Unified Client for Ricoh SOP Deployment Guide for AutoStore

Deployment Guide

Version 1.1
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>March 18, 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 Nuance Communications, Inc. All rights reserved.

All rights to this document, domestic and international, are reserved by Nuance Communications, Inc. 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 Nuance Communications, Inc.

Trademarks

AutoStore, Equitrac, Nuance, Output Manager and Unified Client are either registered trademarks or trademarks of Nuance Communications, Inc., 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

Unified Client for Ricoh SOP 1.1 Deployment Guide for AutoStore....5

Overview of the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 for AutoStore Deployment.................................................................5

Deploying Nuance Unified Client for Ricoh Smart Operation Panel 1.1 with AutoStore
  - Workflow Outline...........................................................................................................6
Requirements..........................................................................................................................6
Supported Languages..............................................................................................................6

Prepare for Deployment.........................................................................................................7
  Verify that your device is supported..................................................................................7
  Verify prerequisites...........................................................................................................7
  Get installer packages........................................................................................................9

Install and Configure the AutoStore Server........................................................................9
  Install AutoStore.............................................................................................................9

Set Up a Nuance Unified Client for Ricoh Smart Operation Panel 1.1 MFP........................9
  Configure the Ricoh MFP in Unified Client Environment....................................................9
  Install and configure the TLS certificates.......................................................................10
  Ensure that previous applications are cleared...................................................................11

Install Device Registration Service......................................................................................12
  Quick Setup Device Registration Service Instructions......................................................12

Set Up Your First AutoStore Capture Workflow.................................................................21
  License AutoStore...........................................................................................................21
  Configure Scan to Folder.................................................................................................21

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Device Settings...............24
  Application properties.......................................................................................................24
  Nuance Unified Client for Ricoh Smart Operation Panel 1.1 device properties..............25

Files Tab................................................................................................................................28

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Actions Reference.............31
  Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Return Codes....................34

Action Status Codes............................................................................................................35
  How to add a new Device profile....................................................................................36
  How to import Device Information.................................................................................36

Appendix: Additional Configuration Instructions.................................................................37

Troubleshooting....................................................................................................................37
  Device Configuration for AuthOff.....................................................................................38
  Configuring Common Access Card Authentication Solution............................................39
  Configuring SP Mode Settings.........................................................................................40
  Changing the TLS Settings...............................................................................................44
  DRS Authentication Key....................................................................................................46
  Restarting the Device.........................................................................................................47
Unified Client for Ricoh SOP 1.1 Deployment Guide for AutoStore

Overview of the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 for AutoStore Deployment

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 provides a unified client for capture and print management functionality on specific Ricoh-manufactured Multi-Function Printers (MFPs). When deployed to the MFP, Nuance Unified Client for Ricoh Smart Operation Panel 1.1 controls access to the MFP and acts as the gateway for Kofax functionality.

Figure 1: System architecture with AutoStore

This document will walk you through a clean installation procedure. Follow the steps provided here to be able to have an AutoStore Scan to Folder capture workflow configured on your Ricoh MFP device.
Deploying Nuance Unified Client for Ricoh Smart Operation Panel 1.1 with AutoStore - Workflow Outline

1. Prepare for deployment
   a. Verify that your device is supported
   b. Verify prerequisites
   c. Get installer packages (AutoStore, DRS and Nuance Unified Client for Ricoh Smart Operation Panel 1.1 client package)

2. Install the AutoStore server

3. Configure the Ricoh MFP
   a. Configure the device certificate on the device
   b. Ensure that SSL/TLS is enabled
   c. Verify that previous applications are cleared

4. Install and Setup Device Registration Service (DRS)
   a. Install and upload Nuance Unified Client for Ricoh Smart Operation Panel 1.1 client package into DRS
   b. Create and add application in DRS
   c. Add and configure the MFP device in DRS
   d. Install and register the Ricoh device using DRS in AutoStore-only deployment

5. Execute final actions
   a. Select and run action
   b. Locate the auto-added device and configure it in the AutoStore Process Designer

6. Create your first AutoStore workflow and verify installation
   a. License AutoStore
   b. Configure Send to Folder workflow
   c. Verify installation

Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<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 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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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
• Traditional Chinese
• French
• Polish

• Catalan
• German
• Portuguese (Brazil)

• Czech
• Hungarian
• Russian

• Dutch
• Italian
• Spanish

• Danish
• Japanese
• Swedish

• English
• Korean
• Thai

Note: The list of languages available on the client does not necessarily match languages available on the administrative web client.

Note: To be able to use a language's native character set, the Language Keyboard Input Setting should be appropriately set up in Screen Settings.

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

Before you begin, ensure that the following requirements are met for a single-server installation of AutoStore and Device Registration Service (DRS).

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></td>
<td>• 5 GB of <strong>hard disk space</strong> available (including SQL server and prerequisites)</td>
</tr>
<tr>
<td></td>
<td>• The <strong>CPU</strong> is <strong>4 x 2 GHz or greater</strong></td>
</tr>
<tr>
<td>✗</td>
<td>Check that the <strong>operating system</strong> is one of the following 64-bit ones:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 - Standard and Datacenter (enable ASP.NET for Microsoft .NET 4.5 or ASP.NET for Microsoft .NET 4.6. before installation)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 - Standard, Enterprise and Datacenter</td>
</tr>
<tr>
<td>Check</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that you have <strong>Administrative access rights</strong> to Windows on the server.</td>
</tr>
<tr>
<td>☐</td>
<td>Check that all <strong>required Windows updates</strong> are installed.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that <strong>Microsoft Windows Updates is turned ON</strong> while you are deploying AutoStore. This is necessary for the successful installation of Microsoft Windows Identity Foundation (TFS).</td>
</tr>
<tr>
<td>☐</td>
<td>Ensure that <strong>.NET Framework 3.5</strong> is installed on the server (to verify it, launch Server Manager &gt; select <strong>Local Server</strong> &gt; verify that .NET Framework 3.5 is listed under <strong>Roles and Features</strong>). If it is missing it will be installed as part of the AutoStore installation process.</td>
</tr>
<tr>
<td>☐</td>
<td>Ensure that <strong>Windows Identity Foundation 3.5</strong> is installed on the server (to verify it, launch Server Manager &gt; select <strong>Local Server</strong> &gt; verify that Windows Identity Foundation 3.5 is listed under <strong>Roles and Features</strong>).</td>
</tr>
</tbody>
</table>
| ☐     | 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**: 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  
  and **outgoing firewall exceptions** for ports 3350, 8753, 49629, 49630, 50083. (Note that port 3350 is configurable and you should update your firewall accordingly). |
| ☐     | Verify that IE Enhanced Security Configuration is turned OFF for Administrators in **IE Enhanced Security Configuration** (to access this, go to **Server Manager** > then select **Local Server**). |
| ☐     | Check that you have **all required components downloaded** and within easy reach (components and download locations are listed in the section below). |
| ☐     | If you are planning to use any AutoStore **Route component** that requires **client software**, ensure that this software is **installed** on your server machine before starting deployment. |
| ☐     | Verify that you have **Administrative access** to the **device**. |
Get installer packages

Download the client installation packages for AutoStore, the Unified Client for Ricoh SOP and DRS from the Web Licensing Portal (https://weblicense.nsius.com/). Select these products in the list under Software Download and Documents to access the packages.

1. Log in to the Web Licensing Portal.
2. Under Software Download and Documents, select AutoStore 7 or later from the product list. Note that you require AutoStore 7 SP5 or later for the product to work properly.
3. Download the executable file (AutoStore<version_number>.exe) as well as available documentation.
4. Under Software Download and Documents, select the product Device Registration Service (DRS). Download the executable DRS file (<version_number>-DeviceRegistrationService.zip) as well as available documentation.

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

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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1. 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.

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 Nuance AutoStore Installation Guide.

Set Up a Nuance Unified Client for Ricoh Smart Operation Panel 1.1 MFP

Configure the Ricoh 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 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.

### 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):

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.
Install Device Registration Service

Quick Setup Device Registration Service Instructions

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 and 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.

2. Upload Ricoh Client Package.
   a) Download the most recent version of Nuance Unified Client for Ricoh Smart Operation Panel 1.1 from the Web License Portal.
   b) Once the archive downloads, extract <version_number>-RicohSOPClient_<version_number>.zip. The archive contains the RicohSOP<version_number>.xml file.
   c) 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 Nuance Device Registration Service screen opens:

   ![Device Registration Service Screen]

   d) Select the Files tab.
   e) From the Device Type drop-down list, select Ricoh SOP.
   f) 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.
**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>RicohSOP_&lt;version_number&gt;.zip</td>
<td>RSOP_1_&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 devices, including A3 devices. Used for all MFP devices.</td>
</tr>
<tr>
<td></td>
<td>SimpleScanEx_&lt;version_number&gt;.zip</td>
<td>Simple scan (GUI services) for A4 devices. Used only for 306/406 devices.</td>
</tr>
<tr>
<td></td>
<td>Nuance&lt;build_number&gt; production_authOff_&lt;date&gt;.zip</td>
<td>Client application v1.1 with no authentication (example: Nuance_1.30.184production_authOff_2018-1-25.zip).</td>
</tr>
</tbody>
</table>

**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 the 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 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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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 None.

j) In the DRS Service URI field (required), enter the network address.

k) Click the Save button (保存) at the top of the Add Application screen.

4. Add the device in DRS.

a) Select the Devices tab.

b) Click the green (++) button at the top of the left 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. By default, the username is admin and the password is blank.

f) In the Application field, select the application you have created from the list.
g) In the **Device Group** field, select the existing device group from the list.

h) 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.

i) 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.

j) In the **Enable Debug Log** entry, select **True** or **False** (default).

k) In the **Device Type** drop-down list (required), choose between 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 **Scan preview** entry, select **True** or **False** (default).

n) 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.

o) In the **Baseline Installation** entry, select **True**.

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

5. **Install Nuance Unified Client for Ricoh Smart Operation Panel 1.1 client application onto the device.**

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 SOP application and scan GUI service. Click the refresh button on the **Status** bar to display the current status for a device:

The message shows **Device not reachable** if the IP address or the hostname is not valid or the device is currently not visible on the network.

a. From the drop-down list at the top of the **Details** pane, select one of the options depending on your preferences. For details, see **Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Actions Reference** on page 31. **Note**: To go back to default values for assets; you must set and resync.

b. Click the **Run Action** button. You can follow deployment status feedback under Action History.
The installation and registration action may take a few moments to complete. Once finished, a **Successfully completed** message appears in the **Action History** pane at the bottom of the screen.

---

**Upgrading from Ricoh SOP 1.0 to 1.1**

If you want to upgrade from Ricoh SOP 1.0 to Ricoh SOP 1.1, DRS must first be upgraded to version 7.13. DRS 7.12 does not support Ricoh SOP 1.0. The client version is strictly tied to its version of DRS. The process to upgrade to DRS 7.13 is straightforward but contains specific steps that must be taken.

**Upgrading from Ricoh SOP 1.0 to Ricoh SOP 1.1 in case the user has a local database**

To upgrade from Ricoh SOP 1.0 to Ricoh SOP 1.1, complete the following:

1. Upgrade to DRS 7.13.
   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. Copy the Database Upgrade Tool files, **NSi.DeviceManagement.Upgrade.exe** and **NSi.DeviceManagement.Upgrade.exe.config**, to the Service where you installed DRS. For example, C:\Program Files\Nuance\Device Registration Service\Service.

f. Right-click **NSi.DeviceManagement.Upgrade.exe**, and select **Run as administrator** to launch the Database Upgrade Tool.

g. When prompted, click **Run** to begin the upgrade process.

h. When you receive a **Completed successfully** message, the upgrade is complete. Click **Close**.

i. Start the DRS 7.13 service with the newly upgraded database.

**Note:** Optionally, instead of an in-place DRS upgrade, install DRS 7.13 on a separate supported workstation/server to deploy Ricoh SOP 1.1. After installing DRS 7.13, migrate the older DRS database to the new DRS workstation/server.


3. Install the latest Ricoh SOP 1.1 client using DRS 7.13 with a **Full Install** action.

Also note the following:

- Allow DRS 7.13 to uninstall Ricoh SOP 1.0.
- Do not allow DRS 7.13 to manage or install a Ricoh SOP 1.0 environment.
- Do not allow DRS 7.13 to upgrade or migrate an older DRS 1.0 environment.

**Upgrading from Ricoh SOP 1.0 to Ricoh SOP 1.1 in case a remote database is used**

To upgrade from Ricoh SOP 1.0 to Ricoh SOP 1.1, 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 cleared.

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.

![Device Registration System Database Upgrade Tool](image)

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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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**.

3. Go to page 2 and under **Administrator Authentication Management**, go to **User Management > Machine Management** and set **Admin. Authentication** to **Off**.

**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 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 *NSi 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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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 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.
Nuance Unified Client for Ricoh Smart Operation Panel 1.1
Device Settings

These sections describes how to configure a Nuance Unified Client for Ricoh Smart Operation Panel 1.1 device.

Application properties

A Device Registration Service application profile for the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 specifies connection information for an AutoStore 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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 application. You cannot change the application type for an existing application.

<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>Application Type</td>
<td>To create a new Nuance Unified Client for Ricoh Smart Operation Panel 1.1 application in DRS, choose Ricoh SOP for this option. 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>Capture Component</td>
<td>Specifies the capture component. Select:</td>
</tr>
<tr>
<td></td>
<td>• AutoStore</td>
</tr>
<tr>
<td>AutoStore Server Address</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>AutoStore Server Port</td>
<td>The port that the AutoStore server uses to communicate with clients.</td>
</tr>
<tr>
<td></td>
<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 3350.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoStore Server Use TLS</td>
<td>Select True or False. This setting should reflect your AutoStore server configuration. Verify it in the Preference tab of Nuance Unified Client for Ricoh Smart Operation Panel 1.1 component. By default, the AutoStore setting &quot;Use TLS&quot; is OFF. If you leave it as OFF, you should select False in DRS.</td>
</tr>
<tr>
<td>Print Manager</td>
<td>Specifies the print manager type. Select:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>DRS Service URI</td>
<td>The address to the DRS server:</td>
</tr>
<tr>
<td></td>
<td><a href="http://serverAddress:port/DeviceManagementRestService/">http://serverAddress:port/DeviceManagementRestService/</a></td>
</tr>
<tr>
<td></td>
<td>The default port number for this DRS service is 8755.</td>
</tr>
<tr>
<td></td>
<td>Note: The address in this field must be an IP address.</td>
</tr>
<tr>
<td></td>
<td>Note: If TLS is enabled for the DRS service, ensure you change http to https.</td>
</tr>
</tbody>
</table>

**Nuance Unified Client for Ricoh Smart Operation Panel 1.1 device properties**

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The IP address or hostname of a Ricoh device. Note: This is a device only parameter and will not be displayed when configuring parameters for a device group.</td>
</tr>
</tbody>
</table>
| **Inherit Properties from Group** | This option is visible only when a device is located in a group folder in the Devices pane.  
  - **True** specifies to use property settings for the group. The remaining property settings will be inherited from the group and unavailable for configuration here.  
  - **False** specifies to configure property settings separately for this device. The remaining settings will be available for configuration here except in their description.  
  Note: As application is not inherited, you must have separate groups for separate applications. |
<p>| <strong>Username</strong>           | The administrator user name for the Ricoh device.                                                                                          |
| <strong>Password</strong>           | The administrator password for the Ricoh device.                                                                                           |
| <strong>Application</strong>        | A DRS application with Ricoh SOP as its Application Type. When a device is in a group, this property setting is always inherited the group and does not appear for a device. In this case, select AutoStore. |
| <strong>Device Group</strong>       | 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. |
| <strong>Remote Install Password</strong> | The remote password for the Ricoh device. This password is required for uploading the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 installation package to a Ricoh device. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>• True when the device is configured to use TLS (HTTPS).</td>
</tr>
<tr>
<td></td>
<td>• False 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>• True</td>
</tr>
<tr>
<td></td>
<td>• False (default)</td>
</tr>
<tr>
<td>Device Type</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>• C306/406 for specific model C306/406</td>
</tr>
<tr>
<td></td>
<td>• MFP for every other Ricoh Multi-Function Printer device</td>
</tr>
<tr>
<td>Authentication Screen</td>
<td>Presents the authentication screen a user will see when they walk up to a device that is setup with Nuance Authentication. Available options:</td>
</tr>
<tr>
<td></td>
<td>• Welcome screen (default)</td>
</tr>
<tr>
<td></td>
<td>• Logon screen.</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>• True makes the Scan preview option available on the device.</td>
</tr>
<tr>
<td></td>
<td>• False 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 Install action. List items are</td>
</tr>
<tr>
<td></td>
<td>populated by the uploaded files specified on the Files tab. Nuance Unified Client for Ricoh Smart Operation Panel 1.1 installation packages</td>
</tr>
<tr>
<td></td>
<td>are downloaded from the Web Licensing Portal. See Quick Setup Device Registration Service Instructions on page 12 for information about how to add a Nuance Unified Client for Ricoh Smart Operation Panel 1.1 installation package to DRS.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Baseline Installation</td>
<td>Specifies baseline installation:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
</tbody>
</table>

**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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 application and scan GUI service. Click the refresh 🔄 button on the **Status** bar to display the current status for a device:

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

<table>
<thead>
<tr>
<th>Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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>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>
</tbody>
</table>

**Files Tab**

The **Files** tab in the Device Registration Service web client lists available Nuance Unified Client for Ricoh Smart Operation Panel 1.1 installation packages for devices. A package in this list may be
specified in the DRS device configuration for a Nuance Unified Client for Ricoh Smart Operation Panel 1.1.

Download the installation package in ZIP format 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.

**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>RicohSOP_&lt;version number&gt;.zip</td>
<td>RSOP_1_&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 devices, including A3 devices. Used for all MFP devices.</td>
</tr>
<tr>
<td></td>
<td>SimpleScanEx_&lt;version number&gt;.zip</td>
<td>Simple scan (GUI services) for A4 devices. Used only for 306/406 devices.</td>
</tr>
<tr>
<td>Group</td>
<td>Contents</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Nuance&lt;build number&gt;production_&lt;date&gt;.zip</td>
<td>Client application v1.1 with no authentication (example: Nuance_1.30.184production_authOff_2018-1-25.zip).</td>
</tr>
<tr>
<td></td>
<td>Nuance&lt;build number&gt;production_&lt;date&gt;.zip</td>
<td>Client application v1.1 with authentication (example: Nuance_1.30.184production_authOn_2018-1-25.zip).</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 only**

<table>
<thead>
<tr>
<th>Nuance Application</th>
<th>Client Package</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore only</td>
<td>Auth ON</td>
<td>ON</td>
</tr>
<tr>
<td>AutoStore only</td>
<td>Auth OFF</td>
<td>ON</td>
</tr>
</tbody>
</table>
**Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Actions Reference**

Actions that can be performed from the Device Registration Service for a Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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.

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. You can follow deployment status feedback under Action History. This includes the following entries:

<table>
<thead>
<tr>
<th>Action History entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Shows date and time.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies current action type information.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies current action message information (success/fail).</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies current status message information (running/complete).</td>
</tr>
<tr>
<td>Success</td>
<td>Specifies current success message information (Yes/No).</td>
</tr>
</tbody>
</table>
## Action History entry

<table>
<thead>
<tr>
<th>Action History entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Shows all devices in use.</td>
</tr>
<tr>
<td>Address</td>
<td>Shows IP address in use.</td>
</tr>
<tr>
<td>Return Code</td>
<td>Shows Return Code number. For details, see <a href="#">Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Return Codes</a> on page 34.</td>
</tr>
</tbody>
</table>

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>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Install</strong></td>
<td>Performs an Install and Reboot, and Configure and Reboot. Recommended for new installs.</td>
</tr>
</tbody>
</table>
| **Quick Install** | Installs the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 on the device. This action installs the package associated with device configuration, sets required SP modes, restarts the MFP, performs a Configure and Reboot, and also performs Sync Assets, and Sync Workflow buttons actions.  
This action is to be used for upgrades, changing application, or advanced troubleshooting. You must update to the latest Nuance Unified Client for Ricoh Smart Operation Panel 1.1 version using DRS first.  
NOTE: This action will not install the ScanEX. |
<p>| <strong>Uninstall</strong>   | Uninstalls the Nuance Unified Client for Ricoh Smart Operation Panel 1.1 on the device. For more information, refer to <a href="#">Uninstalling Client Using DRS</a> on page 20. |</p>
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Get device settings</strong></td>
<td>Gets current SP Mode settings on the device. Running this Action logs SP Mode settings and their values to a properties file (with the <code>.properties</code> extension). The default path to these properties files is:</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Nuance\Device Registration Service\Service\Plugins \RXOP-SOP\CLITools\output</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
</tbody>
</table>
|                     | 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  
<p>|                     | ... |
|                     | The actual settings and values listed in the file depend on the device. |
| <strong>Set device settings</strong> | 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 |</p>
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and Reboot</td>
<td>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. Run the <strong>Configure and Reboot</strong> action after you complete this action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This action will install the ScanEX.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Restarts the MFP.</td>
</tr>
<tr>
<td>Configure and Reboot</td>
<td>This action is to be used for advanced troubleshooting purposes only. Updates device configuration for the Ricoh SOP package installed on the device and then restarts the MFP. This action must be run after you complete the <strong>Install and Reboot</strong> action.</td>
</tr>
<tr>
<td></td>
<td>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 that have been specified 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>

**Nuance Unified Client for Ricoh Smart Operation Panel 1.1 Return Codes**

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 return codes appear for device actions that you perform through Device Registration Service.

The following return codes may appear for Nuance Unified Client for Ricoh Smart Operation Panel 1.1 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>
</tbody>
</table>
### Return Code

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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.

### Unified Client App status

<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>
</tbody>
</table>
**Unified Client App status** | **Scan GUI Service status** | **DRS status message**
--- | --- | ---
Installed | Not Installed | Installed; Version: Client: 1.30.184 - Scan GUI Service: Not installed

Installed | Error | Installed; Version: Client: 1.30.184 - Scan GUI Service: Error message

Not Installed | Not Installed | Not Installed

Not Installed | Installed | Not Installed

Error | - | Error message

---

### How to add a new Device profile

This task explains how to create a Device profile. The profile enables you to manage Nuance Unified Client for Ricoh Smart Operation Panel 1.1, 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 contains 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>
<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 40</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When accessing workflows, the user cannot perform scan and <strong>You do not have the privileges to use this function</strong> 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 40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must set <strong>Admin. Authentication to Off.</strong></td>
</tr>
</tbody>
</table>
### Issue

- 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.

### Cause

- 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.

### Solution

TLS versions must match service on the Controller and service on JavaVM. Complete the following procedure:

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

For detailed instructions, see [Changing the TLS Settings](#) on page 44.

---

When running Client Installer, **Please wait... Ricoh Persistence Provider message is pending (unknown error)**.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The optional HDD from the device is missing.</td>
<td>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.</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>

---

### Device Configuration for AuthOff

Follow this procedure to use the Auth Off client on the MFP. You should normally need to do this if it was not completed automatically by Device Registration Service.

1. Login [User Tools] as admin.
2. In **User Authentication Management**, press **Off** to turn off user authentication.
3. For **Machine Action When Limit is Reached**, press **Allow Continue Use** to not stop jobs when a limit is reached.

### Configuring Common Access Card Authentication Solution

Nuance Unified Client for Ricoh Smart Operation Panel 1.1 supports Ricoh Common Access Card (CAC) v4 that has authentication capabilities and prevents unauthorized access to MFPs with Output Manager 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. In this instance, Output Manager 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.

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.

Note: The following 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).

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”.

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 to complete the succeeding steps.
3. Press System Sp (press 0 to change bit from 0 to 1, then # to save).
4. Press SP Direct.
5. In **SP Direct** type 5401230, then type 
6. Set the **LSB** to 1 by pressing zero 0 on keypad in CAC configuration. The last two digits should now be 1.
7. Type # to save your changes.


10. Configure the LDAP server.

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**.

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

13. Turn on **Tracking Permission**.
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.
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 **Apply**
3. Click OK.

**DRS Authentication Key**

This security feature has been added to DRS where additional security between the DRS application and the device is enabled using an authentication 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 authentication 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 authentication 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 used 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 TLS is disabled on the device after the initial configuration, the authentication key pinning must be reset. In order to reset the DRS Authorization Key pinning to another DRS instance, use the following actions of the install and configuration options: **Uninstall** and **Full Install**.
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 Nuance Unified Client for Ricoh Smart Operation Panel 1.1 login screen, or if the embedded solution is not installed, the standard Ricoh Smart Operation Panel Home screen with option icons.