Deployment Guide

The following table lists dates for revisions of this document and changes associated with each revision.

<table>
<thead>
<tr>
<th>Document Revision Date</th>
<th>Revision List</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 31, 2019</td>
<td>Updated with installation instructions for ControlSuite environments.</td>
</tr>
<tr>
<td>February 20, 2019</td>
<td>Updated to reflect new device support.</td>
</tr>
<tr>
<td>October 9, 2018</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Symbols Used In This Guide

The following symbols are used in the margins of this guide:

- The accompanying text provides cross-reference links, tips, or general information that can add to your understanding of a topic.

- The accompanying text provides key information about a step or action that might produce unexpected results if not followed precisely.

- Read the accompanying text carefully. This text can help you avoid making errors that might negatively affect program behavior.

© 2019 Kofax All rights reserved.

All rights to this document, domestic and international, are reserved by Kofax. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission of Kofax.

Trademarks

AutoStore, Equitrac, Output Manager, and Unified Client are either registered trademarks or trademarks of Kofax in the United States and/or other countries.

All other brands and their products are trademarks or registered trademarks of their respective holders, and should be noted as such.
Contents

Ricoh PCC 5.1 Deployment Guide for Equitrac and AutoStore............ 5
  Overview of the Ricoh PCC 5.1 for AutoStore and Equitrac Deployment................................................. 5
  AutoStore and Equitrac Solution Overview.......................................................................................... 6
  Deploying Ricoh PCC 5.1 with AutoStore and Equitrac - Workflow Outline............................................. 6
  Requirements........................................................................................................................................ 7
  Supported Languages.......................................................................................................................... 7

Prepare for Deployment....................................................................................................................... 8
  Verify that your device is supported................................................................................................... 8
  Verify prerequisites............................................................................................................................ 8
  Get installer packages....................................................................................................................... 10

Quick Start for Advanced Users......................................................................................................... 11
  Install and Configure the AutoStore Server....................................................................................... 11
  Install Equitrac................................................................................................................................... 12
  Install ControlSuite............................................................................................................................. 13
  Configure Device Registration Service............................................................................................... 18
  Set Up a Ricoh PCC 5.1 MFP................................................................................................................ 28
  Set Up Your First AutoStore Capture Workflow................................................................................. 30
  Set Up Your First Print Workflow........................................................................................................ 33

Process Instructions............................................................................................................................ 34
  Configuring Equitrac to Use with Ricoh PCC 5.1............................................................................... 34
  Using Ricoh PCC 5.1............................................................................................................................ 38
  Ricoh PCC 5.1 Device Settings............................................................................................................. 49

Appendix: Additional Configuration Instructions.................................................................................. 66
Ricoh PCC 5.1 Deployment Guide for Equitrac and AutoStore

Overview of the Ricoh PCC 5.1 for AutoStore and Equitrac Deployment

The Ricoh PCC 5.1 embedded application for AutoStore and Equitrac delivers key AutoStore and Equitrac 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.

Ricoh PCC 5.1 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 Follow-You Printing 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). 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 Ricoh PCC 5.1 application can also be expanded and configured for KofaxAutoStore capture, while the print management capability is provided by Kofax Equitrac.

The following figure illustrates a typical architecture for a system that includes the Ricoh PCC 5.1 for AutoStore and Equitrac:
The Ricoh PCC 5.1 provides device authentication with a single application for Equitrac Follow-You Printing 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 Follow-You Printing and scanning from a common Launcher, provides card reader support, searchable billing codes at device login, and job accounting.

The Ricoh PCC 5.1 supports Equitrac authentication through user name and password, and card swipe with an optional PIN.

The Ricoh PCC 5.1 supports single sign-on (SSO) for Adaptable Authentication API (AAA) system - Ricoh infrastructure.

**AutoStore and Equitrac Solution Overview**

Ricoh PCC 5.1 provides a unified client for capture and print management functionality on specific Ricoh-manufactured Single-Function Printers (SFPs) and Multi-Function Printers (MFPs). When deployed to the MFP, Ricoh PCC 5.1 controls access to the SFP and MFP.

This document will walk you through a clean installation procedure. Follow the steps provided here to be able to have an AutoStore Send to Folder capture and Equitrac Office/Express 5.6 and 5.7 Follow-You Printing workflows configured on your Ricoh SOP SFP and MFP device.

**Note:** If you plan to install Single-Function Printers (SFPs) in DRS that do not support the scan function, you must first create two separate applications:

1. Equitrac environment that will be dedicated for Single-Function Printer (SFP) devices.
2. AutoStore and Equitrac environment that will be dedicated for Multi-Function Printer (MFP) devices.

**Deploying Ricoh PCC 5.1 with AutoStore and Equitrac - Workflow Outline**

1. **Prepare for deployment**
   a. Verify that your device is supported
   b. Verify prerequisites
   c. Get installer packages (AutoStore, Equitrac Office/Express 5.6 or 5.7 with the latest hotfixes, DRS 7.13 and Ricoh PCC 5.1 client package)
2. Install the AutoStore server
3. Install Equitrac Office/Express 5.6 or 5.7 with the latest hotfixes
4. Configure the Ricoh MFP
   a. Configure the device certificate on the device
   b. Ensure that TLS is enabled
   c. Verify that previous applications are cleared
5. Install and Setup Device Registration Service (DRS)
   a. Upload Ricoh PCC 5.1 client package into DRS
   b. Create and add application in DRS
   c. Add and configure the MFP device
   d. Install the Ricoh device using DRS in AutoStore and Equitrac deployment
6. Execute final actions
   a. Select and run action (Quick Install, Full Install, Install and Reboot, Configure and Reboot, Sync Assets, Sync Workflow Buttons, Uninstall, Reboot, Get device settings, and Set device settings)
   b. Locate the auto-added device and configure it in Equitrac System Manager.
7. Create your first AutoStore workflow and verify installation
   a. License AutoStore
   b. Configure Send to Folder workflow
   c. Verify installation
8. Create your first Equitrac workflow and verify installation
   a. License Equitrac
   b. Configure Follow-You Printing workflow
   c. Verify installation

Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equitrac</td>
<td>Version 5.6 or 5.7 or later with all available hotfixes installed.</td>
</tr>
<tr>
<td>AutoStore</td>
<td>Version 7 SP5 or later.</td>
</tr>
<tr>
<td>DRS</td>
<td>Version 7.12 or later.</td>
</tr>
<tr>
<td>Ricoh SOP firmware</td>
<td>Ricoh firmware M2a_System version (Smart Operation Panel firmware) v1.26 or later.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> IM series devices may require M2a_System version 1.06.1 or later.</td>
</tr>
</tbody>
</table>

Supported Languages

The Ricoh PCC 5.1 interface includes support for the languages listed below. The language is selected automatically based on the MFP language. If the MFP language is not available, English is used by default.

- Simplified Chinese
- Finnish
- Norwegian
Prepare for Deployment

Verify that your device is supported

For the latest list of supported Ricoh models, consult your local Ricoh representative or refer to Kofax Supported Device Search webpage (https://www.kofax.com/imagingsupporteddevices).

Verify prerequisites

DOUBLE-CHECK BEFORE YOU START: Before you begin, ensure that the following requirements are met for deploying AutoStore and Equitrac.

If deploying on separate servers, refer to the individual AutoStore and Equitrac server requirements.

**Note:** Before installing Equitrac Office/Express 5.6 or 5.7 and Device Registration Service (DRS) 7.12 ensure that the machine you plan to use meets the operating requirements outlined below. Observe that you MUST have a 64-bit version of operating system.

**Note:** For Windows Servers 2008, 2008 R2, 2012, 2012 R2 and 2016, make sure the server is up to date with the latest service packs, or manually download and install the latest version of Windows Installer from Microsoft. Windows Installer 4.5 is required to install Equitrac 5.7.

**Note:** Print tracking from a memory storage device (USB flash memory devices and SD cards) is not available in this release.

<table>
<thead>
<tr>
<th>Check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>Verify that the server machine is a member of a <strong>domain</strong>.</td>
</tr>
<tr>
<td>☑️</td>
<td>Ensure that the following <strong>hardware</strong> requirements are met:</td>
</tr>
<tr>
<td></td>
<td>• 8 GB of <strong>physical memory</strong> available</td>
</tr>
<tr>
<td>Check</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| • 5 GB of hard disk space available (including SQL server and prerequisites)  
• The CPU is 4 x 2 GHz or greater | 32-bit operating systems are not supported. |
| □ | Ensure that you have Microsoft SQL Server 2008/2008 Express SP3 or later installed. |
| □ | Check that the operating system is one of the following:  
• Windows Server 2016 (x64 with IIS 10.0 and .NET 4.6)  
• Windows Server 2012 R2 (x64 with IIS 8.0 and .NET 4.5)  
• Windows Server 2012 (x64 with IIS 8.0 and .NET 4.5)  
• Windows Server 2008 (x64 with IIS 7.0 and .NET 4.5)  
• Windows Server 2008 R2 (x64 with IIS 7.5 and .NET 4.5) |
| □ | 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. This is necessary for the successful installation of Microsoft Windows Identity Foundation (TFS). |
| □ | Ensure that .NET Framework 3.5 is installed on the server (to verify it, launch Server Manager > select Local Server > verify that .NET Framework 3.5 is listed under Roles and Features). If it is missing, it will be installed as part of the AutoStore installation process. |
| □ | Ensure that Windows Identity Foundation 3.5 is installed on the server (to verify it, launch Server Manager > select Local Server > verify that Windows Identity Foundation 3.5 is listed under Roles and Features). |
| □ | Allow incoming firewall exceptions for the following ports:  
• 80: Device port used for HTTP connections  
• 443: Device port used for HTTPS connections to the device  
• 587: SMTP Email server port used if TLS is enabled  
• 2939: TLS is always on for Equitrac and the default port setting of 2939 is not configurable in DRS  
• 8753: The default port for the Device Registration Service Web Service  
• 8755: The default port for the Device Registration Service REST-based Web Service  
• 9000: The port used by the server to communicate with the web client. This port is specified in the Service settings in the DRS Device Configuration Manager  
• 9100: The default device port used for outgoing print stream  
• 51443: Device port used for configuration |
<table>
<thead>
<tr>
<th>Check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>and <strong>outgoing firewall exceptions</strong> for ports 3310, 8753, 49629, 49630, 50083. (Note that port 3310 (previously 3350) is configurable and you should update your firewall accordingly).</td>
</tr>
<tr>
<td></td>
<td>Verify that IE Enhanced Security Configuration is turned OFF for Administrators in <strong>IE Enhanced Security Configuration</strong> (to access this, go to <strong>Server Manager &gt; Local Server</strong>).</td>
</tr>
<tr>
<td></td>
<td>Check that you have <strong>all required components downloaded</strong> and within easy reach (components and download locations are listed in the section below).</td>
</tr>
<tr>
<td></td>
<td>If you are planning to use any AutoStore <strong>Route component</strong> that requires <strong>client software</strong>, ensure that this software is <strong>installed</strong> on your server machine before starting deployment.</td>
</tr>
<tr>
<td></td>
<td>Verify that you have <strong>Administrative access</strong> to the <strong>device</strong>.</td>
</tr>
<tr>
<td></td>
<td>Verify that you have supported card readers. The Ricoh PCC 5.1 supports Equitrac USB external card readers and Ricoh-supported third-party card readers. For the current list of Equitrac supported card formats, refer to the <a href="https://www.kofax.com/card-reader-product-specs">https://www.kofax.com/card-reader-product-specs</a> page on the Kofax web site.</td>
</tr>
</tbody>
</table>

### Get installer packages

The following components are required for installing the Ricoh PCC 5.1 software in an Equitrac Office/Express 5.6 or 5.7 and AutoStore 7 deployment:

- **Equitrac Office/Express 5.6** (build 5.6.25.5109 or later) or **Equitrac Office/Express 5.7** (build 28.7293 or later) with latest hotfixes available for Windows Server platforms installed: Log in to the [Equitrac Partner Portal](https://partners.equitrac.com/) and download the EO5.6.zip/EE5.6.zip or EO5.7a.zip/EE5.7a.zip files under TECH SUPPORT > Software Downloads > Equitrac Express or Equitrac Office. Download all available hotfixes under TECH SUPPORT > Hot Fixes. After that, download Equitrac Office/Express 5.6 or 5.7 related documentation under TECH SUPPORT.

- **AutoStore 7 SP5** or later: Log in to the [Web Licensing Portal](https://weblicense.nsius.com/) and download the executable AutoStore 7 SP5 or later as well as available documentation under Software Download and Documents > AutoStore 7.

- **Device Registration Service**:
  - Log in to the [Equitrac Partner Portal](https://partners.equitrac.com/) and download the executable DRS file (<version_number>-DeviceRegistrationService.zip or later) as well as available documentation under TECH SUPPORT > Software Downloads > Device Registration Service (DRS) > DRS 7.13 -OR-
  - Log in to the [Web Licensing Portal](https://weblicense.nsius.com/) and under Software Download and Documents, select the product Device Registration Service (DRS). Download the executable DRS file (<version_number>-DeviceRegistrationService.zip or later) as well as available documentation.

- **Ricoh Client Packages**:
  - Log in to the [Web Licensing Portal](https://weblicense.nsius.com/) and under Software Download and Documents > Device Registration Service, select the product Ricoh Unified Client. Download
the client zip package (<version_number>-RicohSOPClient_<version_number>.zip) as well as available hotfixes and documentation.

- Log in to the Equitrac Partner Portal (https://partners.equitrac.com/) and download the executable PCC 5.1 zip file as well as available documentation and hotfixes under TECH SUPPORT > Software Downloads > PCC5.

The following components are required for installing the Ricoh PCC 5.1 software in an Equitrac 6.0 and AutoStore 8 (ControlSuite) deployment:

- **ControlSuite software**: Log into your account, or create an account, at the Kofax Customer Support portal (https://kofaximaging.custhelp.com/). You can access the Entitlement Portal to download ControlSuite, based on the entitlements assigned to you after purchase. Check the Fulfillment Letter you received after purchase for additional information.

- **Ricoh Client Packages**:
  - Log in to the Web Licensing Portal (https://weblicense.nsius.com/) and under Software Download and Documents > Device Registration Service, select the product Ricoh Unified Client. Download the client zip package (<version_number>-RicohSOPClient_<version_number>.zip) as well as available hotfixes and documentation.
  - Log in to the Equitrac Partner Portal (https://partners.equitrac.com/) and download the executable PCC 5.1 zip file as well as available documentation and hotfixes under TECH SUPPORT > Software Downloads > PCC5.

It is recommended to dedicate a folder to all of your downloads for quick and easy access.

**Quick Start for Advanced Users**

For advanced users who have experience setting up the Ricoh solution, the following process acts as an overview of the fundamental steps required to install Ricoh SOP in an Equitrac and AutoStore environment.

- If you are installing Equitrac 5.6 or 5.7 and AutoStore 7.0, continue to Install and Configure the AutoStore Server on page 11 and Install Equitrac on page 12.
- If you are installing Equitrac 6.0 and AutoStore 8.0 in a ControlSuite environment, continue to Install ControlSuite.

**Install and Configure the AutoStore Server**

Once you have verified that all prerequisites are met and all necessary downloads are available, you can start deploying the package. Start by installing the AutoStore server. Follow the component installation order described in this document.

Add the Ricoh SOP component to an AutoStore workflow to provide capture functionality for Ricoh devices with the Ricoh PCC 5.1. When you create the DRS application, specify the AutoStore server address as well as the port number specified on the Preferences tab of the AutoStore component configuration.

For more details about configuring the Ricoh SOP component in AutoStore, refer to the component help in AutoStore Process Designer.

If you are installing AutoStore 8.0 in a ControlSuite environment, continue to Install ControlSuite.

**Install AutoStore**

DOUBLE-CHECK BEFORE YOU START: Before running the AutoStore installer, ensure that you have the latest system updates on your machine and that Automatic Windows Updates are turned ON.
For more information on how to install AutoStore, see the *Kofax AutoStore Installation Guide*.

**Install Equitrac**

**Install the Equitrac server**

In this document, file names are provided for both Equitrac Office and Equitrac Express. To set up the functionality described in this guide, you can choose to select either - as long as you are consistent in your choice throughout the process.

Once you have verified that all prerequisites are met and all necessary downloads are available, you can start deploying the package.

For detailed information about installing Equitrac server, see the *Equitrac Office/Express Administration Guide* and *Equitrac Office and Express Installation Guide*.

**CAS Offline Operation Through DCE Caching**

If the MFP loses its connection to the DCE server, it enters into "offline" mode. At this point, the device can still authenticate user credentials against its own internal cache, if enabled. Users whose credentials match a previously cached set are granted device access; if the credentials do not match, the users are denied access. In offline mode, card swipe capabilities may not function.

To enable Login caching for offline mode, do the following:

1. Open System Manager and navigate to **Configuration > Security and authentication > User authentication**. The User Authentication configuration dialog opens.

   ![Cas Offline Behavior](image)

2. In the **CAS offline behavior** section, select the **Login caching** from the **DCE servers** drop-down list.
   - **Disabled**: PCC follows offline behavior settings; the regular rules for cached only and allow all apply.
   - **Enabled**: PCC attempts to authenticate users with data cached on the DCE.

   DCE login caching determines whether a user login is accepted or denied when CAS is offline. If DCE caching is disabled when CAS is offline, then users cannot login. If DCE caching is enabled when CAS is offline, then DCE allows users to login only if they had previously logged in when CAS was online.

   For example, if DCE caching is enabled, and User1 authenticated while CAS was online, but User2 did not, then if CAS goes offline, User1 can still login, but User2 cannot login until CAS comes online again.

   Once CAS is back online, then User2 can login, and continue to login even if CAS goes offline again.

   **Note**: Account limits are not enforced, and Billing Codes are not validated when DCE is operating without a connection to CAS.

3. Select how DRE servers handle print jobs when CAS is offline.
   - **Auto select**: If account limits are enforced, then the **Do not print** option is used. If account limits are not enforced, then the **Print, charge accounts later** option is used.
• **Do not print:** Users cannot print, and must wait until CAS is back online in order to print.
• **Print, charge accounts later:** Users can print, and then the print job is charged to their account when CAS is back online.

### Install the Equitrac hotfixes

After installing the Equitrac server, install the latest hotfixes you have downloaded from the Partner Portal (in [http://partners.equitrac.com](http://partners.equitrac.com) under TECH SUPPORT > Hot Fixes > Equitrac Office or Equitrac Express):

- Equitrac Office / Express 5.6 with latest hotfixes and EQ56-HF-334058-DCE or later, EQ-HF-321542-SysMgr or later and EQ56-HF-330045-CAS
- Equitrac Office / Express 5.7 or later and EQ-HF-330046-CAS or later

⚠ **Important:** The Core Accounting Server (CAS) hotfix must be installed first. After that, proceed in any order you wish by following the instructions in the hotfix release notes to complete the installation.

### Install ControlSuite

Use the following steps as a guide for installing, licensing, and configuring ControlSuite for your Ricoh deployment. Depending on your environment, some details or steps might vary.

1. Download the installer package (Web Installer or Offline Installer) and run the InstallAssistant application.
2. On the **Welcome** page, click **Get Started**.
3. A Questionnaire page opens asking **Do you want to use the Install Assistant Wizard or manually configure the server?**. Select **Use the Install Assistant Wizard (recommended)** and click **Next**.
4. When asked **What software do you want to install on this server?**, select **ControlSuite** and click **Next**.
5. When asked **Are you installing ControlSuite in a production environment or do you want to build a demo or POC server?**, select **I am building a ControlSuite production environment** and click **Next**.
6. When asked **Do you want to install Equitrac print management capabilities on this server?**, select one of the following options and click **Next**:
   - **Yes, this will be my primary Equitrac Core Accounting Server (CAS)** - Select this option to install the Equitrac core configuration, authentication, and accounting features.
   - **Yes, this server will be a secondary CAS or support print management capabilities** - Select this option if you want to use this as a secondary server.
   - **No, this server will host Equitrac print management capabilities** - Select this option if you already have a primary Equitrac server, but want to add other print capabilities to this server.
7. When asked **What additional Equitrac print management capabilities will this server support?**, select any or all of the following options and click **Next**:
   - **Device Monitoring (DME)**
   - **Print Server (DRE)**
   - **Basic Scanning (Capture & Send)**
   - **MFP Device Support**
   - **Web-based System Manager**
   - **Windows Tools** - This installs the Equitrac Windows System Manager for print driver support.
   - **Reporting/Secondary CAS Server** - This is only available when selecting the secondary CAS option.
8. When asked **Will this server be used to support AutoStore document and image capture?**, select one of the following options and click **Next**:
   - **Yes, this will be my primary AutoStore document and image capture server**
• Yes, the server will support AutoStore document and image capture but will be a secondary server

9. When asked What additional document image and capture capabilities will this server support?, select any of the following options and click Next:
   • Capture from MFP Devices
   • Capture from desktop, web and all other non-MFP sources
   • Document Transformation

10. When asked Will this server be used to support Output Management?, select No, this server will not be used to support Output Management capabilities and click Next.

11. When asked Will this server be used to support mobile devices?, select Yes or No and click Next.

12. When asked Which of the following ControlSuite shared services or tools would you like to install on this server?, select any or all of the following options and click Next:
   • License Server - This is required on at least one ControlSuite server to enable and enforce licensed entitlements.
   • Security Framework - This is required on at least one ControlSuite server to broker communication between ControlSuite components.
   • Device Registration - This option installs the Device Registration Service. This is required to register and configure MFP devices and to initialize and configure Mobile on MFPs.
   • Device Web Service (DWS) - This is required to support web-based MFP devices.

13. When asked Do you want to install ControlSuite Device Control Service?, select the option for Equitrac or No, and click Next.

14. A Summary page opens displaying the components to be installed and deployed in an Equitrac production environment. The components are grouped into their respective functionality. For example, ControlSuite contains Security Framework and Licensing, and Equitrac contains the required print management components. Click Next to continue.

   Click the Advanced link if you want to modify the components to be installed. At this point you can select additional components, but the previously selected components cannot be updated or modified. In order to modify pre-selected components, you need to go back and change your selection through the questionnaire. After any changes have been made click Save and Next to continue.

15. A Summary page opens with the Installation location field. The default location is C:\Program Files, or you can click Browse to select a different location. Click Next to continue.

   You can select the Force download of latest installers option to verify that the latest software is currently installed on your system. This is not required, and will increase the installation time.

16. A Prerequisites page opens displaying the status of the system requirements needed to install and run the selected components.
   • A green check mark beside the feature indicates that the requirements have been met.
   • A red ‘X’ means that a particular feature does not meet the minimum requirement and must be installed or updated before the installation can continue. Click the top level feature to show the list of required features in order to find what needs to be fixed. If available, click the link beside the software that needs to be installed. When selected, the website with the required software opens and you can download and install the required component.
   • A yellow caution means that the minimum requirements are met, but does not meet the preferred requirements to run with optimum results.
17. The Results page opens displaying that the installation was successful. Click Finish to continue.
    Optionally select the Open Configuration Assistant option to immediately configure ControlSuite. Clear this
    option if you want to only install ControlSuite and configure it at another time.

    Note: Do not restart the server until ControlSuite is configured.

Licensing ControlSuite

1. From the Configuration Assistant Licensing page, click the Open Kofax Customer Portal link to
    get access to the Kofax Entitlement Portal. Alternatively, open a web browser and enter https://
    kofaximaging.custhelp.com to access the Kofax Customer Portal.

2. On the Kofax Customer Portal, do the following:
   a) Log in with your existing account credentials, or create an new account if needed. If creating a new
      account, follow the instructions on the Customer Portal.
   b) The Product Registration/Activation List page opens. If not, click the Registration link.
   c) Click ControlSuite on the left navigation menu.
   d) Click the Entitlement Portal link. Returning users are automatically taken to the Kofax Entitlement
      Portal.
   e) New users click Yes when asked if they are the end user.
   f) Enter the Entitlement ID provided in the Fulfillment Letter.
   g) Read and accept the End User License Agreement.
   h) Click Claim Entitlement.
   i) Click Confirm on the Confirm Organization Information pop-up window. You can edit the fields if
      needed.
   j) Click OK on the Entitlement Claimed pop-up window to be taken to the Kofax Entitlement Portal.

3. Once logged into the Kofax Entitlement Portal click Create License Server under License Servers on the
   left hand navigation menu.

4. On the License Server dialog, do the following to create a New License Server:
   a) Enter the license server Name.
   b) Select ETHERNET from the Type drop-down list. ETHERNET is used with a physical computer or a
      VM with a fixed MAC address that does not change.
   c) Enter the License server ID in the ID field. This is the ID created in the Configuration Assistant. You
      can click the Copy icon on the Licenses page and paste it in this field.
   d) Click Save.

5. A View Server page opens displaying that the server was successfully created. Select Map Entitlements
   from the Action drop-down menu.

6. When the Map Entitlements page opens, select the appropriate license and enter the quantity of
   entitlements you want to allocate to your License server and click Save.
   - The list displays the product license type, the quantity of entitlements for the license, its activation ID
     and expiration date.

7. Once the entitlements are successfully mapped to your License server, log out of the Entitlement Portal.

8. Return to the Configuration Assistant to refresh the licences.

9. The assigned licenses are listed in the Feature column.
Licensing AutoStore

AutoStore has a special licensing schema in which you need to proceed server by server and distribute available licenses to every instance. The Licensing AutoStore page is only visible if you have AutoStore on the server you are running the Configuration Assistant.

Verify that the AutoStore quantities you entered in the Entitlement portal have transferred to the Licenses table on the View Server page.

1. Ensure that you are logged into an AutoStore server within your deployment.
2. Launch the Configuration Assistant and go to the Licensing tab.
3. Click Refresh Licenses then select Update license online and click Apply.
4. The Refresh Licenses window displays progress. After successful completion, select the AutoStore Licensing tab.
   The AutoStore Licensing page shows all AutoStore licenses that you have purchased broken down by type (such as User, Capture and Processing Licenses).

<table>
<thead>
<tr>
<th>License</th>
<th>The value of the license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>The total purchased number of a license</td>
</tr>
<tr>
<td>Assigned to other server(s)</td>
<td>Licenses already in use by other AutoStore server instances. If this is the first time that you are assigning AutoStore licenses this number is zero.</td>
</tr>
<tr>
<td>Assign to this server</td>
<td>License value to be assigned to this server</td>
</tr>
</tbody>
</table>

5. Use the slider or type the desired license number directly into the Assign to this server box.
6. Click Next. After the license assignment has completed successfully, click Close.
   You have finished distributing licenses to the AutoStore server instance.
7. Repeat the above steps for all AutoStore server instances in your deployment.

Configure ControlSuite

1. After installing ControlSuite, launch the Configuration Assistant.
2. On the Welcome page, click Get Started.
3. A Databases page opens displaying the installed component database instances.
   The green check mark beside the component indicates that the database is configured correctly. The red warning means that a particular configuration setting is not valid, and the database information must be updated before the configuration can continue. When the databases are validated, click Next to continue.
   Click the edit icon if you need to modify the database.

   Note: It is recommended that a new database is created when installing Equitrac 6.0 on a server with an existing Equitrac database. Although direct upgrades from earlier versions of Equitrac to version 6.0 is not supported, Configuration Assistant may use the existing database and automatically upgrade it as required.

   A Running Database Scripts window opens to locate and connect to the selected databases. If successful, there should be a green check-mark beside each item. Close the database script window when done. A red ‘x’ indicates that a the database was not setup properly.
4. A Certificate Management page opens displaying the list of certificates associated with each component.
   a) Select the check box next to the component and select Generate Self-Signed or Import Certificate from the Select Action drop-down menu. Alternatively, click the + icon to generate a self-signed certificate, or click the Open file icon to import a certificate.
• **Generate Self-Signed** - A pop-up opens where you can provide Friendly name and Expire date for the certificate. If you select the Save to file check box, enter a Password and File path to where to save the certificate, and click OK to continue.

  A Generate Certificate window opens to create the selected certificates. If successful, there should be a green check-mark beside each item. Close the generate certificate window when done.

• **Import Certificate** - A pop-up opens where you can select a certificate Filename and Password, and click OK. Alternatively, click the Browse button to open the location of stored certificates and open the desired file. Click OK to continue.

b) Click Next. A Binding Ports window opens updating the IIS certificates. If successful, there should be a green check-mark beside each item. Close the binding ports window when done.

c) Click Next to continue.

5. A **Core Services** page opens with a list of the installed core services, along with their service credentials, startup type and current status.

• Click the Actions icon beside the Distributed Database Service (DDB) and select Configure if you want to edit its default settings. You can edit the ports used and the data folder and log file locations. Click OK to save the changes or Cancel to leave the defaults. By default this service is not started and it cannot be manually started. The DDB service will start automatically once the security framework is configured.

• Click the Actions icon beside the Licensing Service and select Configure if you want to change the port used. Select Start to start the licensing service if it not already running.

• Click Next.

6. An **Authentication & Security** page opens. The information displayed on this page depends on the installed Security Framework components.

If Security Framework components AA+SSDS+DDB are installed, you can Create Security Admin User credentials for the security admin to have access to configure ControlSuite security registrations, or you can Connect to an Existing Server. These credentials are created when you first install a security framework node, and will be required later.

• If you create an Admin User, enter the Security Admin Credentials Username and Password and click Apply, and then click Next to continue.

  **Note:** The Username must be in the form of domain\username. However, the domain is only utilized for ControlSuite, and is not associated with any AD Domain.

• If you select the Connect to an Existing Server check box, enter the Security Admin Credentials Username and Password associated with that server and click Login and then click Next to continue.

• You can click the Edit icon beside the Host or Port fields to change its defaults.

  An Initializing Security Framework window opens to update the configuration and register the database. If successful, there should be a green check-mark beside each item. Close the security framework window when done.

7. A **CS Enrollment** page opens where you enroll services into the Security Framework.

• Select all the services that need to be enrolled. By default all servers need to be enrolled. Choose Enroll from the Choose drop-down list. Alternatively, you can select Enroll from the Action option to enroll one or more services at a time. You can also Unenroll and Validate the services from the Action option.

• An Enrolling pop-up shows the enrolling status. Close the enrolling window when done, and click Next.

8. A **Services** page opens with a list of the installed services, along with their service credentials, startup type and current status.
If a service cannot run as LocalSystem, select **Credentials** under the **Actions** icon for that service, and supply a valid service account and password, and then click **Test credentials** and **OK** to continue. Once all the credentials have been provided, start all the services, and click **Next**.

**Note:** Equitrac services must be configured to run under user credentials not LocalSystem before starting them. If the host server is restarted before Equitrac services are configured with user credentials, the Device Monitoring Service and SLP Service start automatically after reboot with invalid Service Credentials. If this happens, stop these services and configure them with a valid service account and password, and then restart the services.

9. A **Licensing** page opens displaying the License Server location and Server ID.

   a) If you want to change the License Server location, click the **Edit** icon beside the Server location field to open the **Change License Server Location** window.

   • Confirm the License Server location is correct. Optionally, you can change the default License Server location.

   • Click the **Preview** button to auto-create the **License server ID**. The License Server ID is used to manage your licenses on the Customer Portal. Any licensed features will populate the list.

   • Click **Apply**.

   An **Apply licenses** window opens to initialize and update the product licenses. If successful, there should be a green check-mark beside each item. Close the window when done.

   b) Click the **Copy** icon on the right of the Server ID to copy this ID to the clipboard. The License Server ID is used to register the server and manage your licenses on the Customer Portal.

   c) Click the **Open Customer Portal** link to go to the Customer Portal. Select to login With User Name, and then enter your user credentials. Alternatively, open a web browser and enter **https://kofaximaging.custhelp.com** to access the Customer Portal.

   d) Once the licenses have been assigned to this License Server, click **Refresh Licenses** to update the license.

   • Select **Update license online** and click **Apply** to communicate with the License Server to synchronize the changes or updates to the licenses on Customer portal.

   • Select **This License Server has no access to Internet** to update the license file from the binary downloaded from the Customer Portal, then click **Download License Request**. Open the License File and click **Apply**.

10. A **System Administrators** page opens displaying the configured administrators. Click **Next** to continue. You can click the **Edit** icon beside administrator if you want to modify its settings.

11. A **Launch Applications** page opens where you can launch any of the installed ControlSuite applications directly from the Configuration Assistant. Alternatively, you can use the Start menu to navigate to the appropriate ControlSuite product.

12. Click **Close** to exit the Configuration Assistant.

**Configure Device Registration Service**

Follow these steps to perform an installation of Ricoh PCC 5.1.

**Prepare Device Registration Service for use with AutoStore and Equitrac deployment**

**BEFORE YOU START:** Administrative access to the server is required. All steps outlined are performed from the server where the installation takes place. In Start menu under **Administrative Tools** go to **Server Manager > Local Server > IE Enhanced Security Configuration** > turn off **Administrators**.

1. Install DRS.
a) Download and unzip the **DeviceRegistrationService.zip**. This creates a new folder containing the **DeviceRegistrationService.exe**.

b) Select the installation executable file, right-click it and choose **Run as administrator**.

c) Run the **DeviceRegistrationService.exe** file, and follow the instructions to install DRS.

**Note:** If you installed Equitrac 6.0 and AutoStore 8.0 within ControlSuite, there is an option to install DRS with the ControlSuite installer.

### 2. Upload Ricoh Client Package.

a) Download the most recent version of Ricoh PCC 5.1 from:

- **Equitrac Partner Portal** ([https://partners.equitrac.com/](https://partners.equitrac.com/)): Once the archive downloads, extract `<version_number>-RicohSOPClient_<version_number>.zip`.

b) Upload the Ricoh client package file to DRS: Open a web browser and enter `http://<DRSServerIP>:9000/device`, where **DRSServerIP** is the IP address of the server where you installed DRS. The **Device Registration Service** screen opens:

c) Select the **Files** tab.

d) From the **Device Type** drop-down list, select **Ricoh SOP**.

e) At the bottom of the screen, click the **Upload** button. This opens a file explorer, where you can navigate to the `<version_number>-RicohSOPClient_<version_number>.zip`, unzip and upload the files (the archive also contains the `RicohSOP<version_number>.xml` file). You can also upload here all images used for customizing the Welcome screen. The file type restriction is also validated here, with message listing the allowed extensions shown upon errors.

**Note:** 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 MFP based on the device configurations. The Administrator can additionally also install the latest version of the client, or a previous version (until that version is retired or is not supported).

**Note:** After installing DRS, the uploaded files (using Files tab in DRS) are not part of the installer and will not be removed with the uninstallation.

3. **Create the application in DRS.**
   a) Select the Applications tab.

   b) Click the green button at the top of the left Applications pane. The Add Application function loads into the right pane.

   c) In the Name field (required), enter a name for the application. You can use any name you like; for this example, 'Ricoh' was used.

   d) In the Application Type drop-down list (required), select Ricoh SOP.

   e) In the Capture Component drop-down list (required), select AutoStore.

   f) In the AutoStore Server Address field (required), enter the IP address or hostname used by the AutoStore server.

   g) In the AutoStore Server Port field, enter the server port used by the AutoStore server. The default value is 3310 (previously 3350).

   h) In the AutoStore Server Use TLS field, select True or False. This setting should reflect your AutoStore server configuration. Verify it in the Preference tab of the Ricoh SOP component. By default, the AutoStore setting "Use TLS" is OFF. If you leave it as OFF, you should select False in DRS.

   i) In the Print Manager drop-down list (required), select Equitrac. The rest of the Add Application fields appear below.
j) In the DCE Server Address field(s) (required), enter the IP address(es) or hostname(s) used by the Equitrac Server.

k) In the DRS Service URI field (required), enter the address to the DRS server. The default port number for this DRS service is 8755. Note that the address in this field must be an IP address.

l) In the Authentication entry (required), select True.

m) Click the Save button.

4. Add the device in DRS.

a) Select the Devices tab.

b) Click the green button at the top left of the Devices pane. The Add Device function loads into the right 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 hostname of the device.

e) Enter the Username and Password for the device.

f) From the Application drop-down list (required), select the application you have created (in this example 'Equitrac + AutoStore'). The rest of the Add Device fields appear below.

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

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 drop-down list (required), choose between Single-Function Printer (SFP), Multi-Function Printer (MFP) or Specific model (MP C306/MP C406) device. NOTE: This will affect available workflow applications.

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

m) In the Assign as Home Key Application field, select True or False.
n) In the **Scan preview** entry, select **True** or **False**.

o) In the **Application Package** drop-down 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.

p) In the **Customize Assets** field, choose select **True** or **False**. If **True** is selected, additional fields appear below.

  - In the **Application Logo** drop-down list (required), select relevant image file. The following image types are available: JPG, JPEG, PNG or BMP.
  - In the **Welcome Screen Image** drop-down list (required), select relevant image file.
  - In the **Customize Welcome Screen Text** field, choose select **True** or **False**. If **True** is selected, additional field appear below.
    - In the **Welcome Screen Text** field, enter your text.

**Note:** The Info icons next to field names explain 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 above specifications. Once uploaded, they will show up in the drop-down list (for Application Logo and Welcome Screen Image, respectively depending on the uploaded file’s size). NOTE: Uploaded files that do not conform will not show in the drop-down list.

q) In the **Customize Workflow Buttons** field, choose select **True** or **False**. If **True** is selected, additional field appears below.

  - In the **Workflow Application** selection fields, choose and select available workflow applications for your selected device.

r) Click the **Save** button at the top of the **Add Device** pane.

For more details, see *Ricoh PCC 5.1 device properties* on page 52

5. Install Ricoh PCC 5.1 client application onto the device.

a) From the **Select Actions...** drop-down list at the top of the **Details** pane, select **Full Install**. For details, see *Ricoh PCC 5.1 Actions Reference* on page 60. Note: To go back to 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.

6. Locate the auto-added device and configure it in Equitrac System Manager. For instructions, see the Server-Side Configuration section of this document.

Upgrading from Ricoh PCC 5.0 to 5.1

If you want to upgrade from Ricoh PCC 5.0 to 5.1, DRS must first be upgraded to version 7.12. From DRS 7.12, support for PCC 5.0 has been discontinued. The client version is strictly tied to its version of DRS. The process to upgrade to DRS 7.12 is straightforward but contains specific steps that must be taken.

Upgrading from Ricoh PCC 5.0 to Ricoh PCC 5.1 in case the user has a local database

To upgrade from Ricoh PCC 5.0 to Ricoh PCC 5.1, complete the following:

1. Upgrade to DRS 7.12.
   a. Back up the DRS_LDB.mdf and DRS_LDB_log.ldf files by copying them from the Device Registration Service installation folder to a temporary location. For example, from C:\Program Files\Nuance\Device Registration Service\Service\. 

   Note: The files store application and device configurations. The files are deleted when you uninstall Device Registration Service software. If you do not back up the files, you cannot recover the configurations and you have to manually re-create them in the new version of Device Registration Service.

   Note: Upgrading of DRS does not preserve all Windows settings (for example, the security settings). It is recommended to validate that all settings are correct after you start the DRS service.

b. Uninstall your previous version of DRS using Uninstall a Program (Control Panel in Windows).
c. Install the latest version of the Device Registration Service software. For more information, see section *How to install Device Registration Service in Device Registration Service 7.13 Installation Guide*. You must restart your system for changes to Microsoft SQL Server to take effect. When prompted, you can click **Yes** to restart immediately or **No** to restart manually later.

**Note:** Do not start the DRS service after restart.

d. Replace the new versions of the **DRS_LDB.mdf** and **DRS_LDB_log.ldf** files in the Device Registration Service installation folder with the files that you have backed up.

**Note:** Tool will prompt the user to make changes to the file permissions.

**Note:** If the correct permissions have been granted and you still get a permissions error reported during the upgrade, you will need to get a system admin to grant temporary write access to the two files before the tool runs. Write access can be revoked once the upgrade tool completes.

e. After restoring the LocalDB database files (**DRS_LDB.mdf** and **DRS_LDB_log.ldf**), the user is prompted with the following dialog box upon starting it.

![Device Registration Service](image)

After clicking **Yes**, the user may run the Upgrade Tool.

**Note:** Optionally, instead of an in-place DRS upgrade, install DRS 7.12 on a separate supported workstation/server to deploy Ricoh PCC 5.1. After installing DRS 7.12, migrate the older DRS database to the new DRS workstation/server.

2. Install the latest Ricoh PCC 5.1 client using DRS 7.12 with a **Full Install** action.

Also note the following:

- Allow DRS 7.12 to uninstall Ricoh PCC 5.0.
- Do not allow DRS 7.12 to manage or install a Ricoh PCC 5.0 environment.
- Do not allow DRS 7.11 to manage, install or upgrade a Ricoh PCC 5.1 environment.

**Upgrading from Ricoh PCC 5.0 to Ricoh PCC 5.1 in case a remote database is used**

To upgrade from Ricoh PCC 5.0 to Ricoh PCC 5.1, complete the following:

1. Open **Device Registration System Configuration**.
2. Stop service.
3. Clear **Enable Local DB**.
4. Click **Properties**.
5. Enter database information and click **Test Connection** to ensure connection is successful.

6. Click **OK**.

7. Start DRS Upgrade tool and ensure **Enable Local DB** is unchecked.

8. Click **Properties** to ensure database information is available and click **OK**.

9. Click **Run**.

**Database Upgrade Tool**

The database upgrade tool is run after an existing DRS installation has been successfully upgraded, with the backed-up database correctly restored, but before the DRS service is started. The tool goes through all
existing application profiles, devices and device groups, and perform necessary modifications to have the database records ready for the latest DRS release.

Complete the following:

1. Move the DRS Database Upgrade Tool's main executable (NSi.DeviceManagement.Upgrade.exe and its configuration file (NSi.DeviceManagement.Upgrade.exe.config) backed up previously to the Service subfolder of the Device Registration Service installation folder (for example, C:\Program Files \Nuance\Device Registration Service\Service).

2. Once started, the DRS Database Upgrade Tool retrieves the database connection currently configured in DRS Device Configuration Manager and performs the necessary initialization on this database. Click Run to begin the upgrade process.

During the process, the administrator is informed of application profiles, device groups, and individual records that have been processed, any errors encountered, and if the upgrade was successful.

3. Once processing has been successfully completed, the log will display Completed successfully message. Click Close to exit the tool.
4. Start DRS 7.13 service with the newly-upgraded database records.

Uninstalling Client Using DRS

Complete the following task.

1. Open a web browser and enter http://DRSServerIP:9000/device (where DRSServerIP is the IP address or the host name of the server where you installed DRS) to open the DRS web client interface. The Device Registration Service screen opens.

2. Select the Devices tab.

3. Select the device to be uninstalled.

4. Select Uninstall from the Select Action drop-down menu.

5. Click the Run Action button 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.

If you wish to set the device back to default settings, following an uninstall of the Ricoh PCC 5.1 client using DRS, you will need to manually reset admin authentication to Off for the User Management and Machine Management settings.

Complete the following task.

1. On the device, select User Tools and go to Machine Features > System Settings.
2. Log in with administrator credentials, and in Available Settings, select Administrator Tools.

DRS Authorization

When MFP TLS is enabled on the device and DRS is used to configure a device (in case a DRS other than the original DRS used for configuration is used), the client returns a Request unauthorized error.

In this case, the user must uninstall the client if they want to use a different DRS.
Set Up a Ricoh PCC 5.1 MFP

Configure the Ricoh SFP or MFP in Unified Client Environment

BEFORE YOU START

⚠️ Important: Specific Ricoh device settings vary by geographic location and setup. Consult your Ricoh technician for any Single-Function Printer (SFP)- and Multi-Function Printer (MFP)-specific settings needed for your particular deployment.

📝 Note: Ensure that MFP has Java application version 12.0 or later.

If you expect to wake up the MFP from sleep mode using a card swipe, you must set this setting first: Service > Screen Features > Screen Device Settings > Screen device always-connection Setting.

📝 Note: User customization through the Ricoh Address Book is not a supported compatible feature with Ricoh SOP authentication.

⚠️ Important: A hard disk drive (HDD) is required to be installed on SFP and various MFP devices (for example, SP C842DN and MP C306) in order to be supported.

Install and configure the TLS certificates

Before performing any Device Registration Service (DRS) actions, it is recommended that you verify the following TLS certificate configuration on the Ricoh MFP.

📝 Note: If you are not using a self-signed certificate (generated by the device), but instead using a certificate signed by a Certificate Authority (CA), you must import the CA certificate into DRS.

After installing DRS 7.13, complete the following steps.

1. Verify that the device certificate is installed and the TLS certificate is specified.
   a) On 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), open Device Management > Configuration > Security > SSL/TLS.
   b) If the SSL/TLS certificate is not selected, select it.
c) Click OK.

2. Verify that the Ciphertext Priority option is selected.
   b) In the Permit SSL/TLS Communication field, select Ciphertext Priority.

Note: If you are not using a self-signed certificate (generated by the device), but instead using a certificate signed by a Certificate Authority (CA), you must import the CA certificate into the appropriate Trusted Root CA store of the system where DRS is installed.

Note: To use Ricoh configuration tools, you must select at least one of the following options: TLS1.0, TLS1.1, or TLS1.2 (support for SSL 3.0 has been discontinued). Support for the newer cryptographic protocols such as TLS 1.1 and 1.2 are provided to Windows through the Security Support Provider Interface (SSPI) API. To enable TLS versions, use Registry Editor. Once the registry changes are made, you may need to restart your server.
Note: This can be also configured using operation panel under **Extended Feature Settings** by selecting available functions (this operation/screen is displayed in MFP only after login with Administrator credentials):

![Extended Feature Settings](image)

c) Click **OK**.

**Ensure that previous applications are cleared**

If you had previous solutions configured on the device and these have not been removed properly you need to clear any existing notification events.

This action should only be performed if previous applications were not properly removed from the device.

**Set Up Your First AutoStore Capture Workflow**

At this point in the deployment workflow, you should already have a fully functioning installation. To verify this, create and configure an AutoStore capture workflow (Send to Folder) and test it on your device.

**License AutoStore**

This is the prerequisite step before you can start configuring your first AutoStore workflow. For more information, see *Nuance AutoStore Installation Guide*.

**Configure Scan to Folder**

1. Select the **Home** tab and choose **New**.

2. Define **Task Properties** and click **OK** on the **Task Properties** dialog.
3. Click and drag the **Ricoh SOP** icon from the **Capture** list located on left side of the **AutoStore Process Designer Toolbox** anywhere on the newly created workflow canvas on the right side of the screen to an AutoStore workflow to provide AutoStore capture functionality for Ricoh devices on which the Ricoh PCC 5.1 is installed.

4. Scroll down to the bottom of the **Route** list and click and drag **Send to Folder** to the workflow.
5. Right-click on the Ricoh SOP icon and select Properties.

6. Select the Preferences tab. Your settings under Server must match the ones you specified in DRS. If you kept the default values there, type 3310 (previously 3350) in the Web Server Port field, and leave Use SSL unchecked. Otherwise, ensure that these values match the ones you set in DRS.

7. Select the Groups tab, and click on Common Group for the Ricoh SOP component configuration.

8. Select Add Form > Basic Form. Name the form ‘Sample’ and click on the Components tab to configure the folder to route the scan to.

9. Select ... and add the path of the destination folder.
10. Click ... next to Folder path and create a folder such as c:\Scans to send scans to. Check off Rename file to ensure file names are unique.

11. Click OK. and Save to save the configuration to a folder such as c:\asconfigs.

12. Click Start at the top of AutoStore Process Designer. You should now be able to start and use this workflow from the MFP.

AutoStore has a lot more AutoStore capture workflows to offer. Consult the downloaded product documentation on how to set those up.

**Set Up Your First Print Workflow**

At this point in the deployment workflow, you should already have a fully functioning installation. To verify this, create and configure a simple print workflow (Follow-You Printing) and test it on your device.

For more information on how to setup Follow-You Printing and use I-Queue Printing, the *Equitrac Office/Express Administration Guide*.

**Use Follow-You Printing**

1. Login at the device: Enter valid login credentials using the on-screen keyboard (invoked by tapping within the User ID field), or by using a swipe card, or (optional) select the desired Quick Selection option from the list on the screen, if available.
2. The Launcher screen appears.

Press the Follow-You Printing container from the displayed functions. The Follow-You Printing screen displays all the queued documents associated with your login credentials or release key. By default, the list displays documents in order from longest-queued to most-recently queued.

3. Select the job(s) that you want to print and press Print.
Available operations on the Follow-You Printing screen

- Select - or + to adjust the number of copies
- Select the Force Mono switch to force color jobs to print in black and white
- The top line of the documents list indicates the number of documents available. To select or deselect all documents, press the checkbox next to Print Jobs
- Select or deselect individual print jobs by pressing the print job's respective selection checkbox
- Select Print to release all selected documents

The following options are available by selecting the menu icon at the top right of the screen:

- Select Select All to select all documents
- Select Delete to remove all selected documents from the Job List without printing them
- Select Refresh to refresh the current page
- Select Print & Save to print and save all selected documents from the Job List

Process Instructions

This section describes detailed process to install Ricoh PCC 5.1 in an AutoStore and Equitrac environment.

Configuring Equitrac to Use with Ricoh PCC 5.1

This section documents how to configure Equitrac to use with the Ricoh PCC 5.1.

Important: Specific Ricoh device settings vary by geographic location and setup. Please consult your Ricoh technician for any MFP-specific settings needed for your particular deployment.
Configure Equitrac
Configure the authentication for the Ricoh PCC 5.1 component to work with Equitrac authentication.

The Ricoh PCC 5.1 provides copy control, scanning, and secure printing on specific Ricoh manufactured Multi-Functional Products (MFPs). Embedded on the MFP, Ricoh PCC 5.1 controls access to the MFP, and acts as the gateway for Kofax functionality. Users must authenticate to gain access to Kofax-controlled device functions.

Ricoh PCC 5.1 communicates with servers and tracks User activity. During a user session, MFP activity is captured.

Ricoh PCC 5.1 requires Smart Operations Panel G2 or later.

Ricoh PCC 5.1 Features
Ricoh PCC 5.1 supports the following features:

**Authentication**
Requires users to enter valid authentication information to unlock the MFP functions. Users can enter their authentication data via the MFP panel, or by using a valid authentication card (when authentication cards are implemented).

**Follow-You Printing®**
After successful login at the MFP, the user can access the virtual print queue to "pull" a print job to this device. Through the Follow-You screen on the MFP, users can see a list of documents in the queue, then select, delete, or release documents for printing. See *Using Follow-You Printing* or end-user instructions.

**Scan-to-Me®**
Allows users to scan a document and email it to their own address, and optionally to other addresses via the CC field (if enabled). Users can specify scan options (for example: duplex, color, size) and document format prior to initiating a scan. See *Scanning* for end-user instructions.

**Capture and Send capability**
Allows SOP to use third-party applications to scan to multiple scan destinations through the Scan Processing Engine (SPE). Currently, SOP allows SharePoint (Teamsite) to scan to a web-based location, and RightFax to scan directly to a Fax number.

**Card self-registration**
Allows users to associate an unassigned card with their user credentials. Once associated, each time the user swipes the card, the system automatically recognizes the card and associated user.

**Billing Code support**
Users can change their jobs to a particular code, and the Equitrac Office/Express database tracks the characteristics of jobs changed to the code. Billing codes must be enabled on the Equitrac server. Refer to the Creating & Managing Accounts chapter in the
Equitrac Office or Equitrac Express Administration Guide.

Campus card support
When enabled on the Equitrac Express server, campus card payment systems including Blackboard UNIX, Blackboard Windows, and CBord Retail Transaction Interface. At the MFP, users can authorize themselves as valid campus card account holders, make copies, release jobs, and pay for these services in real time, directly from their campus card account. See the Managing Devices chapter in the Equitrac Express Administration Guide.

Offline operation
In the event that SOP fails to connect to the Equitrac DCE service, you can configure SOP to continue the MFP lock down, allowing users to authenticate based on account information stored in local MFP cache. SOP gathers job data in local cache, and forwards the accounting details to the DCE service when it is back online.

Integration with third party applications
SOP tracks job details generated from supported third party applications. Currently, the third-party applications supported for scan are SharePoint, RightFax, and GlobalScan NX.

Support for multiple DCE servers
You can designate up to 4 different DCE servers - one primary, and up to three backup servers. We recommend that the primary DCE is located on-site to allow for the fastest possible data transfer. Other DCE servers can be located off-site.

Installation and Configuration
This section describes how to install Ricoh PCC 5.1 on supported multifunction printers (MFPs) and configure the product for initial start-up. In addition to this guide, ensure that you have any documentation related to your Equitrac product suite and any documentation for your MFP.

Note: This guide assumes that you are installing the Equitrac products (servers and embedded applications) in a Windows network environment. This guide does not provide any information for third-party software (including databases) or operating system support.

Server-Side Configuration Scenario
Ricoh PCC 5.1 supports multiple product servers either individually, or simultaneously. The client can either act as a Ricoh Authentication Agent, or run as a regular Android application on the SOP. The following is a breakdown of the supported scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Servers and authentication</th>
<th>EO/EE</th>
<th>Authentication Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore and Equitrac (Ricoh SOP)</td>
<td>Equitrac-AutoStore-Auth ON</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AutoStore and Equitrac (Ricoh SOP)</td>
<td>Equitrac-AutoStore-Auth OFF</td>
<td>Yes</td>
<td>No*</td>
</tr>
</tbody>
</table>
* Requires the CAC authentication to function in Equitrac-Auth-OFF mode.

**Additional Documentation**

You may need to refer to one of the following documents when performing server-side configuration tasks.

<table>
<thead>
<tr>
<th>Guide</th>
<th>When to refer to this guide</th>
<th>Where to find the guide</th>
</tr>
</thead>
</table>
| Equitrac Office and Express Planning Guide | Before installing Equitrac Office or Express, use this guide to select the appropriate combination of product variables to support the needs of your institution or organization. | Installed automatically with Equitrac in the Program Files \
\(<\text{Equitrac Installation Folder}\>\Documentation folder. |
| Equitrac Office and Express Installation Guide | Use this guide to perform an initial installation or upgrade.                               | Installed automatically with Equitrac in the Program Files \
\(<\text{Equitrac Installation Folder}\>\Documentation folder. |
| Equitrac Office and Express Administration Guide | After installing Equitrac Office or Express, use this guide to configure advanced options for use on your campus or in your organization. | Installed automatically with Equitrac in the Program Files \
\(<\text{Equitrac Installation Folder}\>\Documentation folder. |
| Device Registration Service User Guide | Use this online help guide to determine basic use cases and User-related setups.           | The DRS help is found by clicking on the Help button within the DRS application.        |
| Device Registration Service Installation Guide | Use this help guide to determine installation and upgrade processes.                        | Locate this file on the Equitrac Partner Portal.                                        |
| Tips and Troubleshooting Guide        | Use this guide to determine the setup of DRS in a multi-site deployment.                    | Locate this file on the Equitrac Partner Portal.                                        |

**Equitrac Card Readers**

Equitrac USB card readers are typically automatically detected by the device upon start-up. There is no MFP or server configuration required for Ricoh PCC 5.1 to recognize card reader hardware. Some card readers can be configured to detect multiple card types. If your card reader supports more than one type of card, we recommend configuring it for only the type of card used.

**Note:** Card reads within authentication work flows must be configured on the server in System Manager. Otherwise, card reads are not recognized. For detailed information about configuring authentication workflows, see the Equitrac Office/Express Administration Guide.

**Card reader setup**

Ricoh devices have more than one available USB port. Equitrac card readers can occupy the USB port located to the left side of the SOP Panel, and can also leverage the internal mini-USB port.
Note: Third-Party card readers which are supported by the Ricoh device may also be used. Such readers may require a separate license. Additional MFP setup and configuration is required for Ricoh-supported 3rd party card readers.

USB Keyboards
Starting with the Ricoh PCC 5.1 release, Ricoh Smart Panel devices no longer support the use of USB keyboards. The on-screen software keyboard is used instead.

Server Side Configuration
At this point in the deployment workflow, you should already have a fully functioning installation.

For more information on server side installation and features, see the Equitrac Office/Express Administration Guide and Equitrac Office and Express Installation Guide.

Using Ricoh PCC 5.1
This section documents typical use cases and screen elements of the Ricoh PCC 5.1.

⚠️ Important: Specific Ricoh device settings vary by geographic location and setup. Please consult your Ricoh technician for any MFP-specific settings needed for your particular deployment.

Elements of Ricoh PCC 5.1 User Interface
The Ricoh PCC 5.1 user interface is touch-based. Use your finger or a pointing device such as a stylus to make common touchscreen type gestures, type on the soft keyboard, scroll lists of options, and perform certain system commands. Users can swipe the screen to reveal more options, as indicated by the carousel dots. The screen requires that minimal pressure be applied when navigating the system. The user interface for the Ricoh PCC 5.1 is presented in three areas:

Figure 2: Typical Launcher Screen, indicating the three areas
Figure 3: Alternate screen, showing Navigation Button

- Title Bar. This area is controlled by the Device, and is used primarily to access the system. The following options are possible:
  - **Login** button: Presents the login screen to authenticate and gain access to the Ricoh PCC 5.1.
  - **Logout** button: Logs the currently logged in user out.
  - **Moon**: Engages system sleep mode. This is disabled when a user is logged in.
  - The currently logged in user's name.
  - The **System Home** button: Returns the user to the Ricoh Smart Operation Panel Home Screen.

- Main Window. This area is controlled by the Ricoh PCC 5.1, and is the main interface. Most user selection and workflow activity is handled through interaction with this area of the UI. Depending upon the currently active screen, the following options are possible:
  - **Notification Bar**. Indicates the current workflow or screen. Also indicates when a list of recent system notifications is available. Press the notification icon (when present) to display:
    - Status notification
      - Error notification
    - All available workflows. These are determined by the administrator when Ricoh PCC 5.1 is setup, and by the privileges of the user currently logged in. Workflows that act as gateways to additional workflow groups are enclosed in square braces. For example, **[Scan]** opens a menu with additional options.
  - **OS Bar**. This area is controlled by the underlying operating system, and is used primarily for navigation. Depending upon the currently active screen, the following options are possible:
Typical User Workflows

This section describes how to login to Ricoh PCC 5.1 and use its screens and features on the MFP. This section also provides information about entering billing codes and using campus cards.

If your administrator has enabled account limit enforcement, and/or color quotas, and/or billing codes, read the following paragraphs before you use Ricoh PCC 5.1.

Account limits – Account limits ensure that you have sufficient funds in your account to pay for print jobs before the jobs are released from the queue. As you release print jobs in using Equitrac, the software continuously checks your output against your estimated account balance. If the total cost of printing selected documents is more than your estimated available fund balance, the server will not release the print jobs. Instead, if escrow is enabled in the server settings, an error message appears indicating that the balance is not enough to pay for the printing or copying. After you add funds to your account, you can login again to release your jobs. In the case of copy jobs, the embedded application stops the copy job at the point when the estimated account balance is exceeded, and locks access to the MFP functions. This is available only as a licensable feature in Equitrac Office or Equitrac Express.

Note: Advanced MFPs have a 'multi-page copy pipeline'. The MFP may eject a few pages beyond the account limit on high-speed machines.

Billing Codes – A billing code is a unique combination of characters that represent a charge-back group. You can assign your transactions to a particular code, and Equitrac Office or Equitrac Express tracks the characteristics of copy or print jobs assigned to the code.

Color quota – Color quotas are used to limit the amount of color copying and printing that you can produce. As you copy or print, Ricoh PCC 5.1 compares your output to your color quota balance (in number of pages). Once you reach the quota, the application disables the color function on the MFP. If you still have funds remaining in your account, you can switch settings to black and white and continue to produce black & white copies or print black & white documents only. You are able to produce color output only when your color quota is reset on the server.

Logging Into Ricoh PCC 5.1

To log into Ricoh PCC 5.1, users must login from the PCC login screen.

• If the Home key assignment is set to Embedded for Ricoh SOP, the Launcher screen is displayed after a user logs in from the Welcome screen.
• If the Home key assignment is set to System Home, the Ricoh home screen is displayed.
After the Ricoh PCC 5.1 starts, a Server Status screen appears.

Note: If all servers are online, this screen will not appear and you will be redirected to Welcome page instead.

After you close Server Status screen, you can display the Login screen either by tapping anywhere in the main window, or swiping across the screen in either direction:

Note: Ricoh PCC 5.1 acts as a device Authentication Agent, allowing it to lock and unlock the device and collect transactions.
On this screen, users must provide valid authentication credentials before they can access the device functions available to them.

Note: DRS quick shortcut options cannot be selected as defaults on the Welcome screen by default. Only the first item in the DRS deployed shortcut list will be selected.

The login process follows this general path:

1. Touch anywhere on the Welcome screen, or use touchscreen type gestures to swipe in either direction on the screen to display the Login screen.
2. (Optional) Select the desired Quick Selection option from the list on the screen, if available.
3. Enter valid login credentials using the on-screen keyboard (invoked by tapping within the User ID field), or by presenting your card.

Depending on configuration, one or more login fields may appear. The following are examples of valid login credentials:

- Equitrac primary PIN only
- Equitrac primary and secondary PINs
- Windows Networking credentials - network user name and password
- Present a card at the card reader
- Present a card and Equitrac secondary PIN
- Present a card and provide Windows password
- Equitrac primary PIN and Windows password
- Campus card swiped at the card reader. (for Equitrac Express only)

Note: The last prompt field on the Login screen is masked to protect your login credentials. If secondary prompts are not enabled on the server, the User ID field is masked (**). If secondary prompts are enabled, the second field is masked instead.

4. Touch the Login button. The Launcher screen or selected Quick Selection workflow opens.

If you have difficulty logging in

If your credentials are not validated, an error message appears requiring you to try your login again.
If the system does not recognize the swipe card you used to authenticate, you are prompted to enter your authentication details if the card auto-registration feature is enabled. The next time you swipe the card, your login information is populated automatically. Otherwise, the system displays a "login failed" error.

**Entering Billing Codes**

If billing codes are configured, the Accounting/Billing Code screen opens before a user accomplishes a task. The code entered here applies to copy and scan jobs. If overrides for Follow-You printing are enabled, a billing code which overrides the first can be entered and upon job release in the Follow-You Printing screen.

Note: If an account is configured with only one available billing code to charge against, and billing codes are required, then that code is automatically selected and the Billing Code screen does not appear unless the "Billable" option is enabled.

1. In the **Billing Code** field enter the billing code, if required.

   If you don’t know the code, select the **Search** button, represented by a magnifying glass icon. An onscreen keyboard displays, allowing you to enter search criteria. The keyboard can be dismissed to select from the resulting list of billing codes if it covers some of the results. The list initially contains all billing codes, and then narrows to a subset based on the search criteria entered. The list contains the first 100 codes that matched your search. Use swipe gestures to browse through billing codes and select the correct code, which then populates the Billing Code field.

2. If configured, select whether the job is **Billable** or not by tapping the check box.

   This option determines if the transaction is billed to a user, group, or department, or if it is only entered into the system for reporting purposes.

3. Select **Done** to continue.

   If the Billing Code validation is enabled, the billing code is validated when you select **Done**. If you searched for a code and selected it from the list, it is validated immediately. Billing code validation is set in System Manager > Configuration > Session Flow > Validate Billing Codes.
**Follow-You Printing**

The Follow-You Printing screen displays all the queued documents associated with your login credentials, or release key. By default, the list displays documents in order from longest-queued to most-recently queued.

Each time you release a document from the Job list, the Ricoh PCC 5.1 checks your estimated available account balance. If account limits are enforced, and the total cost of the selected documents exceed the available account balance, an error message displays indicating that the account balance would be exceeded and the items will not be printed. The current pages, documents, costs associated and other information appears in real time for the print jobs selected in the document details window at the lower right of the screen.

**Note:** Account limits are a licensable feature available in Equitrac Office or Equitrac Express.

For more information on how to use Follow-You Printing, see *Use Follow-You Printing* on page 33.

**Scanning**

Ricoh PCC 5.1 offers the ability to perform many different scan tasks, including scanning to email and network folders through SharePoint (team site) and scanning directly a fax through RightFax. To use these options, the Capture and Send function, which enables the Ricoh PCC 5.1 to perform these tasks, must be set up and licensed.

Ricoh PCC 5.1 acts as a user-facing experience to handle numerous scanning solutions. For example, Equitrac Scan-to-Me functions are handled through the Ricoh PCC 5.1, and users can scan to network folders, email addresses or directly to fax recipients based on the workflow chosen. The workflow experience for each feature is identical to an end user regardless of the product used to process the scan. The options available to a user depend upon the administrator's setup, the user's settings, and which features are licensed. Scan settings and processes are handled through the Ricoh Scan GUI service.

Detailed information on setting up scan workflows is found in the *Equitrac Office or Equitrac Express Administration Guide*.

Scanning can proceed either by using the Automatic Document Feeder (ADF) on the device, or by scanning directly from the glass of the MFP one sheet at a time. The actual scanning process and scan settings per job are handled through the Ricoh Scan GUI Service.

**Note:** If a user wants to quit a scan, this can be done using the **Stop** button at any time. However, if the document being scanned is using the ADF, the pages will finish running through the ADF before stopping the process.

**Note:** If a user presses the **Home** button during a scan, the following message is displayed: "Device is scanning. Unable to return to Launcher."

**Note:** Users can append pages to documents mid-scan job when scanning from the glass. However, appending pages to scan jobs through the ADF is not supported.

**Note:** Scanning is accomplished through the Ricoh Scan GUI Service. This service differs when using Ricoh A3 devices.

**Terminology**

For the purposes of this section, the terms used refer to the following:

**Scan Task:** An operation which delivers a scan to a particular end point. This can be a destination such as an email address or network location, or a service such as a RightFax operation.
Documents: One or more pages that will be scanned. There can be as many pages per document as required, within the limits of what the device allows.

Scan Job: A collection of Documents. You can scan multiple Documents at a time, which are then concatenated into a Scan Job.

Job Details: A collection of metadata that is applied to a Scan Job. Typically, any collection of Documents will share the same Job Details through their inclusion in a Scan Job.

Prepare to scan

Log in to the PCC 5 at the device with your credentials. Place the document you want to scan into the Automatic Document Feeder (ADF) or, onto the glass of the scanner.

Note: You can place your document at the start of the workflow, or at any time prior to scanning.

Select a Scan workflow from the available options. Scan workflows are typically set up in System Manager to simplify and automate the Scan process. The following is an example Scan-To-Me screen.

Note: If Capture and Send is not licensed and configured, then only Scan-To-Me functions are available.

Note: The Scan Processing Engine (SPE) component of Equitrac Office or Equitrac Office or Equitrac Express must be installed to enable any scan functionality.

Depending upon the destination of your scan, you may be asked to provide specific meta data. These Job Details are associated with the Scan Job in question. This information determines specific attributes used in the routing and type of scan produced. Depending upon how each Scan workflow is configured on the server, some Job Details are collected automatically based upon your login information. Information that is collected automatically may be changeable. For example, your email address may be filled in automatically when sending a scan as a mail destination in the From attribute. However, if the configuration allows it, you can change this to a different address. In some cases, these attributes are configured to be static, in which case you cannot override them, and they may not appear altogether. For this reason, the changeable fields presented to you at the device may differ from Scan Task to Scan Task, and even from user to user, depending upon configuration. A list of metadata by workflow type includes:

- Scan-To-Me or Scan to Email
• To: The email address to route the completed scan. For this workflow, the To field typically auto-
populated with the email address associated to the logged-in user.
• Cc: The email address of any other recipient to whom the user wants to send the scan.
• Subject: The subject of the email when delivered. Typically, this defaults to Scan-To-Me.
• Body: Any text the user wants to include in the body of the email message containing the resulting
scan.
• File Name: The desired name of the scanned file. This typically auto-populates with system
information.
• Scan To Network Folder
  • Network Folder: The fully qualified UNC path to the network scan folder. The resulting scan is
deposited into this location on the network.
  • File Name: The desired name of the scanned file. This typically auto-populates with system
information.
  • Delivery Format: The desired format for the finished scan. Typically, scans are delivered in PDF format,
but this selection field allows a user to select whatever formats are offered through the device setup.
Press the field and select the desired option. Note that this list can often be scrolled to display more
options than those which fit on screen. See Delivery formats on page 46 for more information.

Note: If a field is static, you will not be able to change the information. These fields appear for your
information only.

Note: If a field has an asterisk (*) next to it, the field is required, and you must provide valid information for
the field if not prepopulated.

Note: One you have entered metadata and started the scan workflow, you must restart a new workflow to
enter different metadata. If you want to reuse the existing data, you can simply start a new scan job and the
fields prepopulate with the last-used metadata.

Important: If you want to change the Scan settings, such as paper size, dpi, or brightness, press the
Change button. This opens a new dialog box. The options for Scan Settings are governed by the abilities
of the MFP hosting the solution. Depending upon licensing and your configuration, full scan integration
with AutoStore is supported. Make the changes you want, then save and you will be returned to the scan
workflow.

Delivery formats

Depending upon the scan task, the Ricoh PCC 5.1 can deliver it in various different file formats. The
supported file formats depend upon the server scan workflow settings, the delivery formats supported by
the device, and the settings configured by the Administrator. See the Equitrac Office or Equitrac Express
Administration Guide for details. Available file formats are:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>OCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF (Image)</td>
<td>Basic PDF - Not searchable.</td>
<td></td>
</tr>
<tr>
<td>MFP’s Output</td>
<td>The PDF created by the device itself. All other formats are created through the SPE.</td>
<td></td>
</tr>
<tr>
<td>Searchable PDF</td>
<td>Basic Searchable PDF.</td>
<td>✓</td>
</tr>
<tr>
<td>TIFFs</td>
<td>A single TIFF image per page scanned.</td>
<td></td>
</tr>
<tr>
<td>Format</td>
<td>Description</td>
<td>OCR</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Multi-Page TIFF</td>
<td>A single TIFF file that contains multiple pages in the file.</td>
<td></td>
</tr>
<tr>
<td>JPEGs</td>
<td>A single JPEG image for each page scanned.</td>
<td></td>
</tr>
<tr>
<td>PNGs</td>
<td>A single PNG graphics file for each page scanned.</td>
<td></td>
</tr>
<tr>
<td>Searchable PDF</td>
<td>Searchable PDF with additional compression. Useful for black and white</td>
<td>✓</td>
</tr>
<tr>
<td>MRC</td>
<td>documents with a large amount of text.</td>
<td></td>
</tr>
<tr>
<td>Searchable PDF/A</td>
<td>Searchable PDF meeting PDF/A-1b Archiving Standards.</td>
<td>✓</td>
</tr>
<tr>
<td>RTF</td>
<td>Rich Text Format, a specification originally published by Microsoft for</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>cross-platform document interchange among software applications.</td>
<td></td>
</tr>
<tr>
<td>Word (.doc) - True</td>
<td>Native Word - 2000 to 2003 - Matches most closely with the scanned text, but</td>
<td>✓</td>
</tr>
<tr>
<td>Page</td>
<td>is more difficult to edit.</td>
<td></td>
</tr>
<tr>
<td>Word (.doc) -</td>
<td>Word 2000 to 2003 - Uses Word formatting to simplify editing, but does not</td>
<td>✓</td>
</tr>
<tr>
<td>Flowing Page</td>
<td>match as closely to the original.</td>
<td></td>
</tr>
<tr>
<td>Word (.docx) - True</td>
<td>Word 2007 and 2010 - Matches most closely with the scanned text, but is</td>
<td>✓</td>
</tr>
<tr>
<td>Page</td>
<td>more difficult to edit.</td>
<td></td>
</tr>
<tr>
<td>Word (.docx) -</td>
<td>Word 2007 and 2010 - Uses Word formatting to simplify editing, but does not</td>
<td>✓</td>
</tr>
<tr>
<td>Flowing Page</td>
<td>match as closely to the original.</td>
<td></td>
</tr>
<tr>
<td>Searchable XPS</td>
<td>Searchable XPS (Microsoft's Portable Document Format).</td>
<td>✓</td>
</tr>
<tr>
<td>Text</td>
<td>Unicode text with no line breaks (line breaks added at the end of paragraphs,</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>but not on the actual line of text).</td>
<td></td>
</tr>
<tr>
<td>PDF/A (image)</td>
<td>PDF meeting PDF/A-1b Archiving Standards.</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Using LDAP Email Search**

LDAP email look-up can be used from the Scan-To-Me screen or any scan to email-enabled feature. In order to use LDAP search, it must be enabled and configured on the server. See the *Equitrac Office or Equitrac Express Administration Guide* for details. If not configured, the search magnifying glass icon does not appear. To perform a search, use the search magnifying glass icons located beside any **To** and **Cc** fields in workflows that use them.
To perform an email search, do the following:

1. Select the **Magnifying glass** button beside the **To** or **Cc** fields to search for and add addresses to the corresponding field.

   **Note:** If there are no search criteria entered, the list below the search box contains the entire LDAP email directory.

After you complete this step, a **Search** screen opens:

2. If not already displayed, press the search magnifying glass icon to display the keyboard.
3. Enter your search criteria. The list below reflects email addresses that match the criteria as you type.
4. When you finish entering your search criteria, or the list displays the correct result, dismiss the keyboard using the down arrow, and then press the appropriate email in the list.
5. Select one or more addresses, and click **OK** to exit the Email Search feature.
6. Make a selection from the results, and touch **OK**. The information populates the **To** or **Cc** field.

**Logout**

The Ricoh PCC 5.1 supports the following logout options at the device:

**Logout button**

To end a user session and log out of Ricoh PCC 5.1, press the **Logout** button on the top bar.

**Logout by card swipe**

While logged in, the user can swipe a card again to log out. This is a convenient way to log out when the application is not the current application on the panel, even for pre-10.x devices.

**Auto logout**

If the user forgets to log out, the Ricoh PCC 5.1 automatically logs out the user after the user has not been active on the MFD control panel for a specified time-out interval. The time period is configured in the **Auto Logout Timer** under **Timer** section in device’s Web Image Monitor webpage.
**Server Connections Timeout**

Server Connections Timeout setting in DRS setting is used to control the connection timeout between DRS and MFP during device (SP modes) configuration and client installation.

**Energy Saving Mode logout**

When the device enters Energy Saving Mode while the user is logged in, the Ricoh PCC 5.1 logs out the user before the device shuts down.

**Powered off logout**

When the device is powered off manually or through auto-power off timer, the Ricoh PCC 5.1 logs out the user before the device shuts down.

**Ricoh PCC 5.1 Device Settings**

These sections describes how to configure a Ricoh PCC 5.1 device.

**Application properties**

A Device Registration Service application profile for the Ricoh PCC 5.1 specifies connection information for an AutoStore server and a Print Manager server. This information allows a device to use capture and print management services on these servers.

These properties appear in the Device Registration Service **Details** pane when you add or edit a Ricoh PCC 5.1 application. You cannot change the application type for an existing application.

---

**Note:** In an environment with Equitrac and AutoStore deployment, separate applications should be created (one Equitrac application for SFP devices and one Equitrac and AutoStore application for MFPs).

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name that uniquely identifies an application.</td>
</tr>
<tr>
<td><strong>Application Type</strong></td>
<td>To create a new Ricoh PCC 5.1 application in DRS, choose Ricoh SOP for this option.</td>
</tr>
<tr>
<td></td>
<td>The remaining properties shown here appear after you make this selection. You cannot change the application type after you save a new application profile.</td>
</tr>
<tr>
<td><strong>AutoStore Server Address</strong></td>
<td>Identifies an AutoStore server to be used to capture documents.</td>
</tr>
<tr>
<td></td>
<td>This can be an IP address, a system name (if the systems are in the same domain), or a fully qualified domain name. We recommend that you use an IP address only if it is static.</td>
</tr>
<tr>
<td><strong>AutoStore Server Port</strong></td>
<td>The port that the AutoStore server uses to communicate with clients.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>This setting must match the port number that is set on the Preferences tab of the Ricoh SOP component settings in AutoStore. The default is 3310 (previously 3350).</td>
<td></td>
</tr>
<tr>
<td>Print Manager</td>
<td>Specifies the print manager type.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication specifies whether:</td>
</tr>
<tr>
<td></td>
<td>• The print manager is responsible to lock the device and authenticate, or</td>
</tr>
<tr>
<td></td>
<td>• Authentication is provided by a third party (CAC for example).</td>
</tr>
<tr>
<td>DRS Service URI</td>
<td>The address to the DRS server:</td>
</tr>
<tr>
<td></td>
<td><code>http://serverAddress:port/DeviceManagementRestService/</code></td>
</tr>
<tr>
<td></td>
<td>The default port number for this DRS service is 8755.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The address in this field must be an IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If TLS is enabled for the DRS service, ensure you change http to https.</td>
</tr>
<tr>
<td>DCE Server Address</td>
<td>The address for the primary device control engine for Equitrac.</td>
</tr>
<tr>
<td></td>
<td>This option is only available when Equitrac is selected for Print Manager.</td>
</tr>
<tr>
<td></td>
<td>Identifies an Equitrac server to be used to print documents. The server type must correspond to the Print Manager setting. This can be an IP address, a system name (if the systems are in the same domain), or a fully qualified domain name. We recommend that you use an IP address only if it is static.</td>
</tr>
<tr>
<td>DCE Server #2 Address</td>
<td>The address of a second fail safe device control engine for Equitrac. This setting is optional.</td>
</tr>
<tr>
<td></td>
<td>This option is only available when Equitrac is selected for Print Manager.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Identifies an Equitrac server to be used to print documents. The server type must correspond to the <strong>Print Manager</strong> setting. This can be an IP address, a system name (if the systems are in the same domain), or a fully qualified domain name. We recommend that you use an IP address only if it is static. This property is only displayed if two DCEs are installed.</td>
</tr>
<tr>
<td>DCE Server #3 Address</td>
<td>The IP address of a third fail safe device control engine for Equitrac. This setting is optional. This option is only available when Equitrac is selected for <strong>Print Manager</strong>. Identifies an Equitrac server to be used to print documents. The server type must correspond to the <strong>Print Manager</strong> setting. This can be an IP address, a system name (if the systems are in the same domain), or a fully qualified domain name. We recommend that you use an IP address only if it is static. This property is only displayed if three DCEs are installed.</td>
</tr>
<tr>
<td>DCE Server #4 Address</td>
<td>The IP address of a fourth fail safe device control engine for Equitrac. This setting is optional. This option is only available when Equitrac is selected for <strong>Print Manager</strong>. Identifies an Equitrac server to be used to print documents. The server type must correspond to the <strong>Print Manager</strong> setting. This can be an IP address, a system name (if the systems are in the same domain), or a fully qualified domain name. We recommend that you use an IP address only if it is static. This property is only displayed if four DCEs are installed.</td>
</tr>
</tbody>
</table>
Ricoh PCC 5.1 device properties

Ricoh PCC 5.1 device properties are configured in the Device Registration Service web console. When configured for a device group, they can be propagated to any device in the group.

The following parameters define the device settings. Click the edit button to edit the parameters for a device. Click the save button to save changes to the parameters or click the cancel button to discard changes.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Ricoh device or device group.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address or hostname of a Ricoh device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a device only parameter and will not be displayed when configuring parameters for a device group.</td>
</tr>
<tr>
<td>Inherit Properties from Group</td>
<td>This option is visible only when a device is located in a group folder in the Devices pane.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong> specifies to use property settings for the group. The remaining property settings will be inherited from the group and unavailable for configuration here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>False</strong> specifies to configure property settings separately for this device. The remaining settings will be available for configuration here except in their description.</td>
</tr>
<tr>
<td>Note:</td>
<td>As application is not inherited, you must have separate groups for separate applications.</td>
</tr>
<tr>
<td>Username</td>
<td>The administrator user name for the Ricoh device.</td>
</tr>
<tr>
<td>Password</td>
<td>The administrator password for the Ricoh device.</td>
</tr>
<tr>
<td>Application</td>
<td>A DRS application with Ricoh SOP as its <strong>Application Type</strong>. When a device is in a group, this property setting is always inherited the group and does not appear for a device.</td>
</tr>
<tr>
<td>Device Group</td>
<td>Click a group name in this box to change group membership. When a device is a member of a group it can optionally inherit device settings defined for the group. This allows you to simultaneously manage settings for multiple devices. Select the [Devices] option in this list to remove a device from group membership and move it to the root folder in the Devices pane. This option is not visible while you are configuring options for a new device.</td>
</tr>
<tr>
<td>Remote Install Password</td>
<td>The remote password for the Ricoh device. This password is required for uploading the Ricoh PCC 5.1 installation package to a Ricoh SOP device.</td>
</tr>
<tr>
<td>MFP TLS (http/https)</td>
<td>Specifies whether the device is configured to use TLS to communicate with the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong> when the device is configured to use TLS (HTTPS).</td>
</tr>
<tr>
<td></td>
<td>• <strong>False</strong> when the device is configured to not use TLS (HTTP).</td>
</tr>
<tr>
<td>Enable Debug Log</td>
<td>Specifies whether you want to enable debug logging:</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Server Connections Timeout</strong></td>
<td>Specifies the timeout used by DRS when making configuration and installation calls to the device such as SP modes and deployment of the Kofax client. Default is 60.</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>When deploying native device applications, you can specify the correct device type to ensure only supported functionality is deployed to the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>C306/406</strong> for specific model C306/406</td>
</tr>
<tr>
<td></td>
<td>• <strong>MFP</strong> for every other Ricoh Multi-Function Printer device</td>
</tr>
<tr>
<td></td>
<td>• <strong>SFP</strong> for SP C840DN, SP C842DN and SP 8400DN Ricoh Single-Function Printer devices (not supported for AutoStore)</td>
</tr>
<tr>
<td><strong>Authentication Screen</strong></td>
<td>Presents the authentication screen a user will see when they walk up to a device that is setup with Authentication. Available options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Welcome</strong> screen (default)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Logon</strong> screen.</td>
</tr>
<tr>
<td><strong>Updating Assets and Workflows</strong></td>
<td>On initial installation of the Ricoh SOP client and configuration of the Ricoh device, it is recommended that you perform a <strong>Full Install</strong> action. A <strong>Full Install</strong> installs the client on the device, configures the device (updating SP modes), performs asset and workflows sync and installs the Scan GUI Service.</td>
</tr>
<tr>
<td></td>
<td>To update an asset (logo image, welcome image, welcome text) at any time following an initial full install, perform a <strong>Sync Assets</strong> action.</td>
</tr>
<tr>
<td></td>
<td>To update customized workflows, at any time following an initial full install, perform <strong>Sync Workflow Buttons</strong> action.</td>
</tr>
<tr>
<td></td>
<td>To update asset(s) and workflows at the same time, perform both <strong>Sync Assets</strong> and <strong>Sync Workflow Buttons</strong> actions.</td>
</tr>
<tr>
<td></td>
<td>On completion of all sync actions, perform <strong>Configure and Reboot</strong> action in order for customized workflows to be displayed on the <strong>Welcome</strong> screen.</td>
</tr>
</tbody>
</table>

---

**Option** | **Description**
---|---
**Device Type** | When deploying native device applications, you can specify the correct device type to ensure only supported functionality is deployed to the device:
  - **C306/406** for specific model C306/406
  - **MFP** for every other Ricoh Multi-Function Printer device
  - **SFP** for SP C840DN, SP C842DN and SP 8400DN Ricoh Single-Function Printer devices (not supported for AutoStore)

**Authentication Screen** | Presents the authentication screen a user will see when they walk up to a device that is setup with Authentication. Available options:
  - **Welcome** screen (default)
  - **Logon** screen.

**Updating Assets and Workflows** | On initial installation of the Ricoh SOP client and configuration of the Ricoh device, it is recommended that you perform a **Full Install** action. A **Full Install** installs the client on the device, configures the device (updating SP modes), performs asset and workflows sync and installs the Scan GUI Service.
  To update an asset (logo image, welcome image, welcome text) at any time following an initial full install, perform a **Sync Assets** action.
  To update customized workflows, at any time following an initial full install, perform **Sync Workflow Buttons** action.
  To update asset(s) and workflows at the same time, perform both **Sync Assets** and **Sync Workflow Buttons** actions.
  On completion of all sync actions, perform **Configure and Reboot** action in order for customized workflows to be displayed on the **Welcome** screen.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign as Home Key Application</td>
<td>Specifies whether the Ricoh PCC 5.1 is invoked by the <strong>Home</strong> key on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong> assigns the client as a home key application on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>False</strong> does not assign the client as a home key application on the device.</td>
</tr>
<tr>
<td></td>
<td>This setting is available for with or without Authentication for the different servers, as displayed in the table <em>Availability of the &quot;Home Key&quot; and &quot;Scan Preview&quot; options</em> on page 57.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Home Key functions require the latest firmware from Ricoh.</td>
</tr>
<tr>
<td>Scan Preview</td>
<td>Specifies whether the Scan preview option is available on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong> makes the Scan preview option available on the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>False</strong> does not make the Scan preview option available on the device.</td>
</tr>
<tr>
<td>Application Package</td>
<td>Select an application package from this list. The selected application package is downloaded to a device by the <strong>Install</strong> action. List items are populated by the uploaded files specified on the <strong>Files</strong> tab. PCC 5.1 installation packages are downloaded from the Equitrac Partner Portal or from the Web Licensing Portal. See <em>Prepare Device Registration Service for use with AutoStore and Equitrac deployment</em> on page 18 for information about how to add a PCC 5.1 installation package to DRS.</td>
</tr>
<tr>
<td>Customize Assets</td>
<td>Specifies whether you want to customize assets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>True</strong> makes the Customize Assets option available on the device. If selected, additional fields appear below.</td>
</tr>
<tr>
<td></td>
<td>• <strong>False</strong> does not make the Customize Assets option available on the device.</td>
</tr>
<tr>
<td></td>
<td>Additional fields:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Application Logo</strong> drop-down list (required):</td>
</tr>
</tbody>
</table>
|                            | Allows you to select relevant image file. Supported file formats: JPG, JPEG, PNG and
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome Screen Image drop-down list (required)</td>
<td>Allows you to select relevant image file. Supported file formats: JPG, JPEG, PNG and BMP. Required Image resolution (WxH) is 174px x 174px.</td>
</tr>
<tr>
<td>Customize Welcome Screen Text field</td>
<td>If True is selected, additional field appear below.</td>
</tr>
<tr>
<td>Welcome Screen Text field</td>
<td>Allows you to enter your Welcome screen text (maximum allowable length of 60 characters from the template).</td>
</tr>
<tr>
<td>Customize Workflow Buttons</td>
<td>Specifies whether you want to customize workflow buttons.</td>
</tr>
<tr>
<td>Workflow Application selection fields</td>
<td>Allows you to configure native and extended applications (MFP). This allows you to configure and control deployment of native device functions (copy, fax, scan, Cloud Apps, and GlobalScan NX) to a single device or multiple devices. Print and Scan transactions performed using Ricoh Cloud Apps are not tracked using the Ricoh SOP 1.1 client as this is not a supported configuration.</td>
</tr>
</tbody>
</table>

Note:
- You can add or configure the following shortcuts with both DRS 7.13 and Equitrac System Manager: Quick Scan, Quick Copy and Quick Fax workflows.
- You can also configure the following shortcuts in DRS 7.13 only: Scanner,
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax, Copy, Cloud Apps, and GlobalScan NX.</td>
<td>However, System Manager can only configure Quick Scan, Quick Copy and Quick Fax.</td>
</tr>
<tr>
<td>• Duplicate shortcuts are not filtered out.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Function Access Control (FAC) will not restrict access to extended Ricoh device applications, such as GlobalScan NX and Ricoh Cloud Apps.

### Availability of the "Home Key" and "Scan Preview" options

Availability of these options is determined as follows:

<table>
<thead>
<tr>
<th>Servers and authentication</th>
<th>Home Key</th>
<th>Scan preview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equitrac-Auth ON</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>AutoStore-Auth OFF</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>Equitrac-AutoStore-Auth ON</td>
<td>Available</td>
<td>Available</td>
</tr>
</tbody>
</table>

**Note:** The Home Key option is supported with the latest firmware from Ricoh.

### Ricoh SOP Device Registration Device Status

When a device is selected on the **Device** tab on the Device Registration Service client web page, the **Status** bar in the **Details** pane displays the current device status for the Ricoh PCC 5.1 application and scan GUI service. Click the refresh button on the **Status** bar to display the current status for a device:

- **Device not reachable** if the IP address or the host name is not valid or the device is currently not visible on the network.

### Ricoh PCC 5.1 Application Status

<table>
<thead>
<tr>
<th>Ricoh PCC 5.1 Application Status</th>
<th>Scan GUI Service Status</th>
<th>Status Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>Installed</td>
<td>Installed; Version: Client: version - Scan GUI Service: version</td>
</tr>
<tr>
<td>Ricoh PCC 5.1 Application Status</td>
<td>Scan GUI Service Status</td>
<td>Status Message</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Installed</td>
<td>Not installed</td>
<td>Installed; Version: Client: version - Scan GUI Service: Not installed</td>
</tr>
<tr>
<td>Installed</td>
<td>Error</td>
<td>Installed; Version: Client: version - Scan GUI Service: Error message</td>
</tr>
<tr>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Not Installed</td>
<td>Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Error</td>
<td></td>
<td>Error message</td>
</tr>
</tbody>
</table>

**Files Tab**

The Files tab in the Device Registration Service web client lists available Ricoh PCC 5.1 installation packages for devices. A package in this list may be specified in the DRS device configuration for a Ricoh PCC 5.1.

Download the installation package in ZIP format from the Equitrac Partner Portal or from the Web Licensing Portal.

Upload package files one at a time using the Upload button on the Files tab in Device Registration Service web client. Images to be used for customizing the Welcome screen must also be uploaded here. The file type restriction would also be validated here, with message listing the allowed extensions shown upon errors.

**Note:** 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 MFP based on the device configurations. The Administrator can additionally also install the latest version of the client, or a previous version (until that version is retired or is not supported).

The files listed in the following table are expanded from the ZIP file.

<table>
<thead>
<tr>
<th>Group</th>
<th>Contents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ungrouped</td>
<td>ScanExample.zip</td>
<td>Files that are not specified in XML group file.</td>
</tr>
<tr>
<td>Ricoh SOP (&lt;version number&gt;)</td>
<td>RSOP_&lt;version number&gt;.xml</td>
<td>Package metadata file for version number.</td>
</tr>
<tr>
<td></td>
<td>SmartScanEx_&lt;version number&gt;.zip</td>
<td>Smart scan (GUI services) for other (including A3) devices. Used for all devices of type MFP.</td>
</tr>
<tr>
<td></td>
<td>SimpleScanEx_&lt;version number&gt;.zip</td>
<td>Simple scan (GUI services) for A4 devices. Used only for device types 306/406 devices.</td>
</tr>
<tr>
<td></td>
<td>Kofax-RSOP-authOff-&lt;version number&gt;.zip</td>
<td>Client application v1.1 without authentication.</td>
</tr>
<tr>
<td></td>
<td>Kofax-RSOP-authOn-&lt;version number&gt;.zip</td>
<td>Client application v1.1 with authentication.</td>
</tr>
</tbody>
</table>

To upload files for a single group, make sure that you upload all of the files listed for the group.

Note: Device types must be installed separately for group (MP C306/MP C406) install. If using Inherit Properties from Group, all device must be the same device type. Different devices can also be mixed but the Inherit Properties from Group option must be unchecked.

After you upload files, you can view the files by selecting Ricoh SOP in the Device Type box on the Files tab. A named group can be selected for the Application Package option in the device settings. This settings determines the files that are installed on the MFP that is pointed to by the device Address option.

CAUTION: Customization templates, installed as part of the DRS installation, are required for certain customized features. These templates should not be removed from the Files tab in the DRS web client. Ensure that files (RicohSOP-Assets-Customization-<version_number>.zip and RicohSOP-Workflow-Buttons-Customization-<version_number>.zip, located at C:\Program Files \Nuance\Device, are backed up post-DRS installation to a secure location.
Application types
Tables in this topic show applications that can be created for different packages.

AutoStore and Equitrac

<table>
<thead>
<tr>
<th>Kofax Application</th>
<th>Client Installed</th>
<th>AutoStore Server TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equitrac-Autostore</td>
<td>Auth ON</td>
<td>OFF</td>
</tr>
<tr>
<td>Equitrac-Autostore</td>
<td>Auth ON</td>
<td>OFF</td>
</tr>
<tr>
<td>Equitrac-Autostore</td>
<td>Auth OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>Equitrac-Autostore</td>
<td>Auth OFF</td>
<td>ON</td>
</tr>
</tbody>
</table>

Ricoh PCC 5.1 Actions Reference
Actions that can be performed from the Device Registration Service for a Ricoh PCC 5.1 device. An action can be performed on a single device or on all devices in a group.

Note: When DRS is performing a Quick Install or Full Install action of Ricoh PCC 5.1 device(s), or when such action has already been queued for execution, it is not recommended to modify the device configurations or the associated application profiles as it could interfere with the ongoing installation process and lead to unpredictable results and/or action failures. Likewise, when a Sync Assets or Sync Workflow Buttons action is being performed or queued, modifications to settings of the respective feature must be avoided.

To perform an action, first select a device on the Device tab in the Device Registration Service web console. Then, in the box at the top of the Details pane, click an available action to perform on the device and click the run button. This includes the following entries:
### Action History entry

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Message</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Success</td>
</tr>
<tr>
<td>Device</td>
</tr>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Return Code</td>
</tr>
</tbody>
</table>

You can follow deployment status feedback under **Action History**.

To perform an action on all devices in a group, first select the group folder on the **Device** tab, and then run the action.

### Action

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Install</td>
</tr>
<tr>
<td>Sync Assets</td>
</tr>
<tr>
<td>Sync Workflow Buttons</td>
</tr>
<tr>
<td>Quick Install</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
</tbody>
</table>

**Uninstall**

Uninstalls the Ricoh PCC 5.1 on the device. For more information, refer to *Uninstalling Client Using DRS* on page 27.

**Get device settings**

Gets current SP Mode settings on the device. Running this Action logs SP Mode settings and their values to a properties file (with the `.properties` extension). The default path to these properties files is:

```
C:\Program Files\Nuance\Device Registration Service\Service\Plugins \RXOP-SOP\CLITools\output
```

The file name of each log includes the IP address of the device followed by an underscore (_) and a Universal Time (UT) date-time stamp (**YYYYMMDDHHMMSS**). For example:

```
10.56.59.31_20160802221258.properties
10.56.59.35_20160802221451.properties
10.56.59.35_20160805204754.properties
```

Each file first lists the day, month, date, local time, time zone and year followed by one property setting and value per line in the following format:

```
#Fri Aug 05 16:48:39 EDT 2016
adminAuthKey.file.tools=false
adminAuthKey.network.file=false
adminAuthKey.machine.general=false
adminAuthKey.file=false
userAuthDocumentServer=1
...
```

The actual settings and values listed in the file depend on the device.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Set device settings**     | This action is to be used for advanced troubleshooting purposes only.  
This action sets configurations that were not completed by **Full Install** or **Quick Install** actions *(or Install and Reboot and Configure and Reboot actions)*.  
Run this action if you get the following warning (return code = 1) on completion of either the **Install and Reboot** or the **Configure and Reboot** action:  
Warning: Some configurations not set |
| **Reboot**                  | Restarts the MFP.                                                                                                                            |
| **Install and Reboot**      | This action is to be used for advanced troubleshooting purposes only.  
This action first uninstalls any package already installed on the MFP, then installs the package associated with the device configuration, sets required SP mode, and then restarts the MFP. The reboot may take some time to complete.  
**Note:** Install and Reboot action removes existing Home Key setting and if client needs to be assigned to the Home Key, a reconfiguration is needed.  
Run the **Configure and Reboot** action after you complete this action.  
**Note:** This action will install the ScanEX. |
| **Configure and Reboot**    | This action is to be used for advanced troubleshooting purposes only.  
Updates device configuration for the Ricoh package installed on the device and then restarts the MFP.  
This action must be run after you complete the **Install and Reboot** action.  
The device will be rebooted two times when you run this action. The Action initially tries to set SP Mode settings to their default values and afterwards applies the new values, including whether to associate the Home key with the client, that have been specified |
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in the Device settings. Warnings that settings were not configured indicates that the Action was unable to apply a setting, which you may choose to manually configure on the physical device.</td>
</tr>
</tbody>
</table>

**Ricoh PCC 5.1 Return Codes**

Ricoh PCC 5.1 return codes appear for device actions that you perform through Device Registration Service.

The following return codes may appear for Ricoh PCC 5.1 history items in the **Action History** panel in the Device Registration Service Web Client.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Successfully installed.</td>
<td>Configuration successfully completed.</td>
</tr>
<tr>
<td>1</td>
<td>Successfully installed. Warning: Some configurations not set.</td>
<td>Configuration successfully completed with message: Warning: Some configurations not set</td>
</tr>
<tr>
<td>100</td>
<td>Successfully installed.</td>
<td>Client package is installed.</td>
</tr>
<tr>
<td>500</td>
<td>Unknown error. Please check Logs folder for details.</td>
<td>General error.</td>
</tr>
<tr>
<td>501</td>
<td>Product not installed.</td>
<td>Application not installed on device.</td>
</tr>
<tr>
<td>503</td>
<td>Device not reachable.</td>
<td>Device unreachable or incorrect admin password.</td>
</tr>
<tr>
<td>603</td>
<td>Request unauthorized.</td>
<td>Produced when the device has been configured by another DRS instance, and thus locked into that instance. To switch to using the current DRS instance, client must be reinstalled.</td>
</tr>
<tr>
<td>605</td>
<td>Configuration servlet unresponsive.</td>
<td>Produced when DRS is unable to establish a working connection with the configuration servlet. Installation and wiring configuration actions depend on that servlet to function correctly.</td>
</tr>
<tr>
<td>Return Code</td>
<td>Message</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>606</td>
<td>Action not supported by current configuration.</td>
<td>Produced when intended action is unavailable given the current configuration.</td>
</tr>
</tbody>
</table>

**Action Status Codes**
The codes in this topic may be displayed in the DRS Action History pane at the bottom of the DRS window after completing an action.

<table>
<thead>
<tr>
<th>Unified Client App status</th>
<th>Scan GUI Service status</th>
<th>DRS status message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>Installed</td>
<td>Installed; Version: Client: 1.30.184 – Scan GUI Service: 1.02.00</td>
</tr>
<tr>
<td>Installed</td>
<td>Not Installed</td>
<td>Installed; Version: Client: 1.30.184 – Scan GUI Service: Not installed</td>
</tr>
<tr>
<td>Installed</td>
<td>Error</td>
<td>Installed; Version: Client: 1.30.184 – Scan GUI Service: Error message</td>
</tr>
<tr>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Not Installed</td>
<td>Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Error</td>
<td>-</td>
<td>Error message</td>
</tr>
</tbody>
</table>

**How to add a new Device profile**
This task explains how to create a Device profile. The profile enables you to manage Ricoh PCC 5.1, Equitrac, AutoStore and authentication settings on the Device through Device Registration Service.

1. Open **Device Registration Service** web client in a supported internet browser window if it is not open already.
2. On the toolbar, click **Devices**.
3. On the **Devices** toolbar, click the add button 📸.
4. In the **Name** box, enter a name to uniquely label the Device profile.
5. In the **Address** box, type an IP address for the device to associate it with this Device profile. This option is specific to a Device and does not appear when you configure properties for a Device group.
6. In the **Username** box, type the administrator user name for the Device. The user name is not required to complete a profile, but may be required to perform Actions on a device.
7. In the **Password** box, type the password associated with the user name.
8. In the **Application** box, select the application to associate with the Device profile.
   The **Application** setting specifies an application profile listed on the **Applications** tab. This defines the client type and server configurations for a device.

9. Edit settings for the Application Device type.

10. Click the save button on the **Add Device** toolbar.

**How to import Device Information**

This task explains how to import Device information into Device Registration Service from a CSV file.

The Application name and type specified for an imported Device must match the name and type of an existing Application on the DRS server where you want to import a Device. The import will fail for a Device if there is no Application on the server with the name and type specified in the DRS Device export file. In a DRS export file, the Application name and type correspond to the values specified in a Device entry by the **ApplicationProfile** and **DeviceType** fields.

1. In your web browser, open the Device Registration Service web client.

2. Click **Devices**.

3. Click the import button on the **Devices** toolbar and select the import method:

   - **Click**
   - **To**
   - **Import from file**
     - To import Device information from a CSV file that was previously exported Device information.
     - Browse to the CSV file and click **Upload**.

   The **Import Results** window shows success or failure for each Device that was specified in the DRS export file and a message for Devices that were not imported successfully.

4. Close the **Import Results** window after you review the results of the import.

5. If necessary, edit properties for imported Devices.

Imported Devices are always added to the root Devices folder. After you successfully import a Device, you can optionally drag it to a group folder with the same Application profile. For more information, see the **DRS Installation Guide**.

**Appendix: Additional Configuration Instructions**

**Troubleshooting**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| 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:  
• **Enabling Home Key Settings** on page 70 |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to manually configure SP Modes on a device.</td>
<td>SP Modes are normally configured by running on a device.</td>
<td>You can manually configure SP Modes on a device using the following procedure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring SP Mode Settings on page 73</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tip: Also check if Baseline installation is an option and if it is inadvertently left as False.</td>
</tr>
<tr>
<td>When accessing workflows, the user cannot perform scan and You do not have the privileges to use this function message appears.</td>
<td>SP Modes are set incorrectly.</td>
<td>You can manually configure SP Modes on a device using the following procedure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring SP Mode Settings on page 73</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must set Admin. Authentication to Off.</td>
</tr>
<tr>
<td>Not able to log in when switching from Equitrac only (Auth On) to AutoStore only (baseline set to false).</td>
<td>There is no indication from DRS that the Service Provider (SP) modes are set wrong.</td>
<td>You must check SP modes when baseline is set to OFF.</td>
</tr>
<tr>
<td>Need to disable Print from USB on the MFP.</td>
<td>Print from USB is not tracked and no quotas or limits are applied.</td>
<td>You can manually disable print from USB/memory stick using the following procedure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disabling Print from USB on page 72</td>
</tr>
<tr>
<td>Need to replace the DRS.</td>
<td>The DRS crashes and cannot be used any longer or similar.</td>
<td>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.</td>
</tr>
<tr>
<td>Issue</td>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Need to replace the DCE.</td>
<td>The DCE crashes and cannot be used any longer or similar.</td>
<td>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 <strong>Configure and Reboot</strong> 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.</td>
</tr>
</tbody>
</table>

- 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. Change the TLS settings on the Controller or change the TLS settings on the Controller.
2. Reboot the device.

For detailed instructions, see **Changing the TLS Settings** on page 77.

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 screen.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user receives an error when running <strong>Full Install, Quick Install</strong> with either Asset or Workflow Customization enabled or when trying to deploy the customization package or perform an <strong>Asset Sync</strong>.</td>
<td>This issue may occur due to an incorrect <strong>DRS Service URI</strong> setting which does not respect the TLS configuration of DRS.</td>
<td>If DRS is configured with TLS enabled, then the URI needs to start with HTTPS. Otherwise, it should start with HTTP.</td>
</tr>
<tr>
<td>The user receives the error <strong>Failed to install the customization package</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The user receives a similar error for <strong>Asset Sync</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An error message occurs when selecting <strong>Refresh Status</strong>.</td>
<td>Occurs due to a missing application package.</td>
<td>Ensure that complete application package is uploaded.</td>
</tr>
<tr>
<td>After performing uninstallation, the device authentication settings were not reset completely in DRS.</td>
<td>Administrator authentication is set to ON.</td>
<td>Administrator authentication must be manually set to OFF to fully put the device back into factory settings.</td>
</tr>
</tbody>
</table>

**Property files generated during action with Equitrac as print manager**

**Equitrac-Home=True and Scan=True**

**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

**Equitrac -Home=False and Scan=False**

**Install and Reboot**
- deviceconfig_tracking_off.properties
- default_deviceconfig.properties
**Equitrac -Home=False and Scan=False**

- `deviceconfig_to_auth_on_preinstall.properties`

**Configure and Reboot**

- `deviceconfig_auth_on.properties`

**Uninstall**

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

---

**Enabling Home Key Settings**

Use this procedure to manually enable the Home key when the Assign as home key application option in the Device settings fails to enable the Home key on an MFP.

The home key is disabled by default. This procedure describes how to enable this feature.

⚠️ **Important:** This procedure requires working in Service Mode, which is typically performed by a Ricoh technician.

1. On the SOP device, open the **Printer** application.
2. Enter SOP Service Mode mode to complete the succeeding steps.
   
   If the SOP Service Mode screen does not appear, the foreground app may be covering the SOP Service Mode screen. Try closing the foreground app by pressing the **Return** or **Home** button.
3. Press **SYSTEM**.

![Figure 4: SOP device System Service settings](image)

4. Press **Screen Device Settings**.
5. Press **Home Key Settings**.

   This displays the **Home Key** settings screen.
6. Press **Home Key Application**.

7. On the **Home Key Application** screen, select the application that starts when a user presses the **Home** key.

   By default, this screen lists the Launcher, which is the Ricoh **Home** key application.

8. Log out of Service Mode.

9. Reboot the device.
Disabling Print from USB
Use this procedure to manually disable print from USB/memory stick on Ricoh devices.

Print from Memory Storage Device is enabled by default. This procedure describes how to disable this feature.

1. Login 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.

Configuring Common Access Card Authentication Solution

Ricoh PCC 5.1 supports Ricoh Common Access Card (CAC) v4 that has authentication capabilities and prevents unauthorized access to MFPs with AutoStore and Equitrac installed.

A US Department of Defense (DOD) CAC authentication solution provides US federal government customers with the ability to use their exiting ID cards with the solution, increasing user satisfaction, security and productivity.

The CAC authentication solution provides the following benefits:
• Easy to use turn-key solution
• Holders of a valid CAC can perform copy, scan, fax, and/or document server functions
• Card is inserted into CAC reader connected to MFP and PIN is entered
• Upon successful authentication the multifunction device is unlocked for use
• Scanning is restricted only to address book users and embedded destinations to prevent anonymous scan-to functions
• After authentication user is automatically registered in MFP’s address book.

For US Government accounts the embedded client can use CAC cards for user authentication when configured with Equitrac. In this instance, Equitrac will operate when Authentication is set to False in the DRS application profile.

**Note:** The Authentication setting is only visible if a Print Manager is selected.

To use CAC authentication when Equitrac 5.6 or later is configured as the authentication provider:

1. Install CAC.
2. Register and configure Ricoh MFP devices using CAC authentication.
3. Swipe your card and enter your CAC PIN code to log in.

**Note:** The following Equitrac features are not supported with CAC login: Function Access Control (monochrome and color copy, scan and fax permissions and copy stop enforcement), Release All at login, Release First at login, Billing Codes at login, and Copy Rules (limit access).

**Note:** CAC does not support Equitrac multi-DCE environment.

### Setting Alternate Primary PIN as UPN

Equitrac offers an optional alternate primary PIN that the user can enter instead of the primary PIN. Alternate primary PIN can be used for an additional level of security as it serves as another primary PIN for the user.

Open Equitrac System Manager and go to **Configuration → Users** and click on a user. In **Properties of…** dialog box, set the Alternate primary PIN as **UPN** from CAC server.

### Configuring and Using DRS for a CAC Device

#### Selection on the Ricoh SOP device – DRS Web client

2. When selecting an **Auth Off** application in device, a **Baseline Installation** option is shown.
3. Make sure you select the **Baseline Installation** as **false**.

**DRS action steps**

1. Select the device which has CAC on it.
2. Run action “Full Install”.

**Note:** You must set Home key to **System Home** and not **Kofax Embedded for Ricoh SOP** in CAC environment.

### Configuring SP Mode Settings

This procedure describes how to configure Service Provider (SP) modes. The SP Mode settings are normally configured by the **Configure and Reboot Action** Action. You can use this procedure to configure settings.
manually when a device does not allow Device Registration Service to configure SP Mode settings through the Action.

⚠️ **Important:** This procedure requires working in Service Mode, which is typically performed by a Ricoh technician.

1. On the Home screen, go to Printer (scroll screen) and press the Printer icon.
2. Enter SOP Service Mode mode (press Reset, then 806182 and then press and hold C) to complete the succeeding steps.
3. Press System SP to enter SP Mode (press 0 to change bit from 0 to 1, then # to save).
4. Press SP Direct.

![SP Mode Settings](image)

5. In SP Direct type 5401230 on keypad, then type #.
6. Set the LSB to 1 by pressing zero 0 (Note: Value of the bit at index 0 is changed when pressing 0) on keypad in CAC configuration.
   The last digit should now be 1.

   Note: As for MFP and MPC306/MPC406 devices: SP-5420 must be set to 1 for CAC (in order for copy to work) and 0 for none-CAC installation (in order for copy to track).

7. Type # to save your changes.

The label **LDAP authentication** in step 8 will be changed to **Custom authentication** after the machine is rebooted.

10. Configure the LDAP server, as described in the *Equitrac Express Administration Guide*.

11. Enable **Machine action when limit is reached** in **System Settings** (Administration tools).

   Set this to **Stop Job** or **Finish Job and Limit**.
12. Enable the network by setting **User tools > Login > Exit > Screen Features > Interface Settings > Set to Machine Network.**

![Image of Machine Administrator interface]

**Note:** The authentication logic customization feature becomes valid when the following condition is satisfied.

13. Turn on **Tracking Permission.**

![Image of System Settings interface]

### Changing the TLS Settings

Changing the TLS settings can be performed on JavaVM and on the Controller using the Web Image Monitor. The Web Image Monitor 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. Follow these steps to open the Web Image Monitor:

1. Open a web browser and enter http://<MFP IP Address> in the **Address** field. The device web page opens.
2. Click **Login** and enter your administrator User Name and Password.
Changing the TLS settings on JavaVM

1. Open the Web Image Monitor and log in.
2. Go to Device Management > Configuration > Extended Feature Settings > Administrator Tools and change the settings.

3. Click Apply

Changing the TLS settings on the Controller

1. Open the Web Image Monitor.
2. Go to Device Management > Configuration > SSL/TLS and change the settings.
3. Click OK.

**Paper Type Setup**

If you notice that your tracking and pricing for copies is different than expected, please ensure you have the paper type set to Tray 1 and Plain Paper. Follow these steps:

1. Open a web browser and enter `http://<MFP IP Address>` in the Address field. The device web page opens.
2. Click **Login** and enter your administrator User Name and Password. The Web Image Monitor page opens.
Note: The Web Image Monitor page may differ in appearance and location of functions by device. The basic functionality remains the same.

5. Under Tray 1, from the Paper Weight drop-down list, select any of the Plain Paper options.
6. If you are using the Bypass Tray, ensure it is also using this setting.
7. Click OK.

DCE Pinning

Purpose

DCE pinning services are used to reduce a man-in-the-middle attack (MITM) and provide additional security by pinning your client to a specific DCE that belongs to your configuration for the duration of that configuration.

Details

This additional security is achieved through certificate pinning where you are bound to the DCE using the certificate that the DCE provides upon connection and use it to validate the trust of subsequent communications with that server.

Note: You are not allowed to change the DCE endpoints until you reconfigure the client application again (until then, you are bound to the DCE you have configured initially).

Possible failures

You may receive connection failures if the following possibilities occur:

- Failure to create JavaKeystore (JKS) for any reason (example: HDD issues)
- Failure to write to the JKS for any reason (example: corrupt file, HDD issues)
• Invalid certificate is provided by the DCE (MITM server, DCE has changed its certificate sometime after).

**Recovery**

Validate if the DCE you are unable to connect to has the same certificate (since your initial client application configuration) in order to eliminate a possible MITM attack.

To recover from connection issues related to DCE pinning that are not related to hardware failures (HDD):

• Perform a **Configure and reboot** action for a new configuration using the DRS, or
• Perform a **Full Install** action.

**Note:** New configuration means that either a DCE endpoint has changed (IP, FQDN) or DCE endpoints have been added or removed from the list.

**Reset**

To reset DCE pinning, only **Uninstall** and **Full Install** actions must be used.

**DRS Authorization Key**

This security feature has been added to DRS where additional security between the DRS application and the device is enabled using an authorization key. This additional security check will confirm that only the initial DRS instance that was used to deploy or configure the device can be used to update the configuration of the embedded client on the device.

The DRS Authorization Key is pinned to a device or group of devices when a **Full Install** is performed, the DRS Authorization Key is pinned to the device the first time the device is configured within the DRS application and is kept on the device and this authorization key cannot be changed. If any DRS configuration actions, such as Sync Assets, Sync Workflow Buttons or Configure and Reboot do not contain the pinned authorization key, the request will fail and failure message will be displayed in DRS.

The DRS Authorization Key is stored in the DRS database and it is uniquely generated every time a device is added into the same used DRS application. If the same device is added to another DRS instance, then the DRS Authorization Key will be different.

**Note:** If TLS is not enabled on the device, the DRS Authorization Key pinning will not be engaged. Once the device is pinned to a given DRS instance, only that DRS instance can perform the following actions of the install and configuration options: **Sync Assets**, **Sync Workflow Buttons** and **Configure and Reboot**.

**Note:** If you go from TLS enabled to TLS disabled, the Authorization Key Pinning must be reset.

**Note:** If want to move the control from one DRS to another DRS, the second DRS must run **Full Install**.

**Note:** In order to reset Authorization Key pinning, DRS must run **Full Install** or **Uninstall**.

**System Configuration Settings**

**CAUTION:** When installing Equitrac, you **must** use the settings listed under **Auth On**. Auth Off settings handle other configurations of Ricoh PCC 5.1.

<table>
<thead>
<tr>
<th>Configuration Path</th>
<th>Auth On</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service &gt; Screen Features</td>
<td>Either</td>
<td></td>
</tr>
<tr>
<td>&gt; Screen Device Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Path</td>
<td>Auth On</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Home key settings &gt; Home key application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service &gt; Screen Features &gt; Screen Device Settings &gt; Screen device always-connection Setting</td>
<td>Active</td>
<td>Needed for card reader auto-wakeup</td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; Administrator Authentication Management &gt; Admin. Authentication</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; Administrator Authentication Management &gt; Available Settings</td>
<td>Administrator Tools</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; Enhanced Print Volume Use Limitation &gt; Stop Printing</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; Enhanced Print Volume Use Limitation &gt; Tracking Permission</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; Machine action when limit is reached</td>
<td>Stop Job</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; User Authentication Management &gt; Custom Auth &gt; Available Functions Copier</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; User Authentication Management &gt; Custom Auth &gt; LDAP Servers</td>
<td>Not Programmed</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Path

<table>
<thead>
<tr>
<th>Configuration Path</th>
<th>Auth On</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; User Authentication Management &gt; Custom Auth &gt; Other Functions</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; User Authentication Management &gt; Custom Auth &gt; Printer Job authentication</td>
<td>Entire</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Machine Features &gt; System Settings &gt; Administrator Tools &gt; User Authentication Management &gt; OFF</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>User Tools &gt; Screen Features &gt; Interface Settings</td>
<td>Machine Network</td>
<td></td>
</tr>
</tbody>
</table>

### Restarting the Device

A restart of the device is recommended after installing or uninstalling new software. Follow these steps:

1. Locate the physical on/off switch of the device, then press until the device screen displays a dialog indicating the device is shutting down.
   
   You can then release the button. The shutdown process may take as long as 7 minutes.

   **Note:** Once the screen shuts down, the device’s blue LED indicator light continues to flash. The device is not fully shut down until this light stops flashing.

2. Once the device is fully shut down, press the on/off button again. The screen indicates the startup is in progress.

Depending upon the device’s setup, the main display will either show the Ricoh PCC 5.1 login screen, or if the embedded solution is not installed, the standard Ricoh Smart Operation Panel Home screen with option icons.

### Supporting a Mixed Fleet Environment

If you have an existing fleet of PCC 4 devices and are adding PCC 5.1 to your environment, refer to the *PCC 4 Setup Guide* for all PCC 4 devices.