Kofax Unified Client for Ricoh

Getting Started Guide

Version: 1.3.0

Date: 2024-04-08

© 2024 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Chapter 1

Kofax Unified Client for Ricoh

The Unified Client for Ricoh delivers key AutoStore and Equitrac or Output Manager embedded features and functionality direct to the Ricoh Smart Operating Panel (SOP) devices. This client application can also be configured as a Unified Client that provides an integrated user experience for both print and capture workflows direct at the device.

Unified Client for Ricoh controls access to the device, and acts as the gateway for Kofax functionality. Users must authenticate to gain access to Kofax-controlled device functions such as Print-to-Me and document capture. The embedded client uses the Device Registration Service (DRS) to configure and deploy the embedded client to single or multiple Ricoh devices that are equipped with the Smart Operation Panel (SOP), using one of the following server configurations:

1. AutoStore and Equitrac components.
2. AutoStore and Output Manager components.
3. Equitrac component only.
4. Output Manager component only.
5. AutoStore component only.

The Capture (with process and route) functionality within the client is provided via Equitrac's Scan-to-Me and/or Capture and Send capability and the Unified Client for Ricoh Smart Operation Panel application can also be expanded and configured for Kofax AutoStore capture, while the print management capability is provided by Kofax Equitrac.

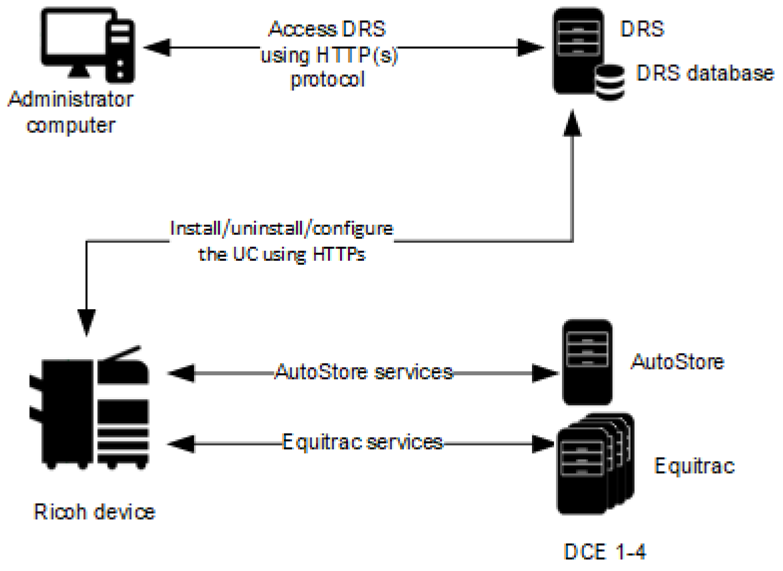
The Unified Client for Ricoh provides device authentication with a single application for Equitrac Print-to-Me and scanning into Scan-to-Me, Capture and Send with Equitrac, or AutoStore workflows. This client secures access to devices, allows user to select functions such as Print-to-Me and scanning from a common Launcher, provides card reader support, searchable billing codes at device login, and job accounting.

The Unified Client for Ricoh supports Equitrac authentication through user name and password, and card swipe with an optional PIN.

The Unified Client for Ricoh supports single sign-on (SSO) for Adaptable Authentication API (AAA) system - Ricoh infrastructure.

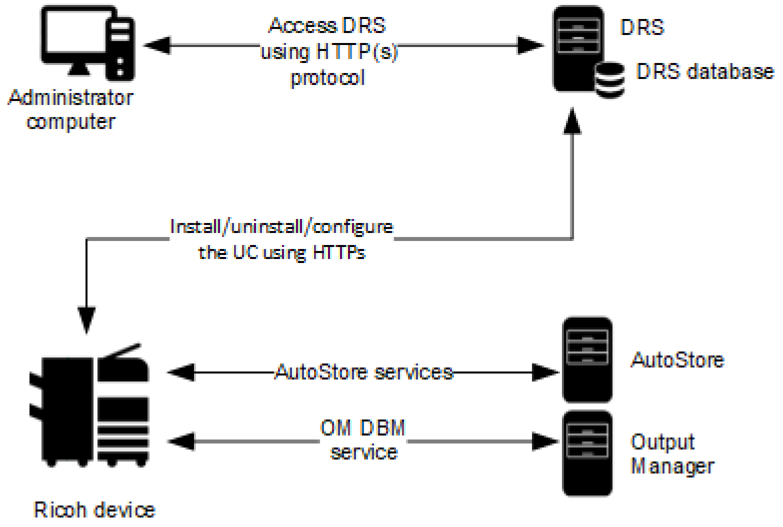
AutoStore and Equitrac

This figure illustrates a typical architecture for a system that includes the Unified Client with Equitrac and AutoStore:



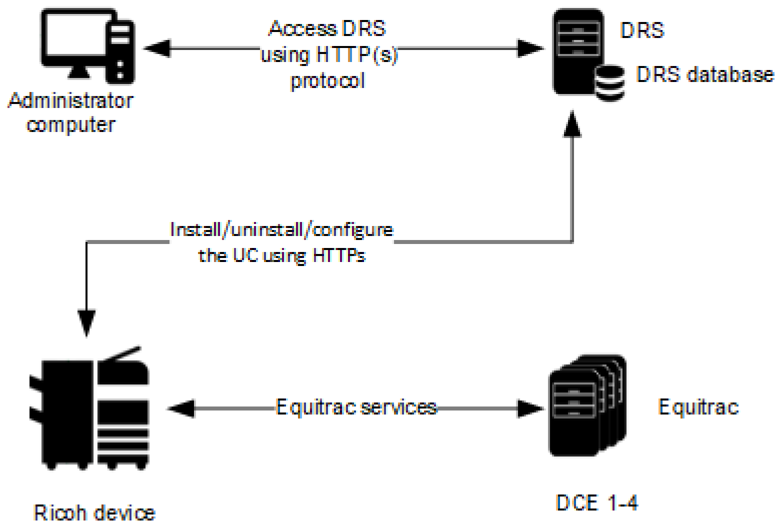
AutoStore and Output Manager

This figure illustrates a typical architecture for a system that includes the Unified Client with Output Manager and AutoStore:



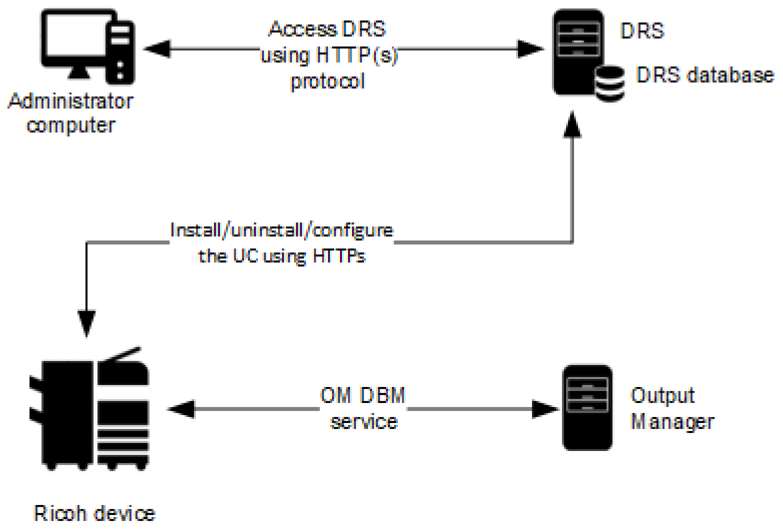
Equitrac

This figure illustrates a typical architecture for a system that includes the Unified Client with Equitrac only:



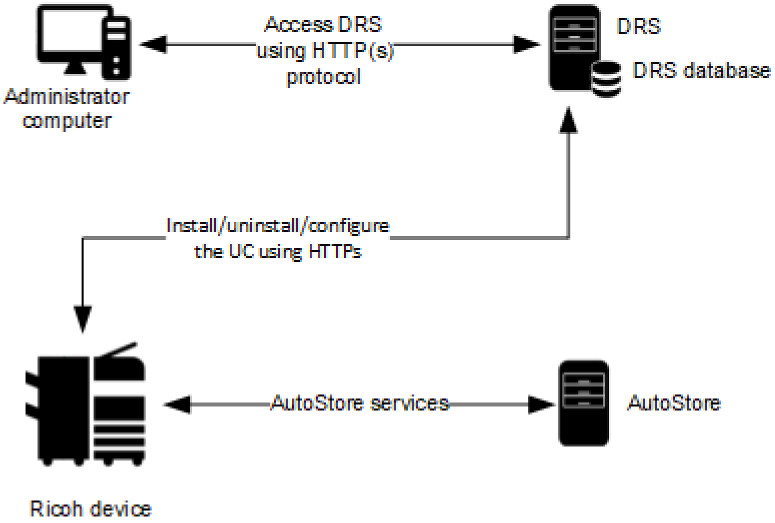
Output Manager

This figure illustrates a typical architecture for a system that includes the Unified Client with Output Manager only:


Administrator computer
Access DRS using HTTP(s) protocol
DRS
DRS database
Install/uninstall/configure the UC using HTTPs
Ricoh device
OM DBM service
Output Manager

AutoStore

This figure illustrates a typical architecture for a system that includes the Unified Client with AutoStore only:


Administrator computer
Access DRS using HTTP(s) protocol
DRS
DRS database
Install/uninstall/configure the UC using HTTPs
AutoStore services
AutoStore
Ricoh device

Chapter 2

Before you begin

Prerequisites

Before you begin, ensure that the following requirements are met.

Use the following links to view the technical specifications and minimum requirements for each of the ControlSuite components. Specific requirements depend on the number of servers in a deployment, operating systems, expected production volume, and other applications in the environment.

- AutoStore
- Equitrac
- Output Manager
- DRS
- DWS

Check	Description
□	Verify that your device is supported. For the latest list of supported Ricoh models, consult your local Ricoh representative or refer to the Kofax Supported Device search web page (https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices.
□	If you are using the Card Reader setting from DRS, on the Ricoh device, verify that the followoing system configuration setting is **On**, for both Auth On and Auth Off configurations: **Service** > **Screen Features** > **Screen Device Settings** > **Screen device always-connection Setting** When this setting is on, it prevents an issue when using AutoStore in an Auth Off configuration. This occurs when you wake a device from Sleep mode and open AutoStore, the USB card reader might not be immediately available.
□	Ensure that the device has Java application version 12.0 or later.
□	Ensure that the device supports SmartSDK 2.1 or later.
□	Verify that the server machine is a member of a domain.
□	Verify that you have Administrative access rights to Windows on the server.
□	Check that all important Windows updates are installed.
□	Verify that **Microsoft Windows Updates** is turned on while you are deploying AutoStore, which is required to install Microsoft Windows Identity Foundation (TFS).

Check	Description
□	Ensure that **Windows Identity Foundation 3.5** is installed on the server (launch **Server Manager** > **Local Server** and verify that Windows Identity Foundation 3.5 is listed under Roles and Features).
□	Verify that IE Enhanced Security Configuration is turned off for Administrators in IE Enhanced Security Configuration (to access this, go to **Server Manager** > **Local Server**).
□	Verify that you have Administrative access to the device.
□	Verify that you have supported card readers. The Ricoh device supports Equitrac USB external card readers and Ricoh-supported third-party card readers.
□	If you are using an IPv6 address, verify that your Ricoh device is a Gen 2.5 device. Refer to the Kofax Supported Device web page.

DRS and unified client communication ports

The following table provides general information on ports and protocols for the DRS server and the Unified Client for HP.

Component	Device display menu protocol	Device file transport protocol	Default communication port	Port configurable	Required device components
DRS server	HTTP, HTTPS	HTTP, HTTPS	Web server: 8753 REST-based web service: 8755 Client Server: 9000 Web client: 9000	Yes	
Unified Client for Ricoh	HTTP, HTTPS	HTTP, HTTPS	AutoStore application port: - AutoStore server: 3310 (used by Ricoh Unified Client) - AutoStore server: 3350 (used by Ricoh SOP) Output Manager application port: - http: 8068 - https: 8069 Equitrac application port: - 2939 Device port used for connections to the device: - http: 80 - https: 443 Ricoh SOP (internal device components): - 51443		The 51443 port is used by Ricoh SOP devices for collecting and configuring device information.

Supported card readers

The Unified Client for Ricoh supports the following card readers.

Kofax card readers

- Kofax Micro ST Reader
- Kofax Micro Card Reader
- Kofax Equitrac ID Card Reader

The Unified Client for Ricoh has also been tested with the following card readers.

Third-party card readers

- Baltech Micro2
- Baltech Micro
- Baltech ID Card Readers USB Gen 2 Business Connect compatible
- Elatec TWN3 KBD [09D8:0310]
- Elatec TWN4 KBD [09D8:0410]
- RFIDeas pcProx RDR-7L81AKU KBD [0C27:3BFA]
- RFIDeas pcProx RDR-80581AKU KBD [0C27:3BFA]
- RFIDeas RDR-6381 APU
- RFIDeas RDR-7581 APU
- RFIDeas RDR-6081 APU
- HID Omnikey 5427 (AU-205H)
- Inepro SCR 708 [0110/1DA6]
- Inepro Spider [0110/1DA6]

When a third-party card reader is used, then a third-party card reader license is required.

Chapter 3

Configure DRS

Use DRS to configure and deploy the unified client

This section covers all server options. Some steps might not apply to your configuration.

ⓘ

- Administrative access to the server is required. Perform these steps from the server where the installation takes place.
- If you are using Microsoft Internet Explorer, go to **Start** > **Administrative Tools** > **Server Manager** > **Local Server** > **IE Enhanced Security Configuration** and turn off Administrators.

1. If you are using Equitrac 6.3.1 and AutoStore 8.3.1, you can install Device Registration Service (DRS) within ControlSuite. If you are using Equitrac 5.6 or 5.7 and AutoStore 7 SP6, install DRS separately:
    a. Unzip the `<version_number>-DeviceRegistrationService.zip` file. This creates a new folder containing the `DeviceRegistrationService.exe` file.
    b. Right-click the file and select **Run as administrator**.
    c. Follow the instructions to install DRS.
2. Upload the Ricoh Client Package.
    a. Download the Unified Client for Ricoh SOP software package, `KofaxRicohUnifiedClient-<version>.zip`, from the Kofax Downloads Web site (https://delivery.kofax.com).
    b. Unzip the file. This creates a new folder, containing the `RicohSOP<version_number>.xml` file.
    c. Open DRS. In a Web browser, enter `http(s)://<DRSServerIP>:9000/device`, where `DRSServerIP` is the IP address of the server where you installed DRS.
    d. Select the **Files** tab.
    e. From the **Device Type** list, select **Ricoh SOP**.
    f. At the bottom of the screen, click **Upload**. Go to the `KofaxRicohUnifiedClient-<version>.zip` file, unzip it, and upload the files. You can also upload any images you want to use to customize the Welcome screen. The file type restriction is also validated, with a message listing the allowed extensions when errors appear.

ⓘ Future updates of the client configurations can be also uploaded from here.

The administrator can check build information for the specific package version and DRS decides what should be installed to the device based on the device configurations. The administrator can also install the latest version of the client, or a previous version (until that version is retired or is not supported).

After installing DRS, the uploaded files (using **Files** tab in DRS) are not part of the installer and will not be removed if you uninstall.

! You can delete cached user information and transactions on the device by uninstalling then re-installing the unified client.

3. Create the application in DRS.
   a. Select the **Applications** tab.
   b. Click the green (⊕) button at the top of the left **Applications** pane.
   c. In the **Name** field (required), enter a name for the application.
   d. In the **Application Type** list (required), select **Ricoh SOP**.
   e. In the **Server Configuration** list, select one of the following options: **AutoStore and Equitrac**, **AutoStore and Output Manager**, **Equitrac**, **Output Manager** or **AutoStore**.

      Based on the server selection, only some of the following application fields are visible.
   f. If you select **AutoStore** as part of the configuration, complete the following information:
      - In the **AutoStore Server Address** field (required), enter the IP address or hostname used by the AutoStore server.
      - In the **AutoStore Server Port** field, enter the server port used by the AutoStore server. The default value is 3310 (previously 3350).
      - In the **AutoStore Server Use TLS** field, select **True** or **False**. This setting must match your AutoStore server configuration. Verify it in the **Preference** tab of the **Ricoh SOP** component. By default, the AutoStore setting **Use TLS** is on.
      - For the **Trust Self-signed Certificate for AutoStore** option, select **True** or **False**.

      ⓘ If you are using a CA certificate, select **False**. You must use either all self-signed certificates or all CA certificates. You cannot combine the two types of certificates.
   g. If you select **Equitrac** as part of the configuration, complete the following information:
      - In the **DCE Server Address** fields (required), enter the IP address or the hostname used by the DCE Server. If your deployment contains multiple DCE servers, up to three more can be added in the remaining DCE Server fields.
      - For the **Trust Self-signed Certificate for DCE** option, select **True** or **False**.

      ⓘ If you are using a CA certificate, select **False**. You must use either all self-signed certificates or all CA certificates. You cannot combine the two types of certificates.

   h. If you select **Ouput Manager** as part of the configuration, complete the following information:

      - In the **Print Manager Address** field, enter the IP addresses or the hostnames used by the Output Manager server.
      - In the **Print Manager TLS Port** field, enter the port number used by the Output Manager server.
      - In the **Print Manager Use TLS** field, select **True** or **False**.
      - For the **Trust Self-signed Certificate for Output Manager** option, select **True** or **False**.

        > If you are using a CA certificate, select **False**. You must use either all self-signed certificates or all CA certificates. You cannot combine the two types of certificates.

   i. For the **Server Certificate Pinning** option, select **True** to bind a certificate to the server upon connection and use it to validate the trust of subsequent communications with that server.

   j. If a **Trust Self-signed Certificate** option is **False** and a **Use TLS** option is **True**, then the **Server Certificates** field appears. Select the server certificate file from the list.

      > Include all server certificate files into one zip file, with a maximum of five server certificate files. Only Base-64 encoded X.509 (.cer) certificates are supported.

   k. If you select **Equitrac** or **Ouput Manager** as part of the configuration, complete the following information:

      - For the **Bypass Button** option, select **True** to allow a user to skip authentication to use the device native functions without logging in or **False** to remove this option.
      - In the **Authentication** entry (required), select **True**.

   l. Click **Save** (💾) .

4. Add the device in DRS.

   a. Select the **Devices** tab.

   b. Click the green (⊕) button at the top left of the **Devices** pane.

   c. In the **Name** field (required), enter a name for the Ricoh device or device group that identifies it on the network.

   d. In the **Address** field (required), enter the IP address or the fully-qualified hostname of the device. When using the hostname, ensure that the server is configured properly with the DNS server to resolve the hostname.

      > For the IP address, you can enter IPv4 or IPv6 addresses depending on the configuration of your system. If you enter an IPv6 address, brackets ([ ]) are automatically added to it if missing when you exit from the field.

   e. Enter the **Username** and **Password** for the device.

   f. From the **Application** list (required), select the application you have created. The rest of the **Add Device** fields appear.

g. In the **Remote Install Password** field (required), enter the administrator password.

> ⓘ This password can be changed by the device administrator regardless of the domain credentials.

h. In the **MFP TLS (http/https)** entry, select **True** (default) or **False**. It is recommended that you use https or higher TLS settings for installation.

> ⓘ The following DRS actions only support HTTPS: **Quick Install**, **Full Install**, **Configure and Reboot**, and **Quick Configure**.

i. In the **Enable Debug Log** entry, select **True** or **False**.

j. In the **Server Connections Timeout** entry (the timeout used by DRS when making configuration and installation calls to the device such as SP modes and deployment of the client.), select a specified period of time (default is 60).

k. In the **Device Type** list (required), choose between Single-Function Printer (**SFP**), Multi-Function Printer (**MFP**) or Specific model (**MP C306/MP C406**) device.

> ⓘ This selection affects available workflow applications.

l. In the **Authentication Screen** field, select **Welcome** (default) or **Logon**.

m. In the **Card Reader Model** list, select the type of card reader for the device.

n. In the **Assign as Home Key Application** field, select **True** or **False**.

o. In the **Scan preview** entry, select **True** or **False**.

p. In the **Application Package** list (required), select an application package from this list. The selected application package is downloaded to a device by the **Install** action. List items are populated by the uploaded files specified on the **Files** tab.

q. In the **Customize Assets** field, choose select **True** or **False**. If **True** is selected, the following fields appear:

   - In the **Application Logo** list (required), select the image file. The following image types are available: JPG, JPEG, PNG or BMP.
   - In the **Welcome Screen Image** list (required), select relevant image file.
   - In the **Customize Welcome Screen Text** field, choose **True** or **False**. If **True** is selected, the **Welcome Screen Text** field appears. Enter your text.
   - In the **Customize Application Name** field, choose select **True** or **False**. If **True** is selected, the **Application Name** field appears. The default name is Kofax Unified Client. You can enter a new name, up to 60 unicode characters.

> ⓘ The information (ⓘ) icon next to the field names explains the file type, image resolution, and text length restrictions.

To upload the assets, go to the **Files** tab and select a file that conforms to the previous specifications. Once uploaded, the file appears in the list (for Application Logo and Welcome Screen Image, respectively depending on the uploaded file's size).

> ℹ Uploaded files that do not conform do not appear on the list.

r. In the **Customize Workflow Buttons** field, choose **True** or **False**. If **True** is selected, the **Workflow Application** field appears. Choose the available workflow applications for your device.

s. In the **Use Authorization Key** field, select **True** to use additional security between the DRS application and the device, to confirm that only the initial DRS instance that was used to deploy or configure the device can be used to update the configuration on the device.

> ℹ If you change this setting from **True** to **False**, you must uninstall the unified client and install it again to remove the cached DRSAuthKey on the device.

t. Click **Save** (💾) at the top of the **Add Device** pane.

5. Install the client application onto the device.

   a. From the **Select Actions** list at the top of the **Details** pane, select **Full Install**.

   > ℹ To go back to the default values for assets, you must set and resync.

   b. Click the **Run Action** icon (▶) to run the action. This may take a few minutes to complete. Once finished, a **Successfully completed** message appears in the **Action History** pane at the bottom of the screen.

Chapter 4

Additional information

Product documentation

The full product documentation set for the Unified Client for Ricoh 1.3.0 is available online at the Kofax ControlSuite 1.4.0 site. This documentation set consists of the following documentation to assist you with installing, configuring, and using the product.

- ControlSuite Clients Help, which contains help for the Unified Client for Ricoh, DRS, and other components and clients
- ControlSuite server help, which contains help for ControlSuite installation and configuration
- Release Notes
- Technical Specifications

Troubleshooting

Issue	Cause	Solution
The Unified Client fails to connect to servers by SSL handshake issue.	Device TLS settings and ControlSuite servers TLS settings might not be matched.	• Use a network capture tool to verify the cipher suites which are used by device and server for SSL handshake. • Verify that the TLS ciphers on the servers matched with the ones sent from device.
On Ricoh IM C3000 devices, if you receive the message Log data capacity is full, then the DRS installation or uninstallation is stopped.	• The installation hangs at the "Preparing device configuration" stage. • The uninstallation hangs at the "Resetting device configuration" stage.	Clear the log file.

Issue	Cause	Solution
Your device is having trouble connecting to DRS with an IPv6 address when configuring the Unified Client.	IPv6 addresses are only supported on Ricoh Gen 2.5 devices. Refer to the Kofax Supported Device web page.	If the device is not Gen 2.5, you must use IPv4 addresses.
Home key on an MFP was not enabled by Assign as home key application Device setting.	• Device configuration may not be implemented yet for a particular MFP. • Install and Reboot action was performed previously.	You can enable the Home key manually on an MFP using the following procedure to enable home key settings.
Need to manually configure SP Modes on a device.	SP Modes are normally configured by running on a device.	You can manually configure SP Modes on a device using the following procedure to configure SP mode settings. ⓘ Also check if Baseline installation is an option and if it is inadvertently left as False.
When accessing workflows, the user cannot perform scan and You do not have the privileges to use this function message appears.	SP Modes are set incorrectly.	You can manually configure SP Modes on a device using the following procedure to configure SP mode settings. You must set Admin. Authentication to Off.
Not able to log in when switching from Equitrac only (Auth On) to AutoStore only (baseline set to false).	There is no indication from DRS that the Service Provider (SP) modes are set wrong.	You must check SP modes when baseline is set to off.

Issue	Cause	Solution
Need to disable Print from USB on the MFP.	Print from USB is not tracked and no quotas or limits are applied.	You can manually disable print from USB/memory stick using the following procedure: **1.** Log in to the Web Image Monitor application (which allows users to remotely monitor and change the network configuration via web browsers as long as the target MFP is networked and has an IP address) by entering the IP address of MFP on your browser. **2.** Go to **Device Management** > **Configuration** > **Device Settings** > **System** . **3.** Go to **Media Slot Use** > **Print from Memory Storage Device** and select **Prohibit**. **4.** Select **Prohibit** for disabling print from storage devices (USB or SD card). **5.** Click **OK**.
Need to replace the DRS.	The DRS crashes and cannot be used any longer or similar.	The customers are advised to back up their DRS database after they have completed the configuration. Restoring the database will restore the saved Authorization key for each device. If this is not available, the customer must run the Uninstall command first to fully remove the RSOP client from the device and then they will be able to set the configuration again as the client will accept the new Authorization key after a new install.

Issue	Cause	Solution
Need to replace the DCE.	The DCE crashes and cannot be used any longer or similar.	If the customers have to point to a new DCE, they must go to DRS and update the list of DCEs. Pinning will be re-established with all DCEs in the new list when the new list of DCEs are sent down from DRS by using the Configure and Reboot action. The client will ensure that the same DRS is used which was initially used to set the initial list of DCEs by checking the Authorization key which will be provided by DRS in the request to change the DCEs.
• DRS fails to execute the Full Install action. Device is not reachable and requires a manual reboot to execute Full Install. • The message Device not reachable is received.	• The TLS settings are changed on the device. • The IP address or the host name is not valid or the device is currently not visible on the network.	TLS versions must match service on the Controller and service on JavaVM. Complete the following procedure: **1.** In a Web browser, enter http://<MFP IP Address> in the Address field. **2.** Click **Login** and enter your administrator User Name and Password. **3.** Change the TLS settings on JavaVM: **a.** Open the Web Image Monitor and log in. **b.** Go to **Device Management** > **Configuration** > **Extended Feature Settings** > **Administrator Tools** and change the settings. **c.** Click **Apply**. **4.** Change the TLS settings on the Controller: **a.** Open the Web Image Monitor. **b.** Go to **Device Management** > **Configuration** > **SSL/TLS** and change the settings. **c.** Click **OK**.

Issue	Cause	Solution
When running Client Installer, Please wait... Ricoh Persistence Provider message is pending (unknown error).	The optional HDD from the device is missing.	The optional HDD is required to be installed on SFP and various MFP devices (for example, SP C842DN and MP C306) in order for Kofax to be supported.
The Login button is not visible at the top right corner of the screen and the Welcome or Login screen is showing. The user is unable to login.	Pressing the Stop button at Welcome screen takes user interface into restricted mode.	Complete the following procedure: **1.** Dismiss the Welcome screen by clicking the hamburger menu and selecting Administration from the drop-down list. **2.** Click the Continue Printing button to exit access restricted mode. The Login button is now visible at the top right corner of the Ricoh panel and the user is able to login.
An error message occurs when selecting Refresh Status.	Occurs due to a missing application package.	Ensure that complete application package is uploaded.
After performing uninstallation, the device authentication settings were not reset completely in DRS.	Administrator authentication is set to ON.	Administrator authentication must be manually set to OFF to fully put the device back into factory settings.

Property files generated during action with Equitrac as print manager

Install and Reboot

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`
- `deviceconfig_to_auth_on_preinstall. properties`

Configure and Reboot

- `deviceconfig_auth_on.properties`
- `deviceconfig_home_key_on.properties`

Uninstall

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`

Install and Reboot

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`
- `deviceconfig_to_auth_on_preinstall. properties`

Configure and Reboot

- `deviceconfig_auth_on.properties`

Uninstall

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`