Device Registration Service

Installation Guide

Ver. 7.13

NUANCE

Contents

Introduction 3
Product features 3
Device Registration Service Pre-Requisites 3
Component prerequisites 4

Installing Device Registration Service 5
How to install Device Registration Service 5

Upgrading Device Registration Service 10
Upgrading Device Registration Service If a Remote Database Is Used 11
Database Upgrade Tool 12

Configuring Device Registration Service 14
How to configure Device Registration Service 14
Using DRS Authentication Key 17
Configure AutoStore to work with a remote DRS Server for Konica Minolta devices 18

Starting Device Registration Service 19
How to start Device Registration Service 19

Migrating Device Configurations 21

Communication Port Reference 23

Introduction

Product features

Device Registration Service enables you to perform the following tasks:

- Manage Device Registration Service configuration settings.
- Manage applications, device groups, and devices through a single web-based interface.
- Manage Microsoft Windows services and database administration.

Device Registration Service consists of the following components:

- Device Registration Service
- Device Configuration Manager
- Plug-ins for:
  - Konica Minolta
  - Ricoh
  - Samsung
  - Toshiba
  - Epson
  - Xerox

For more information on using the Device Registration Service and Device Configuration Manager components, refer to the component Help files.

Device Registration Service Pre-Requisites

Verify that the Device Registration Service environment meets the requirements listed here:

Before you install Device Registration Service on Microsoft Windows 8 and Microsoft Windows 10 or Microsoft Windows 2008, 2012 and Microsoft Windows 2016 Server machines, enable ASP.NET for Microsoft .NET 4.5 or ASP.NET for Microsoft .NET 4.6:

Microsoft Windows 8:

1. Open Control Panel.
2. In **Category** view, click **Programs**.
3. Under **Programs and Features**, click **Turn Windows features on or off**.
4. In **Turn Windows features on or off**, select **.NET Framework 4.5 Advanced Services**.

5. Select **.NET Framework 4.5**.

Microsoft Windows 10:

1. Open Control Panel.
2. In **Category** view, click **Programs**.
3. Under **Programs and Features**, click **Turn Windows features on or off**.
4. In **Turn Windows features on or off**, select **.NET Framework 4.6 Advanced Services**.
5. Select **.NET Framework 4.6**.

Microsoft Windows 2008 R2/2012 R2 Server:

1. Open **Server Manager**.
2. Click **Add Roles and Features** and then **Features**.
3. Restart the Virtual Machine.

Microsoft Windows 2012 Server:

1. Open **Server Manager**.
2. Click **Add Roles and Features** and then **Features**.
3. Select **.NET Framework 4.5**.
4. Restart the Virtual Machine.

Microsoft Windows 2016 Server:

1. Open **Server Manager**.
2. Click **Add Roles and Features** and then **Features**.
3. Select **.NET Framework 4.6.2**
4. Restart the Virtual Machine.

Component prerequisites

This section lists component-specific system requirements.

Ricoh ESA

- Microsoft Visual C++ 2010 runtime
- Oracle Java SE Runtime Environment (JRE) 8
- .NET 3.5. For supported versions of the Java platform on Ricoh devices, see the requirements section of the Ricoh Combined Client User Guide in the Device Registration Service Help after you install Device Registration Service.

Ricoh SOP 1.1/RIcoh PCC 5.1

- Oracle Java SE Runtime Environment (JRE) 8, Update 161
- Customization templates, installed as part of the DRS installation, are required for certain customized features.

Xerox EIP

- Microsoft Web Service Enhancements 3.0

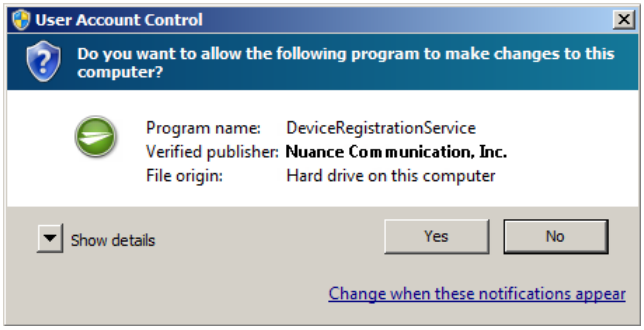
Any additional prerequisites are installed during the installation process.

Installing Device Registration Service

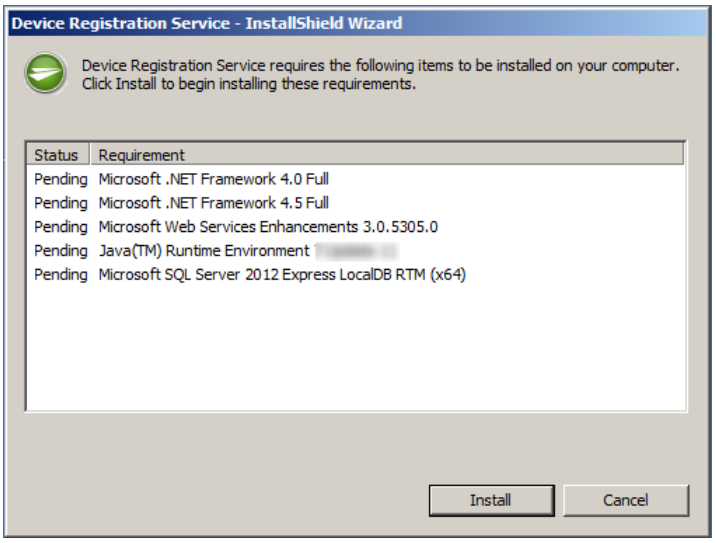
How to install Device Registration Service

Complete the steps in this procedure to install the Device Registration Service.

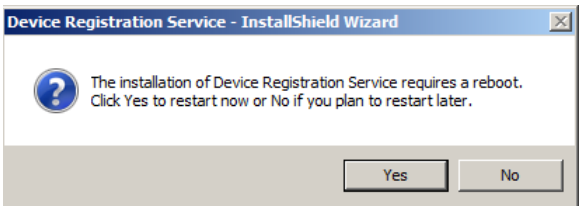
1. Right-click the executable file for Device Registration Service and click to **Run as administrator**, then click **Yes** to continue.



2. Click **Install** to install the required software.



3. Click **Yes** if the installation wizard prompts to reboot the machine.



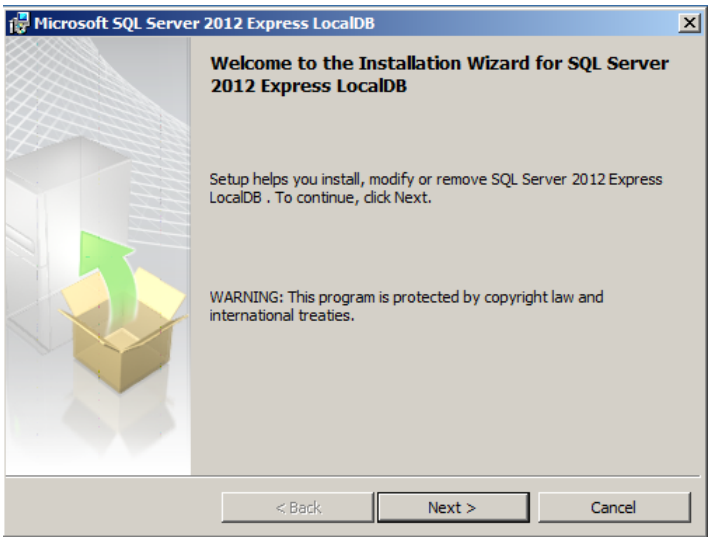
Note: Contact your system administrator if you are uncertain about whether to reboot the machine.

The installation continues automatically after the machine restarts. If the installation does not continue after the machine restarts, run the executable again to restart the process.

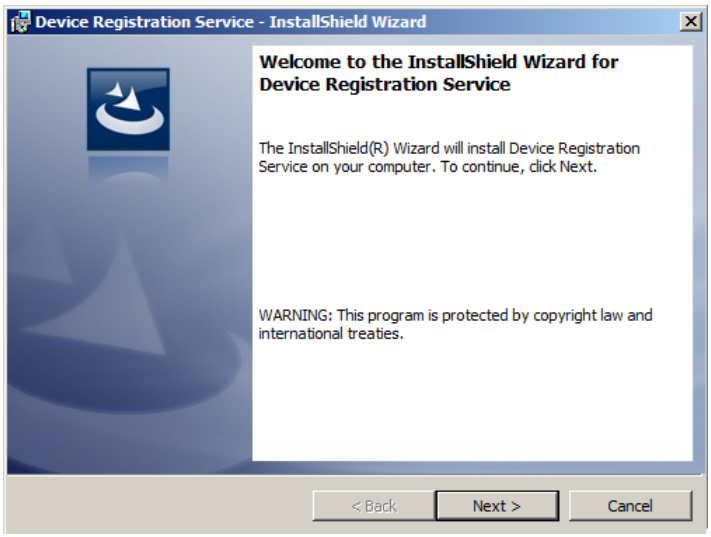
4. On the **Java Setup** dialog box, click **Install**.

5. After Java is installed, click **Close**.

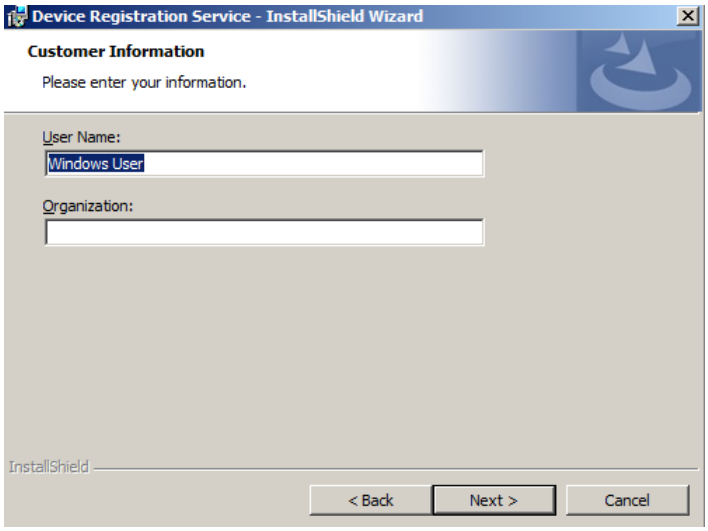
6. Click **Next** to install Microsoft SQL Server Express or Express LocalDB.



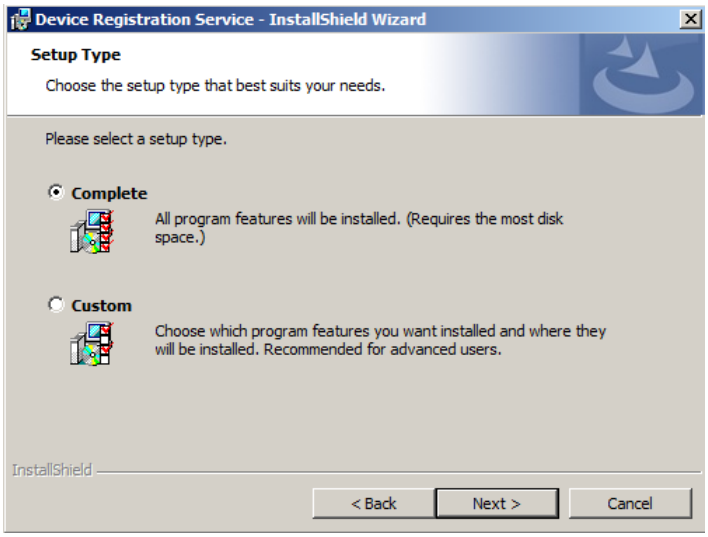
7. Review and accept the Microsoft SQL Server license agreement.
8. Click **Install** to start the Microsoft SQL Server installation.
9. Click **Finish**.
10. Click **Next** to start the Device Registration Service installation.



11. Review and accept the license agreement.
12. On the **Customer Information** screen, enter customer information and click **Next**.

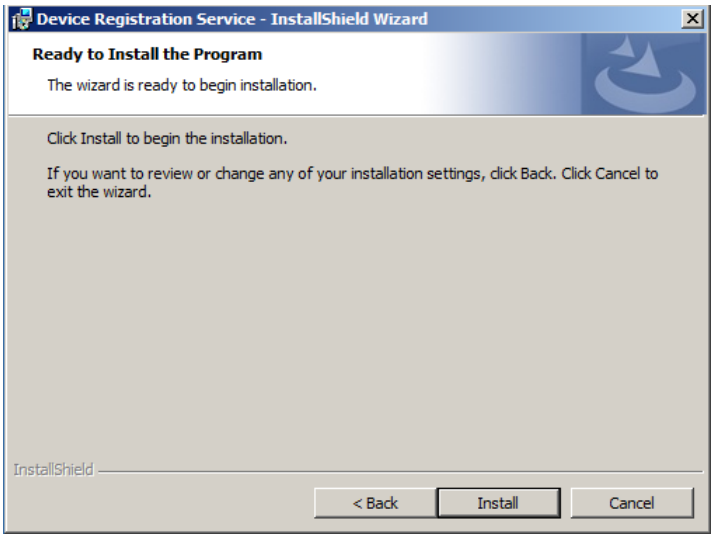


13. On the **Setup Type** screen, select the setup type and click **Next**.



Note: The **Custom** setup type offers the ability to customize the install location and is recommended for advanced users.

14. Click **Install**.



15. Click **Finish** to complete the installation.

CAUTION: Customization templates, installed as part of the DRS installation, 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 (x86)\Nuance\Device`, are backed up post-DRS installation to a secure location.

Refer to How to configure Device Registration Service on page 14 for more information on checking for updated Device Registration Service software.

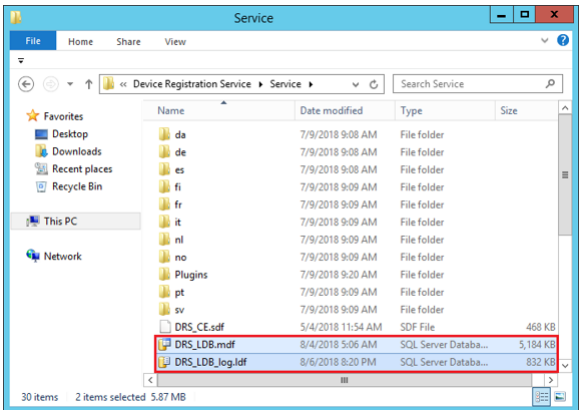
Upgrading Device Registration Service

This procedure describes how to upgrade the Device Registration Service software when upgrading from Ricoh PCC 5.0 to 5.1, or upgrading from Ricoh SOP 1.0 to 1.1.

Note: Ricoh PCC 5.1: Upgrade from DRS 7.11 to at least DRS 7.12 for PCC 5.1. It is recommended to upgrade to DRS 7.13 to access the new features.

Upgrading in case the user has a local database

1. 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 (x86)\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 service settings, for example the security settings. Therefore you will want to validate all settings are correct after you start the DRS service.

2. Uninstall your previous version of DRS using **Uninstall a Program** (**Control Panel** in Windows).
3. Install the latest version of the Device Registration Service software as described in How to install Device Registration Service on page 5.
   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.

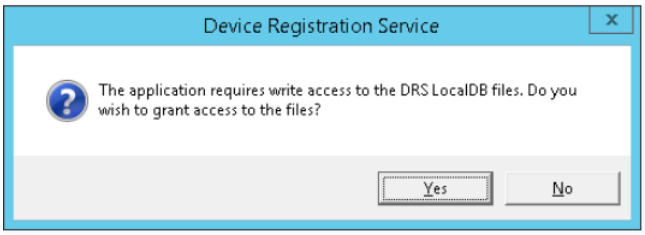
Note: Optionally, instead of an in-place DRS upgrade, install DRS 7.13 on a separate supported workstation/server to deploy Ricoh PCC 5.1/Ricoh SOP 1.1. After installing DRS 7.13, migrate the older DRS database to the new DRS workstation/server.

4. 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 backed up in step 1 on page 10. The user may now run the Upgrade Tool.

   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.

5. 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.



   Click **Yes** to run the Upgrade Tool.

6. Install the latest Ricoh PCC 5.1/SOP 1.1 client using DRS 7.13 with a **Full Install** action.

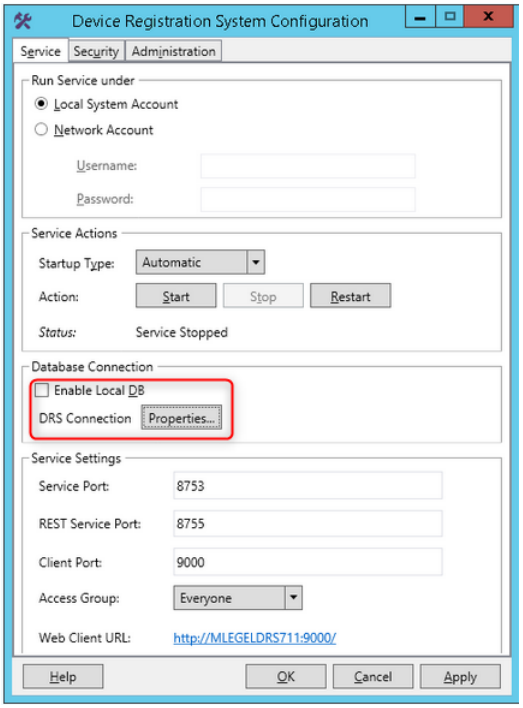
Upgrading Device Registration Service If a Remote Database Is Used

This procedure describes how to upgrade the Device Registration Service software when upgrading from Ricoh PCC 5.0 to 5.1 or upgrading from Ricoh SOP 1.0 to 1.1 if a remote database is used .To upgrade from Ricoh PCC 5.0 to Ricoh PCC 5.1, complete the following:

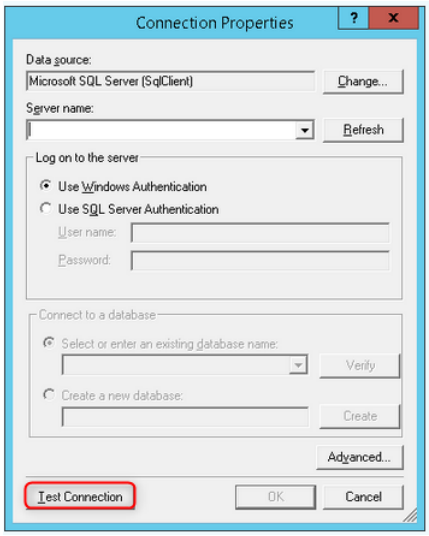
Upgrading from Ricoh PCC 5.0 to 5.1 or upgrading from Ricoh SOP 1.0 to 1.1 in case a remote database is used

Complete the following:

1. Open **Device Registration System Configuration**.
2. Stop service.
3. Uncheck **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

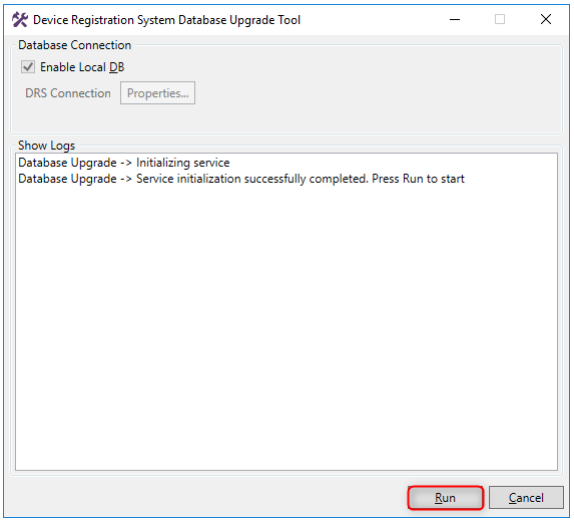
The database upgrade tool is intended to be run after an existing Device Registration Service installation has been successfully upgraded, with the backed-up database correctly restored, but before the DRS service is started yet. The tool goes through all existing application profiles, devices and

device groups, and (assuming they are already valid) performs necessary modifications to have the database records ready for the latest DRS release, including but not limited to: initialize properties newly introduced, convert and/or modify existing values to meet new features' requirements, and so on.

Note: In DRS 7.13, the upgrade tool (`NSi.DeviceManagement.Upgrade.exe`) is located at `C:\Program Files (x86)\Nuance\Device Registration Service\Service`.

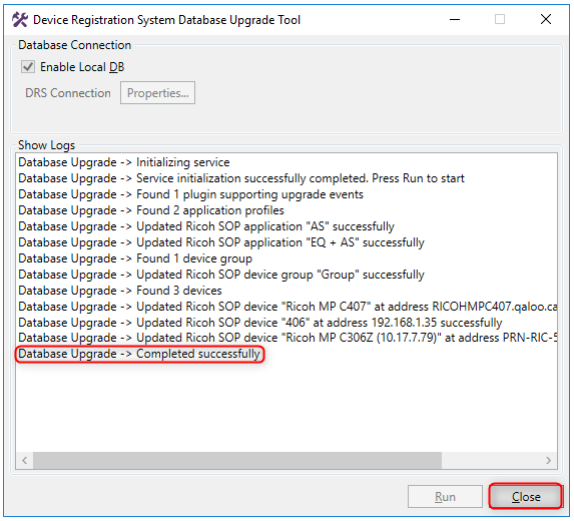
Process:

1. 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. Once service has initialized, 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.

2. Once processing has been successfully completed, the log will display **Completed successfully** message. Click **Close** to exit the tool.



3. Start DRS 7.13 service with the newly-upgraded database records.

Configuring Device Registration Service

How to configure Device Registration Service

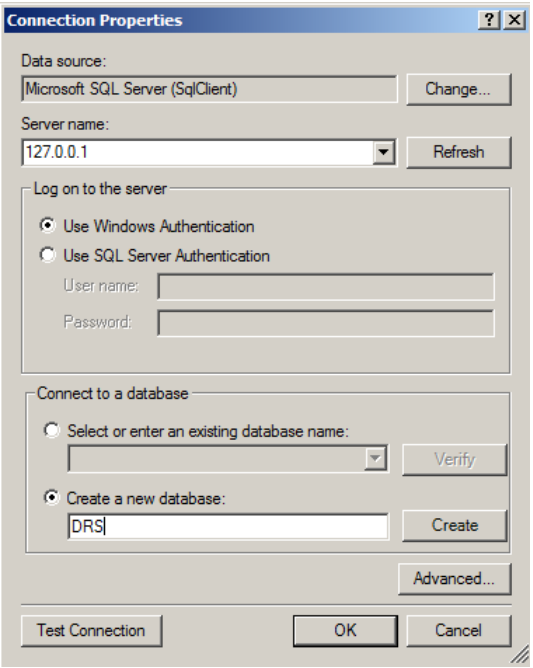
Perform configuration of the Device Registration Service after you complete the installation.

1. On the Windows **Start** menu, select **All Programs** > **Nuance** > **Device Registration Service** > **Device Configuration Manager**.
2. Click **Yes** when prompted to make changes to the computer.
3. Configure settings on the **Service** tab as described in the following table:

Settings	Description
Run service under	You can run the service under the local system account or a network account. The selected account needs system permissions to run the service. The account proper permission to manage, update and configure the SQL Server database when Windows Authentication is used to connect to the SQL Server.
Service Actions	Select the Microsoft Windows service startup type for the Device Registration Service.
Database Connection	A database repository stores the configuration options that you specify in Device Registration Service. The repository can reside in Microsoft SQL Server Express or Express LocalDB installed with Device Registration Service, or it can reside on a remote instance of Microsoft SQL Server. Select **Enable Local Db** to use the Express LocalDB. Complete step 4 on page 15 to use a remote instance of Microsoft SQL Server.

Settings	Description
Service Settings	Device Registration Service requires several ports to be specified for communication between the Web service and Web client. The Web client is the browser that you will use to access Device Registration Service. An **Access Group** should be specified. The access group is a user or group of users who will have access (and permission) to use Device Registration Service.

4. To use a remote instance of Microsoft SQL Server to host the repository:
   a) Clear the **Enable Local DB** check box, and then click **Properties** to open the **Connection Properties** dialog box.



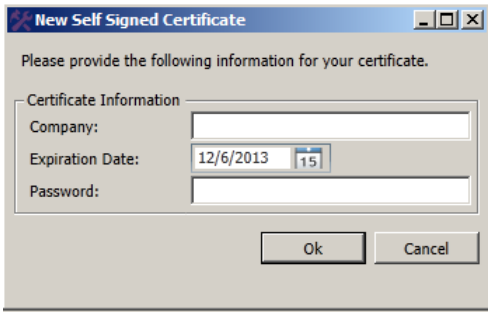
   b) Configure Microsoft SQL Server settings as described in the following table:

Settings	Description
Server name	For the default instance of SQL Server, enter the server name or IP address of the server that is running SQL Server. If you are using a named instance of SQL Server, enter the instance name as well in the format, *server_name\instance_name*.
Log on to the server	Select the type of authentication for connecting to the server. For the selected type, verify that the credentials have permissions to update or create a database on the specified instance of Microsoft SQL Server.
Connect to a database	Select an existing database or create one with the latest schema.

   c) Click **Test Connection** to test the settings.
   d) Click **OK** if the connection is successful.
5. On the **Security** tab, enable TLS on the web service or the web client:

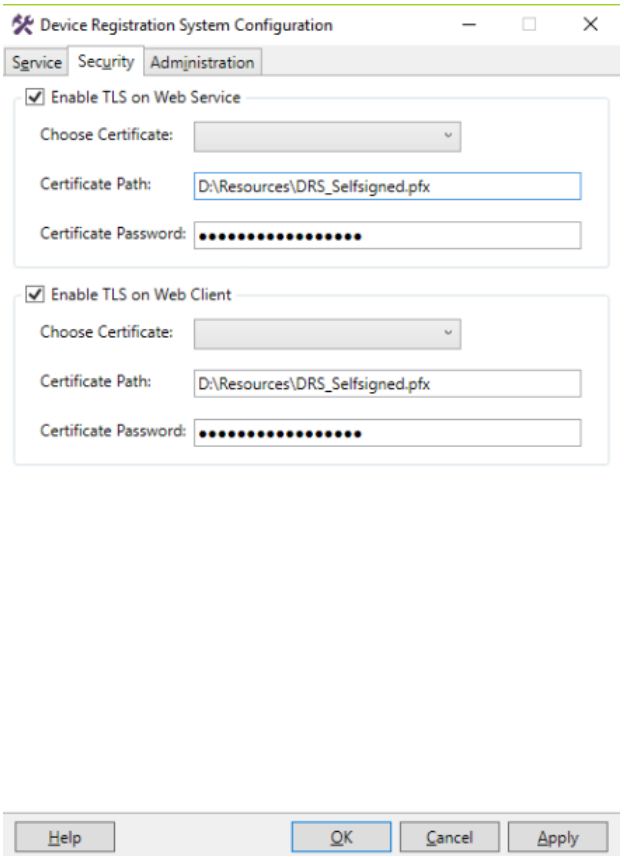
To create a self-signed certificate:

a) Select **Enable TLS on Web Service** or **Enable TLS on Web Client**.
b) In the **Choose Certificate** box, click New Self-Signed.
c) Enter the certificate information and click **OK**.



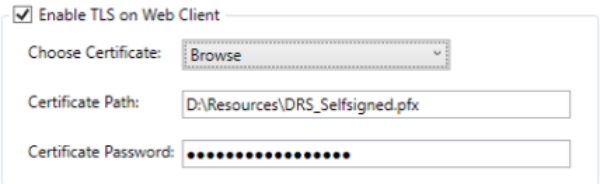
d) In the **Certificate Path** box, type the location where you want to store the certificate.

The **Certificate Password** is the same password that you entered when creating the certificate. The masked field automatically populates with the password that you entered.



To use an existing certificate:

a) Select **Enable TLS on Web Service** or **Enable TLS on Web Client**.
b) In the **Choose Certificate** box, click Browse.



c) In the **Certificate Path** box, type the path to the certificate.
d) In the **Certificate Password** box, type the certificate password.

Note: DRS supports TLS 1.0, 1.1 and 1.2. Support for SSL 3.0 has been discontinued.

6. Configure logging settings on the **Administration** tab as described in the following table:

Settings	Description
Web Service Logging	In the **Log Path** box, type the path to the location where you want to store the web service log file, or click **Browse** to select the location. To generate more detailed log files for debugging and advanced troubleshooting with Support, select the **Enable Tracing** check box. **Note:** This option may affect Device Registration Service performance. Enable tracing only when it is necessary. Click **Show Logs** to open the log file in a text editor.
Web Client Logging	In the **Log Path** box, type the path to the location where you want to store the web client log file, or click **Browse** to select the location. To generate more detailed log files for debugging and advanced troubleshooting with Support, select **Enable Tracing**. **Note:** This option may affect Device Registration Service performance. Enable tracing only when it is necessary. Click **Show Logs** to open the log file in a text editor.

Refer to the Device Configuration Manager Help for more information on logging.

Using DRS Authentication Key

Customers are advised to back up their DRS database after they complete the configuration. Restoring the database will restore the saved DRS Authorization Key for each device. If not available, run the **Uninstall** command first to fully remove the Ricoh client from the device and then set the configuration again as the client will accept the new DRS Authorization Key after a new install.

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**.

Configure AutoStore to work with a remote DRS Server for Konica Minolta devices

Attention: Instructions in this topic apply only for DRS version 7.6 or earlier. For DRS version 7.7 or later, you only need to configure settings on the **Device Registration** tab of the Konica Minolta iOption settings after you add the component to an AutoStore workflow.

To use Device Registration Service version 7.6 or earlier for Konica Minolta iOption devices when DRS and AutoStore are hosted on separate machines, you must manually edit the `Web.config` file located in the `KonicaPanelClient` folder in the AutoStore program files folder. Here is the path to default location for this file on the AutoStore server:

```
C:\Program Files (x86)\Notable Solutions\AutoStore 7\KonicaPanelClient
\Web.config
```

Use a text or code editor to change the following lines in the file:

```
add key="DrsServiceBaseUri" value="http://DRS_server:service_port" />
add key="DrsToolUri" value="http://DRS_server:client_port" />
```

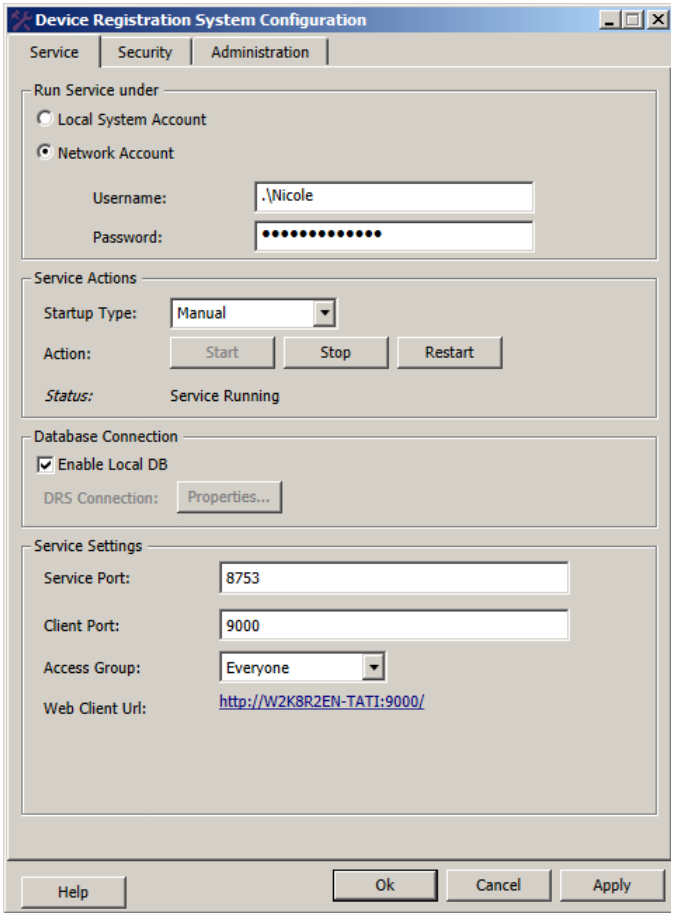
You can specify a fixed IP address or host name for *`DRS_server`*. If you are unsure of what values to use, on the DRS Server, click **Start** > **All Programs** > **Nuance** > **Device Registration Service** > **Device Configuration Manager** to open the **Device Registration System Configuration** dialog box. The ports and URL are displayed in the **Service Settings** group box on the **Service** tab of this dialog box.

Note: These one-time instructions only apply for Konica Minolta devices, and only when AutoStore and DRS are hosted on separate machines. For other device manfacturers, or when AutoStore and DRS are on the same machine, the **Device Registration** component settings in AutoStore will allow the AutoStore component to communicate with the DRS server.

Starting Device Registration Service

How to start Device Registration Service

1. On the Windows **Start** menu, click **All Programs** > **Nuance** > **Device Registration Service** > **Device Configuration Manager**.
   This opens the **Device Registration System Configuration** dialog box.
2. Click **Yes** if you are prompted to confirm that you want to make changes to the computer.
3. On the **Service** tab, in **Run Service under** choose a designated local or domain account to run DRS service instead of running the service under Local System Account (due to the Windows update's removal of the SQL server database instance). Click **Log on as a service** permission to the account:
   a) Open Local Security Policy, click **Start** > **Control Panel** > **Administrative Tools** > **Local Security Policy** (double-click).
   b) In the console tree, double-click **Local Policies** and then click **User Rights Assignment**.
   c) In the details pane, double-click **Log on as a service**.
   d) Click **Add User or Group...**, and then add the appropriate account to the list of accounts that possess the Log on as a service right.
4. Allow **Full control** permission of the two LocalDB database files to the account and restart the service.
5. Click the link for **Web Client URL**.



This opens Device Registration Service in your default web browser.

Migrating Device Configurations

Starting with AutoStore version 7.0, the Ricoh ESA and Xerox EIP Connect Unified Clients do not support the device manager tool in the Ricoh ESA and Xerox EIP Connect non-Unified Clients. To use AutoStore 6.0 device configurations in AutoStore 7.0, use the Device Registration Service migration tool to migrate the configurations to AutoStore 7.0.

Open the migration tool from the AutoStore 7 installation folder. The default path to the tool is `C:\Program Files (x86)\Notable Solutions\AutoStore 7\DeviceMigrationTool.exe`. The folder location for your environment may vary. The migration tool Help provides more information on converting AutoStore 6.0 device configurations to CSV files for import into Device Registration Service.

The following table lists the procedures for migrating configurations:

Unified Client	Procedure
Ricoh ESA	**1.** Install Device Registration Service and create the application profile. **2.** Export the AutoStore 6.0 configuration with the non-Unified Client device manager tool. Access the device manager tool through the non-Unified Client component **Preferences** tab. **3.** Convert the exported file with the migration tool. **4.** Import the converted file into Device Registration Service.

Unified Client	Procedure
Xerox EIP Connect	**1.** Install Device Registration Service and create the application profile. **2.** If the AutoStore 6.0 configuration contains device groups, create device groups with the same group names in Device Registration Service. **3.** Convert the AutoStore 6.0 `RegistrationGroups.xml` file with the migration tool. The default location of the file is `C:\XeroxEIPCapture`. The migration tool creates a separate CSV file for each device group in the file. **4.** Import the converted files into Device Registration Service.

The *Device Registration Service User Guide* and Device Registration Service Help explain how to create applications, create device groups, and import device configuration files.

Communication Port Reference

The following tables provide general information on ports and protocols for DRS server and unified or combined clients. The component Help files contain information on configuring the components.

Table 1: DRS and Unified or Combined Client ports

Component name	Device Display Menu Protocol	Device File Transport Protocol	Default Communication Port Numbers	Port Modifiable?	Required Device Components and Notes
DRS server	HTTP, HTTPS	HTTP, HTTPS	• Web server: 8753 • REST-based web service: 8755 • Client Server: 9000 • Web client: 9000	• Yes	

Component name	Device Display Menu Protocol	Device File Transport Protocol	Default Communication Port Numbers	Port Modifiable?	Required Device Components and Notes
Combined Client for Konica Minolta	HTTP, HTTPS	FTP/WebDAV	• Web application: 3348 Device setting for web server • OpenAPI: 50001 • OpenAPI SSL/TLS: 50003 TCP Socket setting • 59158 • SSL/TLS: 59159 • ASCII mode: 59160	• Yes (except for Web server Open API SSL/TLS)	The Web application port number should match the component setting in AutoStore (or the Output Manager setting when not using AutoStore).
Combined Client for Ricoh	HTTP, HTTPS	HTTP, HTTPS	AutoStore application port: • AutoStore server: 8084 Output Manager application port: • 8068 • (SSL): 8069 Ricoh ESA (internal device components): • 9999	• Yes	Xlet Java Xlet VM card with AutoStore Xlet on the device for communication with the AutoStore server.

Component name	Device Display Menu Protocol	Device File Transport Protocol	Default Communication Port Numbers	Port Modifiable?	Required Device Components and Notes
Unified Client for Ricoh SOP / Ricoh PCC5	HTTP, HTTPS	HTTP, HTTPS	AutoStore application port: • AutoStore server: 3350 Output Manager application port: • 8068 • (SSL): 8069 Equitrac • 8443 Ricoh SOP (internal device components): • 51443		The 51443 port is used by Ricoh SOP devices for collecting and configuring device information (see page 21, *Protocols and Ports* in Security White Paper for Device Manager NX Pro).
Unified Client for Samsung	HTTP	FTP/WebDAV	• Web application: 3349 • FTP port: 3281 • WebDAV port: 13392 DRS on a remote server: • Service port: 8753 • Web client: 9000	• Yes Note: All port settings for this component are configured on the **Preferences** tab of the component settings.	The Web application port number should match the component setting in AutoStore (or the Output Manager setting when not using AutoStore).
Unified Client for Xerox	HTTP, HTTPS	FTP/SMB	Output Manager server ports: • HTTPS: 8069 • HTTP: 8068 • nettcp: 8070 Web app port: • 3241	Yes	No applet IIS web application connects to the AutoStore web service. The device connects to the IIS web application.

Component name	Device Display Menu Protocol	Device File Transport Protocol	Default Communication Port Numbers	Port Modifiable?	Required Device Components and Notes
Unified Client for Epson v1.0	HTTP, HTTPS	HTTP, HTTPS	eCopy ShareScan application port: • eCopy ShareScan server: 9655/9656 Equitrac • 8443	Yes	
Unified Client for Toshiba	HTTP, HTTPS	HTTP, HTTPS	AutoStore application port: • AutoStore server: 3310 Equitrac • 8444	Yes	