.

When a separate report server is set up, an execution can be done on the main server.

Option list

Options	Descriptions
-NR {Host name or IP address}	Change the host name or IP address of the report server set on the main server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN

Option to change information on the main server set on the OCR server

This option can be executed on the OCR server.

Option list

Options	Descriptions
-NM {Host name or IP address}	Change the host name or IP address of the main server set on the OCR server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN

Option to change information of the main server set on the mobile server

The option can be executed on the mobile server.

Option list

Options	Descriptions
-NM {Host name or IP address}	Change the host name or IP address of the main server set on the mobile server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN

Option to change information of the main server set on the flow server

The option can be executed on the flow server.

Option list

Options	Descriptions
-NM {Host name or IP address}	Change the host name or IP address of the main server set on the flow server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN
-SM {http or https}	Changes the main server SSL settings configured on the flow server. Enter "http" to unset the SSL settings. Enter "https" to set the SSL settings.
-PM {Port number}	Changes the port number of the main server set on the flow server. Available port numbers are 0 - 65535.



Refer

Execution example→"When the host name and IP address are changed with the main server and print server of a distributed configuration" (P.384)

Option to change information on the Main Server set on the Image Log server

This option can be executed on the Image Log server.

Option list

Options	Descriptions
-NM {Host name or IP address}	Changes the host name or IP address of the Main Server set on the Image Log server to what you have input in {Host name or IP address}. Input it in any one of the following formats which can communicate externally. • IPv4 format IP address • IPv6 format IP address • FQDN

Options to display what is set at present and options for help

Options	Descriptions
-G	Display the host name or IP address, a port number and the SSL settings set at present. The server to be displayed for settings depends on the server to be executed as follows. • All-in-one structure server and multiplexing server The setting for the server to execute it is displayed. • Main Server The setting for the server to execute it is displayed. For the multiplexing server, that setting is displayed too. • Print Server The setting for the server to execute it and for the main server are displayed. • Flow Server The setting for the server to execute it and for the main server are displayed.
-H or --HELP	Help is displayed.



Refer

Execution example→“Save the setting before change” (P.380)

Execution example

When you change the host name or the IP address of the server in all-in-one structure

Save the setting before change

Save the settings before change in the text file in case that failure should occur.

1. Open a command prompt window as an administrator.
2. Enter the following command and press the <Enter> key.

```
cd /d c:\{Installation destination of ApeosWare Management Suite}\Utils\Hostname Setting
```

3. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -G > {Arbitrary file name}.txt
```

What has been set is saved in the text file.

Change with command

1. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -N {Host name or IP address of after change}
```

The setting is changed. It may take time to finish it.

2. Restart the server.
3. Set the device and client as necessary.

When you change the port number of the server in all-in-one structure

Change with command

1. Perform the following steps.

- When you change a port number to provide the web service
Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -P {Port number of after change}
```

The setting is changed. It may take time to finish it.

- When you change a port number for SSL
Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -PSSL {Port number of after change}
```

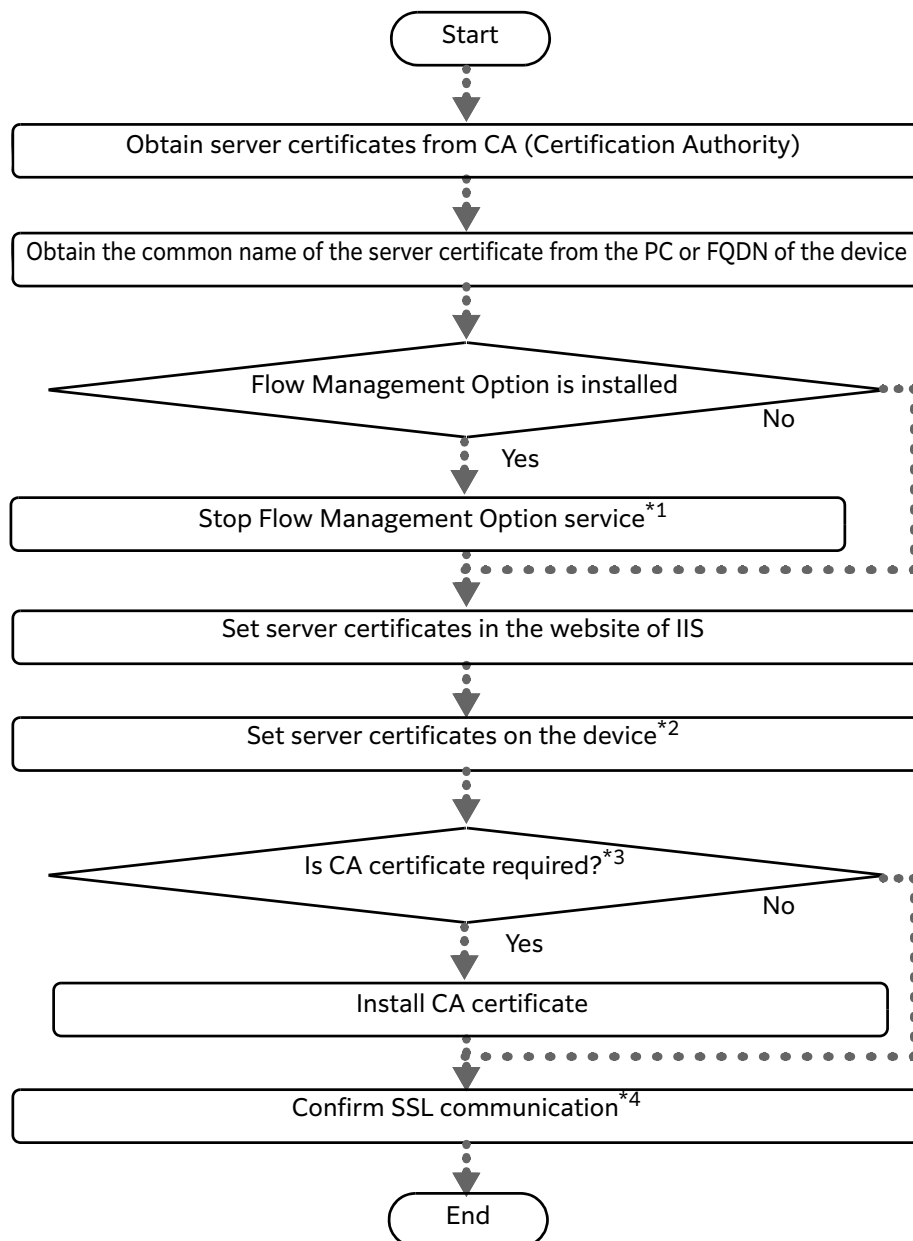
The setting is changed. It may take time to finish it.

2. Restart the server.
3. Set the device and client as necessary.

When you encrypt the server communication in all-in-one structure (SSL)

Encrypt the server communication

Execute the following procedure to encrypt communication.



*1 For procedures, refer to “Features Guide Flow Management Option” > “2.4 Start or Stop Flow Management Option Service”.

*2 Refer to the manual provided with the device you are using.

*3 Any one of the following cases:

- With the set server certificate, safety cannot be confirmed with the web client root certificate, and a security warning is displayed in the web browser
To prevent the security warning from being displayed, accept the certificate or install a root CA certificate corresponding to the server certificate to the web client.
- When server certificate requires an intermediate certificate for the authentication based on the root certificate
To the configured PC, store the CA certificate of the intermediate certification body.
- With types that authentication of server certificate is not made based on the root certificate
To the web client, store the CA certificate of the root certification body.

- *4 To the website to be used on the ApeosWare Management Suite server software for which the server certificate is set, access from the web client by using the URL below. Enter the same FQDN or the IP address as the common name of the server certificate for the host name. Make sure the default page of IIS is displayed, and the key mark appears on the bottom right of the web browser window.

```
https://{Host name}/
```



Note

- When the server certificate for SSL communication with a device has been installed on the PC with ApeosWare Management Suite installed, reboot the PC.
- When the certificate for SSL communication with Active Directory has been installed on the PC with ApeosWare Management Suite installed, restart the ApeosWare Management Suite Core Service.

When LDAPS communication is performed with the ApeosWare Management Suite server and LDAP server

Install a root CA certificate and a certificate of intermediate certification authority on the Windows certificate store.

Save the setting before change

1. Perform the steps described in “Save the setting before change” (P.380).

Changing SSL with a command

1. Open a command prompt window as an administrator.
2. Enter the following command and press the <Enter> key.

```
cd /d c:\{Installation destination of ApeosWare Management Suite}\Utils\Hostname Setting
```

3. Change SSL on the logon server
Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -S https -P {Port number for SSL communication}
```

The setting is changed. It may take time to finish it.

4. Restart the server.
5. Set the device and client as necessary.

When the host name or IP address of the database server are changed with the structure separating the database

Save the setting before change

Save the settings before change in the text file in case that failure should occur.
Perform this operation on the main server.

1. Open a command prompt window as an administrator.
2. Enter the following command and press the <Enter> key.

```
cd /d c:\{Installation destination of ApeosWare Management Suite}\Utils\Hostname Setting
```

3. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -G > {Arbitrary file name}.txt
```

What has been set is saved in the text file.

Change with command

1. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -D {IP address of after change} [-DE or -DU {User name} -DP {Password}]
```

The setting is changed. It may take time to finish it.

2. Restart the server.

3. Set the device and client as necessary.

When the host name and IP address are changed with the main server and print server of a distributed configuration

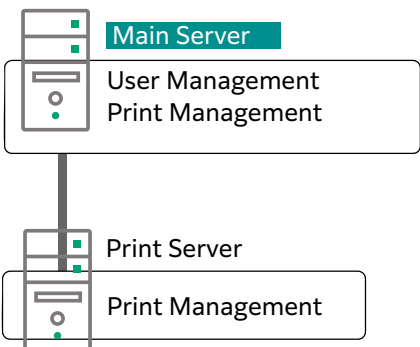
This section describes the procedure to be performed when either the host name or IP address has been changed on the main server, print server, or both in distributed configurations.

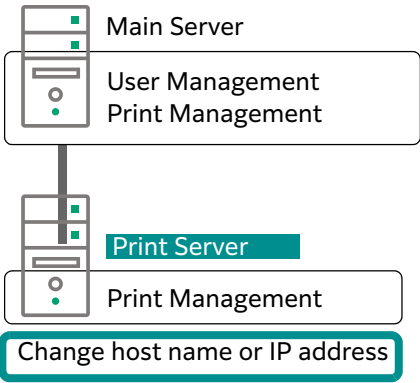
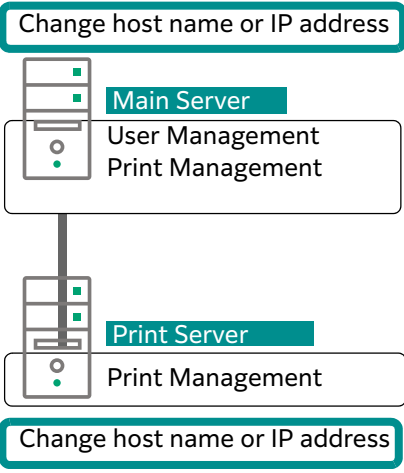


Note

The distributed configuration with the separated print server is available for use only with Enterprise Edition.

Change flow

Condition*1	Content of implementation and order
Change host name or IP address  The diagram illustrates a distributed configuration. At the top, a box labeled 'Main Server' contains two sub-components: 'User Management' and 'Print Management'. Below it, connected by a vertical line, is a box labeled 'Print Server' which contains a 'Print Management' component.	(1) Execute the contents of "Saving settings of before change on the print server" (P.385)*2 (2) Execute the contents of "Change with command" (P.381) with the Main Server (3) Execute the contents of "Changing the host name or IP address of the main server set on the print server" (P.386) with the print server*2

Condition ^{*1}	Content of implementation and order
 Main Server User Management Print Management Print Server Print Management Change host name or IP address	(1) Execute the contents of "Saving settings of before change on the print server" (P.385) ^{*2} (2) Execute the contents of "Change with command" (P.381) with the print server ^{*2}
 Change host name or IP address Main Server User Management Print Management Print Server Print Management Change host name or IP address	(1) Execute the contents of "Saving settings of before change on the print server" (P.385) ^{*2} (2) Execute the contents of "Change with command" (P.384) with the Main Server (3) Execute the contents of "Changing the host name or IP address of the main server set on the print server" (P.386) with the print server ^{*2} (4) Execute the contents of "Change with command" (P.384) with the print server ^{*2}

*1 The main server and the print server are supposed to link.

*2 If there are more than one print server, execute the same procedure for each print server.

Saving settings of before change on the print server

Save the settings before change in the text file in case that failure should occur.

1. Log on to a PC on the print server with the Administrator permission.
Log out if you are already logged on and logged in to ApeosWare Management Suite.
2. Open a command prompt window as an administrator.
3. Enter the following command and press the <Enter> key.

```
cd /d c:\{Installation destination of ApeosWare Management Suite}\Utils\Hostname Setting
```

4. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -G > {Arbitrary file name}.txt
```

What has been set on the main server and print server is saved in the text file.

Changing the host name or IP address of the main server set on the print server

1. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -NM {Host name or IP address of main server after change}
```

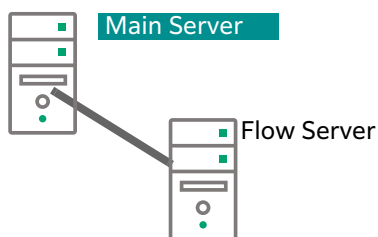
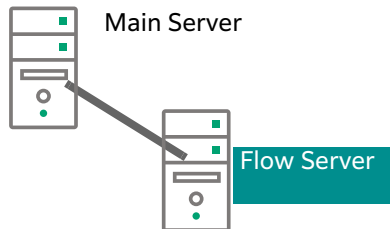
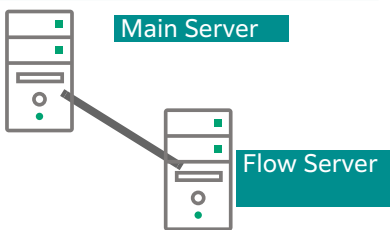
The setting is changed. It may take time to finish it.

2. Restart the server.

When the host name and IP address are changed with the main server and flow server of a distributed configuration

Procedures are described when either the main server or the flow server or both host names or both IP addresses are changed with a distributed configuration of Enterprise Edition.

Change flow

Condition	Content of implementation and order
Change host name or IP address 	(1) Execute the contents of "Saving settings of before change on the flow server" (P.386) (2) Execute the contents of "Change with command" (P.384) with the Main Server (3) Execute the contents of "Changing the host name or IP address of the main server set on the flow server" (P.387) with the flow server
 Change host name or IP address	(1) Execute the contents of "Saving settings of before change on the flow server" (P.386) (2) Execute the contents of "Change with command" (P.384) with the flow server (3) Start the main server
Change host name or IP address  Change host name or IP address	(1) Execute the contents of "Saving settings of before change on the flow server" (P.386) (2) Execute the contents of "Change with command" (P.384) with the Main Server (3) Execute the contents of "Change with command" (P.384) with flow server (4) Start the main server

Saving settings of before change on the flow server

Save the settings before change in the text file in case that failure should occur.

1. Log on to a PC on the flow server with the Administrator permission.
Log out if you are already logged on and logged in to ApeosWare Management Suite.

2. Open a command prompt window as an administrator.
3. Enter the following command and press the <Enter> key.

```
cd /d c:¥{Installation destination of ApeosWare Management Suite}¥FM¥tools¥Hostname Setting
```

4. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -G > {Arbitrary file name}.txt
```

What has been set on the main server and print server is saved in the text file.

Changing the host name or IP address of the main server set on the flow server

1. Enter the following command and press the <Enter> key.

```
HostnameSetup.exe -NM {Host name or IP address of main server after change}
```

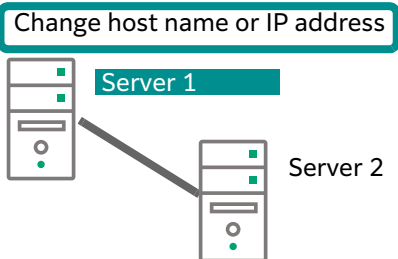
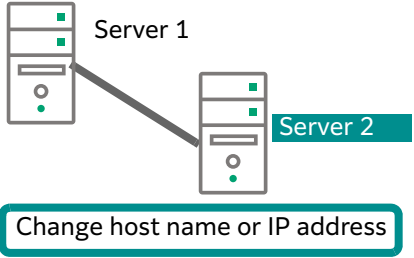
The setting is changed. It may take time to finish it.

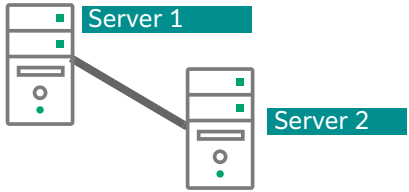
2. Restart the server.

When the host name or IP address is changed with the server of multiplexing configuration

Procedures are described when the host name or IP address on the server is changed with a distributed configuration of Enterprise Edition.

Change flow

Condition	Procedure of implementation and order
 Change host name or IP address Server 1 Server 2	(1) Execute the contents of “When you change the host name or the IP address of the server in all-in-one structure” (P.380) with server 1 (2) Execute the contents of “Changing the host name or IP address of the server set for a device group” (P.388) with server 2*1
 Server 1 Server 2 Change host name or IP address	(1) Execute the contents of “When you change the host name or the IP address of the server in all-in-one structure” (P.380) with server 2 (2) Execute the contents of “Changing the host name or IP address of the server set for a device group” (P.388) with server 1*1

Condition	Procedure of implementation and order
Change host name or IP address  Change host name or IP address	(1) Execute the contents of “When you change the host name or the IP address of the server in all-in-one structure” (P.380) with server 1 (2) Execute the contents of “Changing the host name or IP address of the server set for a device group” (P.388) with server 2*1 (3) Execute the contents of “When you change the host name or the IP address of the server in all-in-one structure” (P.380) with server 2 (4) Execute the contents of “Changing the host name or IP address of the server set for a device group” (P.388) with server 1*1

*1 After that, set a device and client as necessary.

Changing the host name or IP address of the server set for a device group

1. Login to ApeosWare Management Suite.
2. Select [Service Settings] > [Device Management] > [Device Groups] in the menu.
3. Operate the following in the [All Device Group] page.
 - (1) In the [Operation] column of target device group, click .
 - (2) Click [Properties].
4. Operate the following in the [Device Group Properties] page.
 - (1) Click [Basic Settings].
 - (2) Select a host name and IP address after change in [Primary Server IP Address/Host Name].
 - (3) Select a host name and IP address after change in [Secondary Server IP Address/Host Name].
 - (4) Click [Save and Close].

When the time and intervals set in the [Device Data Condition Update Settings] page come, the changed information is updated to a device.

When changing the report server information

The command “HostnameSetup.exe” is not available for the report server.

If the instance name of the database used for the report server is changed, uninstall the report server and reinstall it with the updated instance name.

Operation Log

The storage location and file name of the operation log of Command “HostnameSetup.exe” are as follows.

Storage location	File name
{Data Storage Location Folder}*1\Data\Common Utility\Hostname Setting\logs	AWHST-hst-system-{Year and date when file was created}.log

*1 If default setting is not changed, the path is “C:\FUJIFILM\ApeosWare MS”.

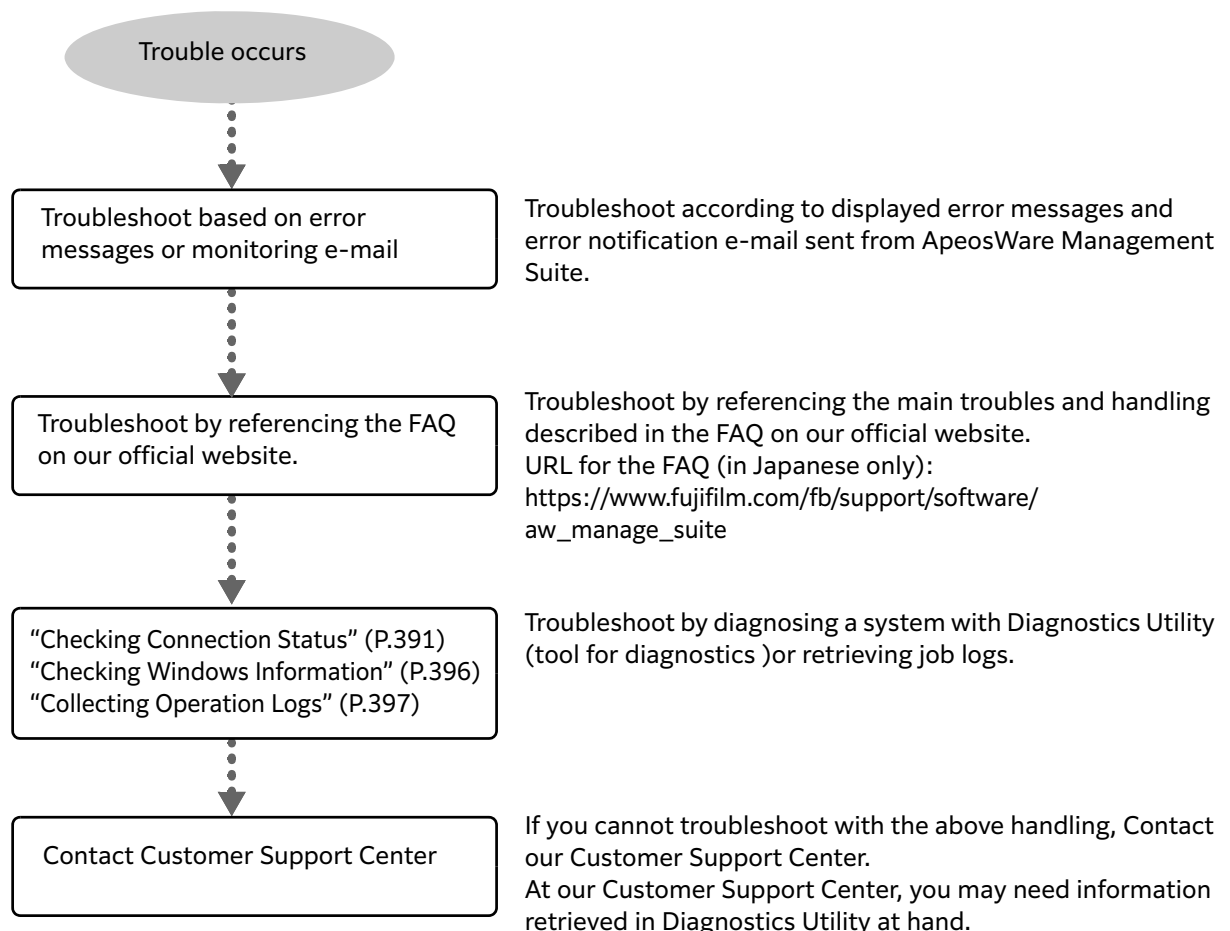
Notes

- If [Authentication/Accounting Mode] is set to other than [No Authentication Required] for the registered device group, execute the "HostnameSetup.exe" command first, and then perform the following steps to change the host name of the ApeosWare Management Suite server, SSL settings, and port number.
 - (1) From the administrator screen menu, select [Service Settings] > [Device Management] > [Device Groups].
 - (2) Select the desired device group and then display the properties.
 - (3) On the [Device panel settings and registered data management] screen, change the [Server URL] host name, SSL settings, and port number to the host name, SSL settings, and port number after change.
 - (4) If [Authentication/Accounting Mode] is set to either [Remote Authentication] or [Custom Authentication], [Primary Server IP Address/Host Name] on the [Basic Settings] screen will also be changed to the host name, SSL settings, and port number after change.
 - (5) Run the update process to update devices with the new device group information.
- With the Image Log Management feature used and the host name of the incoming server changed, if the host name of the node (Main Server in an all-in-one structure, incoming server of Image Log reception separation configuration and Image Log core reception separation structure) including the incoming server has been changed, perform the following steps.
 - (1) From the administrator screen menu, select [Service Settings] > [Device Management] > [Device Groups].
 - (2) Select the desired device group and then display the properties.
 - (3) On the [Communication Settings] screen, change the [Image Log Transfer Destination] host name to the new host name.
 - (4) Run the update process to update devices with the new device group information.
- If information on the Image Log core server has been changed, perform the following steps.
 - (1) Open IIS (Internet Information Services) on the Main Server and restart the ApeosWare Management Suite site.
 - (2) If there is Image Log receiving server, restart the core service of the Image Log receiving server.
- If the Google Drive linkage function or e-mail modern authentication is used, and the main server host name is changed, change the redirect URI previously set for the OAuth provider to the host name after the change.
 For specific procedures for setting the redirect URI, refer to the following.
 - Google Drive linkage: [Google Drive Settings]
 - E-mail modern authentication: [Network Settings]

Troubleshooting

Troubleshoot according to the following flow if a trouble occurs during the operation of ApeosWare Management Suite.

Flow of troubleshooting



Note

The operation log, which is a file to record events that happen in the ApeosWare Management Suite software, is also referred to as the system log. Errors that occur in the software are recorded in operation logs. Because of that, the content of job logs may serve troubleshooting well.

Using Diagnostics Utility

With Diagnostics Utility, you can do the following:

- Check connection status between servers and devices
- Collect operation logs, Windows information, and ApeosWare Management Suite settings information
- Obtain certificate information

You can use Diagnostics Utility to diagnose the system and solve the troubles.

You may need information retrieved in Diagnostics Utility when contacting our Customer Support Center at the time of trouble.

Starting Diagnostics Utility

Diagnostics Utility is operated on a server and in a client.

Start Diagnostics Utility according to the following procedure.

When you start from the DVD-ROM

1. Insert the DVD-ROM into the DVD drive.
2. Select one when the window to select a language appears, and then click [OK].
3. Perform the following steps.
 - (1) Click the [Tool List] tab.
 - (2) Double-click [Diagnostics Utility].

When you start by copying from the DVD-ROM

1. Insert the DVD-ROM into the DVD drive.
2. Open the folder "cm\tools" from the DVD-ROM in Windows Explorer and copy the "dgt" folder to an arbitrary place. Open the folder "dgt" copied and double-click the file "ADTUI.exe".

When you start after installation



Note

Diagnostics Utility is not installed on the report server. To execute Diagnostics Utility on the report server, start it with the DVD-ROM or copy it from the DVD-ROM to start.



Refer

"Setup Guide"

1. Select [FUJIFILM ApeosWare Management Suite] > [Diagnostics Utility] on Startup menu in Windows program.

Checking Connection Status

This section describes how to check the status of a connection with a server or a device using Diagnostics Utility.

1. Start Diagnostics Utility.



Refer

"Using Diagnostics Utility" (P.390)

2. Perform the following steps.
 - (1) Select [Device].
 - (2) Input in [IP Address or Host Name] the IPv4 address, IPv6 address or FQDN of the device whose connection status is to be checked.
 - (3) Click [Add].

Servers are added to [Devices/Servers List:] on the [Check Connection Status] tab. Repeat Steps

(2) and (3) to add all the additional devices if necessary. Up to 10 items including devices and servers can be added.

3. Perform the following steps.

- (1) Select [Server].
- (2) Input in [IP Address or Host Name] the IPv4 address, IPv6 address or FQDN of the server whose connection status is to be checked.
- (3) Click [Add].
Servers are added to [Devices/Servers List:] on the [Check Connection Status] tab. Repeat Steps (2) and (3) to add all the additional servers if necessary. Up to 10 items including devices and servers can be added.

4. When you have specified a SNMP community name or user name different from the factory default, select a device in [Devices/Servers List] and click [Communication Settings].

■ Using SNMP v1/v2 to check connection status

- (1) Select [SNMP v1/v2].
- (2) When you have specified a custom community name for the device, enter the community name in [Community Name (Default value is used if left blank):].
- (3) Click [OK].

■ Using SNMP v3 to check connection status

- (1) Select [SNMP v3].
- (2) When you have specified a custom user name for the device, enter the user name in [User Name].
- (3) When you have specified a custom authentication password for the device, enter the password in [Authentication Password (Default value is used if left blank)].
- (4) When you have specified a custom encryption password for the device, enter the password in [Encryption Password (Default value is used if left blank)].
- (5) Click [OK].

5. Click [Start] from the [Check Connection Status] tab.

Connection status check starts. When the check completes, the result is displayed in [Connection Status Details:].

[Connection Status Details:] displays the following items:

Items	Attribute	Descriptions
Local		
OS information		
OS information retrieval	Only when the retrieval of OS information was not possible, "Could not retrieve OS information" is displayed.	When Operating System information retrieval has failed, all the other items in [OS information] are not displayed.
OS name	The OS used for executing Diagnostics Utility is displayed.	-
Operating System Version & Service Pack Version	OS version and service pack used for executing Diagnostics Utility are displayed.	-
User name	The name of the user who has executed Diagnostics Utility is displayed.	-
User Permission	The permission of the user who has executed Diagnostics Utility is displayed.	-
Resources		When multiple hard disks or memory cards are used, all the hard disks and memory cards are listed.
Remaining capacity of each HDD	Remaining capacity in each hard drive on the computer used for executing Diagnostics Utility is displayed.	-
Memory	The amount of memory on the computer used for executing Diagnostics Utility is displayed.	-

Items		Attribute	Descriptions
Local (Continued)			
Network information			
	Network information retrieval	Only when the retrieval of information was not possible, "Could not retrieve network information" is displayed.	When network information retrieval has failed, no other items in [Network information] than this one are displayed.
	Computer name	The name of the computer used for executing Diagnostics Utility is displayed.	-
	Domain name	The name of the domain with which the computer used for executing Diagnostics Utility is affiliated is displayed.	Either the domain name or the workgroup name is displayed.
	Workgroup name	The name of the workgroup with which the computer used for executing Diagnostics Utility is affiliated is displayed.	
	Network adapter card name		The items from [IP address retrieval method] through [Default gateway] is displayed repeatedly for all the network cards.
	IP address retrieval method	One of the following options is displayed: DHCP/Manual	-
	IP Address	One of the following options is displayed: DHCP address for the computer used for executing Diagnostics Utility/ "Unable to retrieve the IP address".	If "DHCP address retrieval failed" occurs, in the [Description] column, "Settings for IP address and default gateway may be incorrect" is displayed.
	Subnet Mask	Displays the subnet mask of the computer used for executing Diagnostics Utility.	-
	Default gateway	Displays the default gateway of the computer used for executing Diagnostics Utility.	If the IP address and the default gateway network address do not match, in the [Description] column, "Settings for IP address and default gateway may be incorrect" is displayed. If the default gateway has not been set, in the [Description] column, "Default gateway is not set" is displayed.

Items	Attribute		Descriptions
Local (Continued)			
FireWall			
Windows Firewall	One of the following statuses is displayed: Start/Stop/Starting/Stopping/Pause / Paused/Processing/None/No Authenticated	Whether the Windows Firewall service is running is displayed.	
McAfeeVirusScan	One of the following statuses is displayed: Start/Stop/Starting/Stopping/Pause / Paused/Processing/None/No Authenticated	The operating status of McAfee® VirusScan is displayed.	
Remote			
Device information			
IP address or host name of device with which the connection status is checked		The items from this to [Location] are repeated for all devices whose status is to be checked.	
Connection	One of the following statuses is displayed: On/Off/A system error has occurred	A ping test is performed between two devices and the test result is displayed.	
Device information retrieval	If no information has been retrieved via the SNMP connection with a device, one of the following messages is displayed. Communication was not possible with the device./ SNMP communication was not possible with the device./ A system error has occurred.	When information was retrieved from the device, only [Device information retrieval] is displayed.	
System Settings			
Machine information		If none of [Printer Name], [Model Name], and [Location] was retrieved, "- Attribute does not exist. -" is displayed.	
Printer Name	Displays the "sysName" information that has been retrieved from the MIB in the device.	-	
Model Name	Displays the "sysProductName" information that has been retrieved from the MIB in the device.	With our device or Fuji Xerox's, the product name and the ROM version are displayed.	
Installation Location	Displays the "sysLocation" information that has been retrieved from the MIB in the device.	-	
Server information			
IP address or host name of server with which the connection status is checked		The items from this to [Connection] are repeated for all servers whose status is to be checked.	
Connection	One of the following statuses is displayed: On/Off/A system error has occurred	A ping test is performed between two servers and the test result is displayed.	

6. The result displayed in [Connection Status Details:] can be saved in CSV format. To save the result, click [Save...] and specify a folder and a file name in the [Save File] dialog box. The CSV file of [Connection Status Details:] has the following columns.

Column	Items	Descriptions
1	Check item name	Items to be checked such as "Operating System information" and "network information".
2	Check item value	Connection status values including "On" and "Off".
3	Descriptions	Detailed check result. If the setting may be incorrect, one of the following marks is added at the end of a line. ×: Strong possibility of incorrect setting △: Settings may be incorrect

Checking Windows Information

Use Diagnostics Utility to collect the following Windows information. The collected information is saved in a ZIP file.

- Operating System information such as name, version and computer resource
- Network settings such as computer name and TCP/IP options
- Event logs
- Internet Information Services log and settings information
- Active processes
- Installed applications
- Certificate information

1. Start Diagnostics Utility.



Refer

"Starting Diagnostics Utility" (P.391)

2. Select the [Retrieve Information] tab.

3. Perform the following steps.

- (1) To specify the log period, select a checkbox for [Specify Period For Log Retrieval] and select the [Begin Date:] and [End Date:].
- (2) Click [Settings...] of Job Log Analyzer.

4. Perform the following steps.

- (1) Modify the options in the [Log Settings] dialog box as necessary.
To protect the confidential information in the log that is saved in the ZIP file, select the [Set Password] checkbox and enter a password in [Password:]. The ZIP file is encrypted with the entered string.



Note

Enabling [Mask the log private information] does not mask the Windows information.

- (2) To save the settings you have modified, click [OK]. To not save the settings, click [Cancel].

5. Confirm that [Windows Information] is selected and then click [Retrieve].

**Note**

When server software and tools of ApeosWare Management Suite are installed on the PC, the software name is displayed in [List of Information to Retrieve]. When you select the checkbox for an application or a tool, the operation logs are retrieved from the selected application or tool.

6. In the [Save File] dialog box, select the folder in which to save the ZIP file of the Windows information.

7. Click [Save...].

Windows information retrieval starts.

When Windows information retrieval completes, the result is displayed in [Retrieval Result].

8. You can save the result displayed in [Retrieval Result] in CSV format. To save the result, click [Save...] and specify a folder and a file name in the [Save File] dialog box.

The CSV file of [Retrieval Result] has the following columns.

Column	Items	Descriptions
1	Retrieval item name	Name of the item to be retrieved such as "Windows information" and "event log".
2	Retrieval result	When information retrieval failed, an "X" is displayed. When succeeded, nothing is displayed.
3	Descriptions	The reason for retrieval failure is displayed.

Collecting Operation Logs

You can collect the operation logs in bulk from ApeosWare Management Suite using Diagnostics Utility. The collected operation logs are saved in ZIP files.

**Note**

The audit log and debug log are included in the log acquired by Diagnostics Utility.

The audit log is an event log related to business audit. The debug log is a log that we use for software debugging. Whether or not to acquire the debug log can be set using the "Log settings" tab of the Diagnostics Utility.

1. Start Diagnostics Utility.

**Refer**

"Starting Diagnostics Utility" (P.391)

2. Select the [Retrieve Information] tab.

3. Perform the following steps.

(1) To specify the log period, select a checkbox for [Specify Period For Log Retrieval] and select the [Begin Date:] and [End Date:].

(2) Click [Settings...] of Job Log Analyzer.

4. Perform the following steps.

(1) Modify the options in the [Log Settings] dialog box as necessary. To protect the private information in the log saved in the ZIP file, the following options are available:

- Select [Set Password] to protect the ZIP file with the string entered in [Password:].
- Select [Mask Private Log Information] to display confidential information such as the user name or password as "<<<hash value>>>".

(2) To save the settings you have modified, click [OK]. To not save the settings, click [Cancel].

5. Select the checkbox for the target application in [List of Information to Retrieve:].
The name of the installed software of ApeosWare Management Suite is displayed in [List of Information to Retrieve:].
6. Click [Retrieve].
7. In the [Save File] dialog box, select the folder in which to save the ZIP file of the operation logs.
8. Click [Save...].
The operation log retrieval starts.
When the operation log collection completes, the result is displayed in [Retrieval Result].
9. You can save the result displayed in [Retrieval Result] in CSV format. To save the result, click [Save...] and specify a folder and a file name in the [Save File] dialog box.

Outputting Detailed Logs, Changing the Log Size Limit

Make a change with Diagnostics Utility so that you can output detailed logs. Then, make a change to the upper limit of the size of logs to retrieve. Implement the settings for outputting detailed logs only when you are instructed by our representative.



Note

“Detailed log” is also referred to as “Debugging log”.

1. Start Diagnostics Utility.



Refer

“Starting Diagnostics Utility” (P.391)

2. Select the [Log Settings] tab.
3. Perform the following steps.
 - (1) Select the checkboxes of any detailed logs you want to retain from the [Log Information:].
 - (2) Select the [Enable Log Size Limit] checkbox and estimate the maximum log size.
We recommend 40 GB or more as the maximum log size.
 - (3) Click [Apply].

Showing Logs

The log batch display tool can be used to show the content of the log as a list.

1. Insert the DVD-ROM into the DVD drive.
2. Open the folder “cm\tools\dgt” from the DVD-ROM in Windows Explorer.
3. Double-click “ADTLogViewer”.
The log batch display screen is displayed.
The list of logs narrows down the log display content to [All], [Image Log Management] or [Meter].

Starting or Stopping ApeosWare Management Suite Services

This section describes how to manually start and stop the ApeosWare Management Suite services.

Starting ApeosWare Management Suite Services

ApeosWare Management Suite services are launched automatically when the ApeosWare Management Suite server is started.

When you wish to manually start the ApeosWare Management Suite services after they stop for some reasons, you can start the services from the Windows management tool.

Start the services according to the following sequence.

SQL Server (FXAW)

ApeosWare Management Suite Proxy Service

ApeosWare Management Suite Core Service

ApeosWare Management Suite Multi Task Service

ApeosWare Management Suite mDNS Service

ApeosWare Management Suite Printer Port Service

ApeosWare Management Suite Email Print Service

ApeosWare Management Suite Image Log Management Core Service

World Wide Web Publishing Service

ApeosWare Management Suite Update Service

ApeosWare Management Suite Flow Management Service

ApeosWare Management Suite Monitoring Service

Stopping ApeosWare Management Suite Services

ApeosWare Management Suite services are stopped automatically when the ApeosWare Management Suite server is shut down.

When you wish to manually stop the ApeosWare Management Suite services for performing an installation or a restoration, stop the services according to the following sequence.

ApeosWare Management Suite Monitoring Service

ApeosWare Management Suite Flow Management Service

ApeosWare Management Suite Update Service

World Wide Web Publishing Service

ApeosWare Management Suite Image Log Management Core Service

ApeosWare Management Suite Email Print Service

ApeosWare Management Suite Printer Port Service

ApeosWare Management Suite mDNS Service

ApeosWare Management Suite Multi Task Service

ApeosWare Management Suite Core Service

ApeosWare Management Suite Proxy Service

Print Spooler

SQL Server (FXAW)



Note

- Make sure to stop ApeosWare Management Suite Monitoring Service first before stopping the Update Service.
- You cannot stop ApeosWare Management Suite Flow Management Service from the Windows monitoring tool. To stop the service, execute the batch command. For more details on the batch command, refer to “Features Guide Flow Management Option”.

Appendix

Formats of Job Log Files (SOAP Collection)

This section describes the formats of job log files collected by using SOAP (Simple Object Access Protocol).

Basic Structure of Job Log Files

This section describes the rows comprising job log files and the file formats of job log files.

Rows comprising job log files

Job log files are comprised of the following rows.

- **Title Row**
Item names of job logs such as “Printer Name”, “Branch Number”, and “MIB Type” are entered.
- **Document Data Row**
Information such as the document size, original impressions, document type, and output color of original impressions is recorded in these rows. The document data row is not recorded for jobs that do not include original sheets such as print jobs.
- **Impression Data Row**
Information such as the number of impressions, output color, and size of impressions is recorded. The paper data row is not recorded for jobs for which the number of print sheets is 0 such as file transfer of scanned documents.
- **Paper Data Row**
Information such as the number of sheets, paper size, and paper type to be printed is recorded. The paper data row is not recorded for jobs that do not include print sheets such as file transfer of scanned documents.
- **Fax Processing Data Row**
Information such as the recipient telephone number, Fax image size, and Fax images sent is recorded. This is recorded only for fax jobs.
- **Basic Data Row**
Only basic information of jobs such as the printer name and service type is recorded. This row is recorded only when information does not exist in the Fax data row, paper data row, impression data row, or document data row, such as for jobs for which print data is stored on a device or print jobs that are aborted.

Example of copy job

This section describes job log files when copying is executed.

Printer Name	Branch No.	...	Job ID	...	Printing Size	...	Paper size	...	Document Size	...
Apeos1	1 of 3	Abbreviated	123	Abbreviated		Abbreviated		Abbreviated	A4	The rest is omitted.
Apeos1	2 of 3		123		A4					
Apeos1	3 of 3		123				A4			

This example is a job for copying an A4 size document on A4 size paper. This job is comprised from a document data row, impression data row, and paper data row.

- The name of the device that executed the job is recorded in "Printer Name".
- Since the job is comprised of 3 rows, values are recorded in "Branch No." of each row such "1 of 3" (first of three rows), "2 of 3" (second of three rows), and "3 of 3" (third of three rows).



Note

Copy jobs are not always limited to 3 rows. 4 or more rows may be recorded depending on the selection of output color and size of the paper.

- Since it is 1 copy job comprised of 3 rows, the same value is recorded in "Job ID".
- Since information concerning the document is recorded in the document data row, a value is recorded in "Original Size" and values are not recorded in the printing item and the paper items.
- Since information concerning the impressions to be printed is recorded in the impression data row, a value is recorded in "Printing Size" and values are not recorded in the original items and the paper items.
- Since information concerning the paper on which to print is recorded in the paper data row, a value is recorded in "Paper Size" and values are not recorded in the original items and the printing items.

Example of print job

This section describes job log files when printing is executed from a computer.

Printer Name	Branch No.	...	Job ID	...	Printing Size	...	Paper size	...	Document Size	...
Apeos1	1 of 2	Abbreviated	234	Abbreviated	A4	Abbreviated		Abbreviated		The rest is omitted.
Apeos1	2 of 2		234				A4			

This example is a job for printing on A4 size paper from a computer. This job is comprised from an impression data row and paper data row. Since a document is not scanned, a document data row is not included.

- The name of the device that executed the job is recorded in "Printer Name".
- Since the job is comprised of 2 rows, values are recorded in "Branch No." of each row such "1 of 2" (first of two rows) and "2 of 2" (second of two rows).
- Since it is 1 print job comprised of 2 rows, the same value is recorded in "Job ID". Since information concerning the impressions to be printed is recorded in the impression data row, a value is recorded in "Printing Size" and a value is not recorded in the paper items.
- Since information concerning the paper on which to print is recorded in the paper data row, a value is recorded in "Paper Size" and a value is not recorded in the printing items.

Example of fax job

This section describes job log files when a document is scanned and sent by a fax.

Printer Name	Branch No.	...	Job ID	...	Document Size	...	Recipient Fax Number	...	Fax Image Size	...
Apeos1	1 of 2	Abbreviated	345	Abbreviated	A4	Abbreviated		Abbreviated		The rest is omitted.
Apeos1	2 of 2		345				XXXXXXXX		A4	

This example is a job for faxing A4 size paper. This job is comprised from an document data row and fax data row. Since a document is not printed, an impression data row and paper data row are not included.

- The name of the device that executed the job is recorded in "Printer Name".
- Since the job is comprised of 2 rows, values are recorded in "Branch No." of each row such "1 of 2" (first of two rows) and "2 of 2" (second of two rows).
- Since it is 1 print job comprised of 2 rows, the same value is recorded in "Job ID".
- Since information concerning the document is recorded in the document data row, a value is recorded in "Original Size" and values are not recorded in the fax items.
- Since information concerning the fax processing is recorded in the fax data row, a value is recorded in "Fax Recipient Phone Number" and "Fax Images Size", and a value is not recorded in the original items.



Fax jobs comprised on one row with a branch number of "1 of 1" also exist.

Format of job log files

A job log file is a text file of CSV format.

Items Recorded in Job Log Files (by Service Type)

The following table categorizes items recorded in job log files by service type.

○: Recorded

×: Not recorded

△: Dependent on model and service details

Items	Service types						
	Printing	Copying	Scan	Faxing	System Sheet	File Transfer	E-mail Transfer
Printer Name	○	○	○	○	○	○	○
Branch No.	○	○	○	○	○	○	○
MIB Type	○	○	○	○	○	○	○
Product Name	○	○	○	○	○	○	○
Job ID	○	○	○	○	○	○	○
Service types ^{*8}	○	○	○	○	○	○	○
Host name	△	×	×	△	×	△	×
User name	△ ^{*6}	△	△	△	○	△	△
Document name ^{*9}	△ ^{*7}	×	×	△	×	△	×
Job Owner Name	△	△	△	△	×	△	×
Job Client ID	△	×	×	△	×	△	×
Print Status	○	○	○	○	○	○	○
Ports	△	×	△	△	×	△	×
Data Type	△	×	△	△	×	△	×
IP Address ^{*5}	△	×	×	△	×	△	×
Output Tray	△	○	×	×	○	×	×
Pages per Side	○	○	○	○	○	○	○
Select Paper Tray	△	○	×	×	○	×	×

Items	Service types						
	Printing	Copying	Scan	Faxing	System Sheet	File Transfer	E-mail Transfer
Logging Date ^{*10}	○	○	○	○	○	○	○
Log Collection Time ^{*10}	○	○	○	○	○	○	○
Printer Date ^{*11}	○	○	○	○	○	○	○
Printer Time ^{*11}	○	○	○	○	○	○	○
Print Start Date	○	○	○	○	○	○	○
Print Start Time	○	○	○	○	○	○	○
Print End Date	○	○	○	○	○	○	○
Print End Time	○	○	○	○	○	○	○
Total Printed Impressions ^{*12}	○	○	○	○	○	○	○
Total Printed Impressions Since Power On ^{*12}	○	○	○	○	○	○	○
Error	○	○	○	○	○	○	○
Printing Output Color	△	○	×	×	○	×	×
Printing Size	△	○	×	×	○	×	×
Impressions	△	○	×	×	○	×	×
Paper type	△	○	×	×	○	×	×
Paper size	△	○	×	×	○	×	×
Number of sheets	△	○	×	×	○	×	×
Job Template Name	×	×	△	×	×	△	△
Number of Copies ^{*1}	○	○	×	×	○	×	×
Staple Count ^{*1}	○	○	×	×	○	×	×
Original Color	×	○	○	△	×	△	○
Original Impressions ^{*1}	×	○	○	△	×	△	○
Original Type	×	○	△	△	×	×	△
Document Size	×	○	△	△	×	×	△
Recipient IP Address	×	×	△	×	×	△	○
Folder Number	△	×	△	△	△	△	△
Recipient Fax Number	△	×	×	△	×	△	×
Fax Remote Terminal Name	△	×	×	△	×	△	×
F code	△	×	×	△	×	△	×
Fax Line ^{*1}	△	×	×	△	×	△	×
Fax Start Date ^{*2}	△	×	×	△	×	△	×
Fax Start Time ^{*3}	△	×	×	△	×	△	×
Fax Complete Date ^{*2}	△	×	×	△	×	△	×
Fax Complete Time ^{*3}	△	×	×	△	×	△	×
Fax Duration ^{*1}	△	×	×	△	×	△	×

Items	Service types						
	Printing	Copying	Scan	Faxing	System Sheet	File Transfer	E-mail Transfer
Remote ID	△	×	×	△	×	△	×
Fax Images Sent ^{*1}	×	×	×	△	×	×	×
Fax Image Size	△	×	×	△	×	△	×
FAX Speed Dial Number	×	×	×	△	×	×	×
Service Details	○	○	○	○	○	○	○
Related Job ID ^{*4}	△	×	×	△	△	△	×
Account ID ^{*14}	△	△	△	△	△	△	△
Card No.	△	△	△	△	△	△	△
Meter 1 ^{*12}	○	○	○	○	○	○	○
Meter 2 ^{*12}	○	○	○	○	○	○	○
Meter 3 ^{*12}	○	○	○	○	○	○	○
Billing Meter Number ^{*1}	○	○	×	×	○	×	×
Recipient Information	×	×	×	×	×	○	○
Staple Type	○	○	×	×	○	×	×
Fold Type	○	○	×	×	○	×	×
Fold Count ^{*1}	○	○	×	×	○	×	×
Punch Type	○	○	×	×	○	×	×
Punch Count ^{*1}	○	○	×	×	○	×	×
Bind Count ^{*1}	○	○	×	×	○	×	×
UUID	○	○	○	○	○	○	○
Document number	△	×	△	△	△	△	△
Cause of Error	○	○	○	○	○	○	○
Job Error Code	○	○	○	○	○	○	○
Fax Sender ID	△	×	×	△	×	△	×
Fax Dial-In Number	△	×	×	△	×	△	×
Fax Recipient Information	△	×	×	△	×	△	×
Fax Call Type	△	×	×	△	×	△	×
Fax Transmission Speed	△	×	×	△	△	△	×
Fax Reconnection Flag	△	×	×	△	×	△	×
Name in Address Book	×	×	×	△	×	×	×
Send Fax Status	×	×	×	△	×	×	×
Fax Communication Result	×	×	×	△	×	×	×
Stored Fax Pages ^{*1}	△	×	×	△	△	△	×
Stamp Type ^{*13}	△	△	×	×	△	×	×
Roll Sheet Size ^{*13}	△	△	×	×	△	×	×
Roll Length ^{*13}	△	△	×	×	△	×	×

- *1 For jobs for which information cannot be retrieved, normally "0" is displayed.
- *2 For jobs for which information cannot be retrieved, normally "0000/00/00" is displayed.
- *3 For jobs for which information cannot be retrieved, normally "00:00:00" is displayed.
- *4 When an operation such as fax transmission or fax reception is executed, multiple job logs may correspond. In that case, the main job ID is displayed as the Related job ID in the sub job log.
- *5 Indicates whether the IP address of the client computer can be retrieved. Normally the IP address of the device can be retrieved.
- *6 Since the user name is not saved in job logs at the device, they cannot be retrieved via Port 9100.
- *7 Since the document name is not saved in job logs at the device, they cannot be retrieved via Port 9100.
- *8 "File Transfer" is recorded for the service type at the time of storing print jobs in a device with stored print. Then, "Secure Print Spool", "One Copy Sample Print", "Delayed Print Spool" or "Private Print Spool" are recorded for the details of service. "Print" is recorded for the service type at the time of printing print jobs stored in a device from the control panel. Then, "Secure Print", "Sample Print", "Delayed Print" or "Private Charge Print" are recorded for the details of service.
- *9 For Secure Print, Delayed Print, and Private Charge Print, the document name specified with [Stored Document Name] of the printer driver is recorded.
- *10 The log retrieval time is the time indicated by the clock of the ApeosWare Management Suite server.
- *11 The time of the internal clock of the printer is the time indicated by the clock of the device when logs were retrieved.
- *12 The total print page number and the meter value are the values when logs were retrieved.
- *13 Only job log MIB type [FX MIB (SOAP-WF)] devices can retrieve this item.
- *14 Converted to an account name if com.fujifilm.fb.apesosware.joblog.export.accountmapping=true has been specified in joblogexport.properties.

Details of Job Logs of Devices Corresponding to SOAP Retrieval

When the authentication/accounting features are being used, the retrieved log information such as User name and User ID may differ from the intended result depending on the authentication status of jobs received by the device, or the setting status of the authentication/accounting features at the device.

Examples are shown below.

Example 1:

The login user name of the client computer, not the user name corresponding to User ID registered on the device, is recorded in User name.

Example 2:

"UnknownUser", not User ID set with the printer driver, is recorded in Job owner name.

Example 3:

A stored document name is recorded in Document name.

Log information differs when "Print Accounting/Management" is set to "Off" and when it is set to "On" for the authentication/accounting features at the device.

This section describes each case.

When "Print Accounting/Management" is set to "Off"

This section describes the case in which "Print Accounting/Management" is set to "Off" for the authentication/accounting features at the device.

When "Print Accounting/Management" is set to "Off", job log information becomes as follows regardless of the print job type or whether the authentication/accounting features are being used.

Job log items	Values recorded in job logs
Service types	Printing
Service Details	Printing
Print Status	Complete

Job log items	Values recorded in job logs	
Job Owner Name	When [Always Use the Same Authentication Information] is set on the [Default Settings] tab of the printer driver User ID set with the printer driver	When [Display Authentication Entry Screen per Job] is set on the [Default Settings] tab of the printer driver, and only the stored ID is specified UnknownUser
User name	Login user name of client computer	
AccountID	Account ID set with the printer driver	
Card No.	Blank	

When “Print Accounting/Management” is set to “On”

This section describes the case in which “Print Accounting/Management” is set to “On” for the authentication/accounting features at the device.

When “Print Accounting/Management” is set to “On”, job log information differs depending on the print job type. Job types are roughly categorized into the following three types.

Normal print

Normal print jobs from the printer driver. Also, when “Control by Job Login Results” is set for “Receive Control” with the “Charge Print” setting of the device.

Stored print

Print jobs once stored on the device. The four following types of print jobs are included.

- Secure Print
- Sample Set
- Delayed Print
- Private Print

Charge print

All print jobs once stored on the device.

The setting of “Charge Print” of the device is categorized into the following two types.

- When “Control by Job Login Results” is set for “Receive Control”, and “Save All” is set for “Job Login Failure”

With this setting, failed print jobs that failed authentication are also included.

- When “Save All” is set for “Receive Control”

With this setting, all print jobs are targeted.

This section categorizes and describes each job type.

Normal print

With normal printing, values recorded in job logs differ depending on the following causes.

- Authentication status on the device of the User ID set with the printer driver
- Method of setting the authentication information in the printer driver

This section describes each case.

When user ID is not registered on device

Job log items	Values recorded in job logs
Service types	Printing
Service Details	Printing
Print Status	Canceled
Job Owner Name	User ID set with the printer driver
User name	Login user name of client computer
AccountID	Account ID set with the printer driver
Card No.	Blank

When user ID is registered on device

Job log items	Values recorded in job logs			
	When password is incorrect	When password is correct		
		For local authentication	When account ID is correct with network authentication	When account ID is incorrect with network authentication
Service types	Printing			
Service Details	Printing			
Print Status	Canceled	Complete		Canceled
Job Owner Name	User ID set with the printer driver			
User name	Login user name of client computer	User name corresponding to user ID registered on device		Login user name of client computer
AccountID	Account ID set with the printer driver		Account ID corresponding to user ID registered on device	Account ID set with the printer driver
Card No.	Blank	Card ID corresponding to user ID registered on device (only when card authentication also is used)		Blank

When “Display Authentication Entry Screen per Job” is set on the default settings tab of the printer driver, and only the stored ID is specified

Job log items	Values recorded in job logs
Service types	Printing
Service Details	Printing
Print Status	Canceled
Job Owner Name	UnknownUser
User name	Login user name of client computer
AccountID	Account ID set with the printer driver
Card No.	Blank

Stored print

For stored printing, the values recorded in job logs differ when the print jobs are stored on the device and when the stored print jobs are printed from the control panel of the device.

Also, the document name specified with “Stored Document Name” of the printer driver is recorded as the document name of the job log for Secure Print, Delayed Print, and Private Charge Print.

This section describes each case.

When print jobs are stored on device

Job log items	Values recorded in job logs	
	When authentication information is correct	When authentication information is incorrect
Service types	File Transfer	
Service Details	Secure Print Spool, One Copy Sample Print, Delayed Print Spool, Private Print Spool	
Print Status	Complete	Canceled
Job Owner Name	User ID set with the printer driver When only the stored ID is specified with the settings of the printer driver, “UnknownUser”	
User name	User name corresponding to user ID registered on device	Login user name of client computer
AccountID	Account ID corresponding to user ID registered on device	Account ID set with the printer driver
Card No.	Card ID corresponding to user ID registered on device (only when card authentication also is used)	Blank

When stored print jobs are printed from the control panel

Job log items	Values recorded in job logs
Service types	Printing
Service Details	Secure Print, Sample Print, Delayed Print, Private Print
Print Status	Complete When the User ID at the time of print job storage is deleted from the device, “Canceled”
Job Owner Name	User ID set with the printer driver
User name	User name corresponding to user ID registered on device
AccountID	Account ID corresponding to user ID registered on device
Card No.	Card ID corresponding to user ID registered on device (only when card authentication also is used)

Charge print

For charge printing, the values recorded in job logs differ when the print jobs are stored on the device and when the stored print jobs are printed from the control panel of the device.

When print jobs are stored on device

Job log items	Values recorded in job logs
Service types	File Transfer
Service Details	Charge Print
Print Status	Complete
Job Owner Name	User ID set with the printer driver When only the stored ID is specified with the settings of the printer driver, "UnknownUser"
User name	Login user name of client computer
AccountID	Account ID set with the printer driver
Card No.	Blank

When stored print jobs are printed from the control panel

Job log items	Values recorded in job logs
Service types	Printing
Service Details	Charge Print
Print Status	Complete When printing is unavailable due to the setting of "Output Color" set on the device, "Canceled"
Job Owner Name	User ID set with the printer driver When only the stored ID is specified with the settings of the printer driver, "UnknownUser"
User name	Login user name of client computer
AccountID	Account ID set with the printer driver
Card No.	Blank

Format of Each Item

This table indicates the data formats recorded in the items of job logs.

Job log item	Descriptions	Format
Printer Name	Device name registered in the database of ApeosWare Management Suite	Text

Job log item	Descriptions	Format
Branch No.	Number indicating the row number within 1 job log Example: "1 of 1" for a job log with only 1 row or "1 of 2" and "2 of 2" for a job log comprised of 2 rows  Refer "Basic Structure of Job Log Files" (P.401)	Total branch numbers (integers) of branch numbers (integers)
MIB Type	Type of Management Information Base	• If the collection type is [SOAP HDD available] or [No SOAP HDD] FX MIB(SOAP) • If the collection type is [SOAP HDD available (WF)] FX MIB(SOAP-WF)
Product Name	Model name of device	Text
Job ID	ID attached to job	Integer
Service types	Service type that executed job	Any one of the following programs • Copying • Scan • Faxing • Printing • System Sheet • File Transfer • E-mail Transfer • Job Flow
Host name	Host name of computer that instructed jobs such as printing or direct faxing	Text
User name	User name corresponding to user ID	Text
Document Name	Name of printed or direct faxed document	Text
Job Owner Name	Authenticated user ID or job owner name set in the printer driver or fax driver	Text
Job Client ID	ID sent from the printer driver or fax driver	Text
Print Status	Status of printing	Any one of the following programs • Complete • Complete (With warning) • Canceled • Canceled (System) • Unknown
Ports ^{*1}	Protocol used in sending jobs from a PC such as printing or direct faxing	Text
Data Type ^{*1}	Sent or received data type	Text
IP Address	IP address of device and IP address of client computer	IP address of device\IP address of client computer. When an IP address of client computer does not exist, only the IP address of the device is included, without the delimit symbol (\)
Output Tray ^{*1}	Output destination of paper	Text

Job log item	Descriptions	Format
Pages per Side ^{*1}	Setting of pages per side	Text
Select Paper Tray ^{*1}	Name of paper tray	Text
Logging Date	Date on which job logs were collected Date of ApeosWare Management Suite server clock	yyyy/mm/dd
Log Collection Time	Time at which job logs were collected Time of ApeosWare Management Suite server clock	hh:mm:ss
Date of printer internal clock	Date on which job logs were recorded Date of clock of printer	yyyy/mm/dd
Time of printer internal clock	Time at which job logs were recorded Time of clock of printer	hh:mm:ss
Print Start Date	Date on which printing started	yyyy/mm/dd
Print Start Time	Time at which printing started	hh:mm:ss
Print End Date	Date on which printing ended	yyyy/mm/dd
Print End Time	Time at which printing ended	hh:mm:ss
Total Printed Impressions	Total pages printed from device installation until present	Integer
Total Printed Impressions Since Power On	Total pages printed from device power-on until present	Integer
Error	Information concerning errors is not recorded in this item	0
Printing Output Color ^{*1}	Output color of the printed impression	Text
Printing Size ^{*1}	Size of the printed impression	Text
Impressions	Number of impressions processed	Integer
Paper type ^{*1}	Type of paper	Text
Paper size ^{*1}	Size of paper	Text
Number of sheets	Sheets of paper	Integer
Job Template Name	Name of job template used	Text
Number of Copies	Number of prints	Integer  Note For devices whose MIB type is [FX MIB (SOAP-WF)], "1" is recorded after printing by specify sort for each set.
Staple Count	Number of staples	Integer
Original Color ^{*1}	Color of document	Text
Original Impressions	Impressions of document	Integer
Original Type ^{*1}	Original Type	Text
Original Size ^{*1}	Size of document	Text
Recipient IP Address	Recipient IP address for file transfer or e-mail transmission	IP address of recipient

Job log item	Descriptions	Format
Folder Number	Folder number of own terminal or remote terminal	Integer
Recipient Fax Number	Fax number of recipient	Text
Fax Remote Terminal Name	Name registered in remote terminal	Text
F code	F code used in communication	Text
Fax Line	Categorized as extension, external line, or IP fax (SIP) Existence of IP fax (SIP) feature differs depending on your model	Any one of the following programs • Number (Extension) • Number (External Line) • Number (IP Fax (SIP)) • Number • Unknown
Fax Start Date	Date on which faxing started	yyyy/mm/dd
Fax Start Time	Time at which faxing started	hh:mm:ss
Fax Complete Date	Date on which faxing ended	yyyy/mm/dd
Fax Complete Time	Time at which faxing ended	hh:mm:ss
Fax Duration	Time elapsed from start of faxing until faxing ends	Integer
Remote ID	ID for identifying own terminal	Text
Fax Images Sent	Images sent or received	Integer
Fax Image Size ^{*1}	Size of sent or received fax image	Text
FAX Speed Dial Number	Speed dial number of remote terminal	Integer
Service Details ^{*1}	Type of service for which job is executed	Text
Related Job ID	ID of parent job recorded in child job when a parent job and child job are generated	Integer
Account ID	Account ID entered with the control panel, printer driver, or fax driver	Text
Card No.	For the models of Japanese specification, the card No. is any of: Card number of copy card Card ID of IC card read by IC Card Gate 1.0. It must be maximum 7 digits (0 to 9999999). For the models of Asia Pacific specification, no value is recorded.	Integer when a value is recorded. (Blank) when no value is recorded.
Meter 1	Value recorded in "Meter 1" of the device	Integer
Meter 2	Value recorded in "Meter 2" of the device	Integer
Meter 3	Value recorded in "Meter 3" of the device	Integer
Billing Meter Number	Number of meter targeted for charging	Any one of the following programs • 0 • 1 • 2 • 3 • 101 • 102 • 103 • 104

Job log item	Descriptions	Format
Recipient Information	Recipient address for a file transfer or e-mail transmission	Text
Staple Type ^{*1}	Type of stapling	Text
Fold Type ^{*1}	Type of paper folding	Text
Fold Count	Number of folds executed in job	Integer
Punch Type ^{*1}	Type of hole-punching of paper	Text
Punch Count	Number of hole-punches executed for job	Integer
Bind Count	Number of binds executed for job	Integer
UUID	Printed on paper, this is an ID for identifying job logs	Text
Document number	The number of the document automatically attached within a folder	Text
Cause of Error	Reason job completed with an error	Text
Job Error Code	Code expressing the content of the error that occurred during job execution	Text
Fax Sender ID	Own fax sender ID	Text
Fax Dial-In Number	Dial-in number of recipient	Text
Fax Recipient Information	Information of fax recipient	Any one of the following programs • Unknown • Name in Address Book • Fax Remote Terminal Name • Remote ID • Ports • Recipient Fax Number • The Others • (Blank)
Fax Call Type	Categorized as outgoing call and incoming call	Any one of the following programs • Outgoing Call • Incoming Call • Unknown • The Others • (Blank)
Fax Transmission Speed	Transmission speed of fax	Text
Fax Reconnection Flag	Categorized as whether to reconnect or not reconnect	When reconnecting, it is true When not reconnecting, it is false or (blank)
Name in Address Book	Address name registered in address book	Text
Send Fax Status	Status of sending	Any one of the following programs • Send Wait • Sending • Sending with Retry • Completed • The Others • (Blank)

Job log item	Descriptions	Format
Fax Communication Result	Result of communication	Any one of the following programs • Good • Busy • Busy (Auto Retry) • Auto Retry • Terminated • Resend Required • Error • The Others • (Blank)
Stored Fax Pages	Number of pages stored to be sent	Integer
Stamp Type	Stamp Type	(Blank)
Roll Sheet Size ^{*1}	Width of the Roll Sheet in use	Text
Roll Length	Length of the Roll Sheet in use	Integer

*1 For details on the recorded string, refer to “Details of Items” (P.416).

Details of Items

This section shows the details of items with numerous values among the items recorded in text format in job logs.



Note

(Blank) indicates that nothing is recorded in that item.

Ports

Text		
Parallel	Serial	EtherTalk
lpd	NetWare:PServer	NetWare:RPrinter
Netware	IPP	SMB
Port9100	USB	HTTP
Report/List	PS Initialize	Salutation
SMTP	POP3	BMLinkS
FTP	HDD	G3
G4	WebDAV	OEMHTTP
ThinPrint	Media	The Others

Data Type

Text		
Auto	HP-PCL	HP-GL
HP-PJL	PostScript	PDF
ESC/P	PR201H	TIFF
DIAGNOSTIC	ART	PLW
KS	KSSM	XJCL
JFIF	Bitmap	RAW
BILEVEL	DocuWorks	HP-PCLXL
XPJL	KS5895	EXIF
HCOMP	XPS	PDFA
CALS	CGM	GRF
GCGL	FXMMR	ZJS
Unknown	(Blank)	



Note

XPS is the abbreviation for “XML Paper Specification”.

Output Tray

Text		
Auto	Exit tray	Side tray

Text		
Sorter	Bin X X is the number of the bin	Stacker bin X X is the number of the bin
Finisher	(Blank)	

Pages per Side

Text		
Auto	1 Page	2 Pages
4 Pages	8 Pages	9 Pages
16 Pages	32 Pages	The Others
(Blank)		



Note

If the job log MIB type is "FX MIB (SOAP-WF)", "1 Up" is always recorded.

Select Paper Tray

Text		
Auto	Tray X X is the number of the tray	Tray 2-X Tray 2 is a multi-tray X is the number of the tray
Tray (Bypass)	Separators tray	Roll X X is the Roll number
The Others	(Blank)	

Original Type

Text		
Photo-text mixed	Photo	Text
Map	Graphics	Highlighter
Inkjet	Printed picture	Blueprint
Transmissive	Non-uniform density document	Unknown
(Blank)		

Output Color

Text		
Full Color	Dual Color	Single Color
Black & white	The Others	(Blank)

Size

Text		
Full Color	Dual Color	Single Color
Black & white	The Others	(Blank)
A0	A1	A2
A3	A4	A5
A6	A7	A8
A9	A10	ISO B0
ISO B1	ISO B2	ISO B3
ISO B4	ISO B5	ISO B6
ISO B7	ISO B8	ISO B9
ISO B10	ISO C3	ISO C4
ISO C5	ISO C6	Envelope ISO specified length
B0	B1	B2
B3	B4	B5
B6	B7	B8
B9	B10	11 x 17" (Ledger)
c(17x22")	d(22x34")	e(34x44")
Postcard	8.5 x 11" (Letter)	8.5 x 14" (Legal)
Taiwan 16K	Taiwan 8K	5.5 x 8.5" (Statement)
8.5 x 13" (Folio)	7.25 x 10" (Executive)	8.5 x 10.83" (Quarto)
Japanese Envelope Chou #3	Japanese Envelope Chou #4	SRA3
Monarch Envelope	Mainland China 16K	Mainland China 8K
A4 Cover	Letter Cover	Special A4
Special_A3	Double Postcard	13x18"
13x19"	Spanish	DT Special A3
8.5x13.4"	Japanese Envelope Kaku #2 (240 x 332 mm)	Japanese Envelope Chou #3 (120 x 235 mm)
Envelope C5 (162 x 229 mm)	Envelope C4 (229 x 324 mm)	Others (Special A0)
Others (Special A1)	Others (Special A2)	Others (A)
Others (B)	Others (C)	Others (D)
Others (E)	Others (B_10.5)	Others (C_15)
Others (D_21)	Others (E_30)	Others (OTHER)
The Others	Unknown	(Blank)

Paper type

Text		
Plain paper	OHP film	Envelope
Label paper	Form	Coated paper
Tracing paper	Recycled paper	Rolled paper

Text		
Tab paper	Opaque film	Tack film
Thin paper	High quality paper	Custom Paper 1
Custom Paper 2	Custom Paper 3	Custom Paper 4
Custom Paper 5	Gift wrapping paper	Special glossy paper
Thick paper	Postcard	Special paper
Side 2	Prepunched paper	Index paper
The Others	Unknown	(Blank)

Service Details

Service types	Text
Copying	Copying
	Copy Server - Copy
Scan	SCAN
	Xdom Scan
	Xdom Copy
	Reserve Fax Polling
	Reserve Secure Polling Fax
	Store Scan Document
	Copy Server - Scan
	Web Scan
	Scan BMLinkS
	Auto Gradation Correction

Service types	Text
Faxing	FAX
	Outgoing Direct Fax
	Mailbox To Fax
	Email to Fax
	Fax Broadcast
	Auto Send Fax
	Manual Send Fax
	Fax Immediate Send
	Auto Send Fax - Remote Folder
	Fax Polling Send
	Fax Mailbox Polling Send
	Send Fax Report
	Fax Relay Broadcast
	Fax Relay Broadcast Send
	Fax Remote Maintenance
	Send Internet Fax received by Fax (Auto)
	Fax/Internet Fax Broadcast
	Server Fax Send
Printing	Printing
	Secure Print
	Sample Print
	One Copy Sample Print
	Print E-mail
	Delayed Print
	Media Print
	Media Index Print
	Charge Print
	Digital Camera Print
	Digital Camera Index Print
	Document Print
	Document Index Print
	OEMDOD Print
	FRE Print
	Web Print
	Private Print Transfer
	Print Auto Received Fax
	Print Manual Received Fax
	Immediate Print Received Fax
	Sample Print File for Free Fax Polling
	Sample Print File for Secure Fax Polling

Service types	Text
Printing (Continued)	Print Inbound Polling Fax
	Fax Immediate Polling Print
	Fax Multi-Polling Print
	Fax Immediate Multi Polling Print
	Print Inbound Relay Broadcast Fax
	Print Inbound Internet Fax
	Mailbox Print
	Scan Mailbox Print
	Print Data Mailbox Print
	Print Stored Faxes
	Print Stored Internet Faxes
	E-mail Mailbox Print
	Mailbox Print
	Copy Server - Print
	BMLinkS Preprint
System Sheet	PostScript Initialize Print
	Print Report
	Options List
	Job History Report
	Error History Report
	Startup Report
	Font List
	Stored Documents List
	DV Report
	Maintenance Report
	Fax Activity Report
	Fax Broadcast Report
	Fax Relay Broadcast Report
	Fax Multi-Polling Report
	Fax Transmission Report
	Fax Protocol Monitor Report
	Fax Unsent Report
	Internet Fax Transmission Report
	Internet Fax Unsent Report
	Calibration Chart
	Test Print
	Stamp List

Service types	Text
File Transfer	MAILBOX
	Secure Print Spool
	Delayed Print Spool
	Charge Print Spool
	Scan to CentreTool
	Scan to File
	Fax Auto Receive
	Fax Manual Receive
	Fax Mailbox Receive
	Fax Polling
	Secure Polling Fax Receive
	Fax Relay Broadcast Receive
	Internet Fax Mailbox Receive
	Mailbox To File
	Mailbox To PC
	E-mail To Mailbox
	Print Mailbox Documents
	Mailbox To SMB
	Fax Protocol Monitor Report To Mailbox
	Copy Server Edit
	Receive Private Charge Print Job
	Private Print Transfer
	Store to USB
	Instruct To Print
E-mail Transfer	Scan to E-mail
	Fax to E-mail
	Send Internet Fax
	Send Fax (Auto) received by Internet Fax
	Mailbox To Email
	Mailbox To Internet Fax
	Store and Send Link
	Scanner and Send Link
Job Flow	Job Flow Service
	External Service Request
	Job Flow Service Log Transfer



Note

For services that do not correspond to the above, [Service Type] and [Service Details] will be recorded as "Unknown".

Staple Type

Text		
No	Left Top Single	Left Bottom Single
Right Top Single	Right Bottom Single	Top Dual
Bottom Dual	Left Dual	Right Dual
Left Tail Single	Right Tail Single	Center Tail Dual
Left Center Single	Right Center Single	Top Center Single
Center Tail Single	Saddle Staple	The Others
(Blank)		

Fold Type

Text		
No	Bi-Fold	Z-Fold
Letter C-Fold	Letter Z-Fold	The Others
(Blank)		

Punch Type

Text		
No	Top-*	Left-*
Right-*	Bottom-*	On-*
The Others	(Blank)	

Roll Sheet Size

Text		
A0	A1	A2
A3	A4	ISO B0
ISO B1	ISO B2	ISO B3
ISO B4	B0	B1
B2	B3	B4
Others (Special A0)	Others (Special A1)	Others (Special A2)
Special_A3	Special A4	Others (A)
Others (B)	Others (C)	Others (D)
Others (E)	Others (C_15)	Others (E_30)
a(8.5x11")	b(11x17")	c(17x22")
d(22x34")	e(34x44")	Others (OTHER)
The Others	Unknown	(Blank)

Formats of Job Log Files (Printer MIB Collection)

This section describes the formats of job log files collected by using Printer MIB (Management Information Base) that is compliant with RFC 1759.



Note

You cannot register a device to collect job logs using SOAP, or MIB as a device using Printer MIB. In addition, you cannot register our device or Fuji Xerox's that is not targeted for collecting job logs as a device to collect job logs using Printer MIB.

Basic Structure of Job Log Files

This section describes the rows comprising job log files and the file formats of job log files.

Rows comprising job log files

Job log files are comprised of the following rows.

- Title Row

Item names of job logs such as "Printer Name", "Branch No.", and "MIB Type" are entered.

- Data Row

Data corresponding to the items of the title row is recorded. The description on the recorded data is provided in "Format of Each Item" (P.410).



Note

- The previous "Total Printed Impressions" is recorded in the first data row.
- When there is no "Total Printed Impressions" update in collecting logs for the day, a job log file is not created.

Format of job log files

A job log file is a text file of CSV format.

Format of Each Item

This table indicates the data formats recorded in the items of job logs.

Job log item	Descriptions	Format
Printer Name	Device name registered in the database of ApeosWare Management Suite	Text
Branch No.	Number indicating the row number within 1 job log "1 of 1" is always recorded.	Total branch numbers (integers) of branch numbers (integers)
MIB Type	Type of Management Information Base	Printer MIB
Product Name	Model name of device. This is not retrieved from some devices.	Text Blank when not retrieved
Job ID	Not recorded	(Blank)
Service types	Not recorded	(Blank)
Host name	Not recorded	(Blank)
User name	Not recorded	(Blank)
Document Name	Not recorded	(Blank)
Job Owner Name	Not recorded	(Blank)

Job log item	Descriptions	Format
Job Client ID	Not recorded	(Blank)
Print Status	Not recorded	(Blank)
Ports	Not recorded	(Blank)
Data Type	Not recorded	(Blank)
IP Address	IP address of device	IP address of device
Output Tray	Not recorded	(Blank)
Pages per Side	Not recorded	(Blank)
Select Paper Tray	Not recorded	(Blank)
Logging Date	Date on which job logs were collected Date of ApeosWare Management Suite server clock	yyyy/mm/dd
Log Collection Time	Time at which job logs were collected Time of ApeosWare Management Suite server clock	hh:mm:ss
Printer Date	Not recorded	(Blank)
Printer Time	Not recorded	(Blank)
Print Start Date	Not recorded	(Blank)
Print Start Time	Not recorded	(Blank)
Print End Date	Not recorded	(Blank)
Print End Time	Not recorded	(Blank)
Total Printed Impressions	Total pages printed from device installation until job log collection	Integer
Total Printed Impressions Since Power On	Total pages printed from device power-on until job log collection	Integer
Error	Error information is not recorded in this item. 0 is always recorded.	0
Printing Output Color	Not recorded	(Blank)
Printing Size	Not recorded	(Blank)
Impressions	Not retrieved. 0 is always recorded.	0
Paper type	Not recorded	(Blank)
Paper size	Not recorded	(Blank)
Number of sheets	Not retrieved. 0 is always recorded.	0
Job Template Name	Not recorded	(Blank)
Number of Copies	Not retrieved. 0 is always recorded.	0
Staple Count	Not retrieved. 0 is always recorded.	0
Original Color	Not recorded	(Blank)
Original Impressions	Not retrieved. 0 is always recorded.	0
Original Type	Not recorded	(Blank)
Document Size	Not recorded	(Blank)
Recipient IP Address	Not recorded	(Blank)
Folder Number	Not recorded	(Blank)
Recipient Fax Number	Not recorded	(Blank)
Fax Remote Terminal Name	Not recorded	(Blank)
F code	Not recorded	(Blank)

Job log item	Descriptions	Format
Fax Line	Not retrieved. 0 is always recorded.	0
Fax Start Date	Not retrieved. 0000/00/00 is always recorded.	0000/00/00
Fax Start Time	Not retrieved. 00:00:00 is always recorded.	00:00:00
Fax Complete Date	Not retrieved. 0000/00/00 is always recorded.	0000/00/00
Fax Complete Time	Not retrieved. 00:00:00 is always recorded.	00:00:00
Fax Duration	Not retrieved. 0 is always recorded.	0
Remote ID	Not recorded	(Blank)
Fax Images Sent	Not retrieved. 0 is always recorded.	0
Fax Image Size	Not recorded	(Blank)
FAX Speed Dial Number	Not recorded	(Blank)
Service Details	Not recorded	(Blank)
Related Job ID	Not recorded	(Blank)
AccountID	Not recorded	(Blank)
Card No.	Not recorded	(Blank)
Meter 1	Not retrieved. 0 is always recorded.	0
Meter 2	Not retrieved. 0 is always recorded.	0
Meter 3	Not retrieved. 0 is always recorded.	0
Billing Meter Number	Not retrieved. 0 is always recorded.	0
Recipient Information	Not recorded	(Blank)
Staple Type	Not recorded	(Blank)
Fold Type	Not recorded	(Blank)
Fold Count	Not retrieved. 0 is always recorded.	0
Punch Type	Not recorded	(Blank)
Punch Count	Not retrieved. 0 is always recorded.	0
Bind Count	Not retrieved. 0 is always recorded.	0
UUID	Not recorded	(Blank)
Document number	Not recorded	(Blank)
Cause of Error	Not recorded	(Blank)
Job Error Code	Not recorded	(Blank)
Fax Sender ID	Not recorded	(Blank)
Fax Dial-In Number	Not recorded	(Blank)
Fax Recipient Information	Not recorded	(Blank)
Fax Call Type	Not recorded	(Blank)
Fax Transmission Speed	Not recorded	(Blank)
Fax Reconnection Flag	Not recorded	(Blank)
Name in Address Book	Not recorded	(Blank)
Send Fax Status	Not recorded	(Blank)
Fax Communication Result	Not recorded	(Blank)
Stored Fax Pages	Not retrieved. 0 is always recorded.	0

Troubleshooting for Image Log

When an error is not resolved even if troubleshooting is conducted, obtain an operation log by the diagnosis tool and send it to the person in charge of our company.



Refer

"Collecting Operation Logs" (P.397)

Error message

Reception service error

Log code	Message	Cause	Action
0070-020004-AWILM	You have failed in initialization of the reception service.	The module cannot be initialized.	Restart Image Log Management Receive Service.
0070-020008-AWILM	The content of the HTTP request is wrong.	An unexpected HTTP request is received.	Check if a job is ended with an error on the device from which an image log is sent. If it is ended with an error, check the error code.
0070-020023-AWILM	Content information: {Data Type} cannot be saved.	Data cannot be saved.	Check the available space of the hard disk and if other data can be saved.
0070-020024-AWILM	Content information: {Data Type} cannot be moved to the receiving spool.		
0070-020025-AWILM	Roll-back processing from the receiving spool cannot be performed.		

Extraction service error

Log code	Message	Cause	Action
0070-030018-AWILM	The folder: <<<{Folder name}>>> cannot be obtained from the receiving spool.	Processing to obtain the receiving spool folder failed.	Check if the receiving spool can be accessed or not.
0070-030019-AWILM	The folder: <<<{Folder name}>>> cannot be created in the extraction spool.	Processing to create the folder in the extraction spool failed.	Check the available space of the hard disk and if other data can be saved. Check if the extraction spool is in the status to create folders.
0070-030020-AWILM	The file: <<<{File name}>>> cannot be copied to the extraction spool.	Processing to copy the file to the extraction spool failed.	Check the available space of the hard disk and if other data can be saved. Check if the extraction spool is in the status to copy files.
0070-030030-AWILM	Attribute file: <<<{File name}>>> cannot be saved.	Processing to save the attribute file failed.	Check that the image log storage is in the status to save files. Check the available space of the hard disk.
0070-030031-AWILM	The attribute file cannot be saved in the image log storage. (Job ID: <<<{UUID}>>>, Reception ID: <<<{Reception ID}>>>)	Processing to save the attribute file in the image log storage failed.	Check that the image log storage is in the status to save files. Check the available space of the hard disk.
0070-030032-AWILM	Attribute file: <<<{File name}>>> cannot be saved.	Processing to save the attribute file failed.	Check that the image log storage is in the status to save files. Check the available space of the hard disk.
0070-030046-AWILM	The content information cannot be saved in the image log storage. (Job ID: <<<{UUID}>>>, Reception ID: <<<{Reception ID}>>>)	Processing to save the content information in the image log storage failed.	Check that the image log storage is in the status to save files.
0070-030047-AWILM	Content file: <<<{File name}>>> cannot be saved in the image log storage.	Processing to save the content file in the image log storage failed.	Check that the image log storage is in the status to save files.
0070-030048-AWILM	Thumbnail image file: <<<{File name}>>> cannot be saved in the image log storage.	Processing to save the thumbnail image file in the image log storage failed.	Check that the image log storage is in the status to save files.
0070-030049-AWILM	Extracted text file: <<<{File name}>>> cannot be saved in the image log storage.	Processing to save the extracted text file in the image log storage failed.	Check that the image log storage is in the status to save files.
0070-030050-AWILM	Content file: <<<{File name}>>> cannot be deleted.	Processing to delete the content file failed.	Check if the extraction spool is in the status to delete files.
0070-030051-AWILM	Thumbnail image file: <<<{File name}>>> cannot be deleted.	Processing to delete the thumbnail image file.	Check if the extraction spool is in the status to delete files.

Log code	Message	Cause	Action
0070-030052-AWILM	Extracted text file: <<<{File name}>>> cannot be deleted.	Processing to delete the extracted text file failed.	Check if the extraction spool is in the status to delete files.
0070-030053-AWILM	The archive file of received data cannot be saved in the image log storage. (Job ID: <<<{UUID}>>>, Reception ID: <<<{Reception ID}>>>)	Processing to save the archive file of received data in the image log storage failed.	Check that the image log storage is in the status to save files.
0070-030054-AWILM	The folder: <<<{Folder name}>>> cannot be deleted from the extraction spool.	Processing to delete the folder in the extraction spool failed.	Check if the extraction spool is in the status to delete folders.
0070-030056-AWILM	Data with which an error occurred (Job ID: <<<{UUID}>>>, Reception ID: <<<{Reception ID}>>>) cannot be moved to the folder: <<<{Folder name}>>>.	Processing to move the receiving data of the job with which an error occurred during extraction processing failed.	Check if the files in the extraction spool can be accessed.
0070-030069-AWILM	The server license of Image Log Management is invalid or not registered.	Authentication of the license failed.	Check the status of the license with License Activator.
0070-030100-AWILM	Synchronization of the database of the main node and configuration file failed.	Synchronization processing of the database of the main node and configuration file failed.	Check that ApeosWare Management Suite of the main node works properly.
0070-030106-AWILM	Timeout occurred during encryption of image log data.	Timeout occurred during encryption of image log data to be stored in the image log storage.	Execute the extraction processing again when the load on the server is not high.

Registration service error

Log code	Message	Cause	Action
0070-090008-AWILM	Registration processing failed due to an unexpected error.	The image log information is inappropriate or SQL Server does not work.	Check the activation status of [SQL Server (FXAW)] of [Service Status] in the System Management screen.
0070-090012-AWILM	Decryption of image log data failed.	Decryption failed when image log data was obtained from the image log storage.	Check that the correct decryption key is set.
0070-090014-AWILM	Processing to update the attribute file failed.	Update of image log data in the image log storage failed.	Check the available space of the hard disk and if other data can be saved.
0070-090021-AWILM	Synchronization of the database of the main node and configuration file failed.	Synchronization processing of the database of the main node and configuration file failed.	Check that ApeosWare Management Suite of the main node works properly.
0070-090024-AWILM	Timeout occurred during encryption of image log data.	Timeout occurred during encryption upon update of image log data in the image log storage.	Check if encryption can be done when the load on the server is not high.
0070-090025-AWILM	Timeout occurred during decryption of image log data.	Timeout occurred during decryption upon acquisition of image log data from the image log storage.	Check if decryption can be done when the load on the server is not high.

Image Log setting screen error

Log code	Message	Cause	Action
0070-060006-AWILM	The configuration file cannot be read. [<<<{File name}>>>]	Reading of the configuration file may be blocked by antivirus software. Or the configuration file may be damaged, or its content is inappropriate.	Check the settings of the antivirus software.
0070-060008-AWILM	The license is invalid.	The valid period of the license may be expired.	Activate License Activator and check [License Status].
0070-601083-AWILM	The search results cannot be downloaded.	Processing to download the search results file failed.	Execute download again. Check the activation status of each service with [Service Status] in the System Management screen.
0070-601010-AWILM	The monitor settings cannot be obtained.	Communication with the SQL Server failed. Or an error occurred on the SQL Server.	Check the activation status of [SQL Server (FXAW)] of [Service Status] in the System Management screen.
0070-601089-AWILM	The group ID cannot be found.	The group ID of the monitor target did not exist upon generation of a monitoring report.	Change the monitor target or delete the monitor target in question in Monitor Settings.
0070-066911-AWILM	An error occurred during image log monitoring processing.	Any of the following problems occurred in the image log monitoring feature. • The mail server is stopped. • The mail server settings are wrong. • The database cannot be accessed. • Information necessary for email notification cannot be obtained.	• Check the mail server settings. • Check the settings of the antivirus software. • Check the activation status of [SQL Server (FXAW)] and [Image Log Management Core Service] with [Service Status] in the System Management screen.
0070-066912-AWILM	An error occurred during image log monitoring processing. (Reason: {Reason})	An invalid group is set in Monitor Settings.	Change the monitor target or delete the monitor target in question in Monitor Settings.
0070-012002-AWILM	You have failed in initialization of the email transmission settings.	You have failed in initialization of the email transmission settings.	Check if the settings are correct in the [Network Settings] page of the System Management screen.
0070-601085-AWILM	You do not have a permission to view Monitoring History.	You do not have a permission to view the Monitoring History screen.	Log in as the image log administrator.
0070-601086-AWILM	You do not have a permission to view Monitoring History of this group.	You do not have a permission to view Monitoring History of the selected group.	Log in as the image log administrator or image log group administrator of the relevant group.
0070-060087-AWILM	Decryption of image log data failed.	Decryption failed when image log data was obtained from the image log storage.	Check that the correct decryption key is set.

Log code	Message	Cause	Action
0070-601082-AWILM	The content file cannot be downloaded.	Processing to download the file failed.	Execute download again. Check the activation status of each service with [Service Status] in the System Management screen.
0070-060137-AWILM	Timeout occurred during decryption of image log data.	Timeout occurred during decryption upon acquisition of image log data from the image log storage.	Check if decryption can be done when the load on the server is not high.
0070-601024-AWILM	Decryption of image log data failed.	Decryption failed when image log data was obtained from the image log storage.	Check that the correct decryption key is set.
0070-601093-AWILM	Timeout occurred during decryption of image log data.	Timeout occurred during decryption upon acquisition of image log data from the image log storage.	Check if decryption can be done when the load on the server is not high.
0070-601095-AWILM	Timeout occurred during encryption of image log data.	Timeout occurred during encryption upon update of image log data in the image log storage.	Check if decryption can be done when the load on the server is not high.

Dealing with Image Log Troubles

Image log search menu is not displayed.

Do you login as a user with an image log search/monitor permission?

To search image logs, a login user needs to have an image log search/monitor permission.

Login as a user with an operation permission or obtain the permission from a user with a user management permission.



"Access Permissions to the Operation Screen" (P.18)

Documents processed by the device are not reflected in the image log search results.

Is the device working normally?

Check if the power of the device is ON. Also check if any error such as a hard disk failure occurs on the device.

Is the image log control feature enabled in the specification settings of the device?

To search the image log, it is necessary that the image log control feature and image log transfer feature are enabled or [Yes] is selected in [Specification Settings] > [Common Settings] of the device.

Check the device settings on the control panel.



The image log control feature and image log transfer feature can be set in the device update features of DM.



Refer

"Image Log Control Settings" (P.84)

Is the image log retention period expired?

If the image log retention period is expired, the image log is archived and excluded from the search targets.

Select [Service Settings] > [Image Log Control] > [Restore Archive] in the administrator screen menu, restore the archived data, set the search target data in [Archived Data], and make a search again.



Refer

"Restore Archive" (P.321)

Monitoring results email does not come.

Are the settings of the sending mail server correct?

Select [System Settings] > [Network Settings] in the administrator screen menu and check if the settings of the SMTP server and SMTP authentication are correct.



Refer

"Network Settings" (P.40)

Is the mail address set correctly?

Select [Service Settings] > [Image Log Control] > [Image Log Monitoring Setting] > [Monitoring Settings] in the administrator screen menu and set the monitoring conditions and mail address.

Check if the mail address is correctly set.



Refer

"Monitoring Settings" (P.324)

Is email sending blocked by antivirus software?

When you have blocked email sending by antivirus software, you cannot receive monitoring results email.

In this case, remove the following files from the settings to block email sending.

- In the case of All-in-One Configuration

Files to remove
{Installation Folder}\Image Log Management\awilm-services\awilm-core\bin\AWILCoreService.exe
{Installation Folder}\WinSvc\Mon\bin\MonSvc.exe

- In the case of Separation Configuration

Files to remove
{Installation Folder of core server}\Image Log Management\awilm-services\awilm-core\bin\AWILCoreService.exe
{Installation Folder of core server}\WinSvc\Mon\bin\MonSvc.exe
{Installation Folder of receiving server}\WinSvc\Mon\bin\MonSvc.exe



Note

By default, {Installation Folder} is "c:\Program Files\FUJIFILM\ApeosWare MS".

Restore data that became an error due to hardware.

When the image log storage cannot be accessed during extraction of image logs for some reasons (for instance, stop of the storage hardware), it results in an error, and the data under processing is moved to a specific error folder.

In this case, if you remove the cause and perform the following operation, the data in the error folder becomes the extraction processing target again.

Execute this operation from Explorer or command line.

(1) Move to the next folder.

{Installation Folder}/Image Log Management/Utils/extractor-error-restore

(2) Activate the next batch file.

awilm-extractor-error-restore.bat



Note

By default, {Installation Folder} is "c:\Program Files\FUJIFILM\ApeosWare MS".