RICOH CloudStream

Device Management Guide

About this Guide

This guide details the features and functionality available in RICOH CloudStream.

RICOH CloudStream offers a total solution for secure and large-scale, integrated management of devices. In addition to providing remote management of device settings, monitoring of devices, and output of reports, RICOH CloudStream can also expand the print and scan functionality of devices. The expanded functionality of the devices can improve user convenience and administrator operation efficiency for management cost savings.

Important

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Ricoh Company, Ltd., its contractors and partners, assume no liability resulting from errors or omissions in this document or from the use of the information contained herein.

Ricoh Company, Ltd. reserves the right to make changes to the product design without reservation and without notification to its users.

Trademarks

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or website is not intended to convey endorsement or any other affiliation with Ricoh products.

Windows, Windows Server, and Internet Explorer are registered trademarks of Microsoft Corporation.

Java is a registered trademark of Oracle in the United States and other countries.

Android and Chrome are registered trademarks of Google Inc.

All other trademarks and copyrights are the property of their respective owners.

All screens used within this guide are for illustration purposes only, i.e., screens may vary based on actual system configuration.

Revision History

Date	Revision	Revision Details
2023-01-01	A.0	First release of document
2024-01-29	A.1	Updated License Management, Email Server Settings, and DM Agent usage.
2024-05-24	A.2	Added instructions for Print&Scan support, Device Policy dashboard, User Management, User registration, SIEM Transfer, and System embedded templates.
2024-08-29	A.3	Updated instructions to connect Device Management (DM) tenant to Print&Scan(PS) tenant. Added a function to support hiding/unhiding job names in Dashboards and Reports. Improved DM Agent Deployment Tool logging.
2024-09-19	A.4	Updated Supported Printers page to include IM C320F. Added 'Trust All Certificates' details to DM Agent Network Range List on page 33. Added new topic Data Flow (Device Management) on page 381 to supply port information.
2024-11-01	A.5	Updated User PIN topic to indicate requirement for User Admin role privileges. Added Flexible Administrator Role on page 174, Uninstall the Flexible Admin Role on page 186, and Flexible Admin Role - Supported Models on page 185. Updated port details in Data Flow (Device Management) on page 381 topic.
2024-11-30	A.6	Updated OpenID Connect Authentication Profile on page 164 to include Okta support. Added topics Import User Cards on page 327 and Export User Cards on page 330.
2024-12-16	A.7	Updated Supported Printers topic to direct user to external site. Added information about Deleting Users in Edit User Properties on page 317 Updated installation details in Install Print&Scan PC

Date	Revision	Revision Details
		Client on page 225.
2025-01-24	A.8	Added Supply Replace Count on page 88 topic. Removed Add License details from License Management on page 121 Added Identify Device DM/PS Version on page 73 topic. Updated DM Agent Troubleshooting on page 42to include SOP panel error message troubleshooting. Updated Device Monitoring Service Polling & Discovery on page 303 to include information message after Discover Now button is pressed. Added Delete profile subtopic in Authentication Profiles on page 150.
2025-04-07	A.9	Added information about the Configuration Task Logs within the System Logs on page 214 topic. Added Set CloudStream PS as the Home Screen Application on page 245 topic. Added Alert Policy for Brother Consumables on page 208 topic. Updated System Logs on page 214 topic. Updated Generate Onboarding Codes on page 148 topic. Updated Certificates and Service Locator URL on page 145 topic. Updated Hide Sensitive Data on page 131 subtopic. Updated Device Reports on page 336 topic.
2025-07-31	A.10	Added Brother MPS Integration on page 299 topics. Updated Login to Print&Scan with OIDC on page 220 topic. Updated DM Agent Deployment Tool Installation on page 30, and Uninstall or Upgrade DM Agent on page 41 topics. Updated Add Devices to CloudStream DM on page 27 topic. Updated Email Server Settings on page 133 topic.

Date	Revision	Revision Details
2026-01-08	A.11	Added Deactivate or Reactivate a Device on page 77 Updated SIEM Data Transfer on page 138 topics Removed SDK/J information from related DM Agent Deployment Tool topics
2026-06-01	A.12	Added Monitor Devices with @Remote topics

Symbols and Tables

The following symbols are used in the manual to help you identify content quickly.

Important:

This symbol indicates important points to note when using the application.

Note:

This symbol indicates supplementary information that you may find helpful when completing a task.

[Bold Text]

Bold text with brackets indicates the name of buttons displayed on the computer screen.

Bold Italic Text

Bold and italic text indicates the name of the screen or field displayed on the computer screen.

Tables

The following tables are used in the manual to guide and inform you of necessary information and steps.

Prerequisites

Prerequisites
Requirement 1
Requirement 2

- This type of table lists all the requirements or the prerequisites necessary before you perform the instructions.
- It may include links to where you can acquire or perform required configurations.

Order of Steps

Order	Instructions
1	Instruction 1
2	Instruction 2

- Please follow the order described in this table before you start the steps.
- It usually includes links to the steps and other helpful information.

List of features and functions

Link to Feature 1

Link to Feature 2

- The features are not in order or may not be dependent on each other.
- The information includes links to the steps and other helpful information.

Information

Item	Description
Item 1	Description for Item 1
Item 2	Description for Item 2

- The table may be used to list settings available for the specific function. It is also used to list column headers and other helpful information.
- The information may include links and other helpful information.

NOTE

You agree and acknowledge that Ricoh will delete the information provided by you (including your personal data) within a reasonable period of time after the termination of your license of the Software (including trial and NFR licenses).

Table of Contents

Getting Started

RICOH CloudStream offers a total solution for secure and large-scale, integrated management of devices. In addition to providing remote management of device settings, monitoring of devices, and output of reports, RICOH CloudStream can also expand the print and scan functionality of CloudStream-managed devices, including devices from vendors.

The expanded functionality of the devices can improve user convenience and administrator operation efficiency for management cost savings. RICOH CloudStream provides remote management of device settings, monitoring of devices, and output of reports. RICOH CloudStream Dashboard focuses on displaying actionable items which require your immediate attention.

How to set up RICOH CloudStream

1 

Administrator Login on page 24

Login and change your password.

2 

Access Profiles and Accounts on page 287

Create the following access profiles.

- Device Administrator
- SNMP (v1/v2 and v3)
- SDK/J Platform

3 

Email Server Settings on page 133

Configure the SMTP Email Server.

4 

Generate Onboarding Codes on page 148

DM Agent onboarding code is required to add Ricoh devices.

5 

Add Devices to CloudStream DM on page 27

Install DM Agent to devices to add them to CloudStream DM.

6 

Print and Scan on page 219

If you have a RICOH CloudStream Print&Scan license, you have to setup the Print&Scan tenant, install PC Client, and deploy the RICOH CloudStream Print&Scan Embedded.

7 

Register Users on page 311

Configure the authentication profiles, then allow end users to register their LDAP or OpenID Connect(OIDC) account to CloudStream DM. Users can register their account if you purchase any RICOH CloudStream Print&Scan license.

Important: Steps 6 and 7 require a RICOH CloudStream Print&Scan license.

Familiarize the CloudStream DM portal and its features in CloudStream DM Main Features on page 22.

CloudStream DM Main Features

The RICOH CloudStream Device Management (DM) portal allows you to manage multiple devices, configure system settings, and manage users and administrators, all of that in one simple application.

The table below gives a summary of each main menu of CloudStream DM.

Area	Description
Dashboard	This section focuses on displaying actionable items which require your immediate attention. The dashboard uses real-time data and displays it graphically and interactively to manage and monitor your fleet of devices. Read more about this in Dashboard on page 46.
Device List	This is where all your devices are listed. You can also see the device's information from this menu. Read more about this in Managing Devices on page 61.
Device Configuration	This section contains features that allow you to configure printer settings. You can also deploy printer firmware, embedded applications, and device policies. Read more about this in Device Configuration on page 234.
System	This section contains the features that allow you to configure email server, activate licenses, view certificates, create alert policies and more.

Area	Description
	Read more about this in System Settings on page 119.
User Management	This section helps you monitor registered end-users properties, including card creation and PIN settings. Read more about this in User Management on page 308.
Reports	Generate reports and create scheduled report tasks in this section. Read more about this in Reports on page 332.

Administrator Login

Open a browser, then access the RICOH CloudStream Device Management (DM) portal using the URL given to you by the sales representative.

The URL will look like this:

`https://(Domain Name).(Region).cloud-stream.ricoh.com/customer.html`

Note: Please use the latest version of the browser.

Follow the steps below to login and update admin information

Order	Instructions
1	Login and Change Password on page 24. After logging in, you can view the Login User Menu on page 26.
2	Update Admin Information on page 26.
3	Create other Administrator accounts. Refer to Administrator Accounts on page 190 for more details.

If you have configured the local administrators and wanted to add LDAP or OIDC accounts as administrator to CloudStream DM, refer to External Administrators on page 196.

Login and Change Password

Login to the application as a default admin and set up the necessary system configurations.

You can find the following features in the Login screen.

Feature	Description
Login using local admin or LDAP admin user	Input user name and password and click the **[Login]** button. To login, follow the steps below. You can also refer to Local Administrators on page 190.
Login using external admin with OIDC	Click **[Login with OIDC]** button and proceed to authenticate with the selected OIDC authentication provider. To login, follow External Administrators on page 196.

Feature	Description
Reset your password via Forgot Password?	Click the link and provide your email address. You can refer to Local Administrators on page 190 and check ***Change Password via Forgot Password*** topic.
Open Cookie Policy and Imprint	Click this if you want to read the CloudStream DM Cookie Policy and Imprint.

To login using default admin. follow the steps below.

1. Copy the URL given to you and paste it in a browser.

List of supported browsers
Google Chrome
Mozilla Firefox
Microsoft Edge

2. In the login screen. keep the ***Profile*** empty.
3. In the user name, enter 'admin'.
4. Enter the temporary password emailed to you.
5. Click **[Login].**
6. For first time login, a pop-up dialog will display; enter the current (temporary) password given to you.

   The default admin's temporary password is emailed to the contact person's email address with the email subject "*[RICOH CloudStream] Welcome to RICOH CloudStream*". The contact person is someone within your company who made the order for RICOH CloudStream Device Management.
7. Enter your new password and confirm it.

   Note: The new password must have the following:
   - Must be 9 characters long.
   - Must have an uppercase character.
   - Must have a special character.
   - Must have a numeric character.

8. Click **[OK].**
9. After confirming the change, login using your new password again.

A successful login will display the Dashboard screen.

Login User Menu

When you login to the CloudStream DM application, you can find the login user menu by clicking the user name in the top-right part of the application.

You can find the following in the user menu.

- Change Password: This allows you to change your password.
- Help: Clicking this will redirect you to the CloudStream DM help site.
- Logout: This allows you to logout from the application
- Version: Displays the CloudStream DM version number.

Update Admin Information

You must update the default admin's email address after the first login. This is an essential step, so if you forget your password, a temporary password will be emailed to you.

To change your email address, please follow the steps below:

1. On the left-hand side navigation, click ***System.***
2. Expand, ***Security***, and select ***Admin Accounts.***
3. Click the admin account.
4. In the ***Edit-Admin Accounts***, add the following:
    - First Name
    - Last Name
    - Email
    - (Optional) Phone
5. Click **[Save].**

Add Devices to CloudStream DM

The DM Agent application is required for Ricoh devices to initiate all communication to the RICOH CloudStream Device Management (DM) server. Once a working DM Agent application is running on the device, it is added to the CloudStream DM, and a DM Agent Certificate is assigned to it.

Use the DM Agent Deployment tool to install the DM Agent application on multiple devices in just one operation.

As of version 1.7.0, the DM Agent Deployment Tool does not require administrator privileges to run and install. Per-user installation can be performed. It is recommended to remove the older versions of the Deployment Tool before using the new version.

Quick Links

Uninstall or Upgrade DM Agent on page 41
Update Firmware on page 39
DM Agent Troubleshooting on page 42

Before running the installer CloudStream DM, make sure the following prerequisites are met.

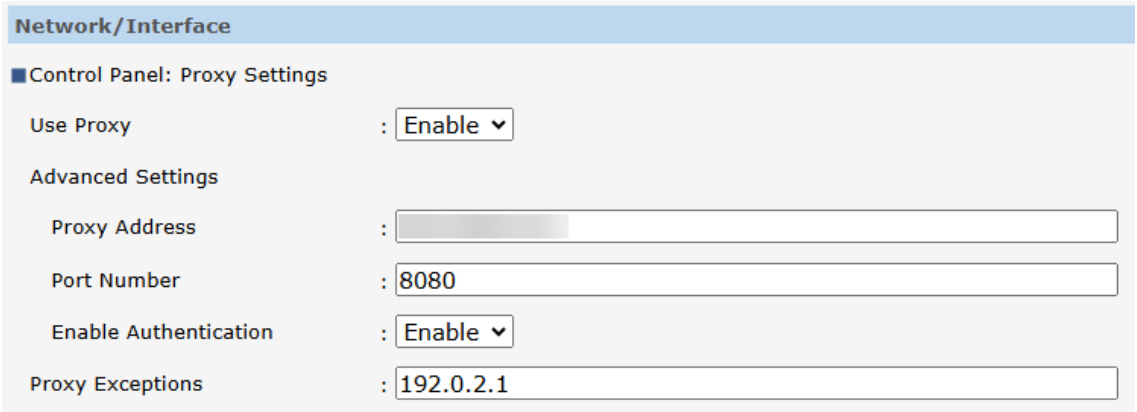
Prerequisites
Important: You have enough RICOH CloudStream Device Management licenses. If the available license is not enough, please purchase an additional license and activate it in License Management on page 121.
Install the tool in DM Agent Deployment Tool Installation on page 30.
Target devices are connected to the same network where the DM Agent Deployment Tool is running. Please find the list of supported model names in Supported Printers on page 380. **Note:** It is recommended that the devices have the latest system firmware version installed. You can upgrade the device firmware by following the steps in Update Firmware on page 39.
Gather the following information. • ***DM Agent Onboarding code.*** See Generate Onboarding Codes on page 148. • ***Service Locator URL.*** Go to Certificates and Service Locator URL on page 145 to copy the URL.
If you use a proxy server, please gather the ***proxy information.***

Prerequisites

For the DM Agent to work correctly, the proxy setting must be set correctly in the Web Image Monitor. Login to the device's WIM, browse to Device Management → Configuration →Screen. Scroll down to locate the Network/Interface section, and look for the Control Panel: Proxy Settings.

- If you have devices that can be registered: Set 'Use Proxy' to Disable.
- If you have devices that cannot be registered: Set 'Use Proxy' to Enable and add 192.0.2.1 to the Proxy Exceptions list.

Test the configuration to ensure device registration is successful.



To install DM Agent, follow the steps below.

Note: Only devices in IPv4 address can be added to CloudStream DM.

Order	Instructions
1	(Optional) Setup the Display Name Format on page 29
2	Add the Access Profiles • Device Administrator Access Profile on page 288 • SNMP Access Profile on page 290 • SDK/J Platform Access Profile on page 289 If one of the target devices uses SDK/J, you must obtain SDK/J password information from the device, and an SDK/J Platform account must be created in CloudStream DM.
3	Install the tool in DM Agent Deployment Tool Installation on page 30

Order	Instructions
4	DM Agent Connection Settings on page 31
5	DM Agent Proxy Settings on page 32
6	DM Agent Network Range List on page 33
7	DM Agent Update and Install on page 35
8	(Optional) DM Agent Summary on page 37
9	(Optional) Check the installed application in device's WIM. a. Open the device's Web Image Monitor (WIM) by typing in the device's IP address in the browser. b. Login as device local admin. c. Go to ***Device Management*** and select ***Configuration***. d. Go to ***Extended Feature Settings*** then click ***Uninstall***. e. All embedded application installed in the device is displayed in ***Uninstall*** page. Confirm that the **CloudStream DM** application with type SOP is displayed in the list.

Note: You can update the DM Agent version by either running a configuration task in CloudStream DM, or adding the DM Agent column to the Device List View. See Update the DM Agent Application on page 286 or Identify Device DM/PS Version on page 73 for more details.

Setup the Display Name Format

Before adding the devices, you might consider changing the default ***Display Name Format***. The ***Display Name Format*** is the format used by newly added devices to display their ***Display Name***.

The default ***Display Name Format*** is ***$[model]$($[ip]$)***, and when new devices are added to CloudStream DM, the devices' ***Display Name*** will be their Model Name (IP Address).

DM Agent Deployment Tool Installation

Use the DM Agent Deployment tool to deploy the DM Agent application to multiple devices at once.

The tool has the following features you can use.

- Add Devices to CloudStream DM on page 27
- Uninstall or Upgrade DM Agent on page 41
- Update Firmware on page 39

Note: If you want to update the DM Agent version by running a configuration task in CloudStream DM, go to Update the DM Agent Application on page 286 for more details.

Before you begin, make sure the following prerequisites are met.

Prerequisites
The DM Agent Deployment tool will run on the following OS only. Please make sure to use one of the operating systems from the list: • Windows Server 2019 Standard/Essentials/Datacenter (64-bit) • Windows Server 2022 Standard/Essentials/Datacenter (64-bit) • Windows 10 (64-bit) • Windows 11 (64-bit)
• The tool requires Amazon Corretto 17 installed on the computer. If a previous version is installed, you must uninstall it before proceeding. The installer will check to determine if Amazon Corretto 17 is installed on the server. If not, a notification message is displayed and you must click Install to proceed. The DM Agent install will proceed automatically after a successful Corretto install.
• If installing DM-Agent Deployment Tool version 1.6.0 or earlier: The DM Agent Deployment Tool must be installed with Administrator access rights and will be installed per user access. Administrator access is not required to run the tool. • If installing DM-Agent Deployment Tool version 1.7.0 or later: The tool can be installed using any access rights.
Download the DM Agent Deployment Tool from the Systems section. 1. Go to ***Systems.*** 2. Click ***Software Download.***

Prerequisites
3. Select ***DM Agent Deployment Tool.*** The download will start after clicking.

Follow the steps to install the tool.

1. Run the installer ***DMAgentDeployToolSetup***.

   The DM Agent Deployment Tool Installer installs the necessary files to run the tool. The installer will check to determine if Amazon Coretto 17 is installed on the server. If not, a notification message is displayed and you must click Install to proceed. The DM Agent install will proceed automatically after a successful Corretto install.

2. Select the language to use.
3. Click **[OK]**.
4. Click next to see the ***License Agreement*** screen.
5. Read the License Agreement then select “I accept the terms in the license agreement” and click **[OK]**.
6. Select the destination folder. A folder is selected by default.
7. Click **[Install].**

To open the tool, go to window's taskbar search box and search for DM Agent Deployment Tool.

DM Agent Connection Settings

1. From your window's taskbar search box, search for DM Agent Deployment Tool, then open the tool.
2. (Optional) If you would like to switch to another language, click on the ***Language*** text in the top-right part of the application.
3. Select ***Install DM Agent*** as ***Action***.
4. Click **[Continue]** to open the ***Connection Settings*** screen.
5. In the Connection Settings screen, enter the ServiceLocator Address. You can find the ServiceLocator Address in Certificates and Service Locator URL on page 145.

   Copy the address except the https:// or the http:// part, then paste it here.

   If the address does not include a port, add port 443 at the end of the address.

   Example: `myservicelocator-msl.cloudstream.ricoh.com:443`

6. Enter the DM Agent Onboarding code. If you don't have the code yet, you can generate the code here: Generate Onboarding Codes on page 148.

   Note: The onboarding code is necessary for the DM Agent Deployment tool to run and register devices. If the code entered is not correct, the installation will not proceed.

   You can register multiple devices by using just one onboarding code.

   Also, you can use the same onboarding code to register another set of devices. As long as the onboarding code has not expired, you can use it to register multiple devices at any time within the valid duration.

7. Enter the Device Administrator user name and password. The credential must match one of the device's user administrators. You must also create an account with the same credential in Device Administrator Access Profile on page 288.
8. After completing the connection settings, go to DM Agent Proxy Settings on page 32.

DM Agent Proxy Settings

If you do not want to use a proxy server, set the Proxy method to ***No proxy***, then click **[Continue]**. Skip the steps below and proceed to DM Agent Network Range List on page 33.

Important: To use the DM Agent Proxy settings when adding the device to CloudStream DM, disable the device's Proxy settings via WIM or the device panel. This will allow the device to connect to the CloudStream DM using the proxy server settings you configured in the DM Agent Tool instead of the device's proxy settings.

1. If you want to use proxy, select either from the two:
   - Proxy with basic authentication
   - Proxy with Kerberos authentication - If this is selected, the following fields are required:
     - KDC
     - Realm

       Service Principal Name
2. Enter the ***Server Address***, either hostname or IP address.
3. Enter the ***Server Port Number.***

   Specify the port number of the Proxy server. Paired with the Server Address, the values will be used to connect to the Proxy server.
4. Enter the Proxy User Name and Password.

Use the User Principal Name (UPN) if using Basic Proxy authentication and Kerberos, and down-level logon name format for NTLM proxy authentication.

5. After completing the proxy settings, go to DM Agent Network Range List on page 33.

DM Agent Network Range List

Add devices to the Network Range List by specifying the IP address, host name, IP range, or simply importing the device list.

After adding the device IP Address/hostname, you can search them to check if they are discoverable.

Follow the order below to add and discover devices.

Order	Instructions
1	Adding Device Manually on page 33 or Importing Device List on page 33
2	Trust All Certificates on page 34
3	Search for Devices on page 34

Adding Device Manually

In the Network Range List screen, click the Add + button to specify device's IP address or host name.

- One hostname: If selected, enter the hostname of a device.
- One IP Address: If selected, enter the IPv4 of the device.
- Specify IP Range: If selected, enter an IP address in ***From*** and ***To*** then specify the ***Subnet Mask***.

Importing Device List

You also have the option to import the device range list in CSV format. Click the Import  button to upload the file. Here is a sample import/export file format.

Line 1:`"From","To","Subnet Mask"`

Succeeding lines:`"10.85.7.1","10.85.7.255","255.255.255.0"`

Line 1 must have the text "From","To","Subnet Mask", then write the IP address range in the succeeding lines.

If you want to input one IP Address, add the following line: `<IP Address>,,,`

If you want to input a hostname, add the following line: `<hostname>,,,`

Note: You can also download the list of IP Address ranges by clicking the Export button.

Trust All Certificates

Check the “Trust All Certificates” to allow the DM Agent tool to bypass the certificate check and remove the security SSL/TLS that provides the encryption of data during the communication.

If you decide to uncheck this setting, ensure that the device “Permit SSL/TLS Communication Settings” is set to “Ciphertext/Clear Text”. If this setting is not possible, you must install the printer device’s certificate in the Windows CA root to the machine where the DM Agent tool is running to allow the communication.

Search for Devices

To discover the devices, click **[Search]** at the bottom of the list grid.

The search will display a pop-up dialog with the number of devices that are found, not found, and not supported. All devices that were found are displayed in the list.

Devices that are 'not found' and 'not supported' are not displayed in the list. However, you can see them and the reason for the failed discovery by clicking the **[Discovery Log]**.

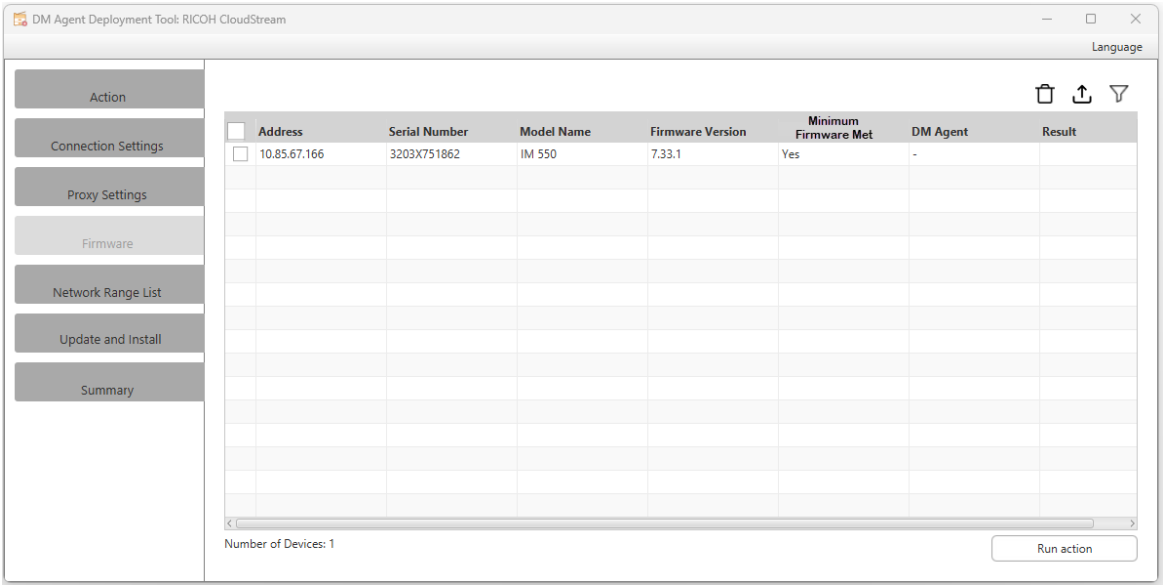
The device activity log will look like this: <date and time>, <device IP address/hostname>, <action performed>, <result and reason of the discovery>

For example: 2024-05-02 12:04:03, 10.10.20.21, Device Discovery, Failed: -- init -- Device not reachable.

The example above shows that the device discovery of device 10.10.20.21 failed because the device was not reachable.

Please proceed run the action in DM Agent Update and Install on page 35.

DM Agent Update and Install



All available devices are displayed on the list grid with their device information. You can delete the devices from the list or export them to a CSV file.

Column Header	Description
Address	The devices IP address or hostname.
Serial Number	The serial number of the device.
Model Name	The device model name.
Firmware Version	If the device allows the tool to read its firmware information, it will be displayed here, else, it will display "Unknown".
Minimum Firmware Met	This column will display three possible values. • “Yes” if the device's current firmware version is equal or above the minimum required firmware (list is located in C\Program Files\Ricoh\DMAgentDeployment\firmwareVersion). • “No” if the device's current firmware version is below the minimum required firmware (list is in C\Program Files\Ricoh\DMA-gentDeployment\firmwareVersion). Device with "No" status cannot be updated because it is below the minimum firmware requirement. • “Unknown” if there is a problem in the device not allowing the process to read firmware info.

Column Header	Description
DM Agent	Displays the DM Agent version if installed and "-" if not installed.
Result	Initially this column is empty. After clicking the **[Run Action]** button, the result is shown after the process. • Failed (if the action failed) • Succeeded (if the action succeeded) The Firmware Version column, Firmware Status column, and DM Agent columns are also updated accordingly after clicking **[Run Action]**.

Run Action

Click the **[Run Action]** button to execute the action selected.

Action	Result
Install DM Agent	The tool will install a DM Agent application to the devices in the list. If RICOH CloudStream Device Management license is insufficient, the installation will still proceed, and devices will still be registered but shall display "blank" or as unmanaged device in CloudStream DM application. After running the operation, the ***Result*** and ***DM Agent*** columns are updated based on the result of the installation. If the DM Agent is successfully installed, the following will be displayed. • Result column: Success • DM Agent column: The DM Agent version. Optionally, you can check the DM Agent Summary on page 37 screen to see the logs.
Uninstall DM Agent	The application will be uninstalled from the device. If the device does not have the DM Agent application installed, it will just **skip** the process. After running the operation, the ***Result*** and ***DM Agent*** columns are updated based on the result of the uninstallation. If the DM Agent is successfully uninstalled, the following will be displayed. • Result column: Success • DM Agent column: -

Action	Result
	Optionally, you can check the DM Agent Summary on page 37 screen to see the logs.
Firmware Update	The device's firmware is updated. After running the operation, the ***Result***, ***Firmware Version***, and ***Firmware Status*** columns are updated based on the result of the update. If the firmware is successfully updated, the following will be displayed. • Result column: Success • Firmware Version column: Firmware version if device allow the tool to read its firmware information, else "Unknown" is displayed. • Firmware Status column: Yes or Unknown Optionally, you can check the DM Agent Summary on page 37 screen to see the logs.

Note: If the result displays fail, please refer to DM Agent Troubleshooting on page 42.

DM Agent Summary

When you perform ***Search*** by clicking the **[Search]** button in ***Network Range List*** screen, the Device Discovery is added to the Summary followed by the Trace Log and Library Logs folder paths.

Device Discovery has the following information.

- discovered
- not found (device not reachable, authentication failed or any other exception)
- not supported (device does not support DM agent)

After you perform DM Agent install, DM Agent uninstall, or firmware update actions, the Summary is updated with the following information:

- Device Discovery: 10 discovered, 0 not found, 0 not supported
- Firmware Update: 0 succeeded, 0 failed

- DM Agent Install/Uninstall: 5 succeeded, 5 failed
- Reinitialize: 0 succeeded, 0 failed

The above is an example that shows 10 devices are discovered and the install/uninstall action succeeded to 5 and failed to other 5 devices. Firmware Update count will be updated accordingly if you perform a firmware update action.

You can see the logs of the operation in Summary Install/Uninstall/Firmware Update/ Reinitialize Log.

Note: If the result displays fail, please refer to DM Agent Troubleshooting on page 42.

If you are installing DM Agent, check the devices in CloudStream DM Device List. You can find topics about managing and monitoring devices in Managing Devices on page 61.

Note: In the Device List, click ***refresh*** to help load newly added devices.

DM Agent Deployment Tool Logs

You can find the DM Agent Deployment Tool logs in the following path:

C:\ProgramData\Ricoh\DMAgentDeployment\CloudStream

The folder result_output logs the tasks you executed with the DM Agent Deployment tool, such as installing and uninstalling the DM Agent embedded from devices.

Result_output logs contain the following information:

<date and time>, <device IP address/hostname>, <action performed>, <result and reason of the discovery>

For example:

> 2024-05-02 12:19:00, 10.10.20.21, Install DM Agent, Succeeded.
>
> 2024-05-02 12:13:00, 10.10.20.22, Uninstall DM Agent, Failed:--Read time out--.
>
> 2024-05-02 12:20:00, 10.10.20.23, Update Firmware, Failed:--Error processing file--.

The example above shows that the DM Agent installation to device 10.10.20.21 succeeded, while the task DM Agent Uninstall to device 10.10.20.22 failed, same with firmware update to device 10.10.20.23.

The table below describes how to troubleshoot the errors:

Error	Troubleshooting
Read time out	The firewall is blocking the connection, please turn it off or modify its rules to accept ports 20 and 21.
Connection closed by remote host	The firewall is blocking the FTP connection, please turn it off or modify its rules to accept ports 20 and 21.
FTP response 421 received	An error occurred during the FTP transfer. Please wait and try again later.
Error processing file	Invalid firmware file sent to the device. Download another firmware file.

Update Firmware

This operation will upgrade the firmware of the target device.

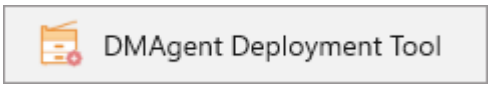
Prerequisites
Install the tool in DM Agent Deployment Tool Installation on page 30.
Target devices are connected to the same network where the DM Agent Deployment Tool is running. Please find the list of supported model names in Supported Printers on page 380.
The Firmware update process uses FTP to send the firmware file to the device. Therefore, FTP must be activated on the device.

The overall flow of updating the firmware is listed below.

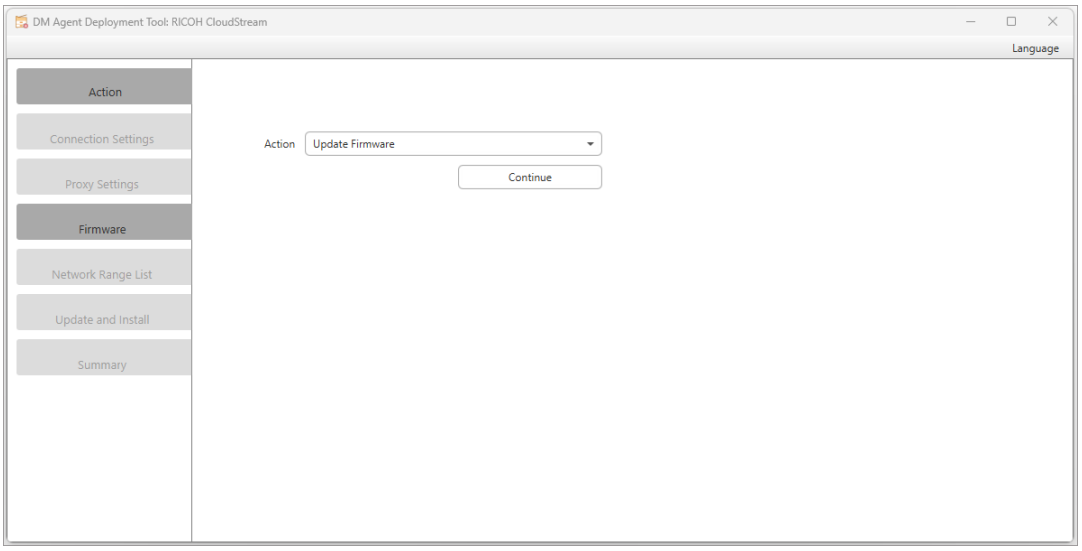
Order	Instructions
1	Select ***Update Firmware*** as action. Please see instructions below.
2	DM Agent Network Range List on page 33
3	DM Agent Update and Install on page 35
4	(Optional) DM Agent Summary on page 37

Note: If the device does not have the DM Agent application installed, it will just **skip** the process. Please check the logs for details.

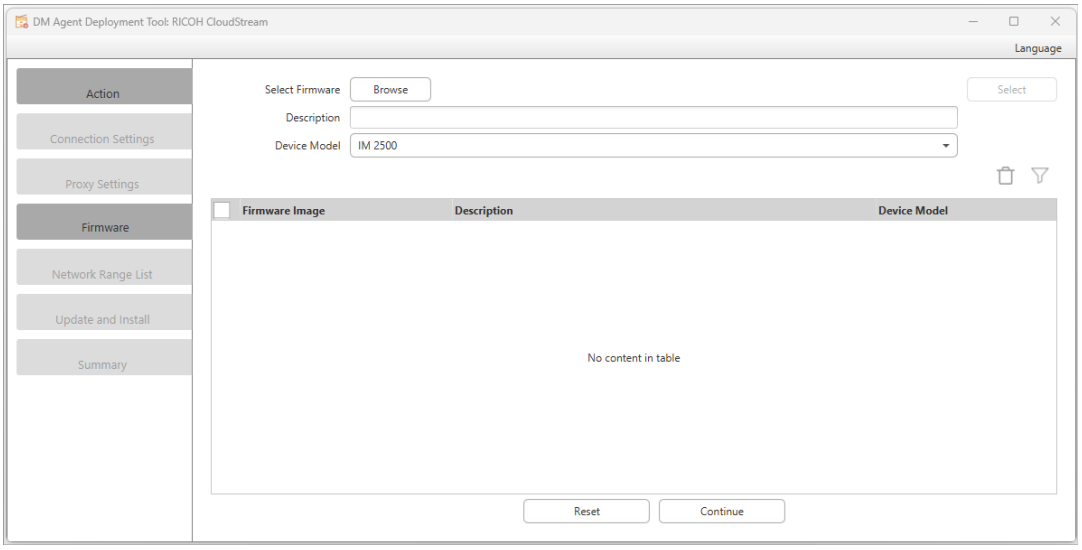
1. From your window's taskbar search box, search for DM Agent Deployment Tool.



2. Click on the tool and the following application is displayed like the image below.



3. Select ***Update Firmware*** as ***Action***.
4. Click **[Continue]**.
5. On the ***Firmware*** screen, click the **[Browse]** button.



6. Choose a file in .pkg or .zip file type.
7. (Optional) Add a description of the firmware.
8. Select the Device Model. For the list of models, please refer to Supported Printers on page 380.
9. Click **[Select]**.

   If the same device model is selected for another firmware, an error is shown with two options:

- Cancel the operation by closing the error pop-up and selecting another device model.
- Replace the device model with the selected firmware.

The firmware will be uploaded to the file to the repository and display it in the list grid.

10. Upload as many packages as you want. After that, click **[Continue]**.
11. Proceed to add devices in DM Agent Network Range List on page 33.

Uninstall or Upgrade DM Agent

Uninstall DM Agent

This operation will uninstall the DM Agent application from the target device.

Important: When the DM Agent application is uninstalled from the device, the license assigned to the device will be released back to the available number of Device Management licenses.

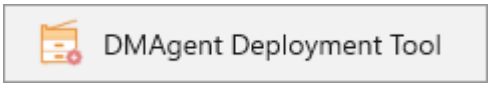
Prerequisites
Target devices are connected to the same network where the DM Agent Deployment Tool is running. Please find the list of supported model names in Supported Printers on page 380.

The overall flow of uninstalling DM Agent is listed below.

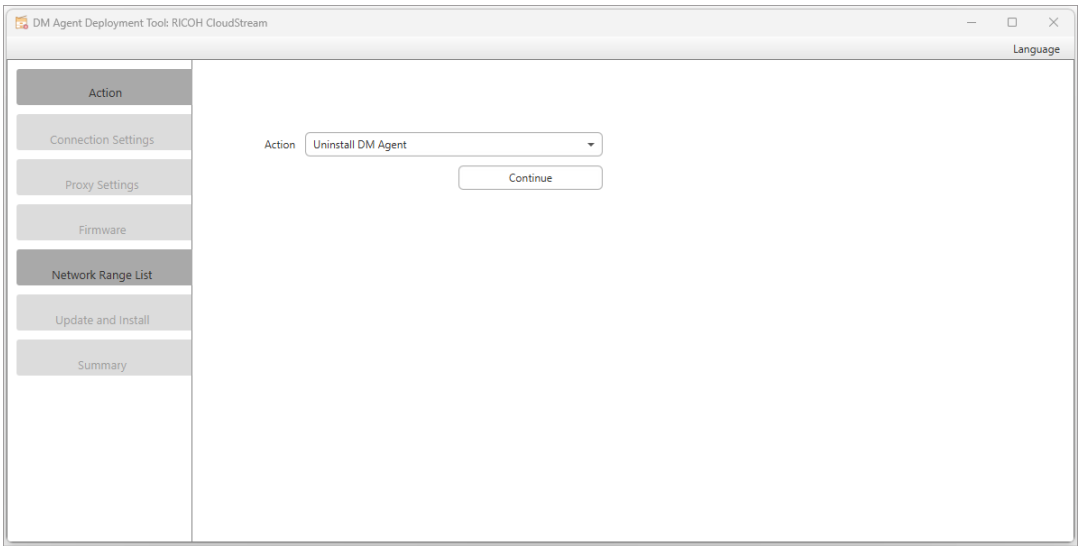
Order	Instructions
1	Select ***Uninstall DM Agent*** as action. Please see instructions below.
2	DM Agent Network Range List on page 33
3	DM Agent Update and Install on page 35
4	(Optional) DM Agent Summary on page 37

Note: If the device does not have the DM Agent application installed, it will just **skip** the process. Please check the logs for details.

1. From your window's taskbar search box, search for DM Agent Deployment Tool.



2. Click on the tool and the following application is displayed like the image below.



3. Select ***Uninstall DM Agent*** as ***Action***.
4. Click **[Continue]**.
5. After setting the action, please go to DM Agent Network Range List on page 33.

Upgrade the DM Agent Deployment Tool

Note:
If you need to upgrade the DM Agent Deployment Tool to version 1.7.0 or later, an Administrator must uninstall the current version before individual users can begin installing DM Agent Deployment Tool 1.7.0 or later. As of version 1.7.0, Administrator privileges are not required to perform the install; however version 1.6.0 and earlier require Administrator access to uninstall.

If the earlier version is not uninstalled first, it will not interfere with a user installing and using version 1.7.0; however, both versions are listed in Programs and Features for the logged in user.

The simplest method to perform an upgrade is to launch a newer version of the DM Agent Deployment Tool. From the Action List, select **Install DM Agent**. Choose the devices with an older version of the DM Agent that you want to update. You will not need to provide the onboarding code using this method.

DM Agent Troubleshooting

Quick Links

SOP Panel Error Messages. on page 43
Re-install DM Agent application. on page 44

Check device account settings. on page 44
Devices are supported, and firmware is updated. on page 45

SOP Panel Error Messages.

If an error occurs during the DM Agent start-up process on a device, the error information is displayed on the SOP Panel, as shown in the panel capture below. Text appears in this location only when an error must be resolved.

Refer to the table below for possible error messages and resolutions.

Error Message	Cause/Resolution
Device information retrieval failed	DM Agent cannot get device information from the device. such as Serial Number, IP address, model name, etc. To resolve, reboot the device or re-install the application (see below) and then reboot the device.
Unable to obtain valid access or SNMP profile	DM Agent cannot find the correct access or SNMP profile. To resolve, create at least one correct device access profile and SNMP profile in CloudStream that matches the access profiles in the device.
Action failed during initialization	DM Agent failed to get Device information in all retry attempts.

Error Message	Cause/Resolution
	To resolve, reboot the device or check the CloudStream server error.
Initialization failed due to certificate error	A client certificate error has occurred. To resolve, use the Deployment Tool to re-install the DM Agent application and create a new client certificate.
Initialization failed due to JSON error	The response from the server could not be parsed, which means that the Server returned the incorrect format JSON string to the DM Agent and it cannot be read. Contact your Ricoh Support Team for assistance.
Initialization failed due to server response error	The server either did not return a response or returned an error. Contact your Ricoh Support Team for assistance.
Initialization failed due to Kerberos error	This message only appears if using a Kerberos proxy and indicates that the DM Agent failed to configure the Kerberos service on the device. To resolve, configure the Kerberos Proxy to correct the settings.

Re-install DM Agent application.

1. Run an Uninstall action on devices. Please see Uninstall or Upgrade DM Agent on page 41.
2. (Optional) Restart the devices.
3. Run DM Agent installation action to devices. Please see Add Devices to CloudStream DM on page 27.
    a. Before installing again, please ensure the DM Agent application is uninstalled. You can check if the DM Agent application is installed on the device by going to its Web Image Monitor (WIM).
    b. Make sure to input the correct credentials in Connection Settings. If the DM Agent onboarding code already expired, generate a new one here Generate Onboarding Codes on page 148.

Check device account settings.

When you identify the target devices, please make sure the following conditions are met.

- The device's local admin matches the application's device administrator account. Please see Device Administrator Access Profile on page 288.
- The device's SNMP configuration matches the application's SNMP account. Please see SNMP Access Profile on page 290.
- The device's SDK/J Platform matches the application's SDK/J account. Please see SDK/J Platform Access Profile on page 289.
- No DM Agent application is installed on the device. Uninstall the DM Agent first before installing again.

Devices are supported, and firmware is updated.

DM Agent supports a list of Ricoh devices; please check the list in Supported Printers on page 380.

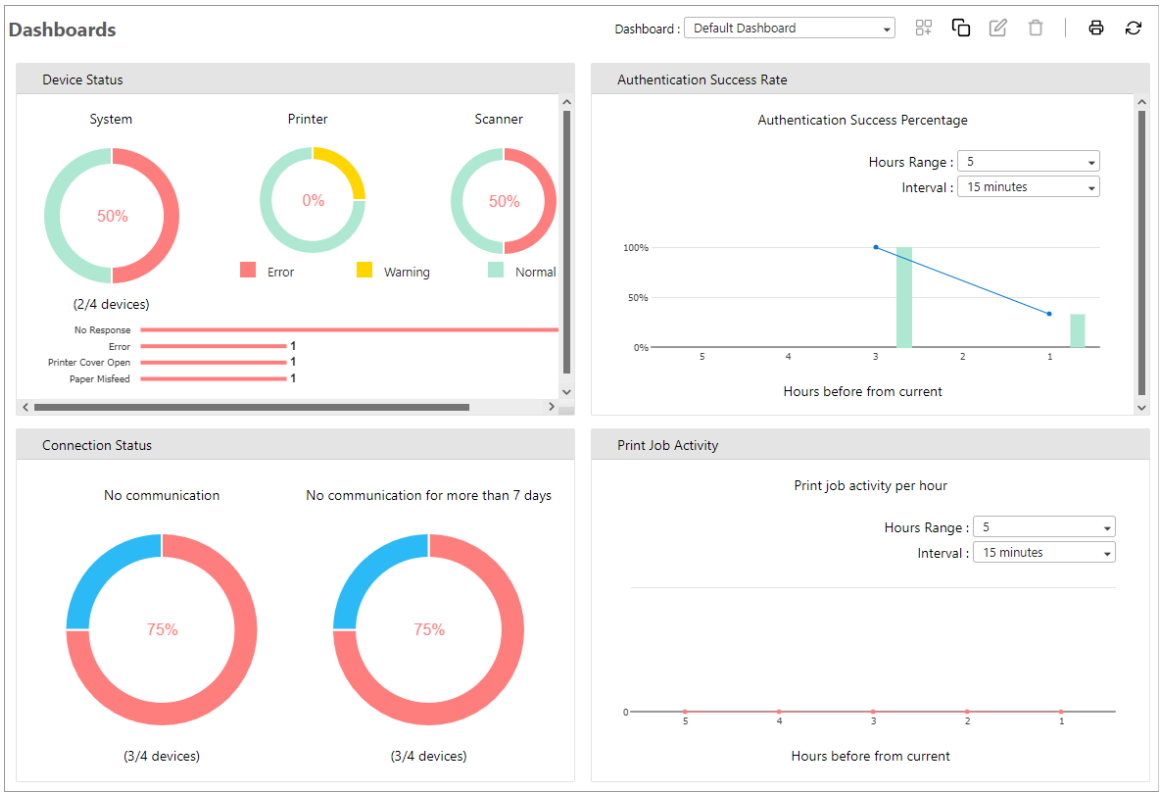
Please make sure the devices' firmware is updated to the latest firmware version.

Dashboard

The ***Dashboards*** section focuses on displaying actionable items which require your immediate attention. The dashboard uses real-time data and displays it graphically and interactively to manage and monitor your fleet of devices.

Here is a list of functions you can explore to maximize the use of the ***Dashboards*** feature.

A dashboard is displayed like the image below. By default, the dashboard is empty. Add a device to populate the data in the dashboard.



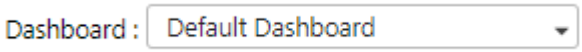
Create Dashboard

A default dashboard is what you see in ***Dashboards*** section the first time you login to RICOH CloudStream Device Management. To create a customized dashboard, you have to duplicate the default dashboard and then customize the new dashboard to your liking.

The custom dashboard is only visible to the administrator account who created it. The default dashboard is the only public dashboard visible to other administrators.

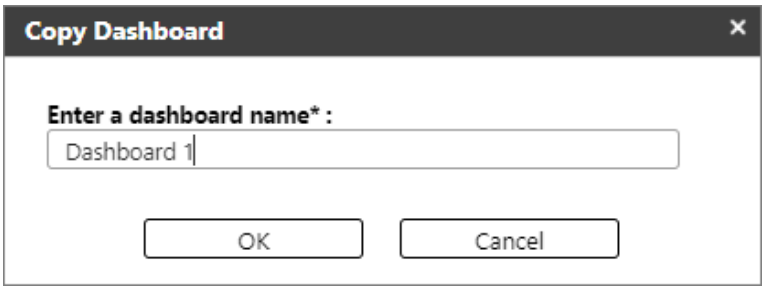
To create a customized dashboard, follow the steps below.

1. Login as an administrator.
2. In the ***Dashboards*** screen, make sure the default dashboard is selected in Dashboard dropdown menu.



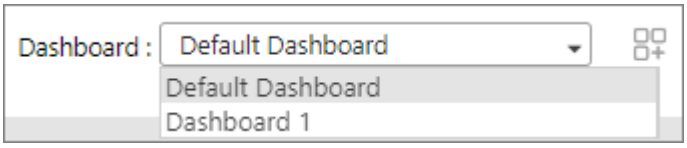
> **Note:** If you have created a custom dashboard, you can also duplicate them. In such case, select the custom dashboard you want to copy.

3. Click the Duplicate icon.
4. A dialog is displayed; please input the dashboard name. The name must not be a duplicate of the existing dashboards.



An example above shows that "Dashboard 1" is the name of the duplicate dashboard.

5. Click **[OK].**
6. Click the Dashboard dropdown, and you will see the duplicate dashboard.



7. Select the new dashboard.

8. Click the Edit Dashboard icon to modify the displayed widgets.

   A similar dialog is displayed.

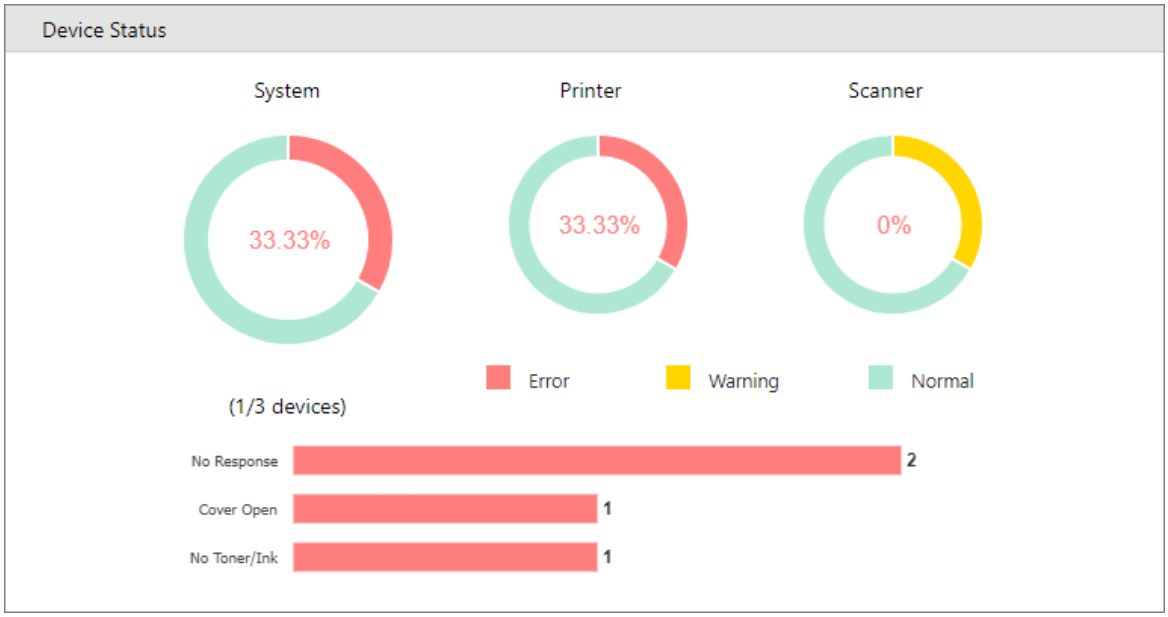
9. Select from the dropdown the type of widget you want to display in the ***Dashboards*** screen.
10. (Optional) Move the widget by dragging and dropping. Click and hold the widget, then drop it to arrange the widget.
11. Click **[OK].**

Note: If you want to delete a dashboard, go to Rename Dashboard and Delete Dashboard on page 59.

Device Status

The ***Device Status*** dashboard shows the current status of the devices. The graph shows the percentages of devices that are in error, in warning state, and normal.

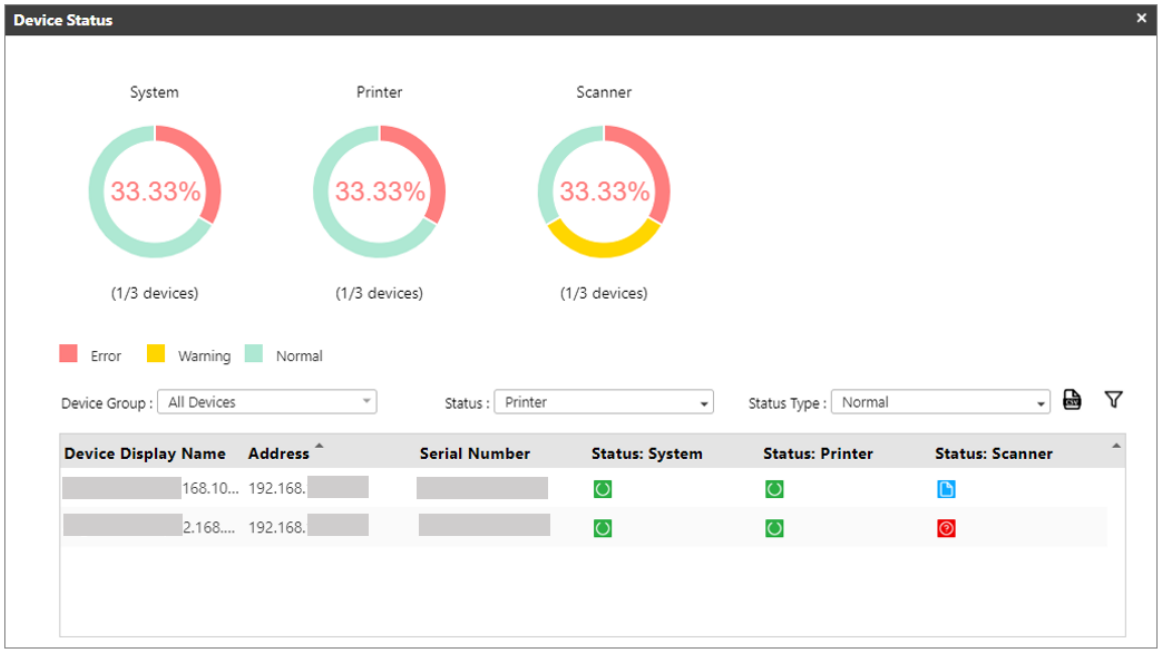
An example below is how ***Device Status*** is displayed in the dashboard.



The horizontal bar graphs show the types of error status the devices are experiencing. At the end of the bar, you can find the total number of devices in such a state.

Click a part of the graph to open the Device Status window to show the devices in the same state.

For example, if you click the green portion of the Printer status, you will see a similar screen pop-up.



On the above screen, you can see all the devices whose Printer status is normal.

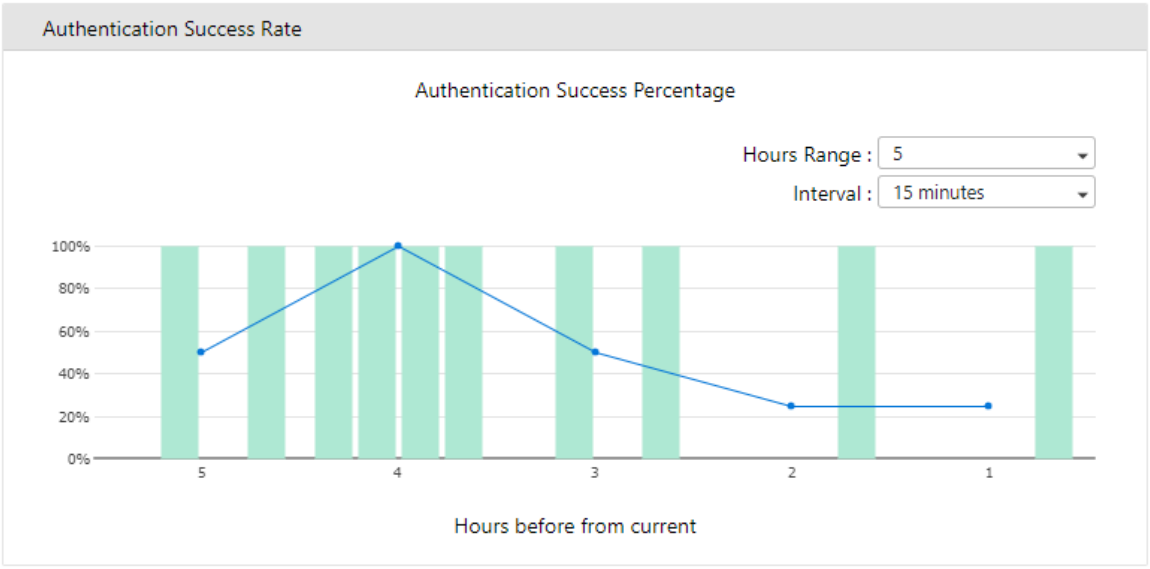
The Device Status detailed screen also has the following functions you can use.

Item	Description
Device Group	Select a group in the dropdown to display the devices within that group.
Status	Select a status you want to filter. Options are Printer, System, and Scanner.
Status Type	Select the type of status you want to see. Options are Error, Warning, and Normal.
Export from CSV	Click this icon to export the list in the table into a CSV file.
Filter	Click this icon to filter the device in the table.
X	Closes the Device Status details screen.

Authentication Success Rate

Authentication Success Rate dashboard shows the percentages of successful authentication based on the range.

An example below is how ***Authentication Success Rate*** is displayed in the dashboard.



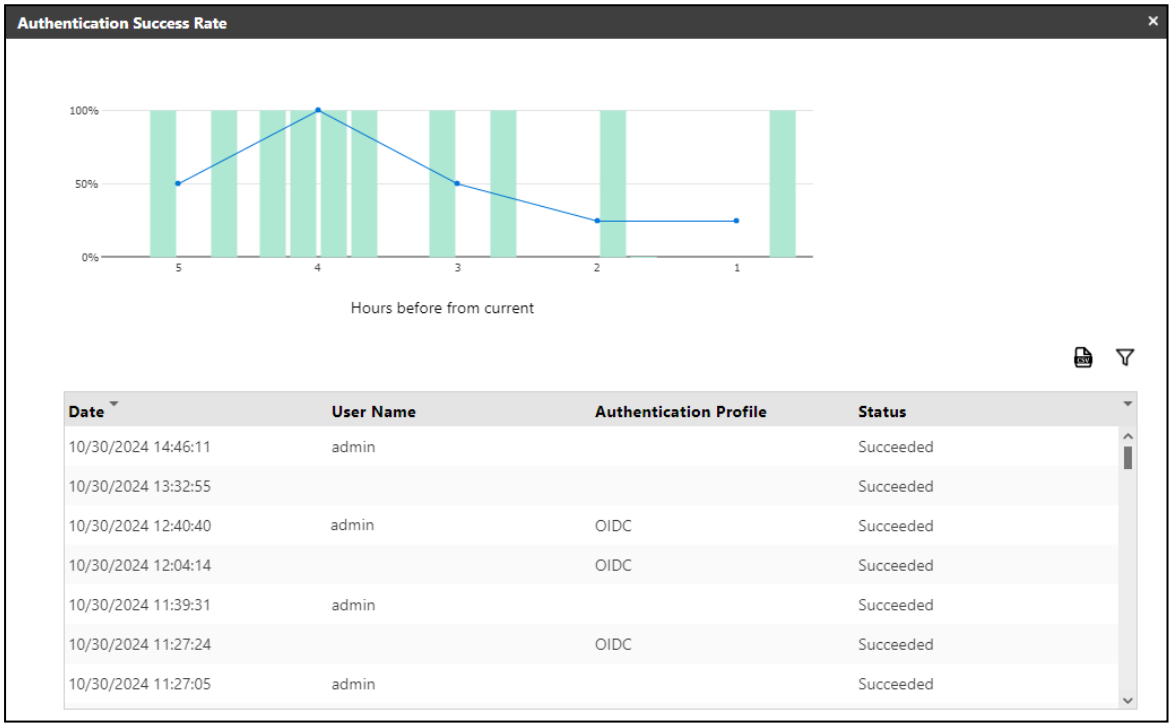
To change the data displayed in the dashboard, modify the following settings to see the line and bar graph update based on your selection.

Item	Description
Hours Range	Select past hours to show from now. Options are 5 hours, 10 hours, and 15 hours. The default is 5 hours.
Interval	Select the interval to a group in minutes.

Item	Description
	Options are 10 minutes, 15 minutes, 20 minutes, and 30 minutes. The default is 15 minutes.

Click a part of the graph to open the Authentication Success Rate window showing the authentication records.

For example, if you click the green portion of the graph, you will see a similar screen pop-up.



On the above screen, you can see all authentication records.

The Authentication Success Rate detailed screen also has the following functions you can use.

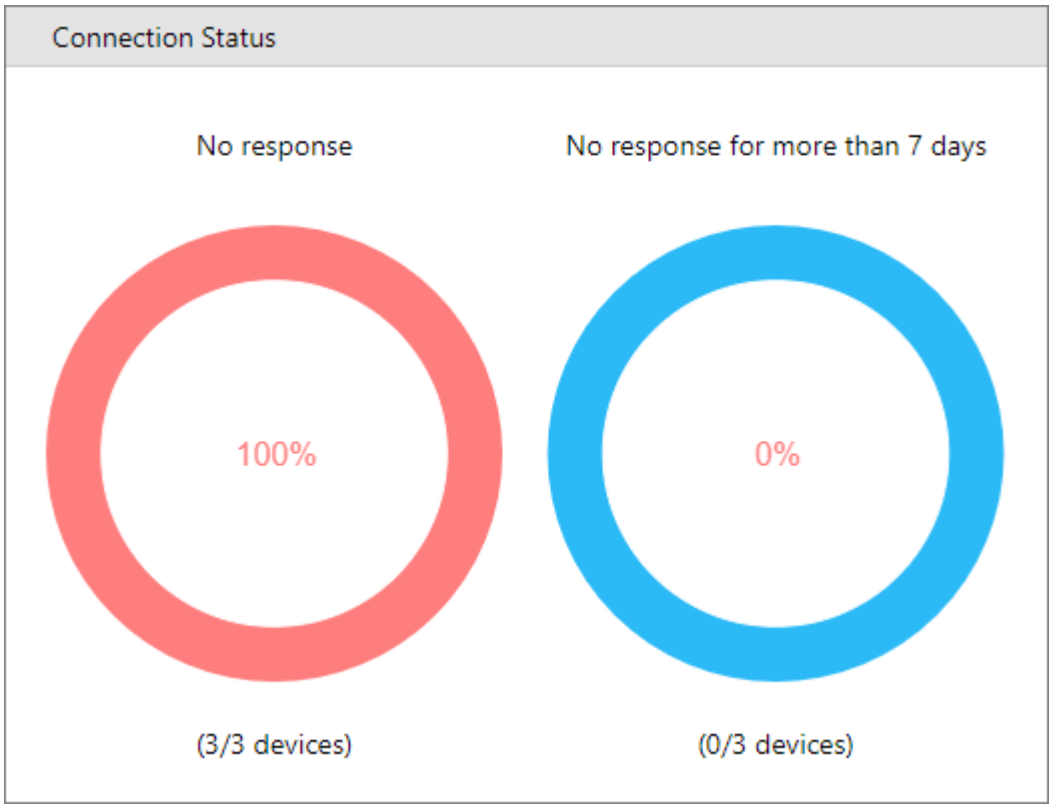
Item	Description
Export from CSV	Click this icon to export the list in the table into a CSV file.
Filter	Click this icon to filter the device in the table.
X	Closes the Authentication Success Rate details screen.

Connection Status

The ***Connection Status*** dashboard shows the device's connection record.

- The first donut chart (No response) shows the data of devices that have no response today.
- The second donut chart (No response for more than 7 days) shows the data of devices that had no response more than seven days from today.

An example below is how a ***Connection Status*** is displayed in the dashboard.



When clicking the RED section of the charts, a full layout will be displayed, filtered by the selected value.

When clicking the BLUE section, no action will be taken.

For example, if you click the RED portion of the Connection status, you will see a similar screen pop-up.

From the above screen, you can see all the devices that are unresponsive to the current day.

The Connection Status detailed screen also has the following functions you can use.

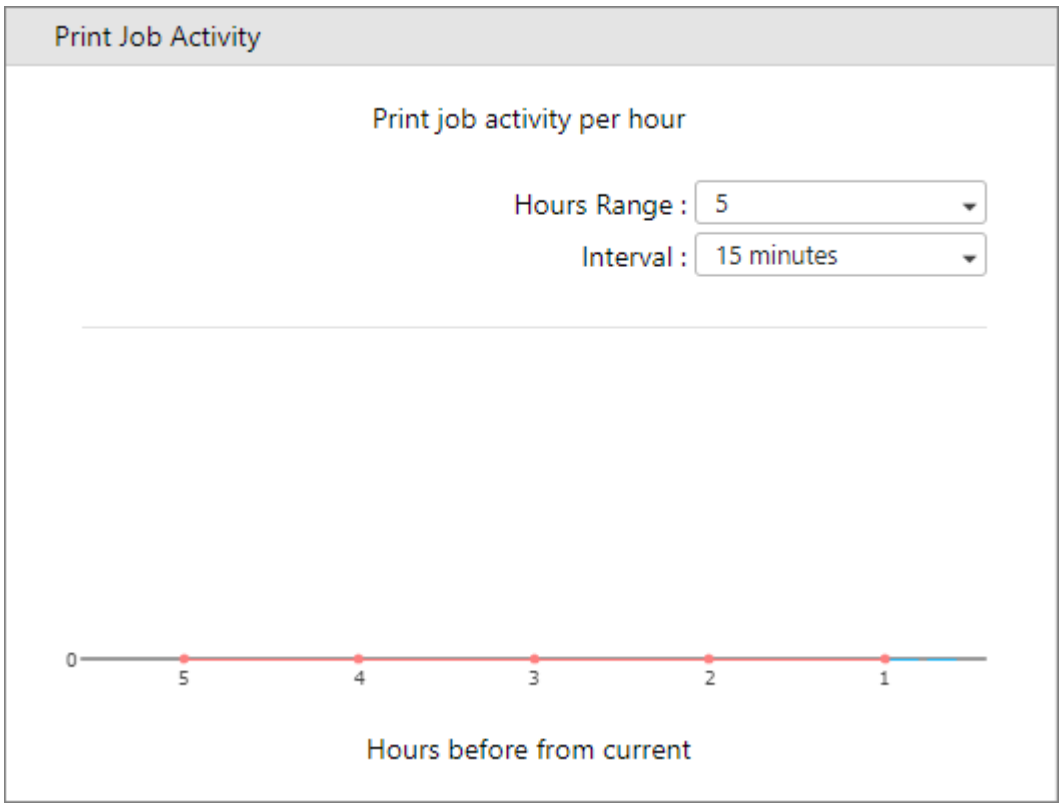
Item	Description
Device Group	Select a group in the dropdown to display the devices within that group.
Status Type	Select the type of status you want to see. Options are No response, No response for more than seven days.
Export from CSV	Click this icon to export the list in the table into a CSV file.
Filter	Click this icon to filter the device in the table.
X	Closes the Connection Status details screen.

Print Job Activity

The ***Print Job Activity*** dashboard shows the print job activity of the devices per hour. The column chart shows the print job activity with an interval grouped by the set hours range.

To use this dashboard you must have a RICOH CloudStream Print&Scan license.

An example below is how a ***Print Job Activity*** is displayed in the dashboard.



Note: The line graph represents the average print job activity per hour, while the column graph represents the activity per interval.

Item	Description
Hours Range	Select past hours to show from now. Options are 5 hours, 10 hours, 15 hours. Default is 5 hours.
Interval	Select interval to group in minutes. Options are 10 minutes, 15 minutes, 20 minutes, 30 minutes. Default is 15 minutes.

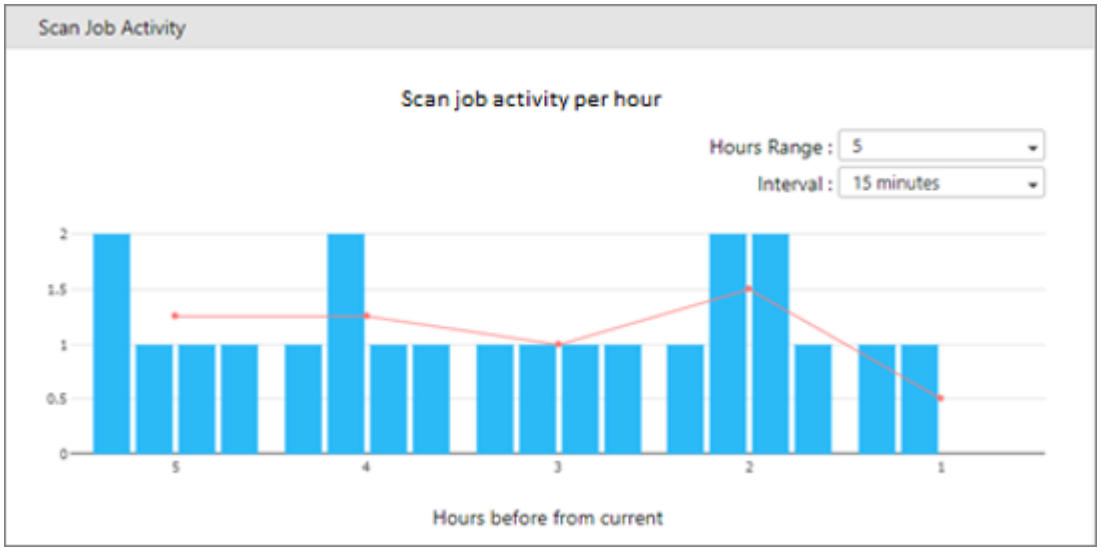
Click a part of the graph, and it will open the Print Job Activity window.

Scan Job Activity

The ***Scan Job Activity*** dashboard shows the scan job activity of the devices per hour. The column chart shows the scan job activity with an interval grouped by the set hours range.

To use this dashboard you must have a RICOH CloudStream Print&Scan license.

An example below is how a ***Scan Job Activity*** is displayed in the dashboard.



Note: The line graph represents the average scan job activity per hour, while the column graph represents the activity per interval.

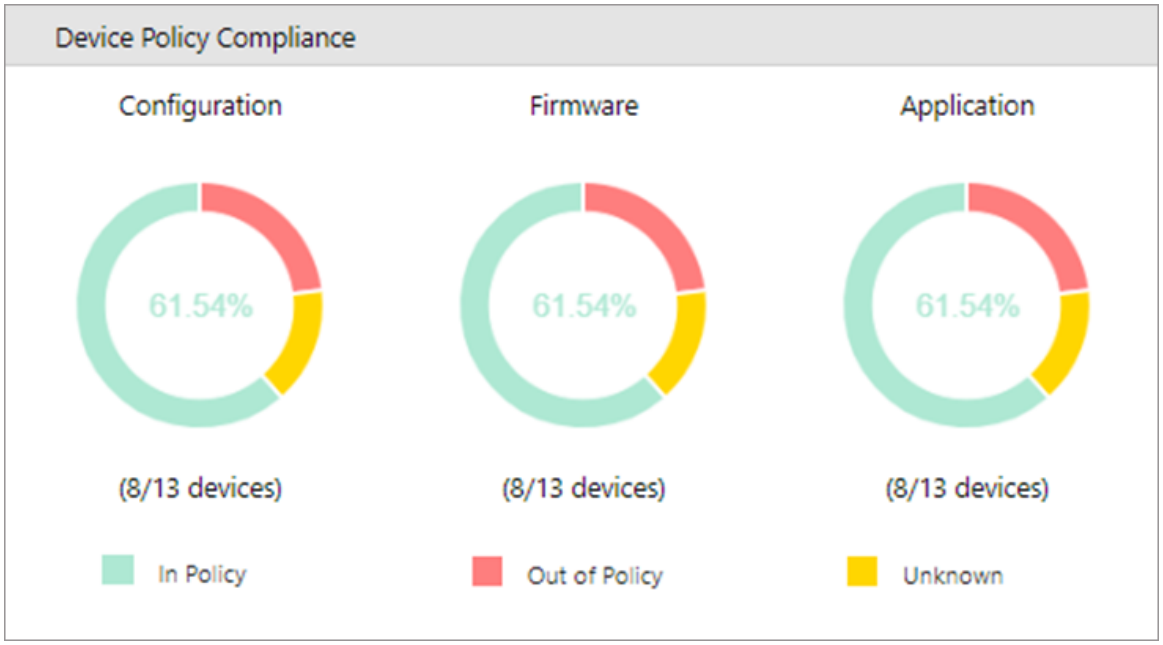
Item	Description
Hours Range	Select past hours to show from now. Options are 5 hours, 10 hours, 15 hours. Default is 5 hours.
Interval	Select interval to group in minutes. Options are 10 minutes, 15 minutes, 20 minutes, 30 minutes. Default is 15 minutes.

Click a part of the graph, and it will open the Scan Job Activity window.

Device Policy Compliance

The Device Policy Compliance dashboard shows whether the devices are compliant with the security standards. The security standards are set when creating a configuration, embedded, and/or firmware policy.

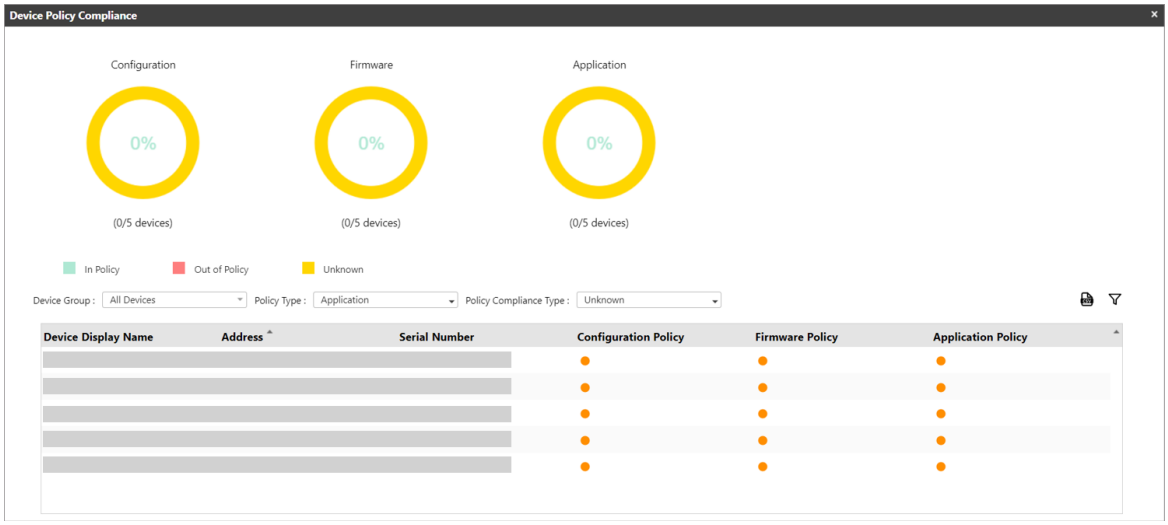
An example below is how the ***Device Policy Compliance*** is displayed in the dashboard.



The percentage in the middle of the chart shows the percentage of fleet devices compliant with the policy.

Policy Status	Description
In Policy	The devices will become 'In Policy' depending on the result of the Policy Check. • If the Policy Check with 'apply' as enforcement type returns a 'success', the device will become 'In Policy'. • If the Policy Check with 'check' or 'apply' as enforcement type returns a 'match', this indicates that the device already conforms to the device policy therefore the device is 'In Policy'.
Out of Policy	Out-of-Policy status is attained if the Policy Check results in 'fail' or 'skip'. Out-of-Policy devices do not have the same settings as the device policies (configuration policy, embedded policy, firmware policy), the device is offline, or unable to communicate with the device. Refer to Troubleshooting Out-of-Policy devices on page 57 for more details.
Unknown	An 'Unknown' status is attained if the Policy Check or Apply is currently being processed. If the device is not assigned to any device policy, then it will be considered 'Unknown'.

Clicking the chart will open the Device Policy Compliance detailed screen, similar to the image below.



Item	Description
Device Group	Select a group in the dropdown to display the devices within that group.
Policy Type	Select policy type. Options are • Configuration (Configuration Policy) • Firmware (Firmware Policy) • Application (Embedded Policy)
Policy Compliance Type	Select the type of policy compliance status you want to see. Options are In Policy, Out of Policy, and Unknown.
Export from CSV	Click this icon to export the list in the table into a CSV file.
Filter	Click this icon to filter the device in the table.
X	Closes the Device Policy Compliance screen.

Troubleshooting Out-of-Policy devices

When the device becomes Out-of-Policy, check the cause of failure during the Policy Check. You can read the reason when you open the device's Activity Logs on page 91.

- Check if the device is online. Access the device's Web Image Monitor(WIM) to verify. The device should be online during the Policy Check.
- Check if the device does not support the device policy settings.

  If the target device does not support the setting set in the device policy, the result will display 'skip' or 'fail', putting the device in Out-of-Policy status.

  For example:

You created a Configuration Policy that sets the access control for Copy and Fax, aiming to require users to authenticate before using the Copy and Fax feature of the device.

After the Policy Check, the devices that do not support Fax are placed in Out-of-Policy status.

To fix this problem, create a new Configuration Policy that sets the Copy access control only and select the devices that do not support Fax as target devices. By doing so, the devices will become 'In Policy'.

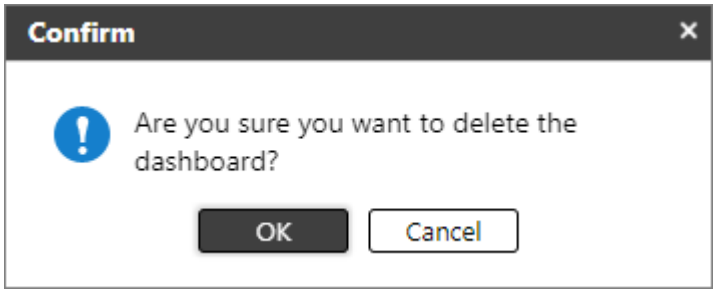
Rename Dashboard and Delete Dashboard

Delete Dashboard

Customized dashboards can be deleted except for the default dashboard.

To delete a dashboard, do the following.

1. Login as an administrator.
2. Go to the ***Dashboards*** screen.
3. Select the custom dashboard you want to delete.
4. Click the Delete icon.
5. Confirm by clicking the **[OK]** button.



After a dashboard is deleted, the default dashboard will be displayed as the selected dashboard.

Note: You can create a new dashboard in Create Dashboard on page 47.

Rename Dashboard

You can modify the name of a customized dashboard, but you cannot do the same to a default dashboard.

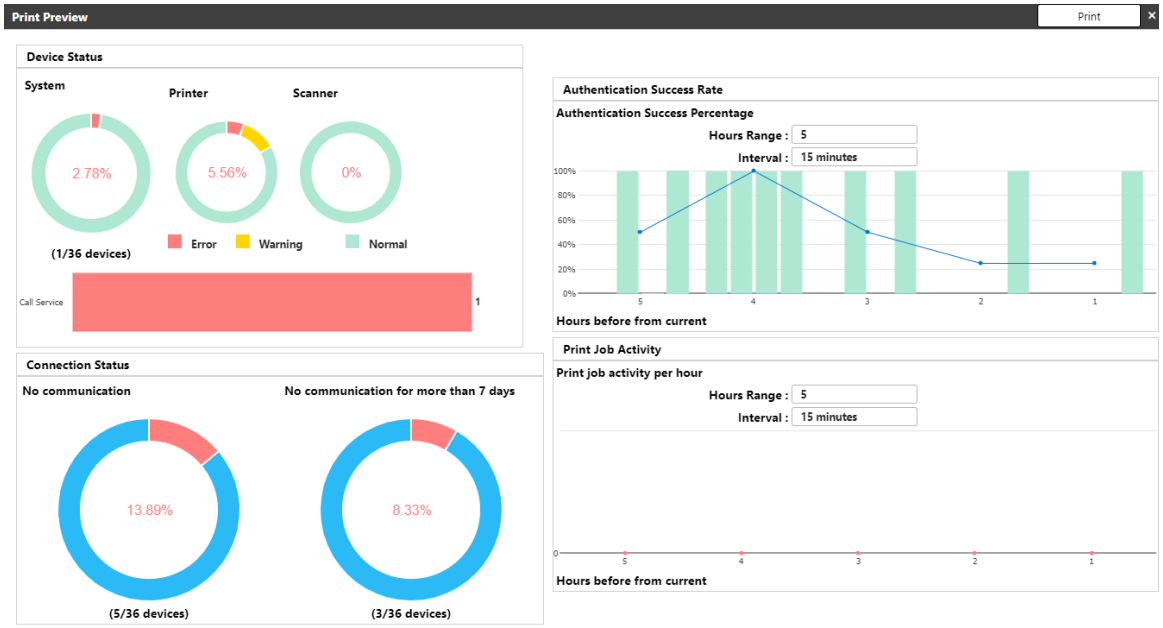
To edit a dashboard's name, do the following.

1. Login as an administrator.
2. Go to the ***Dashboards*** screen.
3. Select the custom dashboard you want to rename.
4. Click Rename Dashboard icon.
5. Modify the name. The name must not be a duplicate of the existing dashboards.
6. Click **[OK].**

Print Dashboard

Clicking the Print icon will display a print preview of the dashboard; click the **[Print]** button to initiate printing.

A sample preview screen is displayed below.



When the **[Print]** button is clicked, the operating system's standard printing screen is displayed.

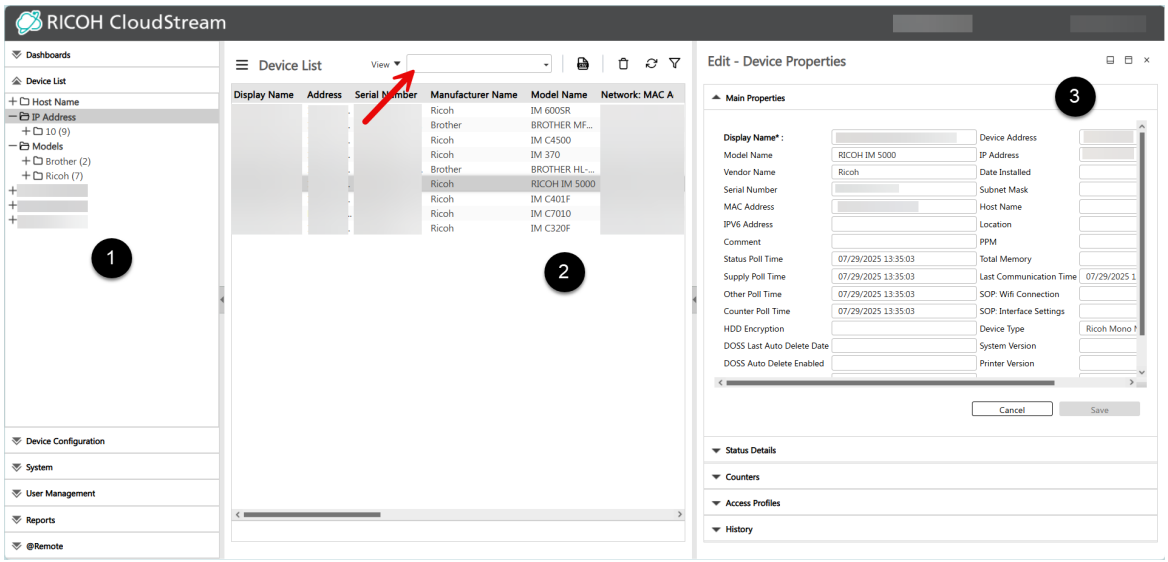
Before proceeding, check if the destination is correct. Modify the destination if necessary, then click **[Print]** to start printing.

Managing Devices

The Device List section displays all Device Management Agent (DM Agent)-managed devices and Work from Home (WfH) Client-managed devices. The devices are grouped based on IP Address, Model Name, and Hostname. If you are managing Brother devices, these devices are listed under a separate entry in the Models list.

In this section, you can create categories and groups to manage your fleet efficiently. Selecting a device in the Device List grid will display the device properties.

Please see an example below when the Device List is populated.



Here is a list of what you see in the ***Device List*** section.

Number	Description
1	The "IP Address" and "Models" are called ***Categories*** The folder "192" is a ***Group*** under the category "IP Address". • The categories "IP Address", "Models", and "Host Name" are default categories. • Create customized categories and groups in Create Categories and Groups on page 64.
2	The Device List displays all your registered devices. • You can control the type of device information displayed in the list by setting the View. For more details, go to Set Device View on page 70. • When searching for a device or group, you can narrow down your search by using the filter.

Number	Description
	See Filter Device List on page 67 for more details. • Export device list into CSV file. Click the  export icon to export the list. If you apply filter on your list view, only the devices shown in the filtered list will be exported. Similarly, if you open a group with limited number of devices, only the devices within the group is exported. The exported filename will be in this format: <Date and time and timezone> DeviceList.csv • To add devices go to Add Devices to CloudStream DM on page 27. **Important:** You can only add devices if you have enough Device Management licenses. Even if the DM Agent embedded deployment is successful, the devices **will not be added.** Please acquire additional licenses and then activate them in License Management on page 121. • To de-activate or re-activate an MFP device go to Deactivate or Reactivate a Device.
3	The Device Properties pane is opened when you select a device in the Device List. Please see Device Main Properties on page 79.
4	Work from Home (WfH) Devices on page 101.

Important: Clicking the **[Delete]** button in the Device List will only remove the device from the list temporarily if a certificate is still active.

Note that when the “Atremote Management Mode” in the Device List is set to “Managed,” it is not possible to delete a device from the DeviceList.

You must properly delete the device and its certificate. To delete a device, please go to Remove Device from CloudStream DM on page 75.

In summary, you can effectively manage and monitor your devices by using the following functions.

Manage Device List Display

Create Categories and Groups on page 64.
Set Device View on page 70.
Filter Device List on page 67.

Viewing Device Properties

Device Main Properties on page 79.
Status Details on page 82. • Toner / Ink Status on page 84. • Paper Tray Status on page 86. • Output Tray Status on page 87.
Counters on page 89.
Activity Logs on page 91.
Optional Properties on page 94.
Access Profiles on page 97.
History on page 98.

Work from Home

Work from Home (WfH) Devices on page 101.
Set Work from Home Polling on page 103.
View WfH Device Groups on page 104.
WfH Device Properties on page 105.
Change WfH Device State on page 108.
Work from Home (WfH) Client on page 111. • Install Work from Home Client on page 112. • Add Devices to WfH Client Computer on page 117.

Configure Devices

Configuration Task on page 272.
Device Policies on page 261.
Alert Policy on page 201.

Deactivate Device

Deactivate or Reactivate a Device on page 77

Remove Device

Remove Device from CloudStream DM on page 75.

Create Categories and Groups

Grouping devices help you manage the fleet effectively. Functions such as Configuration Task on page 272 and Device Policies on page 261 let you select a specific group of devices as their target receiver of the settings.

You can easily group the devices in one view by dragging devices from the unassigned groups to the customized group.

To create a group, follow the steps below:

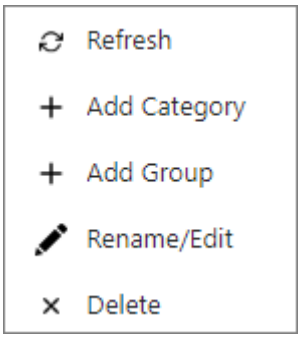
Order	Instructions
1	Create a Custom Category on page 64.
2	Create a Group on page 65.
3	Move Devices to the Group on page 66.

Create a Custom Category

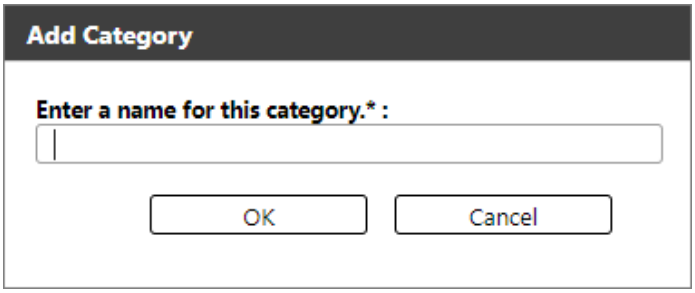
A custom category is a node that is displayed below the default categories (IP Address, Models, and Host Name).

Note: You must create a category before you create a group.

1. Go to ***Device List.***
2. On the left-hand side, right-click on the empty area.

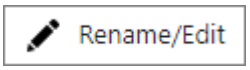


3. Click **[+ Add Category].**



4. Enter the name of the Category. The name must not be a duplicate of the existing categories.
5. Click **[OK].**

Every custom category has a default "unassigned" group, which contains all the devices in the list. Expand the category to see the 'unassigned' group.

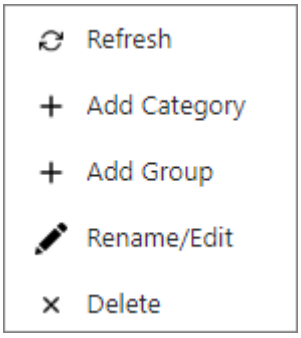
You can edit the name of the category by selecting **[Rename/Edit]** 

in the right-click options.

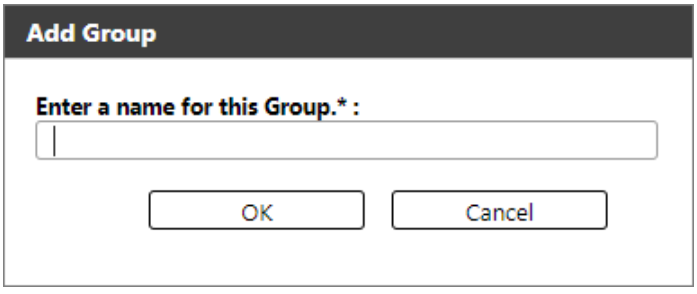
Create a Group

A group can only be created under a category. You must select the category where you want your group to be added.

1. Go to the ***Device List.***
2. On the left-hand side, select a category where you want the group to be added.



3. Right-click and select **[+ Add Group].**

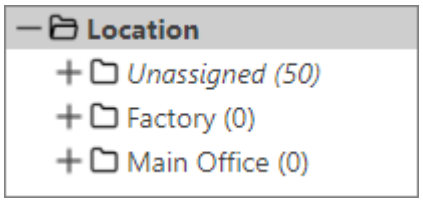


4. Enter the name of the group. The group name must not be a duplicate of the existing groups within the selected category.
5. Click **[OK]**.

The created group will be displayed under the selected category. By default, the number of devices besides the group name is zero. The number will change when you start moving devices to the group.

Note: You can create multiple groups in one category, and a group can have one or more sub-groups. To create a sub-group, select a group in step #1 instead of a category. From the group, right-click and add a group.

An example below shows the groups "Factory" and "Main Office" are created under the category "Location". Both newly created groups have zero devices in them; drag devices to the group to add them.



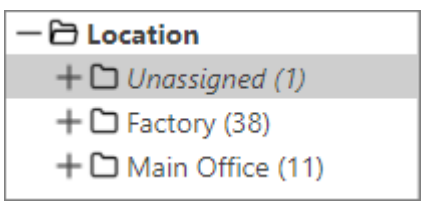
Move Devices to the Group

Every category has an "Unassigned" group which contains all devices that have not been placed in a named group. Add devices to the group by dragging the devices.

1. Click the "Unassigned" group.
2. In the list of devices, select a device or multiple devices.

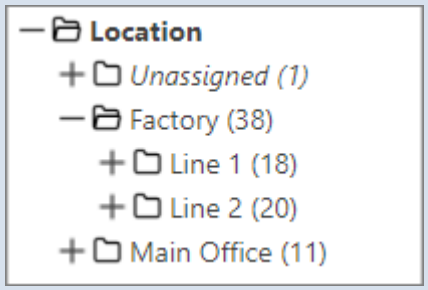
   You can use your keyboard keys to select multiple devices. Click the first device, then press *Ctrl* or *Shift*, and then click the last device. *Ctrl* lets you click multiple devices, while *Shift* selects all devices between the first and last device.
3. Click and hold, then drag them to the group where you want the devices to be added.

An example below shows the groups "Factory" and "Main Office" now have devices under them.



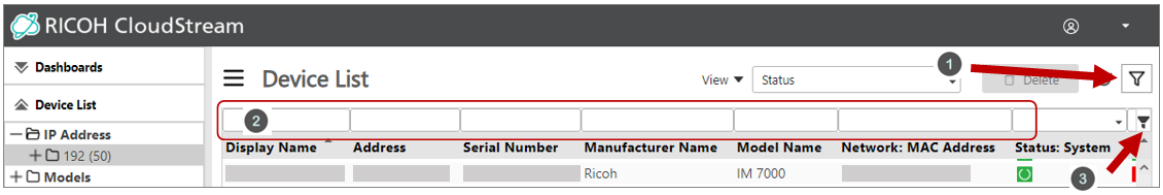
Note: A device can only exist in one group. If you want to sort devices within a group, you can create a sub-folder and add the groups from there.

The example below shows devices grouped within the "Factory" group.



Filter Device List

Use the filter function to narrow down your search.



1. Click filter icon so the filter boxes will display.
2. Input the value in the box above the column where you want to search.

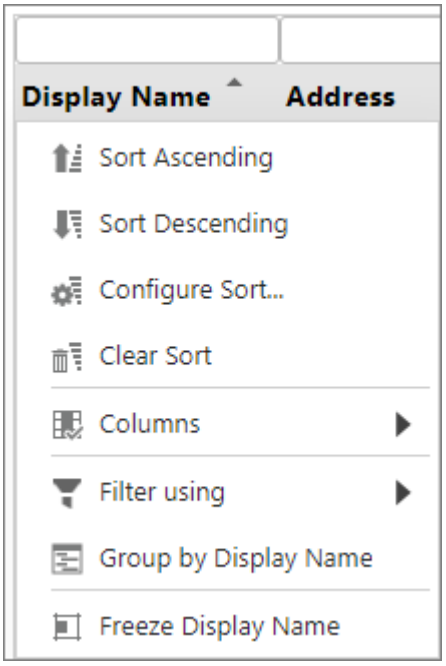
   For example, to search for the device IM 7000, input "IM 7000" in the search box above the Model Name column.
3. Click the filter search button. You can also press the '*Enter*' key on your keyboard.

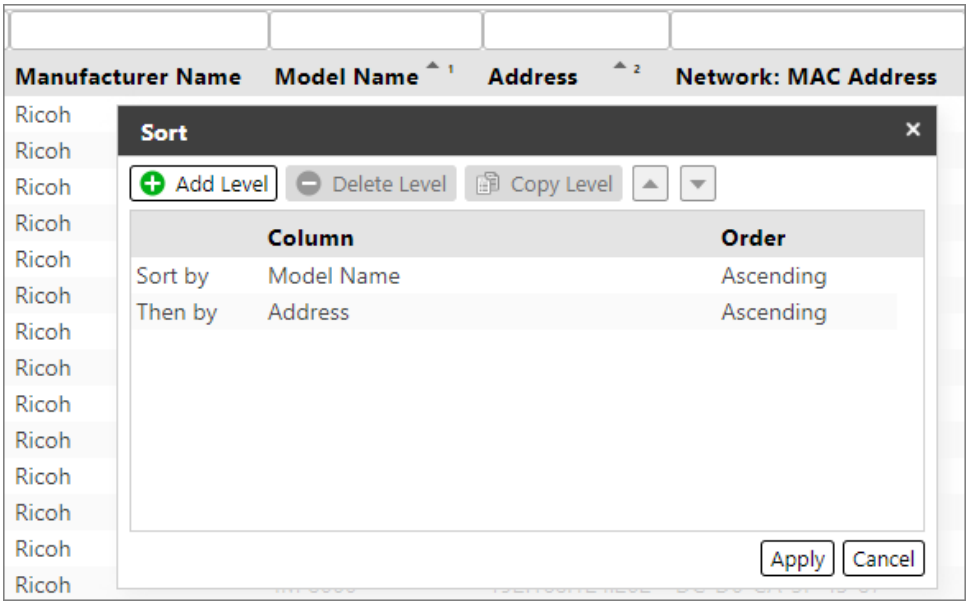
All devices that match your search will be displayed in the list.

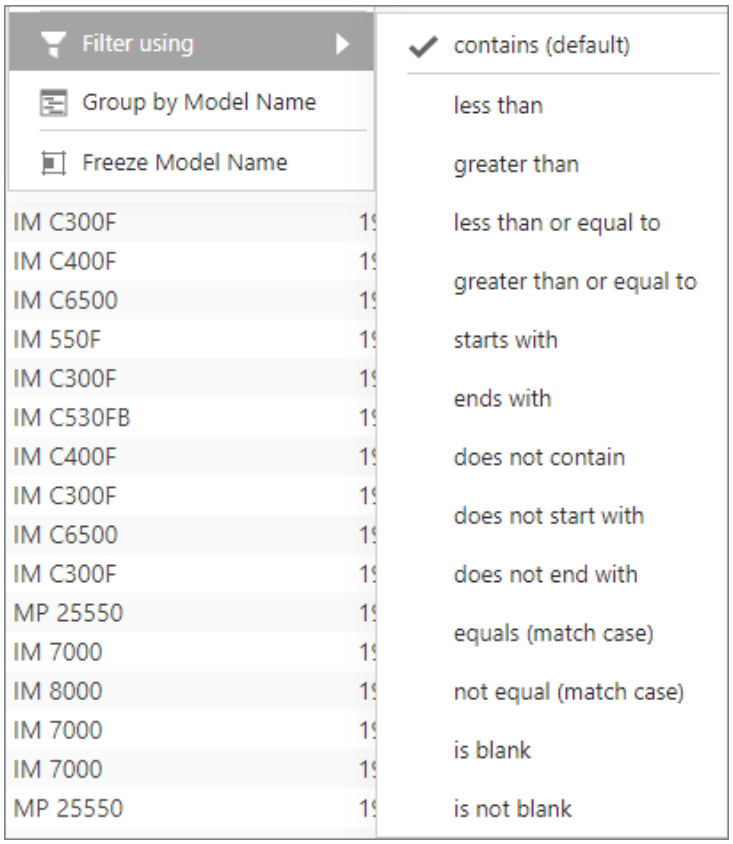
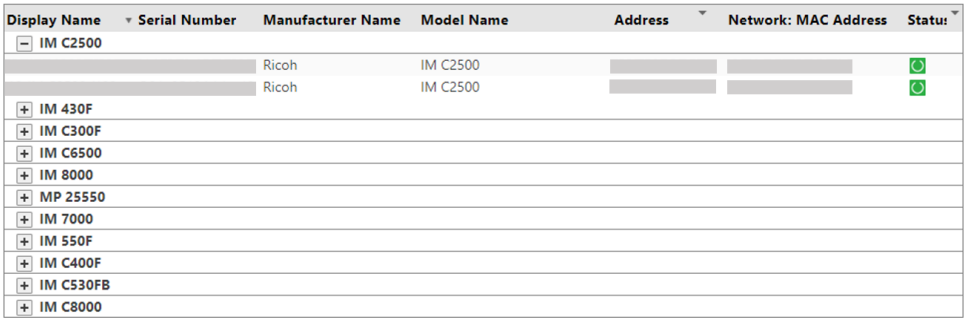
Note: If you want to remove the search result, delete the text you inputted or items you selected from the search boxes, then click the filter search button. Clicking the filter button will not remove the filter criteria but will only hide the search boxes.

Filter by value

You can also filter and sort the values using the following options. Right- click on one of the columns to view the sub-menus.



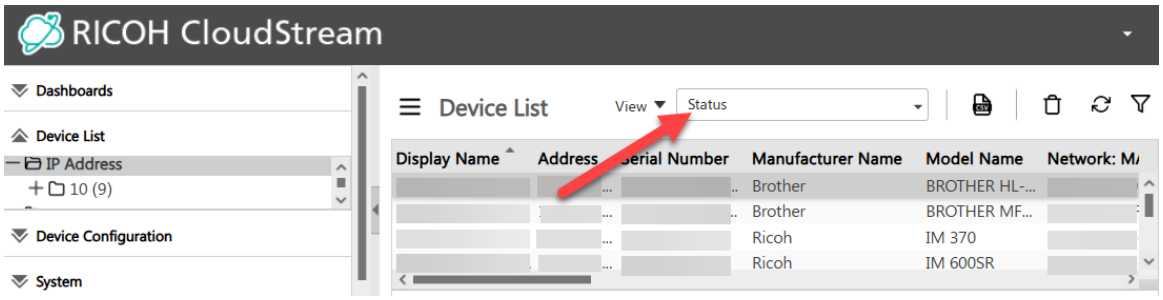
Option	Description
Sort Ascending	Sorts the device list in ascending order. If there is an active search criterion, the search results will be sorted in ascending order when this option is selected.
Sort Descending	Sorts the device list in descending order. If there is an active search criterion, the search results will be sorted in descending order when this option is selected.
Configure Sort	Allows you to sort by level. When selected, the following dialog will display.  For example: Add a second level to sort the device based on Address. All devices will be sorted based on the Model Name and then will be

Option	Description
	sorted based on Address. You can see the level displayed in the column name.
Clear Sort	Clears all sorting configurations. If there is no active sorting option, this menu is not displayed.
Columns	Allows you to select the columns displayed in the list.
Filter using	When selected, more filter options are displayed. Select the option you want to use. When the filter is applied, all devices that match the filter criteria will be displayed in the list. 
Group by <Column name>	Groups the list based on the selected column. For example, when ***Group by Model Name*** is clicked, the following will be displayed.  Click **ungroup** from the sub-menu to remove the grouping.

Option	Description
Freeze <Column name>	Moves the selected column to the farthest left and freezes it. You can scroll to the right to see other columns, but frozen columns will remain displayed.

Set Device View

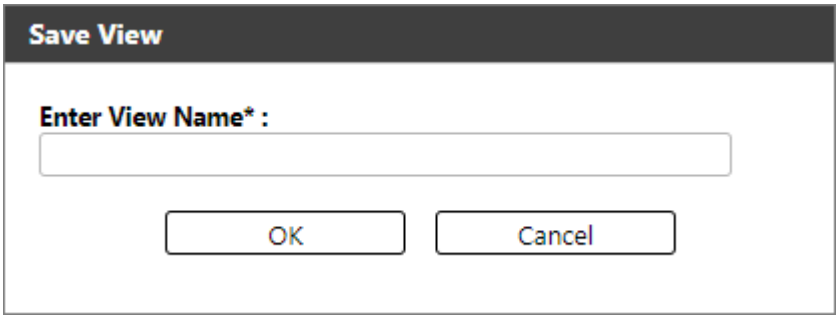
You can select the view in the top right corner. You can select either Basic on page 71, Counters on page 71, or Status on page 72.



To customize a view, follow the steps below:

1. Click the view dropdown and select the type of view you want to copy.
2. Click the ***View***  button.

3. Click ***Save As.***
4. Enter the name of the view in the pop-up dialog.



5. Click [OK].
6. Click the view dropdown and select the custom view you created in the previous step.
7. (Optional) Right-click on the column header and click ***Columns***, then select the desired columns.
8. (Optional) Create filters. Follow the steps in Filter Device List on page 67.

Below is the list of columns displayed based on the selected View.

Note: To understand the status icons, please go to Status Details on page 82.

Types of Views	Columns
Basic	• Display Name • Address • Serial Number • Manufacturer Name • Model Name • Network: MAC Address • Network: IP Address • Network: Host Name • Status: System • Status: Printer • Device WIM location • Device: WIM Comment • Other Poll Time • Group • Configuration Policy • Application Policy • Firmware Policy • Licenses
Counters	• Display Name • Address • Serial Number • Model Name • Network: MAC Address • Configuration Policy • Application Policy

Types of Views	Columns
	• Firmware Policy • Licenses • Date/Time: Last Counter Poll • Counters: Device Total • Counters: B&W Copies • Counters: Full Color Copies • Counters: Single-color Copies • Counters: Two-color Copies • Counters: B&W Prints • Counters: Full Color Prints • Counters: Single-color Prints • Counters: Two-colors Prints • Counters: B&W Received Fax Prints • Counters: Single-color Received Fax Prints • Counters: Duplex Prints
Status	• Display Name • Address • Serial Number • Manufacturer Name • Model Name • Network: MAC Address • Status: System • Status: Printer • Configuration Policy • Application Policy

Types of Views	Columns
	• Firmware Policy • Licenses • Status: Copier • Status: Scanner • Status: Fax • Date/Time: Last Counter Poll

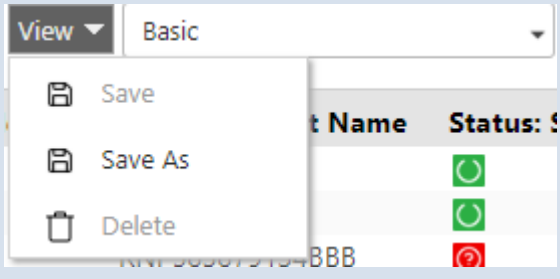
Identify Device DM/PS Version

You can add columns to the Device List that indicate the DM Agent and/or Print&Scan Embedded versions installed on a device. You can add these columns to any View type in the Device List.

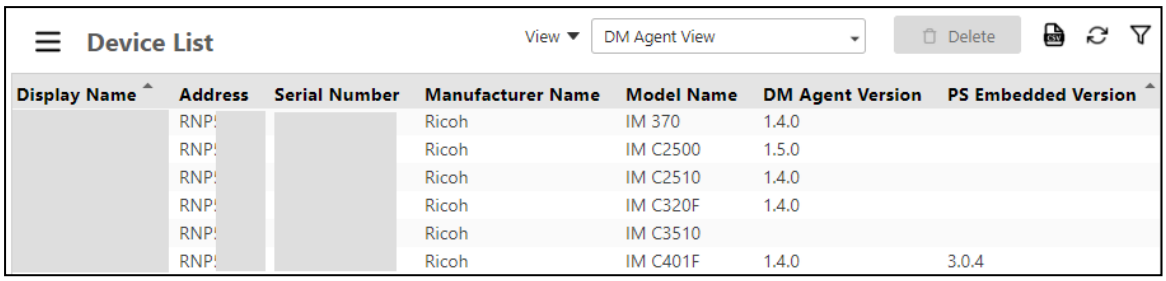
1. Load the Device List.
2. Right-click anywhere on the column header, and select **Columns** from the menu. Click **DM Agent version** and / or PS Embedded Version to check them and thereby add these columns to the current view.
3. Click away from the right-click menu to close it and view the added columns.

   You can click on the column name and drag it left or right to change the location where it appears. If you always want to view these columns immediately without scrolling, drag the columns left so you will see them immediately when this Device List view loads.

Note: Ensure you save the view. Click on the View drop-down button and select Save As. Enter a name for the view.



The columns are displayed and indicate the specific version of DM Agent and PS Embedded installed on the device. If DM Agent or PS Embedded is not applied to the device, the column is blank.



Note: These columns are not included in generated reports.

Remove Device from CloudStream DM

To remove a device from RICOH CloudStream Device Management, you must do the following.

Order	Instructions
1	**Remove device association from the following functions.** • Configuration Task on page 272. • Device Policies on page 261. • Alert Policy on page 201. **Note:** If the device belongs to one of the target groups of the functions listed above, you are not required to remove the device from the group. The device will simply be removed from the group after you delete them.
2	**Uninstall RICOH CloudStream Print&Scan embedded from device.** If a RICOH CloudStream Print&Scan embedded application is installed on the device, please run an uninstall configuration task to remove the application from the device. Steps are provided in Uninstall Print&Scan Embedded App on page 284.
3	**Revoke the device's certificate.** You can find the instructions to revoke certificate in Certificates and Service Locator URL on page 145. Go to the ***Revoke Certificate*** section for steps. If you delete the device by clicking the **[Delete]** button in the device list, the device will be added back to the list during device polling. You must revoke the device certificate so it will stop contacting the device and retrieve data.
4	**Uninstall DM Agent embedded from the device.** Go to Uninstall or Upgrade DM Agent on page 41. You can uninstall the DM Agent embedded even if steps #1, #2, #3 are not performed, however: • The RICOH CloudStream Print&Scan embedded application in the device will stop working. If you add the device again by installing the DM agent application, the RICOH CloudStream Print&Scan embedded will re-connect and establish communication to the

Order	Instructions
	cloud servers. The RICOH CloudStream Print&Scan embedded should work properly, if not, you must uninstall the embedded then install it again. • If DM Agent is uninstalled without revoking its certificate, the certificate will remain in the Certificate Management. If you add the device again by installing the DM Agent embedded, a new certificate will be issued to the device. The previous certificate will not be used. • If DM Agent embedded is removed from the device, the license assigned to the device will be added back to the Device Management available licenses.
5	**Delete the device from Device List.** Select the device from the list then Click **[Delete]** button and confirm the removal of the device from the list.

Deactivate or Reactivate a Device

If a device is using a available license that you prefer to allocate to another device, you can use the Deactivate feature to mark a device as unlicensed, without actually deleting the device from CloudStream. This feature removes the device from the Device list, and moves it to the Deactivated List. While in the inactive state, the device is not included in any category/group view counts and it does not consume a license.

Note: Deactivated devices are included in generated reports.

This option ensures that the device maintains historical data, and is available to be reactivated when necessary. Once reactivated, the device will again be automatically assigned a license, if available and will again appear in the Device List.

To deactivate a device

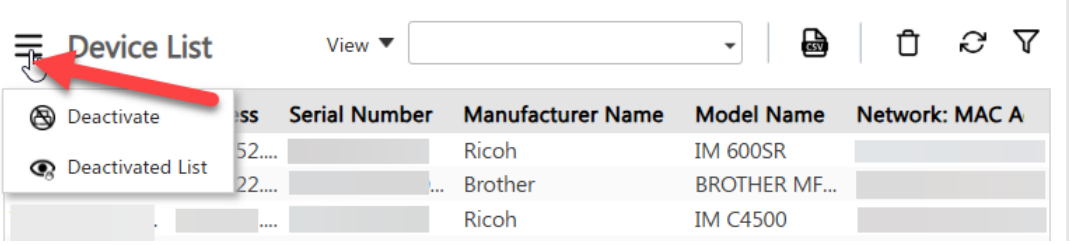
1. Select the device you want to deactivate in the Device List.
2. Click the ☰ button beside the Device List heading to view the submenu (shown below).

3. Select **Deactivate device** from the submenu.
4. In the confirmation dialog, click **Yes** to confirm that you want to deactivate the device.

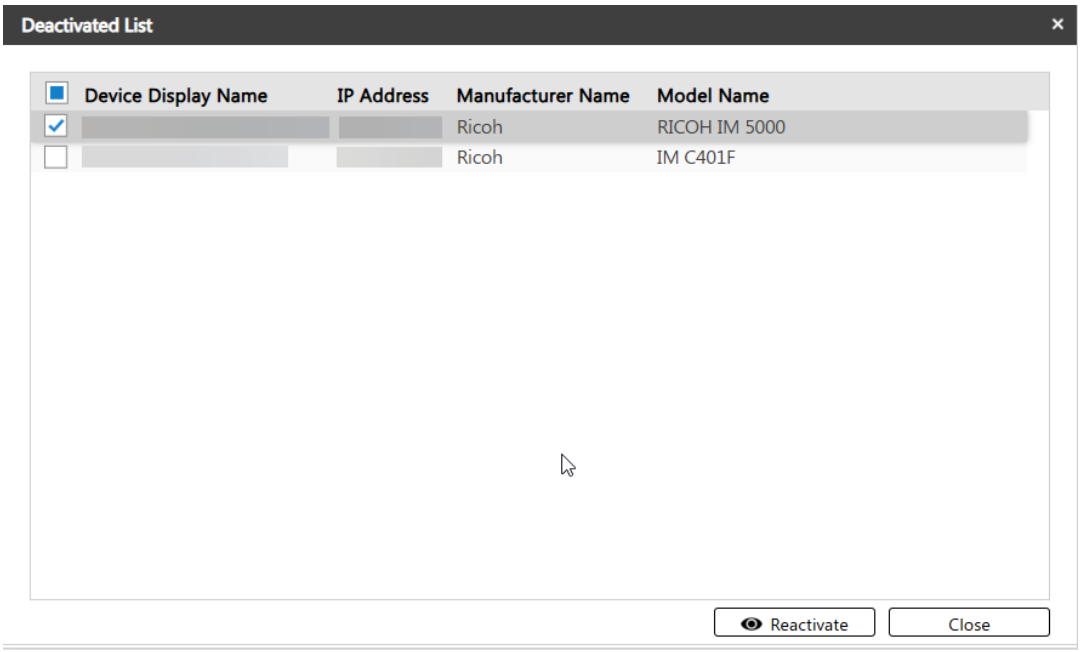
The device is removed from the Device List and can be found in the Deactivated List.

To view the deactivated list and reactivate devices

1. Click the ☰ button beside the Device List heading to view the submenu (shown below).



2. Select **Deactivated List**.
3. To reactivate a device, enable the checklist for that device, and then click Reactivate.



If there is a license available to assign to this device, the device is removed from the Deactivated list and you can now find it in the Device list. However if a license is not available to assign to the device, an error appear indicating an insufficient available license. You must either purchase a license, or remove/deactivate another device to reactivate device(s) as needed.

Device Main Properties

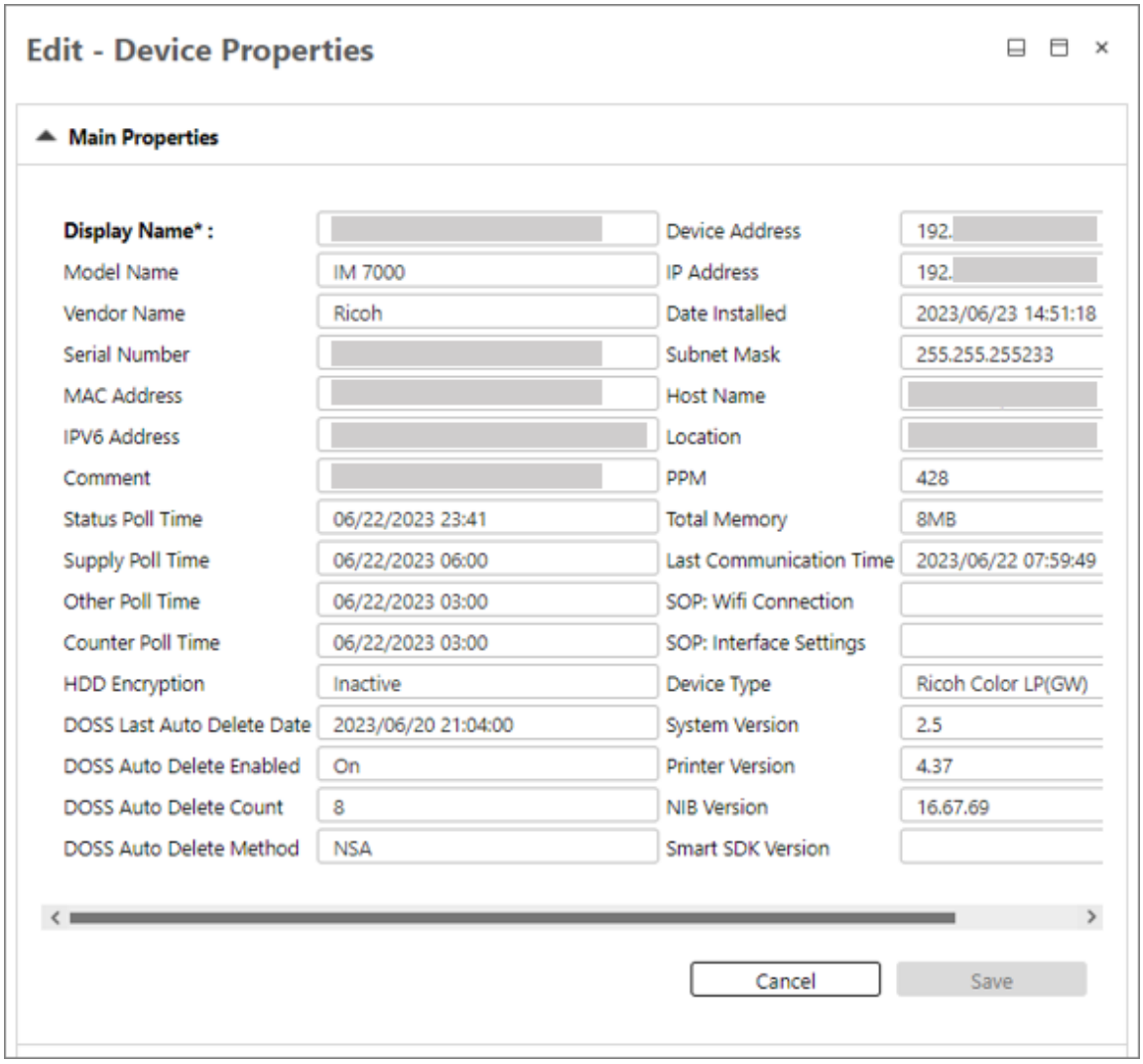
Device main properties are displayed in the table below. With the exception of the Display Name, these properties are not editable in this screen because they are read from the device only.

Note: The information is obtained via polling. If there are changes in a device's information, the data will be updated in the next polling cycle. For non-Ricoh devices, only Main Properties, Status Details, Counters, Access Profiles and History are displayed.

Device Properties	
Display Name - Displays the name of the device in CloudStream DM. You can edit the device's name in CloudStream DM. This setting does not affect the actual device's settings. Please click **[Save]** after modification. If you change the device name in this screen, you will override the default Device Name setting from Device Display Format on page 129.	Device Address - This is the address used by CloudStream DM to access the device.
Model Name	IP Address - Displays the IPv4 address of the device.
Vendor Name	Date Installed - Displays the date and time the device was registered to CloudStream DM. - This setting may display empty as CloudStream DM does not support the setting.
Serial Number	Subnet Mask
MAC Address	Host Name
IPv6 Address - Displays the IPv6 address of the device if available. - This setting may display empty as CloudStream DM does not support the setting.	Location - This setting may display empty as CloudStream DM does not support the setting.
Comment - This setting may display empty as CloudStream DM does not support the setting.	PPM - Displays the number of pages that can be printed per minute.
Status Poll Time - Displays the date and time of the last status polling.	Total Memory

Device Properties	
Supply Poll Time - Displays the date and time of the last supply polling.	Last Communication Time
Other Poll Time - Displays the date and time of the last other polling.	SOP: Wifi Connection - This setting may display empty as CloudStream DM does not support the setting.
Counter Poll Time - Displays the date and time of the last counter polling.	SOP: Interface Settings - This setting may display empty as CloudStream DM does not support the setting.
HDD Encryption - Displays if HDD encryption is active or inactive	Device Type - Displays the detailed device type description.
DOSS Last Auto Delete Date - This setting may display empty as CloudStream DM does not support the setting.	System Version
DOSS Auto Delete Enabled	Printer Version
DOSS Auto Delete Count	NIB Version
DOSS Auto Delete Method	Smart SDK Version

An example of device a main properties is displayed below:


Edit - Device Properties
Main Properties
Display Name* :
Model Name
IM 7000
Vendor Name
Ricoh
Serial Number
MAC Address
IPV6 Address
Comment
Status Poll Time
06/22/2023 23:41
Supply Poll Time
06/22/2023 06:00
Other Poll Time
06/22/2023 03:00
Counter Poll Time
06/22/2023 03:00
HDD Encryption
Inactive
DOSS Last Auto Delete Date
2023/06/20 21:04:00
DOSS Auto Delete Enabled
On
DOSS Auto Delete Count
8
DOSS Auto Delete Method
NSA
Device Address
192.
IP Address
192.
Date Installed
2023/06/23 14:51:18
Subnet Mask
255.255.255233
Host Name
Location
PPM
428
Total Memory
8MB
Last Communication Time
2023/06/22 07:59:49
SOP: Wifi Connection
SOP: Interface Settings
Device Type
Ricoh Color LP(GW)
System Version
2.5
Printer Version
4.37
NIB Version
16.67.69
Smart SDK Version
Cancel
Save

Status Details

The following status information is supplied in this screen:

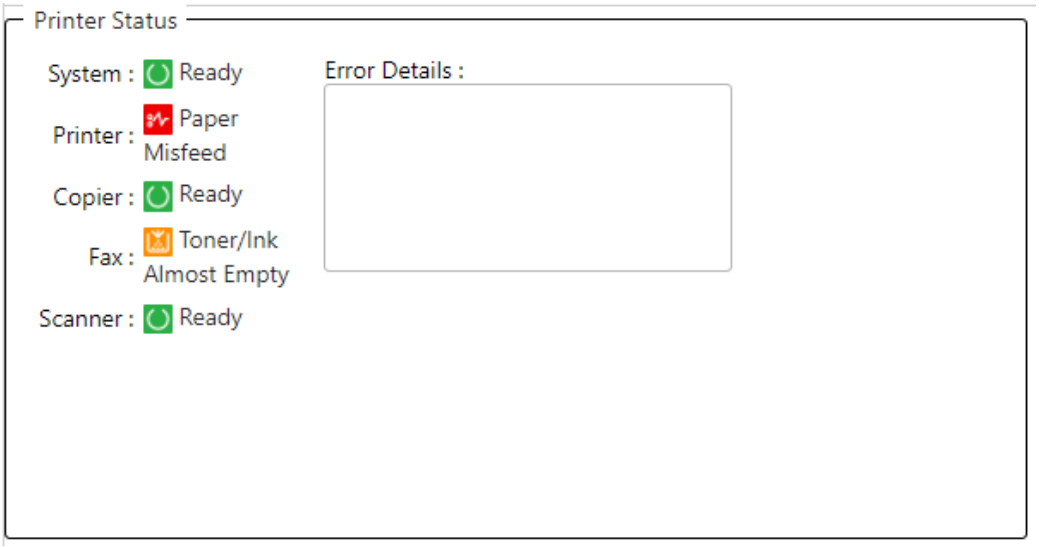
System Status on page 82. Displays the availability of the device on the network.
Printer Status on page 82. Displays the status of the printer function. When more than one status has occurred at the same time, the status with higher priority is displayed.
Toner / Ink Status on page 84. Displays the colors of the toner/inks and the remaining amount of each toner/ink.
Paper Tray Status on page 86. Displays the paper tray types and the paper orientation, size, type, and amount of remaining paper for each tray.
Output Tray Status on page 87. Displays the types of output trays and the status of each tray.
Supply Replace Count on page 88. Displays the replace counts if available for the selected device. If no replace counts are available, this status does not appear.

System Status

Displays the connectivity status of the device on the network. If the Status: System reports as "Ready", the device is connected and reachable by CloudStream. However, if the Status: System reports as "No Reply", the device is not reachable, and therefore polling information for printer, toner/ink, paper try, output try and supply replace counts will also report as "No Reply".

Printer Status

There are five printer statuses, and an example of Printer Status is displayed below.



Note: If you want to see all device status history, go to History on page 98.

Details of each status are described in the tables below.

System Status

Icon	Description
	No reply
	Service Call
	Waiting for Supply
	Out of toner/ink
	Paper jam
	Out of paper
	ADF paper jam
	Maintenance
	Fax transmission error
	Cover is open
	Other error
	Access attack detection
	Available

Printer Status

Icon	Description
	No reply
	Out of toner/ink
	Paper jam
	Out of paper
	Cover is open
	Other error
	Offline
	Warm-up
	In use
	Toner/ink low
	Paper low
	Caution
	Low energy mode-waiting
	Available

Fax Status

Icon	Description
	No reply
	Service call
	Out of toner/ink
	Paper jam
	ADF paper jam
	Out of paper
	Cover is open
	Other error
	Warming up
	In use
	Toner/ink low
	Caution

Copier Status

Icon	Description
	No reply
	Service call
	Receiving maintenance
	FAX transmission error
	ADF paper jam
	Cover is open
	Other error
	In use
	Out of toner/ink
	Paper jam
	Out of paper
	Warming up

Icon	Description
	Low energy mode-waiting
	Available

Icon	Description
	Toner/ink low
	Caution
	Low energy mode-waiting
	Available

Scanner Status

Icon	Description
	No reply
	Service call
	ADF paper jam
	Cover is open
	Other error
	In use
	Caution
	Low energy mode-waiting
	Available

Toner / Ink Status

This displays the colors of the toner/inks and the remaining amount of each. For devices that do not support the detection of the remaining amount of toner/ink and for some monochrome MFPs, this item may be displayed as "Unknown".

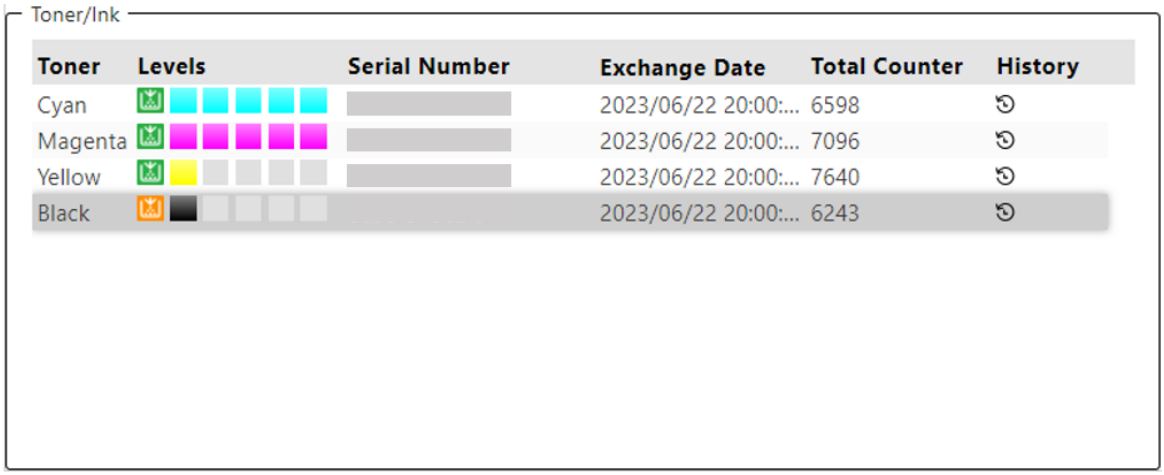
The table below shows examples of how the remaining amount of toner is represented. The color of the indicator is the same as that of the corresponding toner/ink.

Note: The total amount of toner/ink of a specific color is divided into five partitions. Each partition covers 20% of the whole toner/ink, and it is represented by a box.

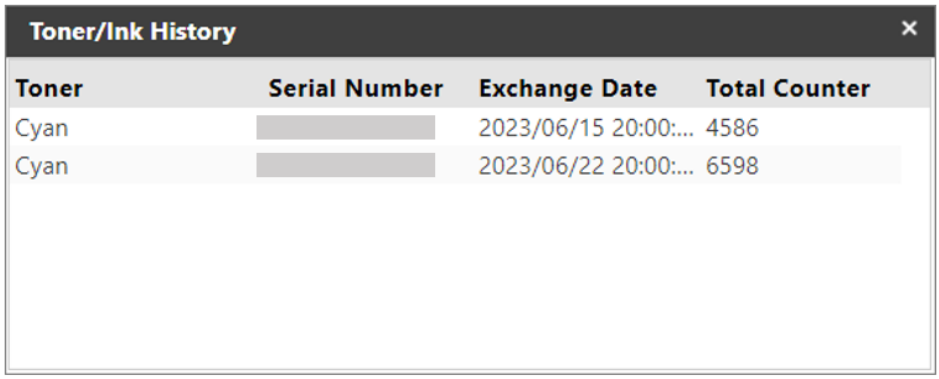
Example toner status	Explanation
	The Black (K) toner cartridge has 80 - 100%.
	The Cyan (C) toner cartridge has 60 - 80% remaining. The empty box indicates that a minimum of 20% of the cyan toner has been used.
	The Magenta (M) toner cartridge has 40 - 60% remaining.

Example toner status	Explanation
	The empty boxes indicate that a minimum of 40% of the magenta toner has been used.
	The Yellow (Y) toner cartridge has 20 - 40% remaining. The empty boxes indicate that a minimum of 60% of the yellow toner has been used.
	The Black (K) toner cartridge has 0 - 20% remaining. The empty boxes indicate that a minimum of 80% of the black toner has been used.
	Running out of toner/ink.
	Out of toner/ink.
 Unknown	Remaining toner is unknown.
 OK	The toner level cannot be obtained for the device, but it's not low or empty.

A sample screenshot of Toner/Ink status is displayed below.



As you can see in the above example, each color has a ***History*** icon  . When you click this icon, the toner history dialog will display.



The dialog displays the history of toner cartridge replacement. You can find the date and time the cartridges were replaced, including the serial number and the total number of pages printed before the cartridge was replaced.

Paper Tray Status

This displays the paper tray types and the paper orientation, size, type, and amount of paper remaining for each tray.

Each tray displays icons that indicate its current status. You can find the description of each icon in the tables below.

Paper Orientation

Icon	Description
	Paper orientation: Landscape
	Paper orientation： Portrait

Tray Status

Icon	Description
	Out of paper
	Other error

Paper Tray Status

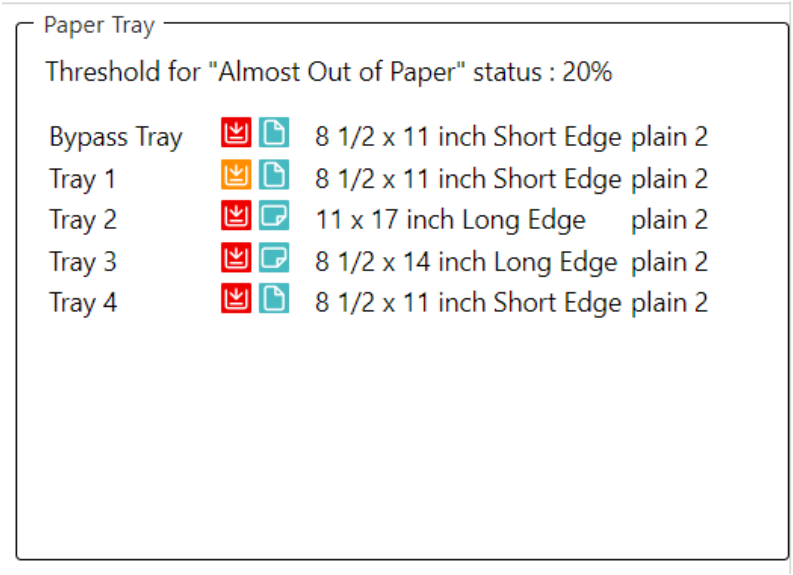
Icon	Description
	Out of paper
	Paper low Remaining paper is 0% to 20%.
	Remaining paper is 20% to 40%.
	Remaining paper is 40% to 60%.
	Remaining paper is 60% to 80%.
	Remaining paper is 80% to 100%.

Rolled Paper Tray Status

Icon	Description
	Out of Paper
	Remaining paper is 0% to 20%. ***(*)***
	Remaining paper is 20% to 40%.
	Remaining paper is 40% to 60%.
	Remaining paper is 60% to 80%.
	Remaining paper is 80% to 100%.

(*) The default value is 20%. Some devices allow the threshold to be changed. (0% < Paper amount <= Threshold)

Note: Information about the low-paper threshold value is displayed on top of the paper tray information. If the paper in the tray reaches the threshold value, the Paper Low icon is displayed.



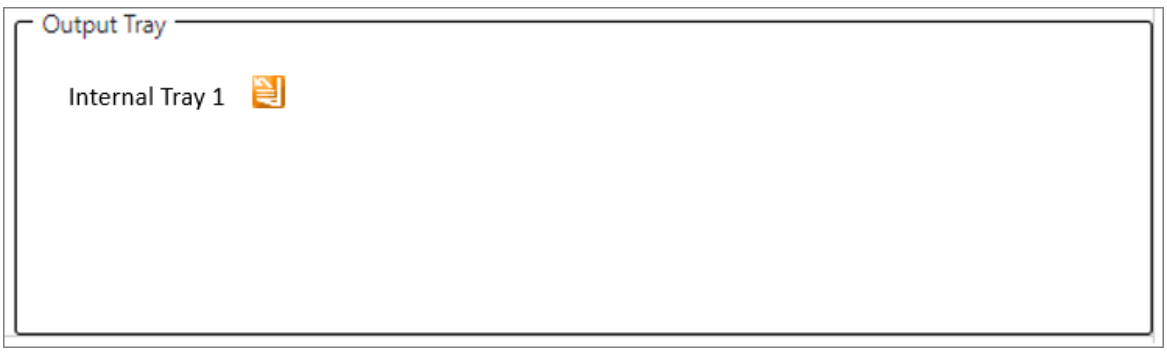
Output Tray Status

This displays the types of output trays and the status of each tray.

The status of the output tray indicated by each icon is as follows:

Icon	Description
	Catcher tray overflow. This indicates that the output paper tray is full, and the tray overflows.
	Paper in tray. This indicates that there is paper in the output tray.
	Other error.
	(Normal) Nothing is shown.

The example below shows that there is a paper in the Internal Tray.



Supply Replace Count

Important: This count applies to Brother manufactured devices only.

If available for the selected device, this section can display the supply replacement counts for the items listed below.

Note: If no counts are available for the selected device, this section does not appear.

Only counts that are available for the selected device are displayed. For example, if the device is monochrome, only the Black Toner/Ink Replace count appears; Cyan, Magenta and Yellow counts will not be listed.

- Black Toner/Ink Replace Count
- Cyan Toner/Ink Replace Count
- Magenta Toner/Ink Replace Count
- Yellow Toner/Ink Replace Count
- Drum Unit Black Replace Count
- Waste Toner Box Replace Count
- Belt Unit Replace Count

Counters

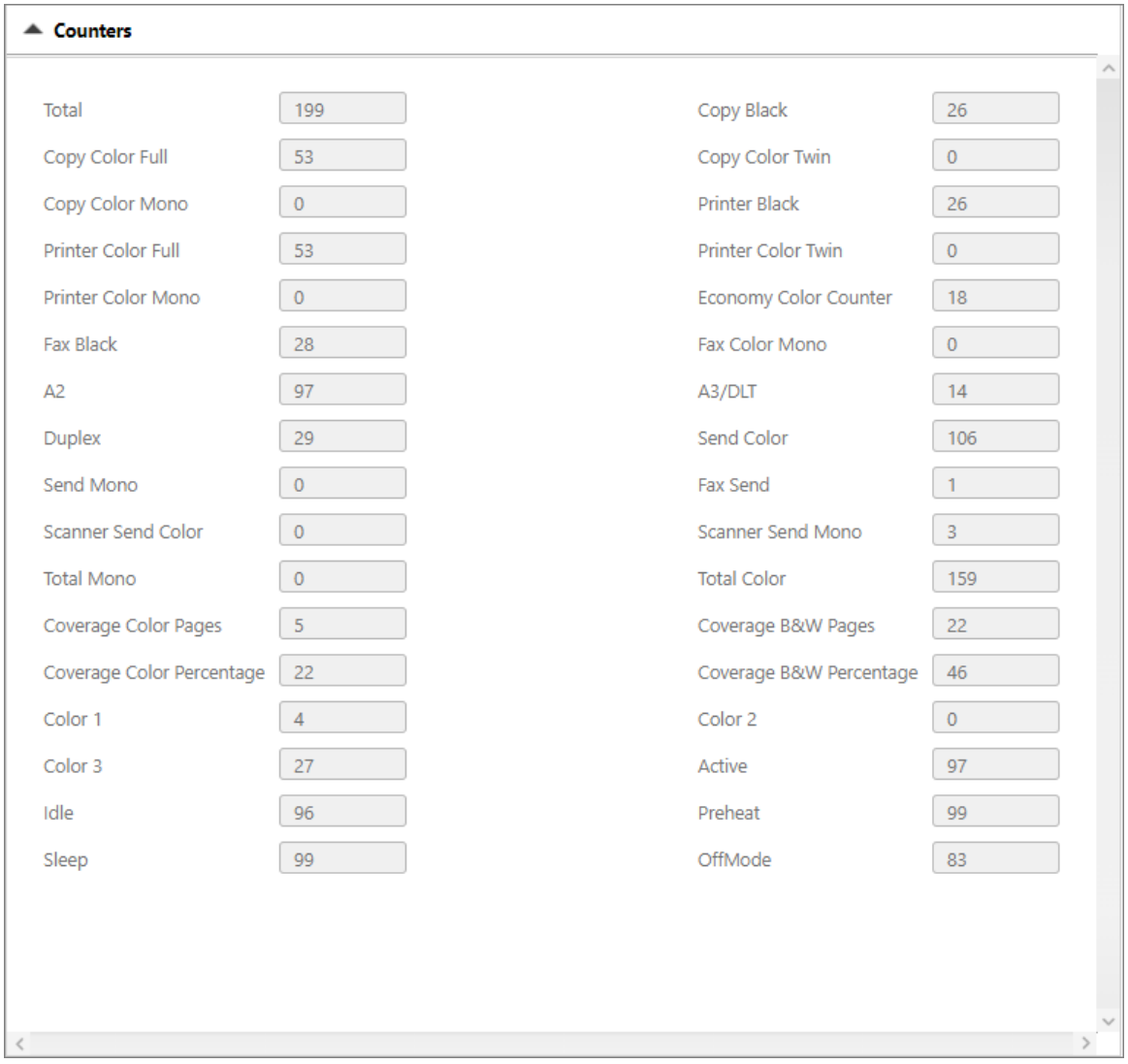
The device's main properties are displayed in the table below.

Note: The information is obtained via polling. If there are changes in a device's information, the data will be updated in the next polling cycle.

Device Counters	
Total - Indicates the total value of the counters for the copier, printer, and fax functions. The *Total* counter provides the sum of all toner usage on this device. It is a cumulative total of monochrome and color toner usage (if applicable).	Copy Black - Indicates the counter values for the copier function.
Copy Color Full	Copy Color Twin
Copy Color Mono	Printer Black
Printer Color Full	Printer Color Twin
Printer Color Mono	Economy Color Counter
Fax Black	Fax Color Mono
A2	A3/DLT
Duplex	Send Color
Send Mono	Fax Send
Scanner Send Color - Indicates the counter value for the scanner send color function.	Scanner Send Mono - Indicates the counter value for the scanner send B&W function.
Total Mono	Total Color
Coverage Color Pages - Coverage is the total toner usage (in units of 1%) per sheet of A4 page. For example, when an entire A4 sheet is filled with solid black, black toner coverage is 100%.	Coverage B&W Pages
Color 1, 2, 3 - Indicates the counter values categorized in Low, Med, and High for coverage of color pages. The unit of the counter is side(s). The default thresholds for each coverage category are as follows: Color 1 (Low): Lower than 5 % Color 2 (Mid): 5% to 20 %	Active - Indicates the counter value of the total running time of the device. The unit of the counter is minute(s).

Device Counters	
Color 3 (High): 20 % or higher	
Idle - Indicates the counter value of the total inactive time of the device. The unit of the counter is minute(s).	Pre-heat - Indicates the counter value of the time the device was in preheating mode. The unit of the counter is minute(s).
Sleep - Indicates the counter value of the time the device was in sleep mode. The unit of the counter is minute(s).	OffMode - Indicates the counter value of the time the device was in off mode. The unit of the counter is minute(s).

An example of device counters is displayed below:



Note: If you want to see all device counter history, go to History on page 98.

Activity Logs

The ***Activity Logs*** record the activities performed on the device, such as configuration tasks, device policies execution, and other operations.

Open this node if you want to know the result of an operation you executed on the device. The Activity Log Details on page 92 tables below provides detailed information about the selected activity log.

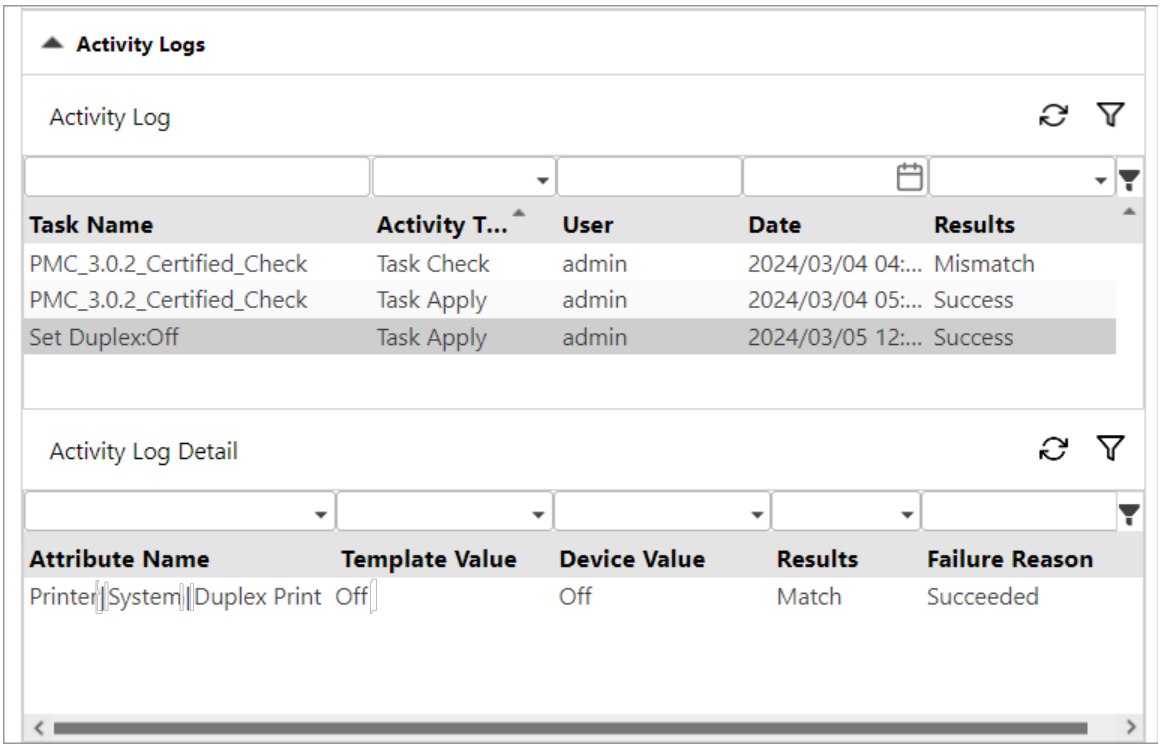
Activity Log

Columns	Description
Task Name	Displays the name of the configuration task executed. When a configuration policy, firmware policy, or an embedded policy is executed, the Task Name will be empty for that task.
Activity Type	Displays the type of activity the device performed • **Task Apply:** Shows when running an "Apply" Configuration Task. • **Task Check**: Shows when running a "Check" Configuration Task. • **Task Reboot**: Shows when running a "Reboot" Configuration Task. • **Policy Apply**: Shows when a Device Policy ran with "Apply" enforcement type. • **Policy Check**: Shows when a Device Policy ran with "Check" enforcement type
User	The user name of the administrator who initiated the activity.
Date	The Date and time the activity started.
Results	The result of the activity. • **Success**- The activity was completed successfully. • **Mismatch**- At least one attribute in the template is different from the device. This is applicable to "Task Check" and "Policy Check" activity types only. • **Partial Failure**- The activity ran but encountered a failure. Please see the ***Activity Log Details*** for information about the failure. If you run a configuration task with firmware that is not compatible with the target device, you will get a "Partial Failure" result. Please use a compatible firmware.

Columns	Description
	• **Processing**- The activity is still running; please wait.

When an activity is clicked from the ***Activity Log*** table, the detail of the activity is displayed in the ***Activity Log Details.***

An example of an activity log and details is displayed below.



Activity Log Details

When you click an activity log, the log details of that activity is displayed in the Activity Log Details table. The table has the following columns.

Columns	Description
Attribute Name	The name of the setting applied to or checked on the device. For example, an attribute name is displayed as "Printer|System|Duplex Print" when applying an SDP template with Duplex Print: Off as a setting. The *Printer* is the category, the *System* is the sub-category, and the *Duplex Print* is the setting. The same way the attributes are displayed when running an XDP template.
Template Value	The value that is configured in the template. In the example above, the value is "Off".
Device Value	The value retrieved from the device. If the device's Duplex Print value is set to "Off", then value is "Off".

Columns	Description
Results	The result of the activity for the attribute. If the type is "Task Apply" or "Policy Apply", the following will happen. 1. The template value will be compared to the device value. 2. If the value matches, it will return "Match" and no action will be taken. 3. If the value does not match, it will apply the template value to the device. 4. If the application succeeds, it will return a success; otherwise, failure. The following are the possible results. • **Success** - The template value is applied successfully to the device. • **Failure** ◦ Indicates that the task fails to apply the template value to the device. The details are displayed in the ***Failure Reason*** column. ◦ When the activity type is "Task Reboot", it would return fail if it failed to restart the device. ◦ Regardless of the activity type, if the connection to the device fails, it will return a failed result. • **Match** - The template value matches the device value, so nothing is applied. • **Not Match** - The template value did not match the device value. This kind of result is only displayed if the activity type is "Task Check" and "Policy Check". • **Skip** - The attribute is not found in the device. For example, if the device does not have FAX, applying a fax attribute to it will return 'Skip'.
Failure Reason	The details of the error. Examples: • Bad Data - Invalid request data. • Access Denied - No client certificate information.

Optional Properties

This node displays the two optional device properties; Custom Properties on page 94 and Installed Applications on page 95.

Custom Properties

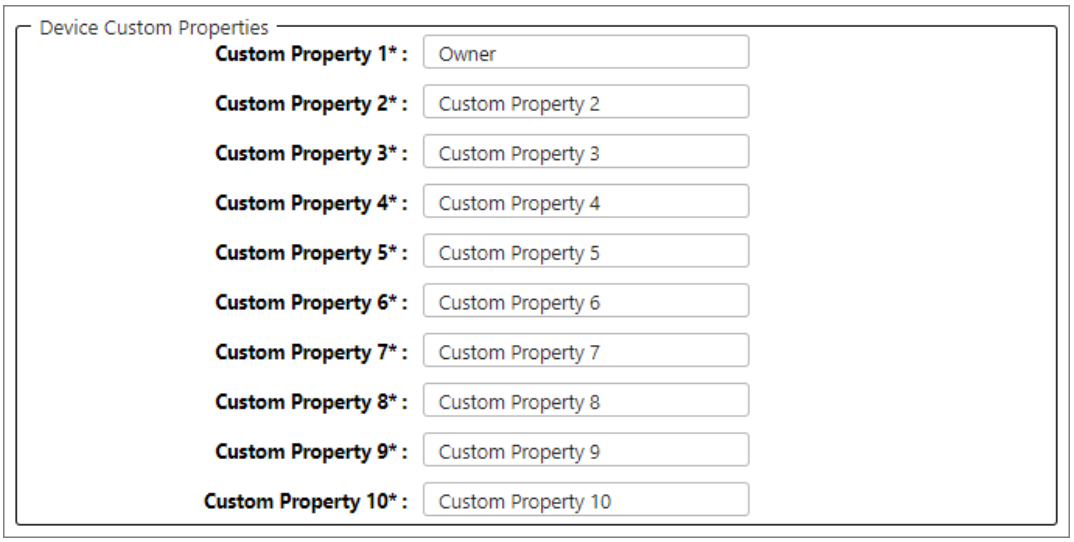
A custom property helps you and other admins add customized information to the device as an optional property.

For example, if you want to add information about the device's owner as a property, you can set the property to "Owner", then input the name of the owner of the device.

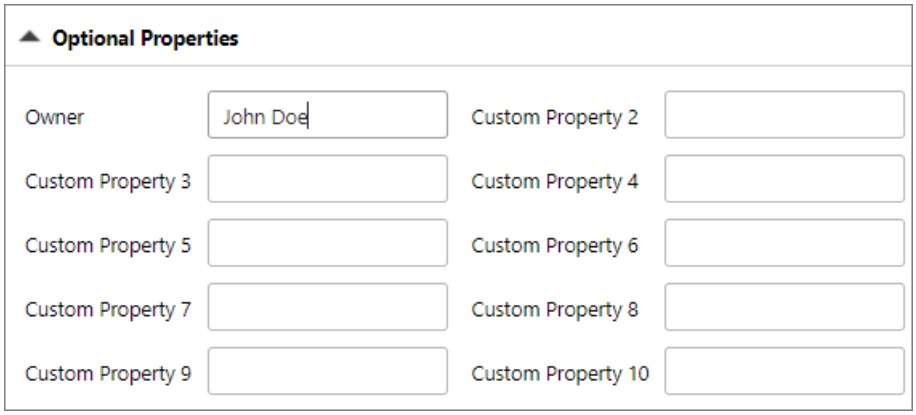
To do so, please follow the steps below.

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.
4. In the ***Device Custom Properties***, select a custom property and overwrite the name of your preference.

   In this example, the Custom Property 1 value is "Owner".



5. Click **[Save]**. (Scroll down to see the save button)
6. Logout from CloudStream DM, then login again.
7. Go to ***Device List.***
8. Select the device you want to edit.
9. Open ***Optional Properties*** and you will see the property displayed as "Owner".

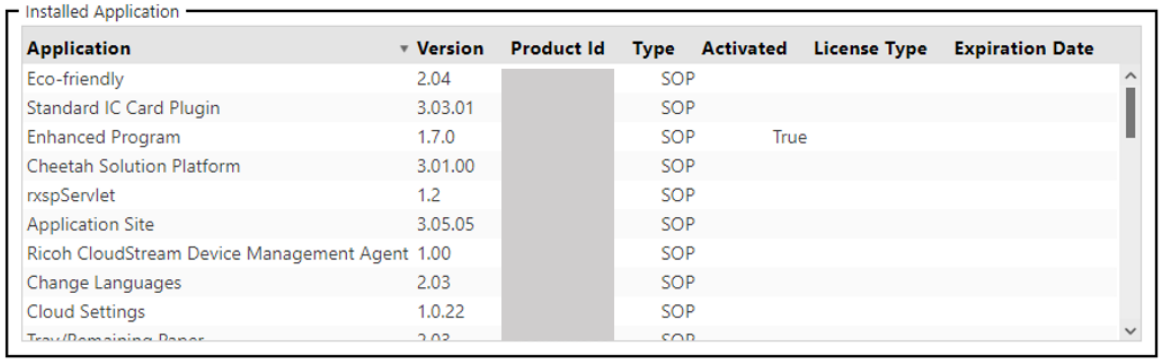


10. Enter a value for the "Owner" property.
11. Click **[Save].**

Note: More display information can be found in Display Settings on page 127.

Installed Applications

Displays the list of applications that are installed on the device.



The table has the following columns.

Column Header	Description
Application	The Application Name. The application installed to the device is displayed here. The RICOH CloudStream Device Management DM Agent is also displayed here.
Version	The application's version number.
Product ID	The product ID of the application.
Type	This item displays the type of application. The value can be one of the following: • **SOP**: A native application.

Column Header	Description
	• **J**: A legacy application. • **SOP&J**: A hybrid application.
Activated	This item displays whether an application is activated. • **True**: Indicates that the application is active. • **Blank**: It indicates that the application is either: ◦ not activated ◦ does not need to be activated ◦ the value for this item is not retrieved.
License Type	This item displays the application license type. • **Trial**: A license type is a trial license. • **Blank**: A license type is others, or a license type is not retrieved.
Expiration Date	This item displays the application's expiration date. If there is no expiration date, a blank is displayed.

Access Profiles

This node displays the device's profile for each access account. Access accounts are used by RICOH CloudStream Device Management to communicate to devices via DM Agent.

Note: The Access Profile node displays the profiles used by the DM Agent as read-only. You cannot manually change the profile for each access account.

Here is the list of access accounts:

- Device Administrator - To create a profile for this account, go to Device Administrator Access Profile on page 288.
- SNMP - Uses SNMPv1/2 and SNMP v3. To create a profile for this account, go to SNMP Access Profile on page 290.
- SDK/J Platform - To create a profile for this account, go to SDK/J Platform Access Profile on page 289.

The Device Management (DM) Agent installed on the MFP identifies the correct profile created in ***Access Profiles*** in the ***Device Configuration*** section. The DM Agent uses the profile to perform polling, configurations, and other operations.

Note: In case the access account value is modified, the DM Agent will look for another profile that matches the device settings and update the Profiles in the Access Profile node. If there is no profile that matches the device's settings, then the device becomes disconnected.

History

This node shows the Counters History on page 98 and Status History on page 98 of the device.

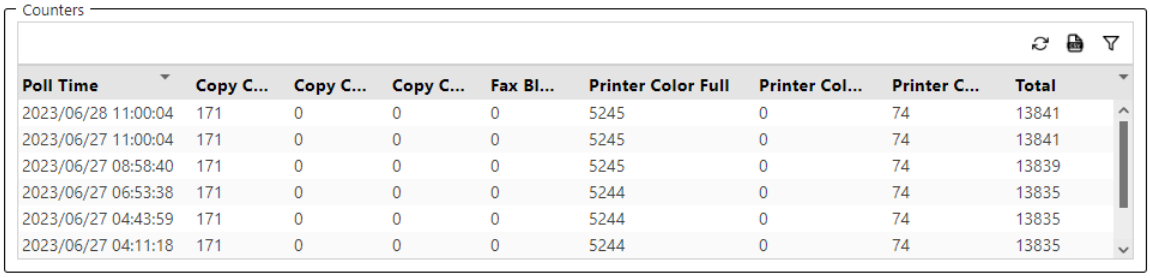
Counters History

The ***Counters*** history table displays the counters retrieved from the device at each polling time.

You can find the following columns in the table.

Column Headers
Poll Time - The date and time the counters were polled from the device.
Copy Full Color
Copy Color Mono
Copy Color Twin
Fax Black
Printer Color Full
Printer Color Mono
Printer Color Twin
Total - Indicates the total value of the counters for the copier, printer, and fax functions.

An example of the ***Counters*** history is displayed below.



Poll Time	Copy C...	Copy C...	Copy C...	Fax Bl...	Printer Color Full	Printer Col...	Printer C...	Total
2023/06/28 11:00:04	171	0	0	0	5245	0	74	13841
2023/06/27 11:00:04	171	0	0	0	5245	0	74	13841
2023/06/27 08:58:40	171	0	0	0	5245	0	74	13839
2023/06/27 06:53:38	171	0	0	0	5244	0	74	13835
2023/06/27 04:43:59	171	0	0	0	5244	0	74	13835
2023/06/27 04:11:18	171	0	0	0	5244	0	74	13835

The above example shows that a page is printed in full color at 2023/06/27 8:58:40, making the ***Printer Color Full*** counter increase by 1.

Note: On the top-right corner, you can find the export to CSV icon. Clicking this icon will export the contents of the table to a CSV file.

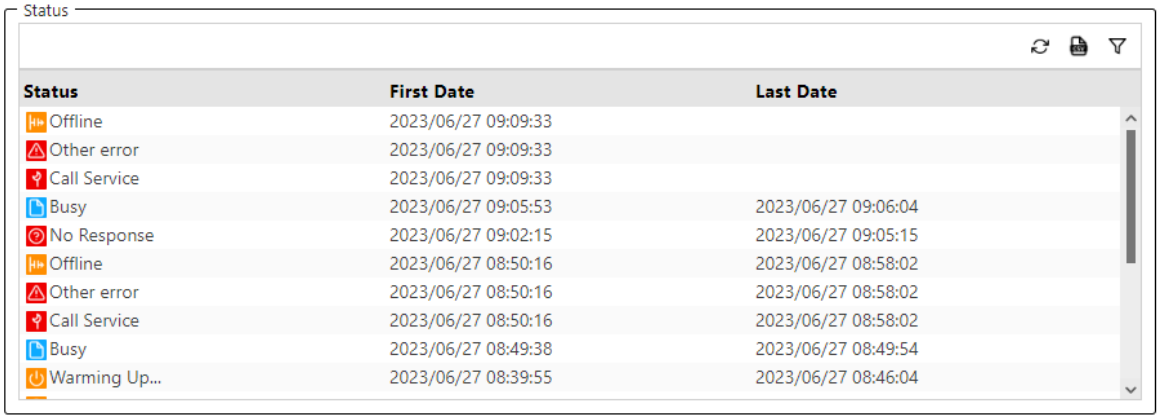
Status History

The ***Status*** history table displays the states the device has gone through. One entry is shown for each state.

You can find the following columns in the ***Status*** history table.

Column Headers
Status - Displays the state of the device on a specific date and time. An icon with a description is displayed. To know more about different device statuses, go to Status Details on page 82.
First Date - Displays the date and time the device entered a state described in the ***Status*** column.
Last Date - Displays the date and time the status ended. The Last Date is displayed when the device enters a different state. If the Last Date is Null or empty, this indicates that the status is still active.

An example of the Status history is displayed below.



Note: On the top-right corner, you can find the CSV export to CSV icon. Clicking this icon will export the contents of the table to a CSV file.

@Remote

This node shows the @Remote properties of the device, if the device is registered with an @Remote appliance. This information is supplied by the @Remote Center and is read-only.

You can find the following fields in the table.

Field
Machine ID
Cutoff Date
Service Depot Phone No
Supply Order Phone No
Connection Type
Service Depot
Supply Order From
Encryption Length

Work from Home (WfH) Devices

The Work from Home (WfH) feature allows users working from home to add their network and USB-connected printers to RICOH CloudStream Device Management (DM) by installing the WfH Client to the user's home PC. The WfH Client detects the devices connected to the home network, then pushes the information to CloudStream DM.

You can find the following topics below.

WfH Device Supported Functions

The list below shows the information and functions supported by WfH devices.

CloudStream DM Features	Support
Device Information	Display the following information. • **Properties**: Manufacturer, Model, Serial Number, Mac Address, Location, Installed Memory • **Status Details**: System Status, Printer Status, Toner Status • **Device Counters**: Total, Printer Black, Printer Color Full, Fax Black, Fax Color, Copy Black, Copy Color Full, Fax Send, Duplex, A3/DLT, Total Color, Total Mono, Scanner Send Mono, Scanner Send Color More information is described in WfH Device Properties on page 105. **Note:** Other device information not mentioned above is **not** retrieved, and no value is displayed.
Device List	Grouped in ***WfH*** group by Hostname and ***NA*** by IP Address category. More information is described in View WfH Device Groups on page 104. **Note:** WfH devices **cannot** be added to other groups or categories.

CloudStream DM Features	Support
Reports	WfH devices are included in the reports. Please see Reports on page 332. **Note:** If a user is not registered to User Management and prints documents to a WfH device, the printing transaction of the device will still be recorded but will not be associated to a user account, instead, it will be associated with an "unknown" user in the reports.
Device Configuration	WfH devices do **not** support device configuration.
Device Policies	WfH devices do **not** support device policies.
Alert Policies	You can create an alert policy using WfH devices. Please see Alert Policy on page 201.

WfH Device States

As an administrator, you can accept or ignore the user's WfH devices by changing their status. Here is a list of WfH device statuses.

State	Description
Accepted	Devices in this state are tracked by CloudStream DM. With this state, the WfH device properties, status, and counters are retrieved at the WfH device polling interval.
Pending	Devices in the Pending state are not tracked. The device information and print jobs are not retrieved.
Ignored	Usually, users send information about their user-owned devices, which are connected to their home network where the WfH Client service is running. Ideally, user-owned devices are not tracked, so you can set the device state to "Ignored". When the device is set to the Ignored state, it will be displayed in the hidden devices of the WfH devices node.

Set up WfH Client and Add WfH Devices

Set up and monitor WfH Clients and devices by following the order of instructions below.

Order	Instructions
1	Set Work from Home Polling on page 103.
2	Work from Home (WfH) Client on page 111. Instructions for WfH users to install the WfH Client to their home PC.
3	View WfH Device Groups on page 104 and WfH Device Properties on page 105.

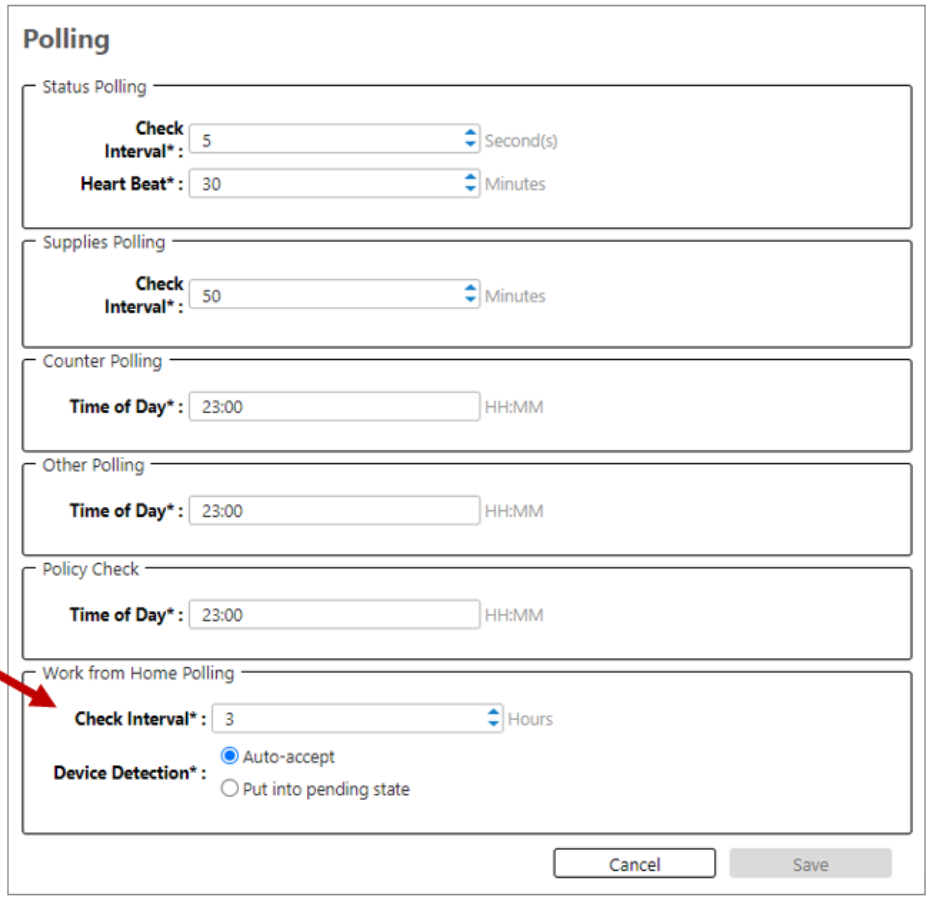
Order	Instructions
4	Change WfH Device State on page 108.

Important: If you do not have enough Device Management licenses, your WfH devices will not be added. Please acquire additional licenses, then activate them in License Management on page 121.

Set Work from Home Polling

The initial WfH device state depends on the value of WfH ***Device Detection.*** To change the initial device state, do the following:

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Click ***Polling***



4. In ***Work from Home Polling***, set the **Device Detection** value.

- **Auto-accept:** If selected, all new devices reported by a WfH Client will be automatically added as a tracked device and be in “Accepted” state. This is the default mode.
- **Put into pending state:** When this mode is selected, all new devices will be put into “Pending” state and will not be tracked. You have to manually accept the devices in the *Work from Home* node in the ***Device Properties***.

5. Set the ***Check Interval.*** This is the WfH device information polling interval. WfH device information is gathered every interval and posted in CloudStream DM.

   The field accepts values in hours, from 1 to 24. The default value is 3 hours.

6. Click **[Save].**

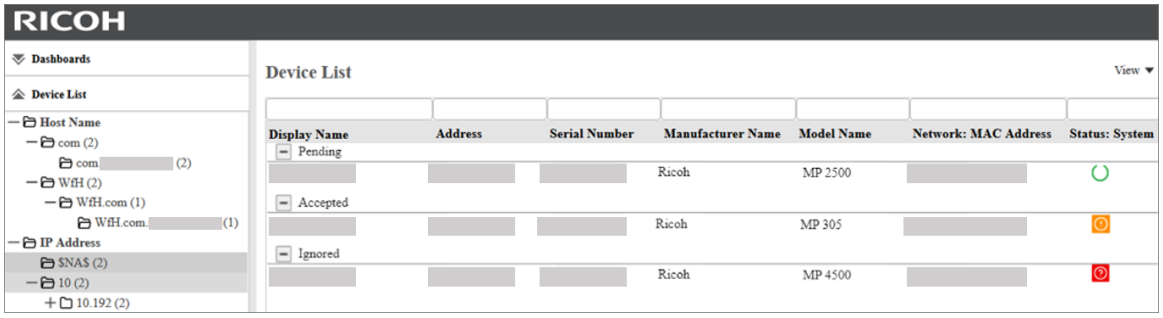
Newly detected WfH devices will have the status you set in ***Device Detection***. If you want to stop tracking a device, change its state to "Ignore".

View WfH Device Groups

WfH devices are displayed in the ***Device List*** under the ***Host Name*** category. A ***WfH*** group is added by default and shows all WfH devices. You can also find WfH devices in the ***IP Address*** category under the ***NA*** group. Click the device from the list to view the WfH Device Properties on page 105.

Note: If the *WfH* and *NA* groups are not displayed, this implies that no WfH device has been discovered. Please check the configuration in the WfH Client or the device’s address and port.

When you open the ***WfH*** or ***NA*** group, the devices are grouped based on their state, as you can see in the image below.



The device’s IP Address will not be displayed, so the ***Device Display Name*** and ***Address*** will be different for WfH devices.

- ***Device Display Name*** will be the WfH Client machine’s “`<Hostname>.<DomainName>`”.

For example, the user installs the WfH Client to their laptop with hostname "COMP12345" and is connected to a domain "CompanyDomain".

The resulting Display Name is "COMP12345.CompanyDomain".

- ***Address*** will become "`<Hostname>.<DomainName>.WfH`"

To change the state of the device, please go to Change WfH Device State on page 108.

Important: The *WfH* or *NA* group may appear when you create a task or any operations that allows you to select a device or group. However, WfH devices will not display for selection. Please refer to Work from Home (WfH) Devices on page 101 for the list of functions you can carry out on WfH devices.

WfH Device Properties

A WfH device will display less device information compared to a DM Agent-managed device.

There are four nodes displayed for a WfH device.

Main Properties on page 105.
Status Details on page 106.
Counters on page 107.
Work from Home on page 108.

Note: The WfH device information is obtained via polling. If there are changes in the device's information, the data will be displayed in the next polling cycle.

Important: Information retrieved from *USB-connected WfH devices* is limited to the following only:

- **Properties**: Manufacturer, Model, Serial Number, Installed Memory, Comment
- **Status Details**: System Status, Printer Status
- **Counters**: Total, Printer Black, Printer Color Full

Main Properties

The table below lists the device information retrieved from a WfH device.

WfH Device Properties	
Display Name	Device Address

WfH Device Properties	
Model Name*	Vendor Name
Serial Number*	MAC Address
Location	Installed Memory*
Comment*	Manufacturer*

Note: The ***Display Name*** is the WfH Client machine's "<Hostname>.<DomainName>", while the ***Address*** is WfH Client machine's "<Hostname>.<DomainName>.WfH".

The USB-connected Work from Home devices only display the properties with an asterisk (*).

Status Details

Displays the Printer Status and the Toner Level Status only.

For ***Printer Status***, System and Printer information are the only status shown. When more than one status has occurred at the same time, the status with higher priority is displayed.

System

Icon	Description
	No reply
	Service Call
	Waiting for Supply
	Out of toner/ink
	Paper jam
	Out of paper
	ADF paper jam
	Maintenance
	Fax transmission error
	Cover is open
	Other error
	Access attack detection
	Available

Printer

Icon	Description
	No reply
	Out of toner/ink
	Paper jam
	Out of paper
	Cover is open
	Other error
	Offline
	Warm-up
	In use
	Toner/ink low
	Paper low
	Caution
	Low energy mode-waiting
	Available

For ***Toner Level Status***, a list of examples below shows how the remaining toner levels are represented in the Status Details node.

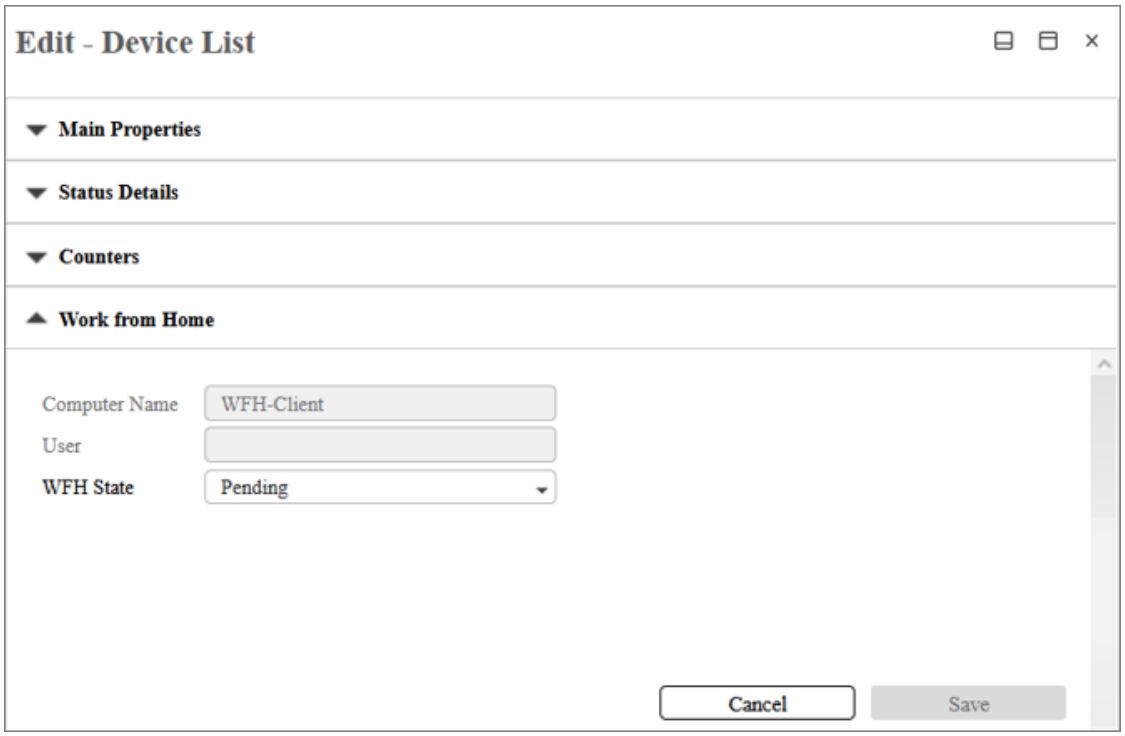
Example toner status	Explanation
	The Black (K) toner cartridge has 80 - 100%.
	The Cyan (C) toner cartridge has 60 - 80% remaining. The empty box indicates that a minimum of 20% of the cyan toner has been used.
	The Magenta (M) toner cartridge has 40 - 60% remaining. The empty boxes indicate that a minimum of 40% of the magenta toner has been used.
	The Yellow (Y) toner cartridge has 20 - 40% remaining. The empty boxes indicate that a minimum of 60% of the yellow toner has been used.
	The Black (K) toner cartridge has 0 - 20% remaining. The empty boxes indicate that a minimum of 80% of the black toner has been used.
	Running out of toner/ink.
	Out of toner/ink.
 Unknown	Remaining toner is unknown.
 OK	The toner level cannot be obtained for the device, but it's not low or empty.

Counters

The table below lists the counters retrieved from a WfH device.

Device Counters	
Total - Indicates the total value of the counters for the copier, printer, and fax functions. The ***Total*** counter provides the sum of all toner usage on this device and is a cumulative total of monochrome and color toner usage (if applicable).	Printer Black - Indicates the counter values for the printer function.
Printer Color Full	Fax Black
Fax Color	Copy Black
Copy Color Full	Fax Send
Duplex	A3/DLT
Total Color	Total Mono
Scanner Send Color - Indicates the counter value for the scanner send color function.	Scanner Send Mono - Indicates the counter value for the scanner send B&W function.

Work from Home



Information about ***Work from Home*** node is described below.

Item	Description
Computer Name	Displays the name of the computer where the WfH Client service is running. The name is read-only.
User	Displays the user name of the user associated with the device. The user name is read-only.
WfH State	Allows you to view and set the state of the device. To know more about the WfH device state, go to Change WfH Device State on page 108.

Change WfH Device State

1. Login as an administrator.
2. From the ***Device List*** section, expand ***Host Name*** or ***IP Address.***
3. Click the ***WfH*** group in ***Hostname*** category, or the ***NA*** in ***IP Address*** category.
4. All WfH devices are displayed in the list. Locate the device you want to edit.

> **Note:** Non-Ricoh devices that are connected to the WfH Client are also detected by CloudStream DM. However, CloudStream DM does not support non-Ricoh devices; please change the status of these devices to "Ignored".

5. In the ***Device Properties***, expand the ***Work from Home*** node.
6. Change the value of ***WfH State***. Options are Accepted, Pending, and Ignored.
7. Click **[Save].**

Note: For corporate devices, please change their state to “Accepted”, so the device information will be reflected in Device Properties. If the device is a personal device that should not be managed by the system, set it as "Ignored".

The table below shows the result of changing the WfH device state:

State Transitions	Result
From: Pending or Ignored **To:** Accepted	• The WfH device will be tracked. • The device information will be posted in the device properties. • The properties of new devices will remain empty until the next device polling interval. • If the device was previously accepted, the previous data will be displayed in the device properties. Please wait for the next device polling interval to retrieve the latest information from WfH device. • Generating device reports will include WfH devices with “Accepted” state. • If an ignored device is accepted, the device is moved to the ***Accepted*** group in the device list grid.
From: Accepted or Ignored **To:** Pending	• The WfH device will not be tracked, and the device information will not be collected during device polling. • Information in device properties will not be updated. • Device printing information will not be collected. • The device will not be included when generating reports. • If an ignored device is set to pending, the device is moved to the ***Pending*** group in the device list grid.
From: Pending or Accepted **To:** Ignored	• The WfH device will not be tracked, and the device information will not be collected during device polling. • The device will not be included when generating reports. • Ignored devices are displayed in the ***Ignored*** group.

Generate a WfH Device Report

Follow the instructions below to generate a report consisting of Work from Home (WfH) devices.

Prerequisites
WfH devices are detected and the status is "Accepted".
You have the role with privileges to generate reports.

1. Login as an administrator with reports privileges.
2. Go to the ***Reports*** section.
3. Expand ***Report Templates***, then select ***Device Reports.***
4. From the list of report templates, select the ***Device List*** template.
5. Generate the report.

   You can generate a report now or schedule a report task to generate a report.

   - If you want to generate a report now, click  [Run Immediately]. For detailed steps, refer to Run a Report Immediately on page 334.
   - If you want to schedule a report to be generated at a specified time, click  [Run On Schedule]. For detailed steps, refer to Run a Report on Schedule on page 350.
6. If you decide to run immediately or schedule a report, you will see the ***Parameters*** section. Go to Report Target and select the WfH group as the Device Group.
7. Proceed to create the report or schedule the report.

The Device List report will contain the WfH devices and their information.

Refer to Reports on page 332 for more details.

Work from Home (WfH) Client

Ricoh devices connected to your home network can be monitored by the RICOH CloudStream Device Management (DM) with the aid of Work from Home (WfH) Clients.

Install the WfH Client to your home PC, then add the devices in your Window's Printers & Scanners. You can add network and USB-connected devices to your home PC where your WfH Client service is running.

When WfH devices are detected by the CloudStream DM, your Administrator will assign a status to your devices.

Status	Description
Accepted	When your device is marked as 'Accepted', it is tracked by CloudStream DM. With this state, your Administrator has access to the device information such as device properties, status, and counters.
Pending	Devices in the 'Pending' state are not tracked; therefore, CloudStream DM does not retrieve the device information and print jobs.
Ignored	Your Administrator will set your personally owned printers as 'Ignored', so they will not be tracked and monitored by CloudStream DM. After you configure the WfH Client, please remember to inform your Administrator of the list of your personal printers so they can be set as 'Ignored'.

Before you start the installation, please take note of the following prerequisites.

Prerequisites
WfH users' operating systems must be Windows 10 and above.
Must have an available Device Management license to add WfH devices to CloudStream DM. If there are no available licenses, please purchase additional licenses and activate them in License Management on page 121.
Download the WfH Client installer in Systems section. 1. Go to ***Systems.*** 2. Click ***Software Download.*** 3. Select ***Work from Home Client***. The download will start immediately. If you do not have access to CloudStream DM, request the installer from your IT Administrator.
Gather the following information. • WfH Client Onboarding code. See Generate Onboarding Codes on page 148.

Prerequisites
• Service Locator Address and Server port. You can copy your service locator in Certificates and Service Locator URL on page 145. • If you will use a proxy server, gather the proxy server information.
Your account is registered with CloudStream DM User Management. You can register the following account types. • LDAP account - If there is an MFP with RICOH CloudStream Print&Scan embedded installed, you can register your account by logging in to the device. Follow the steps in Register an LDAP User on page 315 to register. • OpenID Connect (OIDC) account - Follow the steps in Register an OIDC User on page 313 to register. If you are not registered to User Management and prints documents to a WfH device, the printing transaction of the device will still be recorded but will not be associated to a user, instead, it will be associated to an "unknown" user in the reports. Ensure to login using your registered account to the home PC where the WfH Client service is running.

Note: The WfH Client onboarding code is time sensitive. Please make sure to use the code within the validity period. If the code expires, please generate it again.

To install WfH Client follow the steps below:

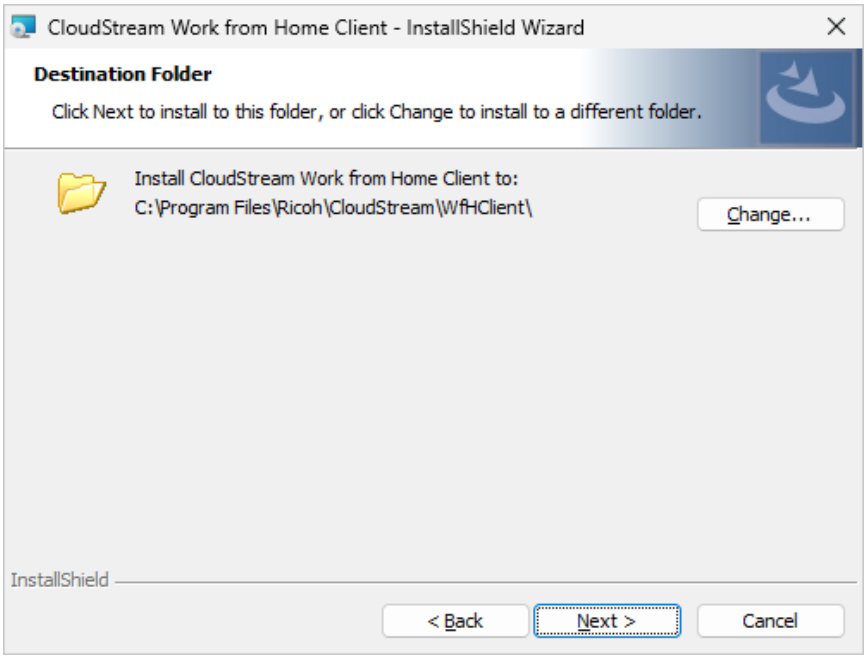
Order	Instructions
1	Install Work from Home Client on page 112.
2	Add Devices to WfH Client Computer on page 117.

Note: Please refer to Work from Home (WfH) Devices on page 101 for the list of features a WfH device supports.

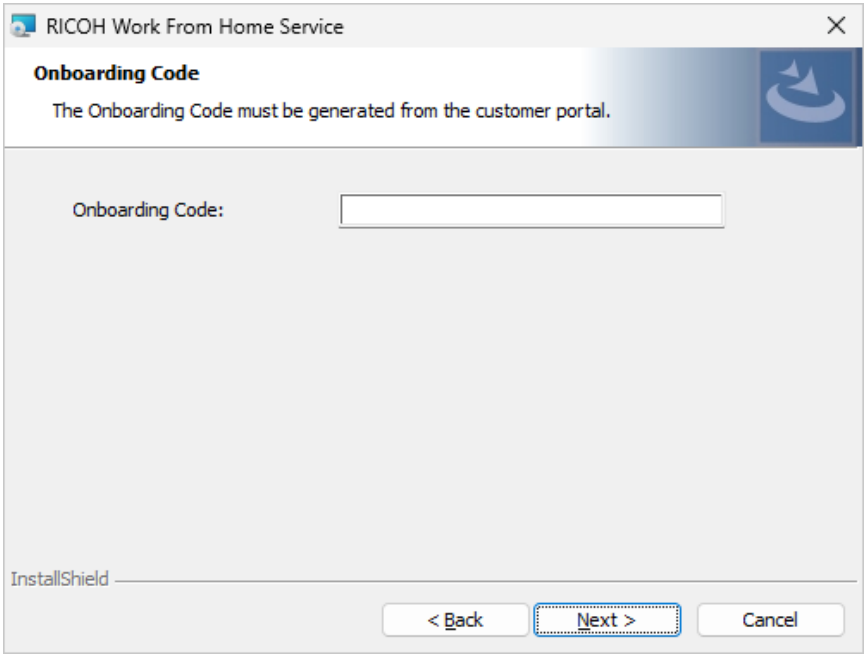
Install Work from Home Client

1. Login to your home PC using the user account registered to CloudStream DM.
2. Run the installer ***WfHClientSetup.exe.*** Please make sure you have administrator rights to install the application on your client machine.
3. In the installation wizard, read the information, then click **[Next].**

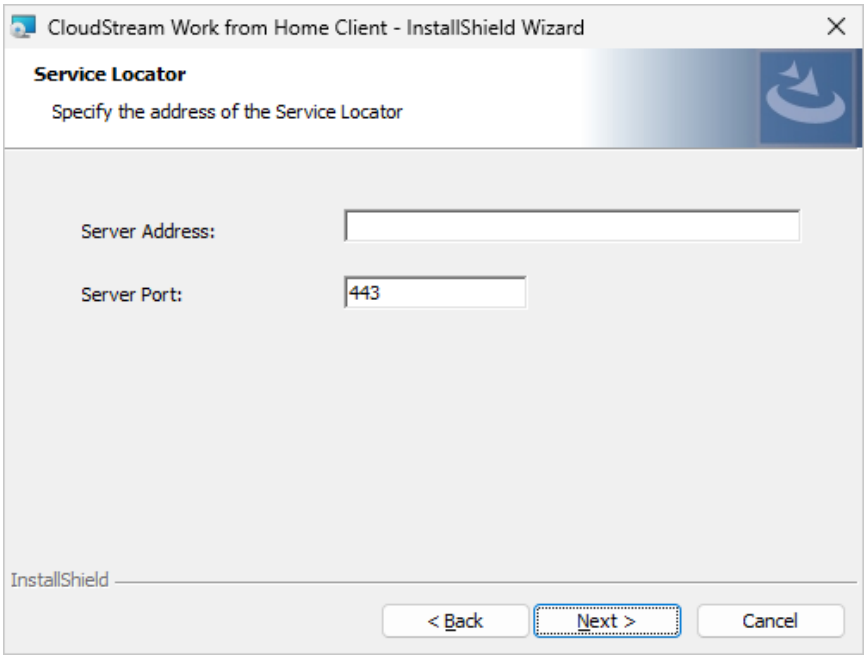
4. Read the Software License Agreement and agree to the license agreement, then click **[Next].**
5. (Optional) Select the destination folder location. By default, a location is already specified; you can modify the path by clicking the **[Change…]** button. Once a folder is selected, click **[Next].**



6. In this screen, input the WfH Client onboarding code and click **[Next].**



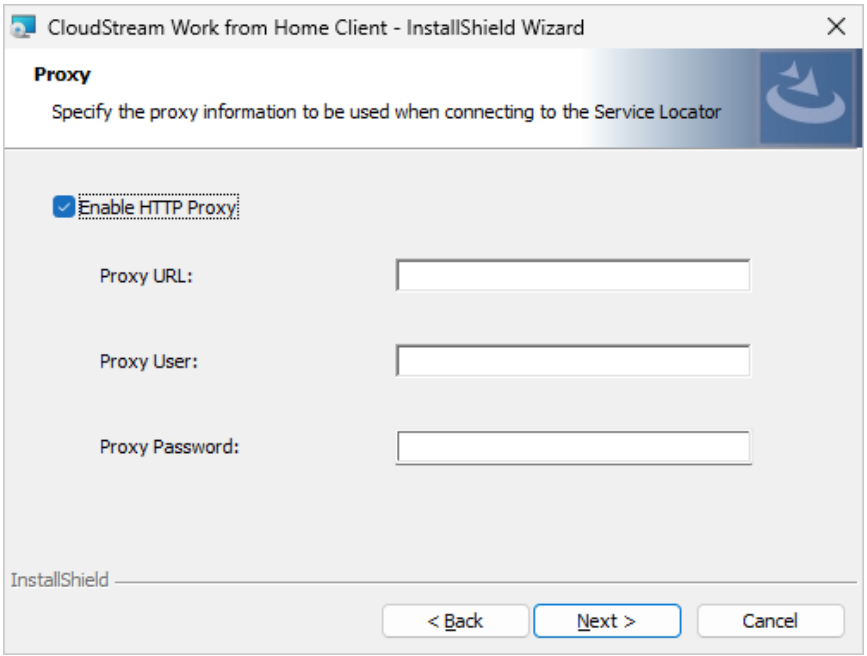
7. Enter the Service Locator address and the Server Port. The default port is 443.



Note: The service locator address is given after purchasing the application. If you have the Service locator URL, remove the protocol and the port, leaving only the service locator's address.

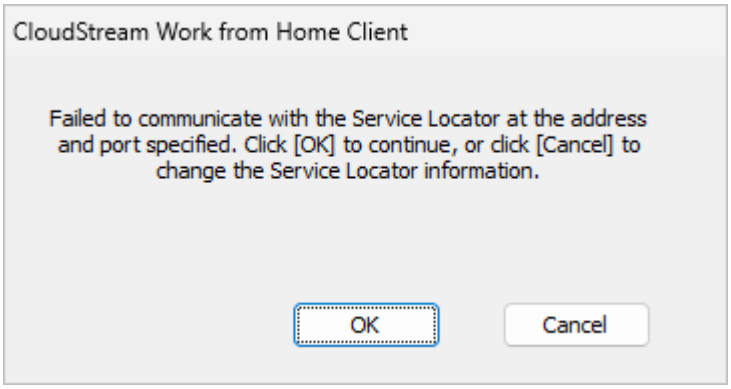
This field requires the service locator address and not the URL. An example of a service locator address is `msl-mymsl.com`, while the service locator URL is `https://msl-mymsl.com:443`.

8. (Optional) If you want to use Proxy server, please check ***Enable HTTP Proxy*** to enter the Proxy Server information. Otherwise, leave it unchecked.

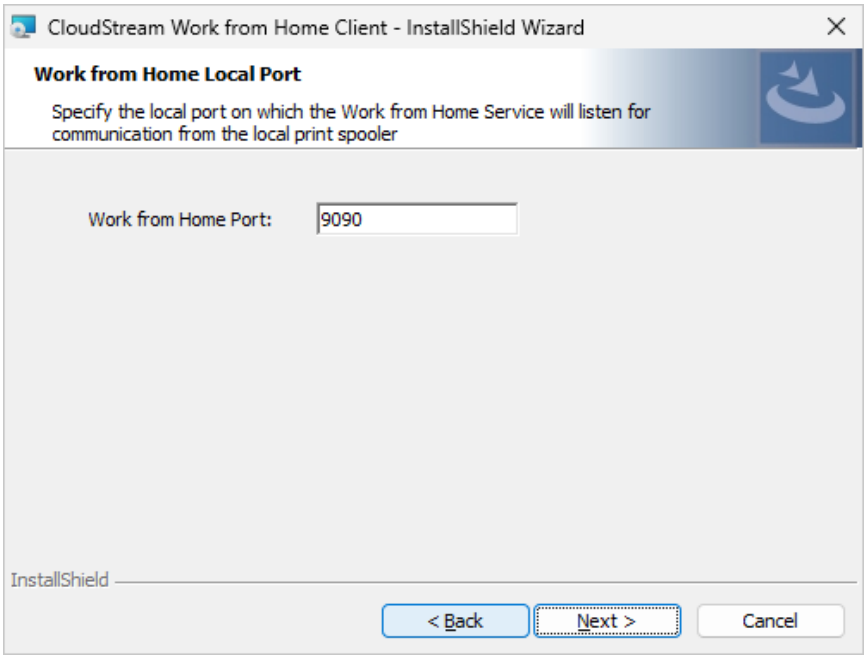


9. Click **[Next].** The tool will connect to the Server using the information you have provided, and the result will be displayed in a pop-up dialog.

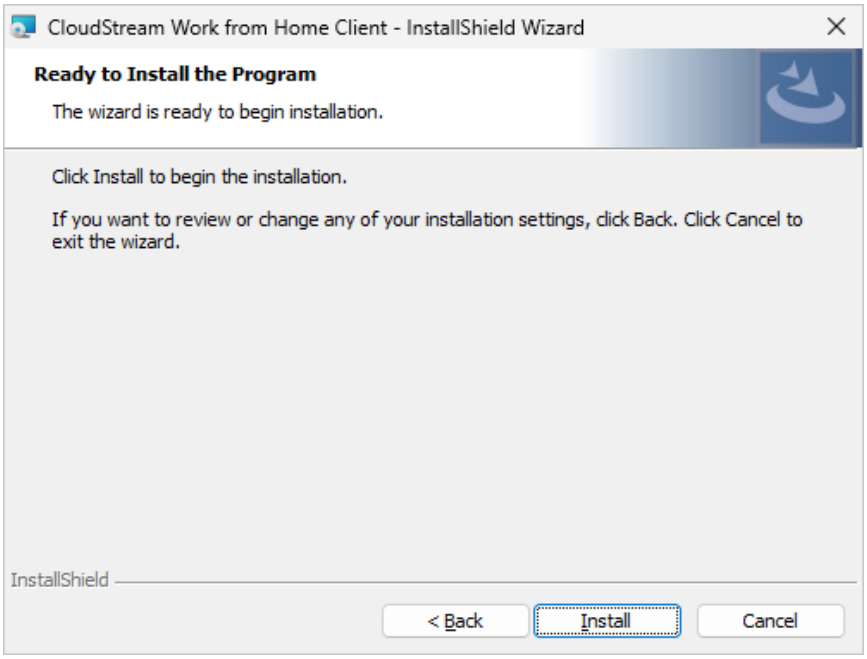
   If you encounter this error, please check your previous inputs are correct. If your onboarding code is expired, please generate a new one.



10. Input the Work from Home port, then click **[Next].** The default is 9090.



11. Click **[Install]** to start the installation, and after the installation is complete, click **[Finish].**



Completing the installation will run the Work from Home service automatically. To check the service, open services.msc and look for ***Work from Home*** service. The service must be running to detect WfH devices.

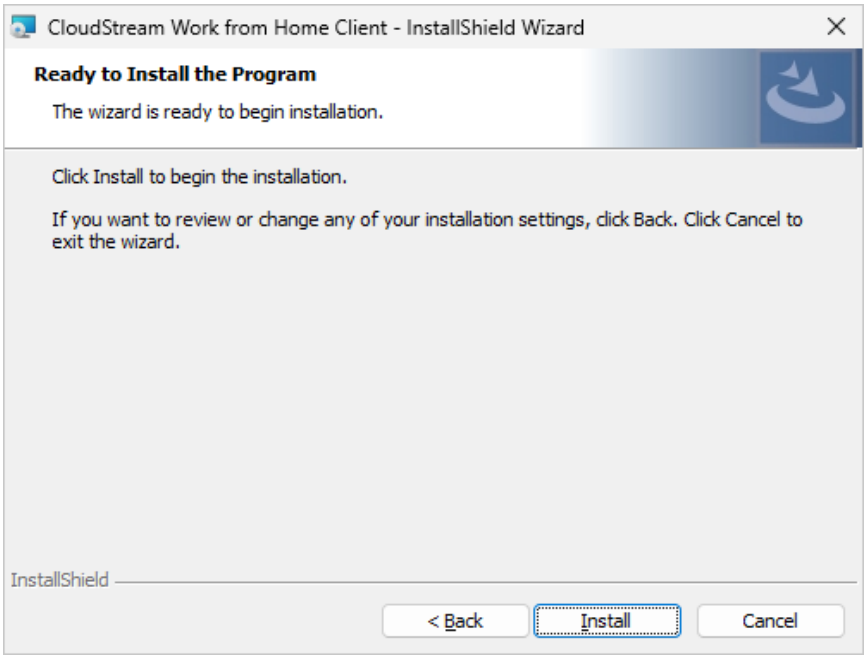
Important: WfH devices must be accepted by the Administrators after discovery. WfH users must supply the correct device model name to the Administrators so that they can accept the WfH devices.

Upgrade the Work from Home Client

To upgrade the WfH Client, run a newer version of the installer.

1. Login to your home PC using the user account registered to CloudStream DM.
2. Run the installer ***WfHClientSetup.exe.*** Please make sure you have administrator rights to install the application on your client machine.
3. In the installation wizard, read the information, then click **[Next].**
4. Read the Software License Agreement and agree to the license agreement, then click **[Next].**
5. Click **[Install]** to start the installation, and after the installation is complete,

click **[Finish].**



Completing the installation will overwrite the Work from Home service with the new version automatically.

Add Devices to WfH Client Computer

Add Ricoh devices to your Home PC where the WfH Client is installed. The WfH Client service will use the printer's IP Address and Port to communicate with the device.

You can find the following information on this topic.

Add Network Printer on page 117.
Add USB-Connected Printer on page 118.
Remove Printer on page 118.

Important: WfH devices must be accepted by the Administrators after discovery. WfH users must supply the correct device model name to the administrators so that they can accept the WfH devices.

Add Network Printer

1. Login to your PC and open ***Printers & Scanners.***
2. Click the ***Add a printer or scanner*** button.

3. Look for the WfH printer in the list. If your printer is not listed, scroll down, and click the link **The printer that I want isn't listed.**
4. Select the option to find your printer. In this example, the printer will be added using TCP/IP address or hostname.
5. Click **[Next]** and input the hostname or IP address and the Port name.
6. After the device is detected, select the printer driver to be installed on the PC. If you have a copy of your device driver from your local folder, browse and select the driver, then proceed to the next screen.
7. Specify the printer's name.
8. (Optional) Select to share the printer then finish the installation.

After installation, the printer is displayed in the list of printers on the ***Printer & Scanners*** screen. All printers listed on the screen will be discovered by the WfH Client service as long as the printer is online and the address and port information are correct.

Add USB-Connected Printer

1. Connect the device to the PC via a USB cable. This action will automatically add the printer driver to your PC.
2. Please wait for the USB printer installation to be completed. Then open Printers & Scanners.
3. Make sure your USB-connected printer is added to the list of printers.

Note: You can connect one or more USB devices to your PC, and the WfH Client service will discover the connected devices.

Remove Printer

1. Login to the PC where the WfH Client is installed.
2. Open the ***Printers & Scanners*** window.
3. Select the WfH device (Network or USB connected).
4. Click **[Remove device].**
5. Click **[Yes].**

Important: Please inform the administrator that the device is removed and will not be monitored so that the WfH device can be deleted from the application.

System Settings

System settings have the following main functions:

- ***Server Settings*** contains display formatting, email server settings, data storage, repository management, and system information.
- ***Security*** contains client certificates, authentication profiles, admin roles and accounts, local password policy, and client registration.
- *Alert policies* enable administrators to create an alert policy that informs the recipient whenever a group of devices exhibits the set condition.
- *Logs* allow administrators to view system logs such as alert policy logs, audit logs, authentication logs, and report logs.

Here is a list of System Settings:

- Server Settings
  - License Management on page 121.
  - License Summary on page 126
  - Display Settings on page 127.
  - Email Server Settings on page 133.
  - SIEM Data Transfer on page 138.
  - Data Storage and Repository on page 142.
- Security
  - Client Certificates on page 145.
  - LDAP Authentication Profile on page 151.
  - Auth Agent Installation on page 155.
  - OpenID Connect Authentication Profile on page 164.
  - Administrator Roles on page 171.
  - Administrator Accounts on page 190.
  - Local Admin Password Policy on page 194.
  - Register Authentication Clients on page 200

- Alert Policy on page 201.
- System Logs on page 214.
- Software Download on page 218.
- Print and Scan on page 219.

All the settings listed above can be accessed from the left-hand side navigation menu when you open the System section.

Please make sure that the account used to login has an assigned role that can modify the system settings. Please see Administrator Accounts on page 190 for more details.

License Management

The License Management page allows you to view activated licenses, delete expired licenses, and monitor the number of licenses used by your devices. Options and features on this page are described within this topic.

The License Summary page allows you to view a summary of all activated licenses. Refer to License Summary on page 126 for details.

RICOH CloudStream supports the following types of licenses.

- **RICOH CloudStream Device Management** license - With this type of license, you can add devices to CloudStream DM, including Work from Home devices. You can assign policies and send configuration tasks to the devices.

  This type of license is displayed in the CloudStream DM's License Management.

- **RICOH CloudStream Print&Scan** license - With this license, you can use the RICOH CloudStream Print&Scan embedded application for secure printing and scanning.

  This type of license is **not** displayed in License Management. However, you can manage them in the RICOH CloudStream Print&Scan' Portal. To access the portal, refer to Print and Scan on page 219.

You can find the following instructions to manage your licenses.

Check Available Licenses on page 122. Helps you monitor the expiration and availability of your regular and extended licenses.
Extend License Expiration on page 122. Shows you the list of licenses that will be used for extending the expiration date of your existing regular licenses.
Delete Expired License on page 123. Helps you remove licenses that are already expired.
Customer ID on page 124. Shows your Tenant ID or Customer ID.

Note: Set the *License Expiry Notification* feature to notify you when a license is about to expire. Configure the settings in Email Server Settings on page 133.

Check Available Licenses

The Ricoh team will activate your product key after purchasing a RICOH CloudStream Device Management license. You will find three tables on the License Management page.

Tables	Description
Activated Licenses	All active licenses are displayed here. Please regularly check the expiration of each license. **Note:** You can set the *License Expiry Notification* feature to notify you when a license is about to expire. Configure the settings in Email Server Settings on page 133.
Licenses for Extension	These are licenses that extend the expiration date of the existing (regular) license. When a regular license expires and there is a matching license for extension available, the regular license's expiration date is extended by using the license for extension. Go to Extend License Expiration on page 122.
Activated Features	With the license, CloudStream DM can manage, monitor, and configure devices. This table displays the available units for each type of license. License units are randomly assigned to the devices, and all available units are displayed here.

Important: If a license is not extended after it expired, the number of available units will decrease, affecting the functionality available.

You must have enough available RICOH CloudStream Device Management license before you add new devices to CloudStream DM.

Similarly, you must have enough RICOH CloudStream Print&Scan license before you deploy RICOH CloudStream Print&Scan embedded application to the devices.

Extend License Expiration

As long as you have the license to extend the regular license, then you do not need to worry about extending your license for the extension will happen automatically.

To understand how the licenses are extended, please read the following information.

- The number of units of a regular license (license displayed in Activated Licenses table) must match any license in the License for Extension table.

For example:

Activated Licenses: • License A with 1000 units • License B with 2000 units	License for Extension table: • License E1 with 1000 units period of 6 months • License E2 with 1000 units period of 1 year

Scenario	Result	Reason
If License B expires	License B is not extended and expired.	The regular license's units should match to license for extension units. In the above example, both extension licenses (E1 and E2) are of 1000 units, and License B requires 2000 units.
If License A expires	License E2 is used. License A expiration date is extended to 1 year.	The system will use the license with the longest period.

- When an extension license is used, it will be shown in grey text and listed at the bottom of the list. You can click **[Delete Used]** button to remove the used licenses.

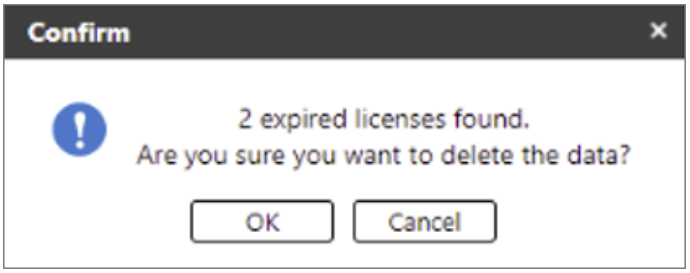
Delete Expired License

A license can only be deleted the day after it has passed the expiry date.

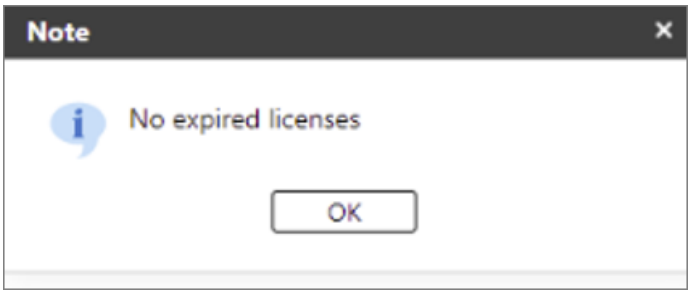
An expired license will have an expired indicator beside the product key.

All expired licenses in the list will be deleted when you click the **[Delete Expired]** button.

- If there is at least one expired license in the list, a pop-up dialog will display showing the number of expired licenses about to be deleted. Click **[OK]** on the dialog to remove the expired licenses. An example is shown below.



- If no expired licenses are in the list when the **[Delete Expired]** button is clicked, the following message will be displayed.



Expired Licenses

When a license expires, the number of units in the ***Available*** column in ***Activated Feature*** table will decrease based on the license's total number of units.

An expired license will remain on the list until removed.

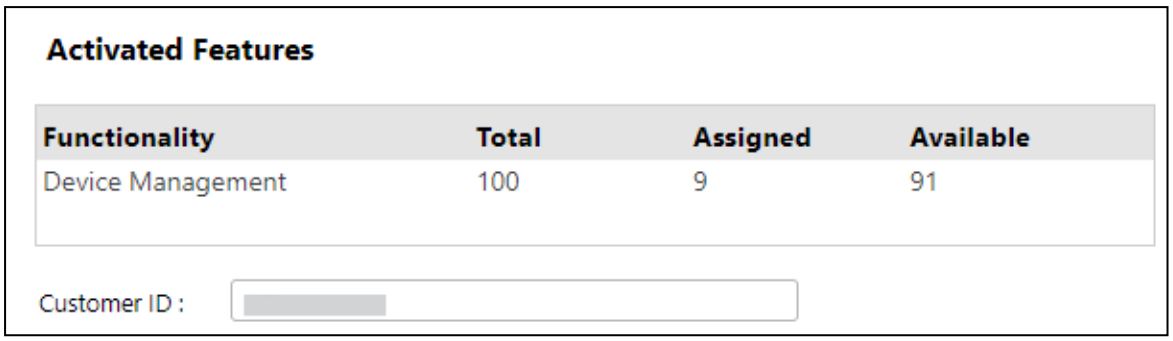
The license will expire the day after the expiry date. If the expiry date is the 1st of January 2025, the license will become unusable on the 2nd of January 2025.

Customer ID

The customer ID is required when you contact Ricoh support.

You can find your Customer ID in License Management.

1. Login as an administrator.
2. Go to the ***System*** section.
3. Expand ***Server Settings*** and click on ***License Management.***
4. Scroll down to view your Customer ID shown beneath the Activated Features section.


Activated Features
Functionality
Total
Assigned
Available
Device Management
100
9
91
Customer ID :

License Summary

The License Summary page allows you to view a summary of all activated licenses.

- **Activated Licenses Summary:** Groups and displays activated licenses

  The table groups licenses into rows based on the name of the license, the license type, the activation and expiry date, and the total number of licenses that belong to the group.

- **Remaining Licenses Summary:** Groups and display extension licenses

  The table summarizes the extension licenses into rows based on the license name and period.

Display Settings

The ***Display*** section helps the administrator set the following settings.

Note: If the changes in the display format are not reflected after saving, please re-login to CloudStream DM to see the changes.

Country Settings

Item	Description
Country	You can change the default country. The default value of the country setting depends on the regional CloudStream DM server's system locale. **Note:** Changing the country does not change the language used in CloudStream DM, please change the language in the login screen.

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.
4. In the ***country*** drop-down menu, select a country of your choice.
5. Click **[Save].** (Scroll down to see the save button)

Date Display Format

The Date Display Format lets you change the Time Zone and the date formatting. These settings apply only to data within the application.

Item	Description
Reports Time Zone	Select the time zone from the list.

Item	Description
Date Display Format	Select the date display format from the following: • [YYYY/MM/DD] • [MM/DD/YYYY] • [DD/MM/YYYY]

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.
4. In the ***Date Display Format***, select a value for ***Reports Time Zone***.
5. Select a value for ***Date Display Format.***
6. Click **[Save].** (Scroll down to see the save button)

Note: The default value is determined based on the regional CloudStream DM server's system time zone.

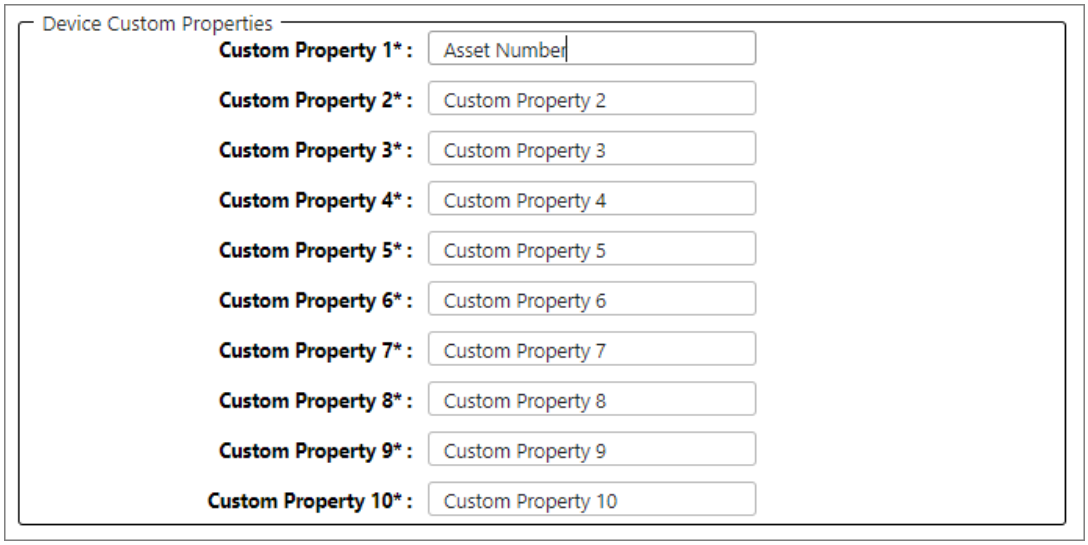
Device Custom Properties

Device Custom Properties allows administrators to add custom property labels. You can set up to ten custom properties, which will be shown in the device's optional properties.

Item	Description
Custom Property 1-10	Set the custom property labels for all devices.

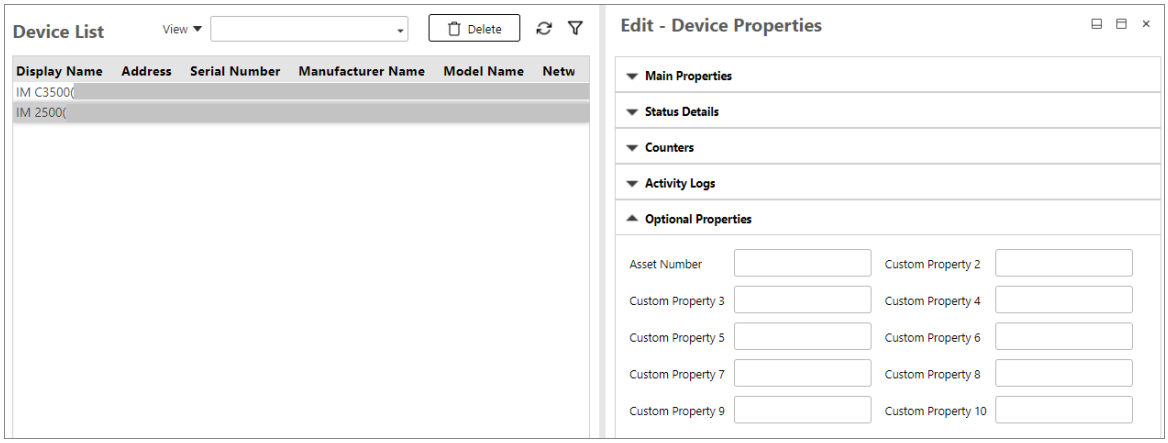
1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.
4. In ***Device Custom Properties***, select a custom property and overwrite with the name of your preference.

   For example, Custom Property 1 value is "Asset Number".



5. Click **[Save].** (Scroll down to see the save button)

After saving, you can find the custom property changes in the device optional properties.



Device Display Format

The Device Display Name Format allows you to format how devices are displayed in the Device List's Display Name column. The setting lets you select multiple attributes, and the device's name will display according to the selected attributes.

For example, if you want the devices to display the Serial Number, then the IP Address, followed by the Model Name. To do so, right-click on the Device Display Name Format text box then you will see a list of device attributes. In this example, click Serial Number, then do the same steps to select the IP Address and the Model Name. The Device Display Format will then look like this: $[serial]$$[ip]$$[model]$

The default device display name is "model name (IP address of the device)" or '$[model]$$[ip]$' in the text box.

Note: An Administrator can view the properties of a device within the Device List, and can manually enter a Display Name. In this case, the manual entry overrides the Device Display Name format described below

Item	Description
Device Display Name Format	Specify the format of the device display name. The default device display name is "model name (IP address of the device)". **Note:** In case that the device display name is over 64 characters, it will be cut by 64 characters. The items to be included in the display name can be entered manually or selected from the list of variables. To display the list of variables, right-click the text box. • [Model Name] • [Address] • [Serial Number] • [IP Address] • [MAC Address] • [Host Name] • [Vendor Name] • [WIM Location] • [WIM Comment] • [PPM] • [Custom Property] 1–10 **Note:** The configured format is applied only to newly registered devices. If you made changes now, you changes will be applied to new devices only.

Target Device Association Category

The ***Target Device Association Category*** allows you to select a certain device category such as “Host name”, “IP Address”, “Models”, and custom categories. The groups within the selected category will be displayed as target group options to create a Device Policy. To know more about device policy, please see Device Policies on page 261.

Item	Description
Target Device Association Category	Select the category of the devices associated with the Device Policies (Configuration Policy, Firmware Policy, Embedded Policy). The groups will be displayed in ascending order the same as the Device List. The selected device category will also be used to set the Alert Policies.

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.
4. In the ***Target Device Association Category***, select a category.

   For example, select IP Address category.
5. Click **[Save].** (Scroll down to see the save button)

After saving, the only category displayed in the Device Policy Target Group is "IP Address".

Hide Sensitive Data

To hide sensitive data in the Print Activity dashboard, Scan Activity dashboard, and generated reports, follow the steps below.

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***Display***.

4. In the ***Hide Sensitive Data***, choose or more options:

Value	When Checked	When Unchecked
Don't Record Job Name for Print&Scan Activities	The print and scan jobs are recorded, but their job names are **not saved** in the CloudStream DM database, so the job names are **not** displayed in the dashboard and in the generated report. If you decide to uncheck this setting, new jobs are recorded with their names and displayed in the dashboard and report. However, the names of the jobs before them cannot be displayed because they were not saved.	The print and scan jobs are recorded, and their names are **saved** in the CloudStream DM database. You can find the job names displayed in the print activity and scan activity dashboards and in the generated report. If you decide to check this setting, new jobs are recorded, but their names are not saved. Jobs whose names are saved in the database will still be displayed, while the new job names will not be saved and, therefore, cannot be displayed.
Don't Record User Name for Print&Scan Activities	When a print and scan job is completed, the user name is not saved in the database. As a result, the dashboards and reports that contain this information will not be able to display the information. In Dashboards, the User Name column will display 'Unknown'. In Reports, the User ID and User Name columns will display 'Unknown'.	The user name is saved in the database and displayed in corresponding fields in both dashboards and reports.

5. Click **[Save].** (Scroll down to see the save button)

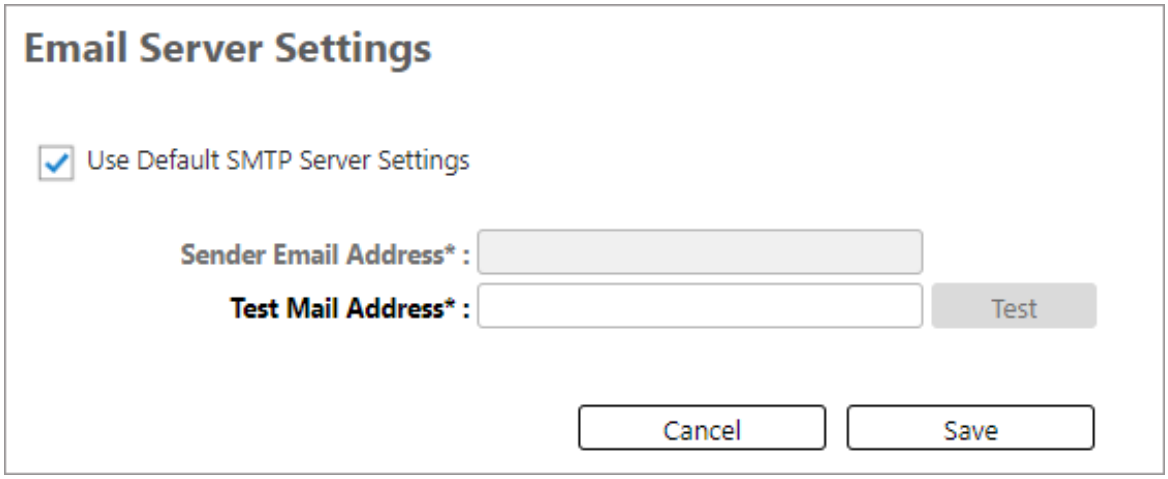
Email Server Settings

Email messaging is a requirement before creating alert policies and other features that send email messages.

You can also set the License Expiry Notification to notify the specified email addresses days before the licenses expire and help you procure an extension license before the expiration date. Refer to License Expiry Notification on page 135.

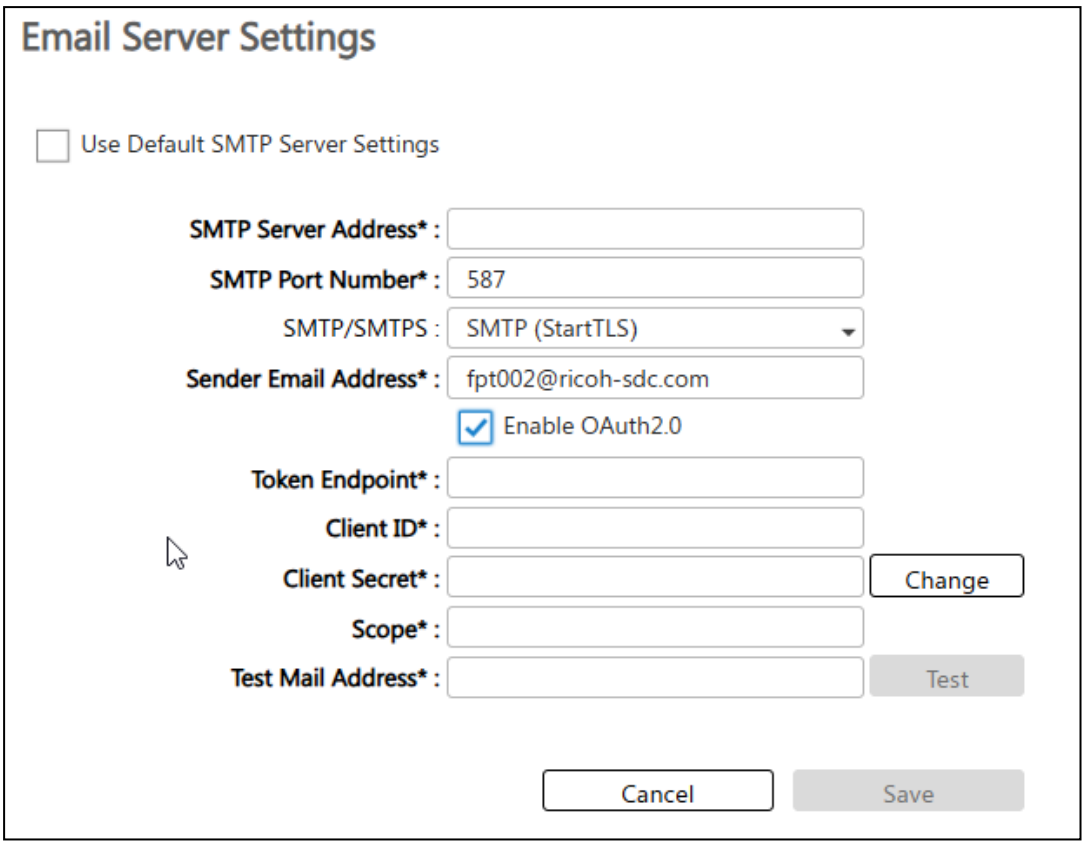
The RICOH CloudStream Device Management (DM) has a built-in Email Server system that you can use. Check the "Use Default SMTP Server Settings" and try sending a test email by adding your email address in the Test Mail Address field and clicking [Test]. By testing the default SMTP server, you will receive an email sent from CloudStream DM that ends with "cloudstream.ricoh.com".

Important: To use the system email server, you must check *Use Default SMTP Server Settings*.



If you would like to use your own Email Server, you can do so by following the instructions below.

1. Login as an administrator.
2. Go to the ***System*** section.
3. Expand ***Server Settings*** and click on ***Email Server Settings.***
4. Uncheck "Use Default SMTP Server Settings" to use your own SMTP server. After you disable the checkbox, additional settings appear.



5. Provide values to the required settings in the table below. If enabling OAuth2, proceed to step 6 instead.

Settings	Description
SMTP Server Address	Enter the address of the SMTP server. Default value is "smtp". This is a required field.
SMTP Port Number	Enter the port number of the SMTP server. The default is 587. This is a required field.
SMTP/SMTPS	Specify whether or not to use a secure connection. This is a required field. • No Security - The connection is not encrypted. • SMTPS (SMTP over SSL) - The connection is encrypted. This is the default selection. • SMTPS (StartTLS) - The connection is initially created over plain text. If the server supports the StartTLS command, the connection is updated to an encrypted channel.
Sender Email Address	Enter the sender's email address. This is a required field. This is the email address shown in the emails "From" field.
Account Name	Enter the account name you want to use for authentication. Default value is 'smtpuser". This is a required field.

Settings	Description
Password	Enter the password to use for authentication. This is a required field.
Test Mail Address	Enter the email address to send a test email. This field is required when you click the **[Test]** button. Use the **[Test]** button to check the connection to the email server.

6. Enable the OAuth2 checkbox if enabling SMTP with OAuth 2.0 authentication.

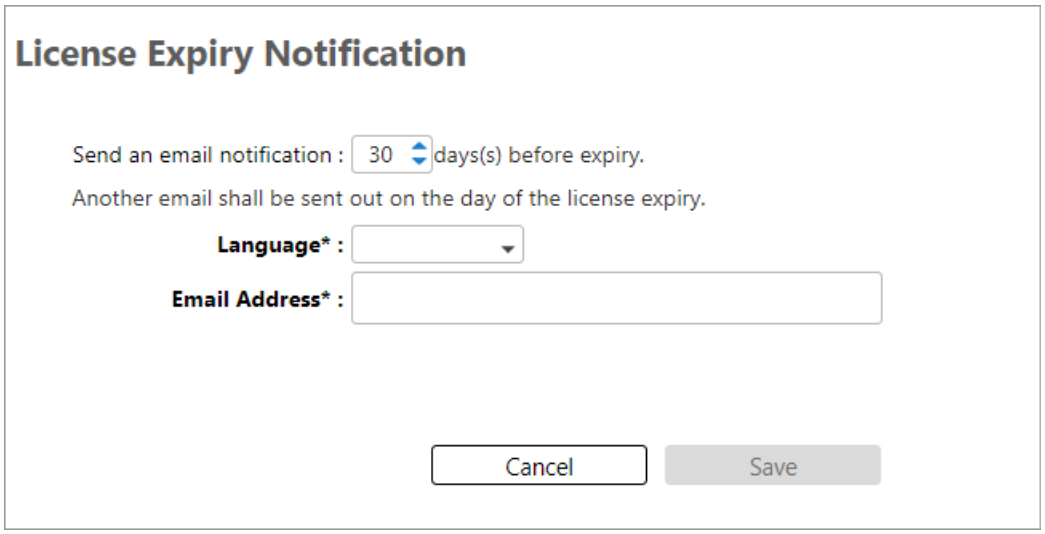
OAuth2 Settings	Description
Token Endpoint	Enter the URL of the token endpoint that is used to contact the provider to obtain an access token.
Client ID	Enter the Client ID of the application registration for which the mailbox is configured and used to send email over SMTP.
Client Secret	Enter the Client Secret of the application registration for which the mailbox is configured and used to send email over SMTP. The password is filed and encrypted before it is saved.
Scope	Enter or more scopes that Cloudstream will use to place a request to the provider. For Microsoft Exchange, the default scopes would be "https://outlook.office365.com/.default", "offline_access" If entering more than one scope, ensure you leave a space between each scope.
Test Mail Address	Enter the email address to send a test email. This field is required when you click the **[Test]** button. Use the **[Test]** button to check the connection to the email server.

7. Complete the information required on this page and click **[Save].**

Check the test email account you entered to ensure the connection to the email server is successful.

License Expiry Notification

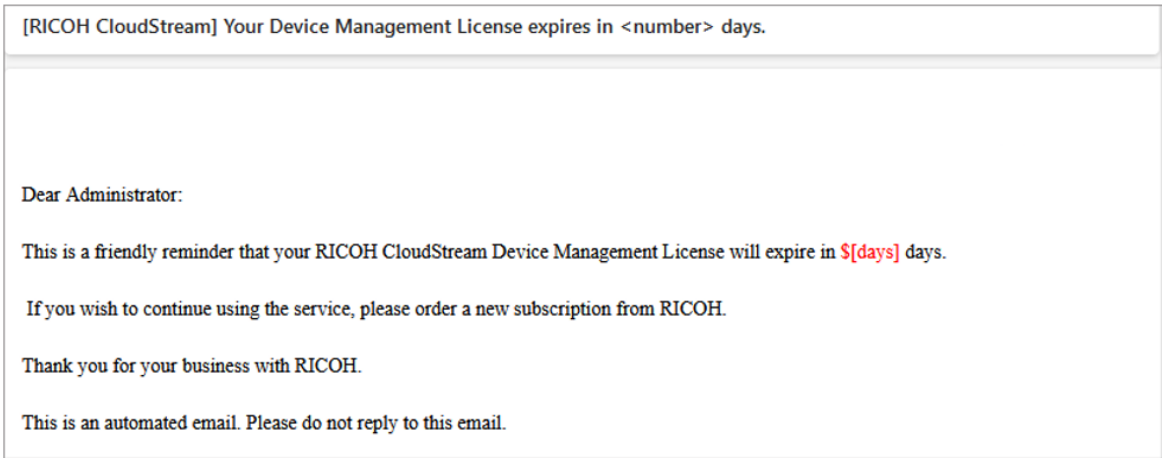
The License Expiry Notification allows you to specify the number of days a notification is sent before the license expires.



There are three settings you must configure.

Settings	Description
Days	Select from 1 to 90 days. Select the number of days the notification is sent before the license expiration date. For example, if the number of days selected is 20 and the license expiration date is January 31, the email recipients will receive a notification email on January 12 (20 days before expiration) and another notification on January 31 (the expiration date).
Language	Select the language to be used. The content of the email notification is translated to the chosen language.
Email Address	Specify the recipients email addresses separated by a comma.

The recipients will receive an email notification similar to the image below. Note that **<number>** and **$[days]** is the number of days you set in the License Expiry Notification.


[RICOH CloudStream] Your Device Management License expires in <number> days.

Dear Administrator:

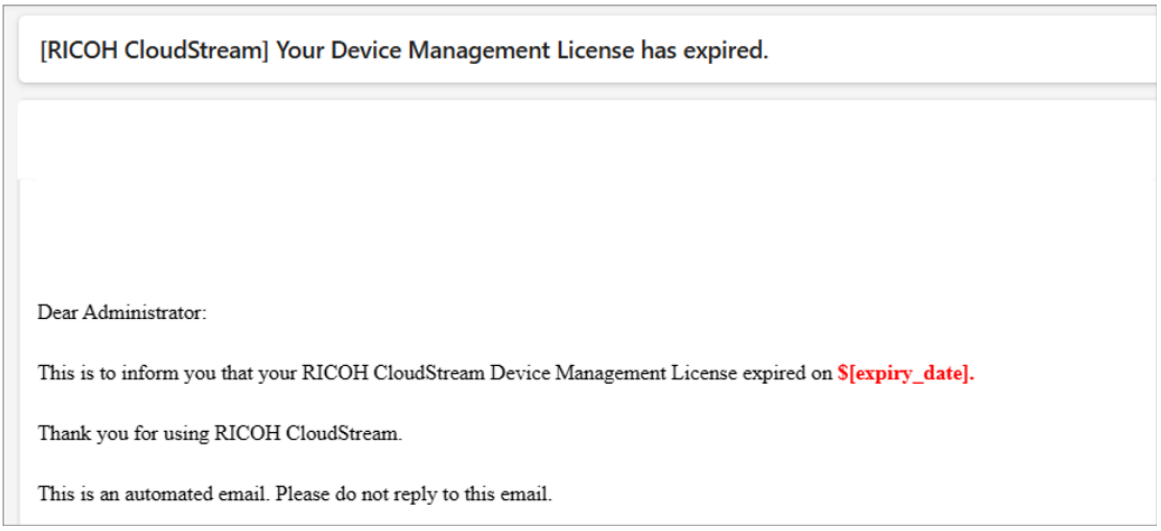
This is a friendly reminder that your RICOH CloudStream Device Management License will expire in $[days] days.

If you wish to continue using the service, please order a new subscription from RICOH.

Thank you for your business with RICOH.

This is an automated email. Please do not reply to this email.

On the day of the expiration date, you will receive an email notification similar to the image below. Note that the $[expiry_date] is the license expiration date.


[RICOH CloudStream] Your Device Management License has expired.

Dear Administrator:

This is to inform you that your RICOH CloudStream Device Management License expired on $[expiry_date].

Thank you for using RICOH CloudStream.

This is an automated email. Please do not reply to this email.

If you receive the above emails, please go to **[System]**, expand **[Security Settings]**, and click ***License Management*** to see the licenses about to expire. For details go to License Management on page 121.

It is recommended that you purchase an extension license so the system will automatically renew your licenses without interruption. Please contact Ricoh Sales in your region to place the order.

SIEM Data Transfer

Security Information Event Management (SIEM) allows you to collect volumes of data in real time so security teams can detect and block attacks. CloudStream DM SIEM Transfer feature enables you to configure the connection to the SIEM Splunk server and download SIEM logs.

Important: CloudStream currently supports Splunk Enterprise only.

Preconditions

You must have an Uninstall Print&Scan Embedded App on page 284 license to set up the SIEM settings. Contact Ricoh to purchase the license.

In order to transfer SIEM log data from CloudStream DM to your SIEM tool, you must allow the tool to access the CloudStream DMenvironment in your network.

Please allow connections to your network's IP addresses listed in the table below, depending on your region.

Region	CloudStream DM IP Address
Europe (*.eu.cloudstream.ricoh.com)	20.113.73.197
North America (*.na.cloudstream.ricoh.com)	20.252.6.56
Asia Pacific (*.ap.cloudstream.ricoh.com)	20.227.2.98
Canada (*.ca.cloudstream.ricoh.com)	20.220.243.35

Note: You can determine the region by looking at your CloudStream DM URL.

For example, if the URL is https://mycompany.na.cloudstream.ricoh.com, this indicates that the region is North America because of na.cloudstream.ricoh.com in the URL.

A token is generated. Please see Generate HEC Token on page 140.

1. Login as an administrator.
2. Go to ***System*** and expand ***Server Settings.***
3. Click ***SIEM Transfer Settings.***
4. Check ***Enable SIEM Transfer.***
5. Enter the hostname of the SIEM solution.Enter the port number.

6. Enter the SIEM authentication token.
7. Click **[Save].**

Saving the configuration will establish a connection to the SIEM. If the connection is successful, the configuration is saved. If the connection fails, an error message is displayed, and the configuration is not saved. Please input the required fields again and click **[Save].**

Important: SIEM Transfer is executed once every day at a fixed time (sequentially after UTC+0). When the transfer starts, you will see data populating in the *SIEM Transfer table.*

SIEM Transfer Table

The table has the following columns.

Column Header	Description
Date	Displays the date and time the data transfer started.
Status	Displays the result of the transfer. • Succeeded - successful data transfer. • Failed - data transfer failed. • Skipped - data transfer is skipped. When it's time to transfer data but there is no new data to be transferred, the status will display 'Skipped'.
SIEM Transfer Log Details	Displays the details of the transfer. • Successful transfer will display the details of the data transferred. • Failed transfer will display the reason for the failure. • Skipped transfer will display the following message: “No SIEM log data to be transferred or the additional data is not available”.

Download SIEM Data Transfer

You can download SIEM Data Transfer details into CSV file format. Click the icon in the top right corner of the table.

A CSV file containing the details is downloaded immediately. The file's name is in this format <Date and Time>_SIEMTransferLogDetails.

Filter Details

Use the filter function to find specific data transfer information.

a. Click the icon.

b. In the column's search box, enter the value you want to search for.

c. Click the bottom icon or press enter from your keyboard.

The details that match your search criteria are displayed in the list.

To remove the search result list, please delete the values from the column search box, then click icon or press enter from your keyboard.

Generate HEC Token

The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token-based authentication model. You must generate a token before you configure the CloudStream DM SIEM Transfer feature.

Important: CloudStream DM only supports a SIEM tool called "Splunk Enterprise".

For **Splunk Cloud Platform**, to generate a token, follow the steps below:

1. Access your Splunk Cloud Platform.
2. Click ***Settings***, then click **[Add Data].**
3. Click ***monitor***, then click ***HTTP Event Collector.***
4. In the ***Name*** field, enter a name for the token.
5. (Optional) In the ***Source name override*** field, enter a name for a source to be assigned to events that this endpoint generates.
6. (Optional) In the ***Description*** field, enter a description for the input.
7. (Optional) If you want to enable indexer acknowledgment for this token, click the ***Enable indexer acknowledgment*** checkbox.
8. Click **[Next].**
9. (Optional) Make edits to the source type and confirm the index where you want HEC events to be stored.
10. Click **[Review].**
11. Confirm that all settings for the endpoint are what you want.
12. If all settings are what you want, click **[Submit]**. Otherwise, click **<** to make changes.
13. (Optional) Copy the token value that Splunk Web displays and paste it into another document for reference later.

14. (Optional) Click ***Track deployment progress*** to see progress on how the token has been deployed to the rest of the Splunk Cloud Platform deployment. When you see a status of "Done", you can then use the token to send data to HEC.

The steps are coming from docs.splunk.com and you can find more instructions in Splunk site.

To enable HEC for use with Amazon Web Services (AWS) Kinesis Firehose, you must file a ticket with Splunk Support. Standard HEC is enabled by default on all Splunk Cloud Platform deployments and does not require a Splunk Support ticket.

To generate a token for **Splunk Enterprise**, follow the steps below.

1. Access your Splunk Cloud Platform.
2. Click ***Settings***, then click **[Add Data].**
3. Click ***monitor***, then click ***HTTP Event Collector.***
4. In the ***Name*** field, enter a name for the token.
5. (Optional) In the ***Source name override*** field, enter a name for a source to be assigned to events that this endpoint generates.
6. (Optional) In the ***Description*** field, enter a description for the input.
7. (Optional) If you want to enable indexer acknowledgment for this token, click the ***Enable indexer acknowledgment*** checkbox.
8. Click **[Next].**
9. (Optional) Make edits to the source type and confirm the index where you want HEC events to be stored.
10. Click **[Review].**
11. Confirm that all settings for the endpoint are what you want.
12. If all settings are what you want, click **[Submit]**. Otherwise, click **<** to make changes.
13. (Optional) Copy the token value that Splunk Web displays and paste it into another document for reference later.

The steps are coming from docs.splunk.com and you can find more instructions in Splunk site.

Data Storage and Repository

Repository Management

The following files are stored in the cloud server.

- Firmware packages
- Extended Device Preference resources and device preferences
- SDK/J Platforms
- Embedded Applications

You can view the files in the System section.

1. Go to ***System*** and expand ***Server Settings.***
2. Click ***Repository Management***.

Column Header	Description
Name	The name of the file. For XDP resource name, the name specified for the resource file is displayed.
Description	Displays the description of the file. For Embedded application, the build version and the expiration date are displayed here.
Type	The type of file stored.
Date/Time Registered	The date and time the file was stored on the cloud server. For XDP, if the resource file is overwritten, the date and time will display the updated date.
Usage Count	The number indicates how many functions are currently using the file. If the usage is zero, the **[Delete]** button will be enabled, allowing you to delete unused files.

Data Storage Policy

Data storage policy allows you to manage the retention period for status, counter, and log data.

The data retention policy will follow the values set on this page. The data older than the storage policy will not be kept and will be deleted.

The following are available policies for storing data.

Item	Description
Status	Specify the storage period of the status history retrieved from devices. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 2 years.
Counter	Specify the storage period of the counter information retrieved from devices. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 2 years.
Device Activity Logs	Specify the storage period of the device activity logs. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 3 months.
Alert Policy Logs	Specify the storage period of the alert policy logs. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 3 months.
Audit Logs	Specify the storage period of the Audit logs. Specify one of the following: • 1–31 day(s) • 1–12 month(s)

Item	Description
	• 1–5 year(s) The default value is 3 months.
Authentication Logs	Specify the storage period of the Authentication logs. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 3 months.
Report Logs	Specify the storage period of the original data used for generating reports. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) The default value is 3 months.

Client Certificates

Onboarding codes are time-sensitive and are used to add DM Agent-managed devices and configure the WfH client and Auth Agent. All generated and valid onboarding codes are displayed in the ***Onboarding Codes*** table. Generated codes will expire after 24 hours at most depending on the validity period.

When a device, WfH device, or an Auth Agent is added to the application, an equivalent client certificate is generated by the system. The certificates will be displayed on the ***Certificate Management*** table.

A code and a certificate can be one of the following Client Types:

- **DM Agent** - The code and certificates generated with this client type will be used in adding and managing Ricoh devices. More DM Agent details are described in Add Devices to CloudStream DM on page 27.
- **Auth Agent** - The code and certificates generated with this client type are used to set up and connect authentication agent to the application. See Auth Agent Installation on page 155 for more details.
- **Work from Home Client** - The code and certificates generated with this client type are used to set up the WfH Client and add WfH devices. Please see Work from Home (WfH) Client on page 111.

Here is how to generate a code and manage certificates:

Order	Instructions
1	Generate an onboarding time-sensitive code, then use it for configuration. You can find the steps to generate a code in Generate Onboarding Codes on page 148.
2	The system will issue a certificate to devices, WfH devices, or auth agent after successfully authentication using the time-sensitive codes you generated. Manage the certificate here Certificates and Service Locator URL on page 145.

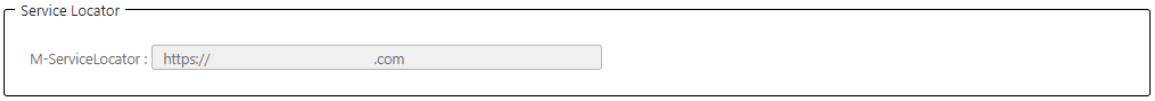
Certificates and Service Locator URL

Find the following topics to manage the certificates and set the Service Locator.

Find the Service Locator URL on page 146.
View Certificates on page 146.

Revoke Certificate on page 147.
Download Root CA Certificates on page 148.

Find the Service Locator URL



1. Go to ***System*** and expand ***Security.***
2. Click ***Client Certificates.***
3. Go to ***Service Locator.***
4. Copy the service locator and note it down for future purposes.

View Certificates

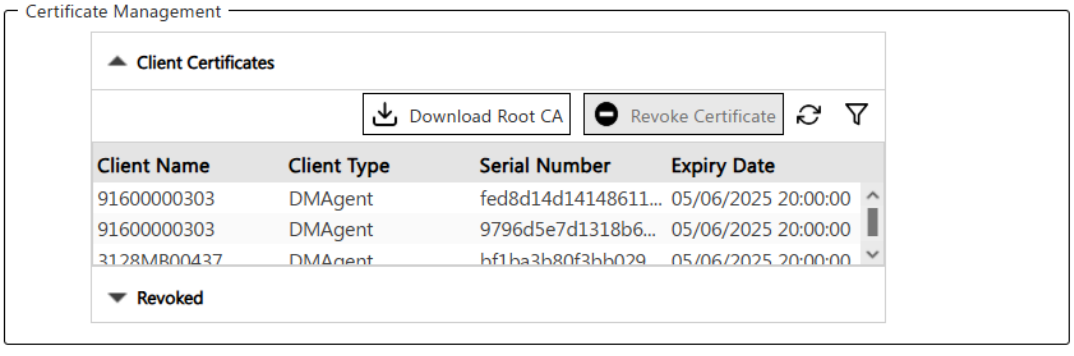
An equivalent certificate is generated when one of the following is registered to CloudStream DM.

- When a device is added, a 'DM Agent' client type certificate is generated. There will be an assigned certificate for each device.
- When an auth agent is configured and connects to CloudStream DM, an 'Auth Agent' client type certificate is generated. There will be an assigned certificate for each auth agent.
- When a WfH device is added, a 'Work from Home Client' client type certificate is generated. There will be an assigned certificate for each WfH client.

You can view the generated certificate in ***System*** section.

1. Go to ***System*** and expand ***Security.***
2. Click ***Client Certificates***.
3. Go to ***Certificate Management.***

   The Certificate Management options are shown below, and described in the following table.



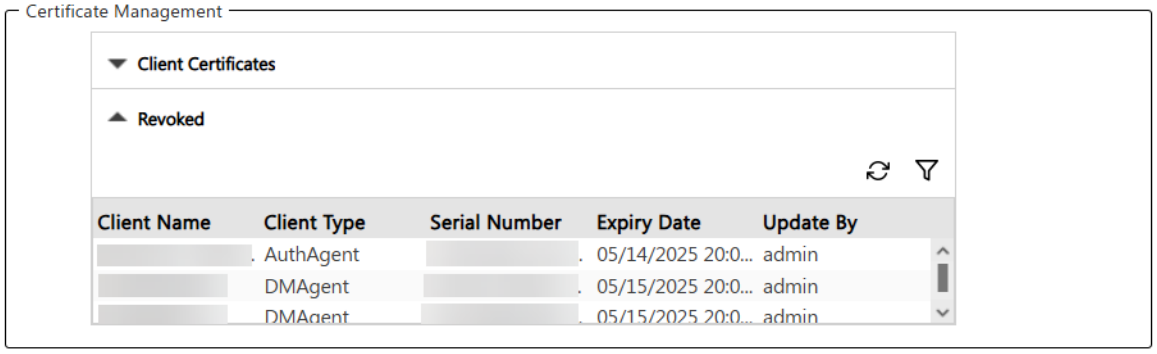
Column Header	Description
Client Name	Displays the name of the certificate. • For the ***DM Agent*** client type, the device serial number will be displayed. • For the ***Auth Agent*** client type, the server computer name will be displayed. • For the ***WfH Client*** client type, the computer name where the WfH Client is running will be displayed
Client Type	Either one of the following is displayed: • Auth Agent • DM Agent • Work from Home Client
Serial Number	The fingerprint of the certificate.
Expiry Date	The date and time the certificate will expire. The certificate will expire one year after its creation. Expired certificates will be revoked.

Revoke Certificate

Revoking the certificate will stop communication with the application. Before revoking a certificate, please make sure that no other admin or user is using the device or the Auth Agent. Revoking a certificate cannot be undone.

1. Login as an administrator.
2. Go to ***System*** and expand ***Security.***
3. Click ***Client Certificates.***
4. Go to ***Certificate Management.***
5. Select the certificate you want to revoke. Use the filter option to narrow down your search. For example, if you are revoking an Auth Agent, filter the Client type first, then locate the Client name.
6. Click **Revoke Certificate**.
7. Confirm to revoke of the certificate.

Once revoked, the certificate appears in the Revoked section of the table only, as shown below.



Note: If you revoke a certificate accidentally, please generate an onboarding code again and re-install the application. A certificate will be generated if the re-installation is successful.

Important: If a certificate is revoked, the following will happen:

- Revoked DM Agent certificate - The device is removed from the Device list.
- Revoked Work from Home certificate - All WfH devices connected to the revoked WfH Client are removed from the Device list.
- Revoked Auth Agent certificate - The Auth Agent is removed from the LDAP Authentication profile's Auth Agent node, causing LDAP users to be disconnected.

Download Root CA Certificates

If using a load balancer or Web Application Firewall trust store, you can download the root CA certificate, without including the private key.

1. Login as an administrator.
2. Go to ***System*** and expand ***Security.***
3. Click ***Client Certificates.***
4. Go to ***Certificate Management.***
5. Select the certificate to download.
6. Click **Download Root CA**.
7. Choose a file location to save the rootCA.pem file.

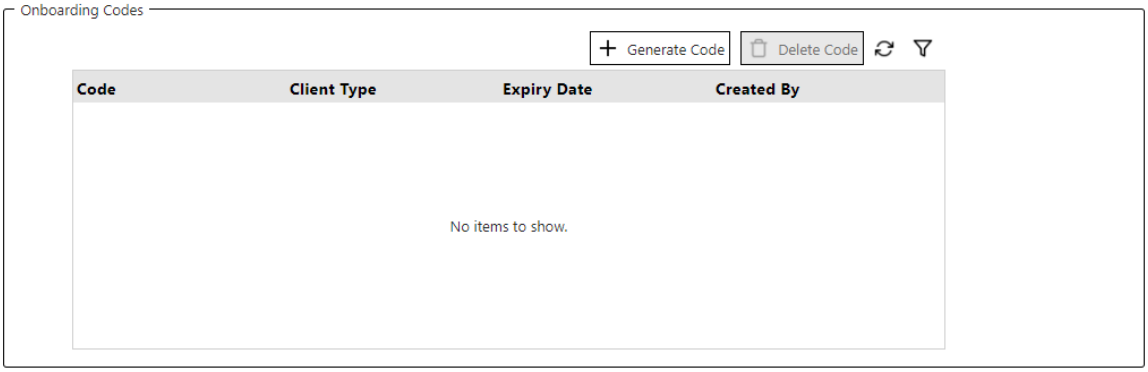
.

Generate Onboarding Codes

Generate time-sensitive onboarding codes to add devices and configure authentication agents.

There are three types of onboarding codes:

- **DM Agent** - The DM Agent Deployment Tool will require this code to deploy RICOH CloudStream Device Management DM Agent embedded to Ricoh devices.
- **Auth Agent** - Use this code to set up the Authentication Agent.
- **Work from Home Client** - Use this code to install the Work from Home Client. The WfH Client enables WfH devices to be added to the CloudStream DM Device List.



Follow the steps below to generate an onboarding code.

1. Login to CloudStream DM as administrator
2. On the left-hand navigation pane, click ***System.***
3. Expand the ***Security*** sub-section.
4. Click ***Client Certificate.***
5. Click **[+ Generate Code].**
6. Enter the onboarding code validity period in hours. Input value from 1 to 24 hours.
7. Select the ***Client Type***. Refer to the above list for types of clients.
8. Click **[Generate Code].**
9. A code is generated and displayed in a dialog; you can click on the code at any time to copy it to the Windows clipboard.
10. Click **[OK].**

Important: The generated code is time-sensitive, so use the code before it expires. If the code expires, you can generate a new code again; just follow the steps above.

Authentication Profiles

Create a profile

Follow the instructions in these topics to create an authentication profile:

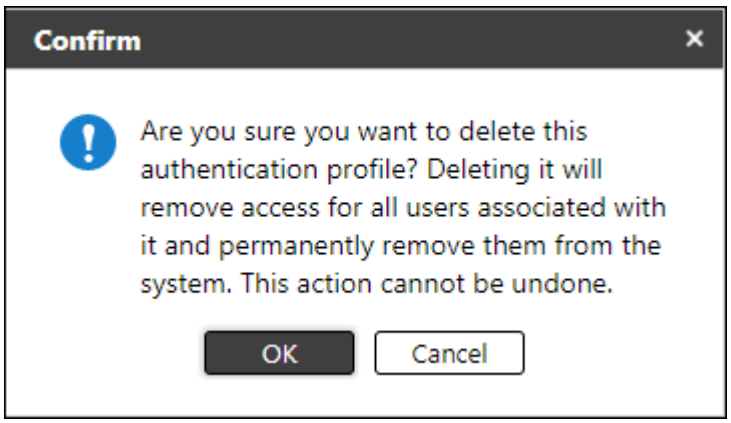
- OpenID Connect Authentication Profile on page 164
- LDAP Authentication Profile on page 151

Delete a profile

Important: Once created, an authentication profile can be deleted, but note the following:

- The action is permanent and there is no Undo function. You must recreate the profile again if necessary.
- Deletion removes access for all associated users, AND removes all associated users from the system.
- Associated groups and departments are also deleted.

1. Login as an administrator.
2. Go to the ***System*** section.
3. Expand ***Security*** and click on ***Authentication Profiles.***
4. Select a profile in the list.
5. Click **Delete.**
6. Read the confirmation message and click **OK** to proceed and delete the profile, or click **Cancel**.



LDAP Authentication Profile

Please perform the following prerequisites before you create an LDAP authentication profile.

Prerequisites
Install the Auth Agent service on a server where an on-site LDAP is configured. An Auth Agent service is also required to be configured if you are planning to add *LDAP Secure* users as administrators. For installation steps, please go to Auth Agent Installation on page 155.
If you are using LDAP Secure, please install the LDAPS server certificate to the trusted root certification authorities certificate store where the Auth Agent is configured.

Follow the steps below to create the LDAP authentication profile.

1. Login as an administrator.
2. Go to the ***System*** section.
3. Expand ***Security*** and click on ***Authentication Profiles.***
4. Click **[Add].**
5. Choose LDAP as type.
6. Enter the name of the authentication profile.
7. Click **[Save].**

   Note: Clicking [Save] will create the auth profile item in the list.

8. Click on the profile and expand the ***LDAP*** node.
9. Provide the following information:

Item	Description
Server Name	Enter the server name. This is a required field.
Port	Enter the port number. The default is 389, and port is a required field. **Note:** If SSL is On, the port number 389 will be automatically changed to 636.
SSL	Enable SSL if required. By default, SSL is off.
Active Directory	Enable Active Directory if required. By default, this item is unchecked. The following are displayed when Active Directory is enabled, please provide value to the required setting:

Item	Description
	• Domain • Alt UPN Suffix
Domain	Enter the domain name of the Active Directory. This setting is required when Active Directory is enabled.
Alt UPN suffix	Enter the UPN suffix of Active Directory users. Add UPN suffixes to user logon processes by providing a single UPN suffix for all users.
Base DN	Enter the start point for searching for an account name. Starting from the base DN, the search is performed toward the end of the branches. Example: ou=member,dc=mycompany,dc=com This item is required.
Search Scope	Specify the range of the search from the base DN. • Single level: The search is performed in the hierarchy that is a level below the base DN. • Subtree: The search is performed in the base DN and all levels in the hierarchy under the Base DN. This is the default option. This item is required.
Search Condition	Enter the search condition. This item is required. The following string is set as the default value: (&(objectClass=organizationalPerson) (sAMAccountName=^)) **Note:** The following characters should be escaped with a backslash (\): "(", ")", "*", "\", "/"
PIN Code Search Condition	Enter the search condition to be used for a user PIN code search. This item is required. The following string is set as the default value: (&(objectClass=organizationalPerson)(PINCode=^)) **Note:** The following characters should be escaped with a backslash (\): "(", ")", "*", "\", "/"
Card Search Condition	Enter the search condition to be used for a user's Card ID search. This item is required. The following string is set as the default value: (&(objectClass=organizationalPerson)(cardID=^)) **Note:** The following characters should be escaped with a backslash (\): "(", ")", "*", "\", "/"
Prefix	Enter the prefix of the LDAP search filter. This setting will become hidden when Active Directory is used.

Item	Description
Suffix	Enter the suffix of the LDAP search filter. This setting will become hidden when Active Directory is used.
Anonymous Bind	Check to enable anonymous binding. This setting is unchecked by default.
Proxy User Name	Enter the name of the proxy user if you want to use a proxy user. This item is not required.
Proxy User Password	Click **[Change Password]**, and then enter the password of the proxy user.
Enable DNS Round Robin	Specify whether or not to enable the DNS round robin function. By default, this setting is enabled. **Note:** The DNS round robin function looks up multiple domain controllers and iterates the list to authenticate the user.
Timeout	Specify the LDAP operation timeout. The default is 5 seconds.
[Test Connection] button	Check whether or not a connection can be established to the LDAP server. A dialog will display to enter your credentials. Enter a working User Name and Password, then click **[Start].** This action will try to connect to the LDAP server and attempt to log in. If ***Use Proxy user*** is checked, the ***Password*** text box will become disabled. This test will bind the Proxy User and retrieve the information of the account entered in the ***User Name*** field.
Login User Name	Enter the attribute to identify the login user name. The default value is "sAMAccountName".
Display Name	Enter the display name. The default value is "displayName".
Email Address	Enter the attribute of the e-mail address of the user. The default value is "mail".
Group	Enter the attribute of the group name. The default value is "memberOf ".
Home Folder	Enter the user home folder attribute. The default value is "homeDirectory".
Card ID	Enter the attribute of the card ID.
User PIN	Enter the PIN code attribute. Only single-byte alphanumeric characters can be used.

Item	Description
Department	Enter the department attribute.
Group Search Mode	Select the method to identify group membership. • Simple Search: Search is performed based on the identifier (DN). • Full Search: Search is performed based on the user login group attribute. The default is Full Search.
Group Name Attribute	Enter the attribute to obtain the group name. Specify this setting when Full Search is selected in Group Search Mode. The default value is "sAMAccountName".
Group Search Condition	Enter the attribute to search for a group. Specify this setting when Full Search is selected in Group Search Mode. The default value is "(&(objectClass=group))".

Note: Click the [Test Connection] button, to check the connection to the LDAP server.

10. Click **[Save].**
11. Expand the ***Auth Agent*** section. Add an authentication agent by moving an auth agent from ***Not Assigned Agent*** pane to ***Assigned Agent*** pane. Use the arrow up button to move the item.

    If an auth agent is not displayed in the list, configure the auth agent as described in Auth Agent Installation on page 155.

    Note: An auth agent can be assigned to multiple LDAP Authentication Profiles. If multiple certificates exist, the Auth Agent shown is the one that uses the latest certificate generated.

12. Click **[Save].**
13. (Optional) Click **[Connection Check]** to test the connection to the LDAP server.

    Enter a working User Name and Password, then click **[Start].** This action will try to connect to the LDAP server and attempt to log in.

    If ***Use Proxy user*** is checked, the ***Password*** text box will become disabled. This test will bind with the Proxy User and retrieve the information of the account entered in the ***User Name*** field.

Note: You can create more than one LDAP type of authentication profile.

Auth Agent Installation

RICOH CloudStream authentications happen in the cloud; however, LDAP and LDAP Secure (LDAPS) cannot authenticate to the cloud without a VPN. Auth Agent is developed to enable onsite and cloud LDAPs to perform authentication in CloudStream DM securely.

You can set up multiple auth agents in your on-premise environment and assign them all to your LDAP authentication profile.

Before you begin, please take note of the system requirements listed below.

Server Requirement for Auth Agent	
Server Requirement	**Minimum:** CPU: Intel Core i5-2300 series or better or Intel Xeon E3 series or better or AMD FX 4200 series or better or AMD Opteron 3200/4200/6200 series or better • Available Memory: 2 GB • Available HDD space: 2 GB **Recommended:** CPU: Intel Xeon E5 v2 series or better or AMD Opteron 3300/4300/6300 series or better • Available Memory: 4 GB • Available HDD space: 3 GB
Operating System	• Windows Server 2022 Std/Datacenter
Virtual Environment	• VMWare EsXi 7.0 • VMWare ESXi 8.0 • Windows Server 2012 R2 Hyper-V* • Windows Server 2016 Hyper-V* • Windows Server 2019 Hyper-V

Follow the order below to set up the Auth Agent.

Order	Instructions
1	Generate the Auth Agent onboarding code. Follow the steps in Generate Onboarding Codes on page 148. **Note:** The Auth Agent onboarding code is time sensitive. Please make sure to configure the auth agent server while the code is valid.
2	Download the auth agent Installer from RICOH CloudStream Device Management by following the steps below. 1. Go to Systems. 2. Click Software Download. 3. Click ***Auth Agent***. The download will start after clicking.
3	Install Auth Agent on page 156.
4	If you are using LDAP Secure, please install the LDAPS server certificate. Install the certificate in a trusted root certification authorities certificate store.

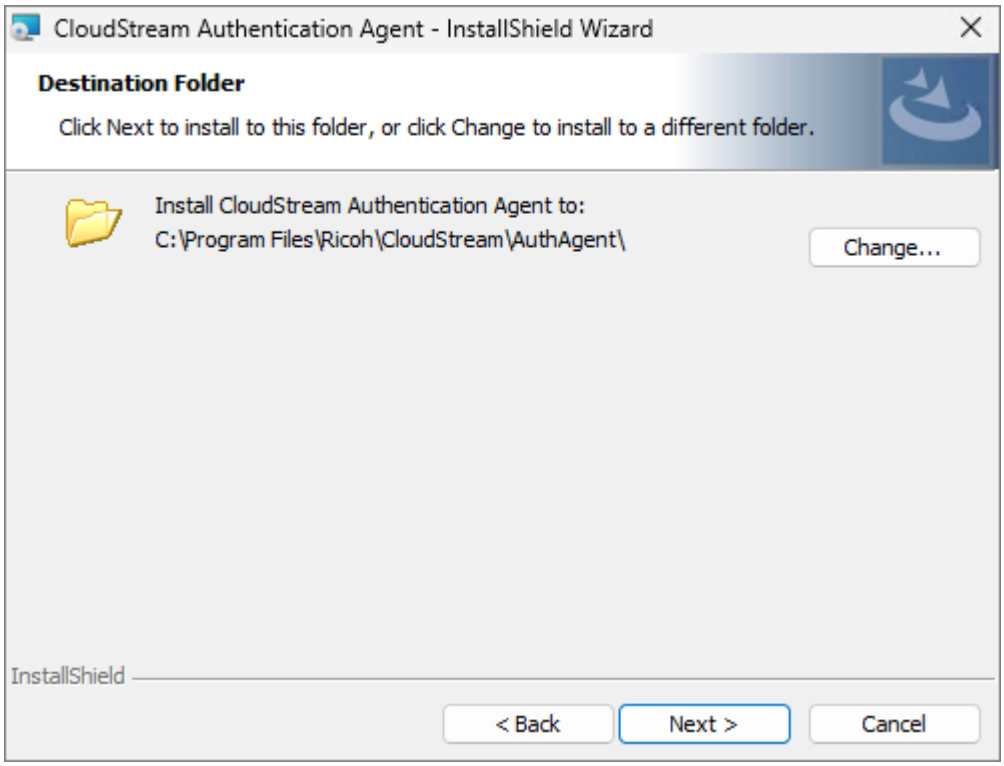
Note: If you want to remove or upgrade an Auth Agent, follow the steps in Remove or Upgrade Auth Agent on page 161.

Install Auth Agent

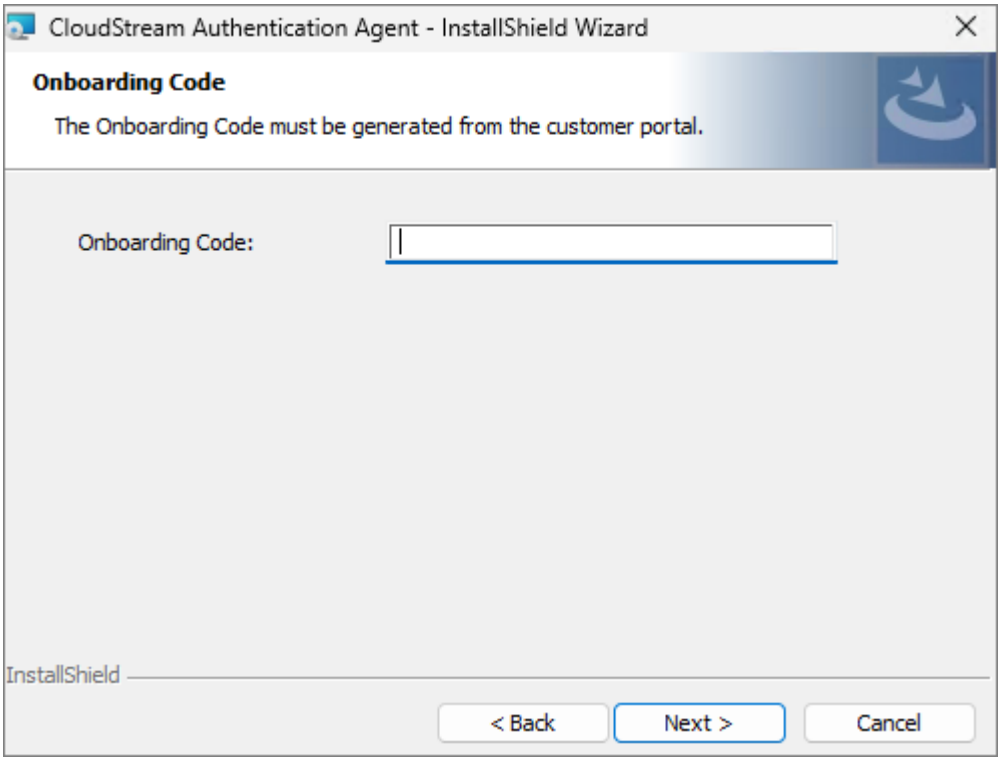
Prerequisites
The tool requires Java Corretto 17 installed on the computer. If a previous version of Java is installed, you must uninstall it before proceeding. The installer will check to determine if Amazon Coretto 17 is installed on the server. If not, a notification message is displayed and you must click Install to proceed. The Auth Agent install will proceed automatically after a successful Corretto install.
Please make sure you have the following information: • Auth Agent onboarding code. Get the code by following the steps in Generate Onboarding Codes on page 148. • Service Locator address. Copy the address from Certificates and Service Locator URL on page 145. • Server port used. • Proxy information if required. • If you are not allowed or cannot use the system account to install the application, please prepare a Windows account that has administrator rights

Prerequisites
to install the application.
You can only install one Auth Agent per computer server. If you want to configure multiple Auth Agents, please prepare one server for each Auth Agent.

1. Run the Auth Agent installer as administrator.
2. In the welcome screen, click **[Next].**
3. Select the destination folder. A folder is selected by default; you can change it by clicking the **[Change...].** Click **[Next]** to proceed.



4. Enter the Auth Agent onboarding code then, click **[Next].**



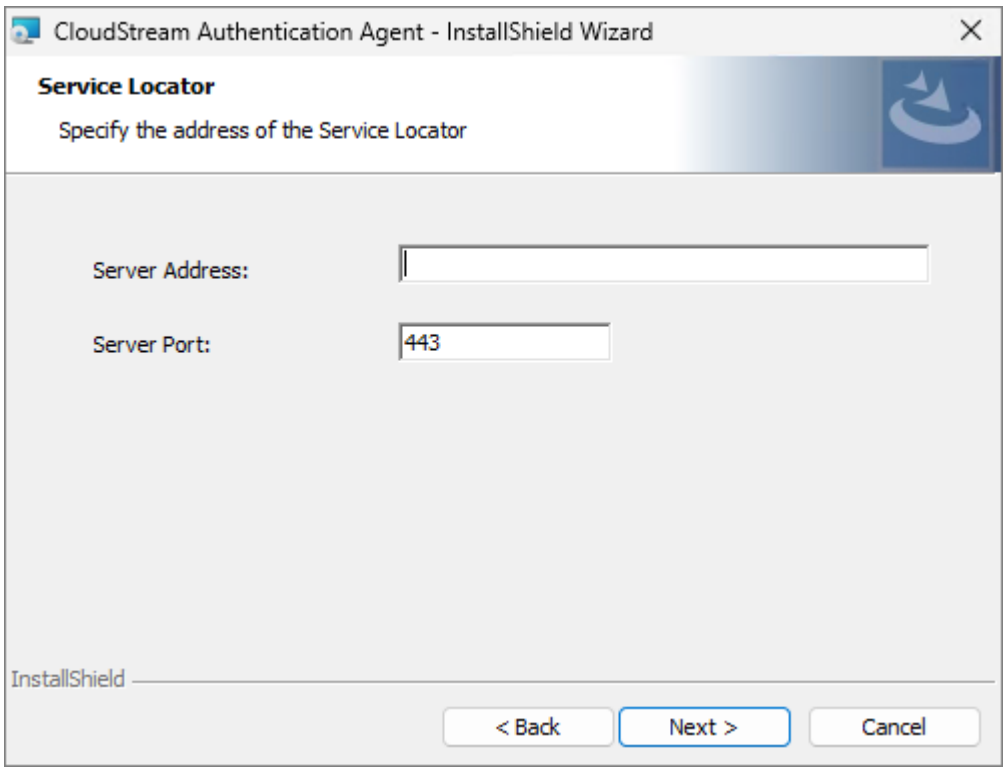
Note: If an invalid or incorrect onboarding code is entered, a pop-up message appears to indicate the problem and prevents the installation. Verify the correct onboarding code and then try again.

5. Enter the Service Locator Address into the ***Server Address*** field.

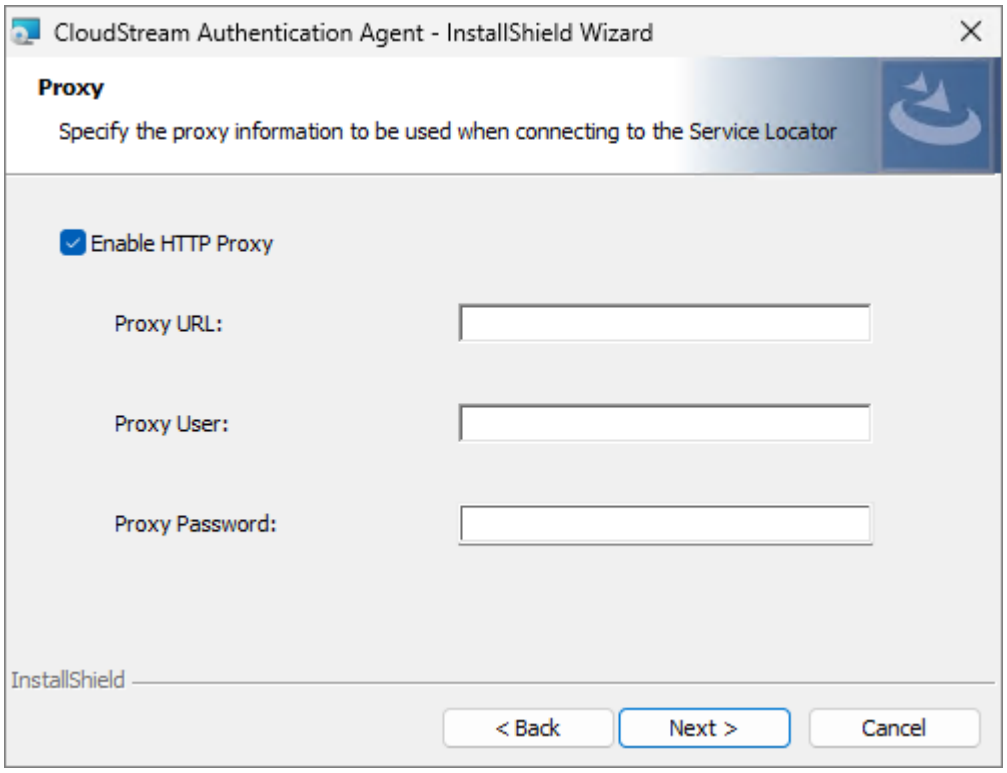
   If you have the Service Locator URL, remove the "http://".

   For Example, if your service locator is "`http://myservicelocator.com:443`", enter "myservicelocator.com" in the ***Server Address*** and "443" in the ***Server Port.***

   Click **[Next].**

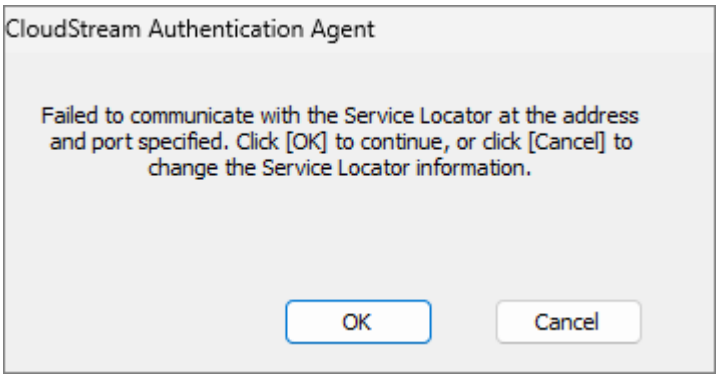


6. (Optional) If you configure the server to use a Proxy Server, please check the ***Enable HTTP Proxy***, then provide the required information.



7. Click **[Next].** Clicking next establishes communication with the ***Service Locator*** using the server address and port you specified.

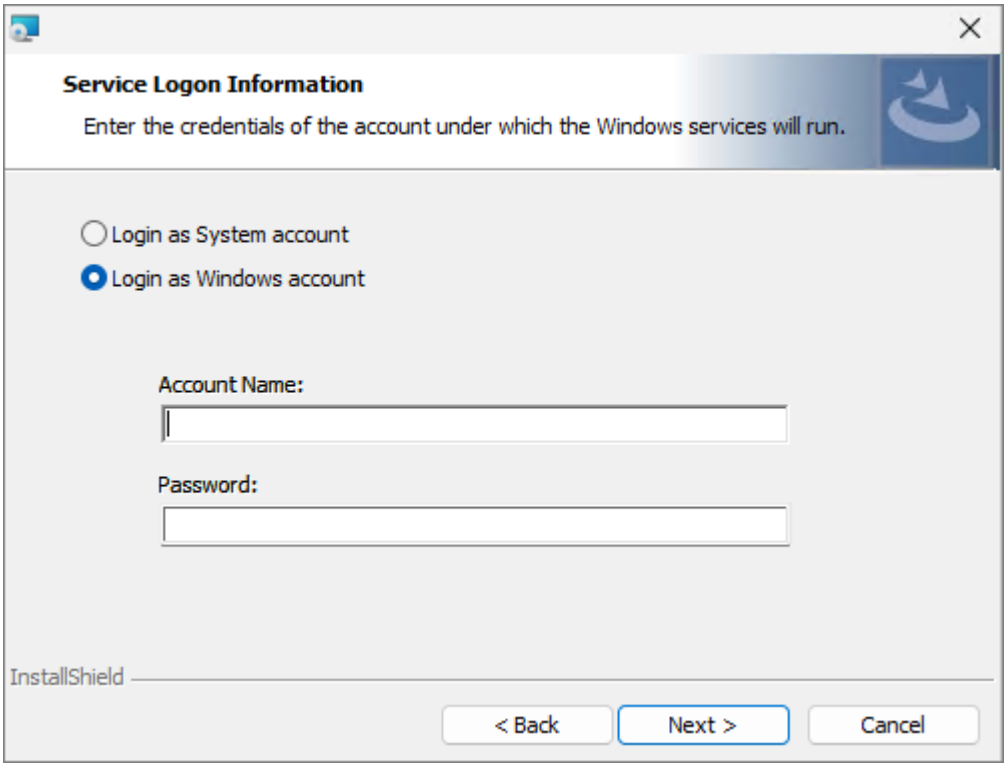
   If the communication fails, an error message will display.



   Please revisit the Server address, port, and onboarding code and make sure the values entered are valid.

8. In the ***Service Logon Information*** screen, please select the type of login you want to use. In this step, you will select the account that has administrator access to the server.

   - If you want to use the system account that you are logged in to, choose **Login as System account.**
   - If you want to input a Windows account, choose ***Login as Windows account.***



9. Click **[Next].**

10. Your auth agent is ready to install; please click **[Install].**

The installer should display a success message and its service must be running.

Note: To check the Auth Agent service, search, and open ***services.msc*** from the Start menu.

Troubleshooting

- If the installation fails, please make sure that the Service Logon Information you provided has administrator rights to install the application.
- If Auth agent is installed, but the service is not running, please run the service manually in services.msc and ensure it is set to run automatically.
- The Onboarding code is time-limited, so make sure the code is valid when installing the auth agent. If you are not certain that the code is valid, please generate a new one.
- If the Auth agent installation fails or the authentication using Auth agent encounters errors, please ensure that the server where the auth agent is running has a stable internet connection.

Check the Auth Agent in CloudStream DM

- **Certificate Management** - Once the auth agent is able to communicate with the service locator, a certificate will be granted to the auth agent. You can find this certificate in ***Systems***, then ***Security***, and click ***Client Certificates***. The auth agent's Client Name is the computer's name. You can use the filter function to filter your search.
- **Auth Agent node in LDAP Authentication Profile** - All certified auth agents will appear in the ***Auth Agent*** node of an LDAP authentication profile. Open an existing LDAP authentication profile or create a new one. Expand the ***Auth Agent*** node and see the auth agent listed in the ***Not Assigned*** pane. Select the auth agent and click the up arrow to assign the auth agent to the profile.

Note: An auth agent can be assigned to multiple LDAP Authentication Profiles.

Remove or Upgrade Auth Agent

A configured Auth Agent establishes a connection to RICOH CloudStream Device Management. Successful communication registers the Auth Agent and assigns a certificate to it. The Auth Agent certificate can be found in ***Certificate Management***.

A certified Auth Agent is displayed in the LDAP authentication profile's ***Auth Agent***, ***Not Assigned*** section.

Upgrade the Auth Agent

To upgrade the Auth Agent, run a newer version of the Auth Agent installer. Enter credentials required for the service to run and then click Install. You do not need to enter the onboarding code if upgrading with this method.

Remove the Auth Agent

Follow the order below to properly remove the Auth Agent from CloudStream DM.

Order	Instructions
1	Please make sure that no LDAP authentication profile is using the Auth Agent. If a profile is still using the Auth Agent, select the Auth Agent from the ***Assigned Agent*** list. Click the down arrow button to move the agent to ***Not Assigned Agent*** list and click **[Save].**
2	Revoke Auth Agent Certificate on page 162.
3	Uninstall Auth Agent on page 163.

Revoke Auth Agent Certificate

1. Login to CloudStream DM as an administrator.
2. Go to ***System***.
3. Expand ***Security*** and click ***Client Certificates.***
4. In ***Certificate Management***, click the filter icon.
5. In the ***Client Type*** column, type "Auth Agent" and then click the filter search icon. You can also press the *'Enter'* key on your keyboard.
6. From the results, look for the Auth Agent's server name and select it.
7. Click **[Revoke Certificate].**
8. Confirm the action to revoke.

The revoked certificate is tagged as revoked in the ***Revoked*** column. An Auth Agent with a revoked certificate will no longer be displayed in the LDAP authentication profile list of available Auth Agents.

Uninstall Auth Agent

1. Login to the server where the Auth Agent is installed.
2. From the Windows start menu, search and open **Programs and Features.**
3. Click ***Ricoh CloudStream Auth Agent.***
4. Proceed to **[Uninstall].**

If you still need to revoke the certificate, you can revoke it after the uninstallation.

OpenID Connect Authentication Profile

CloudStream can connect to the following Identity management services:

- Microsoft Entra ID
- Okta

Please perform the following prerequisites before you create an OIDC authentication profile to connect to either service.

Prerequisites

The OIDC authentication provider must be configured based on the following requirements:

Prerequisites for Microsoft Entra ID and Okta:

- For the Authentication platform, use Web type.
- **Redirect URI** - The redirect URI must be added to the OIDC application's authentication list of Web Redirect URIs.

  The URI can be derived from the CloudStream DM URL which is in format:

  https://**your company domain name**-mauth.region.cloud-stream.ricoh.com/customer.html

  Your redirect URI will be in this format:

  https://{**your company domain name**}-mauth.region.cloud-stream.ricoh.com/login/oauth2/code/

  For example, if the company domain name is 'ABCD' and the region is Asia Pacific, the redirect URL will be:

  https://ABCD-mauth.ap.cloudstream.ricoh.com/login/oauth2/code/

  Note: RICOH CloudStream regions are "ap", "na", "eu", or "ca".
- **Client Secret** - Ensure the client secret is not expired.

Prerequisites for Microsoft Entra ID:

- **Optional and Group Claims** - Optional and group claims should be added.
  - Add "email" claim as ID token.
  - Add "preferred_username" claim as ID token.
  - Add Security group claims:
    - Add an ID token with "GROUP ID"

Prerequisites

- Add an Access token with "GROUP ID"
- Add an SAML token with "Group ID"

- The following configuration is required in Entra ID (Attributes & Claims) and CloudStream to synchronize user information (such as cardid, employeeid, department, etc.). Within the Source Provider, these properties require an equivalent attribute name, which appears in the Source Value dropdown when creating the claim. You will need these Source Attributes in Step 9 below.

CloudStream Attribute Name	Claim Name	Source Attribute
Card ID	Set the Claim name	Select an appropriate source attribute i.e. 'user.extensionattribute1'
Department	If you use the default attribute in CloudStream, set 'department'	If you plan to use the default attribute in CloudStream, set 'department' i.e. 'user.department'
User PIN	Set the Claim Name	Select an appropriate source attribute i.e. 'user.employeeid'

Note: Ensure that the "Source Attribute" matches the purpose of the claim. For example, to pass along the user's cardid value from Entra ID to CloudStream, you might match the "Claim Name: cardid" to a custom attribute in Entra ID.

Prerequisites for Okta:

- **Group Claims** - Add a group claim
  - Group claim type: filter
  - Group claim filter: group that matches regex

Follow the steps below to create an OpenID Connect (OIDC) authentication profile.

Note: Refer to Configure Entra ID OIDC Application on page 168 for general instructions to set up the Entra ID OIDC application.

1. Login as an administrator.
2. Go to the ***System*** section.
3. Expand ***Security*** and click on ***Authentication Profiles.***
4. Click **Add.**
5. Choose OpenID Connect as the type.
6. Enter the name of the authentication profile.
7. Click **Save.**

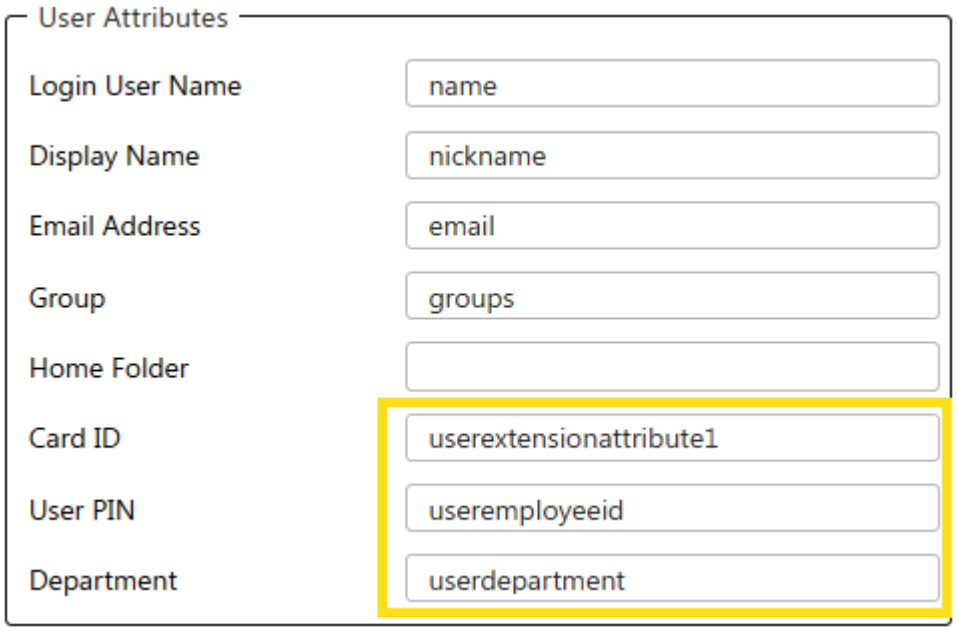
   Note: Clicking Save will create the auth profile item in the list.

8. Expand ***OIDC*** node.
9. Provide the following information to configure the OpenID Connect profile:

Item	Description
Authorization Endpoint	Enter Authorization Endpoint URL.
Token Endpoint	Enter Token Endpoint URL.
JWKS URI	Enter JSON Web Key Set (JWKS)URL.
Issuer	Enter Issuer URL.
Client ID	Enter the Client ID.
Client Secret	Click the **Change Password** button and enter the Client Secret.
Scope	Enter the space-delimited scope values. By default, the value is "openid profile email phone address offline_access". **Note:** If configuring this profile for Okta, ensure you add a scope for 'groups'.
Login User Name	Enter the attribute to identify the login user name. The default value is "preferred_username". **Note:** If you use the document delivery function using a user name and password, be sure to set a deliverable user name attribute for [Login User Name]. The username of job log, job queue, and job history of the scan jobs of the OIDC login user is displayed according to this setting.
Display Name	Enter the display name. The default value is "name".
Email Address	Enter the attribute of the e-mail address of the user. The default value is "email".

Item	Description
Group	Enter the attribute of the group name. The default value is "groups".
Home Folder	Enter the user home folder attribute. **Note:** The Home Folder attribute is not supported for OKTA.
Card ID	Enter the card ID attribute. **Note:** The Card ID attribute is not supported for OKTA.
User PIN	Enter the PIN code attribute. Only single-byte alphanumeric characters can be used.
Department	Enter the department attribute. **Note:** The Department attribute is not supported for OKTA.

Enter the Source Attributes from the Service Provider in the specific CloudStream fields, as shown below in the example. Note that these source attributes are examples only and used for demonstration purposes.



10. Click **[Save].**
11. After saving the authentication profile, click **Check connection**.

    The test should return "Connected successfully" message.

    If the test returns an error, check OIDC Check Connection on page 168 for more details.

OIDC Check Connection

A working OIDC authentication profile should return "Connected successfully" message when you click the [Check connection] button.

> **Note:** A connection test for the Okta identity server is not supported and will return the message "OKTA test connection unsupported".

If it returns an error, please check the following:

- 1011: OIDC connection failed - unauthorized_client [Client ID parameters is malformed or incorrect]

  When the client ID parameter is malformed or incorrect, this error will be displayed. Please check if the Client ID you provided is correct.

- 1012: OIDC connection failed - invalid_request [Request parameter (e.g: Token Endpoint) is malformed or incorrect]

  When a request parameter (e.g: Token Endpoint) is malformed or incorrect, this error will be displayed. Please ensure the parameters provided follow the correct form and correct.

- 1013: OIDC connection failed - invalid_client [Connection to token endpoint was successful but the token cannot be acquired successfully]

  When the connection to the token endpoint server is successful, but the token cannot be acquired successfully.

- 1004: Server error processing request.

  This happens when the check connection is executed and the auth profile fields are empty.

Configure Entra ID OIDC Application

Prerequisites
An Entra ID application is created intended for OpenID Connect (OIDC) authentication.

Follow the order of steps below to set up the Entra ID OIDC.

Order	Instructions
1	Create a Client Secret on page 169.
2	Add Redirect URI on page 169.
3	Add Optional and Group Claims on page 170.

Create a Client Secret

1. Login to portal.azure.
2. Open ***Entra ID Active Directory.***
3. Click ***App registrations.***
4. Click the application you created for OIDC authentication.
5. Go to ***Certificates & secrets.***
6. Click **[+ New client secret].**
7. Add a description, then select the secret's expiration.
8. Click **[Add].**
9. Copy the **Value** of the secret. The ***Value*** will not be displayed again when you navigate away from the screen, so keep a copy before you proceed to the next step.

Add Redirect URI

The redirect URI must be added to the OIDC application's authentication list of Web Redirect URIs. To identify the redirect URI of CloudStream DM, you will need to get your CloudStream DM URL.

The CloudStream DM URL is in this similar pattern: https://**your company domain name**.**region**.cloudstream.ricoh.com/customer.html

Note: RICOH CloudStream regions are "ap", "na", "eu", or "ca".

Please note on **your company domain name** and **region**.

Your redirect URI will be in this format: https://**your company domain name**-mauth.**region**.cloudstream.ricoh.com/login/oauth2/code/

Add the URI by following the steps below.

1. In the Entra ID application, click **[Authentication]** in the left-side menu.
2. If ***Web*** platform is not yet added, click **[Add a platform]**, then choose ***Web***. Add the redirect URI then click **[Configure].**
3. If ***Web*** platform is already added, please go to the ***Web*** section, and in ***Redirect URIs***, click **[Add URI].** Input the redirect URI then click **[Save].**

Add Optional and Group Claims

1. In the application, click **[Token Configuration]** in the left-side menu.
2. Click **[+ Add optional claim].**
3. Add an ID token with "Group ID"
4. Add an Access token with "Group ID"
5. Click **[Save].**

Administrator Roles

Each local admin account is assigned to one or more admin roles. All admin roles are built-in, but you can customize the privileges assigned to each role, with the exception of the Full Admin role.

Note: There are a default set of privileges assigned to the built-in roles. Even accounts assigned Full Admin or Security Admin cannot edit the default set of privileges assigned to these built-in roles.

A role can be assigned to an LDAP group or OIDC group; however, local admin accounts can be assigned to multiple roles.

This section will discuss the following topics:

Terminologies

- **Admin Account** - Local admin who logs in to CloudStream DM to carry out admin tasks. Each account can have one or more admin roles.

  For example, an admin account that manages the devices and manages the application users.

- **Admin Role** - There are nine admin roles, each with a different set of privileges.

  Here is a list of roles.

  Note: Refer to Flexible Administrator Role on page 174 for instructions to enable the role on target devices.

Admin Roles

Role	Description
Full Admin	Can do everything.
Device Operator	Can view all information associated with a device.
Device Basic Admin	Can read all information associated with a device and update basic write operations.
Device Admin	Read/Write all information associated with a device.
User Operator	Can fully access all read privileges associated with users.
User Admin	Can fully access all the read/write privileges associated to users.
Security Operator	Can read user and security profiles to the system. Can read software audit log.
Security Admin	Can add user and security profiles to the system. Can read software audit log.
Report User	Can create, run, and schedule reports.
@Remote CE	Read/Write all information associated with @Remote.

- **Privileges** - There are twelve types of privileges. The privileges granted to each role will determine the type of access the users of the role have. The types of privileges are:

Privileges	Description
SysConfigRead	Display the system settings information.
SysConfigWrite	Update system settings (other than the role, user, LDAP/OIDC profile of a user)
SecurityRead	View the role, user, LDAP/OIDC profile of a user
SecurityWrite	Update the admin roles, use LDAP/OIDC profile of a user.
DeviceBasicWrite	Create/update/delete polling tasks and related tasks. Create/update/delete device groups. Change device access accounts and custom properties. Update e-mail address lists
DeviceAdvancedWrite	Create/update/delete device settings, SDK/J Platform and Embedded Applications Add/update/delete structure change notification policies. Update device drivers
UserRead	View user information
UserWrite	Create/update/delete user information
DeviceRead	View device information
Reports	Create/update/delete/configure schedules for reports

Assign a Group Name to a Role

1. Login to CloudStream DM as an administrator.
2. Go to ***System***.
3. Expand ***Security*** and click ***Admin Roles.***
4. Select the Admin Role you want to assign to the external users when they login to CloudStream DM.

   Note: If you assign a group to an admin role, all users that belong to the group will inherit the role when they login to CloudStream DM. You can only assign one group to a role.

5. If the authentication profile is an LDAP, enter the LDAP group name in the Group Name text field.

6. If the authentication profile is an OIDC, enter the Object ID in the Group Name text field.
7. Click **[Save].**

Edit Privileges and Users

Important: You cannot edit the role type that is assigned to the default Full Admin account. This is cautionary to prevent lockout from the system if only a single Full Admin account exists. If the account is deleted inadvertently, you must contact your Ricoh Support Team for assistance.

1. Login to CloudStream DM as an administrator.
2. Go to ***System***.
3. Expand ***Security*** and click ***Admin Roles***.
4. Select the role you want to modify.
5. Go to ***Privileges*** node.
6. Apply your changes by enabling and disabling the privileges for the role.
7. Click **[Save].**
8. Go to the ***Users*** node.
9. Click the local admin users you want to assign to the role.

   By doing so, the role will also display in admin accounts' role information.
10. Click **[Save].**

Flexible Administrator Role

The Flexible Administrator role (FAR) provides a security role with Custom Privileges for the MFPs. This role is used to limit machine privileges in cases where you want to:

- Limit a user group to update firmware only or to change email settings, protocols, or firmware
- Avoid using one of the four shared Admin accounts on the MFP

FAR authenticates with accounts from OIDC or LDAP, and there is no limit on the number of accounts assigned this role because it is based on group membership.

A user with both general 'user' and Flexible Admin privileges can login to the MFP as a general user, but can switch to a Custom Privilege role to access and configure pre-determined device functions.

Prerequisites

- The DM Agent must be installed on the target models. Refer to Add Devices to CloudStream DM on page 27. Prior to installation, refer to Flexible Admin Role - Supported Models on page 185 to confirm the support list.
- Directory service accounts must be configured to connect to CloudStream. Refer to OpenID Connect Authentication Profile on page 164 or LDAP Authentication Profile on page 151.
- A dedicated group for the Flexible Admin Role must be created within your directory service. This group will be used by the CloudStream Embedded App to authenticate user permissions.

Flexible Admin Role Configuration Procedure

To configure the Flexible Admin role, you must complete the following steps in the order shown below.

Order	Instructions
1	1. Install the Firmware on page 175
2	2. Set the Administrator Authentication on the Devices on page 175
3	3. Enable Custom Privileges on page 177
4	4. Enable External Administrators on page 177

Order	Instructions
5	5. Configure Templates and Groups on page 178
6	6. Test the Setup on page 182
7	7. Disable the Built-in Admin Access on page 183 (Optional)

1. Install the Firmware

Support for the Flexible Admin Role requires specific firmware. You can install the firmware package using the Cloudstream DM portal OR via WIM.

Important: Before proceeding, refer to Flexible Admin Role - Supported Models on page 185 and confirm the models that support this firmware.

Refer to Firmware Template on page 256 to add the package to a template, and then Create a Configuration Task on page 272 and Run a Configuration Task on page 277 to apply this firmware template to the target devices.

The firmware is available from your regional Ricoh Support site (listed below). On the download page, select the target device, and then look for the Firmware Update Tool.

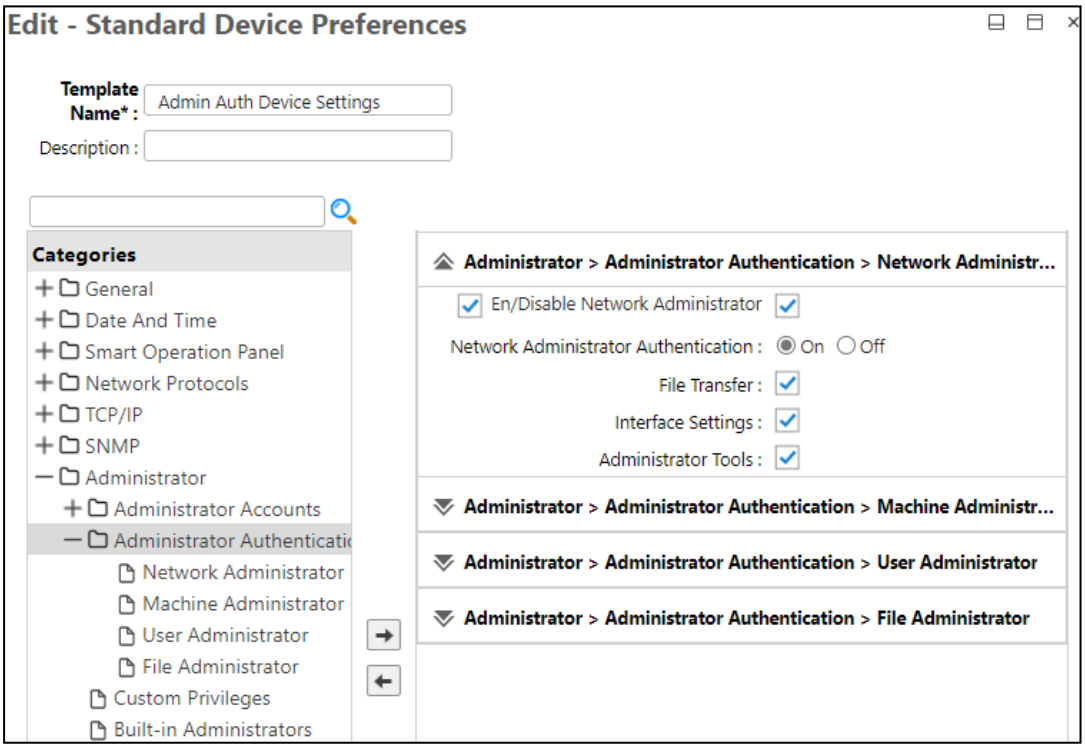
- RCA: https://www.ricoh.ca/en-CA/support-and-download
- RUS: https://www.ricoh-usa.com/en/support-and-download
- RE : https://www.ricoh-europe.com/support/drivers-and-downloads/
- RA: https://www.ricoh-ap.com/downloads

2. Set the Administrator Authentication on the Devices

You must create a Standard Device Preferences (SDP) template that enables all Administrator Authentication preferences on the target device(s), including network, machine, user, and file administrator settings. After creating the template, you can create and run a configuration task to update these preferences on the target device (s).

Note: You can also perform this procedure in WIM. These settings are located under Device Management →Configuration →Device Settings → Administrator Authentication Management.

1. Login as administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences***.
4. Create a blank template in Standard Device Preferences (SDP) on page 238
5. Expand the **Administrator** category and then click **Administrator Authentication**.
6. Click Add  to move the following four subcategories to the right for editing:
   - Network Administrator
   - Machine Administrator
   - User Administrator
   - File Administrator



7. In all four subcategories, **enable ALL options** (as shown in the screen capture above).

Note: Options unchecked in the subcategory are considered outside of the Administrator's control and can be controlled by the general user.

8. **Save** the template.
9. Create a Configuration Task on page 272 and then Run a Configuration Task on page 277 to apply this template to the target devices.

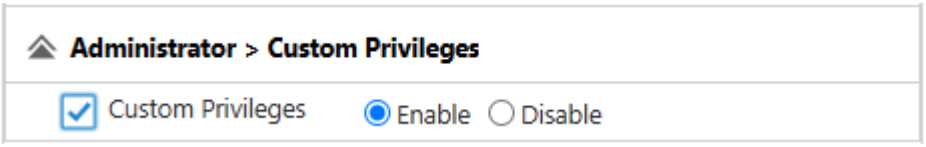
3. Enable Custom Privileges

You can now enable the Flexible Admin role on each MFP via a Standard Device Preferences (SDP) on page 238 template.

Note: For the following device models, Custom Privileges are enabled by default. If configuring FAR on these models, skip this step and proceed to 4. Enable External Administrators on page 177: IM C2010/C2510/C3010/C3510/C4510/C4510A/C5510/C5510A/C6010.

Follow these instructions to create the template:

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
3. Click +Add and choose the option to Create Blank Template.
4. Expand the **Administrator** category and then click **Custom Privileges**.
5. Click Add  to move the setting to the right-hand pane and adjust the preference.
6. Click the [Custom Privileges] checkbox and ensure the [Enable] option is filled.



7. **Save** the template.
8. Create a Configuration Task on page 272 and then Run a Configuration Task on page 277 to apply this template to the target devices.

4. Enable External Administrators

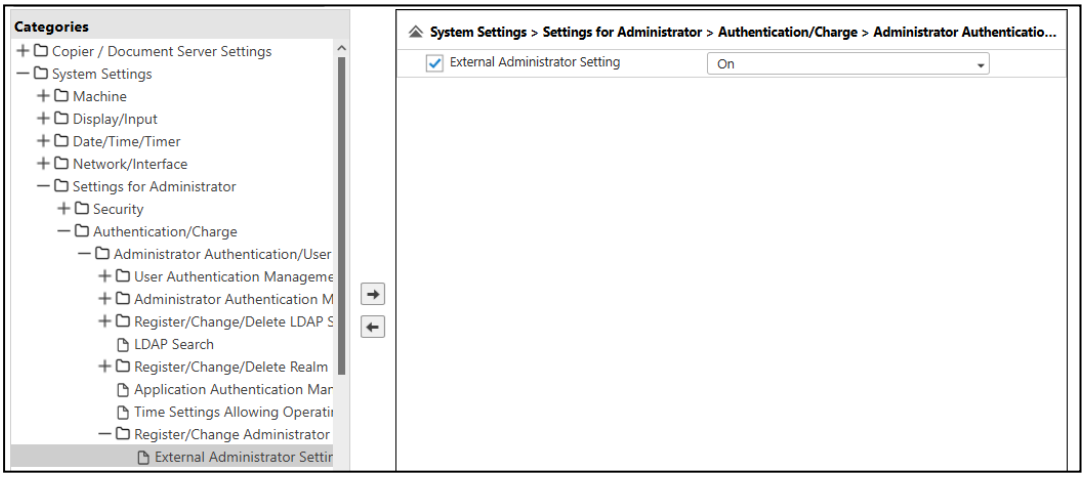
To use the Flexible Admin role on the device, you must enable the External Administrator setting via an Extended Device Preferences template.

Note: You can also perform this procedure in WIM. These settings are located under Device Management →Configuration →Device Settings → Program/Change Administrator.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences***.
4. Click **+Add** and then choose the Option to **Get Settings From Device**.
5. Enter a unique name in the **Resource File** field. The settings extracted from the target device will be named after the resource name you enter here.

   Important: You will use this Resource File within the 5. Configure Templates and Groups on page 178 step below.

6. Expand **System Settings** → **Settings for Administrator** →**Authentication/Change** →**Administrator Authentication/User Authentication/App Auth** →**Register/Change Administrator**.
7. Click **External Administrator Setting** and then click **Add**  .
8. Enable the checkbox for **External Administrator Setting** and select **On** from the list.



9. **Save** the template.
10. Follow the instructions in Create a Configuration Task on page 272 and in Run a Configuration Task on page 277 to apply the template you created above to target devices.

5. Configure Templates and Groups

This procedure allows you to create an Extended Device Preferences template that determines the device privileges that are associated with the specific FAR device group created within your OIDC or LDAP directory service.

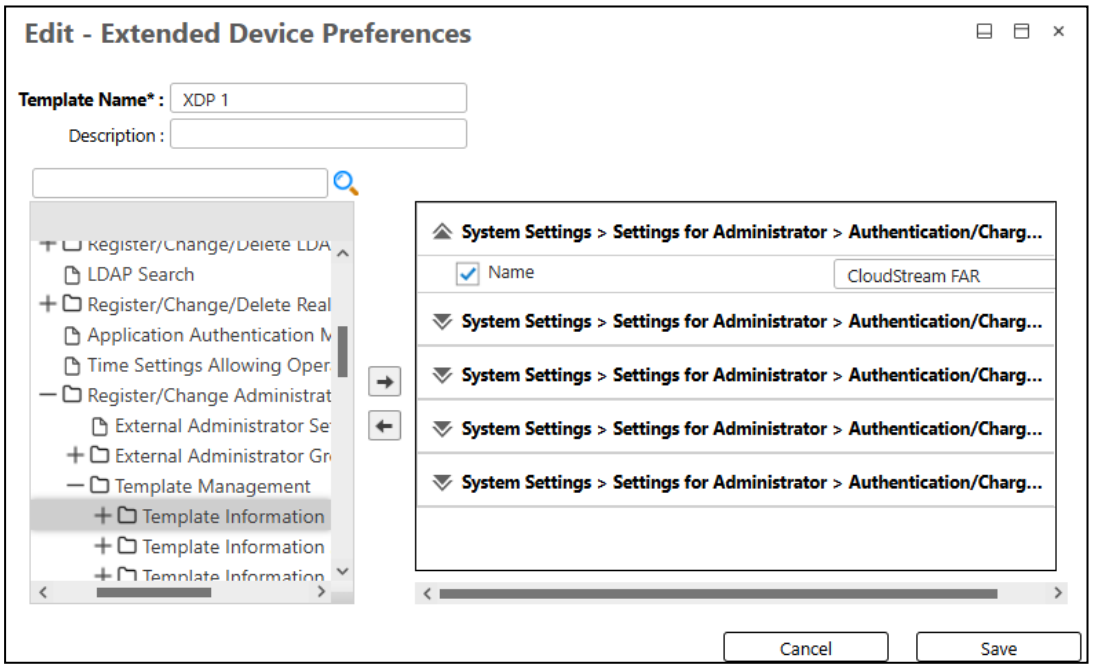
Note: You can also perform this procedure in WIM. These settings are located under Device Management →Configuration →Device Settings → Program/Change Administrator →Custom Privileges.

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
3. Click **+Add** and choose the Option to **Create Blank Template** and select the **Resource file** you created in 4. Enable External Administrators on page 177 above.

To set the Templates:

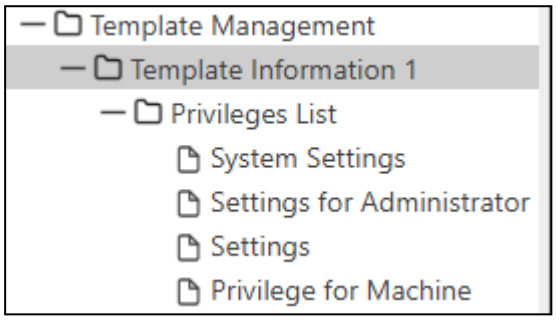
Note: Complete the following instructions for each individual template that you want to create. You can create up to 20 individual templates if necessary.

1. Expand **System Settings** → **Settings for Administrator** →**Authentication/Change** →**Administrator Authentication/User Authentication/App Auth** →**Register/Change Administrator** →**Template Management** →**Template Information 1**.
2. Click **Template 1 Information**, and then click **Add**  .



3. Enter a **name** for the Template.
4. Modify the privileges in the following subsections of the Privileges List. When an option is set to ON, users of this template are able to access these privileges:

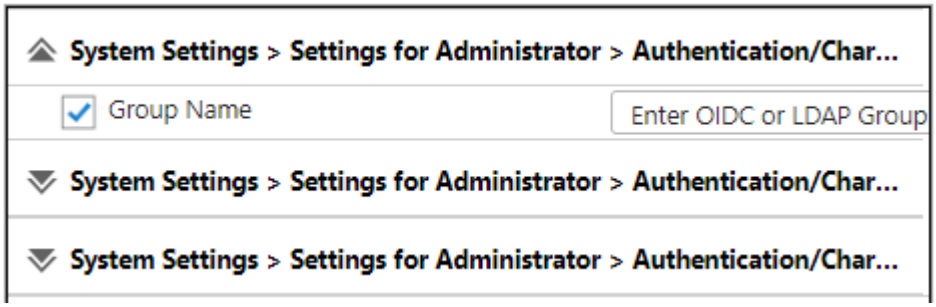
- System Settings
- Settings for Administrator
- Settings
- Privilege for Machine



To set the Groups:

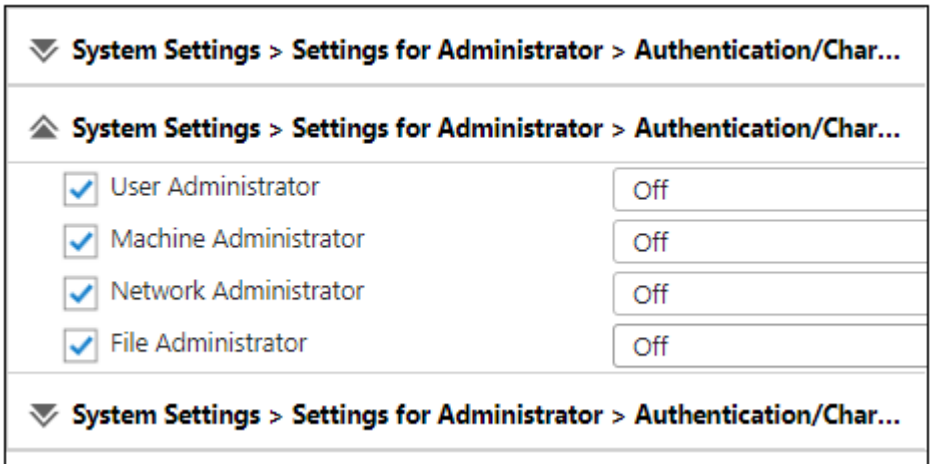
Note: Complete the following instructions for each individual group that you want to create. You can create up to 10 individual groups if necessary.

1. Expand **System Settings→Settings for Administrator→Authentication/Change→Administrator Authentication/User Authentication/App Auth→Register/Change Administrator→External Administrator Group Management**.
2. Click **Group 1**, and then click **Add**  .
3. Enter a group name where the name matches the directory service name:
   - For OIDC, input the Object ID of the group.
   - For LDAP, input the LDAP group name.

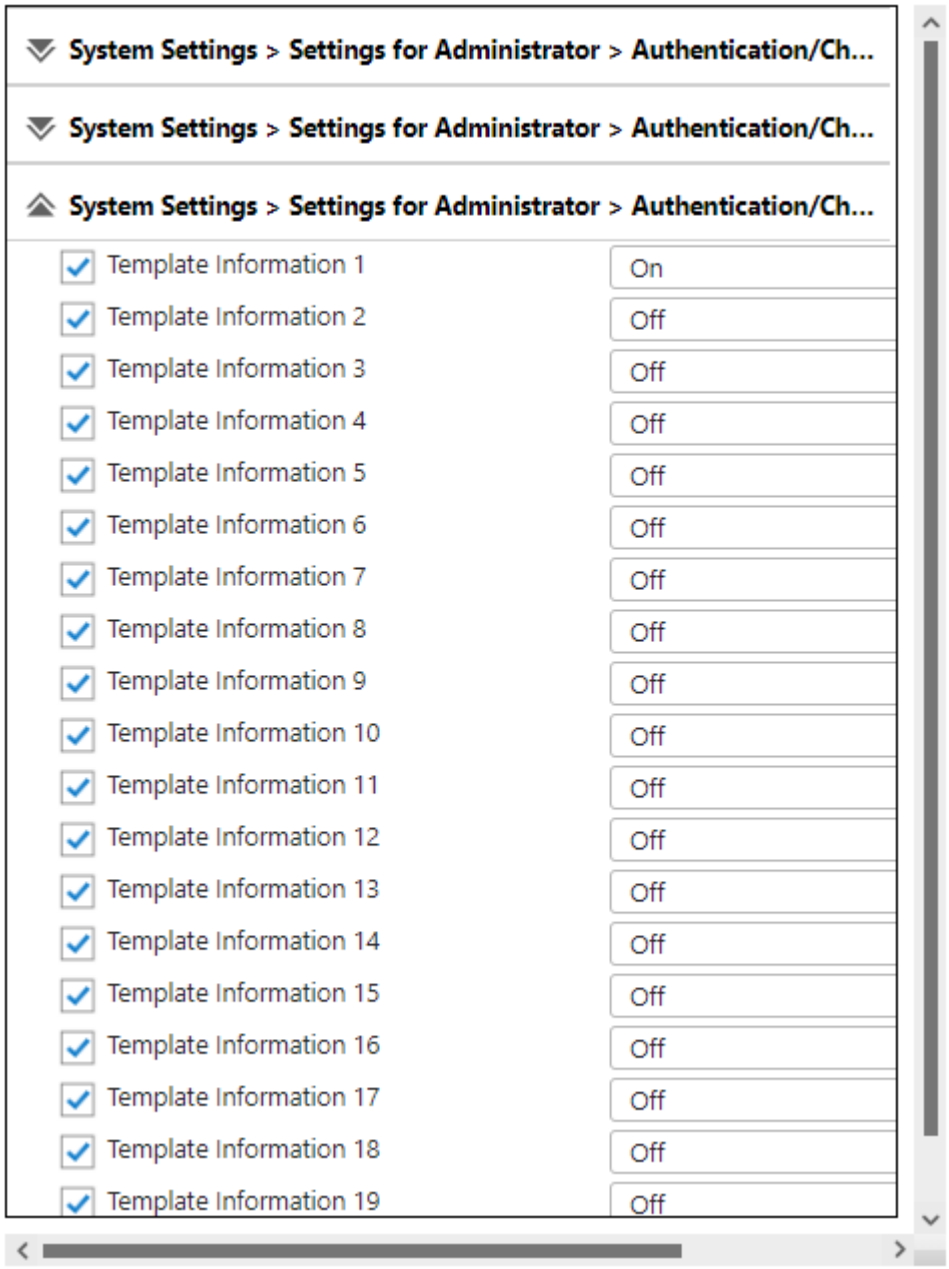


4. Modify the privileges in the subsections of this group.

- **Standard Privileges:** Set to OFF



- **Custom Privileges:** Set to ON, and then select the template that you want this group to use. All other templates must be OFF. When the option is set to ON, users of this template are able to access all privileges within the template.



5. **Save** the template.
6. Follow the instructions in Create a Configuration Task on page 272 and in Run a Configuration Task on page 277 to apply the template you created above to target devices.

6. Test the Setup

To test the FAR access on an MFP, login to the device using a PIN, Card or username/password.

1. After a successful login, tap the **Home** button.
2. Tap the **Menu** icon located on the bottom right of the screen.

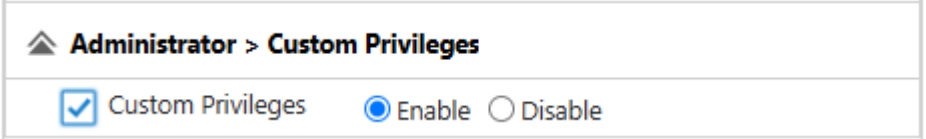
3. Select **Administrator Mode**.
4. If FAR configuration on this device was successful, you will see a screen that asks if you want to switch to the custom-privileges administrator mode.
5. Tap **OK** to proceed.
6. If the group you are assigned to is associated with a template where you can access all privileges, then you can edit all the settings when in Admin mode. If your group is assigned to a template with limited access, then a subset of settings are enabled when in Admin Mode.

7. Disable the Built-in Admin Access

This step is optional and allows you to disable the four shared built-in Admin access accounts to the MFPs for additional security. If you do not disable this account, the four shared Admin accounts can still be used to login and access the device functions.

Important: Before you disable the [Built-in Administrators] ensure that CloudStream can connect to the OIDC or LDAP service to allow device administrator access. You can temporarily re-enable the [Built-in Administrators] option and push the updated template to a device if you need immediate device admin access. Optionally, you can enable the Built-in Supervisor if you decide to disable the Built-in Administrator. This will allow you log into the machine as a supervisor and re-enable the Built-in Administrator, if necessary. You can also re-enable the accounts by pushing an updated template to a device.

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
3. Click **+Add** and choose the Option to **Create Blank Template**.
4. Expand the **Administrator** category and then click **Custom Privileges**.
5. Click Add  to move the setting to the right-hand pane and adjust the preference.
6. Click the **Custom Privileges** checkbox and ensure the **Enable** option is filled.



7. Expand the **Administrator**category and then click **Built-in Administrators**.

8. Click **Add**  to move the setting to the right-hand pane and edit the preference.
9. Click the **Built-in Administrators** checkbox and then click **Disable**.
10. Click the **Built-in Supervisors** checkbox and then click **Enable**. This account will be useful if you need to login and re-enable the Built-in Adminstrator.
11. **Save** the template.
12. Follow the instructions in Create a Configuration Task on page 272 and in Run a Configuration Task on page 277 to apply the template you created above to target devices.

Flexible Admin Role - Supported Models

The Flexible Admin Role is supported on the following models.

Group	Model Numbers
2024 Autumn	IM 6510/C8010
	Pro C5400S/C5410S
2022 Autumn	IM C7010
	IP C8500, C8510
	IM 370F, IM 460F
	IM C2010, C2510, C3010, C3510, C4510, C4510A, IM C5510, C5510A, C6010
	IM C320F
	IM C401F
	IM C3010SD, C3510SD, C4510SD, C6010SD
2020 Autumn	IM2500, IM3000, IM3500, IM4000, IM5000, IM6000
2018 Spring	IM C2000, C2500, C3000, C3500, C4500, C5500, C6000
	IM C300, C400, C400SR
	IM 550, 600 Series

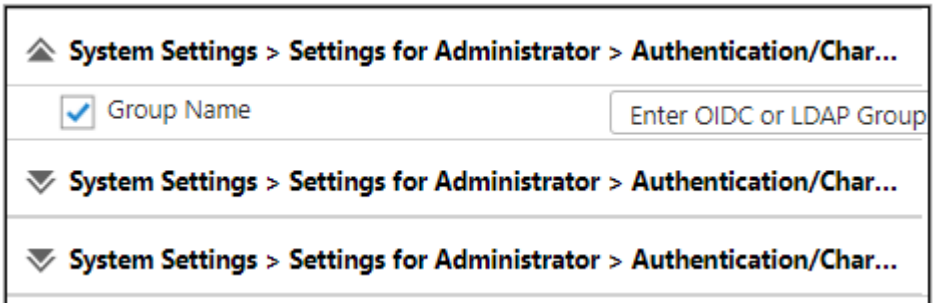
Uninstall the Flexible Admin Role

To remove the FAR functionality from devices, you must follow the order specified below.

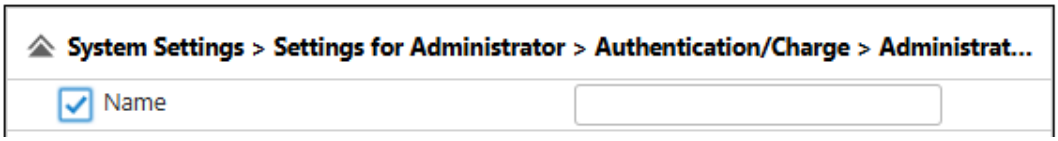
Order	Instructions
1	1. Remove the Group Name and Template on page 186
2	2. Disable External Administrators on page 187
3	3. Disable Custom Privileges on page 188
4	4. Disable the Admin Authentication on the Device on page 188

1. Remove the Group Name and Template

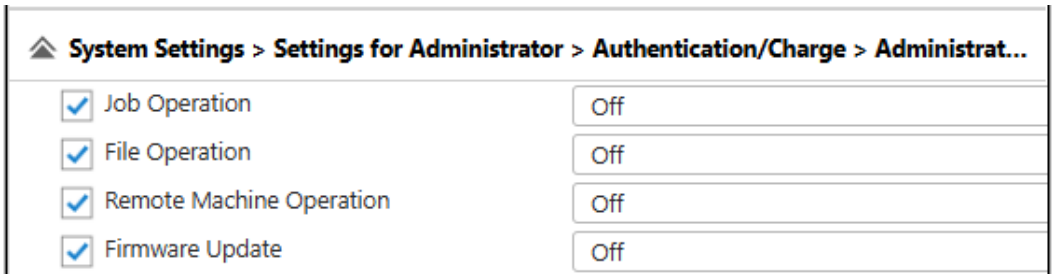
1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
3. Click the Extended Device Preferences template you created in 5. Configure Templates and Groups on page 178 to edit the template.
4. Locate the **System Settings→Settings for Administrator→Authentication/Change→Administrator Authentication/User Authentication/App Auth→Register/Change Administrator→External Administrator Group Management** entry.
5. Check the **Group Name** checkbox and clear the name from the field.



6. Locate the **System Settings→Settings for Administrator→Authentication/Change→Administrator Authentication/User Authentication/App Auth→Register/Change Administrator→Template Management →Template Information 1** entry.



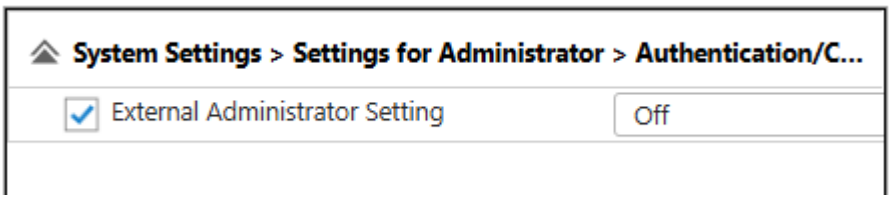
7. Check the Name box, an then clear the name from the Template 1 field.
8. If you previously set any options in the Template's Privileges Lists to On, enable the field and choose Off instead. This includes System Settings, Settings for Administrator, Settings, and Privilege for Machine.



9. **Save** the template.
10. Follow the instructions in Create a Configuration Task on page 272 and in Run a Configuration Task on page 277 to apply the template you created above to target devices.

2. Disable External Administrators

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
3. Click the Extended Device Preferences template you created in 4. Enable External Administrators on page 177to edit the template.
4. Locate the **System Settings→Settings for Administrator→Authentication/Change→Administrator Authentication/User Authentication/App Auth→Register/Change Administrator→External Administrator Setting** entry.
5. Ensure the External Administrator Setting checkbox is enabled, and select OFF from the list.

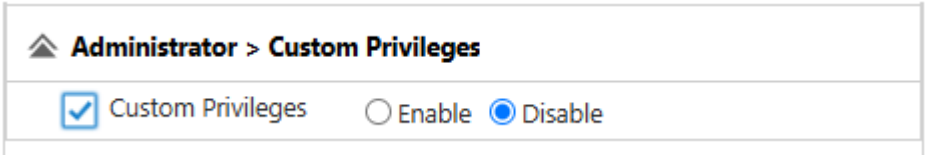


6. Follow the instructions in Create a Configuration Task on page 272 and in Run a Configuration Task on page 277 to apply the template you created above to target devices.

3. Disable Custom Privileges

Note: Custom Privileges are enabled by default and cannot be disabled on the following models:
IM C2010/C2510/C3010/C3510/C4510/C4510A/C5510/C5510A/C6010. If configuring these models, skip this step; otherwise this step will return an error.

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
3. Click the Standard Device Preferences template you created in 3. Enable Custom Privileges on page 177to edit the template.
4. Locate the **Administrator**→ **Custom Privileges** category.
5. Enable the [Custom Privileges] checkbox and ensure the [Disable] option is filled.



6. Locate the **Administrator** category and then click **Built-in Administrator**.
7. Click +Add to the edit the option.
8. Enable the **Built-in Administrator** checkbox.
9. **Save** the template.
10. Create a Configuration Task on page 272 and then Run a Configuration Task on page 277 to apply this template to the target devices.

4. Disable the Admin Authentication on the Device

This step is optional. If continuing to use CloudStream without FAR, do not perform this step.

1. Go to the ***Device Configuration*** section.
2. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences***.

3. Click on the Standard Device Template you created for 2. Set the Administrator Authentication on the Devices on page 175
4. Locate the **Administrator** → **Administrator Authentication** category.
5. For all four subcategories (Network Administrator, Machine Administrator, User Administrator and File Administrator), disable ALL available options.
6. **Save** the template.
7. Create a Configuration Task on page 272 and then Run a Configuration Task on page 277 to apply this template to the target devices.

Administrator Accounts

Administrators manage and configure devices, change system settings, manage certificates, and much more. They can also create other administrators with different levels of access or privileges.

There are two types of administrators.

- Local Administrators on page 190 - The default 'admin' account is an example of a local administrator. As mentioned, you can create other local administrators and assign them to a role.
- External Administrators on page 196 - These types of administrators use an authentication profile to login. Existing admin users from LDAP and OIDC providers can be assigned to a role in RICOH CloudStream Device Management.

Best Practice

Create at least two local administrator accounts, with names that do not have the word admin or administrator in them and disable the default local admin account. These two accounts must be assigned the full admin role. To disable a local admin account, check "Account locked" then click save.

In the event that one account is locked, the other can continue to manage the system and unlock the locked administrator's account.

Here is the list of roles an administrator can be assigned to.

Admin Roles

Role	Description
Full Admin	Can do everything.
Device Operator	Can view all information associated with a device.
Device Basic Admin	Can read all information associated with a device and update basic write operations.
Device Admin	Read/Write all information associated with a device.
User Operator	Can fully access all read privileges associated with users.
User Admin	Can fully access all the read/write privileges associated to users.
Security Operator	Can read user and security profiles to the system. Can read software audit log.
Security Admin	Can add user and security profiles to the system. Can read software audit log.
Report User	Can create, run, and schedule reports.
@Remote CE	Read/Write all information associated with @Remote.

Note: A local administrator can have multiple roles, while the role of an external administrator is determined by the group the admin belongs to. More Admin Roles information is described in Administrator Roles on page 171.

Local Administrators

This section covers the following topics related to local administrator accounts.

Best practice

Create at least two local administrator accounts, with names that do not have the word 'admin' or 'administrato'r in them and disable the default local admin user account. These two accounts must be assigned the full admin role.

In the event that one account is locked, the other can continue to manage the system and unlock the locked administrator's account.

Add Local Administrator

1. Login to CloudStream DM as administrator with Full Admin privileges.
2. Go to ***System***, then expand ***Security***, and click ***Admin Accounts.***
3. Click **[Add]** to display the Add - Admin Accounts screen.
4. Input the user name of the admin account. The user name must not be a duplicate of any existing admin accounts.
5. Click the **[Change]** button to change the password. Input the initial password of the admin account.

   Note: The password must conform to the Local Password Policy; otherwise, the password will not be accepted. Once the account is created, the admin must change their password at first login. You can find the information in Local Admin Password Policy on page 194.
6. Confirm the password and click **[OK].** The password will display masked in the text box.
7. Select the role of the admin account. The role of the admin account will determine the type of access the account will have. You can select multiple roles, or if you plan to give full permission to use all system features, choose "Full Admin".

   This field is required.
8. Input the first name and the last name of the admin account.
9. Enter the email address of the admin account. This item is required.

10. Enter the phone number of the admin account. This item is optional.
11. Click the [**Save**] button.

Once the local admin account is created, please inform the admin user that they can login to CloudStream DM using the user name and password you configured in the above steps. New local administrators are required to change their password at first login.

Login as a New Local Administrator

For first-time login, you must have the following information:

- Access to CloudStream DM URL.
- The user name and password.

Follow the steps below to login.

1. Go to the RICOH CloudStream login site.
2. Leave the Profile empty.
3. Enter the user name and password provided to you.
4. Click **[Login].**
5. For first-time login, a pop-up dialog will display; from there, enter the password given to you.
6. Enter your new password and confirm it.
7. Click **[OK].**
8. After you have successfully changed your password, login again using your new password.

The Dashboard page is displayed after you successfully change your password.

Note: The account will be locked if you input the wrong password more than the set threshold. A Full Administrator account has the access rights to unlock a locked account. Please see details about the account-locked threshold in Local Admin Password Policy on page 194.

Unlock an Admin Account

When an admin account gets locked after multiple failed login attempts, an administrator with Full Admin privilege can unlock the account.

1. Login to CloudStream DM as administrator with Full Admin privilege.
2. Go to ***System***, then expand ***Security***, and click ***Admin Accounts.***
3. Select the admin account you want to unlock.

4. Uncheck the "Account locked" checkbox.
5. Click **[Save].**

Unlocked accounts can log back in to CloudStream DM.

This screen also gives you an option to lock an inactive account; you can do so by checking the "Account locked" checkbox of the account.

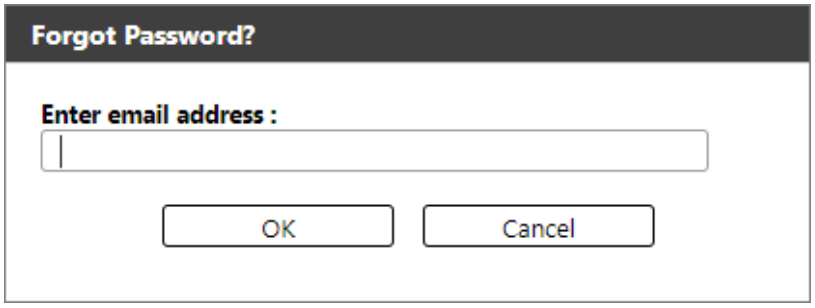
Change Password via Forgot Password

Precondition

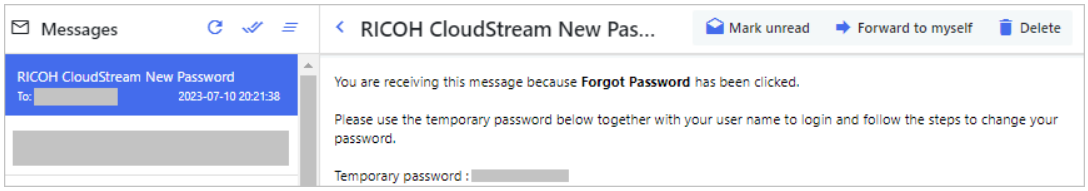
To use "Forgot Password", it is important that the Email Server Settings on page 133 is configured and working. Users who use "Forgot Password" will receive an email containing their temporary password.

Forgot your password? You can change your password using the instructions below.

1. On the RICOH CloudStream login page, click "Forgot Password?".
2. From the dialog, enter your email address registered to the application.



3. Open your email inbox and check the message sent from CloudStream DM. You will receive an email containing your temporary password.



Note: If you can't find the message, please check your spam folder.

4. Go back to the CloudStream DM login page.
5. Enter the username and the password sent to your email address.
6. A dialog will prompt you to change your password; proceed to enter the password.
7. Provide a new password, then confirm it.
8. Click **[OK].**

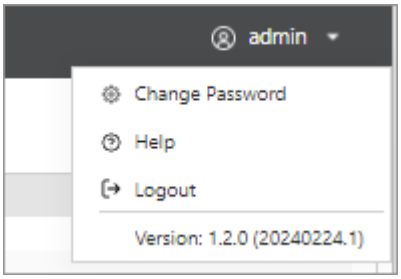
9. After you successfully change your password, login again using your new password.

If the user forgets the password and inputs the wrong password more than the threshold, they can change their password after their account is unlocked.

Change Password from User Menu

You can change your password while logged into the application via the user menu.

1. From the top right corner of the screen, click your username to display the user menu.



2. Select "Change Password".

   A pop-up message will display requiring your current password and the new password.

3. Input your current password and your new password.

   Note: The new password must conform to the Local Password Policy; else the password will not be accepted. Refer to Local Admin Password Policy on page 194 to see the password requirements.

4. Click **[OK].**
5. Logout of the application and login again using your new password.

Local Admin Password Policy

The local administrators' passwords must conform to the local password policy, and the policy applies to new admins or existing accounts that change their passwords.

Note: The password policy does not apply to external administrators and users.

To change the administrator password policy, do the following.

1. Login to CloudStream DM as an administrator with Full Admin privileges.
2. Go to ***System***, then expand ***Security***, and click ***Local Admin Password Policy.***

3. Configure the following settings:

Item	Description
Maximum Password Age	Select the number of days or months before the password expires. The default value is 3 months. Changing the policy will affect all new or existing admin accounts. If the account exceeds the maximum password age, they are required to change their password. It is recommended to change your password every three months.
Account Locked Threshold	Enter the account locked threshold. The default value is 5 times. If a local admin fails to login to CloudStream DM because of an incorrect user name or password, the admin has a specified number of attempts before the account is locked. The number of attempts is the account locked threshold. When an account is locked, another admin must be able to unlock the account by unchecking the "Account Locked" checkbox in System> Security> Admin Accounts. You can specify up to 99 attempts, but it is recommended to allow five attempts only.
Minimum Password Length	Enter the minimum number of characters required in the password. A new admin password will not be accepted if the length is lower than the specified password length. The default value is 9, but you can enter a number from 4 to 128.
Requires Upper Case	When checked, both upper-case and lower-case should be used in the password. By default, this option is enabled.
Requires Numeric Case	When checked, at least one numeric value should be used in the password. By default, this option is enabled.
Requires Special Case	When checked, at least one of the following special characters must be used in the password: {}()[]?!~`<>-@#$%^&+=|\/ By default, this option is enabled.

4. Click **[Save].**

External Administrators

There are two types of external administrators.

- **LDAP administrator** - An external admin who uses an LDAP authentication profile to login to CloudStream DM.
- **OIDC administrator** - An external admin who uses an OpenID Connect authentication profile to login to CloudStream DM.

To allow these external users to login to CloudStream DM as an administrator, follow the instructions for each type.

Setup LDAP type external administrator.

Order	Instructions
1	Install the Auth Agent service on a server where an on-site LDAP is configured. An Auth Agent service is also required to be configured if you are planning to add *LDAP Secure* users as administrators. For installation steps, please go to Auth Agent Installation on page 155.
2	Create an LDAP authentication profile and use the configured Auth Agent. For instructions, please go to LDAP Authentication Profile on page 151.
3	Assign the LDAP group to a role in CloudStream DM. Please go to Assign a Group to a Role on page 197.
4	Login as External LDAP Administrator on page 197.

Setup OpenID Connect (OIDC) type external administrator.

Order	Instructions
1	Create an OIDC authentication profile. For instructions, please go to OpenID Connect Authentication Profile on page 164.
2	Assign the OIDC group to a role in CloudStream DM. Please go to Assign a Group to a Role on page 197.
3	Login as External OIDC Administrator on page 198.

Assign a Group to a Role

1. Login to CloudStream DM as an administrator.
2. Go to ***System***.
3. Expand ***Security*** and click ***Admin Roles.***
4. Select the Admin Role you want to assign to the external users when they login to CloudStream DM.

   Note: If you assign a group to an admin role, all users that belong to the group will inherit the role when they login to CloudStream DM.

5. If the authentication profile is an LDAP, enter the LDAP group name in the Group Name text field.
6. If the authentication profile is an OIDC, enter the Object ID in the Group Name text field.
7. Click **[Save].**

Note: You can assign multiple groups by separating the Object ID or group name with a comma (,).

Login as External LDAP Administrator

1. Go to the CloudStream DM login page.
2. Select the LDAP authentication profile.
3. Enter your user name. Do not include the domain name of your LDAP user account.
4. Input your LDAP password.
5. Click the **[Login]** button.

The Dashboard page is displayed after you successfully login as an LDAP account.

Login Errors

If you encounter an error logging in as LDAP user, please check the following:

- Make sure the LDAP account you login to belongs to the group you assigned to the role. To confirm, please go to the group and check if your account is in the list of members.
- Make sure that the name of the group is used as the role's group name.

- Make sure that the LDAP test connection is successful.
- Make sure that an Auth Agent is assigned to the LDAP authentication profile.

Login as External OIDC Administrator

1. Go to the CloudStream DM login page.
2. Click the **[Login with OIDC]** button.

   The button will not enable if the profile, user name, or password has value.
3. Clicking the **[Login with OIDC]** button will display a page where you can select the OIDC authentication profile you want to be authenticated.

   From the dropdown menu, select the OIDC profile.
4. Login to the OIDC provider with valid credentials.
5. A successful authentication will display the CloudStream DM Consent page. This page will ask for your consent to allow the CloudStream DM service to access your account.

   Please check all three permission to continue using CloudStream DM.

   - profile
   - offline_access
   - email

   Note: After you have given your consent, you do not need to give consent again on your next login.
6. Click **[Submit Consent].**

When a consent is given, you will be redirected to CloudStream DM's Dashboard page. If you did not give your consent or clicked **[Cancel]**, the CloudStream DM cannot sign you in because the service will need all three permissions mentioned in the previous step.

Login Errors

If you encounter an error logging in as an OIDC user, please check the following:

- Make sure the OIDC account you are logging into belongs to the group you assigned to the role. To confirm, please go to the group and check if your account is on the list of members.
- Make sure that the Object ID of the group is used as the role's group name.

- Make sure that correct CloudStream DM URIs are added to the app's Authentication Web URI. Please refer to OpenID Connect Authentication Profile on page 164 for the required configurations.
- Make sure that the authentication profile's ***Login User Name*** value matches the Entra ID application's Optional Claim.

Register Authentication Clients

1. Login as an administrator to CloudStream DM portal.
2. Go to ***System*** and expand ***Security***.
3. Click ***Client Registration***.
4. In the Client Registration page, click **[Add]**.
5. To register a client, you must input the following information.

Item	Description
Client Name	Provide the domain name of the provider you want to register.
Client ID	Enter the Client ID of the authentication provider.
Client Secret	Enter the Client Secret of the authentication provider. Ensure the client secret is not expired.
Redirect URIs	Enter the redirect URI of the authentication provider.
Scopes	Enter scopes of the authentication provider. Example: openid,profile,offline_access,email

6. Click **[Save]**.

Alert Policy

The alert policy helps you monitor the status of devices. When the monitored devices encounter one of the alert triggers set in the policy, CloudStream DM will notify the recipient via email.

You can create multiple alert policies with different trigger configurations and conditions.

Note: Please make sure to set up the Email Server Settings on page 133 prior to creating account policies.

To create an alert policy, follow the steps below:

Order	Instructions
1	Select Alert Triggers on page 201.
2	Configure Notification Condition on page 202.
3	Configure Notification Message on page 205.
4	Add Monitored Devices on page 211.

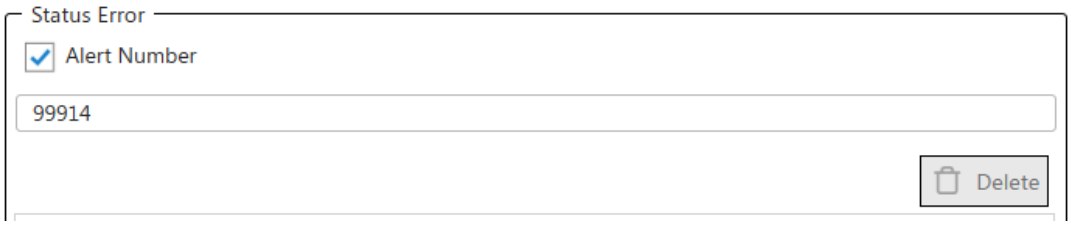
Select Alert Triggers

1. Login as an administrator.
2. Go to ***System*** and click ***Alert Policies.***
3. Click **[Add].**
4. Enter the ***Policy Name***. The name should not be a duplicate of any existing policies.
5. Identify the triggers. You can check multiple triggers. Please see the list below.

Errors	**Warnings**
- Select All (if selected, all items are selected automatically.)	- Select All (if selected, all items are selected automatically.)
- No Toner/Ink	- Offline
- Paper Misfeed	- Toner/Ink Almost Empty
- Call Service	- Alert
- Cover Open	- Replace/Supply

Errors	Warnings
- Device Access Violation - No Paper - No Response - Original Misfeed: ADF - Fax Transmission - Error	- Maintenance - Busy - Almost Out of Paper - Energy Saver Mode - Warming Up

6. Enable a **Status Error**. You can enter one or more status codes to trigger the alert. A notification will be sent when the specified Alert Number appears in the Printer Status Detail. For example, to trigger an alert for "replace WT Box", enable the Alert Number checkbox, and then enter '99914'. If you enter multiple Alert Numbers, a trigger is thrown when any one of the codes match. Please set only ONE Alert Number or ONE Toner Level per Alert Policy, because emails with a supply-specific email subject should be sent to integrate with the MPS order system. Refer to Alert Policy for Brother Consumables on page 208 for more information about using this field.



7. Click **[Save].**

Configure Notification Condition

The ***Conditions*** section determines how the alert notifications will be delivered. There are four conditions for alert notifications options.

A. Notify only if criteria is repeated within specified time interval

Select this if you plan to notify the recipients when the triggers occur the specified number of times within the specified time interval.

When checked, the following will be enabled.

Item	Description
Repeat Count	Enter the threshold count for the times the trigger occurs.
Time Interval	Enter the time interval during which the trigger repeatedly occurs.

Item	Description
	Maximum number • 60 minutes • 24 hours • 7 days

For example, an alert policy is created with the following information:

- Triggers: Cover open
- Condition:
  - ***Notify only if criteria is repeated within specified time interval***
  - Repeat count set to 5.
  - Interval: 1 hour

When the monitored devices encounter Cover Open five times within 1 hour, an email notification is sent to the recipients.

B. Notify only if criteria is sustained for the specified time interval

Notification is sent if there are continuous occurrences within the specified time interval.

When checked, the following will be enabled.

Item	Description
Time Interval	Enter the time interval during which the trigger is sustained. Maximum number • 60 minutes • 24 hours • 7 days

For example, an alert policy is created with the following information:

- Triggers: Service Call
- Condition:

- ***Notify only if criteria is sustained for the specified time interval***
- Interval: 1 hour

When the monitored devices encounter Service Call for 1 hour, an email notification is sent to the recipients.

C. Resend Notification

This condition will resend the notification after the specified time has passed.

Note: Note that you can check this condition with other conditions except for option A.

When checked, the following will be enabled.

Item	Description
Time Interval	Enter the time interval to resend the notification. Maximum number • 60 minutes • 24 hours • 7 days

For example, an alert policy is created with the following information:

- Triggers: Paper Jam
- Condition:
  - ***Resend Notification***
  - Interval: 24 hours

When the monitored devices encounter Paper Jam and the problem is not resolved within 24 hours, a new email notification is sent to the recipients.

D. Notify on cleared conditions

Sends an additional notification once the criteria or the trigger has been cleared.

Note: Note that you can check this condition with other conditions except for option A.

Configure Notification Message

This node allows you create notification messages.

The following languages are supported for the alert policy.

- English
- Français
- Deutsch
- Italiano
- Español
- Nederlands

To create a notification message, follow the steps below:

1. In the ***Message*** section, click **[Add].**
2. Select the language you want to use.

   Note: Please note that after selecting a language, the subject and the body are populated by default values.

3. Modify the subject if necessary. This will be the subject of the alert message sent to recipients.

   Note: Please note the subject can support variables to personalize your notification email. Please see Alert Policy Variables on page 205 to know more.

4. Add the email address of the recipients; you can add as many recipients as you want.

   Note: If you want to create a different message for different recipients, you can create another message item for them.

5. Modify the body of your notification message as necessary. You can use variables to personalize your message or make it more precise. Please see Alert Policy Variables on page 205 to know more about these variables.
6. Click **[Save]**to create the message.

Alert Policy Variables

You can create multiple messages for the alert policy. The messages created in this section will be sent to the specified recipients. You can create an alert policy without specifying any messages, but your contacts will not be notified whenever the trigger

and conditions are met.

The subject and body can be embedded as dynamic parameters using the format $[parameter]$, listed in the table below. These parameters can be selected on the dialog, such as the following:

Subject: **$[discovery_devicecount]$** new devices have been discovered.

Variable Name	Parameter
Device Registered Date	$[device.dev_datecreated]$
Device IP Address	$[device.dev_ipaddress]$
Device MAC Address	$[device.dev_mac_address]$
Device Serial Number	$[device.dev_serialnumber]$
Device Status	$[device.dev_status]$
Device Copier Status	$[device.dev_status_copier]$
Device Fax Status	$[device.dev_status_fax.prev]$
Device Printer Status	$[device.dev_status_printer]$
Device Scanner Status	$[device.dev_status_scanner]$
Device Polling Date	$[device.dev_status_polltime]$
Device Display Name	$[device.displayname]$
Device Customer Property 1	$[device_custom_property.dev_cust_prop1]$
Device Customer Property 2	$[device_custom_property.dev_cust_prop2]$
Device Customer Property 3	$[device_custom_property.dev_cust_prop3]$
Device Customer Property 4	$[device_custom_property.dev_cust_prop4]$
Device Customer Property 5	$[device_custom_property.dev_cust_prop5]$
Device Customer Property 6	$[device_custom_property.dev_cust_prop6]$
Device Customer Property 7	$[device_custom_property.dev_cust_prop7]$
Device Customer Property 8	$[device_custom_property.dev_cust_prop8]$

Variable Name	Parameter
Device Customer Property 9	$[device_custom_ property.dev_cust_prop9]$
Device Customer Property 10	$[device_custom_ property.dev_cust_ prop10]$
Device Status System	$[device.dev_status_ system]$
Device Input Tray Status	$[device_input_tray.dev_ input_status]$
Device Output Tray Status	$[device_output_tray.dev_ output_status]$
Device Printer Version	$[device_ properties.printerversion]$
DOSS Auto Delete Enabled	$[device_properties.doss_ autodelete_enabled]$
Network Host Name	$[device_ properties.system_ systemname]$
System Version	$[device_ properties.systemversion]$
Device WIM Comment	$[device_ properties.wimcomment]$
Device WIM Location	$[device_ properties.wimlocation]$
Toner Level	$[device_toner.dev_toner_ level]$
Toner Level Black	$[device_toner.dev_toner_ level_black]$
Toner Level Cyan	$[device_toner.dev_toner_ level_cyan]$
Toner Level Magenta	$[device_toner.dev_toner_ level_magenta]$
Toner Level Red	$[device_toner.dev_toner_ level_red]$
Toner Level Yellow	$[device_toner.dev_toner_ level_yellow]$

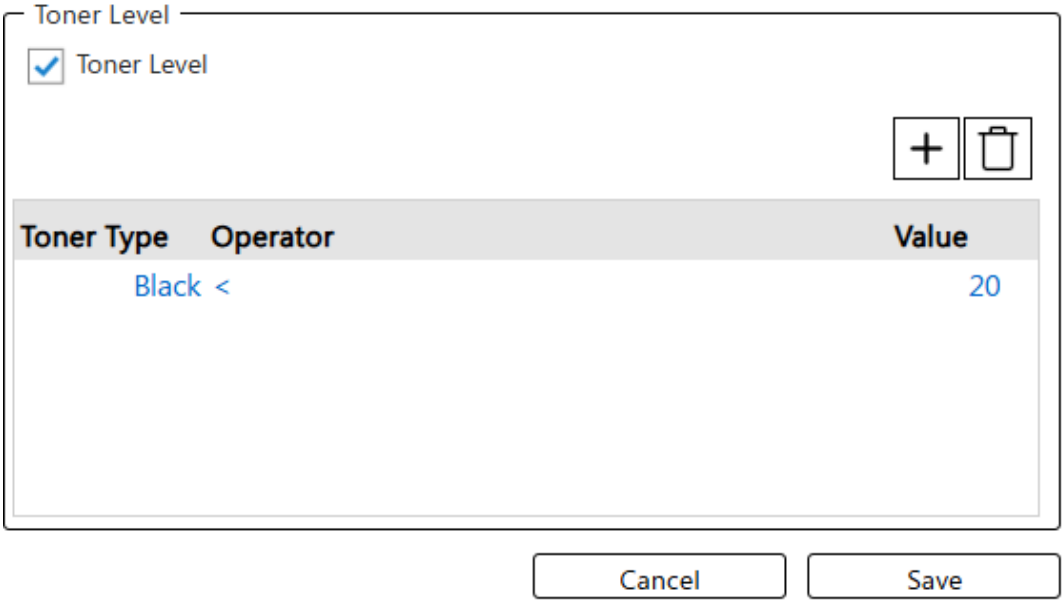
Alert Policy for Brother Consumables

To generate an email that notifies when relevant consumable supplies for Brother devices are needed, specific settings are required to generate the alert details. It is recommended to create an alert policy for each supply needed to integrate Brother MPS.

Note: Please set up the Email Server Settings on page 133 prior to creating account policies.

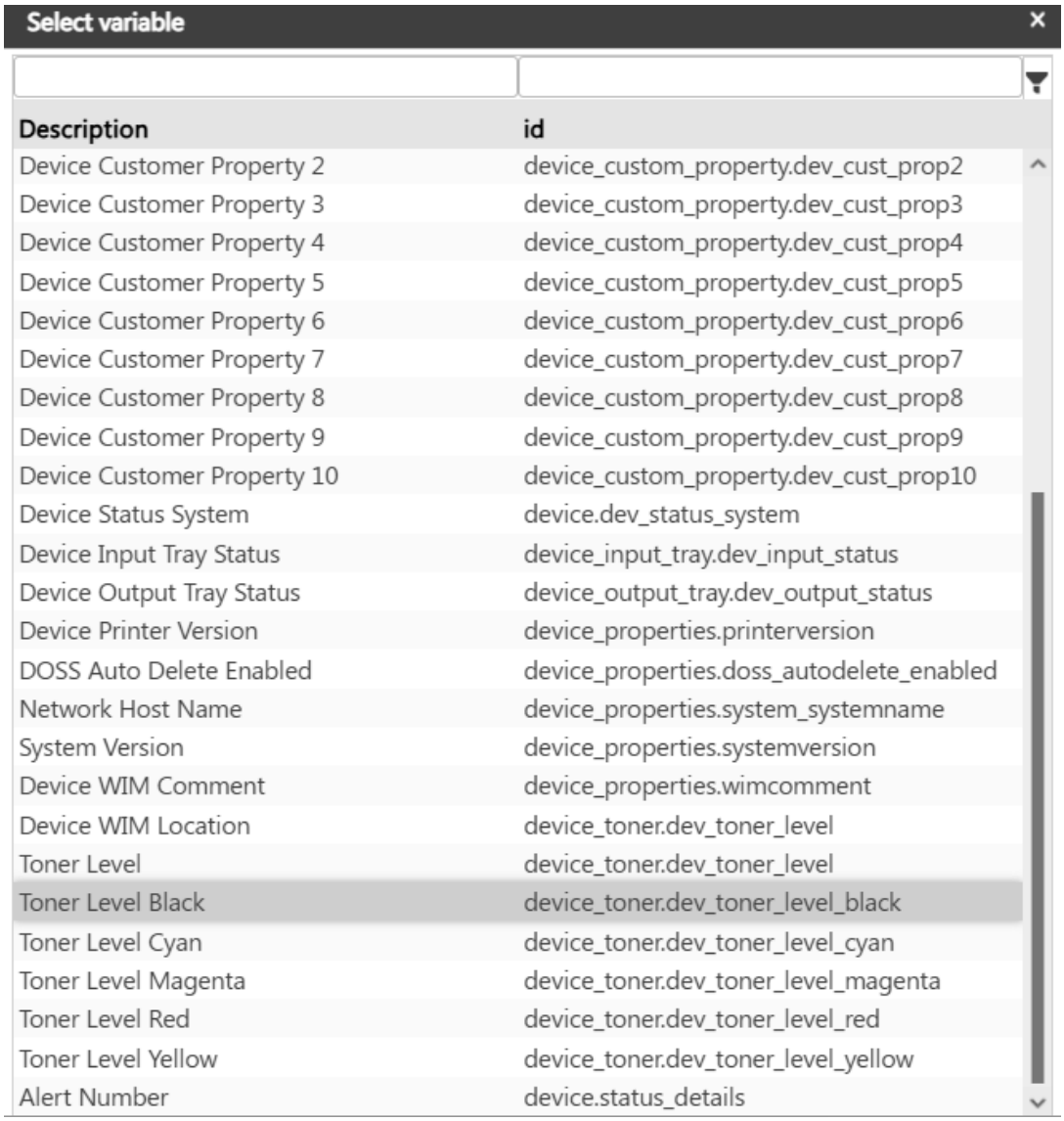
To create an alert notification, follow the steps below:

1. Login as an administrator.
2. Go to ***System*** and click ***Alert Policies.***
3. Click **Add.**
4. In the **General** section, enter the ***Policy Name***.
5. For the **Triggers**, select the criteria that will enable an **Error** or **Warning**.
6. For Other supply alerts (such as Drum/Belt/PF kit options), enable the **Alert Number** checkbox and enter the specific **target status number** from the table below. For example, for Replace WT Box, enter the status code 99901.
7. To set a **Toner** alert, enable the Toner Level checkbox, and then click **+**. A new row appears in the table, and you can click in each column to select the values. In the example below an alert has been created for Black toner when it reaches less than 20%. Remember to click **Save** in the Toner Level section to save each added toner level warning.



Note: If the toner is not set, the Toner/Ink status before removal is displayed. The Toner Almost Empty is displayed when the remaining amount is less then 10% only.

8. Set the conditions.
9. In the **Message** section, click **Add**. Select the Language. Click in the Subject field. The field is automatically populated with default information, including variables. Right-click on a default variable to view a list of replacement variables. The list will pop up on top of the screen and you can choose the suitable variable.



10. Enter the **Email Address** that will receive the message.

11. Modify the body text as needed. The default body uses variables to provide the detected error/warning information that prompted the device state and specific details about the device itself (shown below). You can remove information if it is not relevant.

    _____

    The device status has changed.

    Detected on: $[device.dev_status_polltime]$

    Device Display Name: $[device.displayname]$

    System Status: $[device.dev_status_system]$

    Printer Status : $[device.dev_status_printer]$

    Copy Status: $[device.dev_status_copier]$

    Fax Status: $[device.dev_status_fax]$

    Scanner Status: $[device.dev_status_scanner]$

    IP Address: $[device.dev_ipaddress]$

    MAC Address: $[device.dev_mac_address]$

    _____

12. Click **Save**.
13. Select the Monitored Devices.
14. **Save** the alert.

Target Status

Target Status Number	Description	Subject
99901	Drum End Soon	Status Notification [Drum End Soon]
99902	Replace Drum	Status Notification [Replace Drum]
99903	Belt End Soon	Status Notification [Belt End Soon]
99904	Replace Belt	Status Notification [Replace Belt]
99905	Replace Fuser	Status Notification [Replace Fuser]
99906	Replace Laser	Status Notification [Replace Laser]
99907	Replace PF Kit1	Status Notification [Replace PF Kit1]
99908	Replace PF Kit2	Status Notification [Replace PF Kit2]
99909	Replace PF	Status Notification

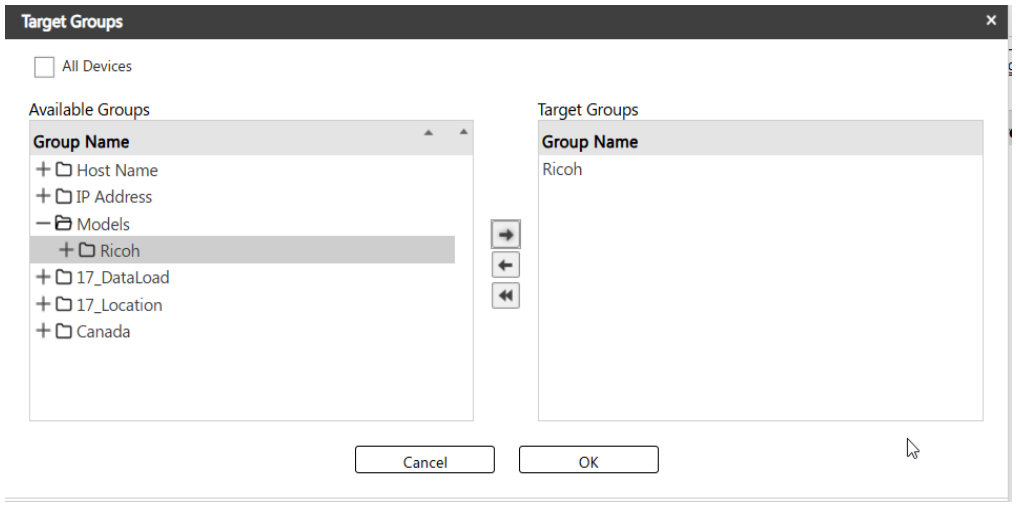
Target Status Number	Description	Subject
	Kit3	[Replace PF Kit3]
99910	Replace PF Kit4	Status Notification [Replace PF Kit4]
99911	Replace PF Kit5	Status Notification [Replace PF Kit5]
99912	Replace PF KitMP	Status Notification [Replace PF KitMP]
99913	WT Box End Soon	Status Notification [WT Box End Soon]
99914	Replace WT Box	Status Notification [Replace WT Box]
	Toner Low (C)	Status Notification [Replace Toner (C)]
	Toner Low (M)	Status Notification [Replace Toner (M)]
	Toner Low (Y)	Status Notification [Replace Toner (Y)]
	Toner Low (BK)	Status Notification [Replace Toner (BK)]
	Replace Toner (C)	Status Notification [Replace Toner (C)]
	Replace Toner (M)	Status Notification [Replace Toner (M)]
	Replace Toner (Y)	Status Notification [Replace Toner (Y)]
	Replace Toner (BK)	Status Notification [Replace Toner (BK)]

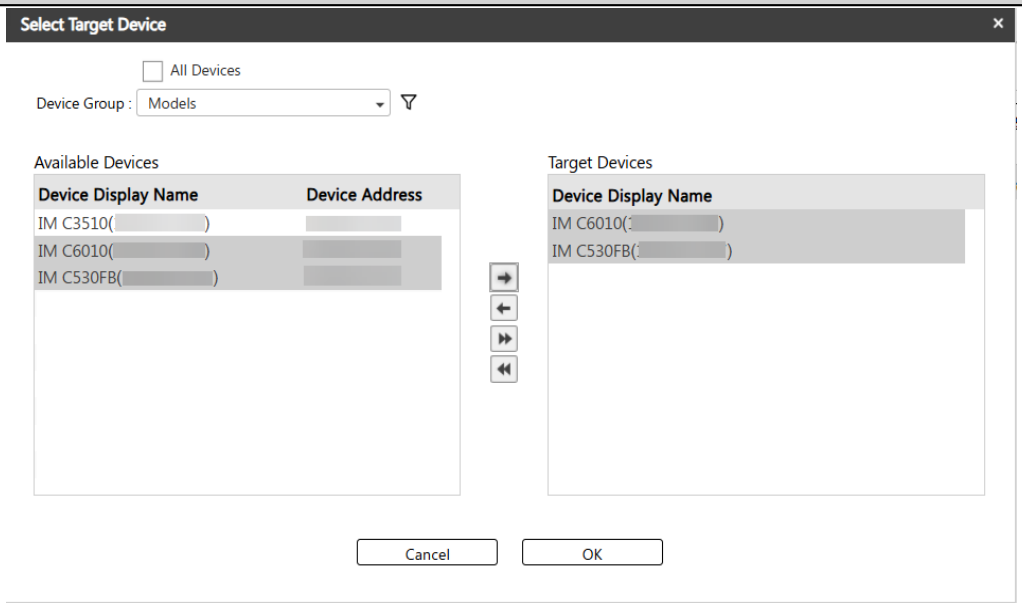
Add Monitored Devices

The alert policy will cover only the devices listed in this section. You can add multiple devices or groups of devices to be monitored.

To add devices to be monitored, you can use the two buttons below to populate the target devices and groups list.

Button	Function
Add Target Group	Clicking this button will display the "Target Groups" dialog. The dialog contains the ***Available Groups*** pane and the ***Target Groups*** pane.

Button	Function
	The list of ***Available Groups*** is based on the Device List groups configuration, whose defaults are Host Name, IP Address, and Models group. The customized groups are also displayed and can be selected as a target group. Like the ***Template*** step, move the device groups from ***Available Groups*** to the ***Target Groups*** pane by clicking the  button. **Note:** If you want to select all devices, you can check the *All Devices* box. Checking this box will add all the devices and or groups to the target devices/groups. 
Add Target Device	Clicking this button will display the "Select Target Devices" pop-up dialog. The dialog contains the ***Available Devices*** pane and the ***Target Devices*** pane. Like the ***Template*** step, use the  button to move devices from ***Available Devices*** to the ***Target Devices*** pane.

Button	Function
	

Filter Devices

For easier selection, use the filter to search for the devices you want to add to the ***Target Devices*** pane.

a. Select a device group.

b. Click the icon and enter the display name or the device's IP address into its corresponding column.

c. Click the bottom icon, or just press enter from your keyboard.

d. Devices that match the search will display in the ***Available Devices*** pane. Select the device from the list.

e. Click button.

You can also perform filtering from the ***Available Devices*** pane.

Note: If you want to select all devices, you can check the *All Devices* box. Checking this box will add all the devices and or groups to the target devices/groups.

System Logs

All logs in the system are stored in the Logs section.

To see the logs, go to the ***System*** section and expand ***Logs*** sub-section. There are five types of logs displayed, listed and described in the sections below.

You also Filter Logs on page 217 and Download logs on page 216 into a CSV file.

Configuration Task Logs

This log presents a consolidated list of all Configuration Tasks pulled from the device activity logs. Administrators can use this log to verify if a Configuration Task has been executed on specific devices.

This log contains the following columns:

- Start Date (including time)
- End Date (including time)
- Task Name
- # Devices: Provides a sum of the Status Columns listed below
- Status Columns: Finished, Started or Queued, Succeeded, Failed or Mismatched

When you click on an entry in the log, the screen splits to show an Activity Log with specific details about the device(s) that were included in the task. Each affected device is listed by Model, IP Address and Serial Number, Activity Type, User, Date and Results. Results can include:

- Success: All of the templates which applied to the device succeeded
- Mismatch: All of the templates which applied to the device is done, however at least one of the item mismatched to the device
- Partial Failure: All of the templates which applied to the device is done, however at least one of the template has failed to apply.
- Processing: At least one of the template is not done. This is for the “End Time“ has not recorded yet.

Click on a device in the Activity Log Detail table to view the specific attribute details affected by the Configuration task.

Alert Policy Logs

The Alert Policy Logs output the activity of alert policies in the system. The history of alert policies in the system can be tracked.

This log contains the following columns:

- Date and time that log is created.
- Alert Policy Name
- Cleared Flag: Check/Uncheck, where “checked” indicates that sending policy is successful on an alert being cleared.
- Email Address: Destination for sending the alert messages.

Audit Logs

The Audit Logs output the changes of the system which the user operates via the user interface. This enables tracking of changes caused by user operations to the system, such as the addition, modification, or deletion of information.

Audit log contains the following columns:

- Date: time that log is created
- Target: Target of the operation. Example: Group, Task, Notification Policy, etc.
- Action: Action of the operation. Example: Add, Update, Delete
- User Name: User name who registers function.
- Details: Details of the operation. Example: {dev_group_type_id=3, dev_group_name=Group A, dev_group_parentid=1}

The Audit Log is generated for the following types of user operation:

- Group
- Filter
- View
- Task/Template
- Access Account
- System Settings

- Authentication and Accounts
- Alert Policies

Authentication Logs

Logs to output the information of authentication on the Server.

Authentication log contains the following column:

- Date: The date/time of the login attempt.
- Type: The type of login. Possible values: Username/Password, PIN, Card swipe.
- User Name: The user who attempted to be authenticated.
- Authentication Profile: Displays the user's external authenticator profile.
- Client Identifier: An identifier for the client from which the login occurred. This will be the Serial Number for an Embedded Device or the Workstation Name of the PC Client.
- Status: Displays if the authentication succeeded or failed.
- Error Code: The error code is displayed here when the authentication fails. The cause of the error is described in the Cause column.
- Cause: Describes the reason for failed authentication.

Report Logs

Logs to output the result of the generated report. The report log contains the following columns:

- Start Time/End Time: The start time when the report task started, and the time when the task completed.
- Task Name: Name of the task that produced the report.
- Schedule Type: The production schedule of the task: Daily, Weekly, Month, etc.
- Task Status: Status may be In Progress, Succeeded, or Failed.

Download logs

You can download logs into CSV file format. Click the icon 

in the top right corner.

A CSV file containing the logs is downloaded immediately. The log's name is in this format <Date and Time>_<Log Type>.

Filter Logs

Use the filter function to find specific log information.

a. Click the  icon.

b. In the column's search box, enter the value you want to search.

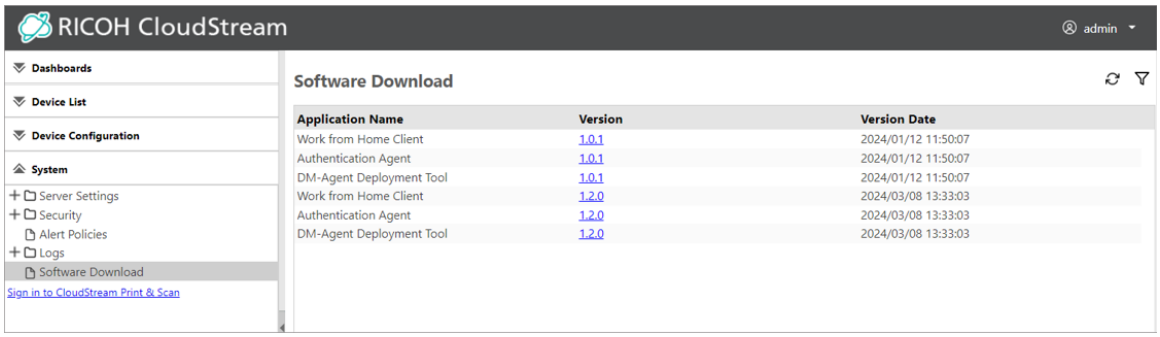
c. Click the bottom  icon or press enter from your keyboard.

The log entry that matches your search is displayed in the list.

To remove the search result list, please delete the values from the columns search box, then click  icon or press enter from your keyboard.

Software Download

In this screen, you can download files that you will need for your device management and configuration.



You can download the following installers from the ***System*** section.

- Work from Home Client
- Authentication Agent
- DM Agent Deployment Tool
- Device Monitoring Service

To download the above installers, please follow the steps below.

1. Login as an administrator.
2. Go to ***Systems.***
3. Click ***Software Download.***
4. In the list, click the version number of the application name you want to download.

The download will start immediately, please check your Downloads folder.

Print and Scan

Print documents securely with RICOH CloudStream Print&Scan license. Registered users can release their print jobs to CloudStream DM-enabled Ricoh devices and perform different secure scan options.

The RICOH CloudStream Device Management (DM) uses a cloud-based print solution that securely stores print data, authenticates users, and deploys customized embedded clients. This centralized print management tool is called the RICOH CloudStream Print&Scan portal, and it focuses on securing and storing print and scan data. The RICOH CloudStream Print&Scan portal is an entirely separate application that collaborates with the CloudStream DM application. If you have acquired a RICOH CloudStream Print&Scan license, you will be given access to the Print&Scan portal so you can configure printer embedded clients and manage printing and scanning operations.

The RICOH CloudStream Print&Scan portal can be opened from the CloudStream DM Systems section. Refer to Configure Print&Scan Embedded Client on page 222 to get there.

Prerequisites
You have a RICOH CloudStream Print&Scan license. Please contact Ricoh sales representative in your region to get a quote.
OpenID Connect (OIDC) Authentication Profile is created. To access the Print&Scan portal, you can either log in from the CloudStream DM portal using your OIDC account or log in directly to the Print&Scan portal using a default local account that has access to the portal. This default account was given to you by Ricoh OpCo when you purchased the Print&Scan license.
Target devices are already added to CloudStream DM.
Target users are registered to CloudStream DM. These users must have access to a client machine where they can send their print jobs.

Follow the steps below to configure device print and scan.

Order	Instructions
1	Login to Print&Scan with OIDC on page 220
2	Assign Print&Scan Administrator on page 221

Order	Instructions
3	Configure Print&Scan Embedded Client on page 222
4	Install Print&Scan Embedded App on page 281
5	Setup the Print&Scan PC Client on page 224

Important: You must use your OIDC account to login to the CloudStream DM portal, then click the link to get redirected to Print&Scan portal. An SSO (Single Sign-on) is activated when you login to CloudStream DM portal, so you do not have to login again in Print&Scan portal.

Login to Print&Scan with OIDC

1. In the CloudStream DM login page, click **[Login with OIDC]**.
2. Select the OIDC profile you would like to be authenticated with.
3. Click the **[Login with OIDC]** button.
4. Proceed to login with the selected authentication provider.

   Successful authentication will log you in to the CloudStream DM portal.

   If you encounter problem logging in, please see Troubleshooting login with OIDC on page 221.
5. Go to **System** node.
6. Click 'Sign in to CloudStream Print & Scan'.

   By clicking the link, you will be redirected to the RICOH CloudStream Print&Scan portal. Since you login as an OIDC external administrator, the system detects your sign-in and automatically logs you in to the portal, so you do not need to provide your credentials.

   It is recommended that you use your OIDC admin account to access the Print&Scan portal.
7. If you are an administrator and have very limited options in your profile, for example, you only see *My profile* and *My documents*, follow Assign Print&Scan Administrator on page 221 to assign access to your OIDC user account.

   Important: The steps found in Assign Print&Scan Administrator on page 221 requires a Print&Scan local user account. The local user credential is given by the Ricoh OpCo. Initially, you are expected to login using a local user with administrator role and provide admin access to the OIDC account you used to log in step 7. After that, you can continue to use your OIDC account with admin privilege to provide other administrators with admin access.

If the other admin is already an administrator, please contact the other admin and request for admin access. You must login via step 7 first before you request for admin access.

For LDAP and local admin account

The CloudStream DM local admin account and LDAP account cannot login to the Print&Scan portal. When LDAP or local admin users click the link, they will see the login screen of the Print&Scan portal. From that screen, they can login using their Print&Scan local user account, which is an account separate from the CloudStream DM portal.

Troubleshooting login with OIDC

- Ensure the admin user's group is added to a role in the system. To know more about roles, go to Administrator Roles on page 171.
- The authentication provider's redirect URI must be correct. For the required configurations, see the precondition in OpenID Connect Authentication Profile on page 164.
- Ensure the OIDC authentication profile is correctly configured. Refer to OpenID Connect Authentication Profile on page 164. If you receive an error message indicating "Please contact your Administrator. The authentication profile may be configured incorrectly", you must contact your Administrator for a resolution before you can login successfully.
- All required permission should be checked before submitting the consent.
- For Entra ID, the client certificate is valid for a 6 month period by default. If the certificate exceeds the period, the user will see the error message indicating "Error: Please check Authentication Profile, you may have set the values incorrectly". To resolve this error, ensure you adjust the Client secret expiry in Entra ID to a longer period of time.

Assign Print&Scan Administrator

Initially, you will be given a local user account with admin access to login to the Print&Scan portal. This account is created so you can assign administrator access to other administrators who login using their OpenID Connect (OIDC) account.

Prerequisites
The OIDC admin account that you are about to assign an administrative role must first login to the Print&Scan tenant using their OIDC account.

Prerequisites

This is an important step so you can search for their email addresses when you create an access control for them.

To login, follow the steps in Login to Print&Scan with OIDC on page 220.

Follow the steps below to assign administrator role to an OIDC admin account.

1. Login to the Print&Scan portal using the local admin user provided by OpCo.

   The Print&Scan portal link will be provided to you by Ricoh OpCo.
2. Once logged in, go to ***Users and access*** and click ***Access control***.
3. In the Access control page, click **[Add]**.
4. In the authentication provider dropdown menu, select the RICOH CloudStream authentication provider.
5. Select "Administrator" as security role.
6. In User or group name, type the email address of the account you wanted to be an admin and click **[Search]**.

   Note: If you cannot find their email addresses, then they must not have signed in successfully to the Print&Scan portal. Please ask them to sign in successfully. Please refer to Login to Print&Scan with OIDC on page 220.
7. In the search result, select the email address.
8. Click **[Save]**.
9. Inform the other admin that their account now has admin access and ask them to sign in again.

Configure Print&Scan Embedded Client

The RICOH CloudStream Print&Scan embedded client must be configured before you can deploy the embedded application to the Ricoh devices.

Note: You can find detailed RICOH CloudStream Print&Scan documentation in Print&Scan.at this link: https://manual.na.ps.cloudstream.ricoh.com/. Copy and paste the URL in a browser.

Prerequisites

Your account is an administrator in Print&Scan portal.

If you don't have admin access, please follow Login to Print&Scan with OIDC on page 220 and request for admin access.

To use the Print&Scan with CloudStream DM, follow the steps below to create or configure the embedded client.

1. In the CloudStream DM login page, click **[Login with OIDC]**.
2. Select the OIDC profile you would like to be authenticated with.
3. Click the **[Login with OIDC]** button.
4. Proceed to login with the selected authentication provider.
5. If this is your first time logging in, you will be asked to submit a consent. Ensure to check all required permission before submitting the consent.

   Successful authentication will log you in to the CloudStream DM portal.

   If you encounter problem logging in, please see ***Troubleshooting login with OIDC*** in Login to Print&Scan with OIDC on page 220.
6. Go to **System** node.
7. Click 'Sign in to CloudStream Print & Scan'.

   By clicking the link, you will be redirected to the RICOH CloudStream Print&Scan portal. Since you login as an OIDC external administrator, the system detects your sign-in and automatically logs you in to the portal, so you do not need to provide your credentials.

   It is recommended that you use your OIDC admin account to access the Print&Scan portal.
8. On the left-hand side, go to the ***Printers*** section and click ***Embedded clients.***
9. Click the edit icon  of the ***RICOH CloudStream Default Embedded***.

   If there is no default embedded client, create a new one by clicking the **[Add]** button.
10. Ensure that the Application Type is ***Standard Gen 2*** and leave device admin and password as is.
11. Select the Type of login the embedded will use. You can choose one of the following:

Item	Description
Card swipe login	When selected, users can only login to the MFP using their registered access card. Refer to Register Cards on page 324 or Register a Card in MFP on page 325 for details.
Short ID login	When selected, users can only login to the MFP using their PIN (Short ID). Their PIN is generated by default when you

Item	Description
	setup the PIN settings. Refer to Configure User PIN on page 321 for details.
Short ID **or** card login	When selected, users can login using their card or PIN. The MFP login screen will display these options to the user.
Username + password login	When selected, users can only login to the MFP by providing their username and password.
Username + password login **or** card login	When selected, users can login using their username and password or by swiping their card. The MFP login screen will display these options to the user.

12. Leave the API Key for installation value as is.
13. Click **[Save].**

Setup the Print&Scan PC Client

The RICOH CloudStream Print&Scan PC Client is a desktop application that automatically creates print queues and installs drivers, allowing users to perform serverless pull-printing from embedded clients.

Note: CloudStream DMdoes not support Direct print queues. Print jobs submitted to a Direct print queue will be processed by the Ricoh CloudStream printer as pull print job.

You can download the installer from the RICOH CloudStream Print&Scan portal overview page. Refer to Configure Print&Scan Embedded Client on page 222 to get there.

Note: You can find detailed Print&Scan PC Client documentation in RICOH CloudStream Client.at this link: https://-manual.na.ps.cloudstream.ricoh.com/docs/ricoh-cloudstream-client. Copy and paste the URL in a browser.

Follow the steps below to configure the RICOH CloudStream Print&Scan PC Client

Order	Instructions
1	Install Print&Scan PC Client on page 225.
2	Login to Print&Scan PC Client on page 227.
3	Print a Document on page 230.
4	Release a Print Job on page 231.

Install Print&Scan PC Client

Prerequisites
RICOH CloudStream Print&Scan tenant's domain name.
Your OIDC account is registered to the CloudStream DM. To register a user, refer to Register Users on page 311.

Note: You can find detailed Print&Scan PC Client documentation in RICOH CloudStream Client.at this link: https://-manual.na.ps.cloudstream.ricoh.com/docs/ricoh-cloudstream-client. Copy and paste the URL in a browser.

1. Run the installer.
2. Read the License agreement and select agree to proceed.
3. Select ***'Advanced installation'*** as the *Installation Type*.

   If you choose *'Quick installation'*, the PC Client application will be installed but you have to edit the *Account Domain Name* and *User Authentication* in Service Configuration dialog after the installation. Refer to Modify PC Client Service Configuration on page 227 for steps.
4. In the Server Parameters screen, enter the following:
   - **Server host name:** Enter the address or host name of the CloudStream server . For “Local" storage mode the address should be the account DNS of the CloudStream primary server.
   - **Account domain name:** Enter the domain name of the target account. It can be found in CloudStream Web UI on the Customer information tab.
   - **User authentication:** Select ***'RICOH CloudStream OAuth2'*** as the *User Authentication*.
   - **Storage mode:** – Select where RICOH CloudStream Client stores the data: Cloud storage, Local storage, or Hybrid (direct print locally, secure print to cloud).
   - **API key:** – Enter the API key from the account settings. If omitted the default (restricted) API key will be used. Default API key will be removed in the future product versions.
   - **Enable secure login for session authentication types:** – Select this option to enable RICOH CloudStream Client registration as an endpoint which must be authorized by the administrator to use insecure login types (such as Session User or User Principal Name).

- **Enable offline installation:** – Enable this option to install RICOH CloudStream Client without registering or checking server connectivity.

5. Select
6. Click **[Next].**

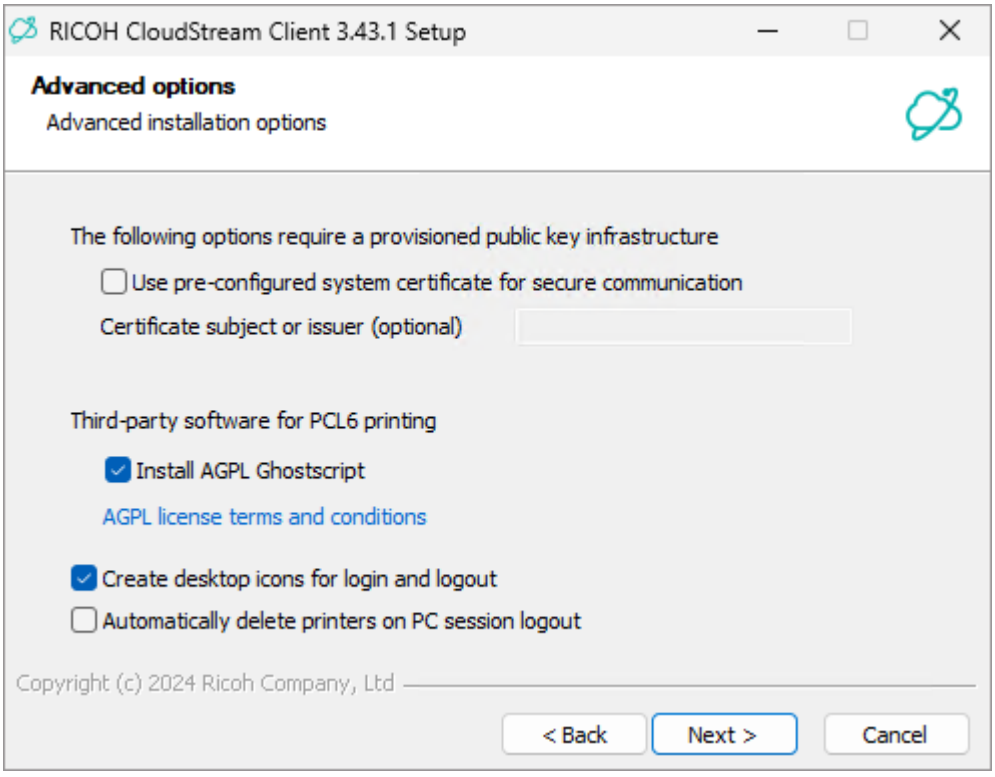
   By clicking [Next], the PC Client will connect to the Print&Scan application.

   If the connection fails, you can still continue to install the PC Client by checking the ***Enable offline installation*** box.

   You can modify and test the connection again after installation. Refer to Modify PC Client Service Configuration on page 227 for steps.

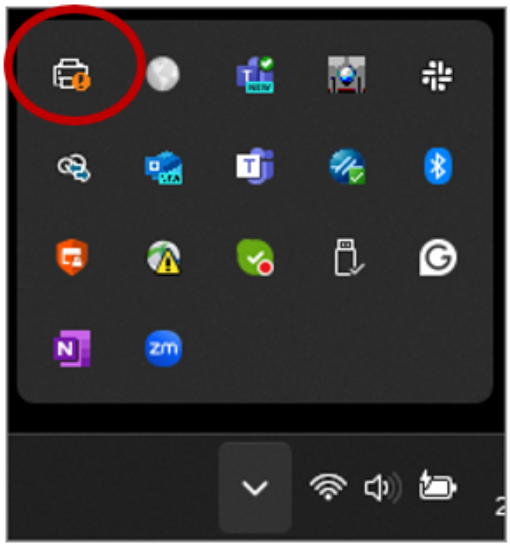
7. On the ***Advanced options***, check *Create desktop icons for login and logout.*

   This will create a shortcut in your desktop so you can click login and logout without going to the notification tray.



8. Click **[Next]**, then click **[Install].**

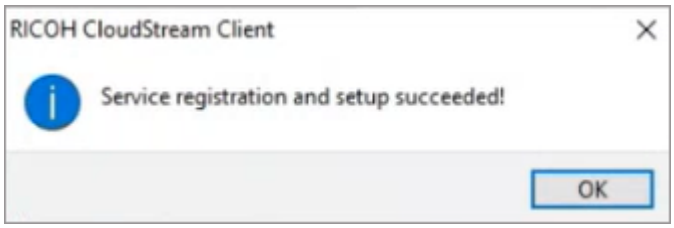
Successful installation will display RICOH CloudStream Print&Scan PC Client in the Notification tray.



Modify PC Client Service Configuration

1. Open the PC Client configuration menu from the notification tray.
2. In the *RICOH CloudStream client configuration* screen, click **[Service setup...].**
3. Enter the domain name in both the *Server host name* and *Account domain name* field.
4. Select ***'RICOH CloudStream OAuth2'*** as the *Authentication Type*.
5. Choose a storage mode. For more information about modes, refer to https://-manual.na.ps.cloudstream.ricoh.com/docs/ricoh-cloudstream-client-overview.
6. Click **[Register service].**

You should be able to register the service successfully and you will see the following message.



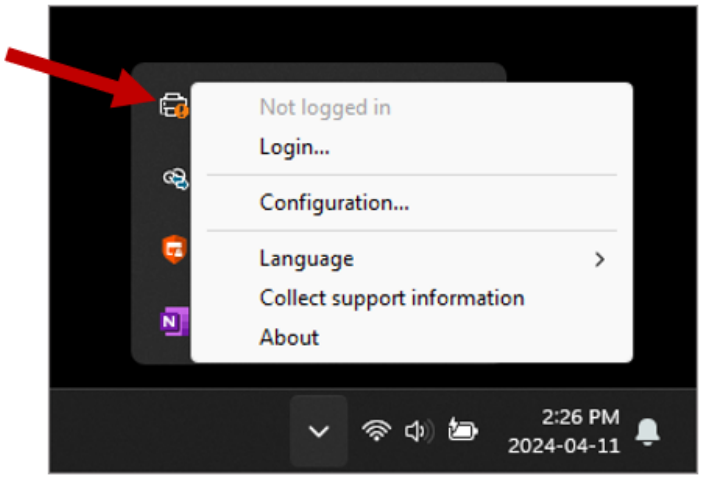
Login to Print&Scan PC Client

Important: Before you login to Print&Scan PC Client, your account must register to the CloudStream DM. The PC Client authenticates the user sending the print job before the job is sent to the printer. To register a user, refer to Register Users on page 311.

Note: You can find detailed Print&Scan PC Client documentation in RICOH CloudStream Client.at this link: https://-manual.na.ps.cloudstream.ricoh.com/docs/ricoh-cloudstream-client. Copy and paste the URL in a browser.

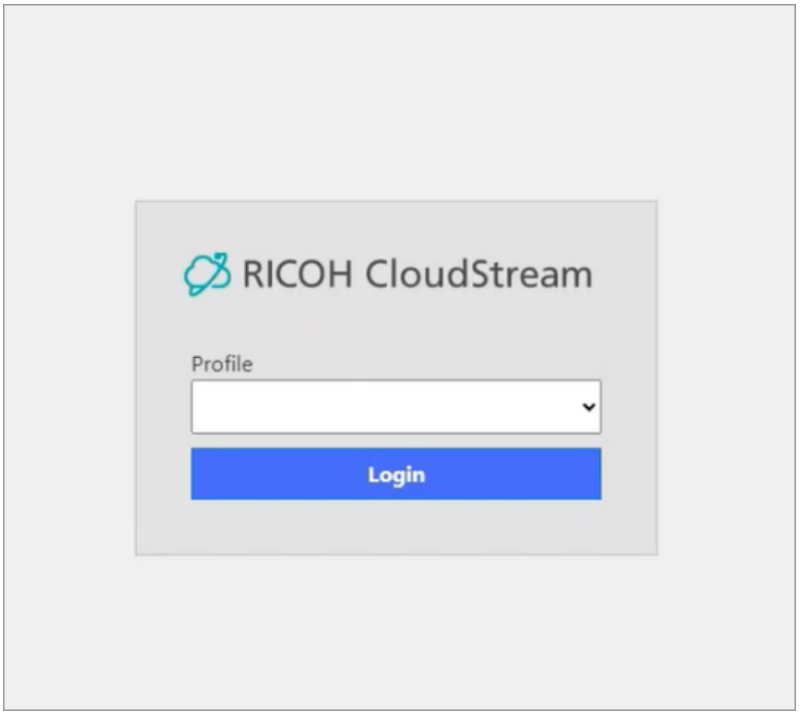
1. After installing the PC Client, open the PC Client login screen to authenticate your account.

   In the notification tab, right-click on the PC Client and click Login.



   If the Login shortcut is added during installation, click the 'Login to Print Service" in your desktop to display the login screen.

2. A browser will open displaying the CloudStream DM login page. Select the profile that you would like to get authenticated with.



3. Click **[Login].**
4. You will be redirected to your external authentication provider, provide the correct credentials to get authenticated.

   If the authentication fails, please contact your IT administrator or the external authentication provider for support.
5. A successful authentication will display the CloudStream DM Consent page. This page will ask for your consent to allow the CloudStream DM service to access your account.

   Please check all three permissions to continue using RICOH CloudStream Print&Scan.

   - profile
   - offline_access
   - email
6. Click **[Submit Consent].**

   If you did not give your consent or click **[Cancel]**, the RICOH CloudStream Print&Scan cannot sign you in because the service will need all three permissions mentioned in the previous step.

   When consent is given, you will return to the success page and displaying:

   "You may now close this browser window and return to the application."

Print a Document

After logging to RICOH CloudStream Print&Scan PC Client, the CloudStream printer is automatically added to your client machine.

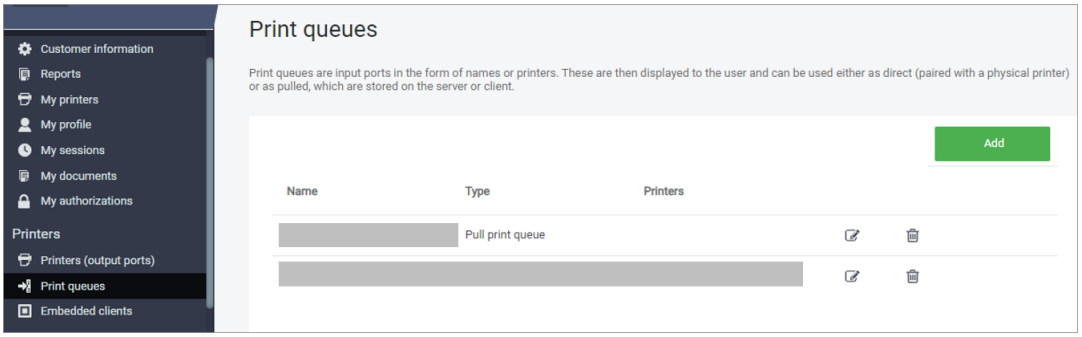
Confirm that the CloudStream printer is added to Window's Printer & Scanner. The CloudStream printer's name is **RICOH CloudStream Printer**.

1. Open a document.
2. Go to File, then print the document.
3. Select ***RICOH CloudStream Printer*** as printer.
4. Proceed to submit the print job.

Note: You can find detailed Print&Scan PC Client documentation in RICOH CloudStream Client.at this link: https://-manual.na.ps.cloudstream.ricoh.com/docs/ricoh-cloudstream-client. Copy and paste the URL in a browser.

If you are an administrator and you have access to the RICOH CloudStream Print&Scan portal, you can see the print job displayed as pending in the print queue. To view, follow the steps below.

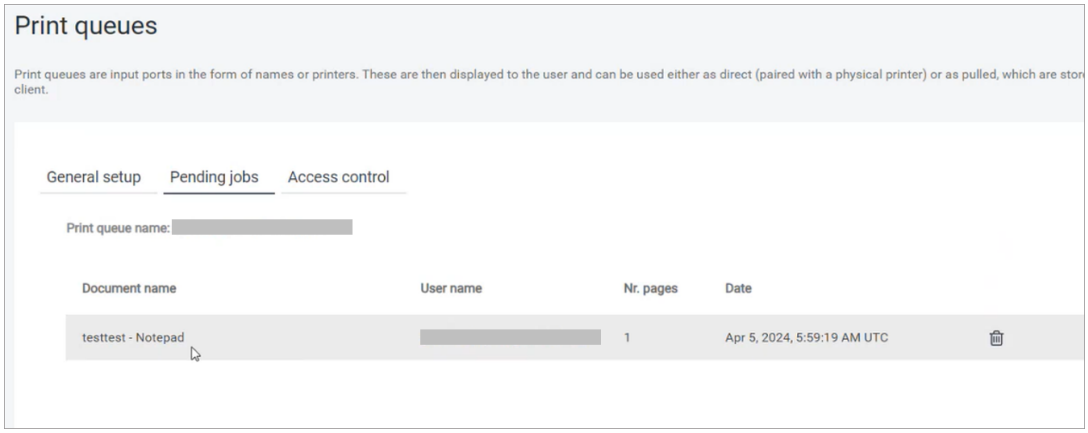
1. Login to Print & Scan portal via CloudStream DM portal using an OIDC admin account.
2. Go to ***Print queues*** under *Printers* section.



3. Click the edit icon beside the ***RICOH CloudStream Printer*** queue.
4. Click the ***Pending Jobs*** tab.

   All documents sent to ***RICOH CloudStream Printer*** from different users are

displayed in the list.



If your print job is not listed, please try again and check if your connection and authentication to the RICOH CloudStream Print&Scan Embedded application is still active.

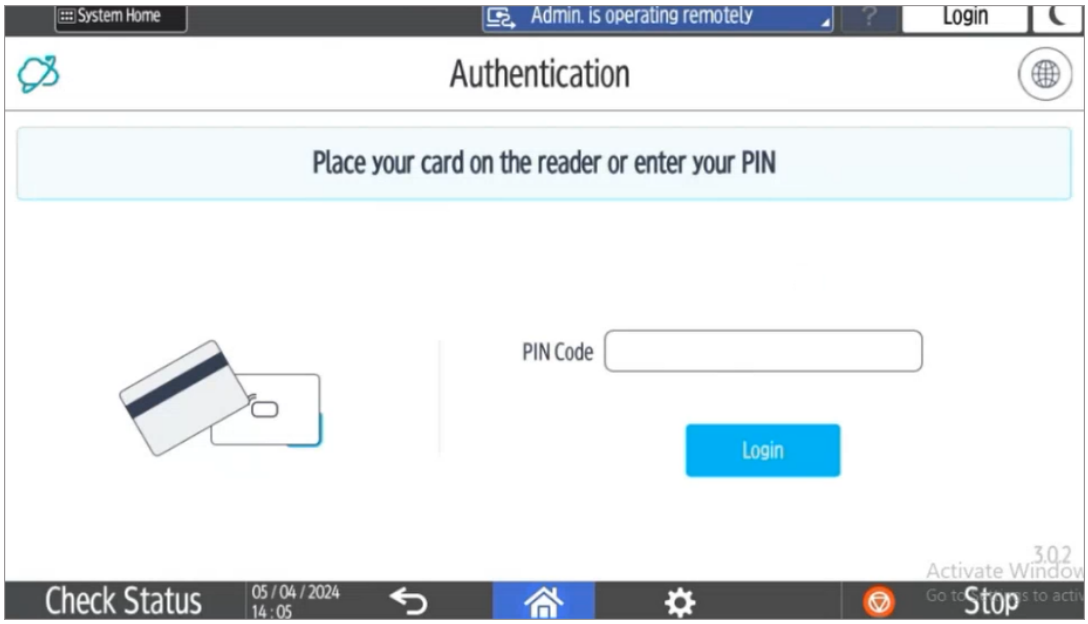
Release a Print Job

After your documents are successfully queued to theRICOH CloudStream Print&Scan Embedded, you can release them to any devices managed by CloudStream DM.

To simply release a document, follow the steps below.

1. Go to any Ricoh device with RICOH CloudStream Print&Scan Embeddedapplication installed.

   Devices with the RICOH CloudStream Print&Scan embedded application display the Print&Scan login screen in the panel similar to the image below.

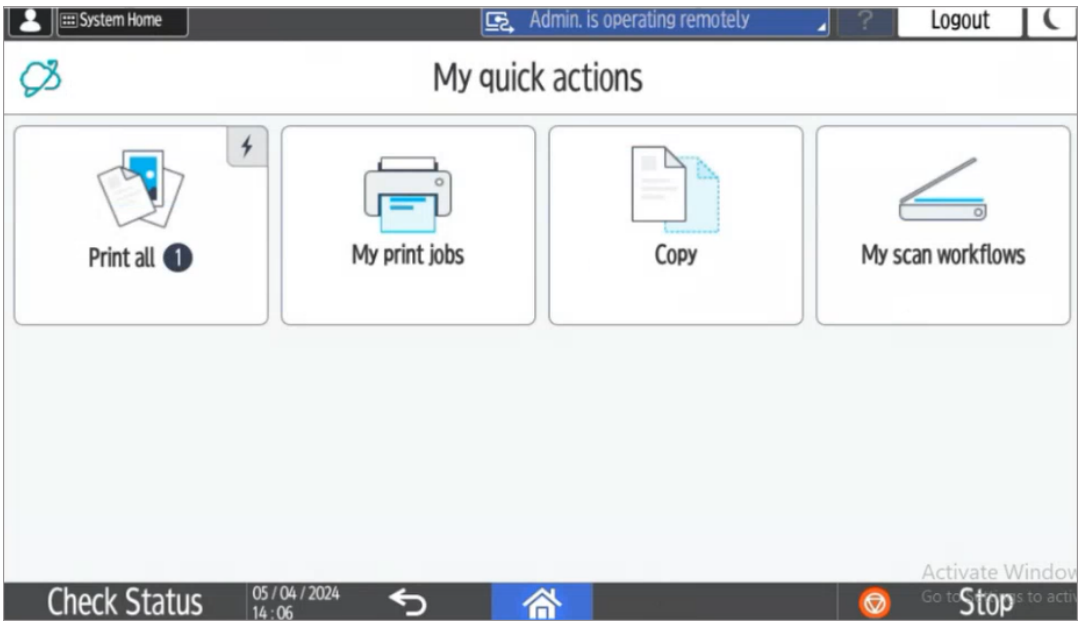


Depending on the configured embedded client, the login screen will display different types of logins. For the example above, the configured model of login is Card swipe and PIN Code (Short ID).

If the device does not have the embedded yet, you can install it by following the steps in Install Print&Scan Embedded App on page 281.

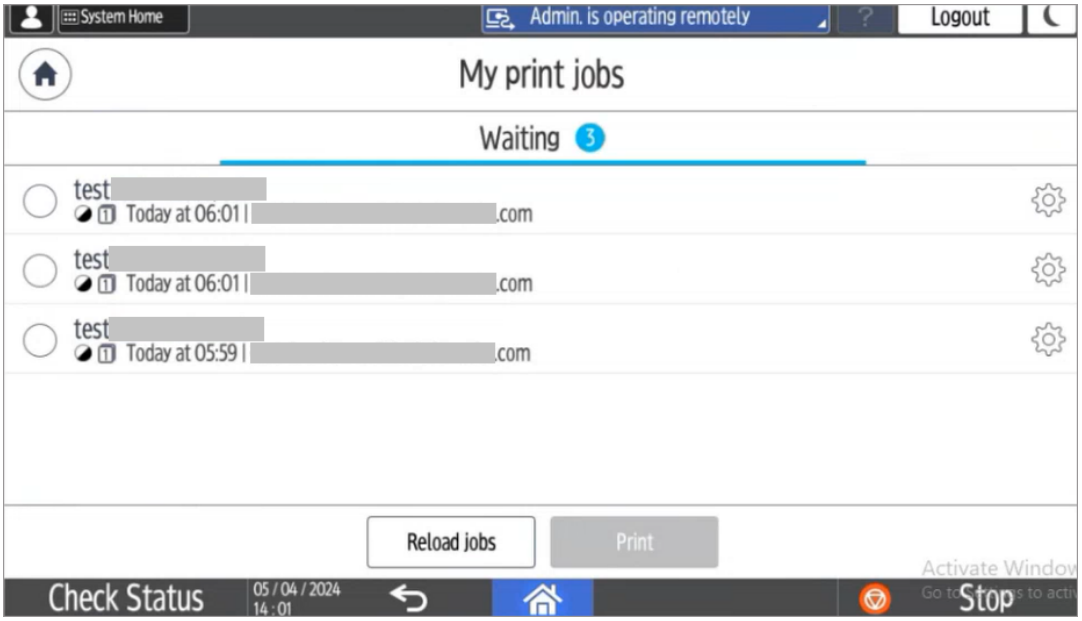
2. Login using the account that you used to send the print job.

   You will see the Print&Scan home screen after a successful login.



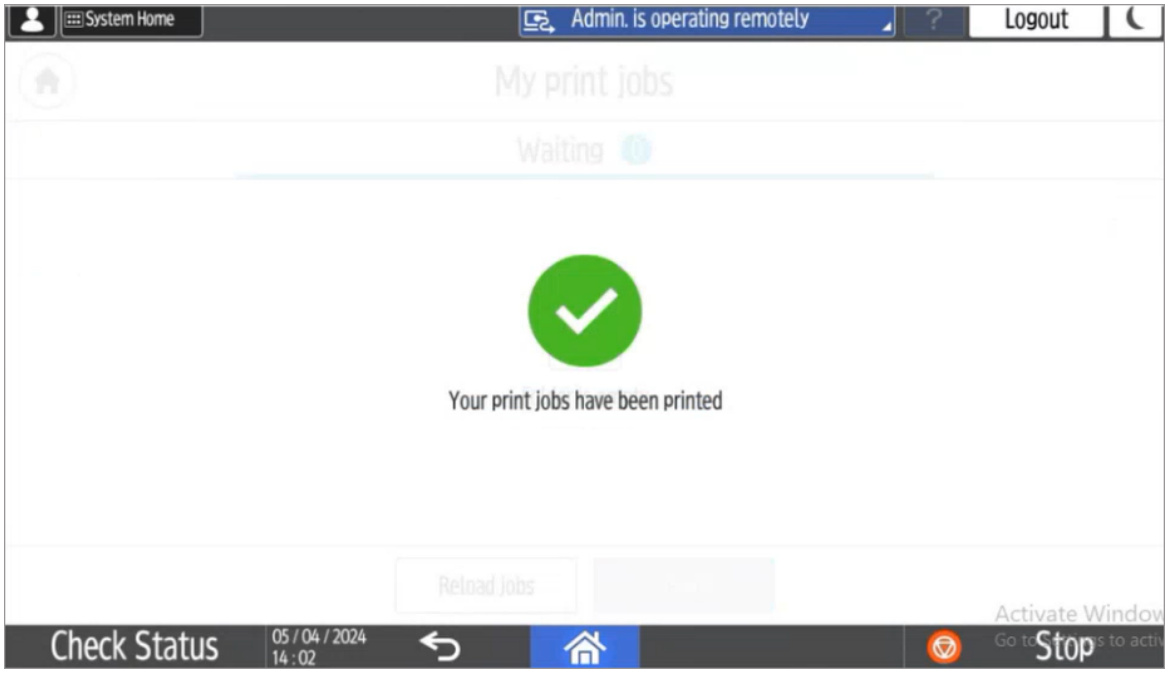
3. Tap **[My Print Jobs].**

   All the print jobs you sent to the ***RICOH CloudStream Printer*** is displayed in the list.



4. Tap the circle to select the document you want to print. You can select multiple documents and print them together.
5. Tap [Print] to start printing.

When all print jobs are printed, you will see this screen.



Device Configuration

Device configuration has functions that allow you to configure printer settings, including deploying printer firmware and embedded applications. You can monitor the devices' compliance with the company's security policies by creating templates containing the company software policies.

Quick Topics:

Topic	Description
Install RICOH CloudStream Print&Scan Embeddedapplication	Installing the RICOH CloudStream Print&Scan Embedded in the devices will allow users to log in to the MFP and perform secure printing and scanning. Install Print&Scan Embedded App on page 281.
Uninstall RICOH CloudStream Print&Scan Embedded application	Follow the steps in to uninstall the RICOH CloudStream Print&Scan Embedded from devices. Uninstall Print&Scan Embedded App on page 284.
Update DM Agent application	Update the DM Agent application installed on the devices. DM Agent is responsible for the communication between the MFP device and the RICOH CloudStream. Update to the latest version of the DM Agent by following the steps in Update the DM Agent Application on page 286.

A list of device configuration functions is displayed below. Click the link to see more.

- Device Configuration Template on page 236 - This allows you to create templates containing device settings like firmware and embedded applications.
    - Standard Device Preferences (SDP) on page 238 - This allows you to create a standard preferences template containing general settings that are not specific to device models.
    - Extended Device Preferences (XDP) on page 247 - This allows you to create an extended device preferences template in which the resource is copied from an existing device.
    - Firmware Template on page 256 - This allows you to create a template for firmware updates.

    - Embedded Application on page 258 - This allows you to create a template for embedded applications.

- Device Policies on page 261 - Device policies help you create policies that monitor device compliance. The policy uses configuration templates to apply or check the desired templates to devices daily. For example, if you want to create a policy that a group of devices must be using a specific firmware version, create the firmware template, and use the template to create your firmware policy.
    - Configuration Policy - This allows you to create policies using the SDP and XDP.
    - Firmware Policy - This allows you to create policies using firmware templates.
    - Embedded Policy - This allows you to create policies using embedded application templates.
- Configuration Task on page 272 - You can check and apply templates to the target devices. The configuration's task type includes device reboot, so that you can reboot the target devices remotely.
- Access Profiles and Accounts on page 287 - Creates device administrator, SNMP, and SDK/J Platform accounts. These account profiles are used to communicate with the Ricoh devices.
- Device Polling on page 294 - Allows you to set the polling settings of devices, including Work from Home devices.
- On-Premise Device Monitoring on page 297 - Installing the service via Device Monitoring Service Installation on page 299 allows you to monitor RICOH devices and 3rd party manufactured devices.

Device Configuration Template

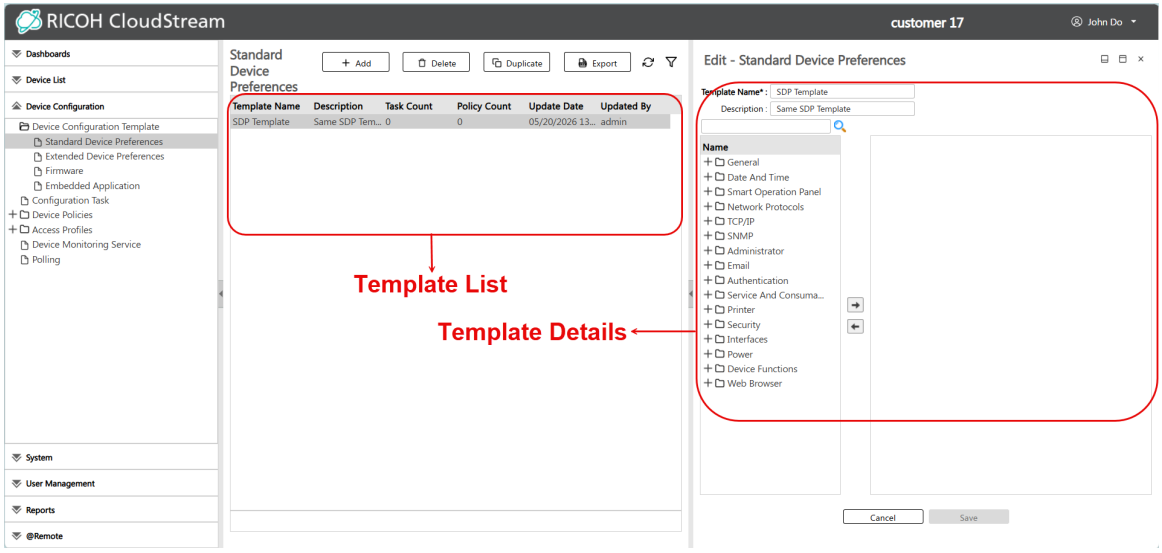
Configuration Templates are created to apply specific settings to multiple devices simultaneously. A set of setting values defined for this purpose is called a “template”. The templates are applied to the target devices with DM Agent Embedded installed.

There are four types of configuration templates, and they are described briefly below:

- Standard Device Preferences (SDP) on page 238 - This template helps you update general setting items that do not depend on the model.
- Extended Device Preferences (XDP) on page 247 - You can create multiple XDP templates and apply configurations to the target devices. The XDP can extract device configuration and resources from a source device. The extracted resource file is used to configure other devices' settings of the same model.
- Firmware Template on page 256 - Using the firmware template containing the firmware files, you can remotely perform firmware upgrades to the devices.
- Embedded Application on page 258 - Allows the administrators to upload device-embedded applications.

Common Template Tools

The screen of each configuration template is divided into two, the template list and the template details.



The template list is the grid that lists all templates created. This is the generic layout of all template list grids. The template list has the following common column headers.

Column Header	Description
Template Name	The name of the template. The template name is unique must not be duplicated.
Description	Template description
Task Count	The number of configuration tasks that use the template.
Policy Count	The number of device policies that use the template.
Update Date	Date and time the template was last updated.
Updated By	The admin user who last updated the template.
Action	Displays the action of the embedded template. The value is either "Uninstall" or "Install or Update". This column is only displayed in the Embedded Application node.

You can sort the columns in ascending or descending order. The sorting button will appear when you hover over to the right part of the column header.

Template detail is the screen that shows when a user selects a template from the list. The template details screen is displayed on either the right-hand pane or the bottom pane.

The Template Details has two default buttons, the **[Save]** and **[Cancel]** buttons.

Item Name	Description
Save	Saves the changes made in the details view. Clicking this button will validate the correctness of the input of the fields. If an invalid value is detected, an error icon will be displayed beside the field in error, and the changes will not be saved. **Important:** If you are modifying a template associated with a device policy, the change will affect the policy status of the devices. Please make sure to execute the associated device policy after saving the changes.
Cancel	Dismisses all changes made in the fields and displays the previously saved value.

Common Template Toolbar

In every configuration template type, the following are the common tools you will find in the toolbar.

Item Name	Description
Add	When clicked, a wizard will display to allow users to create a configuration template.
Delete	A configuration template associated with a configuration policy cannot be deleted. Please remove the template from the associated configuration policy or task before deleting the template.
Refresh	Displays as  icon. When clicked, it refreshes the template list.
Filter	Displays as  icon. When clicked, the filter boxes appear in each column allowing you to input search text to filter the data in the specified column.
Duplicate	This action duplicates a template. Depending on the type of template, this function may not be provided. The copy will keep the original name with a suffix when a template is duplicated. **Note:** This option is available for Standard Device Preferences and Extended Device Preferences.
Export	Exports the selected template into a CSV file. Please see the details in Export SDP Template on page 244. **Note:** This option is available for Standard Device Preferences only.

Standard Device Preferences (SDP)

This template is helpful in updating general setting items that do not depend on the model. Secure information such as passwords and SNMP community names cannot be obtained when the settings are retrieved from the device. The categories of the setting items that can be edited are displayed on the left side of the screen. Select a category to display the screen for editing the setting on the right side of the screen.

General	Authentication
Date and Time	Service and Consumables
Smart Operation Panel	Printer
Network Protocols	Security
TCP/IP	Interface
SNMP	Power
Administrator	Device Functions
Email	Web Browser

Before applying SDP settings to devices, please read the Standard Device Preferences (SDP) Limitations on page 247 for the list of settings that are not supported by CloudStream DM.

The table below lists the methods to create a Standard Device Preferences template.

Methods	Description
Create a Blank Template on page 239.	Create a blank template, and individually select all settings manually.
Get Settings from Device on page 240.	Get settings from an existing Ricoh device, which imports all the settings, and you can make changes after the import.
Import a Template on page 241.	Import a CSV file that contains the standard settings.
Duplicate a Template on page 242.	Duplicate a template and use it as the basis for a new template.

One important step that is common to all methods is setting up the template. To move settings to the template, please go to Add SDP Device Preferences on page 242.

To export an SDP template to a CSV, please go here Export SDP Template on page 244.

Create a Blank Template

Follow these instructions to create a blank template.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
4. Click **[Add].**
5. Enter a name for the template, and optionally add a description that can help you identify the template's contents.
6. Select the ***Create Blank Template*** as ***Option.***
7. Click **OK** to create the template.

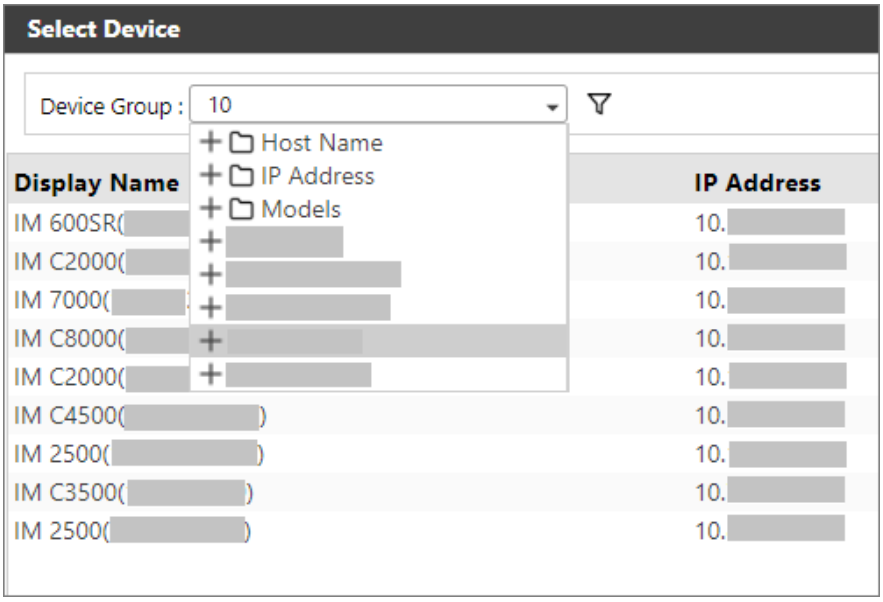
The template is created with empty values in the device preferences.

Get Settings from Device

Obtain the resource settings from a device added to CloudStream DM. Follow the steps to get the settings from a device.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
4. Click **Add.**
5. Enter a name for the template, and optionally add a description that can help you identify the template's contents.
6. Select ***Get Settings from Device*** as ***Option.***
7. Another set of fields appears on the screen to allow you to select the device. Click **[Select Device].**
8. In the dialog, select a device group to display the devices within the group.
9. Select a device from the list.

   You can also click the filter button to display the display box. Input the device's IP Address, or display name, then click search. This will search for the device that matches the search text.



10. When a device is selected, click **[OK].**

> **Note:** Only one device can be selected as the source device. The WfH devices group will not be displayed; thus, WfH device cannot be selected as the source device.

11. Click **[OK]** to create the template.

A template is created with the settings and values copied from the actual device that you selected.

Import a Template

You can import a CSV file to create a template.

Additionally, you can generate the CSV file by exporting a template from the same SDP screen. You can find the instructions to export the template in Export SDP Template on page 244.

To import a CSV file into a template, follow the steps below:

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
4. Click **[Add].**
5. Enter a name for the template, and optionally add a description that can help you identify the template's contents.
6. Select ***Import Settings from File*** as ***Option.***
7. Click **[Choose file].**
8. Select a valid CSV file.

   The selected CSV file must have a similar format to the example below.

   Opened from Excel:

	A	B
1	# Format Version: 5.1.1.0	
2	# Generated at: 10/18/2022 20:44:11	
3	# Function Name: Device Preference Template	
4	# Template Name: Set SNMP v1/v2	
5	# Description: This SDP template will set the SNMP V1 /V2 of the device	
6	Attribute	Value
7	network.SnmpTrapSetting	FALSE

   Opened from notepad:

```
# Format Version: 5.1.1.0
# Generated at: 10/18/2022 20:44:11
# Function Name: Device Preference Template
# Template Name: Set SNMP v1/v2
# Description: This SDP template will set the SNMP V1 /V2 of the device
"Attribute","Value"
"network.SnmpTrapSetting","false"
```

9. Once a valid file is selected, click the **[OK]** button to create the template from the imported file.

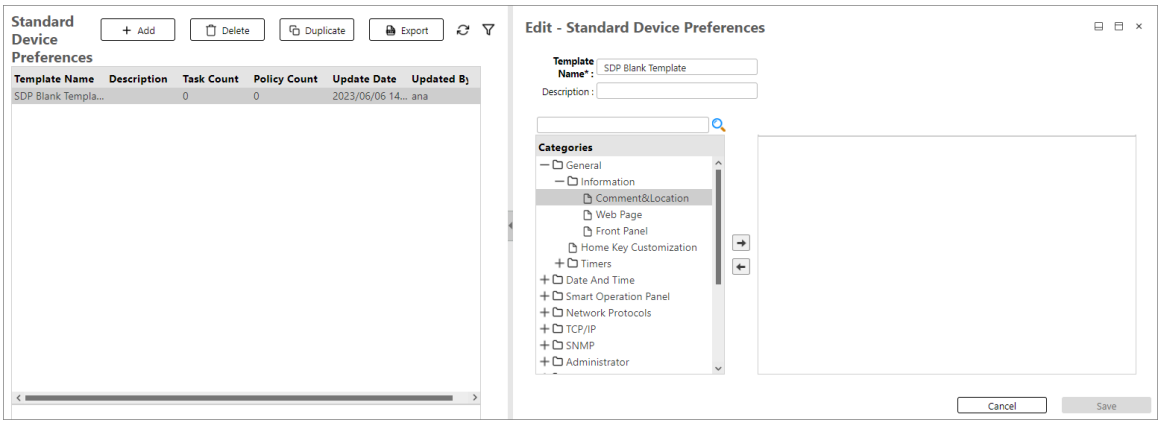
Duplicate a Template

Create a copy of another template and rename it before you modify the preferences as needed. Suppose a template contains settings that are a very close match to the settings you need. In that case, you can easily copy the template, make minor modifications, and then add the modified template to a configuration task.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Standard Device Preferences.***
4. Select an existing template, then click **[Duplicate].**
5. (Optional) Open the new template and change the name and description. The duplicate copy will keep the original name with a suffix.
6. Make necessary modifications to the device preferences area. Please see Add SDP Device Preferences on page 242.
7. Click **[Save].**

Add SDP Device Preferences

An example of an SDP template is displayed below:

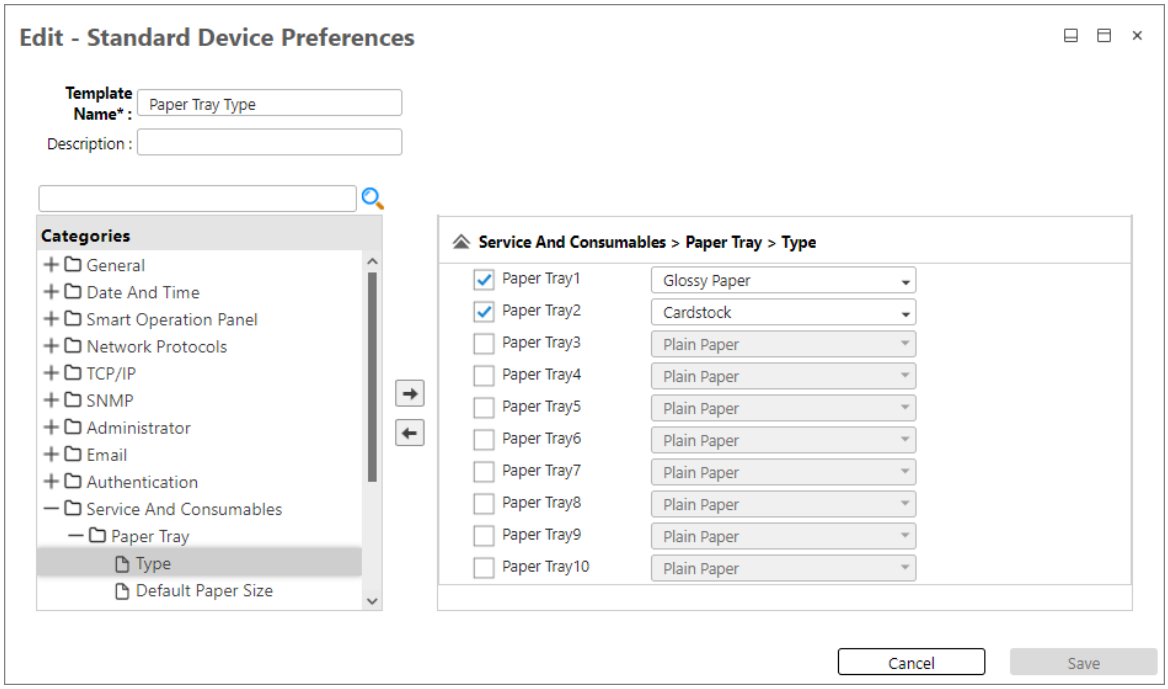


To add settings to the template, you must select the setting from the Categories or Search a Setting on page 243, then move it to the right-hand pane, you can use the following buttons.

Buttons	Icon	Description
Expand	+	Expands the category and displays the sub-categories.
Collapse	-	Collapses the category.
Add		Adds the selected category, sub-category, or node to the right-hand side. If the category has sub-categories when the **[Add]** button is clicked, all the sub-categories under the selected category will be added to the right-hand side.
Remove		Removes all unchecked settings from the right-hand side.

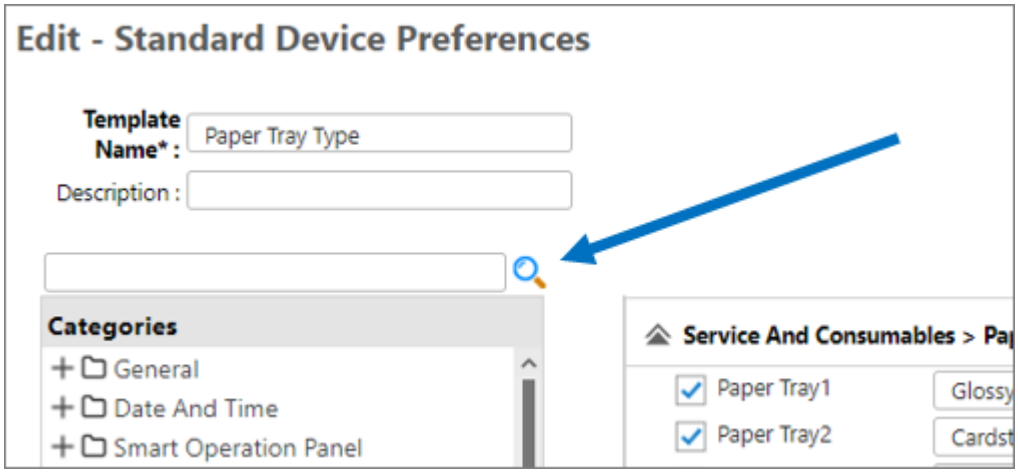
After a category, sub-category, or node is added, you must check the box of the desired setting, then input or select the value of the setting.

The example below shows a template "Paper Tray Type" which aims to set ***Tray 1*** to "Glossy Paper" and ***Tray 2*** to "Cardstock".



Search a Setting

You can use the search function to find settings.



Input the setting's name then click the search icon. All categories that contain the matching setting will be displayed in the Categories pane.

Saving a Template

To save a configuration template, simply click the **[Save]** button.

Please note that saving a template will remove settings which do not have configurations, leaving only the ones that contain configuration items.

For example, select the ***General*** category and add it to the right-hand pane, then configure the ***Information***> ***Comment & Location*** only. When you save the template, only the ***Information***> ***Comment & Location*** node which contains the configuration items is saved and the rest of the nodes are removed.

Export SDP Template

You can export multiple Standard device preferences templates for backup purposes or reuse it for SDP import.

To export the template, follow the steps below:

1. Login as an administrator.
2. Go to ***Device Configuration*** and expand ***Device Configuration Templates.***
3. Click on ***Standard Device Preferences.***
4. Select a template, then click **[Export to CSV].**
5. The download will start right away. Please open your download folder.

The filename of the downloaded CSV contains the date and time the template was exported.

If you want to modify the content of the CSV file, you can open the file and make your changes, but always remember to save the file as CSV.

The document should have the required rows.

- The first six rows/lines must have the content ***# Format Version, #Generated at, #Function name, #Template Name, #Description.***
- The following rows or lines must include the ***Attributes*** then the ***Values*** on the next column. The setting is placed in the Attributes column while the value of the setting is in Value column.

The exported CSV is depicted in the images below.

If you open from MS excel:

	A	B
1	# Format Version: 5.1.1.0	
2	# Generated at: 10/18/2022 20:44:11	
3	# Function Name: Device Preference Template	
4	# Template Name: Set SNMP v1/v2	
5	# Description: This SDP template will set the SNMP V1 /V2 of the device	
6	Attribute	Value
7	network.SnmpTrapSetting	FALSE

Note: MS excel does not quote wrap the attributes and values.

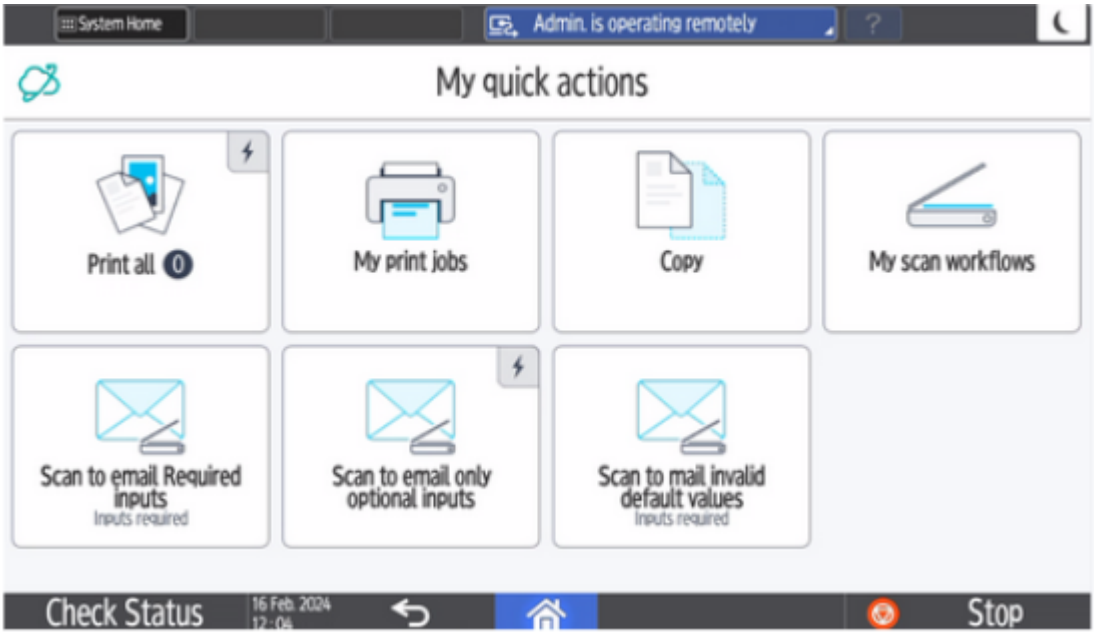
If you open using a text editor:

```
# Format Version: 5.1.1.0
# Generated at: 10/18/2022 20:44:11
# Function Name: Device Preference Template
# Template Name: Set SNMP v1/v2
# Description: This SDP template will set the SNMP V1 /V2 of the device
"Attribute","Value"
"network.SnmpTrapSetting","false"
```

Note: Please ensure that all fields for Attribute and Value are quote wrapped as shown in the text editor view above.

Set CloudStream PS as the Home Screen Application

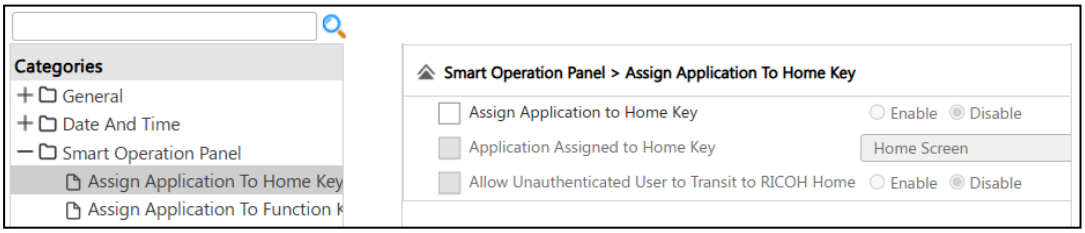
By default, when CloudStream PS embedded is installed on an MFP, the user must login and then navigate to the CloudStream applications using the MFP panel buttons. As shown below, you can change this default and assign the CloudStream PS application to the Home Key. Immediately after login, or when the user presses the Home key, the CloudStream PS embedded applications (My quick actions) are displayed.



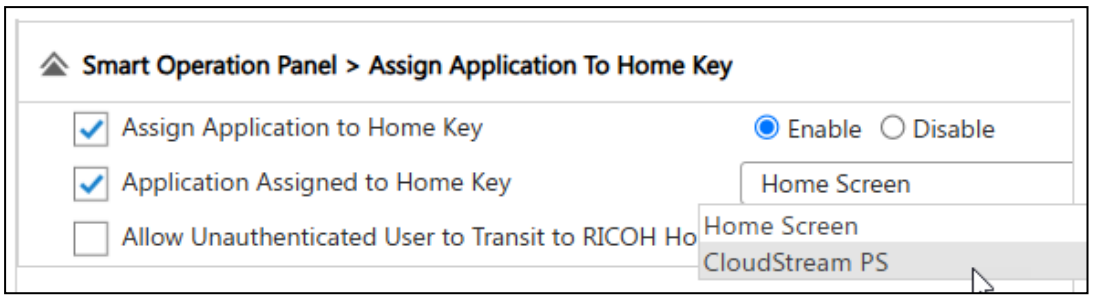
Important: The CloudStream PS (embedded application) version 3.0.5 (or later) is required to support the Home Key feature.

To enable this feature, you can create/modify an SDP template that is applied to the MFP(s):

1. Follow the steps within Standard Device Preferences (SDP) on page 238 to create a new template or modify an existing template.
2. When adding preferences to the template, locate the **Smart Operation Panel Category**, and then click **Assign Application to Home Key**. Click Move right to view the options.



3. Enable the **Assign Application to Home Key** checkbox, and also click **Enable**.
4. Enable the **Application Assigned to Home Key** checkbox, and then select **CloudStream PS** from the list. These settings are shown in the screen sample below.



5. **Save** the template and then create a Configuration Task on page 272 to apply the template to target devices.

Standard Device Preferences (SDP) Limitations

All device settings that are not supported by the SDP feature is listed here.

Running a configuration task using the settings below will fail because the DM Agent cannot get the information from the device.

Unsupported Settings
Date Installed
IPV6 Address
Location
Comment
DOSS Last Auto Delete Date
SOP: Wifi Connections
SOP: Interface Settings

Extended Device Preferences (XDP)

This topic provides instructions to configure Extended Device Preferences (XDP).

Use this feature to expedite the configuration process when deploying or updating a fleet of models. In a few simple steps, administrators can retrieve preferences from existing configured MFPs, and then use the preferences to create a configuration template that can be easily applied to other devices of the same model.

To create an XDP template, please see the prerequisites and order of steps in the following tables.

Prerequisites
The target Ricoh device is added and displayed in the device list. A resource file is retrieved from Ricoh devices to create a template. **Note:** The target device must not be a WfH device.
The device is online and does not display any error in the panel.

Before you attempt to create an XDP template for Ricoh devices, please read the topics below for best practices to consider.

Best Practices for Ricoh XDP Templates on page 248.
Avoiding Preference Conflicts on page 249.

Create an XDP template in three steps.

Order	Instructions
1	Create a template based on a Ricoh device. Follow the steps in **Get Settings from Device** section of the topic Create XDP Template on page 251.
2	(Optional) Create blank template using the resource file extracted in step #1. Follow the steps in ***Create a Blank Template*** section of the topic Create XDP Template on page 251.
3	Add XDP Device Preferences on page 254.

Best Practices for Ricoh XDP Templates

Template Application

- **One template per model** – The best way to ensure a template will be successfully applied to other devices is to apply it only to devices that are the same model as the model you copied the initial settings from to create the template.
- **One template per model family** – Although you can create a template for a model family, bear the following in mind:
    - Different model families may have different settings available. If there are differences within the same model family, the template process will be successful; however, you should start with a device that has ALL the options you want to configure. If you attempt to apply a setting that does

not exist on a model within the same family, the setting will simply be skipped.

- If you plan to create a template that you will apply to multiple types of devices, verify that the settings work properly on all applicable device models. Keep in mind that device capabilities vary across model families and can vary across firmware versions within the same device family.

Note: Refer to Supported Printers on page 380 to see which family your devices belong to.

Include/exclude Ricoh device preferences settings

One way to create a template is to retrieve the resource settings using the Get Settings from Device function from an existing Ricoh device connected to your network. The feature will retrieve the device resource settings and preferences settings.

- The **resource setting** is composed of printer settings that are supported by the Ricoh device. (Example: Copies, SNMPv3, Orientation) The downloaded resource file can be used as the base to create another configuration template with settings that reference the resource file.
- The **preferences setting** contains the corresponding Ricoh device value of the resource settings. (Example: Copies= 3, SNMPv3= On, Orientation= Portrait)

Important: To create a template using Get settings from Device set the Include Preferences to **unchecked** if you intend to modify a few settings from the downloaded resource file. If you want to extract all supported printer settings and its corresponding device value, set the Include Preferences to **checked.**

Avoiding Preference Conflicts

The following examples show known firmware related or specification limitations where specific settings could not be applied to a device.

The table below shows the results when applying the settings to the specified devices. The Category shows where the settings can be found.

For example, you created an XDP template, and you go to Web Image Monitor Settings> Security > Ipsec> Encryption Key Auto Exchange Settings> Security Details and decide to set a value for Tunnel End Point 1 setting. When you apply the template via configuration task to devices IM 600SR and MP C307, the task will return successful, but the value is not applied to the devices. However, if the same template is applied to IM C4500, it will return successful, and the template value will be applied correctly.

The device columns uses the following key:

- **Fail** = Result is “Succeeded” but the new value is not applied in device and Check:Value.
- **F:Apply** = Result is Failed:Apply with reason “The Setting parameters to the device is invalid".
- **Pass** = Result is “Succeeded” and the new value is successfully applied in device and Check:Value.
- **Skip** = Result is Skip- Unsupported Item.
- **Blank** = Not tested

Category	Settings	IM 600SR	MP C307	IM C4500	IM 350F
Fax Features> Reception Settings> Reception File Settings> Prohibit Auto Print	G3-1		Fail	Pass	
Fax Settings> Reception Settings> Reception File Settings> Prohibit Auto Print	G3-1	Fail	Pass		
System Settings> Administrative Tools	Machine Action When Limit is Reached	Fail	Fail	Fail	
System Settings > Administrator Tools> Enhanced Print Volume Use Limitation	Tracking Per-mission	Fail		Pass	
System Settings> Administrator Tools> Enhanced Print Volume Use Limitation	Stop Printing	Fail		Pass	
Web Image Monitor Settings> Device Settings> System> General Settings	Spool Printing	Fail		Fail	
Screen Features Settings> Per-sonal> Language & Input> Key-board & input methods	iWnn IME		Fail		
Web Image Monitor Settings> Printer> IPDS Job Capture Settings	Job capture			Fail	
System Settings> Interface Set-tings> Effective Protocol	IPv4			Fail	
System Settings> Timer Settings> Auto Logout Timer	second(s)		Fail		
System Settings> Timer Settings> Daylight Saving Time	Start Time	F:Apply	F:Apply	F:Apply	F:Apply
Web Image Monitor Settings> Security > Ipsec> Encryption Key Auto Exchange Settings> Security Details	Tunnel End Point 1	Fail	Fail	Pass	
Web Image Monitor Settings>	PFS	F:Apply	F:Apply	F:Apply	

Category	Settings	IM 600SR	MP C307	IM C4500	IM 350F
Security > Ipsec> Encryption Key Auto Exchange Settings> Security Details					
System Settings> Interface Settings> Effective Protocol	IPv6	Fail			
System Settings> Timer Settings> Daylight Saving Time	End Time	F:Apply	F:Apply		F:Apply
System Settings > Administrator Tools	Sleep Mode Entry by Sleep Mode Timer	Skip	Skip	Skip	Skip

Create XDP Template

There are several methods to create an XDP template. To begin, you must create a template that is created from "Get settings from device" to extract the device's resource file. Using the resource file, you can start creating blank templates.

Methods	Description
Get Settings from Device on page 251.	Get settings from an existing Ricoh device, which imports all the settings, and you can make changes after the import.
Create a Blank Template on page 253.	Create a blank template, and individually select all settings manually.
Copy a Template on page 253.	Copy a template and use it as the basis for a new template.

Get Settings from Device

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
4. Click **[Add].**
5. Enter a name for the template, and optionally add a description that can help you identify the template's contents.
6. Select ***Get Settings from Device*** as ***Option.***
7. Another set of fields appears on the screen allowing you to select the source device. Click **[Select Device].**

8. From the pop-up dialog, select a group to display the devices within the group.
9. Select a device from the list.

   You can also click the filter button to display the filter boxes. Input the device's IP Address or Display name, then click search. All devices that match the search will be displayed.
10. When a device is selected, click **[OK]**.

> **Note:** Only one device can be selected as the source device. The WfH devices group will not be displayed; thus, WfH device cannot be selected as the source device.

11. Decide whether to include preferences or not.
    - **Unchecked** – Only the device resource settings are downloaded. The template will display all supported printer settings, and from then, you can set values to your intended settings to modify and apply them to other devices or the same device.
    - **Checked** – Imports resource settings and preferences settings. The template will display all supported printer settings with their corresponding device values. From then, you can modify the values of your intended settings or keep the values already set.

> **Important:** It is recommended to uncheck the ***Include Preferences*** checkbox to download the resource file faster. Creating a template from the source device and excluding the preferences will display the device settings without values. You must input the desired values into the settings before saving the template.
>
> However, if you want to get all printer settings and their values, check***Include Preferences***. Including the preferences during resource extraction is applicable if you plan to set several printer settings. Creating a template with preferences from a device may take a few minutes; please ensure your device is online while the extraction is ongoing.

12. Set the Resource Name. The settings extracted from the target device will be named after the resource name. This file will also be displayed in the "Resource File" drop down list when creating a blank template.
13. Click **[OK].**

If the resource name already exists, you will see an error message asking if you want to overwrite the resource or rename it.

Depending on the number of settings available for the device, downloading settings from the selected source device may take a few moments. The template is added to the Template list when the download is successful.

Preferences and resource files are stored in Repository Management.

Create a Blank Template

Follow these instructions to create a blank template using a previously downloaded Resource file as the basis for the template. The Resource file defines the settings that are available in the template.

Note: Resource files would appear in this list only if a template were previously created using Get Settings from Device, as instructed in the procedure above.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
4. Click **[Add].**
5. Enter a name for the template, and optionally add a description that can help you identify the template's contents.
6. Select ***Create Blank Template*** as ***Option.***
7. Select a ***Resource file*** from the dropdown list that will form the basis for the template.
8. Click the **[OK]** button to proceed.

Depending on the number of settings available, the creation may take a few moments. The template is added to the Template list when the download is successful.

Copy a Template

Another method to create a template is simply creating a copy of an existing template and renaming it before modifying preferences as needed. Suppose a template contains settings that are a very close match to the settings you need. In that case, you can easily copy the template, make minor modifications, and then add the modified template to a configuration task.

1. Login as an administrator.
2. Go to the ***Device Configuration*** section.
3. Expand ***Device Configuration Template*** and click on ***Extended Device Preferences.***
4. Click **[Duplicate].**
5. (Optional) Open the new template and change the name and description. The duplicate copy will keep the original name with a suffix.

6. Make necessary modifications to the device preferences area. Please see Add XDP Device Preferences on page 254.
7. Click the **[Save]** button.

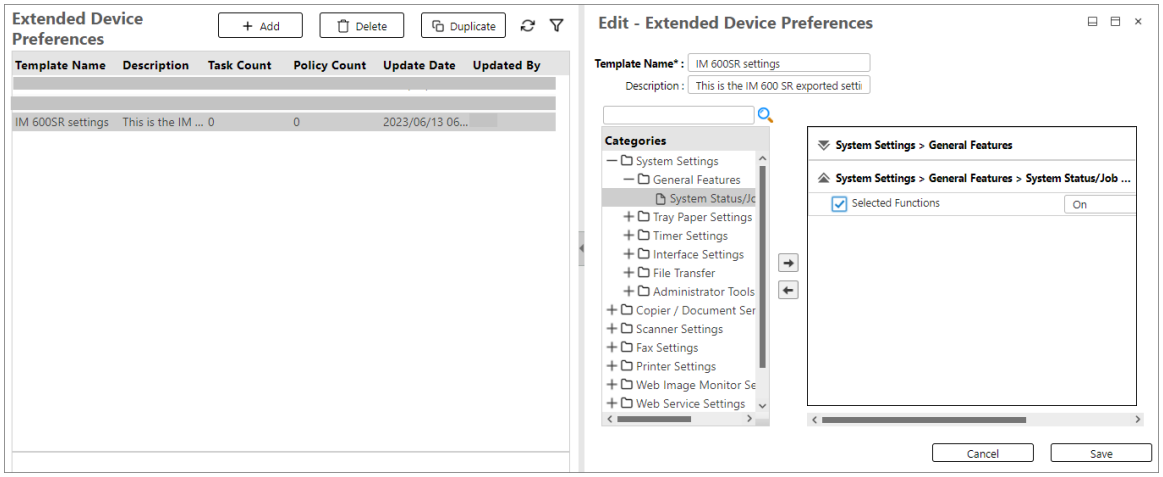
Add XDP Device Preferences

After you create and name a template, you are ready to set the extended device preferences. It's important to note that there are over 1000 individual settings you can modify. Given the sheer number of settings, you can find instructions below on how to select the preferences but this topic does not provide an exhaustive account of the settings themselves.

Important: Refer to Extended Device Preferences (XDP) on page 247 and read *Avoid Preference Conflicts* for current known settings limitations and/or conflicts. The preferences are organized into ten distinct categories, and there are many subcategories within each category. Click on the icon beside a category to view its contents.

View a Preference Set

In the example below, the System Settings preferences are loaded on the right side of the screen. The category or the settings trail the preference belongs to is always shown as the header.



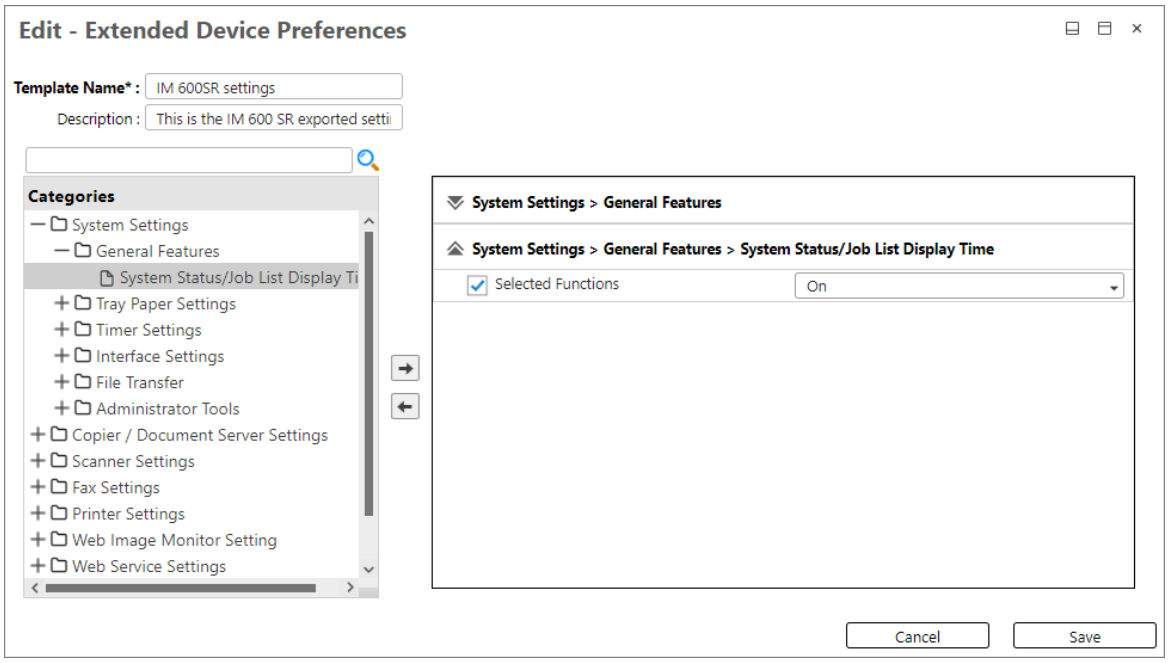
To add settings to the template, you must select the setting from the Categories or Search a Setting on page 255, then move it to the right-hand pane, you can use the following buttons.

Button	Icon	Description
Expand	+	Expands the category and displays the sub-categories.
Collapse	-	Collapses the category.
Add	→	Adds the selected category, sub-category, or node to the right-hand side.

Button	Icon	Description
		If the category has sub-categories when the **[Add]** button is clicked, all the sub-categories under the selected category will be added to the right-hand side.
Remove		Removes all unchecked settings from the right-hand side.

After a category, sub-category, or node is added, you must check the box of the desired setting, then input or select the value of the setting.

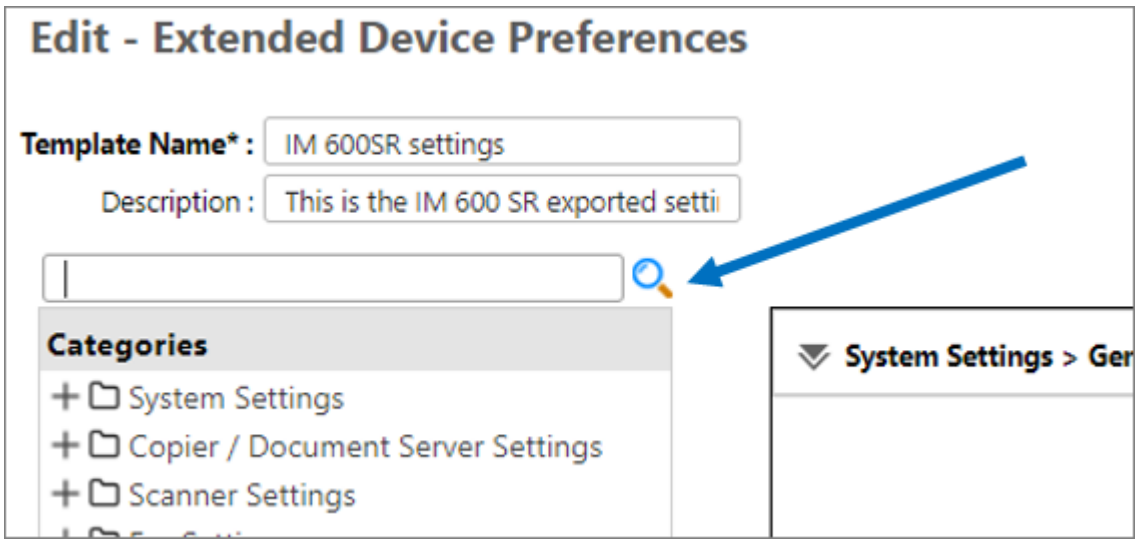
An example below shows a template "IM 600SR settings" which aims to enable the ***Selected Functions*** setting under ***System Settings> General Features> System Status/Job List Display Time.***



Search a Setting

You can use the search function to locate a setting that matches header names, set names, or individual preferences.

A search for "email" will locate all categories and nodes with "email" in their settings and displayed on the Categories pane. Select the preference set from there then add it to the right-hand side.



Saving a Template

To save a configuration template, simply click **[Save].**

Please note that saving a template will remove settings which do not have configurations, leaving only the ones that contain configuration items.

For example, select the ***Email*** category and add it to the right-hand pane, then configure the Email Reception node only. When you save the template, only the Email Reception node which contains the configuration items is saved and the rest of nodes are removed.

Firmware Template

The firmware template in device configuration enables administrators to update device firmware remotely.

Important: SNMP, Device Administrator, and SDK/J access accounts are required to use the firmware template. The template may only be executed properly when the access accounts are configured correctly for the destination device(s).

The following firmware files are supported to create Ricoh firmware templates:

- Firmware individual file - The firmware file must be in .zip file format.
- Firmware full set - The firmware file must be in .zip file format.
- Firmware package - The firmware file must be in .pkg file format.

Follow the instructions below to create a firmware template:

1. Login as an administrator.
2. Go to ***Device Configuration***, expand the ***Device Configuration Template***, then click ***Firmware***.
3. In the Firmware Template screen, click **[Add].**
4. Enter the ***Template Name.***
5. (Optional) Enter the ***Description.***
6. Select an option from the drop-down menu. Choose one of the following options:

Options	Description
Use File in Repository	The list of firmware files uploaded to the cloud repository are displayed when selected. Select one firmware from the list of firmwares. If you select a full set package firmware, the firmware module information is displayed in the bottom table showing the No., Module Name, Version, and Part Number.
Upload New File to Repository	This option allows you to upload firmware to the repository, then select the uploaded firmware from the list to use it as the template's selected firmware package. If a full set package firmware is uploaded, the firmware module information is displayed in the bottom table showing the No., Module Name, Version, and Part Number.

7. (Optional) To upload a new file to the repository, select "Upload New File to Repository" in the previous step, then do the following sub-steps:
    a. Click **[Choose files].**
    b. Select the firmware package from your local drive. You can select an individual or a full set package, but only one package can be chosen.
    c. Enter the description of the firmware package to be uploaded.
    d. Click the **[Upload]** button. By doing so, the firmware package will be uploaded to the cloud repository.
    e. Check the uploaded firmware package on the table. If the upload fails, an error message will display, and the firmware package will not be listed in the table.

    You can repeat steps **a** to **e** if you plan to upload more firmware packages.

To continue creating the firmware template, select one firmware from the table. If you want to set the previously uploaded firmware packages, change the option to "Use File in Repository" and choose the firmware package.

8. After selecting firmware, click **[OK].**

Applying a firmware update to an incompatible device results in a “Partial Failure” and is displayed in the Device Activity Logs.

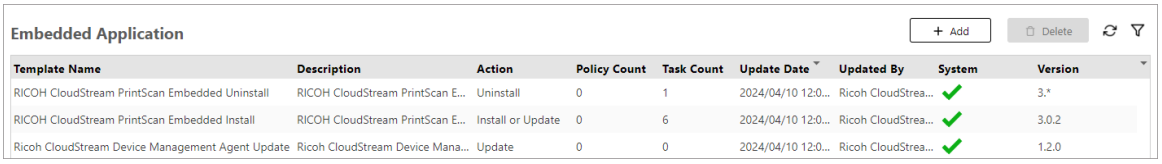
Embedded Application

Use the Embedded Applications template to install, activate, update, or uninstall the Print & Scan embedded App on the device(s).

Please note the following important information:

If the target devices do not have a built-in HDD installed, you must install an HDD before deploying an RICOH CloudStream Print&Scan Embedded. Please refer to Supported Printers on page 380 for the list of printers that require additional storage.
When installing the RICOH CloudStream Print&Scan Embedded, configure the required access accounts before executing the Embedded Applications template. For more details, refer to Access Profiles and Accounts on page 287.
When the RICOH CloudStream Print&Scan Embedded is installed on the Ricoh devices without the VM Card option, the device does not enter Sleep mode.
Only the Print&Scan Embedded app is supported.
Installation of other vendor's applications is not supported.

By default, the system creates three default embedded templates.



- RICOH CloudStream Device Management Agent Update: Use this embedded template to update the DM Agent application installed on the devices. Follow the instructions in Update the DM Agent Application on page 286 to use this template.
- RICOH CloudStream Print&Scan Embedded Install: Use this embedded template to install the Print&Scan embedded in target devices. Refer to Install Print&Scan Embedded App on page 281 for details.
- RICOH CloudStream Print&Scan Embedded Uninstall: Use this embedded template to uninstall/remove the Print&Scan embedded from target devices. Refer to Uninstall Print&Scan Embedded App on page 284 for details.

The default embedded templates are marked as checked under the System column, indicating that they are embedded templates that use the global version of the embedded application, and you cannot delete them. You can view the application version in the Version column.

If you want to create a new embedded template, follow the steps below.

1. Login as an administrator
2. Go to ***Device Configuration***, expand the ***Device Configuration Template***, then click ***Embedded Application.***
3. Click **[Add].**
4. Enter the ***Template Name.***
5. (Optional) Enter the ***Description.***
6. Select an option from the drop-down menu. Choose one of the following options:

Options	Description
Use File in Repository	When selected, the list of embedded application files uploaded to the cloud repository is displayed.
Uninstall	Select the Embedded Application to be uninstalled from the [Application Name (Product ID)] menu. The list of applications obtained from device information is displayed for the selected items in the menu.
Upload New File to Repository	This method uploads the Embedded Application file to the repository. After uploading, you can select the uploaded file in the list to create an embedded application template. This method is used only to apply a custom package and is not normally used.

Option: Use File in Repository

If required, upload the target embedded application file to the cloud repository first before picking the file when you create the embedded application template. To do so, please check **Option: Upload New File to Repository.**

a. Select **Use File in Repository** as an option.

b. Select the embedded application from the table. You can select only one application to create the template.

Option: Uninstall

Choose this option to uninstall the embedded application from the target devices.

a. Select **Uninstall** as an option.

b. Select the ***Application Name (Product ID)*** to be uninstalled.

c. Depending on the Application Name selected, the ***Version to uninstall*** will list all versions available for the selected application. The drop-down ***Version to uninstall*** has a default value of "All," allowing users to uninstall all versions of the application from the target device.

Option: Upload New File to Repository

To upload a new file to the repository, select "Upload New File to Repository", then do the following sub-steps:

a. Click **[Choose files].**

b. Select the embedded application from your local drive. You can select only one application at a time.

c. Enter the description of the embedded application to be uploaded.

d. Click the **[Upload]** button. By doing so, the embedded application will be uploaded to the cloud repository.

e. Check the uploaded embedded application in the table. If the upload fails, an error message will display, and the embedded application will not be listed in the table.

You can repeat steps **a** to **e** if you plan to upload more embedded application files.

7. After selecting an embedded application, click **[OK].**

The embedded application template is listed in the Embedded Application table. The template can now be used to create a Configuration Task on page 272 or Device Policies on page 261.

Device Policies

Device policies allow you to create policy templates containing company security standards, network requirements, etc. Assign them to target devices and monitor the devices' compliance with the policy in the Device Policy Compliance dashboard. Refer to Device Policy Compliance on page 55 for more details.

For example, your company requires all Ricoh MFPs to use the SMB protocol and other settings. To configure the devices and monitor the device's compliance with the requirement, you can create a device configuration template and then create a configuration policy. When executing the policy, use the Device Policy Compliance dashboard to identify which devices are out-of-policy or in-policy. You can also view the policy columns in the Device List to determine the specific version of an application currently applied to each device.

Device policies have three types, each comprising a configuration template, the enforcement type, and target devices or groups.

- **Configuration Policy** - A policy for device preferences.
- **Firmware Policy** - A policy for firmware files.
- **Embedded Policy** - A policy for embedded applications.

Prerequisites
Configuration Templates are created. Please see Device Configuration Template on page 236 for details on how to create the template.
The target devices that the template will be applied or checked must be added to CloudStream DM.

Follow the instructions below to set up the device policies.

Order	Instructions
1	Set the Policy Check. Go to Device Polling on page 294 and set time at which Policy Check should run.
2	Create a Device Policy on page 263. The steps found in this link are applicable for all three types of device policies. (Configuration Policy, Firmware Policy, Embedded Policy)
3	Manage Device Policies on page 268. This topic includes disabling device policies.

Differences between Device Policy and Configuration Task

You may have clarification on device policy and configuration tasks. Here is a comparison of the two.

Device Policy	Configuration Task
The policy's templates are applied every day based on the time of the day set in the Policy Check. Please see Device Polling on page 294 for more details.	You must click the run button to check or apply the configuration templates.
You can only select one firmware template per firmware policy and one embedded template per Embedded policy.	You can select multiple templates for one configuration task.
Use ***Device Policy*** if you want a configuration, a firmware package, or an embedded application to be checked or applied to a device daily. For example: Suppose you want to make all devices always enable ***Toner Saving***. In that case, you must create an SDP template with such configuration, then create a ***Configuration Policy*** that applies the template to the target devices. The set ***Policy Check*** time of day is 23:00 (11 PM). After saving the ***Configuration Policy***, the policy will automatically run at 11 PM. It will continue to run every day at 11 PM. The configuration policy ensures that the devices comply with the created policy. Running the policy means that the template's value is compared to the device. It will skip if the device has the same value as the template. If the device value does not match the template, the template value will be	Use ***Configuration Task*** if you want to set a configuration, update firmware, or configure embedded applications to target devices in just one operation. The configuration task will only run if you press the **[Run]** button. For example: You want to install an embedded application to the device. Create the embedded template, then use that template to create the Configuration task with the 'Apply' task type. Assign the task to target devices, then click **[Run].** By doing so, the template will be applied to the device. Unlike the device policies that runs every day after you create it, the configuration task will run every time you click the button.

Device Policy	Configuration Task
applied to the device.	

Create a Device Policy

All three types of device policies require at least one template and one device or group.

This topic will cover the common steps to create a device policy. Before you begin, please be informed of the following:

- A **Configuration Policy** uses device preferences template. Create this type of template if you would like to implement a policy that checks the device compliance to the configured SDP or XDP template.
    - Standard Device Preferences (SDP) on page 238.
    - Extended Device Preferences (XDP) on page 247.
- A **Firmware Policy** uses only the Firmware Template on page 256. Create this type of policy if you would like to check the device's firmware version is the same as the template you configured. If the device's firmware version is not the same, the firmware will be updated. The policy compliance checking happens every day.
- The **Embedded Policy** uses only the Embedded Application on page 258. Create this type of policy to make sure the device's embedded application version complies to the set embedded template.

Important: All policies will be applied to the target devices every day at the time set in Policy Check polling. For example, the device's settings, embedded version, and firmware version changed policies will all run and apply the settings back to the defined configurations. For more details, please see Device Polling on page 294.

Prerequisites

If you would like to select target groups for the policy, please select the group in the Display Settings on page 127.

Go to ***Target Device Association Category*** and choose the group you would want to display in the ***Device Policies*** device selection.

The following steps are applicable to all three types of policies. Please follow the instructions to create a device policy.

Order	Instructions
1	Enter the name of the device policy and select the enforcement type.
2	Select a template or multiple templates for configuration policy.
3	Add target devices or groups. Users can select devices and groups.

1. Login as an administrator.
2. Go to ***Device Configuration***, then expand ***Device Policies.***
3. Select the type of policy you will create.
   a. If you want to create a configuration policy, click ***Configuration Policies.***
   b. If you want to create a firmware policy, click ***Firmware Policies.***
   c. If you want to create an embedded policy, click ***Embedded Policies.***
4. In the policy you selected, click **[Add].**
5. Enter the name of the policy. The policy name must not be a duplicate of the existing policy. Optionally, enter a description of the policy.
6. Select the **Enforcement Type.**

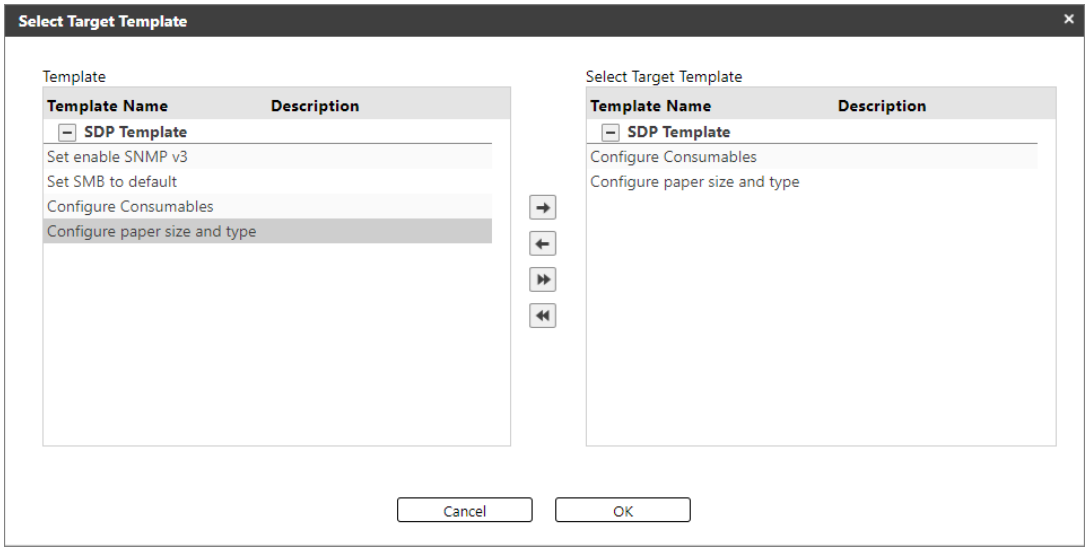
Enforcement Type	Description
Check	A “Check” enforcement type will compare the settings in the template to the target devices' values. You can see the result in the activity log found in device properties.
Apply	An “Apply” enforcement type will compare the template settings to the target device's values. Settings that do not match will be applied to the target devices. You can see the result in the activity log found in device properties. Devices may reboot one or more times depending on the applied settings.
Disabled	Select this type if you want to disable a policy. A policy that is disabled will not be executed during policy check.

7. Click **[Save].**

> **Important:** Please click [Save] button before going to the Templates and Target Devices node. If your policy is not saved, then you cannot add template and target devices.

8. Open the ***Template*** node.
9. Click **[Select Target Template].**

For **configuration policy**, the following will be displayed.



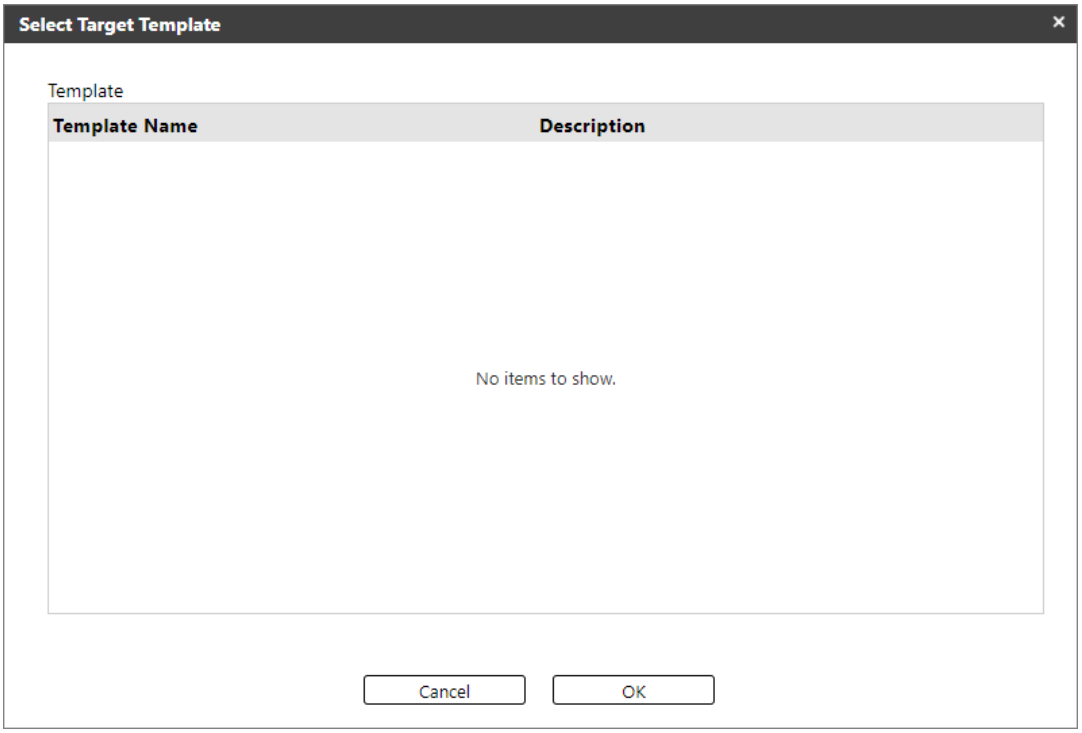
From the left-hand side, the ***Template*** pane lists all the available configuration templates. Select one or more templates, then click the right arrow button to add the template to the ***Target Templates*** pane.

Note: Please note that only the templates listed in the *Target Templates* pane will be added to the policy.

Button	Function
	Adds the selected template(s) to the ***Target Templates*** pane.
	Removes the selected template from the ***Target Templates*** pane.
	Adds all templates from ***Available Templates*** to the ***Target Templates*** pane.
	Removes all templates from ***Target Templates.***
OK	Closes the "Select Target Template" dialog, and the templates listed in the ***Target Templates*** pane are then displayed in a list with their template name and description. When clicked an error message will display if the ***Target Templates*** pane is empty.
Cancel	Cancels the selection of the templates.

For **Embedded and Firmware policy**, the following will be displayed.

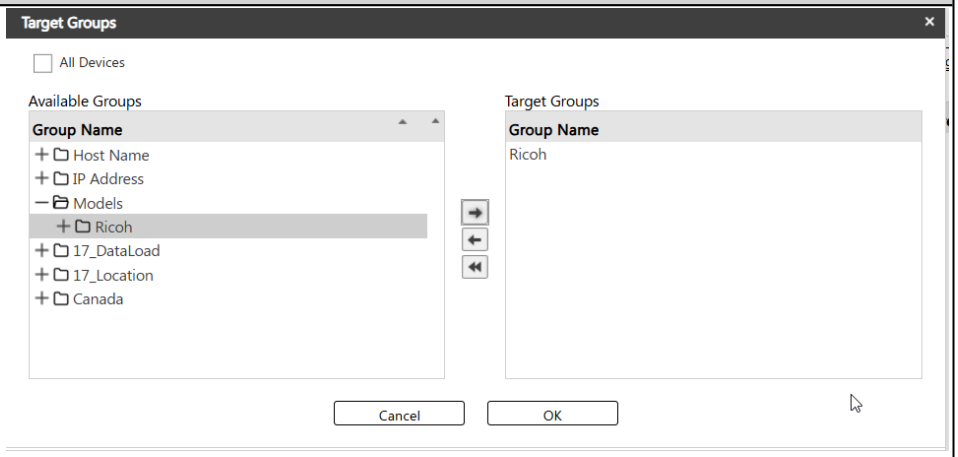
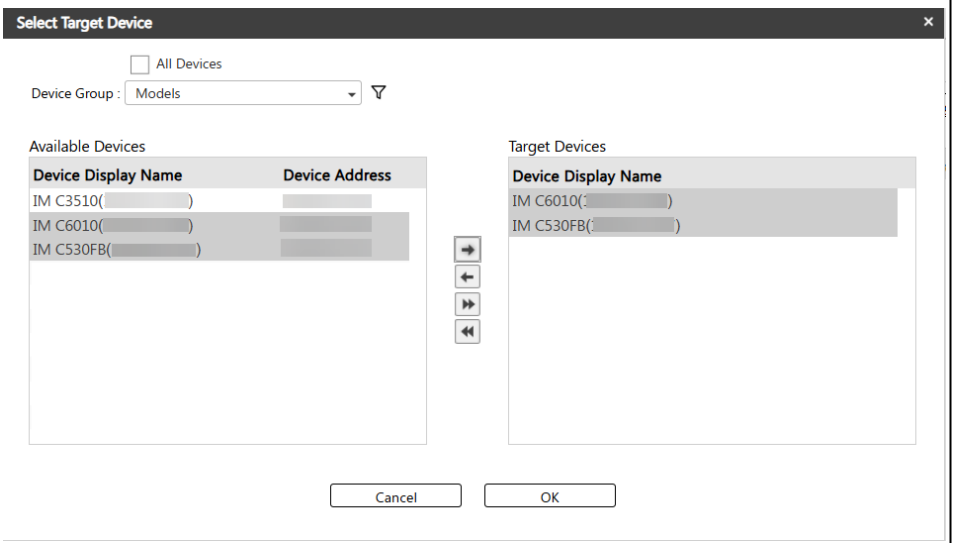
Please select a template from the list and click **[OK].**



10. Click **[Save].** You must save the templates selected before going to the next step.
11. Open ***Target Devices/Groups*** and add devices or groups.

To do so, you can use the two buttons below to populate the target devices and groups list.

Button	Function
Add Target Group	Clicking this button will display the "Target Groups" dialog. **Note:** If there are no available groups, please select the ***Target Device Association Category*** in Display Settings on page 127. The dialog contains the ***Available Groups*** pane and the ***Target Groups*** pane. The list of ***Available Groups*** is based on the Device List groups configuration, whose defaults are Host Name, IP Address, and Models group. Customized groups are also displayed and can be selected as a target group. Like the ***Template*** step, move the device groups from ***Available Groups*** to the ***Target Groups*** pane by clicking the → button. **Note:** If you want to select all devices, you can check the ***All Devices*** box. Checking this box will add all the devices and or groups to the target devices/groups.

Button	Function
	
Add Target Device	Clicking this button will display the "Select Target Devices" pop-up dialog. The dialog contains the ***Available Devices*** pane and the ***Target Devices*** pane. Like the ***Template*** step, use the  button to move devices from ***Available Devices*** to the ***Target Devices*** pane.  **Filter Devices** For easier selection, use the filter to search for the devices you want to add to the ***Target Devices*** pane. a. Select a device group. b. Click the  icon and enter the display name or the device's IP address into its corresponding column.

Button	Function
	c. Click the bottom icon, or just press enter from your keyboard. d. Devices that match the search will be displayed in the ***Available Devices*** pane. Select the device from the list. e. Click the button. You can also perform filtering from the ***Available Devices*** pane. **Note:** If you want to select all devices, you can check the *All Devices* box. Checking this box will add all the devices and or groups to the target devices/groups.

12. Click **[OK]** to add the devices/groups to the list.

You may use the following buttons to remove devices or groups from the list.

Button	Function
Delete	Removes the selected device or group from the list grid. You can also remove devices if you open the "Select Target Devices" dialog and remove the devices from the ***Target Devices*** pane. You can do the same in groups too.
Delete All	Removes all the devices and groups.

Manage Device Policies

Manage the device policies with the help of the following topics.

View Device Policy Results on page 268.
View the policy compliance dashboard. Device Policy Compliance on page 55.
Check Device Policy Status on page 269.
Disable a Configuration Policy on page 270.

Note: The above topics are applicable to all three device policies: Configuration Policy, Embedded Policy, and Firmware Policy.

View Device Policy Results

Device policies will run daily based on the Policy Check time of the day set in Device Polling on page 294. The result of this operation can be found in the device properties activity log.

The results vary based on the enforcement type selected.

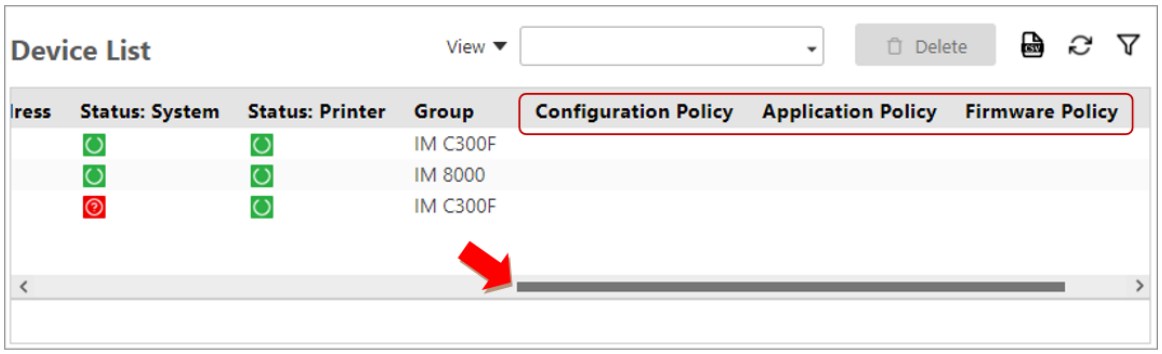
- If the selected enforcement type is ***Check***, the settings in the template are compared to the settings in the device. The 'Check' result of one configuration setting will either be:
  - **Match** - This indicates that the value of the template's setting is the same as the device's setting.
  - **Does not match** - This indicates that the value of the setting in the template and the device is different.
  - **Skip** - This indicates that the template's setting does not exist or is not supported by the target device.

  Important: If the enforcement type is "Check" the template is not applied to the target device; therefore, no policy has been applied yet. The policy monitoring will only take effect when the enforcement type is "Apply."

- If the enforcement type is ***Apply***, the settings in the template will be compared and then applied to the device. Only the settings whose value does not match the device will be applied. If the setting's value in both templates and devices is the same, it will not be re-applied.
  The 'Apply' result of one configuration setting will either be:
  - **Match** - This indicates that the value of the template's setting is the same as the device's setting; therefore, there is no need to apply the same value to the device.
  - **Success** - This indicates that the setting's value is applied successfully to the device.
  - **Fail** - Failed to apply the template setting's value to the device. Possible cause: device error, connection error, or incorrect access account. Please check the description of the error in the activity logs.
  - **Skip** - This indicates that the template's setting does not exist or is not supported by the target device.

Check Device Policy Status

When the device is set as one of the targets of a device policy, you can check its compliance to the policy in the Device List.



Scroll to the right to see the policy status columns.

If the policy columns is not displayed in the list, you can add them by the right-click menu. Select ***Columns*** then click on the policies you want to add to the list.

The device policies (Configuration Policy, Firmware Policy, Embedded Policy) has the following statuses:

Icon	Description
	"In-policy" The device is compliant to the policy.
	"Out-of-policy" The device is incompliant to the policy. To know why the device is out-of-policy, go check the device's Activity Logs on page 91 and see the result of the policy execution. More details about policy result in View Device Policy Results on page 268. To fix the incompliance, you can create a configuration task and run the template that the device is not compliant with. Refer to Configuration Task on page 272 for more details.
	"Unknown" Indicates that the device is not currently assigned to a policy.

Disable a Configuration Policy

Please follow the steps below to disable a configuration policy.

1. Login as an administrator.
2. Go to ***Device Configuration***, expand ***Device Policy***.
3. Select the policy: Configuration Policy, Firmware Policy, or Embedded Policy.
4. Select the device policy you want to disable.

5. On the General section, select "Disable" as the value of the Enforcement Type.
6. Click the **[Save]** button.

The configuration policy will become disabled after saving. A disabled device policy is skipped during the Policy Check. All target devices/models that belong to a disabled device policy are marked as “Unknown”.

Configuration Task

Configuration task allows users to check and apply configuration templates to target devices without associating the device with a policy. For example, you want to upgrade the devices' firmware in the New Device group. To do so, you must create a firmware configuration template containing the information about the firmware to be applied. Then you create a configuration task with the "Apply" task type. In this case, select the firmware template as the target template and the New Device group as target group. Run the configuration task to upgrade the devices' firmware in the New Device group.

In contrast to Device Policies on page 261, configuration templates will only be checked or applied when the run button is clicked.

To create a configuration task, the following are the prerequisites:

Prerequisites
Configuration Templates are created. Please see Device Configuration Template on page 236 for details on how to create the templates.
The target devices that the template will be applied or checked must be added to CloudStream DM.

Run a configuration task in three simple steps.

Order	Instructions
1	Create a Configuration Task on page 272. In this step you will select the template and the target devices/group.
2	Run a Configuration Task on page 277. Running the template will have different results depending on the selected task type.

Important: When running a configuration task, please make sure the target devices are powered on.

Create a Configuration Task

Follow these steps to create the configuration task:

Order	Instructions
1	Enter the name and select a task type. The task's name and the Task Type will determine the course of action when the task is executed.

Order	Instructions
2	(Optional) Select a template. If the task type is "Check Template" or "Apply Template," a configuration template is required. If the type is "Reboot", a template is not necessary.
3	Add target devices or groups. Add the target device and the target groups. Users can select both devices and groups.

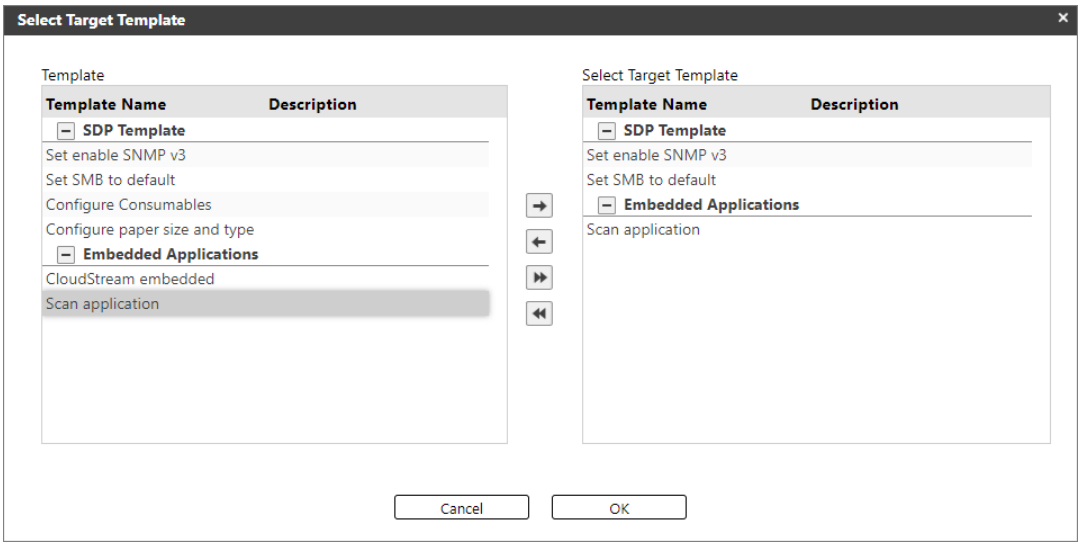
1. Login as an administrator.
2. Go to ***Device Configuration***, then click ***Configuration Task.***
3. In the ***Configuration Task*** screen, click **[Add].**
4. Enter the name of the configuration task. The task name must not be a duplicate of an existing configuration task.
5. (Optional) Enter the description of the task.
6. Select a **Task Type**.

   Select one of the three Task Types depending on how you want to run your configuration task.

Task Type	Description
Check	A “Check” task type will compare items in the configuration template to items from the target devices against which the template is executed. An activity log entry is recorded for the target devices to list the checked items and whether they match.
Apply	An “Apply” task type will compare items in the configuration template to items from the target devices against which the template is executed. The settings will then be applied to the devices. An activity log entry is recorded for the target devices to list the checked items and if they are a match or a change was applied. Devices may reboot one or more times depending on the setting items.
Reboot	When selected, the target devices will restart.

7. Click **[Save].** This will create the configuration template and display it on the list. You must save the template first before you can select the target templates and devices.
8. If the selected Task Type is "Reboot device", please go to step #13 to add the target devices.

9. If the selected Task Type is "Check Template" or "Apply Template", open the ***Template*** node.
10. Click **[Select Target Template].** A sample image is displayed below:



A "Select Target Template" pop-up dialog will display. On the left-hand side, the ***Templates*** pane lists all the available configuration templates. Select one or more templates, then click the right arrow button  to add the template to the ***Target Templates*** pane.

Note: Please note that only the templates listed in the *Target Templates* pane will be added to the configuration task.

Important: Please note the following important information:

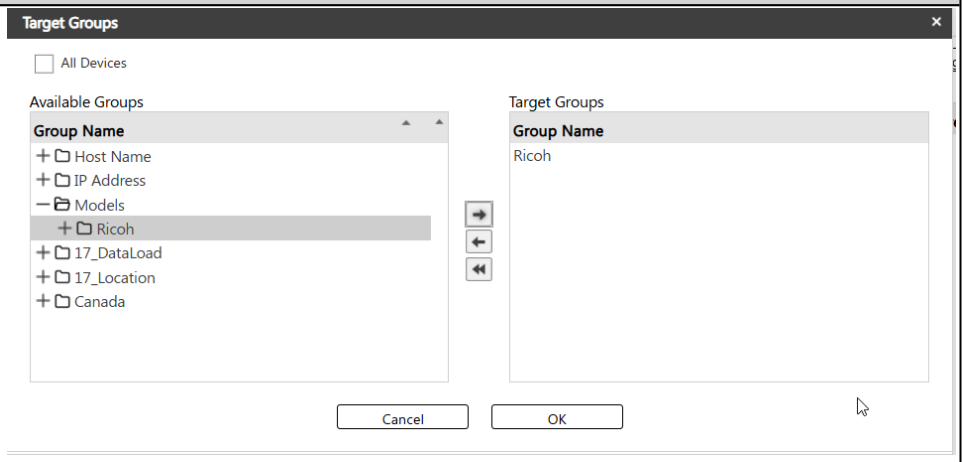
- Please select one firmware template per configuration task. If you want to use another template, please create another configuration task with a different firmware template and run them one at a time.
- When you run a configuration task that updates the firmware but get a "Partial Failure" result in the Activity logs, one possible cause is that the firmware applied is incompatible with the target device. Please check the compatibility of the firmware with the device.
- Please select one embedded template per configuration task. If you want to use another template, please create another configuration task with a different embedded template and run them one at a time.
- If you selected more than one embedded or firmware template, only the last template selected is applied.

Button	Function
	Adds the selected template(s) to the ***Target Templates*** pane.
	Removes the selected template from the ***Target Templates*** pane.

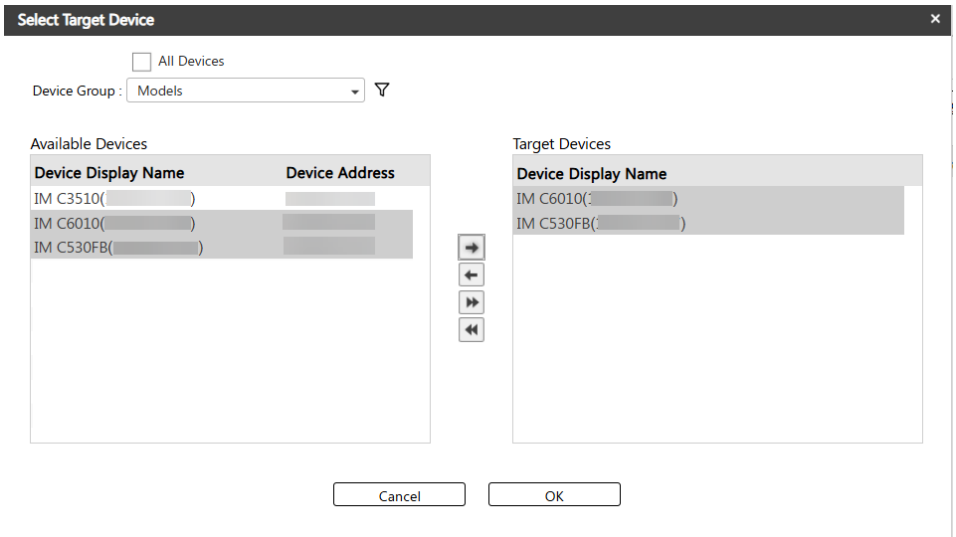
Button	Function
	Adds all templates from ***Available Templates*** to ***Target Templates*** pane.
	Removes all templates from ***Target Templates.***
OK	Closes the "Select Target Template" dialog, and the templates listed in the ***Target Templates*** pane are then displayed in a list with their template name and description. When clicked an error message will display if the ***Target Templates*** pane is empty.
Cancel	Cancels the selection of the templates.

11. Click **[Save].** You must save the templates selected before going to the next step.
12. Open ***Target Devices/Groups***.
13. Add devices or groups. To do so, you can use the two buttons below to populate the target devices and groups list.

Button	Function
Add Target Group	Clicking this button will display the "Target Groups" dialog. The dialog contains the ***Available Groups*** pane and the ***Target Groups*** pane. The list of ***Available Groups*** is based on the Device List groups configuration, whose defaults are Host Name, IP Address, and Models group. Customized groups are also displayed and can be selected as a target group. Like the ***Template*** step, move the device groups from ***Available Groups*** to the ***Target Groups*** pane by clicking the  button. **Note:** If you want to select all devices, you can check the *All Devices* box. Checking this box will add all the devices and or groups to the target devices/groups.

<table>
<tr><th>Button</th><th>Function</th></tr>
<tr><td></td><td> 
</td></tr>
<tr><td>Add Target Device</td><td>Clicking this button will display the "Select Target Devices" pop-up dialog.

The dialog contains the Available Devices pane and the Target Devices pane.

Like the Template step, use the  button to move devices from Available Devices to the Target Devices pane.
 

Filter Devices

For easier selection, use the filter to search for the devices you want to add to the Target Devices pane.

a. Select a device group.

b. Click the  icon and enter the display name or the device's IP address into its corresponding column.

c. Click the bottom  icon, or just press enter from your keyboard.</td></tr>
</table>

Button	Function
	d. Devices that match the search will be displayed in the ***Available Devices*** pane. Select the device from the list. e. Click  button. You can also perform filtering from the ***Available Devices*** pane. **Note:** If you want to select all devices, you can check the *All Devices* box. Checking this box will add all the devices and or groups to the target devices/groups.

14. Click **[OK]** to add the devices/groups to the list.

    You may use the following buttons to remove devices or groups from the list.

Button	Function
Delete	Removes the selected device or group from the list grid. You can also remove devices if you open the "Select Target Devices" dialog and remove the devices from the ***Target Devices*** pane. You can do the same in groups too.
Delete All	Removes all the devices and groups.

15. Click *Save*.

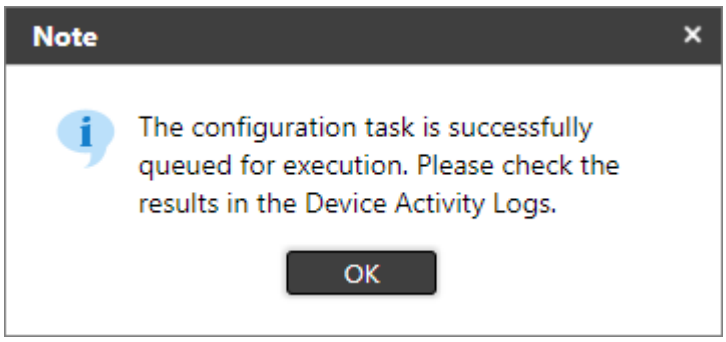
Run a Configuration Task

The configuration task will run based on the selected task type. To run the task, the following conditions must be met.

- If the task type is ***Apply*** or ***Check***, the configuration task must have at least one template and one target device or group.
- If the task type is ***Reboot***, the configuration task must have at least one target device or group.

Run the configuration task by clicking the **[Run]** 

button after selecting the task. If the task is successfully queued, you will see the following message.



Important: Please make sure the target devices are not powered off while the configuration is in progress.

If you encounter problems when running the configuration task, please refer to Troubleshooting tips on page 279

You can find the results in Device Properties then Activity Logs on page 91.

In the Activity logs, look for the configuration task name and select to see the details of the task execution.

The results vary based on the task type selected. Please check the action applied depending on the task type selected.

Task Type	Action
Check Template	If the selected task type is ***Check***, the settings in the template will be compared to the settings in the device. The 'Check' result of one setting will either be: • **Match** - This indicates that the value of the template's setting is the same as the device's setting. • **Does not match** - This indicates that the values of the setting in the template and the device are different. • **Skip** - This indicates that the template's setting is not found in the device. For example, the target device does not support Fax, but the template contains Fax-related settings. The Fax settings in the template will be skipped.
Apply Template	If the task type is ***Apply***, the template's settings will be compared and applied to the device. Please note that only the settings whose value does not match the device will be applied. If the setting's value in both templates and devices is the same, it will not be re-applied. The 'Apply' result of one setting will either be: • **Match** - This indicates that the value of the template's setting is the same as the device's setting; therefore, there is no need to apply the same value to the device.

Task Type	Action
	• **Success** - This indicates that the setting's value is applied successfully to the device. • **Fail** - Fails to apply the template setting's value to the device. Device errors, connection errors, or incorrect access accounts can cause this failure. Please check the description of the error in the activity logs. • **Skip** - This indicates that the template's setting is not found in the device.
Reboot Device	If the task type is ***Reboot Device***, the target devices will reboot with the possible result: • **Success** - This indicates that the device successfully restarted. • **Fail** - This means that the device reboot is unsuccessful. Please see the activity log for the description of the error. When running a Reboot(restart) task, two results will be shown in the Activity Logs on page 91. The first result says "Task Apply" indicating that the reboot request is submitted. Second result is "Task Reboot" which mean, the device is rebooting/ restarting.

Troubleshooting tips

The Configuration task should return a **success** result. If it fails, please see some troubleshooting tips below.

- Please ensure the device Access Accounts match the device settings.

  The SNMP, SDK/J, and Device Administrator access accounts must match the device's settings. Please see Access Profiles and Accounts on page 287 for more details.

- Please ensure that the device has a stable internet connection. This is a factor when deploying embedded tasks to several devices; ensure the device is online.

- Check if the DM Agent is working.

  One of the ways to know if your device can communicate to the CloudStream DM via DM Agent is by checking the poll time. You can check the ***Last Communication Time*** in the ***Device Properties,*** then the ***Main Properties*** section. The time must be relevant to the set polling interval. If the last communication time passed the polling interval, there is a possibility that your

DM agent is not working; thus, no device information was fetched. Please see Device Polling on page 294. In such a case, please re-install the DM Agent via the DM Agent Deployment Tool.

Install Print&Scan Embedded App

The RICOH CloudStream Print&Scan Embedded Install template in the Embedded Application page was created by the System so you can install the updated version of the embedded to your devices. Use this default embedded template to create a configuration task and apply it to the devices you wanted to manage.

Prerequisites
Prior to installing the embedded, make sure an embedded client is configured in RICOH CloudStream Print&Scan portal. Refer to Configure Print&Scan Embedded Client on page 222 for details.
If the target devices do not have a built-in HDD installed, you must install an HDD before deploying an RICOH CloudStream Print&Scan Embedded. Please refer to Supported Printers on page 380 for the list of printers that require additional storage.
Ensure the required ports 7400 and 8705 are open. Please refer to the table in Cloud Terminal Integration to Server on page 282.

To determine if a version of the RICOH CloudStream Print&Scan Embedded is installed on the device, refer to Identify Device DM/PS Version on page 73.

To create the configuration task, follow the steps below.

1. Login as administrator.
2. Go to ***Device Configuration*** section and click on ***Configuration Task.***
3. Click the **[Add]** button.
4. Enter the name of the task.
5. (Optional) Enter a description of the task.
6. Select the type of task you want to execute. In this scenario, choose '**Apply**'.

   There are three types of tasks.

Task Type	Description
Check	If selected, the configuration template settings are compared against the device's settings.
Apply	If selected, the settings in the configuration template are applied to the target devices. If the device has the same settings as the template, it will be skipped.

Task Type	Description
Reboot	If selected, the target devices will restart.

7. Click **[Save]** and go to the ***Template*** node.
8. Click **[Select Target Template].**
9. Select *RICOH CloudStream Print&Scan Embedded Install* and then click  to add the template to Target Templates pane.
10. Click **[Save]** then open ***Target Devices/Groups***.
11. Select the target devices or device groups, then click **[OK]** to create the configuration task.
12. Select the created configuration task and click the **[Run]** button.
13. Go to Device Properties then Activity Logs to see the results. More information is described in Activity Logs on page 91.

> **Important:** If you are installing the RICOH CloudStream Print&Scan Embedded on a GEN2 device via the Application Site, you must reboot the device. You can reboot the device manually or send a reboot configuration task to it.

14. (Optional) Verify if the embedded application was installed correctly in the MFP. To do so, follow the instructions below:
    a. Open the device's Web Image Monitor (WIM) by typing in the device's IP address in the browser.
    b. Login as device local admin.
    c. **Go to** *Device Management* **and select** *Configuration***.**
    d. Go to ***Extended Feature Settings*** then click ***Uninstall***.
    e. All embedded application installed in the device is displayed in ***Uninstall*** page. Confirm that the ***CloudStream PS*** application with type SOP is displayed in the list.

Cloud Terminal Integration to Server

Port	Protocol	From	To	Description
7400	TCP HTTPS	Printer	CloudStream Authentication Service	Cloud terminal integration – communicate with CloudStream Authentication Service to register as trusted endpoints
8705	HTTPS	Printer	CloudStream Terminal Client Service	Cloud terminal integration (SQTS) – connection from Cloud Terminals running on MFDs (e.g. HP Workpath Gen2, KM IWS Gen 2, Ricoh Gen 2) and for sending scanned jobs (e.g., HP Workpath Gen 2,

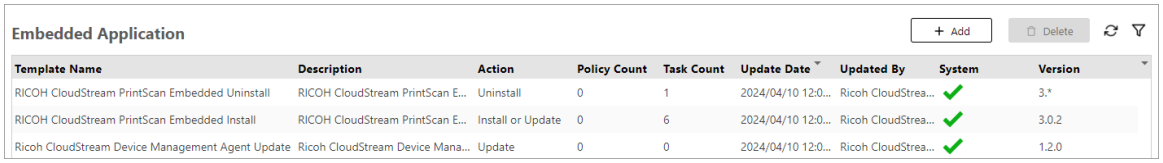
Port	Protocol	From	To	Description
				Ricoh Gen 2)
8706	TCP	Printer	CloudStream Terminal Client Service	Cloud terminal integration – connection from Cloud terminals running on MFDs

Uninstall Print&Scan Embedded App

It would help to do the following before uninstalling the RICOH CloudStream Print&Scan Embedded from the device.

Prerequisites
Removing the device from any device policy and alert policy is recommended.
Make sure the device is online when you are uninstalling the RICOH CloudStream Print&Scan Embedded.

Use the default embedded application ***RICOH CloudStream Print&Scan Embedded Uninstall*** when creating the configuration task.



To create the configuration task, follow the steps below.

1. Login as administrator.
2. Go to ***Device Configuration*** section and click on ***Configuration Task.***
3. Click the **[Add]** button.
4. Enter the name of the task.
5. (Optional) Enter a description of the task.
6. Select the type of task you want to execute. In this scenario, choose '**Apply**'.

   There are three types of tasks.

Task Type	Description
Check	If selected, the configuration template settings are compared against the device's settings.
Apply	If selected, the settings in the configuration template are applied to the target devices. If the device has the same settings as the template, it will be skipped.
Reboot	If selected, the target devices will restart.

7. Click **[Save]** and go to the ***Template*** node.
8. Click **[Select Target Template].**
9. Select *RICOH CloudStream Print&Scan Embedded Uninstall* and then click  to add the template to Target Templates pane.
10. Click **[Save]** then open ***Target Devices/Groups***.

11. Select the target devices or device groups, then click **[OK]** to create the configuration task.
12. Select the created configuration task and click the **[Run]** button.
13. Go to Device Properties then Activity Logs to see the results. More information is described in Activity Logs on page 91.

Update the DM Agent Application

You can update the DM Agent application installed on the devices by running a configuration task in CloudStream DM.

Make sure you have the following precondition.

Prerequisites
The target device is already added to CloudStream DM, and device is online.

1. Login as an administrator.
2. Go to ***Device Configuration***, then click ***Configuration Task.***
3. In the ***Configuration Task*** screen, click **[Add].**
4. Enter the name of the configuration task. The task name must not be a duplicate of an existing configuration task.
5. (Optional) Enter the description of the task.
6. Select **Apply** as **Task Type**, then click **[Save].**
7. Open the ***Template*** node, then click **[Select Target Template].**
8. Select *RICOH CloudStream Device Management Agent Update* and then click  to add the template to Target Templates pane.
9. Click **[Save]** then open ***Target Devices/Groups***.
10. Select the target devices or device groups, then click **[OK]** to create the configuration task.
11. Select the created configuration task and click the **[Run]** button.
12. Go to Device Properties then Activity Logs to see the results. More information is described in Activity Logs on page 91.

Access Profiles and Accounts

There are three types of access profiles, and you can create multiple access accounts for each type.

Device Administrator Access Profile on page 288.
SNMP Access Profile on page 290.
SDK/J Platform Access Profile on page 289.

You must create at least one account for each profile to add devices to CloudStream DM successfully.

Important: Ensure that the authentication information of the access account matches the authentication information configured on the device.

The authentication information of the device administrator must be the same as that of the printer administrator, who has all administrative privileges (Device Administrator, User Management, File Administrator, and Network Administrator).

Assigning Access Account

When a device is added to CloudStream DM, the DM Agent embedded selects the access accounts (SNMP, SDK/J, Device Admin accounts) that work with the device and assigns them as ***Profile***. You can see it in ***Device Properties*** > ***Access Profiles***.

Access accounts used by at least one device cannot be deleted from the Access Accounts screen.

Important: When the access account settings do not match the device's accounts, or vice versa, the DM Agent embedded will look for other accounts in the Access Account screen that works, then assign the accounts to the device and carry on the task.

If no accounts match the device in the Access Account screen, the DM Agent will fail to communicate with CloudStream DM. The DM Agent will try again on the next polling and check if a working account has been created that matches the device's accounts.

To view the device's assigned access account, do the following:

1. Select the device from the ***Device List.***
2. The ***Device Properties*** is displayed; click the ***Access Profiles*** node.
3. Each Access Profile has a setting named "Profile Name". Check the accounts profile and its details displayed as read-only.

Device Administrator Access Profile

Device Administrator Access Profile allows you to create administrator accounts to communicate with devices.

The devices administrator account refers to the account used to log in to the device via the operational panel or from the Ricoh Web Image Monitor (WIM).

You can find the following settings in a device administrator account.

Item Name	Description
Profile Name	The device administrator account profile name.
Description	Description of the device administrator account.
User Name	Enter the user name. The user name can contain up to 32 characters.
Password	Enter the password. The password can contain up to 128 characters. The password will display as masked for security reasons.

Create a Device Administrator Access Account

1. On the left-hand navigation pane, click ***Device Configuration.***
2. Expand ***Access Profiles.***
3. Click ***Device Administrator.***
4. Click **[+ Add].**
5. Enter the ***Profile Name***. The profile name must not be a duplicate of an existing profile.
6. Enter the ***User Name***. This is the device's local administrator user name.

   Note: The user name must not contain the following characters: **":**
   User name with only numbers (0-9) and is less than 9 digits is not accepted.
7. Click **[Change...]** to edit the password field.
8. In the pop-up dialog, input the device's local administrator password and confirm the password, then proceed to click **[OK]**.
9. (Optional) Enter the profile description.
10. Click **[Save].**

The new device administrator access account is displayed in the list grid.

Edit and Delete Account

To view and modify the account's information, select the account from the list, then click **[Save]** after making the necessary changes.

To delete, select the device administrator profile and click **[Delete].** Click **[OK]** on the dialog to confirm the removal of the account. An error will be displayed if the account is still in use.

Important: You cannot delete an access account still being used by a device.

Note:

- To create an SNMP account, go to SNMP Access Profile on page 290.
- To create an SDK/J Platform account, go to SDK/J Platform Access Profile on page 289.

SDK/J Platform Access Profile

You can find the following settings in an SDK/J Platform account.

Setting Name	Description
Profile Name	The device administrator account profile name.
Description	Description of the device administrator account.
Password	Enter the password. The password can contain up to 128 characters. The password will display as masked for security reasons.

Create an SDK/J Platform Access Account.

Follow the instructions below to create an SDK/J Platform account profile.

1. On the left-hand navigation pane, click ***Device Configuration.***
2. Expand ***System Access Profiles.***
3. Click ***SDK/J Platform.***
4. Click **[+ Add].**
5. Enter the ***Profile Name***. The profile name must not be a duplicate of the existing profile.
6. Click the **[Change...]** button to edit the password field.
7. In the pop-up dialog, input the SDK/J Platform password, confirm the new password, then click **[OK].**

8. (Optional) Enter the profile description.
9. Click **[Save].**

The new SDK/J Platform access account is displayed in the list grid.

Edit and Delete Account

To view and modify the profile's information, select the profile from the list, then click **[Save]** after making the necessary changes.

To delete, select the SDK/J Platform profile and click **[Delete].** Click **[OK]** on the dialog to confirm the removal of the account. An error will be displayed if the account is still in use.

Important: You cannot delete an access account still being used by a device.

Note:

- To create an SNMP account, go to SNMP Access Profile on page 290.
- To create a Device Administrator account, go to Device Administrator Access Profile on page 288.

SNMP Access Profile

There are two SNMP protocols to use. Depending on the configuration of the devices, you can create as many SNMP Access Accounts as you want.

In this section, you will find the following topics.

Create SNMP v1/v2 Access Account

Note: Details of each setting described in the steps are found in SNMP Settings List on page 292.

1. On SNMP Access Profile, click **[+ Add].**
2. Enter the ***Profile Name***. The profile name must not be a duplicate of an existing profile.
3. (Optional) Enter the profile description.

4. Specify the ***Retry*** value. The default is 2, and you can modify it to any value from 0 to 5.
5. Specify the desired ***Timeout*** value. The default is 3000; and you can modify it to any value from 500 to 60000.
6. Choose **SNMP v1/v2** as **Protocol.**

   Note: The Read and Write community name is displayed when the selected protocol is SNMP v1/v2.

7. Enter a value to ***Read Community Name***. The default value is "public", and this is a required field.
8. Enter a value to ***Write Community Name***. The value entered will display as masked for security, and this is a required field. By default, this field is empty.
9. Click **[Save].**

The new SNMP v1/v2 access account is displayed in the list grid.

Create SNMP v3 Access Account

Note: You can find the details of each setting described in the steps in SNMP Settings List on page 292.

1. On SNMP Access Profile, click **[+ Add].**
2. Enter the ***Profile Name***. The profile name must not be a duplicate of an existing profile.
3. (Optional) Enter the profile description.
4. Specify the ***Retry*** value. The default is 2, and you can modify it to any value from 0 to 5.
5. Specify the desired ***Timeout*** value. The default is 3000; and you can modify it to any value from 500 to 60000.
6. Choose **SNMP v3**as **Protocol.**
7. Enter ***User Name.***
8. Enter the ***Password*** by clicking **[Change...].**, then confirm the password and click **[OK].**
9. Select the ***Authentication Algorithm.***
10. Enter the ***Context Name***. The default value is "GWNCS". This is not a required item and can be left blank.

11. Enter the ***Encrypted Password*** by clicking **[Change...]**, then confirm the encrypted password and click **[OK].**
12. Select the ***Encryption Algorithm*** to be used.
13. Click **[Save].**

The new SNMP v3 access account is displayed in the list grid. You can create as many SNMP v3 access accounts as you like.

Edit and Delete SNMP Account

To view and modify the profile's information, select the profile from the list, then click **[Save]** after making the necessary changes.

To delete, select the SNMP profile and click **[Delete].** Click **[OK]** on the dialog to confirm the removal of the account. An error will be displayed if the account is still in use.

Important: You cannot delete an access account that is still being used by the device.

Note:

- To create an SDK/J Platform account, go to SDK/J Platform Access Profile on page 289.
- To create a Device Administrator account, go to Device Administrator Access Profile on page 288.

SNMP Settings List

Setting Name	Description
Profile Name	Enter the SNMP account profile name.
Description	Enter the description of the SNMP account.
Retry	Specify how many retry attempts can be performed if a device does not respond during discovery.
Timeout	Specify how long the waiting period is if a device does not respond during discovery. Specify a value between 500 and 60000 milliseconds.
Protocol	Select the type of protocol. • SNMP v1/v2 • SNMP v3 Configuration items vary depending on protocol types.
Read Community	Specify this item when ***SNMP v1/v***2 is selected in ***Protocol***. The Read Community Name can contain up to 15 characters.

Setting Name	Description
Name	
Write Community Name	Specify this item when selecting ***SNMP v1/v2*** in ***Protocol***. The Write Community Name can contain up to 15 characters.
User Name	Specify this item when selecting ***SNMP v3*** in ***Protocol***. The user name can contain up to 32 characters.
Password	Specify this item when selecting ***SNMP v3*** in ***Protocol***. The password can contain up to 128 characters.
Authentication Algorithm	Select the authentication algorithm. • SHA1 • MD5 • SHA2 (224 bit) • SHA2 (256 bit) • SHA2 (384 bit) • SHA2 (512 bit) Specify this item when selecting ***SNMP v3*** in ***Protocol***.
Context Name	Specify this item when selecting ***SNMP v3*** in ***Protocol***. The context name can contain up to 256 characters.
Encrypted Password	Specify this item when selecting ***SNMP v3*** in ***Protocol***. The encrypted password can contain up to 32 characters.
Encryption Algorithm	Select the encryption algorithm. • DES • AES128 Specify this item when selecting ***SNMP v3*** in ***Protocol***

Device Polling

The polling sub-section contains polling information applicable to added devices and Work from Home devices.

Note: Please note that Polling is executed based on the time zone of the administrator who set the Polling Time settings.

Here is a list of polling information you can find on this page.

- Status Polling on page 294.
- Supplies Polling on page 294.
- Counter Polling on page 294.
- Other Polling on page 295.
- Policy Check on page 295.
- Work from Home Polling on page 295.

Status Polling

Item Name	Description	Possible Values	Default Value
Check Interval	Indicates how often the device status is checked internally by the embedded DM Agent in seconds. The status information will only be posted to CloudStream DM if something has changed since the previous check. Otherwise, nothing will be sent.	5 to 999	5
Heartbeat	Indicates how often DM Agent will post the device status to CloudStream DM in minutes. If nothing has changed from ***Check Interval*** for the minutes configured in the ***Heartbeat***, the information will still be posted to CloudStream DM. The ***Heartbeat*** updates the status of each polling type (Status, Supplies, Other).	15 to 999	30

Supplies Polling

Item Name	Description	Possible Values	Default Value
Check Interval	Indicates how often the supplies information will be retrieved internally and posted to CloudStream DM.	30 to 999	60

Counter Polling

Item Name	Description	Possible Values	Default Value
Time of Day	Counter polling will run based on the specified Time of the Day in a 24-hour format. The field accepts a value in HH:MM format.		23:00

Other Polling

Item Name	Description	Possible Values	Default Value
Time of Day	Other polling will run based on the specified Time of the Day in a 24-hour format. The field accepts a value in HH:MM format.		23:00

Policy Check

Item Name	Description	Possible Values	Default Value
Time of Day	The Policy Check will run based on the specified Time of the Day in a 24-hour format. The field accepts a value in HH:MM format. When the Policy Check runs, all Device Policies on page 261 with enforcement type other than "Disabled" will check or apply the policy templates. **Important:** Depending on your policy template, the target devices are required to be online and not in use during the set time of the day. It is recommended to set a time where no one is using the devices.		23:00

Work from Home Polling

Item Name	Description	Possible Values	Default Value
Check Interval	The interval will be used by WfH Client service to poll device information such as status and counters. After polling, the information is reflected in the WfH device properties if the device state is accepted.	Minimum of 1 hour and a maximum of 24 hours	3 hours
New Work From Home Device Detection	This setting determines the status of the newly detected WfH device. The available modes are: • **Auto-accept**: If selected, all new devices reported by a WfH Client will be		Auto-accept

Item Name	Description	Possible Values	Default Value
	automatically added as a tracked device and be in the "Accepted" state, which is the default mode. • **Put into pending state**: When this mode is selected, all new devices are put into the "Pending" state and will not be tracked. The administrator will have to manually accept the devices in the WfH group of the device properties.		

On-Premise Device Monitoring

The On-Premise Device Monitoring service (DMS) allows you to monitor RICOH devices and 3rd party manufactured devices such a Brother.

Important: On-Premise refers to the **server location** only; on-premise devices are not supported.

This service applies only to devices that do not have the DM Agent installed. This service provides monitoring functionality of up to 5000 devices and does not support device management. In cases where you have upwards of 5000 devices, you can dedicate and install the service on a second server.

Devices discovered via the service can poll for the following device information:

Note: The information that can be retrieved from a device is dependent on the model. Dashboards and reports will contain all status and counter information that is retrieved by the Device Monitoring service.

Information	Details
Counters	Total, Copy Black, Copy Color Full, Printer Black, Printer Color Full, Fax Black, Duplex, Total Mono, Total Color
Status	System, Printer
Toner	Toner levels
Properties	Model Name, Vendor Name, Serial Number, MAC Address, Location, Comment

Server Requirements

The server hosting the DMS must meet the following system requirements.

Component	Recommended	Minimum
Server	CPU: • Intel Xeon E5 v2 series or better • AMD Opteron 3300/4300/6300 series or better Available Memory: • 4 GB Available HDD space:	CPU: • Intel Core i5-2300 series or better • Intel Xeon E3 series or better • AMD FX 4200 series or better • AMD Opteron 3200/4200/6200 series or

Component	Recommended	Minimum
	• 3GB	better Available Memory: • 2 GB Available HDD space: • 2 GB
Operating System	• Windows Server 2019 Std/Datacenter/Essentials (64-bit) • Windows Server 2022 Std/Datacenter	
Virtual Environment	• VMWare EsXi 7.0 • VMWare ESXi 8.0 • Windows Server 2019 Hyper-V • Windows Server 2022 Hyper-V	
Database	• Microsoft SQL Server 2019 (Express/Standard/Enterprise) • Microsoft SQL Server 2022 (Express/Standard/Enterprise)	

Ports

Protocol	Port
SNMP	161
HTTPS	443

Device Monitoring Limitation

Devices monitored by the DMS are not supported and will not be removed as target devices when performing the following:

- Extended Device Preferences (XDP) Get setting from device
- Standard Device Preferences (SDP) Get setting from device
- Configuration Task (Add Target Device Only)
- Configuration Policies (Add Target Device Only)
- Firmware Policies (Add Target Device Only)
- Embedded Policies (Add Target Device Only)

Brother MPS Integration

CloudStream can integrate with the Brother automated consumable delivery system (MPS). Brother MPS is supported in major countries in RE region only.

The integration requires installation of the Device Monitoring Service on a separate server to provide monitoring functionality of up to 5000 Brother devices. Note the service does not support device management.

Note: For a list of supported Brother models, refer to https://supportsite.eu.cloudstream.ricoh.com/product/device-support/brother/

Follow the procedures linked below to complete the integration:

1	Device Monitoring Service Installation on page 299	Review the server requirements in On-Premise Device Monitoring on page 297 and then complete the installation tasks. The installer is available in CloudStream from System → Software Download and locate the Device Monitoring Service. Click on the version number to begin the download.
2	Device Monitoring Service Polling & Discovery on page 303	Perform discovery from the Device Monitoring Service that appears under Device Configuration. The discovery range should include all Brother devices that will be monitored from CloudStream.
3	Identify Device Monitoring Discovered Devices in the Device List on page 306	Confirm that the Brother device(s) have been added to the Device List.
4	Polling & Discovery Settings on page 305	Configure polling timing for devices polled by the Device Monitoring Service.
5	Create an Alert Policy for Brother Consumables on page 208	Create an alert policy with custom messaging for specific Brother alert triggers.
6	Run the Device Consumables Replace for Brother MPS Report on page 338	Create a report task to run on a daily schedule with specific parameters needed for Bother devices.

Device Monitoring Service Installation

You can find the following information on this topic.

Prerequisites

Before you start the installation of the Device Monitoring Service (DMS), note the following prerequisites.

Prerequisites
The installer is available to download from CloudStream under the Systems section. Click the version number to start the download. 1. Go to ***Systems.*** 2. Click ***Software Download.*** 3. Select ***Device Monitoring Service***. Click the version number. The download will start immediately.
Gather the following information that will be requested by the installer: • **Device Monitoring Onboarding code:** See Generate Onboarding Codes on page 148. • **Service Locator Address and Server port:** You can copy your service locator in Certificates and Service Locator URL on page 145. • **Proxy Server:** If you will use a proxy server, gather the proxy server information. • **SQL Database:** You will need the SQL server database address, port and database name. You will also need the SQL database authentication credentials. If you do not have a SQL Server installation available, you will need to install SQL Server (full or express). See Configure SQL Server Configuration Manager on page 307. If you are using SQL Express, you may need to configure SQL Express to enable TCP/IP. • **SNMP Authentication:** The DMS will use the profiles created in SNMP Access Profile on page 290 to authenticate with discovered devices.

Installation

Important: Check the version of Java installed on the machine. If Java SE version 17 or later is installed, you must uninstall Java SE before proceeding. The installer will check to determine if Amazon Coretto 17 is installed on the server. If not, a notification message is displayed and you must click Install to proceed. The DMS install will proceed automatically after a successful Corretto install.

1. Run the installer. Choose the Installation language to proceed.
2. In the Welcome screen, click **[Next]**.

3. In the Destination Folder screen, you can change the folder where the DMS will be stored by clicking the **[Change...]** button.
4. In the Service Logon Information, select the credentials to use to run the service.
    - Login as System Account - Uses the credentials used to login to the server.
    - Login as Windows Account - Uses the specified Windows credential.
5. Specify the Friendly Name.

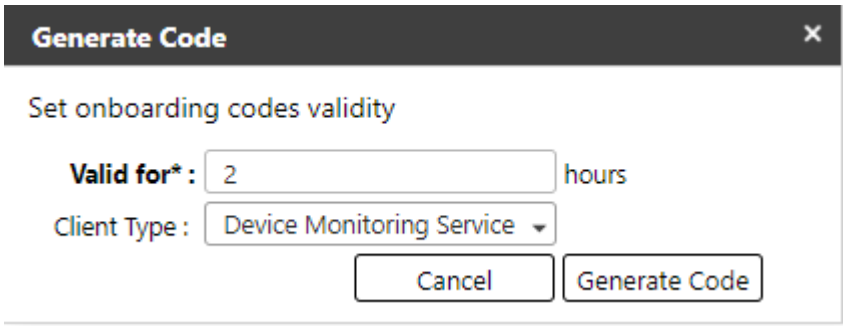
    This name will be displayed in the Customer Portal as the DMS name.

    By default, the value is the name of the computer on which you are installing the DMS.
6. Specify the Onboarding Code.

    Generate an Oboarding code in Customer Portal.

    Go to System> Security> Client Certificate, then generate a DMS onboarding code.

    Ensure that the code you generated does not expire while you are installing the DMS. Generate another code if it expires.



7. Input the Service Locator without the "https://"

    Copy the Service Locator address on the Client Certificate page.

    The default port is 433.
8. If using a proxy server, check "Enable HTTP Proxy", and then input the needed information; if not, leave it unchecked.
9. On the SQL Server Database screen, do the following.
    a. Input the name of the server hostname or the IP address where the MS SQL is configured.
    b. Input the port used by the database. The default port is 1433.

c. The value "ricoh_cs_dmservice" is used as the Database name.

d. Check "Run database creation scripts" if the DMS database has not yet been created. If the database is created already, you do not need to check "Run database creation scripts."

10. Specify the credentials in the Database Logon Information screen.

    Select whether to use windows authentication to access the SQL server or to specify a credential that has access to the SQL Server.

    If you enabled "Run database creation scripts", the "Test connection" button will allow you to check if the credentials you provided can access the MS SQL. Ensure that you enter a working credential to proceed with the installation. If the test connection returns a fail, please check if you have access to the MS SQL and if you are using the correct port.

11. Click **[Install]** to proceed.

If the credential you specified in Service Logon Information (Step 3) cannot authenticate, you will see the message "Service RICOH CloudStream DM Service failed to start."

After a DMS is installed and a certificate is issued, the service will appear in the Customer Portal.

Uninstallation

It is recommended to remove the Device Monitoring application from Microsoft Windows prior to deleting the Device Monitoring Service in CloudStream:

1. Uninstall the DMS software via Microsoft Windows Apps & Features functionality. The application name to uninstall is CloudStream Device Monitoring Server.
2. Go to ***Device Configuration***, then click ***Device Monitoring Service.***
3. Select the Device Monitoring service from the list, and then click **Delete**.
4. You can now optionally delete any devices that were discovered and monitored by the Device Monitoring Service. Refer to Delete Devices on page 306 for instructions.

Upgrade

To upgrade to a new version of the Device Monitoring application, download the latest installer from the Software Downloads page in CloudStream. For an upgrade, the Onboarding code,service locator URL and database set-up details are gathered from the existing install and are not requested during the upgrade process.

1. Run the installer.
2. Select the language.
3. Enter the Service Login information, and then click **Install** to proceed.
4. Once complete, click **Finish** to close the installer.

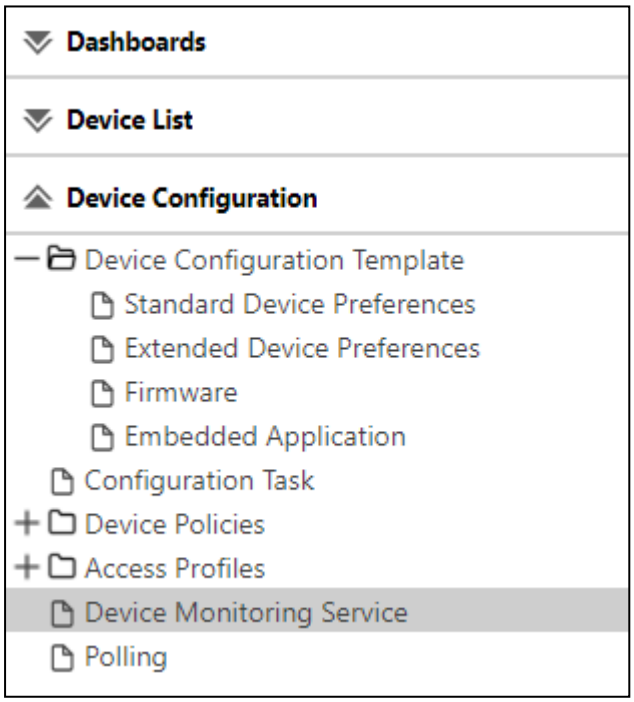
Device Monitoring Service Polling & Discovery

You can find the following information on this topic.

Device Discovery Range on page 303.
Polling & Discovery Settings on page 305.
Identify Device Monitoring Discovered Devices in the Device List on page 306

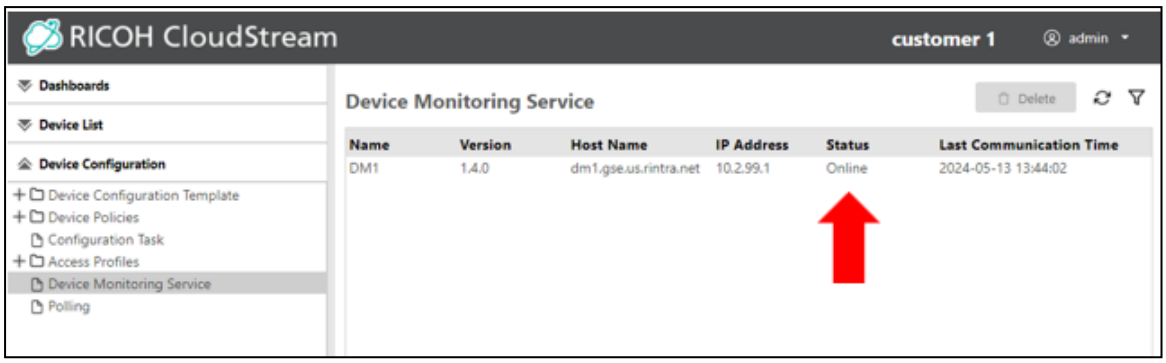
Device Discovery Range

When a new Device Monitoring Service (DMS) is registered with CloudStream, a new DMS option appears in the Device Configuration list.



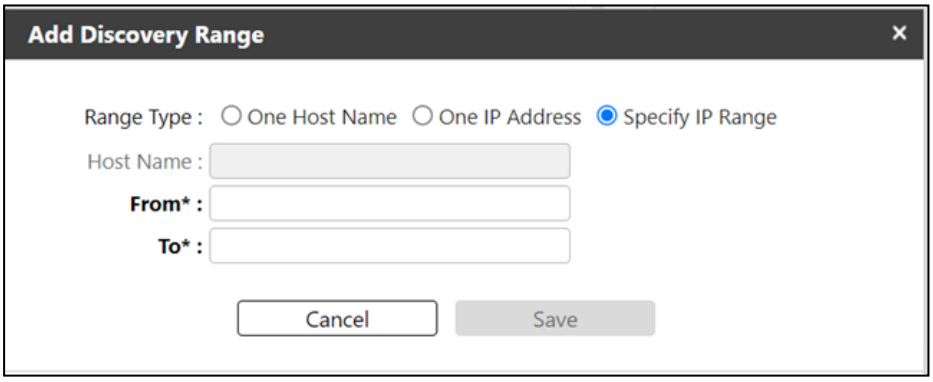
All DMS's that have registered with your Customer ID are listed on this screen. The name refers to the "Friendly Name" created during installation.

Note: The status reports either "online" or "offline". If no services have been contacted by the DMS for more than 15 minutes, the status is reported as "offline".



1. To set the discovery range, click on the entry in the list to select it and view the Discovery Ranges screen.

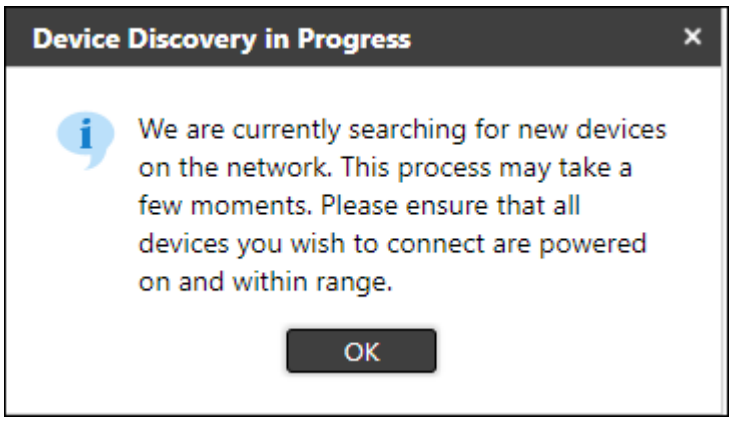
2. Click **Add** to enter a new range.



3. Select one **Range type**, and then enter the Host name (if necessary), and the From and To IP Address range or a single IP Address based on your range selection.
4. Click **Save**.
5. To perform discovery immediately, click **Discover Now**. Otherwise, proceed to set a discovery time of day below.

   An information message will appear to indicate that the search has begun. Click

OK to clear the message.



Important: If more than one On-Premise DMS has the same discovery range, both will report the same devices.

Important: If a Ricoh device installed with DM Agent is discovered by the DMS, it will not monitor this device.

Polling & Discovery Settings

Polling intervals for the DMS are configured under **Device Configuration** → **Polling**.

1. Locate the Device Monitoring Service section.
2. Set the **Check Interval** in hours. The minimum value for the Check Interval is 1 hour, which means the service will perform polling every hour.
3. Set the **Discovery Time of Day** to discover devices. At this time each day, the DMS will run to discover devices within the set discovery range.
4. Click **Save**.

Note: For Brother MPS devices, only the following properties are obtained from polling: Display Name, Model Name, Vendor Name, Serial Number, MAC Address, Device Address, IP Address, Status Poll Time, Supply Poll Time, Other Poll Time, Counter Poll Time, Last Communication Time, Device Type, System Version.

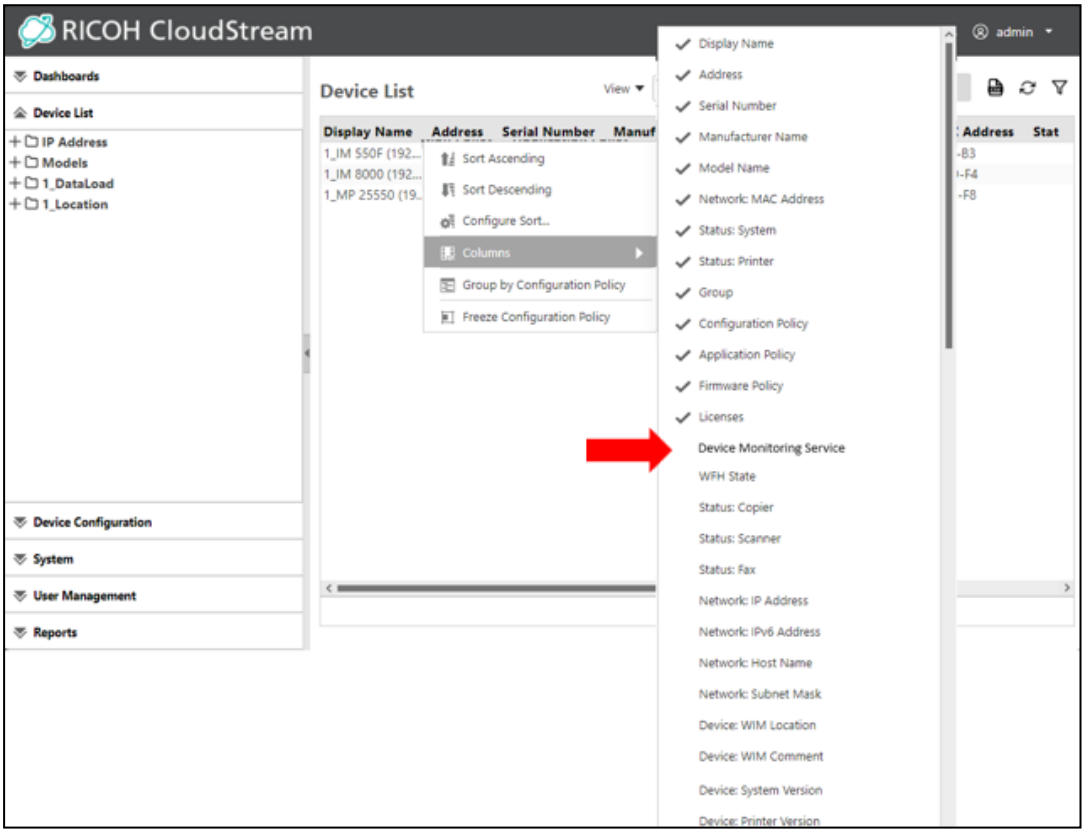
For Brother MPS devices, the following counters are obtained: Total, Copy Black, Copy Color Full (*), Printer Black, Printer Color Full (*), Printer Color Twin (*), Scanner Send Mono, Fax Black, Duplex, Total Mono, Total Color (*)

* These counters always show "0" (zero) for Monochrome devices.

Identify Device Monitoring Discovered Devices in the Device List

To view devices monitored by the DMS, you can add a column to the device list.

1. Go to **Device List**.
2. Right click on the table header to view the sub menu.
3. Select Columns and then select Device Monitoring to check the new column.



4. Click away from the menu to close it.
5. You may need to scroll right to view the Device Monitoring Service column. For devices added by a DMS, this column will show the Friendly name of the DMS that was created when it was installed on the On-premise server.

> **Note:** For any devices added by a DM Agent or WfH client, this column will be empty.

Delete Devices

To delete a monitored device, select the device and click Delete. Note that if Device Discovery is performed again (as described above in Device Discovery Range on page 303) and this device is within the discovery range, the device will appear in the Device List again.

Configure SQL Server Configuration Manager

1. Start SQL Server Configuration Manager.
2. From the navigation tree, select SQL Server Configuration Manager (Local)] → [SQL Server Network Configuration] → [Protocols for SQLEXPRESS].
3. Double-click [TCP/IP] in the list on the right side of the window.
4. Configure the following settings on the [TCP/IP Properties] window:
    - **[Protocol] tab:** Under [General], set [Enabled] to [Yes].
    - **[IP Addresses] tab:** Under [IPALL], specify a port number for [TCP Port]. Use the port number specified here when installing CloudStream. You cannot enter 0 for a port number. To configure each IP address separately, under [IPAll], leave [TCP Port] blank, and then specify a port number for each IP address.
5. Click [OK] to save the settings.
6. From the navigation tree, select [SQL Server Services].
7. Right-click [SQL Server (Instance Name)] in the list on the right side of the window, and select [Restart] from the menu that appears.

User Management

The User Management lists all users registered to the system and stores their data, such as user groups, departments, PINs, and cards.

Important: User Management and user registration is available only if you have a RICOH CloudStream Print&Scan license.

The following topics are helpful in managing the user information.

Register Users on page 311. Instructions on how to register users for User Management.
View User Groups on page 309. Displays information about users' groups.
View All Users Departments on page 310. Displays information about users' departments.
Register Cards on page 324 Instructions on how to register access card with User Management.
Configure User PIN on page 321. Instructions to enable User PIN and email options when PIN is updated.
Edit User Properties on page 317. The topic describes the steps to generate a PIN and assign cards to the user.

Depending on how the embedded client is configured, users can login to MFP using three methods. To know how embedded clients are configured, refer to Configure Print&Scan Embedded Client on page 222.

- **Card login**. This method allows users to login to the MFP using their registered card. To register a card, please go to Register Cards on page 324.
- **User Name and Password login**. Users can login using their user name and password.
- **PIN login**. Users can input their designated PIN to login. Configure the PIN settings in Configure User PIN on page 321.

View User Groups

Registering users to RICOH CloudStream Device Management (DM) will also display their group information in the User Management. The user's groups are retrieved from the external authentication provider, and you cannot edit them in CloudStream DM.

All Users Groups

Go to User Management, then click ***Group*** to view the list of groups that were retrieved from registered users.

The Groups table has the following columns.

Column Header	Description
Group Name	The name of the group or the group's object ID.
Authentication Profile	The authentication profile that was used to register the user. Click the link to view the profile in the Authentication Profiles screen.
Updated By	The value is M-Auth because the groups are internally retrieved by M-Auth after the user registration.
Update Date	The date and time that the group was updated.

Click the group to see the ***Group Details***. You can add a description and view the list of users that belong to the selected group.

User Properties - Groups

When you open user properties, you can find the user group node which displays the groups to which the user is assigned.

1. Open ***User Management.***
2. Click ***Users.***
3. Select the user from the list.
4. In the ***User Properties,*** expand the ***Groups*** node.

All groups that the user belongs to are displayed.

View All Users Departments

Registering users to CloudStream DM will also display their department information in the User Management. The user's departments are retrieved from the external authentication provider, and you cannot edit them in CloudStream DM.

All Users Departments

Go to User Management, then click ***Department*** to view the list of departments that were retrieved from registered users.

The Department table has the following columns.

Column Header	Description
Department Name	The name of the department.
Authentication Profile	The authentication profile that was used to register the user. Click the link to view the profile in the Authentication Profiles screen.
Updated By	The value is M-Auth because the departments are internally retrieved M-Auth after the user registration.
Update Date	The date and time that the department was updated.

Register Users

End users must register themselves to RICOH CloudStream Device Management (DM) so they can use the Ricoh MFP and perform secure printing and scanning. User Management and user registration is available only if you have a RICOH CloudStream Print&Scan license.

There are two types of users who can register for the CloudStream DM application.

- ***LDAP Users*** - See LDAP User Registration on page 311
- ***OpenID Connect (OIDC) Users*** - See OpenID Connect (OIDC) User Registration on page 312

Note: External LDAP or OIDC administrators who login to CloudStream DM portal (not the User Registration page) will not be registered as users in the User Management.

If you plan to register external administrators as users in the User Management, please have them register their own accounts by following instructions below.

LDAP User Registration

Order	Instructions
1	***Install Auth Agent service on your server.*** This step is necessary, so your On-Premise or cloud LDAPS configuration works with CloudStream DM. Please see Auth Agent Installation on page 155 for instructions.
2	***Create an LDAP authentication profile.*** For instructions, please go to LDAP Authentication Profile on page 151.
3	***Add Ricoh devices to CloudStream DM.*** Refer to Add Devices to CloudStream DM on page 27 for instructions.
4	***Configure the embedded client.*** For instructions, refer to Configure Print&Scan Embedded Client on page 222.
5	***Install the RICOH CloudStream Print&Scan Embedded app on the devices.*** For more details, follow the instructions in Install Print&Scan Embedded App on page 281.

Order	Instructions
6	***Register LDAP users.*** LDAP users must login to the MFP to register their accounts with CloudStream DM User Management. For more details, follow the instructions in Register an LDAP User on page 315.

OpenID Connect (OIDC) User Registration

Order	Instructions
1	***Set up the Email Server Settings.*** An email message containing the OTP will be sent to the OIDC user. You must have a working Email Server so users can receive their OTP. The OTP is required to register an OIDC user's access card. If the email server setting is not yet configured, please see the instructions in Email Server Settings on page 133.
2	***Create an OIDC authentication profile.*** For instructions, please go to OpenID Connect Authentication Profile on page 164.
3	***Add Ricoh devices to CloudStream DM.*** Refer to Add Devices to CloudStream DM on page 27 for instructions.
4	***Configure the embedded client.*** For instructions refer to Configure Print&Scan Embedded Client on page 222.
5	***Install the RICOH CloudStream Print&Scan Embedded app on the devices.*** For more details, follow the instructions in Install Print&Scan Embedded App on page 281.
6	***Register OIDC users.*** OIDC users must login to the User Registration page and have their external OIDC provider authenticate them. Successful authentication registers the user to the CloudStream DM User Management. Please refer to Register an OIDC User on page 313 for instructions.

Note: After successful registration, an OIDC user will receive a One-Time Password (OTP) sent to their email. When logging into Ricoh Devices, they must use the OTP as their password to login and register an access card.

Register an OIDC User

Register your OpenID Connect (OIDC) account with RICOH CloudStream Device Management (DM) so you can use your account to login to CloudStream-enabled Ricoh MFPs, where you can release print jobs securely and perform secure scanning.

To register an OIDC account, follow the steps below.

1. Open a browser and go to the CloudStream DM user registration page.

   The user registration page has the same domain as the CloudStream DM portal.

   If you have the portal's URL, copy the domain and append `/registration.html` at the end.

   Typically, the URL will look like this: `https://CompanyName.region.cloudstream.ricoh.com/registration.html`

   Contact your administrator if you still need the URL.
2. In the login screen, click **[Login to OIDC].**
3. Click the dropdown menu and select the OIDC provider where you would like to be authenticated.
4. Click **[Login].**
5. You will be redirected to the OIDC external provider for authentication. Please login to authenticate.

   If the authentication fails, please contact your IT administrator or the external authentication provider for support.

   If you are using Entra ID as your authentication provider and you encounter a redirect URI problem, refer to OpenID Connect Authentication Profile on page 164 for information to setup the correct URI.
6. You will return to the User Registration page and will see a success message saying:

   "Your OIDC login is successful. Please check your email and retrieve the One-Time Password (OTP). Note: Use this OTP together with your username to register an access card".

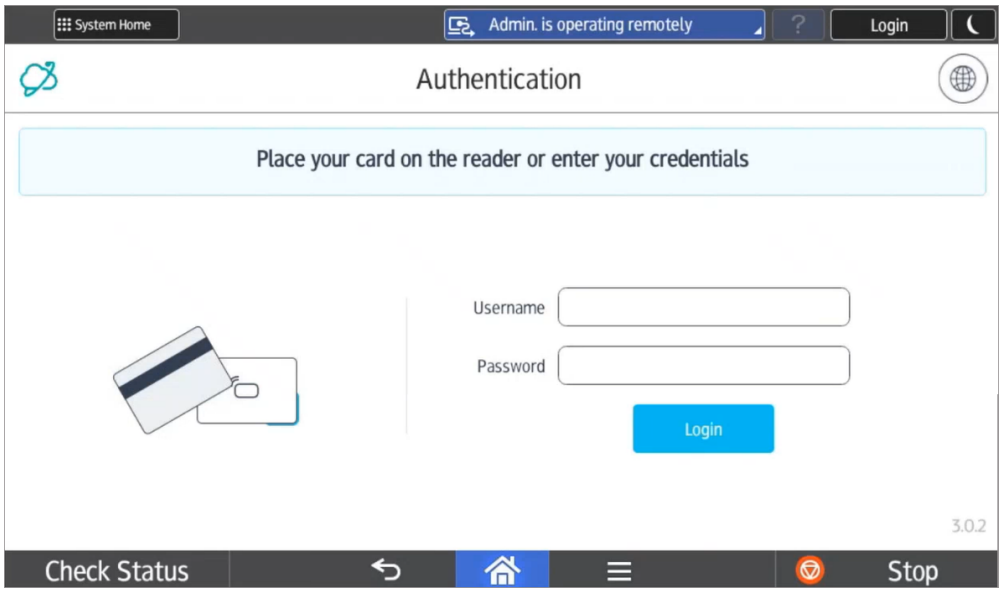
At the same time, the One-Time Password (OTP) is generated and sent to your email.

Note: No OTP will be generated if the registration fails.

7. After you register your OIDC account with CloudStream DM, login to the MFP using your OIDC account.

   a. Go to a Ricoh device with RICOH CloudStream Print&Scan embedded installed.

      A device with Print&Scan embedded will display a screen similar to the image below.



Important: The display in the login screen depends on how the embedded client is configured. To allow OIDC login, the embedded client must have *Username + Password Login or card login* as the login type. For more details, please refer to Configure Print&Scan Embedded Client on page 222.

   b. Enter your OIDC username, including the domain name. For example, myaccount@oidcdomain.com

   c. Enter the OTP sent your email and then click the **[Login]** button.

A successful login will display the RICOH CloudStream Print&Scan ***My quick actions*** screen.

Register your access cards so you can login by tapping your card to the MFP's card reader. To know more about card registration, refer to Register a Card in MFP on page 325.

Alternatively, the CloudStream DM administrator can generate a user PIN that you can use to login to the MFP. Note that the card login or the PIN login must be enabled in the embedded client configuration.

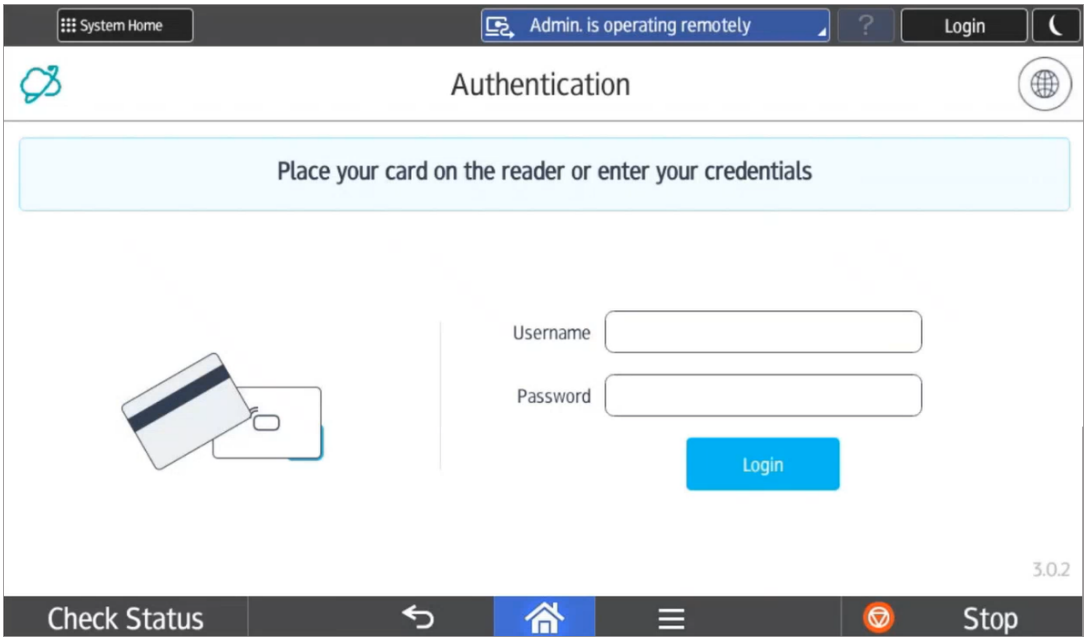
Register an LDAP User

Important: LDAP users can only register their accounts to an MFP with RICOH CloudStream Print&Scan embedded installed.

Register to RICOH CloudStream Device Management (DM) by logging to the MFP using your LDAP account. Below are the steps to register your LDAP account to CloudStream DM.

1. Go to a Ricoh device with RICOH CloudStream Print&Scan embedded installed.

   A device with Print&Scan embedded will display a screen similar to the image below.



Important: The display in the login screen depends on how the embedded client is configured. To allow LDAP login, the embedded client must have *Username and Password Login* as the login type. For more details, please refer to Configure Print&Scan Embedded Client on page 222.

2. Enter your LDAP username including the domain name. For example, myaccount@ldapdomain.com
3. Enter your password and tap the **[Login]** button.

Successful login will register your account to CloudStream DM. The MFP will also display the RICOH CloudStream Print&Scan ***My quick actions*** screen.

When your LDAP account is registered to CloudStream DM, you can start registering your access cards so you can login by tapping your card into the MFP's card reader. Alternatively, the CloudStream DM administrator can generate a user PIN that you can use to login to the MFP. Note that the card login or the PIN login must be enabled in the embedded client configuration.

To know more about card registration, refer to Register a Card in MFP on page 325.

Edit User Properties

All users registered to RICOH CloudStream Device Management (DM) are displayed in the Users List. Go to the ***User Management*** section and click ***Users*** to see the list.

You can find the following information in the list.

Column Header	Description
User Name	The user name that was used to register for CloudStream DM.
Authentication Profile	The Authentication Profile used during user registration. **Note:** Clicking this column will display the Authentication Profile screen.
Display Name	The name of the users. This information is retrieved from the authentication provider.
Email	The email address of the user.
Update By	Initially, the user is registered by a CloudStream service. When an administrator changes the user's PIN, card assignment, or deletes and restores the user account, Update By Column will change to the login administrator's user name.
Update Date	The date and time the update has been made.
User Home Folder	Displays the user's home folder.
Department Name	Displays the department the user belongs to.
User Language	Displays the language set for the user.

Note: User Home Folder, Department Name, and User Language are initially not displayed in the columns. To display these columns, please right-click on the column header and select ***Columns***, from there, click the columns you want to see in the table.

This topic covers the following:

Change User PIN on page 318.
Assign a Card on page 318.
Delete a User on page 319.

Change User PIN

1. Login as an administrator.
2. Go to ***User Management*** section.
3. Click ***Users.***
4. Select a user you want to edit.
5. In the ***User Properties***, click ***Change User PIN.***
6. A dialog showing the user's new PIN is displayed, please make sure to copy the user's PIN before closing the dialog because once you close it, the user's PIN cannot be viewed again.

   Alternatively, you can set up an automatic email option, so the users will receive an email containing their new PIN whenever their PIN changes, to do this please go to Configure User PIN on page 321.
7. Click **[OK].**

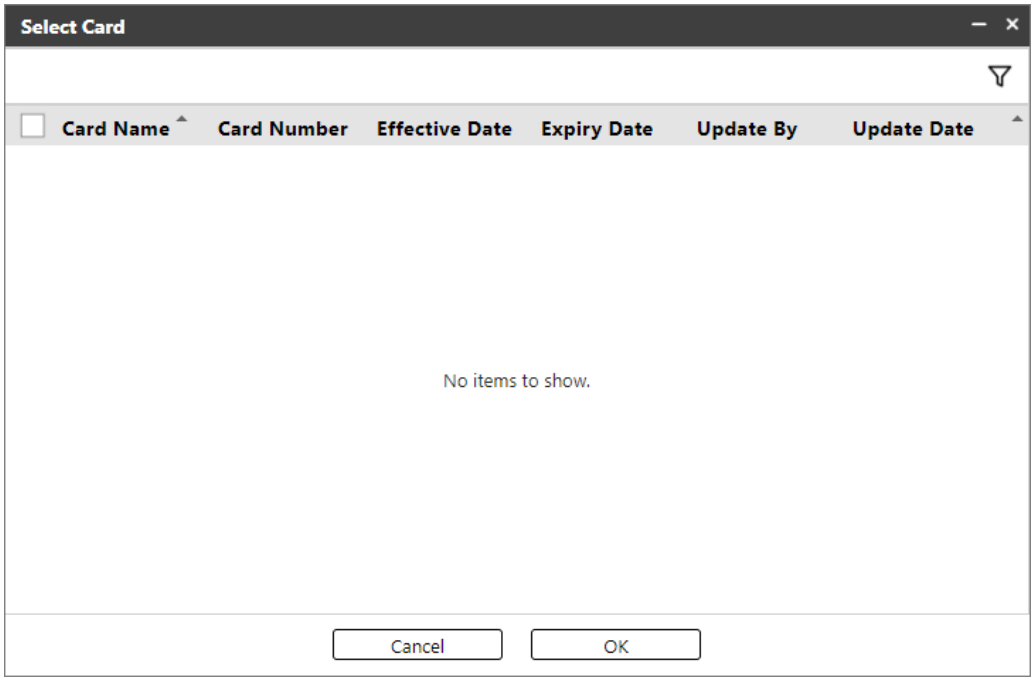
The user's PIN has been generated and the user can start logging in to MFP using a PIN.

Note: The generated PIN is unique for each user, and it is displayed as masked in the ***User PIN*** field.

Assign a Card

1. Login as an administrator.
2. Go to ***User Management*** section.
3. Click ***Users.***
4. Select a user you want to edit.
5. In the ***User Properties***, expand ***Cards.***

   Note: When users register their card from the MFP, the card's information will be added in the user's card list.
6. Click **[Add].** A dialog will display, showing all the registered cards. If you still need to register the cards, register them in Register Cards on page 324.



Item	Description
Card Name	The name of the card.
Card Number	Displays the Card Number.
Effective Date	Displays the start date to use the card.
Expiry Date	Displays the date the card becomes unusable.
Update By	The administrator who updated the card's information.
Update Date	The date and time the administrator updated the card's information.

7. Check a card or multiple cards that you want to assign to the user. You can also select all cards by clicking the checkbox on the column header.
8. After selecting a card(s), click **[OK].**

The cards you selected for the user are displayed in the list and they can use their card to login to Ricoh MFP.

Delete a User

Important: You can only delete accounts that are not associated with a card.

The User screen indicates users that have previously logged into CloudStream. If you prefer to Delete user accounts, you can select one or more accounts, and then click [Delete] to remove the accounts.

If the user is associated with a card, a warning message indicates that the user cannot be deleted. You must un-assign the card from the user account before you can proceed.

A confirmation message will prompt you to confirm the deletion. The users are not fully deleted until purged, but they are hidden from Groups/Departments screens.

Purge or Restore Users

To view a list of all previously Deleted users, click [View Deleted]. From this screen, you can select one or more users and either [Restore] the accounts, or [Purge] them entirely from CloudStream. A confirmation pop-up requires you to confirm that you want to proceed.

If a user has not been purged, you can click [Restore] to re-enable their access.

If you proceed to purge, the user name will continue to appear in CloudStream with two exceptions:

- Generated reports that include configurable fields such as User ID and User Name will display these fields as Unknown.
- The Print Job Activity dashboard will list "Unknown" instead of the User Name.

Purged users cannot login to CloudStream. However, note that if the user account still exists in LDAP or Entra ID, the user can login again to be added as a new user.

Configure User PIN

Note: Only admins assigned the User Admin role can make changes to PIN Settings; otherwise, an "Access Denied" message appears when trying to save User PIN Settings. Refer to Administrator Accounts on page 190 for details.

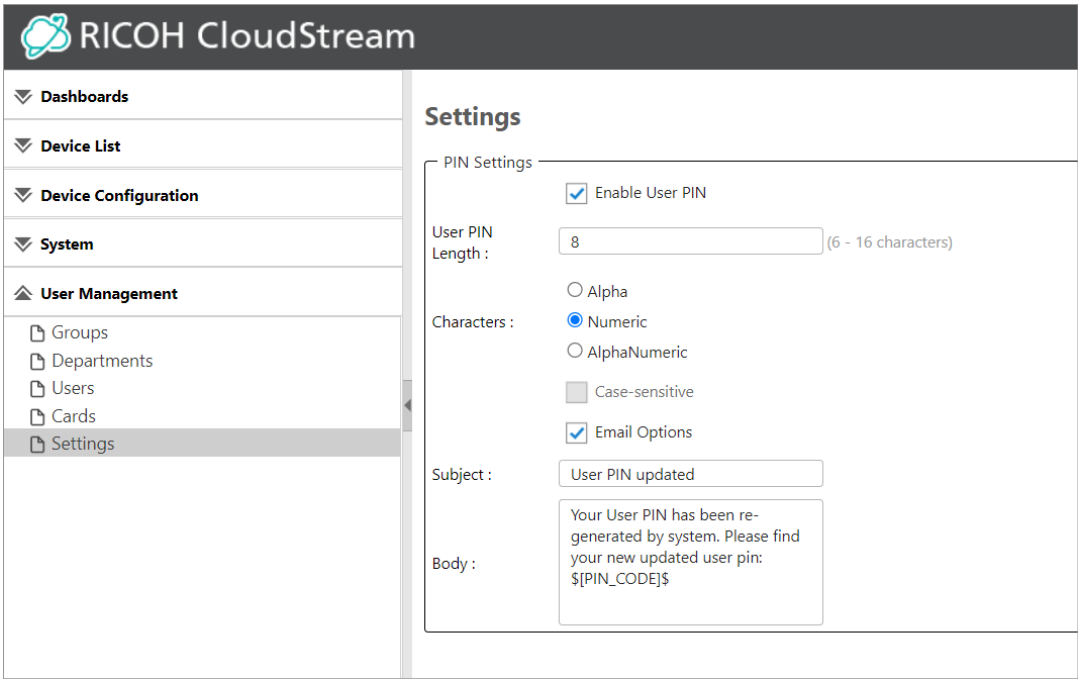
The User PIN Settings configure how the PINs are generated and set up the email options. Access this feature in ***User Management***, then click ***Settings***.

The following are important notes you need to know before you set the User PIN Settings.

- If the 'Enable User PIN' is unchecked, users cannot login to the MFP using a PIN.
- If users were already registered before the User PIN setting is enabled, a PIN is automatically generated for each user.
- Similarly, for new users, a PIN is automatically assigned to them.
- It is recommended that you enable the Email Options so the system will email the users their assigned PIN.
- If you decide to disable the User PIN Settings after PINs are assigned to users, the **[Change User PIN]** button in User Properties will be disabled. However, their PIN is still saved in the system, so when you enable the User PIN Settings again, existing users can still use their old PIN.

Enable the PIN and configure the required settings.

1. Login as an administrator with User Admin privileges.
2. Go to ***User Management*** section.
3. Click ***Settings.*** You will see a similar screen below.



4. Check ***Enable User PIN.*** Enabling this item will also enable the required fields under it.
5. Specify the ***User PIN length.*** This is a required field. Please input a number between 6 to 16 inclusive.
6. Select the type of characters generated for the PIN.
   - **Alpha** - Only alphabet characters are generated.
   - **Numeric** - Only numeric characters are generated.
   - **Alphanumeric** - Both alphabet and numbers comprise the generated PIN.
7. (Optional) Check if you want to allow the PIN to be ***Case-sensitive***.

   If checked, the user PIN is sensitive to capitalization of letters. Users must input the PIN with the same capitalization. This option is only available if the chosen pattern is alpha or alphanumeric.
8. (Optional) Check ***Email Options***. The ***Subject*** and ***Body*** fields will be required when this option is checked.

   Enabling the email option will send the generated PIN to the user's email address. If this option is not enabled, please copy the generated PIN and share it with the user.

   Note: Email Server Setting must be configured for this option to work. Please see Email Server Settings on page 133 for configuration instructions.
9. (Required when Email Option is enabled) Enter email subject.

When ***Email Options*** is enabled, the **Subject** is populated with the following text:

"User PIN updated"

10. (Required when Email Option is enabled) Enter the Body of the email.

    When ***Email Options*** is enabled, the **Body** is populated with the following text:

    "Your User Pin has been re-generated by system please find your new updated user pin: $[PIN_CODE]$"

    > **Note:** The email body must contain the user PIN variable: $[PIN_CODE]$. If not, the user PIN will be appended at the end of the body.

11. Click **[Save].**

> **Note:** If the ***Email Option*** is enabled and you decide to disable it, the value in the ***Subject*** and ***Body*** will be removed. If you enable the ***Email Option*** again, the ***Subject*** and ***Body*** will be populated with their default values.

To change a specific user PIN , go to the User Properties and click the **[Change User PIN]** button. For more details, refer to Edit User Properties on page 317.

Register Cards

One of the methods to login to CloudStream-enabled devices is using an access card. Users can tap their cards to the card reader attached to the device.

To use the cards, you must register them. There are three ways to register a card.

Register a Card in User Management on page 324. Register the card in CloudStream DM's User Management screen, then assign it to the user.
Import User Cards on page 327. This allows you to import a CSV file containing the card information and assigned users. After importing, the registered users can use their card to login to the MFP. If you want to export cards, please refer to Export User Cards on page 330.
Register a Card in MFP on page 325. Allow registered users to register their own card via Card Registration on the Ricoh MFP.

Go to ***User Management*** and expand ***Cards*** to see the following information.

Column Header	Description
Card Name	The name of the card.
Card Number	Displays the Card Number.
Enabled	Displays if the card is enabled or not. Disabled cards cannot be used.
Effective Date	Displays the start date to use the card.
Expiry Date	Displays the date the card becomes unusable.
Update By	The administrator who updated the card's information.
Update Date	The date and time the administrator updated the card's information.

The card is not usable before the ***Effective Date*** and after the ***Expiry Date***.

Register a Card in User Management

Note: You can add a card to the *Cards* list even though the user of the card is not yet registered. You can register the card now, then assign it to the intended user later. For more information go to ***Assign a Card*** topic in Edit User Properties on page 317.

1. Login as an administrator.
2. Go to ***User Management*** then click ***Cards.***
3. Click **[Add].** You will see a similar screen below.
4. Enter the ***Card Number.***

5. Enter the name of the Card.
6. (Optional) Select a user to whom the card will be assigned to. If the user is not yet registered, you can leave this field empty. You can assign the card to the user later.

   You can also select a user name from this list, and then click **Remove User** to delete a user from this card.
7. Check **Enabled** if you want users to use the card, otherwise uncheck it.
8. Select the card's validity.
   - **Indefinite Period** - If selected, the card will have no definite time to use, making the card usable without expiration.
   - **Duration** - If selected, the card can be used within the specified Effective Date and Expiry Date. If the card is expired, you can extend the expiry date by editing the card properties.

     The following are displayed when ***Duration*** is selected.
     - Effective Date - Select the start date to use the card. The card is not usable before the effective date.
     - Expiry Date - Select the date the card becomes unusable.

     Click the calendar icon to select a date from a calendar.
9. Click **[Save].**

Note: CloudStream DM does not store the card information from the user's authentication provider. However, you can allow users to add their cards by themselves. Please see Register a Card in MFP on page 325.

Register a Card in MFP

If your account is registered in CloudStream DM, you can register your access cards so you can just tap your card to the MFP's card reader to authenticate.

Prerequisites

Before you can register your card, please make sure that device displays the card icon indicating that it allows card login.

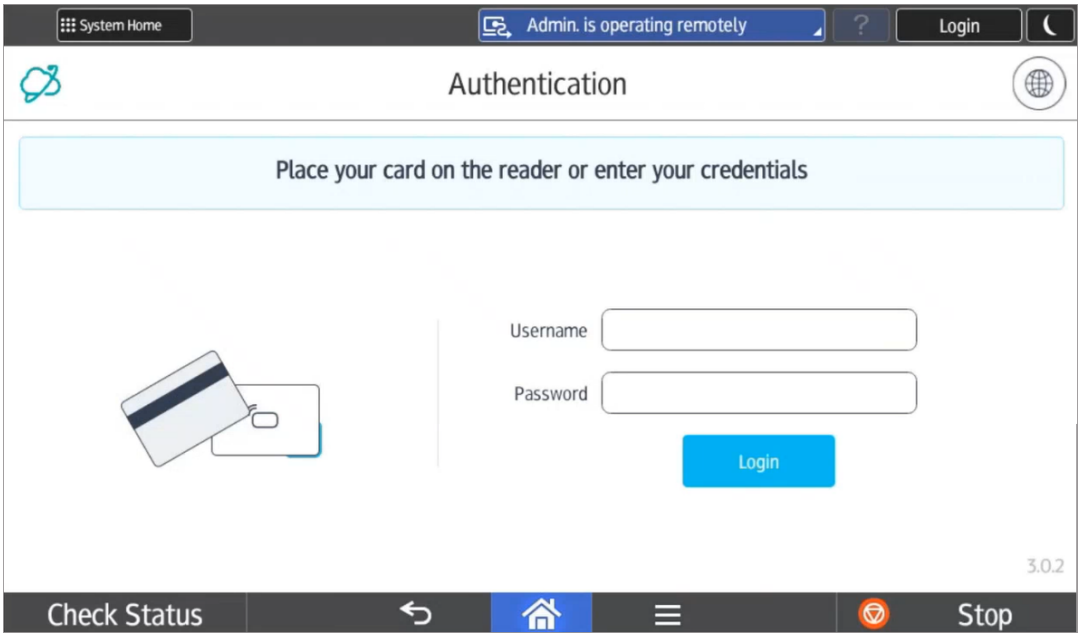
Important: The display in the login screen depends on how the embedded client is configured. To allow card login, the embedded client must have *Card Swipe Login* as the login type. For more details, please refer to Configure Print&Scan Embedded Client on page 222.

Prerequisites
The MFP has a configured and attached card reader. A card reader is where your tap your card so you can authenticate and login to the MFP.
The MFP has RICOH CloudStream Print&Scan embedded installed. To install the required embedded, refer to Install Print&Scan Embedded App on page 281.

1. Go to a Ricoh device with RICOH CloudStream Print&Scan embedded installed.

   Note: Card registration happens in the login screen. You must log out from the MFP if you plan to register a card.

   A device with Print&Scan embedded will display a screen similar to the image below.

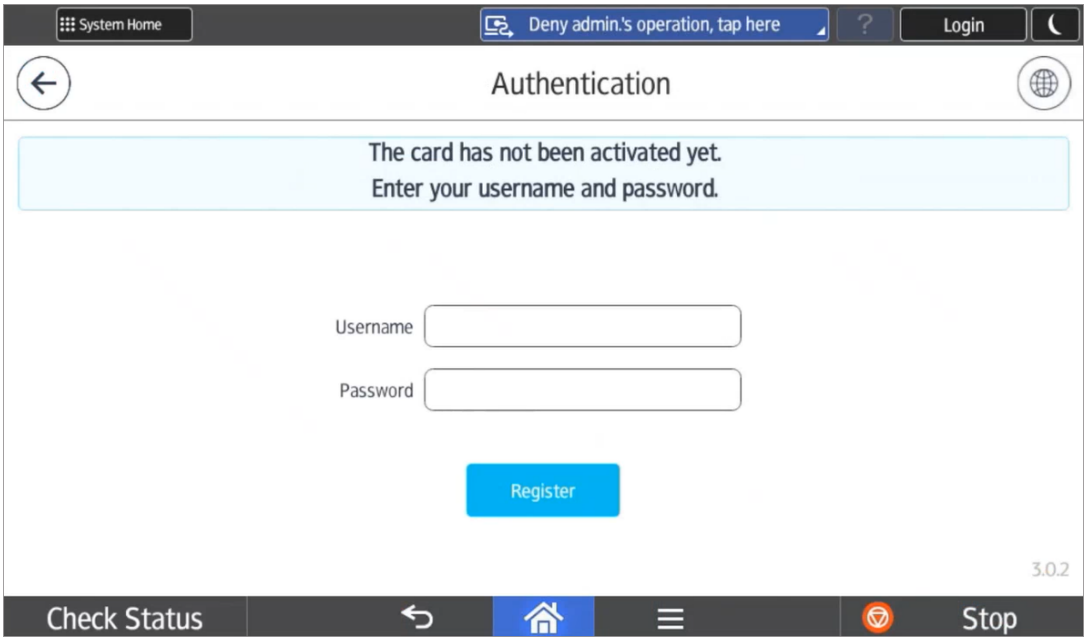


2. Tap your card to the card reader.

   If the card went through without asking for credentials, this means that the card is already registered to the CloudStream DM.

   If the card is not recognized by CloudStream DM, you will be asked to register it under your account.

   "The card has not been activated yet. Enter your username and password."



3. Enter your username including the domain name. For example, myaccount@oidcdomain.com.
4. Enter your password or OTP.
    - If your account is an OIDC, you must use the OTP sent to you as password. To generate the OTP, refer to Register an OIDC User on page 313 for instructions. Note that, by following the steps, you are not re-registering your account, you are simply generating an OTP.
    - If your account is an LDAP, enter your LDAP password.
5. Tap **[Register].**

You can register as many access cards to your account by repeating the same steps.

To remove a card from your account, you must contact your Administrator and request them to remove the card from your account.

Import User Cards

This feature allows you to import a CSV file containing card information.

Note: If you want to export cards, please refer to Export User Cards on page 330.

To import cards, please follow the steps below:

1. Login as an administrator.
2. Go to ***User Management*** then click ***Cards.***

3. Click **[Import].** A pop-up window will appear.
4. Click **[Choose File]** and select CSV file with the following format.

   Line 1: "card_name","card_number,"user_name","card_enabledflag","card_effectivedate","card_expirydate","update_username","update_timestamp"

   Line 2: <the card details following the format in Line 1>

   An example is shown below:

"card_name","card_number,"user_name","card_enabledflag","card_effectivedate","card_expirydate","update_username","update_timestamp"
"company card-1","123456789","userA","true","2024-10-20 09:00:00", "2025-10-19 08:00:00","localadminuser","2024-07-01 09:00:00"
"company card-2","223456789","userB","true","", "","localadminuser","2024-07-01 09:00:00"
"company card-3","233456789","","false","", "","localadminuser","2024-07-01 09:00:00"

   Where:

Column Header	Description
card_name	The name of the card. This item is required and should be unique.
card_number	The card number. This item is required and should be unique.
user_name	The assigned username of the card. If you plan to assign the card after you imported the CSV, leave this part empty "". See line 4 in the example above. In this case, the import process will flag the missing username as an error, and you will have an opportunity to select the username from a drop-down list.
card_ enabledflag	Identifies if the card is active or not. • Set "true", if you want the card to be usable. • Set "false", if want to disable the card's usage. This item is required.
card_ effectivedate	The start date to use the card. The date should be in this format: yyyy-mm-dd hh:mm:ss

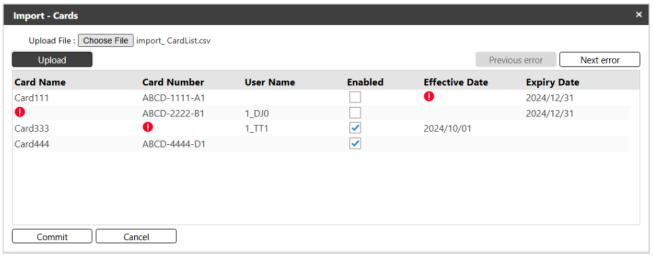
Column Header	Description
	where hh is in 24-hour format. If the card's validity is an indefinite period, leave this part empty "". Indefinite period means the card will not expire. See line 3 and 4 in the example above.
card_ expirydate	The date the card becomes unusable. The date should be in this format: yyyy-mm-dd hh:mm:ss where hh is in 24-hour format. If the card's validity is an indefinite period, leave this part empty "". Indefinite period means the card will not expire. See line 3 and 4 in the example above.
update_ username	The administrator's username who updated the card's information. This item is required.
update_ timestamp	The date and time the administrator updated the card's information. This item is required.

5. Click **[Upload]**.

   The information is read from the csv file and details are validated.

   Note: If you upload an empty CSV file that does not include the correct columns, an error message is displayed.

   Any rows with missing or invalid data are listed in the screen for correction. Specific information that is missing is indicated by a red exclamation mark in the column. Card name and card number must not be empty. If details are missing from these columns, you can correct the information. To select a missing user name, click directly in the field and select the user from the list.



6. Click **[Commit]**to proceed.

> **Note:** If you commit a mix of valid and invalid rows, the valid rows will be imported and removed from the screen and invalid rows will remain for additional correction.

The import will start immediately. If all cards are valid, you will see a message stating "All valid items have been successfully imported" and all imported cards will be displayed.

Troubleshooting Tips

- If the card number already existed in the list, the card's information will be updated.
- If the user name that you have provided in the CSV file is not found in the user management, an exclamation mark appears in the user name field to indicate that the user information is not valid. Click on the user name field to select from a list of valid user names.
- The date fields are not required. Date cells will show a blank when missing in the import file or an exclamation when is included in the import file, but it is in an invalid format. Valid formats are:
  - Date - yyyy-MM-dd – Example: 2024-12-31
  - Date & Time - yyyy-MM-dd hh:mm:ss – Example: 2024-12-31 12:00:00

Export User Cards

Cards displayed in User Management can be exported to a CSV file by clicking the **[Export]** button.

Below is the information you can find when you export the user cards into a CSV file.

- Line 1: "card_name","card_number,"user_name","card_enabledflag","card_effectivedate","card_expirydate","update_username","update_timestamp"
- Line 2: <the card details following the format in Line 1>
- Line N: <the card details following the format in Line 1>

An example is shown below:

```
"card_name","card_number,"user_name","card_enabledflag","card_effectivedate","card_expirydate","update_username","update_timestamp"

"company card-1","123456789","userA","true","2024-10-20 09:00:00", "2025-10-19 08:00:00","localadminuser","2024-07-01 09:00:00"

"company card-2","223456789","userB","true","", "","localadminuser","2024-07-01 09:00:00"
```

```
"company card-3","233456789","","false","", "","localadminuser","2024-07-01 09:00:00"
```

Where:

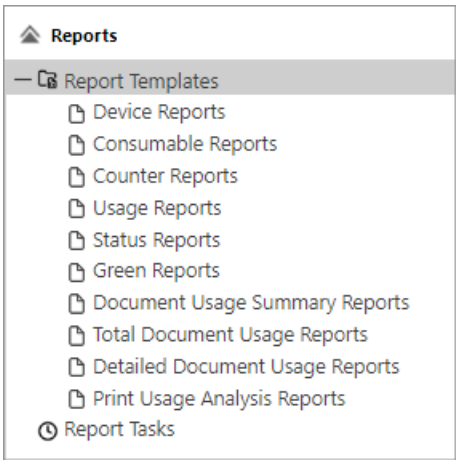
Column Header	Description
card_name	The name of the card.
card_number	The card number.
user_name	The assigned username of the card. If card do not have assigned username, then this part is empty "". See line 4 in the example above.
card_ enabledflag	Identifies if the card is active or not. • "true", if the card is usable. • "false", if the card is unusable or disabled.
card_ effectivedate	The start date to use the card. The date is in this format: yyyy-mm-dd hh:mm:ss where hh is in 24-hour format. If the card's validity is indefinite period, this part is empty "". Indefinite period means the card will not expire. See line 3 and 4 in the example above.
card_ expirydate	The date the card becomes unusable. The date is in this format: yyyy-mm-dd hh:mm:ss where hh is in 24-hour format. If the card's validity is indefinite period, this part is empty "". Indefinite period means the card will not expire. See line 3 and 4 in the example above.
update_ username	The administrator's username who updated the card's information.
update_ timestamp	The date and time the administrator updated the card's information.

If you are looking for steps to import cards, please see Import User Cards on page 327.

Reports

The ***Reports*** section allows you to generate a report using standard and custom templates.

You can also create a scheduled report that will generate and send a report to recipients based on the set schedule.



Reports Templates - Displays the list of report templates. Standard templates are displayed by default. You can create a customized template from a standard template.

Report Tasks - Displays all scheduled reports in a list. Scheduled reports are tasks that will send the generated report to the recipient based on the set interval. For example, a weekly device error report is generated and sent to the operations personnel email.

Here is a list of report types.

Device Reports on page 336.	Document Usage Summary Reports on page 344
Consumable Reports on page 337.	Document Usage Summary Reports on page 344 .
Counter Reports on page 340.	Total Document Usage Reports on page 346.
Usage Reports on page 340.	Detailed Document Usage Reports on page 347.
Status Reports on page 342.	Print Usage Analysis Reports on page 348.

You can accomplish the following tasks in the ***Report*** section.

Create Custom Report Template on page 362. Creates customized report template based on a standard template.
Run a Report Immediately on page 334. By clicking the run button, you can generate a report immediately. You can also download the generated report.
Run a Report on Schedule on page 350. A report is generated and sent to recipients based on the set schedule.

Manage Report Tasks on page 358. Manage all scheduled reports from this screen.

Run a Report Immediately

Reports are generated when a report template is executed via a schedule or running it immediately.

Run report immediately	Represented by icon  Use this to generate a report right away. The contents of the report will be based on the current data held for the selected parameters. Please see Run and Export a Report on page 334.
Run on schedule	Represented by icon  Use this to create a report task. With this feature, you can schedule a report to be generated and sent to recipients once or on a daily, weekly, or monthly basis. Please see Run a Report on Schedule on page 350.

Run and Export a Report

If you plan to generate a report immediately, the ***Run Immediately*** function generates a report and displays it on the screen. From there, you can save the report in CSV, PDF, or Excel file format.

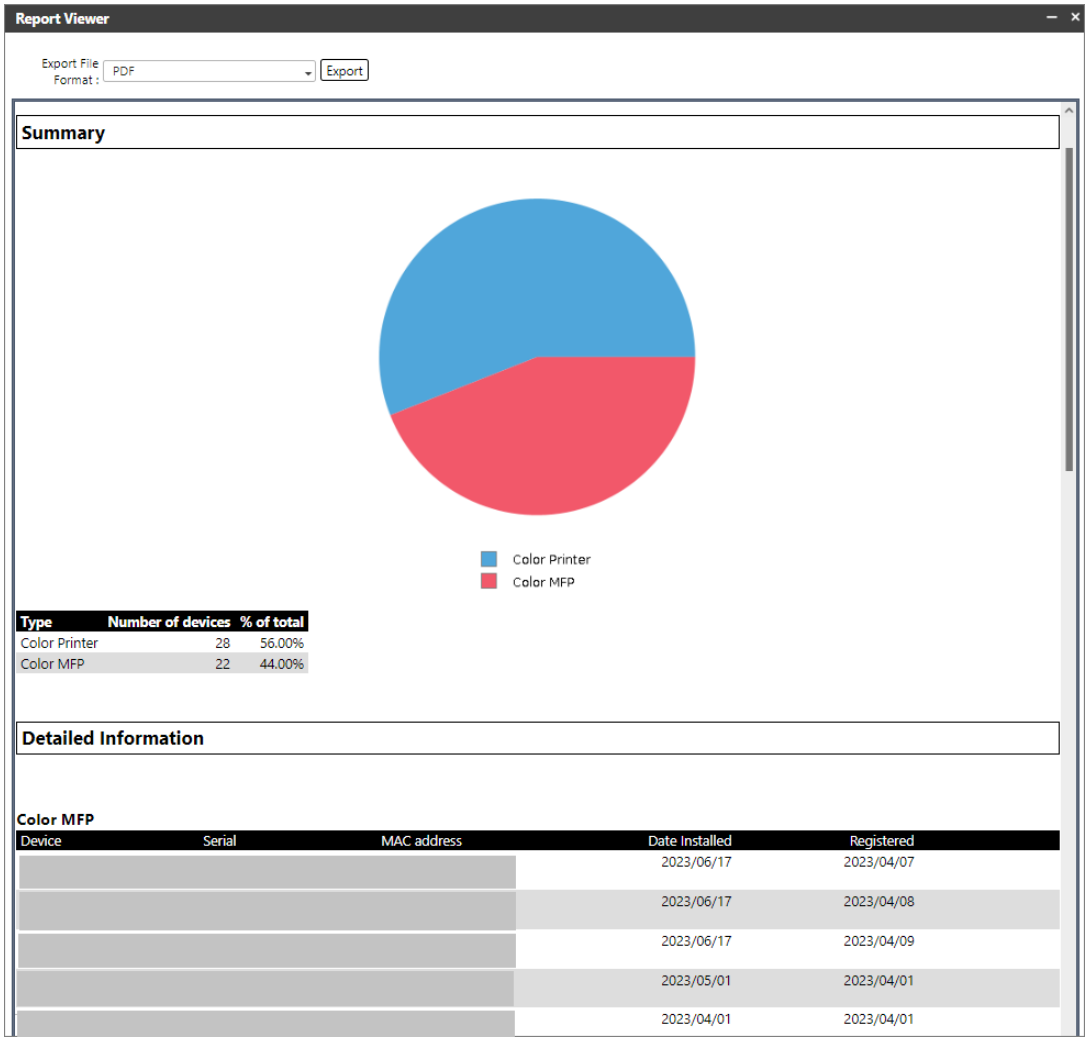
Note: Refer to Reports on page 332 for the list of reports you can generate immediately.

To generate a report immediately, follow the steps below.

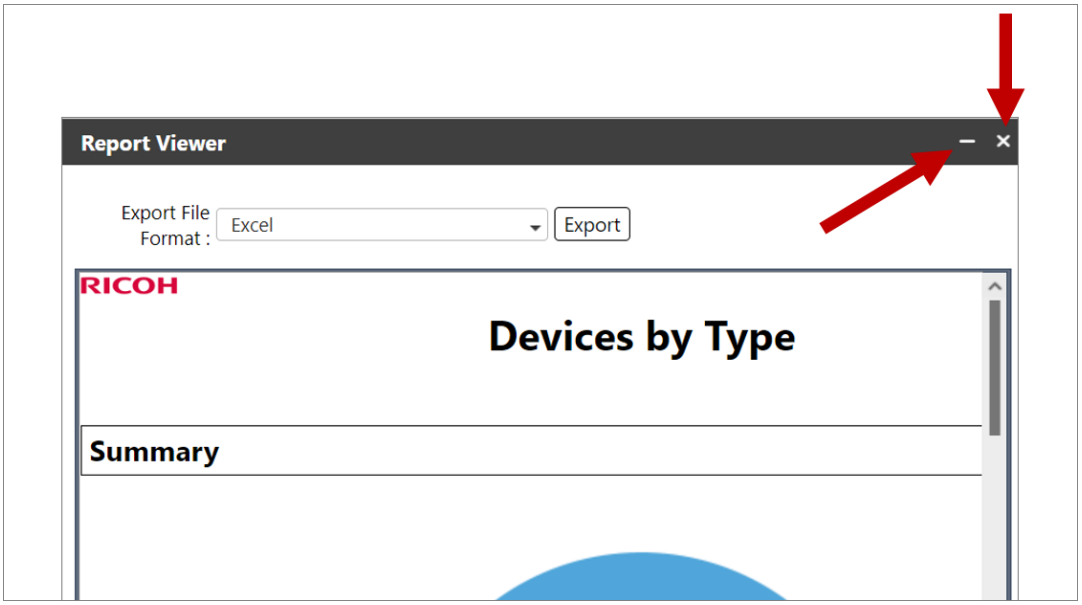
1. Login as an admin with reports privileges.
2. Go to the ***Reports*** section.
3. Expand ***Report Templates.***
4. Select a ***Report Category***. Report templates are categorized based on their purpose.
5. From the list of report templates, select the report template you want to generate a report with.
6. Click  [Run Immediately].

7. A dialog "Run now" is displayed. Specify the correct parameters of your report. Refer to ***Report Parameter*** in Parts of a Report Template on page 370 page for more details.
8. Click **[OK].**

   The report is generated and displayed on the screen similar to the sample image below.



9. In the top left area, you can find the setting ***Export File Format***. Select the file format. Available options are PDF, CSV, and Excel.
10. Click **[Export].**
11. Click **-** icon to minimize the report view or **x** icon to close the view.



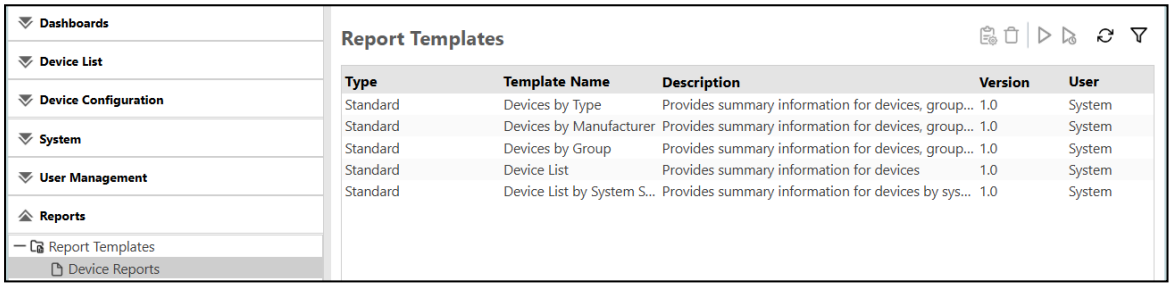
Device Reports

Use a report template in the ***Device Reports*** category to create a report of the device information for each category.

Device Report Templates	Description
Devices by Type	Use this report to view information such as device name and serial number by device type for devices being monitored. Devices are divided into groups: • Color MFP • Color Printer • Monochrome MFP • Monochrome Printer The ratio of device types is indicated in a graph, and the device types, number of devices, and ratio (%) are indicated in a table.
Devices by Manufacturer	Use this report to view summary information of devices being monitored that are totaled for each device manufacturer. This report indicates the ratio of manufacturers in a graph, and it indicates the manufacturers and number and ratio (%) of devices by manufacturer in a table.
Devices by Group	Use this report to view the summary information of devices being monitored that are totaled for each device group in the selected categories. The ratio of the number of used devices in a group is indicated in a graph, and the group names, number of devices, and ratio (%) are

Device Report Templates	Description
	indicated in a table.
Device List	Use this report to view basic information of devices being monitored.
Device List by System Status *	Use this report to view information for devices based on system status. This report can include a Print Status Detail column that is used by Brother manufactured devices.

Device Reports are displayed like the image below:



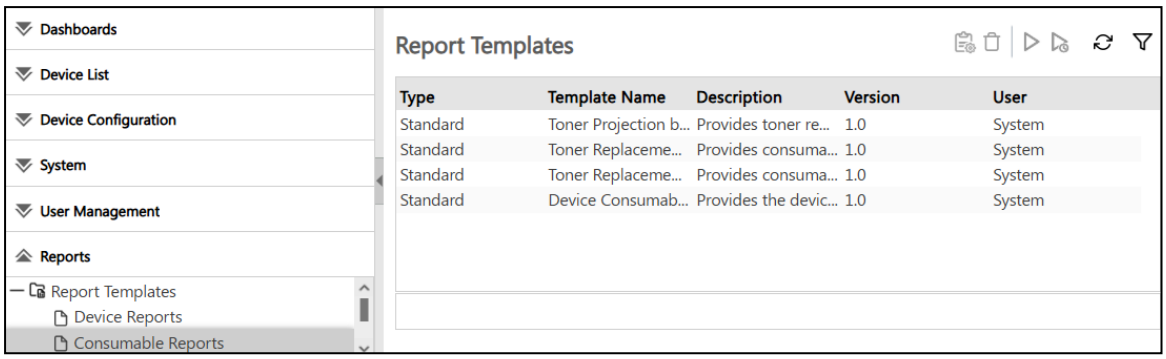
** The Device List by System Status report will be supported in a future release.*

Consumable Reports

Use a report template in the ***Consumable Reports*** category to create a report for when to replace toner for a device.

Consumable Report Templates	Description
Toner Projection by Device	Use this report to display the estimated toner replacement date for devices being monitored.
Toner Replacement by Device	Use this report to view the toner replacement date of devices being monitored for each device.
Toner Replacement by Date	Use this report to view the toner replacement date by month for devices being monitored.
Device Consumable Replace for Brother MPS	Use this report to view the device consumable details for Brother devices only.

Consumable Reports are displayed like the image below:

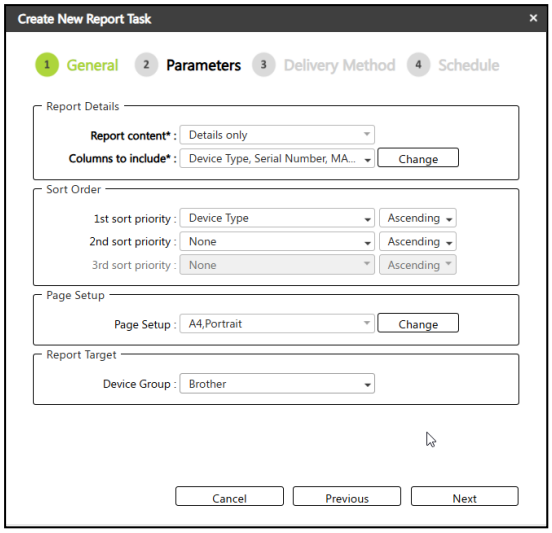


Device Consumables Replace for Brother MPS Report

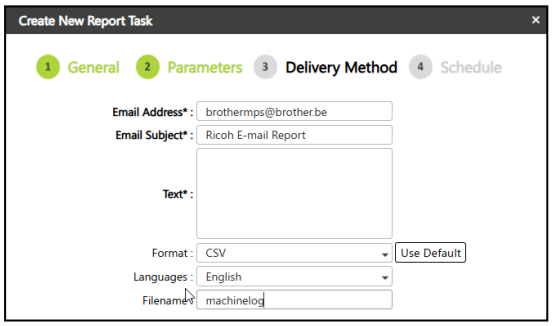
If you have integrated the Device Management Service to monitor Brother devices, you can generate a report that will specifically contain Brother-specific replace information.

Note: The report will contain the following columns: Device Type, Serial Number, MAC Address, Date*1, Total Page Count, Color Page Count, Monochrome Page Count, Black (BK) Toner/Ink Replace Count, Cyan (C) Toner/Ink Replace Count, Magenta (M) Toner/Ink Replace Count, Yellow (Y) Toner/Ink Replace Count, Drum Unit Replace Count, Drum Unit Black (BK) Replace Count, Drum Unit Cyan (C) Replace Count, Drum Unit Magenta (M) Replace Count, Drum Unit Yellow (Y) Replace Count, Waste Toner Box/Waste Tank Replace Count, and Belt Unit Replace Count.

1. Click **Reports** → **Report Templates** →**Consumable Reports**.
2. Select **Device Consumable Replace for Brother MPS** from the reports table.
3. From the toolbar, click **Run on Schedule**.
4. In the Create New Report Task screen, enter a **Task name**, and an optional description. Click Next to proceed.
5. In the **Parameters** screen, change the **Report Target** to a Device Group that **contains the Brother models**. Leave all other settings at their defaults. Click Next.

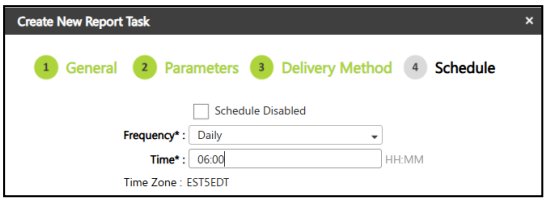


6. In the **Delivery Method** screen, enter the following information as shown below and then click Next to advance.



- **Email Address:** Confirm the email address with your local Brother Operation Company. The MPS email address will be based on the country where the contract has been created. For example, for a French contract, only the French inbox should be used.
- **Email Subject:** Type "Ricoh E-mail Report" (without quotes)
- **Text:** Enter a space in the field to leave it blank
- **Format:** Select CSV
- **Language:** English
- **Filename:** Type "machinelog" (without quotes)

7. In the **Schedule** screen, set the **Frequency** to **Daily** and select a **time** when the report will be generated and sent.



8. Click **OK** to complete the report task.

The task will run according to the schedule you created. To view or modify the task, click **Reports** → **Report Tasks**. Click on the task in the list, and you can modify the details as needed.

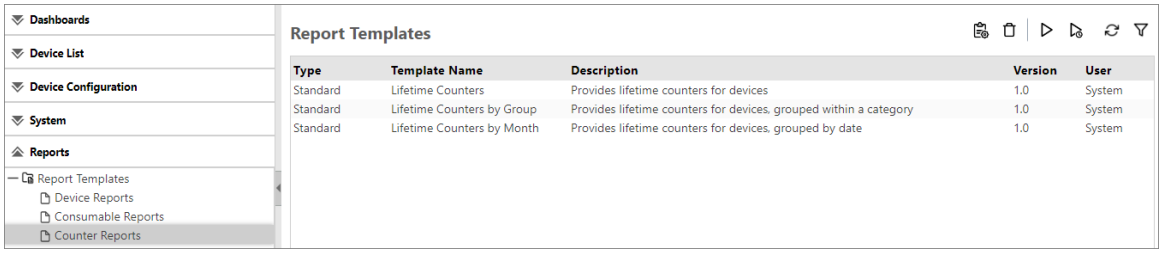
You can find the Report Task logs under **System** →**Logs** → **Report logs**.

Counter Reports

Use a report template in the ***Counter Reports*** category to create a report of device counters.

Counter Report Templates	Description
Lifetime Counters	Use this report to display the counter information of devices being monitored.
Lifetime Counters by Group	Use this report to check the counters by category group for devices being monitored.
Lifetime Counters by Month	Use this report to check the counters of the selected devices at the beginning of the month.

Counter Reports are displayed like the image below:



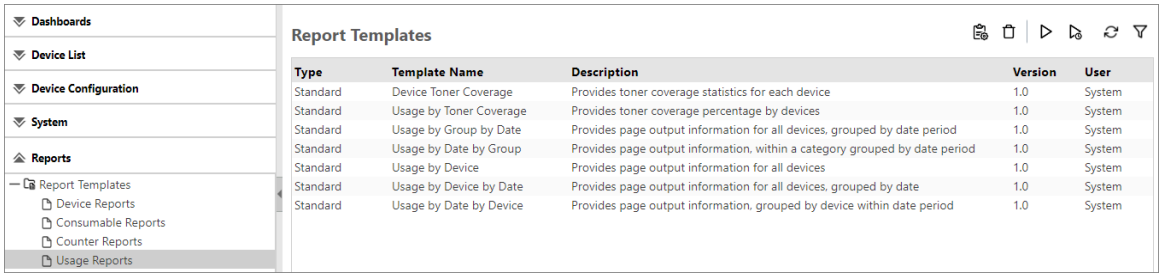
Usage Reports

Use a ***Usage Reports*** standard template to create a report on function usage and output volume for a device.

The table below lists all the standard templates of the ***Usage Reports*** category.

Usage Report Templates	Description
Device Toner Coverage	Use this report to view the toner coverage of all devices (by default), or the selected devices.
Usage by Toner Coverage	Use this report to view the ratio of output pages that correspond to each toner coverage category for the selected devices. • ***Coverage*** is the total toner usage (in units of 1%) per sheet of A4 page. For example, when an entire A4 sheet is filled with solid black, black toner coverage is 100%. • ***Toner coverage*** is divided into three types: low, medium, and high. The defaults for each category are as follows: ◦ Low: Lower than 5% ◦ Mid: 5% to less than 20% ◦ High: 20% or higher
Usage by Group by Date	Use this report to view the number of output pages by ***device group during a fixed period*** for devices being monitored. You can also view the number of output pages by ***device group*** and date in the detailed information.
Usage by Date by Group	Use this report to view the number of output pages by ***date*** during a fixed period for devices being monitored. You can also check the number of output pages by ***date*** for each category group in the detailed information.
Usage by Device	Use this report to view the number of output pages by ***device group*** for devices being monitored.
Usage by Device by Date	Use this report to view the number of output pages by ***device during a fixed period*** for devices being monitored. You can also view the number of output pages by ***device*** and date in the detailed information.
Usage by Date by Device	Use this report to view the number of output pages by ***date during a fixed period*** for the devices being monitored. You can also check the number of output pages by ***date*** for each device in the detailed information.

Usage Reports are displayed like the image below:



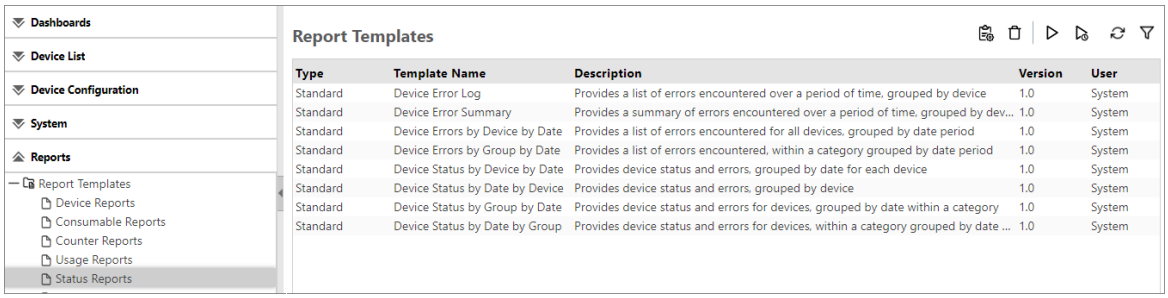
Status Reports

Use a report template in the ***Status Reports*** category to create a device status report and error log report.

Status Report Templates	Description
Device Error Log	Use this report to view the errors that occurred during a fixed period.
Device Error Summary	Use this report to view a summary of the errors that occurred during a fixed period.
Device Errors by Device by Date	Use this report to view the errors that occurred during a fixed period by device and date.
Device Errors by Group by Date	Use this report to view the errors that occurred during a fixed period by category group and date.
Device Status by Device by Date	Use this report to view the status and errors by device during a fixed period. You can also view the status and errors by device and date in the detailed information.
Device Status by Date by Device	Use this report to view the device status and errors by date during a fixed period. You can also view the status and errors by date and device in the detailed information.
Device Status by Group by Date	Use this report to view the errors that occurred during a fixed period by category group and date.
Device Status by	Use this report to view the device status and errors by date during a fixed period. You can also view the device status and errors by date

Status Report Templates	Description
Date by Group	and category group in the detailed information.

Status Reports are displayed like the image below:



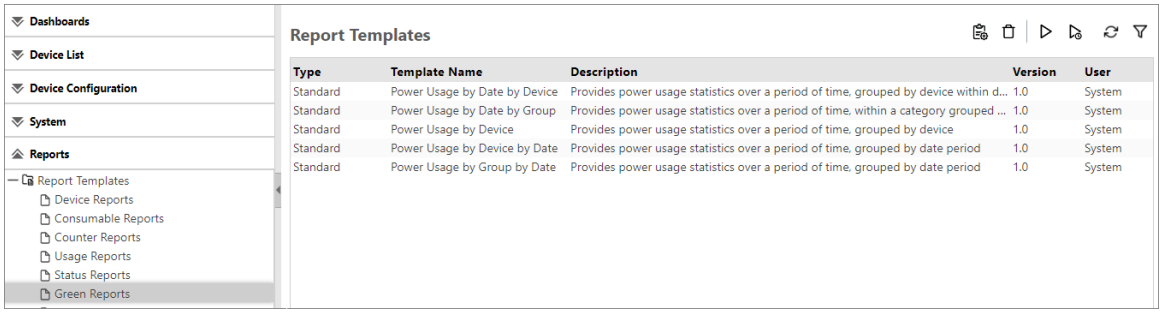
Green Reports

Use a report template in the ***Green Reports*** category to create a power usage report of a device.

Green Report Templates	Description
Power Usage by Date by Device	Use this report to view the power usage by date during a fixed period. You can also view a log of the power usage by date and device in the detailed information.
Power Usage by Date by Group	Use this report to view the power usage by date during a fixed period. You can also view the power usage by date by category group.
Power Usage by Device	Use this report to view the power usage of each device during a fixed period.
Power Usage by Device by Date	Use this report to view the power usage by device during a fixed period. You can also view a log of the power usage by device and date.
Power Usage by Group by	Use this report to view the power usage during a fixed period for each device group in a category. You can also view a log of the power usage by device group and date.

Green Report Templates	Description
Date	

Green Reports are displayed like the image below:



Document Usage Summary Reports

Use a report template in the ***Document Usage Summary Reports*** category to create a summary report of the total document usage (number of printed or sent pages) for a device based on various criteria.

Note: To create reports in this category, the RICOH CloudStream Print&Scan license is required in addition to the Device Management license.

Document Usage Summary Report Templates	Description
Document Usage Summary by Department by Date	Use this report to view the document usage for the selected departments over a fixed period (year, month, and day). Dates with no output are not shown. **Note:** When a user is transferred from one department to another, the department to which the user originally belonged when the job was output is counted.
Document Usage Summary by Department by Document Type	Use this report to view the document usage by job type (print, copy, scan, etc.) for the selected departments. Job types with no output are not shown.
Document Usage Summary by Department by User	Use this report to view the document usage by user in the selected departments. Users with no output are not shown.
Document Usage Summary by Device	Use this report to view the document usage for the selected devices. Devices with no output are not shown. The cost ratio is indicated in a graph, and device names, number of pages, and

Document Usage Summary Report Templates	Description
	cost are indicated in a table. **Note:** The graph and table show top 10 devices for cost, and the other devices are grouped into "Other".
Document Usage Summary by Device by Date	Use this report to view the document usage for the selected devices over a fixed period (year, month, and day). Dates with no output are not shown.
Document Usage Summary by Device by Hour	Use this report to view the document usage over 24 hours for the selected devices. Hours with no output are not shown.
Document Usage Summary by Hour	Use this report to view the total document usage for the selected hours. Hours with no output are not shown.
Document Usage Summary by User	Use this report to view the document usage for the selected users. Users with no output are not shown. The cost ratio is indicated in a graph, and user IDs, number of pages, and cost are indicated in a table. **Note:** The graph and table show top 10 devices for cost, and the other devices are grouped into "Other".
Document Usage Summary by User by Date	Use this report to view the document usage for the selected users over a fixed period (year, month, and day). Dates with no output are not shown.
Document Usage Summary by User by Device	Use this report to view the document usage by device for the selected users. Devices with no output are not shown.
Document Usage Summary by User by Document Type	Use this report to view the document usage by job type (print, copy, scan, etc.) for the selected users. Document types not output are not shown.

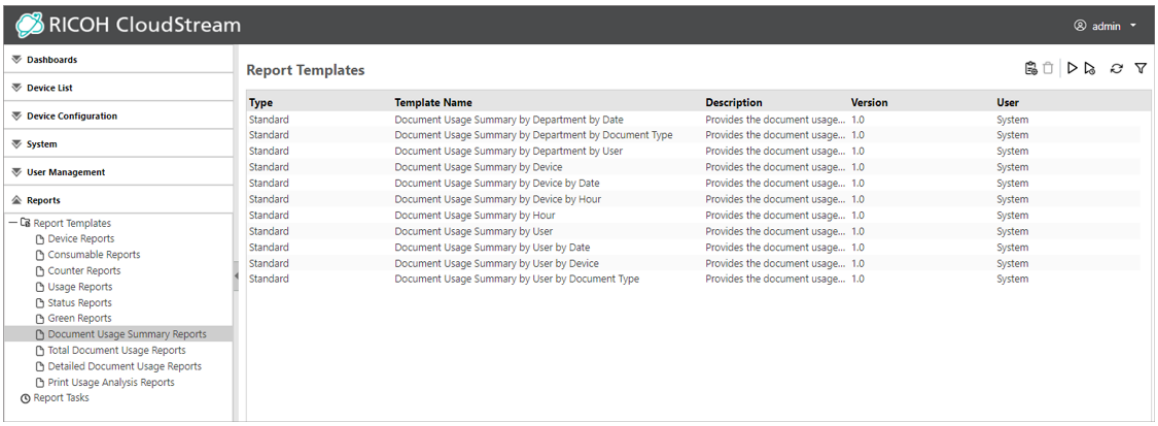
When a department has a hierarchical structure, the document usage summary by department is calculated as a sum of usage of lower levels.

For example: When Department C exists under Department B under Department A and their usage is c, b, a respectively:

- Document usage of Department A is a+b+c
- Document usage of Department B is b+c

- Document usage of Department C is c

Document Usage Summary Reports are displayed like the image below:



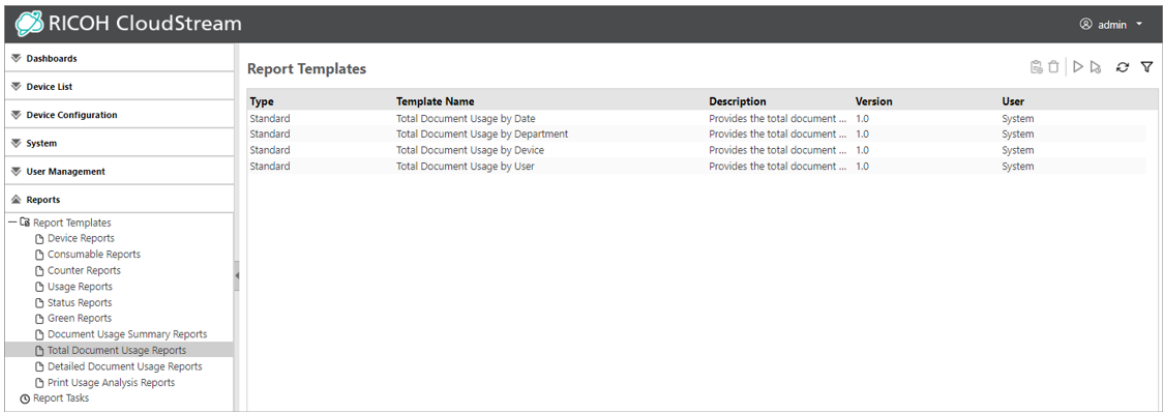
Total Document Usage Reports

Use a report template in the ***Total Document Usage Reports*** category to create a report with the total document usage (number of printed or sent pages per job type).

Total Document Usage Report Templates	Description
Total Document Usage by Date	Use this report to view the total document usage for the specified period. Dates with no output are not shown. The output ratio of the job type (print, copy, scan, fax) is indicated in a graph, and job type names, number of pages, and total cost (a total for all selected periods) are indicated in a table.
Total Document Usage by Department	Use this report to view the total document usage for the selected departments. Departments with no output are not shown. The output ratio of the job type (print, copy, scan, fax) is indicated in a graph, and the job type name, number of pages, and total cost (a total for all selected departments) are indicated in a table.
Total Document Usage by Device	Use this report to view the total document usage by document for the selected devices. Devices with no output are not shown. The output ratio of the job type (print, copy, scan, fax) is indicated in a graph, and job type names, number of pages, and total cost (a total for all selected devices) are indicated in a table.
Total Document Usage by User	Use this report to view the total document usage for the selected users. Users with no output are not shown. The output ratio of the job type (print, copy, scan, fax) is indicated in

Total Document Usage Report Templates	Description
	a graph, and job type names, number of pages, and total cost (a total for all selected users) are indicated in a table.

Total Document Usage Reports are displayed like the image below:



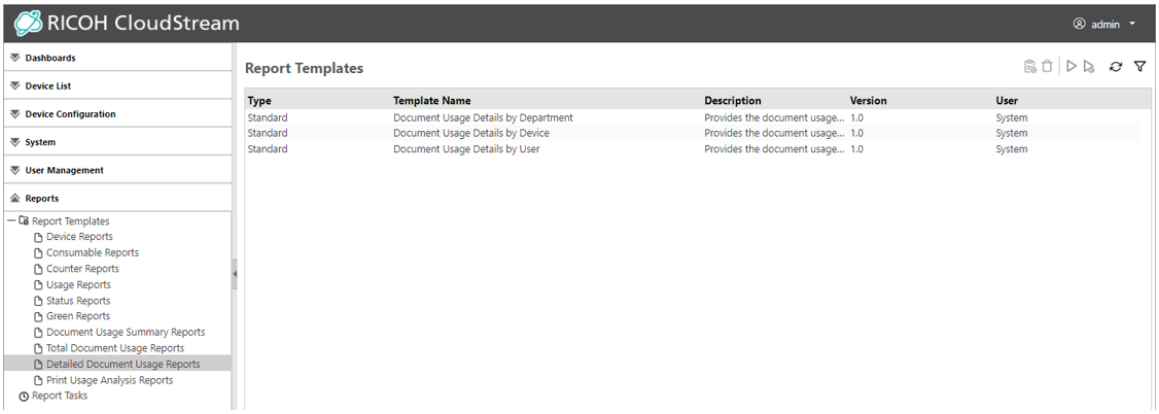
Detailed Document Usage Reports

Use a report template in the ***Detailed Document Usage Reports*** category to create a detailed report of document usage (number of printed or sent pages) based on various criteria.

Note: To create reports in this category, the RICOH CloudStream Print&Scan license is required in addition to the Device Management license.

Document Usage Details Report Templates	Description
Document Usage Details by Department	Use this report to view details of the printed document for the selected cost centers.
Document Usage Details by Device	Use this report to view details of the printed document for the selected devices.
Document Usage Details by User	Use this report to view details of the printed document for the selected users.

Detailed Document Usage Reports are displayed like the image below:



Print Usage Analysis Reports

Use a report template in the ***Print Usage Analysis Reports*** category to create a report of the total print usage based on various criteria.

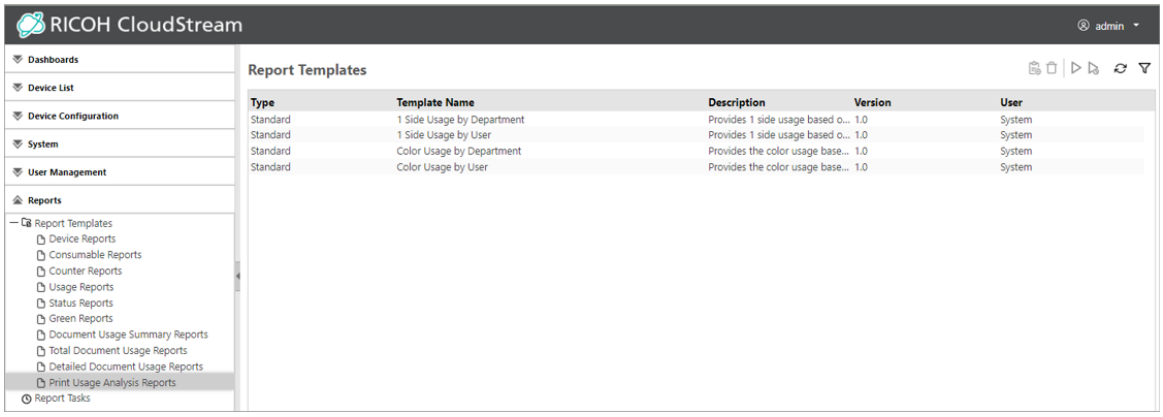
Note: To create reports in this category, the RICOH CloudStream Print&Scan license is required in addition to the Device Management license.

Print Usage Analysis Report Templates	Description
1 Side Usage by Department	Use this report to view the one-sided print usage of the selected cost centers. Departments with no output are not shown. The one-sided print usage by department is indicated in a bar graph, and department names, number of pages, one-sided print usage (%), and cost are indicated in a table. **Note:** The graph and table show top 10 departments for one-sided print usage (%), and the other departments are grouped into "Other".
1 Side Usage by User	Use this report to view the one-sided print usage for the selected users. Users with no output are not shown. The one-sided print usage by user is indicated in a bar graph, and user names, number of pages, one-sided print usage (%), and cost are indicated in a table. **Note:** The graph and table show top 10 users for one-sided print usage (%), and the other users are grouped into "Other".
Color Usage by Department	Use this report to view the color usage for the selected departments. Departments with no output are not shown. The color usage by department is indicated in a bar graph, and department names, number of pages, color ratio (%), and cost are indicated in a table. **Note:** The graph and table show top 10 departments for color

Print Usage Analysis Report Templates	Description
	ratio (%), and the other departments are grouped into "Other".
Color Usage by User	Use this report to view the color usage for the selected users. Users with no output are not shown. The color usage by user is indicated in a bar graph, and user names, number of pages, color ratio (%), and cost are indicated in a table. **Note** **Note:** The graph and table show top 10 users for color ratio (%), and the other users are grouped into "Other".

Note: Savings (%) is the ratio of cost savings by using black-and-white or two-sided output. The ratio is calculated by the following formula: Savings (%)=(1-(Cost after savings/cost before savings)) × 100

Print Usage Analysis Reports are displayed like the image below:



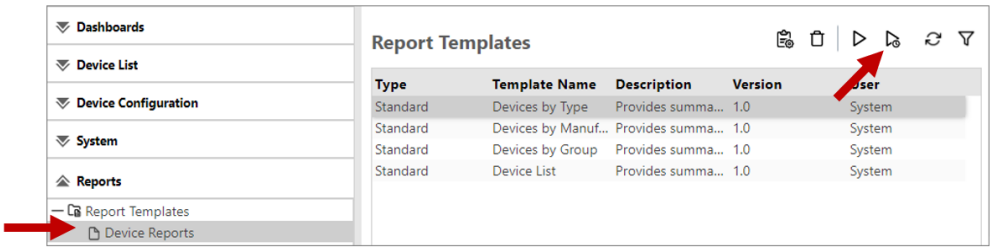
Run a Report on Schedule

A report task is a ***Run On schedule*** report where a report is generated either once, or on a daily, weekly, or monthly basis, and then sends the report to the specified recipients.

Note: When a scheduled task is run, the log is created in the Report Log. Refer to System Logs on page 214 for details.

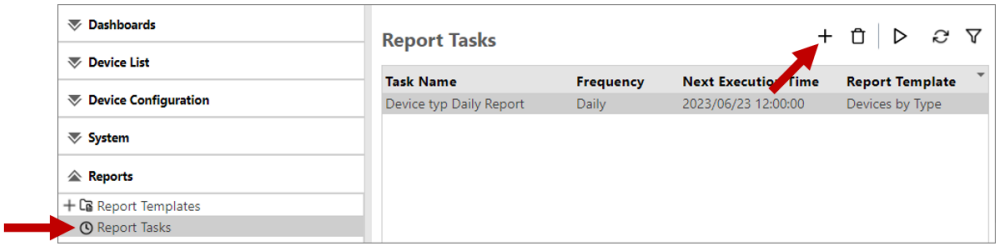
You can create a report task (or Run on Schedule) task from the following screens:

- **Via Report Templates**
  1. Login as an admin with reports privileges.
  2. Go to the ***Reports*** section.
  3. Expand ***Report Templates.***
  4. Select a ***Report Category***. Report templates are categorized based on their purpose.
  5. From the list of report templates, select the report template you want to create a report task with.
  6. Click [Run On Schedule].



  7. Configure a Report Task on page 351.

- **Via Report Tasks**
  1. Login as an admin with reports privilege.
  2. Go to the ***Reports*** section.
  3. Click ***Report Tasks.***
  4. Click + to add a report task.



5. Configure a Report Task on page 351.

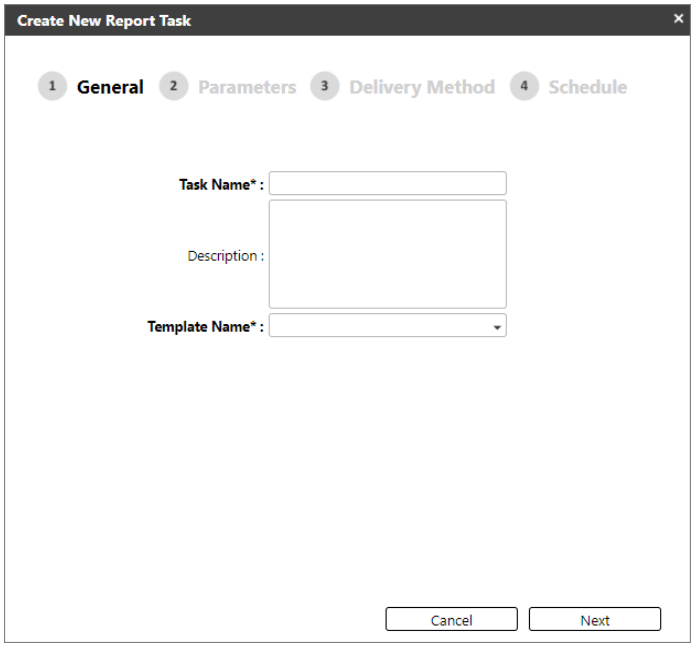
Configure a Report Task

A ***Create New Report Task*** dialog is displayed when running a report on a schedule.

Follow the steps below to schedule a report.

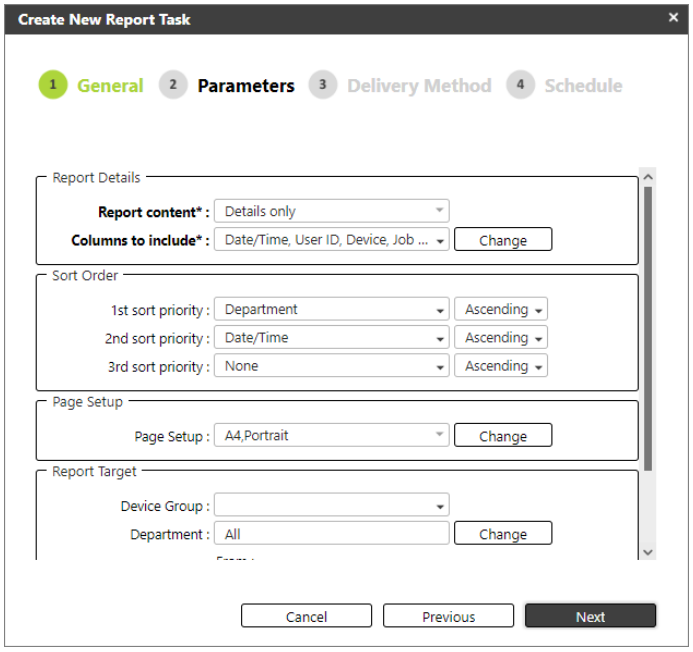
Order	Instructions
1	General on page 351.
2	Parameters on page 352.
3	Delivery Method on page 353.
4	Schedule on page 355.

General



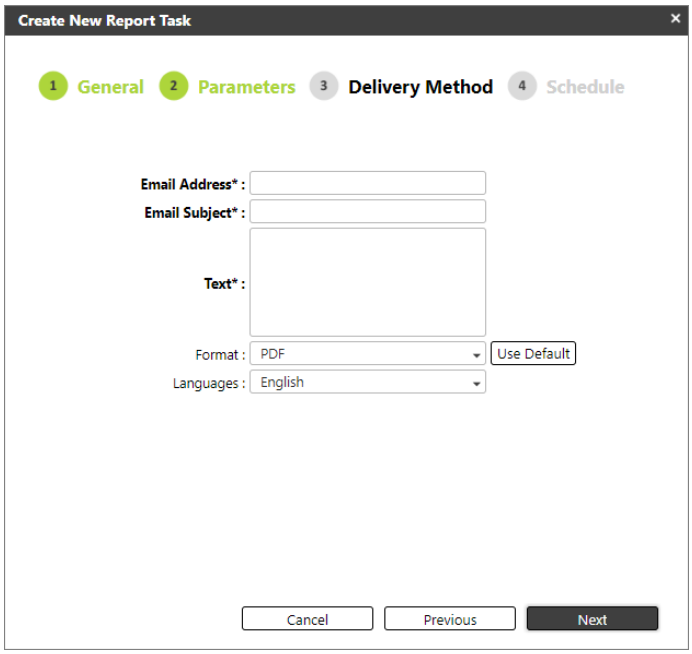
1. Enter the name of the task. The name must not be a duplicate of an existing task in the list.
2. (Optional) Enter a description of the report task.
3. Select the template you want to use to schedule a report.
    - If creating a task from a template, the template name will be the base template and it cannot be edited from the dialog. To change the template, you must close the dialog and select the other template.
    - If creating a task from the ***Report Tasks*** screen, you must select a template from the list.
4. Click **[Next]** to set the Parameters.

Parameters



1. Select the parameters of the report. Required fields must not be empty. Refer to ***Report Parameters*** section in Parts of a Report Template on page 370.
2. Click **[Next]** to set the ***Delivery Method.***

Delivery Method



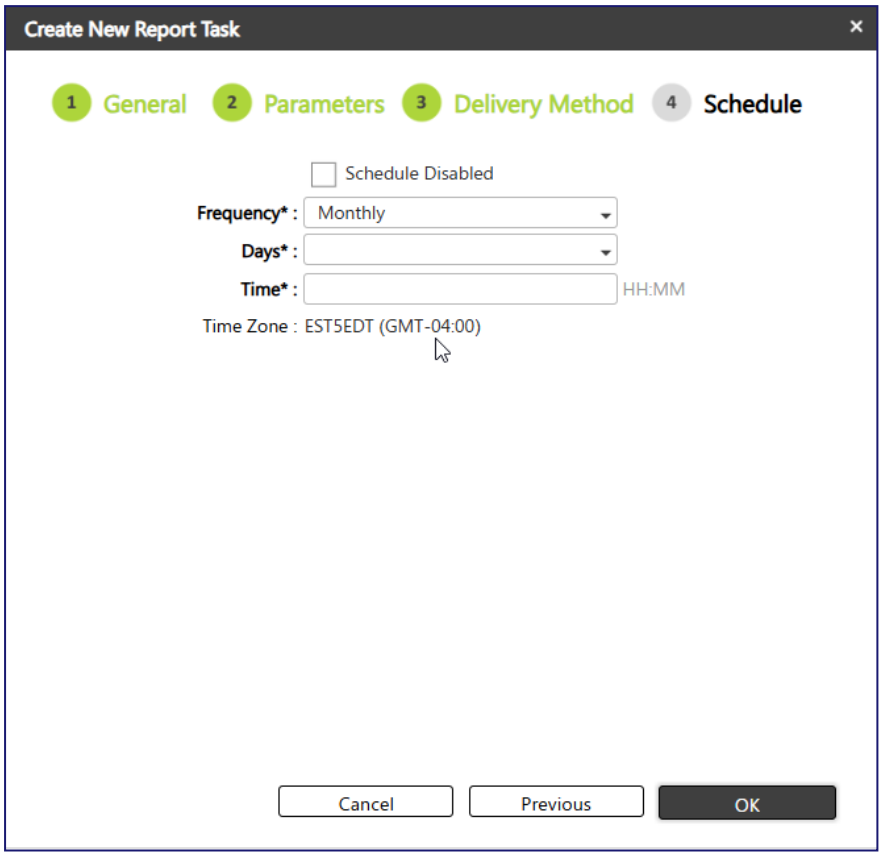
1. Enter the recipient's email address. You can enter multiple email addresses separated by a semi-colon.
2. Enter the Email Subject.
3. Enter the body of the email. The recipients will receive an email with the report. Make sure to write an email body describing the type of report attached.
4. Select how the report will be formatted. By default, PDF is selected, but you can select CSV, HTML, or Excel. Or click the **[Use Default]** button to use the default file format of PDF.

Format	Description	Remarks
PDF	Outputs the report in PDF (Adobe Portable Document Format) file format. Use Adobe Acrobat or another PDF viewer to open the report file.	When you output a report with information using conditions based on device groups or devices, PDF bookmarks are created with selected conditions (device group name, device name, etc.).
CSV	Outputs the report in CSV (Comma Separated Value)	The following character codes are used in the CSV files: • Japanese: Shift-JIS

Format	Description	Remarks
	file format.	• Chinese (Traditional): GB18030 • Other: Windows Latin 1 The first line of the table shows the titles of each item.
Excel	Outputs the report in Excel (Microsoft Excel Spreadsheet) file format. Use Microsoft Excel 2007, 2010, 2013, 2016 or another application that supports Excel files to open the report file. The chart in the Excel file will be a static image.	When a value in a table is changed, the corresponding Excel graph is updated. The layouts of the report displayed in the system and Excel file report may be different.

5. Select the language of the report. By default, the language will be English, but you can select other languages such as:
    - Français
    - Deutsch
    - Italiano
    - Español
    - Nederlands

Schedule



Checking the "**Schedule Disabled**" setting will create the report task but no report will be generated.

Note: A report task will only generate the report if the schedule is enabled.

To set the schedule, make sure the **Schedule Disabled** option is **unchecked**, only then will the report schedule options be displayed.

Select a value for **Frequency**. Available options are:

Frequency	Description	Example
Monthly	This is the default option. If selected, a report is generated and sent to recipients every month. a. Select the day(s) of the month the report task will run. You can check multiple days starting from 1 to 31 and "Last day of month" which will run the task on the last day of each month.	Input: • Days: 1 and 20 • Time: 09:00 Result: The task will run on May 20, then run on June 1st and continue to run every month until the report is disabled.

Frequency	Description	Example
	b. After the days are selected, enter the time to generate and send the report. The setting accepts input in 24-hour format.	
Once	This will generate a report and send it to recipients based on the set Date and Time. a. Enter the time to generate and send the report. The setting accepts input in 24-hour format. b. Enter the date in MM/DD/YYYY format. You can also click on the calendar icon to select date in a calendar view.	Input: • Time: 10:00 • Start Date: June 3, 2023 Result: A report is generated on June 3rd at 10:00 AM, then sent to recipients. The task will run once and will remain in the Report Task list.
Daily	This will generate a report and send it to recipients daily. a. Enter the time to generate and send the report. The setting accepts input in 24-hour format.	Input: • Time: 09:00 Result: A report is generated every 09:00 daily, then sends it to recipients.
Weekly	This will generate a report and send it to recipients weekly. a. Select the day(s) of the week. Available options are Monday to Sunday. b. After the days of the week are selected, enter the time to generate and send the report. The setting accepts inputs in 24-hour format.	Input: • Days: Monday and Friday • Time: 16:00 Result: A report is generated every Monday and Friday at 16:00, then sends it to recipients.
Timezone	Displays the client configured time zone.	The timezone displayed is based on the timezone configured for your customer account.

Click **[OK]** to create the report task. Once a scheduled report is created, you can see the task in the Report Task page. Please check Manage Report Tasks on page 358 for more details.

Note: When a scheduled task is run, the log is created in the Report Log. Refer to System Logs on page 214 for details.

Manage Report Tasks

All scheduled reports are displayed on the Report Task screen. You can manage the report tasks using the following functions.

Icon	Name	Function
	Add	Adds a new scheduled report. You can find the steps to create a new scheduled report in Run a Report on Schedule on page 350.
	Delete	Deletes the scheduled report. There is also an option to disable the schedule instead of deleting the report itself. This will not delete the report but will only stop the creation and sending of reports to recipients. Consider disabling a useful scheduled report before deleting it.
	Run Immediately	When this button is clicked this will immediately generate a report based on the configured parameters and send it to the specified recipients. Please see Run a Report Immediately on page 334. You will see a pop-up dialog saying that the scheduled report is initiated. Although the report is run manually, it will still be generated based on the configured schedule.
	Refresh	This will refresh the list of scheduled reports.
	Filter	Click this filter if you want to unhide or hide the filter columns.
	(Filter)Search	Clicking this will search for the item that matches your input. To use this, make sure to click the Filter icon to enable the filter columns, then input the search text to the desired column then click this button.

Update a Report Task

A report task has four nodes. There are settings you can and cannot modify, please refer to the nodes below.

Task Property on page 358.
Parameters. Refer to ***Report Parameter*** in Parts of a Report Template on page 370 for more details.
Schedule on page 359.
Delivery Method on page 360.

Task Property

Item Name	Description
Task Name	The name of the task. If you want to update the task name, please make sure the new name is not a duplicate of the existing report tasks.
Description	Update the description. Maximum allowed characters is up to 511.
Next Execution Time	This item is not editable. This is the nearest date and time the report task will run. If the report is every Friday, the date will display the nearest Friday's date. The timezone is included in brackets and is based on the timezone configured for your customer account.
Report Template	This item is not editable. The template used to create the report.
Created Date	This item is not editable. The date the task is created.
Schedule Disabled	If checked, the report task will not run.

Note: Please click [Save] after making necessary changes.

Schedule

Note: If you modify the schedule, the ***Next Execution Time*** in the ***Task Property*** will be updated too.

If you disabled the Schedule from this node, the ***Schedule Disabled*** checkbox in the ***Task Property*** will be checked too.

If ***Schedule Disable*** is checked, the following settings cannot be edited. Uncheck ***Schedule Disable*** to edit the ***Frequency***.

Frequency	Description	Example
Monthly	If selected, a report is generated and sent to recipients every month. a. Select the day(s) of the month the report task will run. You can check multiple days starting from 1 to 31 and "Last day of month" which will run the task on the last day of each month. b. After the days are selected, enter the time to generate and send the report. The setting accepts input in 24-hour	Input: • Days: 1 and 20 • Time: 09:00 Result: The task will run on May 20, then run on June 1st and continue to run every month until the report is disabled.

Frequency	Description	Example
	format.	
Once	This will generate a report and send it to recipients based on the set Date and Time. a. Enter the time to generate and send the report. The setting accepts input in 24-hour format. b. Enter the date in MM/DD/YYYY format. You can also click on the calendar icon to select date in a calendar view.	Input: • Time: 10:00 • Start Date: June 3, 2023 Result: A report is generated on June 3rd at 10:00 AM, then sent to recipients. The task will run once and will remain in the Report Task list.
Daily	This will generate a report and send it to recipients daily. a. Enter the time to generate and send the report. The setting accepts input in 24-hour format.	Input: • Time: 09:00 Result: A report is generated every 09:00 daily, then sends it to recipients.
Weekly	This will generate a report and send it to recipients weekly. a. Select the day(s) of the week. Available options are Monday to Sunday. b. After the days of the week are selected, enter the time to generate and send the report. The setting accepts input in 24-hour format.	Input: • Days: Monday and Friday • Time: 16:00 Result: A report is generated every Monday and Friday at 16:00, then sends it to recipients.

Note: Please click [Save] after making necessary changes.

Delivery Method

Item Name	Description
Email Address	You can add more recipients by separating them with a semi-colon.
Email Subject	Edit the email subject.
Text	This is the body of the email. You can modify this if you want.
Format	You can select either PDF, CSV, or Excel file format. You can also click the **[Use Default]** button to select PDF.
Languages	Modify the language used to create the report.

Note: Please click **[Save]** after making necessary changes.
All changes will be applied in the next report execution.

Create Custom Report Template

A customized report template is based on a standard report template. In a standard report template, all settings are fixed and cannot be modified, while in a customized report template, you can set which items in the report will be included and how the report will look.

Important notes when creating a custom report template.

- To specify report generation date, closing day, start date, and end date, see for examples in Examples of Reports Date Range on page 376.
- Depending on the parameter, you can select ***Lock this selection*** to lock the setting and make it read-only. If you enable ***Lock this Selection*** for any of the options, these settings cannot be edited when you create a Report Task that uses this template.
- Columns displayed in the reports are configured by changing ***Columns to Include.***

There are two steps to create a custom report.

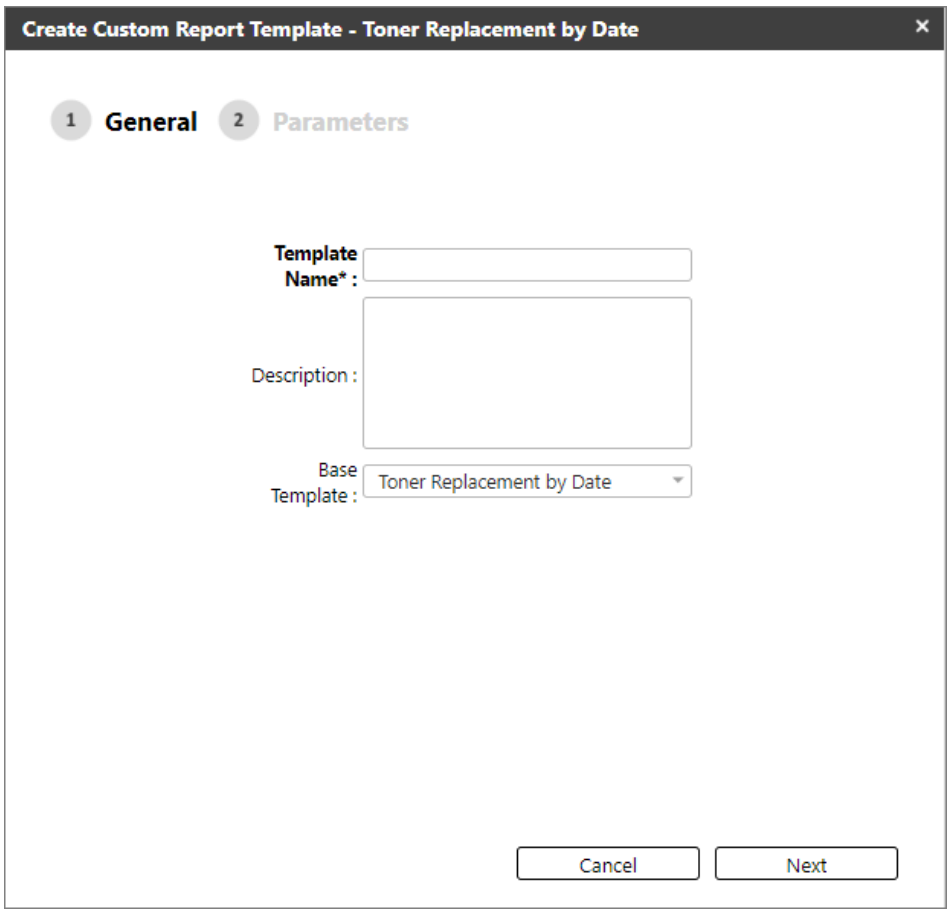
Order	Instructions
1	Create a Custom Template on page 362.
2	Set Custom Report Parameters on page 363.

Create a Custom Template

1. Login as an admin with reports privilege.
2. Go to the ***Reports*** section and expand ***Report Templates.***
3. Select a ***Report Category***. Report templates are categorized based on their purpose. Please select the category that contains the targeted standard or custom report template.
4. From the list of report templates, select the report template which will be used as the basis of your custom report template. The report template can be a standard or custom report template.

   Note: The parameters of the custom report that you will be creating will depend on the base template you select.

5. Click  **[Create Custom Report]**. A similar screen is shown below.



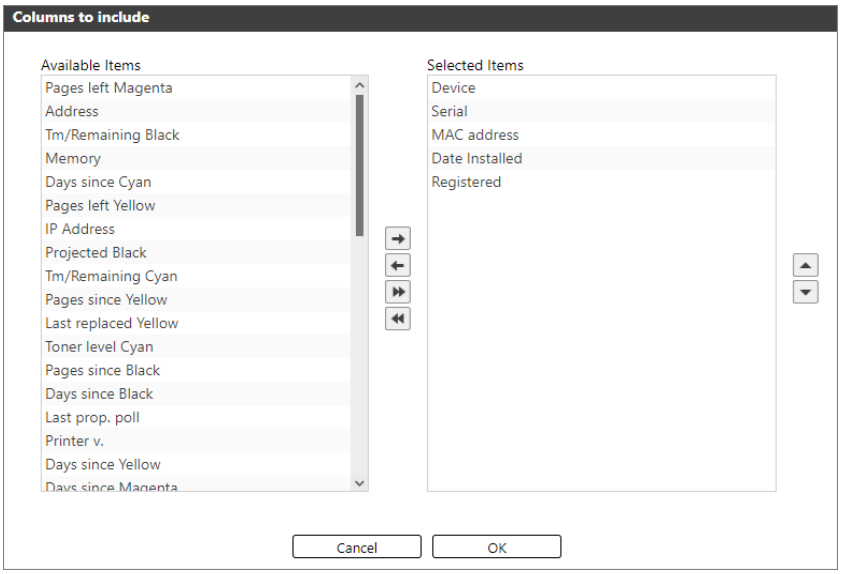
6. Enter the custom report template name. The name must not be a duplicate of an existing report template.
7. (Optional) Input the description of the custom report template.
8. Check the ***Base Template*** if correct. The base template should be the template selected in step # 4. If this is not the base template you want, please go back to step #4 and select the desired base template.
9. Click **[Next]**.

Note: If the template name is empty or a duplicate, an error will be displayed, and you will not be able to proceed to the next step.

Set Custom Report Parameters

Setup the **Parameters** step. If you want to modify the ***General*** settings, go to Create Custom Report Template on page 362.

1. Clicking next will display the ***Parameters*** step. Configure the details and page settings of the report template. The items that appear and can be configured vary depending on the report template type.
2. Select value for ***Report Details.***

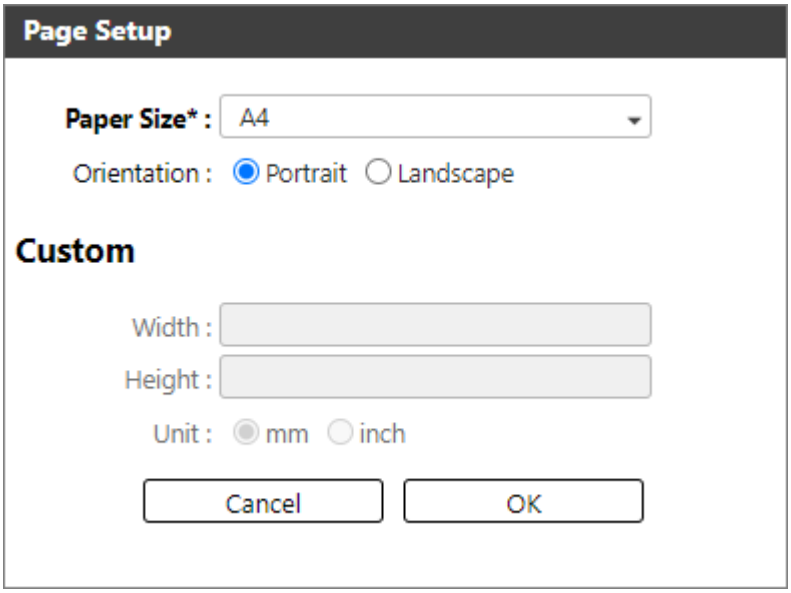
Item Name	Function
Report Content	Displays the report overview and/or details. Available options are: • Summary Only - displays the summary of the report only. • Details Only - only the details of the report are displayed. • Summary and details - both are displayed. **Note:** The available options depend on the base report template. A report template may not support Summary view so the only option available is "Details Only".
Columns to include	Select the columns to be included in the report. Click **[Change...]** to display the dialog where you can set the columns that will be included when the report is generated. The example below shows the items available for selection to create a custom Device by Manufacturer report.  The left-hand side displays the **Available Items**, while the right-hand side is the ***Selected Item*** where the items are the columns that will be included in the report. To move the items to the other side, use the following buttons.  This button will move the selected item to the right-hand

Item Name	Function
	side. The item will be added to the columns to include.  This button will move the selected item to the left-hand side. The item will be removed from the columns to include.  This button will add all items from ***Available*** items to ***Selected*** items.  This button will remove all items from ***Selected*** items.  This button will move the selected item upward. If you want to display the item as the first column in the report, move the selected item to the top.  If you want to move the item to the farthest right column of the report, move the item down to the end of list. Make use of the up and down buttons to arrange your columns.

3. Select value for ***Sort Order***.

Item Name	Function
1st sort priority	Select the first condition for sorting. Be sure to configure the first condition before going to the next priority.
2nd sort priority	Select the second condition for sorting.
3rd sort priority	Select the third condition for sorting.

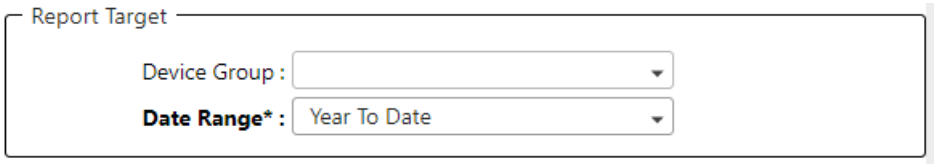
4. Select a value for ***Page Setup.***
5. Click **[Change ...]** to display the ***Page Setup*** dialog box and select the paper size and orientation.



Item Name	Function
Paper Size	Select the paper size to be used to output the report. Available paper sizes: • A4 • A3 • B4 • B5 • Letter • Legal • 11x17 • Custom
Orientation	Select the paper orientation. Available orientations: • Portrait • Landscape
Width	Specify the paper width when the paper size is set to [Custom]. Specify a value from 20 to 5,080 mm.
Height	Specify the paper height when the paper size is set to [Custom]. Specify a value from 20 to 5,080 mm.
Unit	Select the unit (mm, inch) to be used.

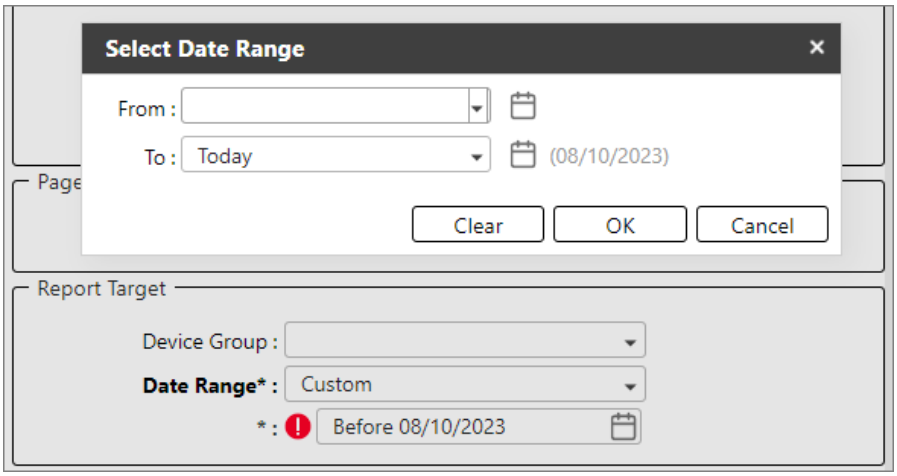
6. Select value for ***Report Target***.

The Report Target settings will not be available for some templates. Some templates will also have different Report Targets based on their purpose.



If the template supports the items listed here, you can configure the items with the information below.

Item Name	Function
Device Group	Select the device group where the report details will be extracted from.
Lock this selection	If this item is checked, the Device Group item will not be editable when the report template is executed.
Date Range	Select the date range. Some examples are described in Examples of Reports Date Range on page 376. Available options are: • **Custom** - A custom date range option will display. Please see the topic below. • **Today** - The current day. • **Yesterday** - The previous day. • **Last Week** - From Sunday to Saturday of the previous week. • **Last Month** - The previous month. • **Last Quarter** - The previous quarter. (January - March, April-June, July-September, October- December). If the current date is August 10, the date range will be from April to June. • **Last Year** - The date range will be from January to December of the previous year. • **Week to Date** - The date range will be from Sunday to the current day. If the current day is August 10, the date range will be from August 6 to August 10. • **Month to Date** - The date from the first day of the month to the current day. • **Quarter to Date** - The first date of the first quarter to the current day.

Item Name	Function
	• **Year to Date** - This is the default value. The date range will be from January 1 of the current year to the current day. To set a custom date, select Custom as value then click on the date or the calendar displayed below it.  **Custom Date Range options:** • **Today** - The current day. • **Yesterday** - The previous day. • **Current day of last week** - The day of the previous week. If the current day is August 10, the current day of last week is August 3. • **Current day of next week** - The day of the next week. If the current day is August 10, the current day of the next week is August 17. • **Current day of last month** - The day of the previous month. If the current day is August 10, the current day of last month is July 10. • **Current day of next month** - The day of the next month. If the current day is August 10, the current day of next month is September 10. • **N days ago** - N refers to a number. If the given number is 10, the date range will be 10 days ago *to* the current day. • **N days from now** - N refers to a number. If the given number is 10, the date range will be 10 days *from* the current

Item Name	Function
	day. • **N weeks ago** - N refers to a number. If the given number is 5, the date range will be 5 weeks ago *to* the current day. • **N weeks from now** - N refers to a number. If the given number is 5, the date range will be 5 weeks *from* the current day. • **N months ago** - N refers to a number. If the given number is 2, the date range will be 2 months ago *to* the current day. The available value for N is between 1 and 12. • **N months from now** - N refers to a number. If the given number is 2, the date range will be 2 months *from* the current day. The available value for N is between 1 and 12.  **Note:** If you select the ***Lifetime Counters*** or ***Lifetime Counters by Group*** template, this field displays the "End Date" only. In this case, the report will retrieve counters from the database up until the selected ***End Date***. If the parameter is not specified, it will select counters with the latest poll time.

7. (Optional) If the template has a Summarization part, then please select a value. The value selected will determine how the report data will be summarized.
   - **Day** - Summarize data by day. This is the default option.
   - **Month** - Summarize data by month.
   - **Year** - Summarize data by year.
8. After all parameters are set, click **[OK]** to create the customized template.

Parts of a Report Template

When you select a report template in the list, the report properties are displayed with two nodes: ***General information*** and ***Report Parameters***.

General information

Item Name	Function
Template Name	The name of the report template. Only the custom report template name can be edited; the standard report template name cannot be edited.
Template Description	The description of the template.
Version	The version number of the template. For a custom report template, it will inherit the version number of its base template. This item cannot be edited.
Type	The type can be custom or standard.
User	The user name of the admin who created the custom template. For standard templates, this field is empty.
Base Template	Displays the base template used to create the custom template. For standard templates, this field is empty.

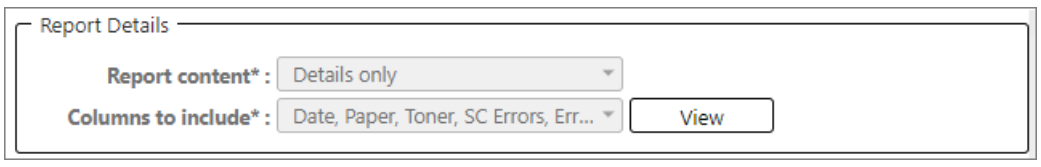
You cannot change the information in General node for Standard templates; however, custom template's name and description can be edited.

Report Parameters

The parameters have the following settings.

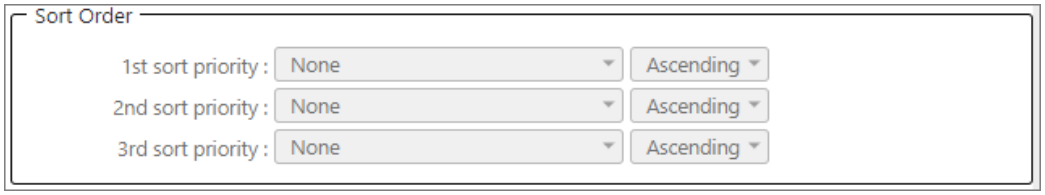
Report Details on page 370.
Sort Order on page 371.
Page Setup on page 372.
Report Target on page 373.
Summarization on page 376.

Report Details



Item Name	Function
Report Contents	Displays the report overview and/or details. Available options are: • Summary Only - displays the summary of the report only. • Details Only - only the details of the report are displayed. • Summary and details - both are displayed. **Note:** The report summary is a short description summarizing the detailed information is shown at the beginning of the report, you can quickly grasp the overall trend.
Columns to include	Select the item columns to be included in the report. Click the **[Change...]** button to display the dialog where you can set the columns to be included in the report. The dialog will display two list panes; the left-hand side displays the available items you can select, while the right-hand side is the columns that will be included in the report. To move the items to the other side, use the following buttons.  - This button will move the selected item to the right-hand side. The item will be added to the columns to include.  - This button will move the selected item to the left-hand side. The item will be removed from the columns to include.  - This button will add all items from ***Available*** items to ***Selected*** items.  - This button will remove all items from ***Selected*** items.  - This button will move the selected item upward. If you want to display the item as the first column in the report, move the selected item to the top.  - If you want to move the item to the farthest right column of the report, move the item down at the end of list. Make use of the up and down buttons to arrange your columns.

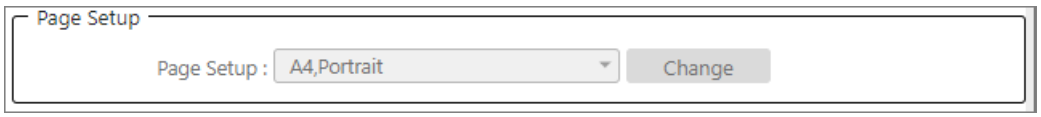
Sort Order



Please select the column item you plan to sort, then select the sorting order.

Item Name	Function
1st sort priority	The selected column and the type of sorting in 1st sort Priority will be implemented before other priorities.
2nd sort priority	The column and sorting type will be implemented after the first priority.
3rd sort priority	The column and sorting type will be implemented after the second priority.

Page Setup

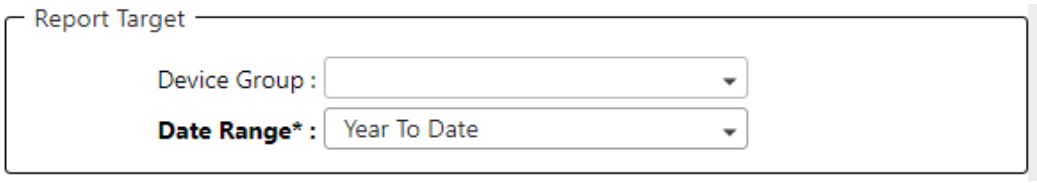


Item Name	Function
Page Setup	Click **[Change ...]** to display the ***Page Setup*** dialog box and select the paper size and orientation.
Paper Size	Select the paper size used to output the report. Available paper sizes: • A4 • A3 • B4 • B5 • Letter • Legal • 11x17 • Custom
Orientation	Select the paper orientation. Available orientations: • Portrait • Landscape

Item Name	Function
Width	Specify the paper width when the paper size is set to "Custom". Specify a value from 20 to 5,080 mm.
Height	Specify the paper height when the paper size is set to "Custom". Specify a value from 20 to 5,080 mm.
Unit	Select the unit (mm, inch) to be used.

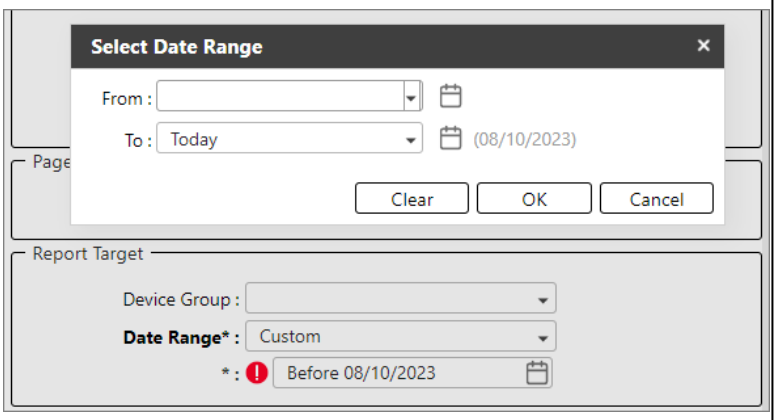
Report Target

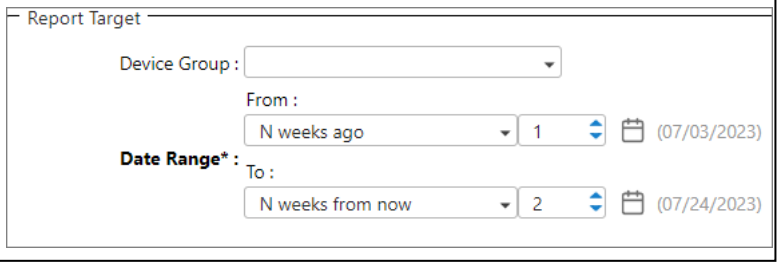
The Report Target settings will not be available for some templates. Some templates will also have different Report Targets based on their purpose.



If the template supports the items listed here, you can configure the items with the information below.

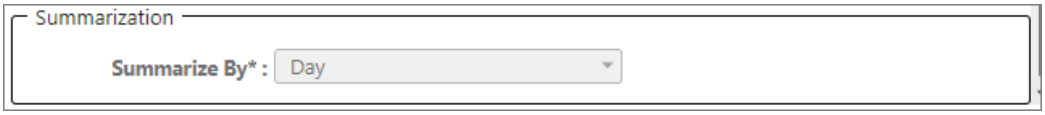
Item Name	Function
Device Group	Select the device group where the report details will be extracted from.
Lock this selection	If this item is checked, the Device Group item will not be editable when the report template is executed.
Date Range	Select the date range. Some examples are described in Examples of Reports Date Range on page 376. Available options are: • **Custom** - A custom date range option will display. Please see the topic below. • **Today** - The current day. • **Yesterday** - The previous day. • **Last Week** - From Sunday to Saturday of the previous week. • **Last Month** - The previous month. • **Last Quarter** - The previous quarter. (January - March, April-June, July-September, October-December). If the current date is August 10, the

Item Name	Function
	date range will be from April to June. • **Last Year** - The date range will be from January to December of the previous year. • **Week to Date** - The date range will be from Sunday to the current day. If the current day is August 10, the date range will be from August 6 to August 10. • **Month to Date** - The date from the first day of the month to the current day. • **Quarter to Date** - The first date of the first quarter to the current day. • **Year to Date** - This is the default value. The date range will be from January 1 of the current year to the current day. To set a custom date, select Custom as value then click on the date or the calendar displayed below it.  **Custom Date Range options:** • **Today** - The current day. • **Yesterday** - The previous day. • **Current day of last week** - The day of the previous week. If the current day is August 10, the current day of last week is August 3. • **Current day of next week** - The day of the next week. If the current day is August 10, the current day of the next week is August 17.

Item Name	Function
	• **Current day of last month** - The day of the previous month. If the current day is August 10, the current day of last month is July 10. • **Current day of next month** - The day of the next month. If the current day is August 10, the current day of next month is September 10. • **N days ago** - N refers to a number. If the given number is 10, the date range will be 10 days ago *to* the current day. • **N days from now** - N refers to a number. If the given number is 10, the date range will be 10 days *from* the current day. • **N weeks ago** - N refers to a number. If the given number is 5, the date range will be 5 weeks ago *to* the current day. • **N weeks from now** - N refers to a number. If the given number is 5, the date range will be 5 weeks *from* the current day. • **N months ago** - N refers to a number. If the given number is 2, the date range will be 2 months ago *to* the current day. • **N months from now** - N refers to a number. If the given number is 2, the date range will be 2 months *from* the current day. 

Item Name	Function
	Note: If you select the ***Lifetime Counters*** or ***Lifetime Counters by Group*** template, this field displays the "End Date" only. In this case, the report will retrieve counters from the database up until the selected ***End Date***. If the parameter is not specified, it will select counters with the latest poll time.

Summarization



If the report template has this section, please select how the data will be summarized.

Item Name	Function
Summarize By	Select how the data will be summarized. • Day • Month • Year

Examples of Reports Date Range

For details about the combinations of the report generation date, closing day, start date, and end date, see the following examples. The calendar under each example shows the date range to be included in the report.

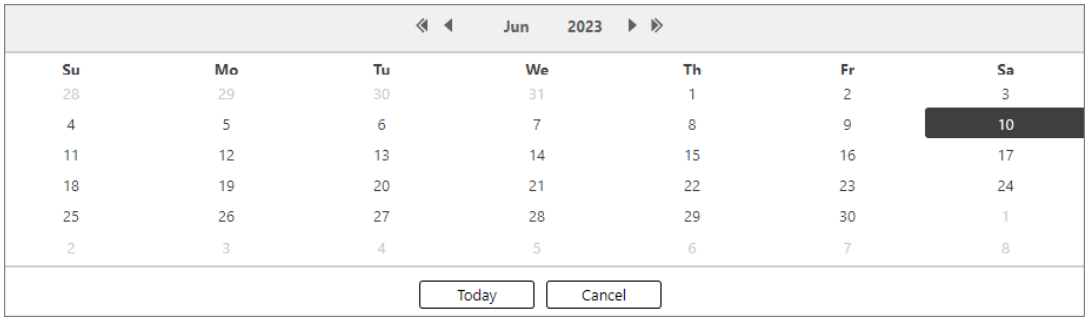
Here is the list of examples:

- Example 1 on page 376.
- Example 2 on page 377.
- Example 3 on page 378.
- Example 4 on page 378.

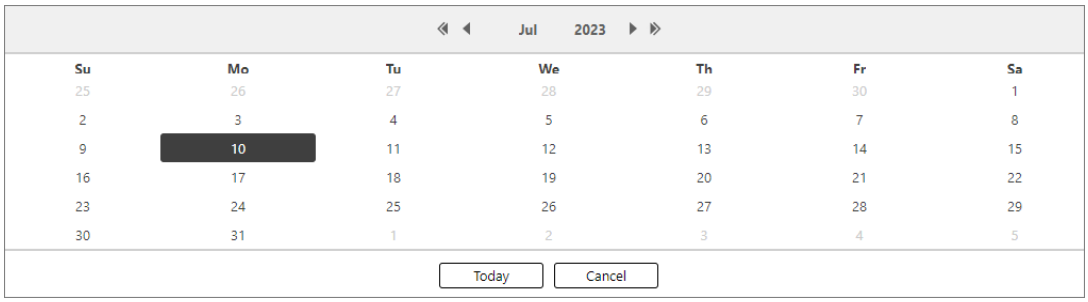
Example 1

Generate a report that starts from June 10 to July 10.

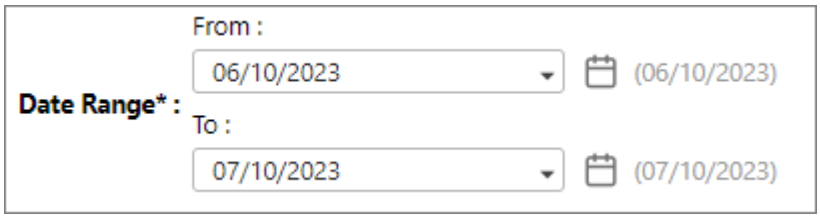
1. In ***From***, click the calendar icon.
2. Select June 10 from the calendar.



3. In ***To***, click the calendar icon and select July 10 from the calendar.



The resulting **Date Range** will be:



Example 2

Generate a report that started 2 months ago until yesterday.

1. In ***From***, click the dropdown menu and select ***N months ago.***
2. A box is displayed beside ***From***, then enter number 2. This means the report will be generated using the data gathered two months ago. If the current date is July 10, two months ago will be May 10.
3. In ***To***, click the dropdown menu and select ***Yesterday.***

The resulting **Date Range** will be:

Example 3

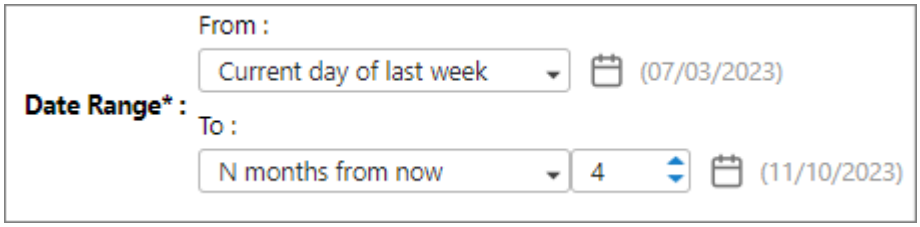
Generate a report that starts last week until the next four months.

1. In ***From***, click the dropdown menu and select ***Current day of last week.*** For example, the current day is July 10, and if this option is selected, the From date will be July 3.
2. In ***To***, click the dropdown menu and select ***N months from now.***
3. A box is displayed beside ***To***, then enter the number 4. This means that the report will be generated using the data gathered last week (July 3) until the next four months (November 10).

Note: The "N months from now" refers to the future months.

- If you set a scheduled monthly report for the next five months, every report generated will cover the last week until the current month. For example, today is September 11, and the data retrieved is from July 3 until September 10.
- In the fifth scheduled month (December), the report will be the same as the report generated in the fourth month (November) because the ***To*** field only specifies ***4 months from now*** covering from July 3 until November 10.
- The same mechanism applies to ***N days from now*** and ***N weeks from now.***

The resulting **Date Range** will be:



Example 4

Generate a report that starts two days ago until the next three months.

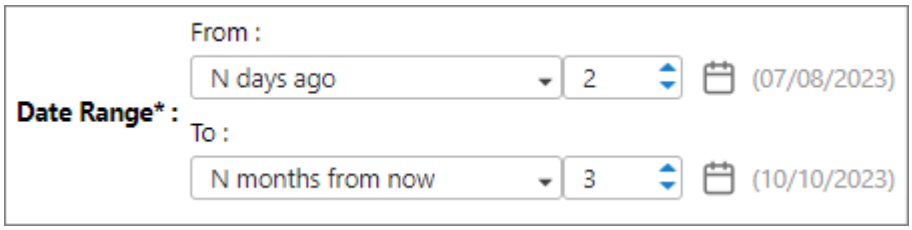
1. In ***From***, click the dropdown menu and select ***N days ago.***
2. A box is displayed beside ***From***, then enter number 2. This means the report will be generated using the data gathered in the last two days.

3. In ***To***, click the dropdown menu and select ***N months from now.***
4. A box is displayed beside ***To***, then enter the number 3. This means the report will be generated using the data gathered from two days ago (July 8) until the next three months (October 10).

Note: The "N months from now" refers to the future months.

- If you set a scheduled weekly report, every report generated will cover the last two days until the current month. For example, today is September 11, and the data retrieved is from July 8 until September 10.
- In the third week of October (October 17), the scheduled report will be the same as the report generated in the second week of October because the ***To*** field only specifies ***3 months from now*** covering from July 8 until October 10.

The resulting **Date Range** will be:



Supported Printers

For the full list of supported devices categorized by vendor, please refer to the following region-specific links:

- AP: https://supportsite.ap.cloudstream.ricoh.com/product/device-support/
- CA: https://supportsite.ca.cloudstream.ricoh.com/product/device-support/
- EU: https://supportsite.eu.cloudstream.ricoh.com/product/device-support/
- NA: https://supportsite.na.cloudstream.ricoh.com/product/device-support/

Data Flow (Device Management)

Web UI

Client	Server	Functions	Request Data	Response Data	Protocol	Port
PC	CloudStream Device Management	Web UI	UI request File upload	UI response File download	HTTPS	443
Mobile	CloudStream Device Management	Web UI	UI request File upload	UI response File download	HTTPS	443

DM Agent Deployment Tool/DM Agent

Client	Server	Functions	Request Data	Response Data	Pro-tocol	Port
DM Agent Deploy-ment Tool	CloudStrea-m Device Man-agement	Get service URLs	-	Service URLs	HTTPS	443
DM Agent Deploy-ment Tool	CloudStrea-m Device Man-agement	Generate client certificate	Onboard-ing code	Client certificate	HTTPS	443
DM Agent Deploy-ment Tool	Printer	Install DM Agent	DM Agent application file	-	HTTPS	443/5144-3
DM Agent	CloudStrea-m Device Man-agement	Get service URLs	-	Service URLs	HTTPS	443
DM Agent	CloudStrea-m Device Man-agement	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443

Client	Server	Functions	Request Data	Response Data	Pro-tocol	Port
DM Agent	CloudStrea-m Device Man-agement	Get polling con-figuration	-	Polling con-figuration	HTTPS	443
DM Agent	CloudStrea-m Device Man-agement	Get device man-agement task	-	Device con-figuration Firmware Application	HTTPS	443
DM Agent	CloudStrea-m Device Man-agement	Post device man-agement result	-	Device information Device con-figuration	HTTPS	443

WfH Client

Client	Server	Functions	Request Data	Response Data	Protocol	Port
WfH Client	CloudStream Device Management	Get service URLs	-	Service URLs	HTTPS	443
WfH Client	CloudStream Device Management	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
WfH Client	CloudStream Device Management	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
WfH Client	CloudStream Device Management	Get polling configuration	-	Polling configuration	HTTPS	443
WfH Client	CloudStream Device Management	Post device information	Device information	-	HTTPS	443
WfH Client	Printer	Monitor device	-	Device information	SNMP/USB	161
WfH Client	CloudStream Device Management	IsWFHDevices	Device manufacturer, model, and	True/False	HTTPS	443

Client	Server	Functions	Request Data	Response Data	Protocol	Port
			serial number			
WfH Client	CloudStream Device Management	Upload logs	Trace logs of the service	-	HTTPS	443
WfH Client	CloudStream Device Management	Post device information	List of previously handled notifications	Notification Information	HTTPS	443

Auth Agent

Client	Server	Functions	Request Data	Response Data	Protocol	Port
Auth Agent	CloudStream Device Management	Get service URLs	-	Service URLs	HTTPS	443
Auth Agent	CloudStream Device Management	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
Auth Agent	CloudStream Device Management	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
Auth Agent	CloudStream Device Management	Get authentication request	-	User information	HTTPS	443
Auth Agent	CloudStream Device Management	Get authentication profiles	-	Authentication profile	HTTPS	443
Auth Agent	CloudStream Device Management	Post authentication result	-	User information	HTTPS	443
Auth Agent	LDAP Server	Authenticate user	User information	User information	LDAP/LDAPS	Any port

Device Monitoring Service

Client	Server	Functions	Request Data	Response Data	Protocol	Port
Device Monitoring	CloudStream Device Management	Get service URLs	-	Service URLs	HTTPS	443
Device Monitoring	CloudStream Device Management	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
Device Monitoring	CloudStream Device Management	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
Device Monitoring	CloudStream Device Management	Get polling configuration	-	Polling configuration	HTTPS	443
Device Monitoring	CloudStream Device Management	Post device information	Device information	-	HTTPS	443
Device Monitoring	Printer	Monitor device	-	Device information	SNMP/USB	161
Device Monitoring	CloudStream Device Management	IsDMServiceDevice	Device manufacturer, model, and serial number	True/False	HTTPS	443
Device Monitoring	CloudStream Device Management	Upload Logs	Trace logs of the service	-	HTTPS	443
Device Monitoring	CloudStream Device Management	Get Notifications	List of the previously handled notifications	Notification Information	HTTPS	443

External Systems

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream Device Management	OIDC ID Provider	Authenticate user	Authentication request	Authentication result	HTTPS	443
CloudStream Device Management	Custom SMTP Server	Email notification	SMTP credentials Email message Report file	-	SMTP/SMTPS	Any port
CloudStream Device Management	Amazon SES	Email notification	SMTP credentials Email message Report file	-	SMTPS	587
CloudStream Device Management	SIEM Service	SIEM integration	Transaction data	-	HTTPS	Any port

CloudStream Device Management Monitoring System

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream Device Management	CloudStream Device Management Monitoring System	Send service health metrics	Service health metrics	-	HTTPS	443
CloudStream Device Management Monitoring System	CloudStream Device Management	Check service health status	-	Service health status	HTTPS	443