RICOH @Remote Connector NX
Install Guide

Complete View of Your Fleet Status

Copyrights

Ricoh Building, 8-13-1 Ginza, Chuo-ku, Tokyo 104-8222, Japan

Trademarks

Ricoh®, the Ricoh Logo, @Remote Connector NX, Device Manager NX Pro, @Remote®, Remote Communication Gate S, Ridoc IO OperationServer, and Web SmartDeviceMonitor are either registered trademarks or trademarks of Ricoh Company, Ltd.

Other product names used herein are for identification purposes only and may be trademarks of their respective companies. Ricoh Company Ltd. disclaims any and all rights to those marks.

The following are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries: Microsoft®, Windows®, Windows Vista®, Windows® XP, Windows® 7, Windows® 8, Internet Explorer®, Excel®, IIS Server, Microsoft® SQL Server® 2008 (Workgroup, Standard, Enterprise), Microsoft® SQL Server® 2008 R2 (Workgroup, Standard, Enterprise), Microsoft® SQL Server® 2012 (Workgroup, Standard, Enterprise), Microsoft® SQL Server® 2012 Express.

Java® is a registered trademark of Oracle America Inc.

Firefox® is a registered trademark of the Mozilla Foundation.

Safari® and AppleTalk® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

Intel® Xeon® and Intel® Core® are registered trademarks of Intel Corporation in the U.S. and other countries.

AMD Opteron™ is a trademark of Advanced Micro Devices Inc.

VMWare® is a registered trademark of VMWare Inc.

Adobe® Acrobat® is a registered trademark of Adobe System Software

Entrust® is a trademark of Entrust, Inc.

Thawte® is a trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

VeriSign™ is a trademark of VeriSign, Inc.

Netware, IPX, IPX/SPX, are trademarks of Novell Inc.

PCL is a trademark of Hewlett-Packard Development Company, L.P.

The Jetty Web Container is copyright Mort Bay Consulting Pty Ltd.

Document Number

CONNECTOR-INSTALL-A.0

Revision History

Date	Revision Number	Revision Details
01/10/14	A.0	First release of document

Some illustrations or explanations in this guide may differ from your product due to improvement or change in the product. Contents of this document are subject to change without notice.

Contents

RICOH

1

About @Remote Connector NX

RICOH @Remote Connector NX provides connectivity to the @Remote Center System to maintain high device availability and efficiency.

@Remote is a remote service for networked output devices connected in a LAN/Broadband environment, letting customers use them with greater convenience and peace of mind. Periodic monitoring of each device on the network keeps track of the connection status and usage of each device.

@Remote minimizes manual tasks by automating meter/ counter reads of network-connected MFP and printers, performing continual fleet monitoring including tracking of the total pages printed by each printer, and automating Service Call notification to minimize downtime.

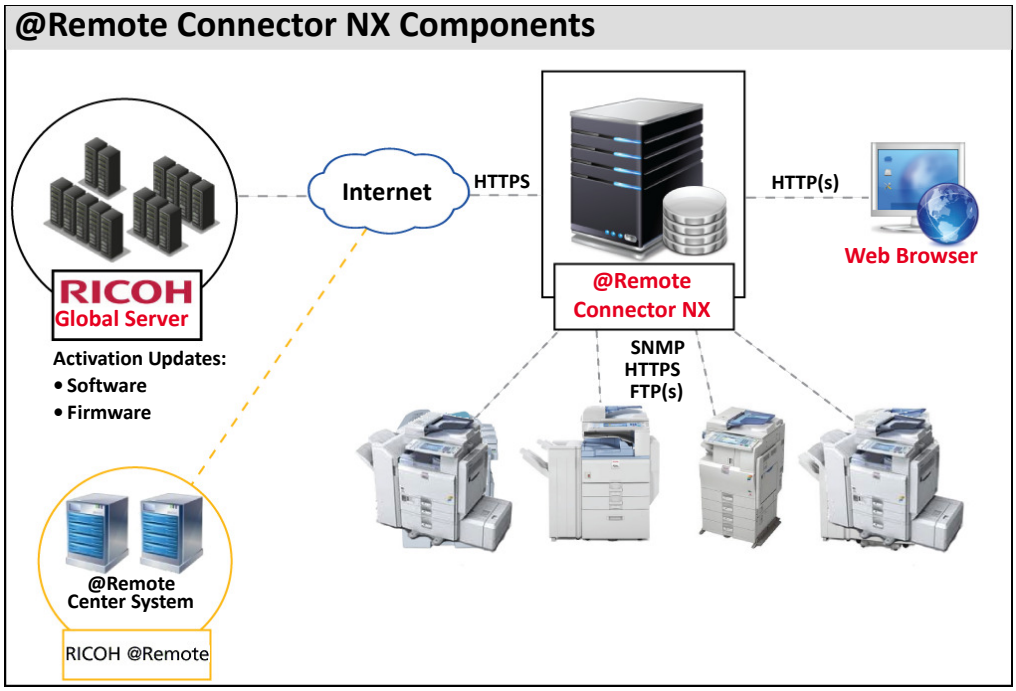
@Remote Connector NX sends backup data to and receives data from the @Remote Center System.

Use this guide to plan and execute the complete @Remote Connector NX installation.

1.1 Components

@Remote Connector NX consists of the components shown in the diagram below.

Every @Remote Connector NX installation requires a pre-installed SQL or SQL Express database. This primary database contains all information necessary to manage and monitor connected devices, as well as system settings, configuration settings and security profiles. See *Install and Prepare the Database* on page 12 for details.



- @Remote Connector NX communicates via HTTPS with the Ricoh Global Server to retrieve and apply software, firmware and SDK application updates.
- @Remote Connector NX sends backup data to and receives data from the @Remote Center System to ensure high availability.
- @Remote Connector NX continually monitors the status of connected devices to ensure device availability and communicates with the connected fleet via HTTPS and SNMP: If a device is set to managed mode within the @Remote Center System, HTTPS is used to communicate; if set to managed mode within the @Remote Center System, SNMP is used to communicate.
- @Remote Connector NX can manage up to 5000 devices.

- Administrators can access the management interface through a supported web browser. See *Web Browser Support* on page 9.

1.2 @Remote Connector NX Services

@Remote Connector NX relies upon two services to communicate. Both services are automatically installed to perform the following tasks:

- The **DM Server** service is used to communicate via HTTP(s) or SNMP with the devices. This service is called the Ricoh DMNX Device Manager Service on the installed computer.
- The **Core Server** service communicates with the @Remote Connector NX database. This service is called the Ricoh DMNX Central Manager service on the installed computer.

1.3 System Requirements

Servers running @Remote Connector NX must meet the following recommended specifications. For minimum requirements, refer to the *@Remote Connector NX Planning Guide*.

Component	Hardware Platform	Operating System

@Remote Connector NX	• CPU:
	  •Intel Xeon X3500 series or better *or*
	  •AMD Opteron 4100/6100 series or better
	• Available Memory: 4 GB
	• Available HDD space: 3 GB (excluding database)
		• Windows Server 2008 Standard/Enterprise SP1+ (32/64-bit)
		• Windows Server 2008 R2 Standard/Enterprise SP1+ (32/64-bit)
		• Windows Server 2012 Standard/Enterprise (32/64-bit)

1.4 Database Requirements

The following databases are supported:

- Microsoft® SQL Server® 2008 (Workgroup, Standard, Enterprise)
- Microsoft® SQL Server® 2008 R2 (Workgroup, Standard, Enterprise)
- Microsoft® SQL Server® 2012 (Workgroup, Standard, Enterprise)

- Microsoft® SQL Server® 2012 Express

The database must be installed prior to the installation of @Remote Connector NX. See *Install and Prepare the Database* on page 12 for instructions.

1.5 Web Browser Support

Device Administrators will connect to the @Remote Connector NX management interface via web browser. The following browsers are supported:

- Firefox 17 ESR or later
- Internet Explorer 8, 9, and 10
- Safari 6.0

1.6 IIS Web Server Support

@Remote Connector NX uses a Jetty Web Server by default. However, you can configure an IIS server to redirect IIS requests to Jetty if you prefer to expose IIS from the Core Server. For instructions, see *Appendix B: IIS Configuration* on page 42.

RICOH

2

Installing the Software

Warning: If installing @Remote Connector NX in a cluster environment, follow the instructions in *Chapter 3: Installing the Software in a Cluster Environment* on page 24.

Before you install the @Remote Connector NX components, first install and configure the SQL Server or SQL Express database. During the installation, you are required to enter the SQL Server address and instance name you created when installing the database. Refer to the workflow diagram on the following page to install and configure the database and @Remote Connector NX.

2.1 Installation Workflow

1 Install and Prepare the Database **Page 12**

Install the SQL Server or SQL Express database and configure the database to allow TCP/IP connections.

↓

2 Install @Remote Connector NX **Page 14**

Install @Remote Connector NX.

↓

3 Configure the @Remote Connector NX Database * **Page 21**

* This step is not required if you allowed the Installation Wizard to automatically create the database scripts during the install. If you did not enable the automatic database configuration option within the Installation Wizard, you must perform this step before the software is ready for use.

↓

4 Activation **Page 23**

Provide the license and activation code to activate the software prior to first use.

2.2 Install and Prepare the Database

Refer to the Microsoft website for full information about downloading and installing SQL or SQL Express. Ensure that you:

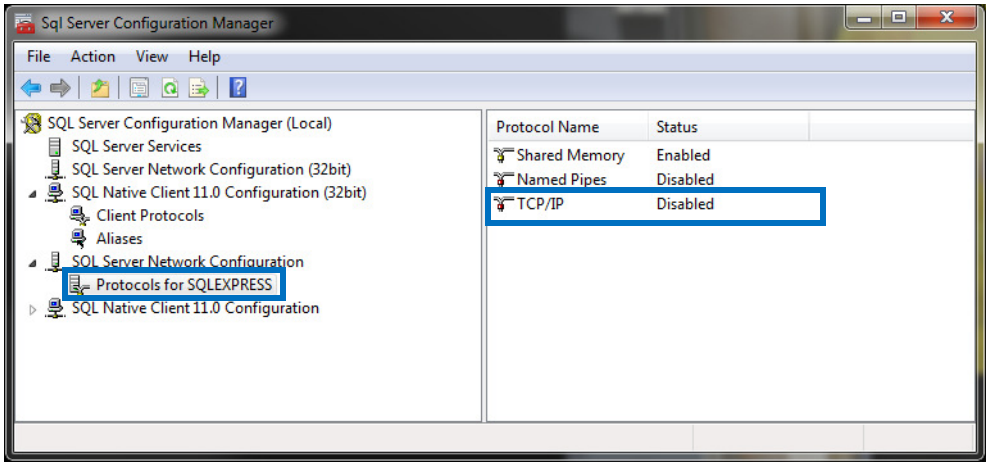
- Install the correct database version for the server architecture (i.e. x64 vs. x86)
- Verify that the installer includes the SQL Server Management Studio. These tools are required to configure the @Remote Connector NX database.
- Pre-determine the mode to use for connecting to SQL: Authentication Mode or Mixed Mode. Record the credentials you create for later reference.
- Complete the remainder of the installation using the defaults.

To Allow TCP/IP Connections

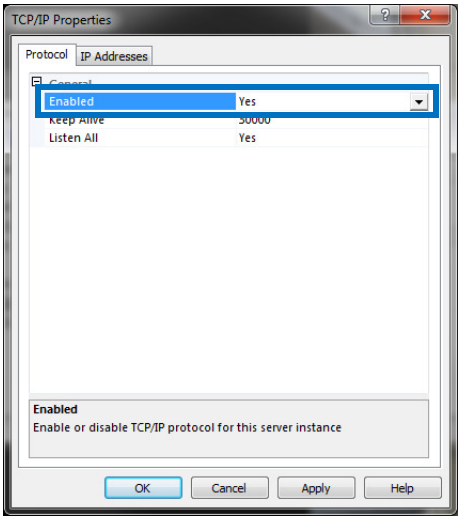
After the database software install is complete, you need to configure the database to allow TCP/IP connections:

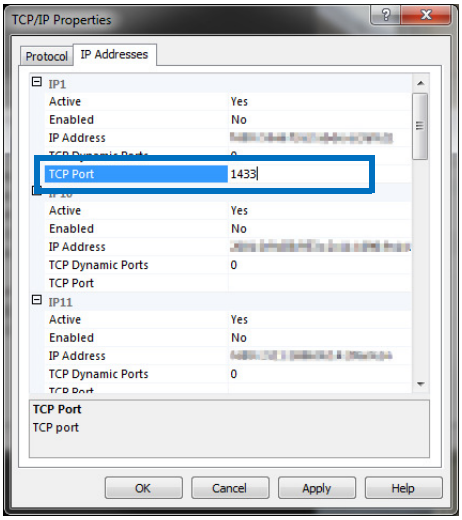
1. Launch the **SQL Server Configuration Manager.**

2. From the list on the left, click SQL Server Network Configuration, and then select **Protocols for SQL Express.** Double-click **TCP/IP** from the list on the right.



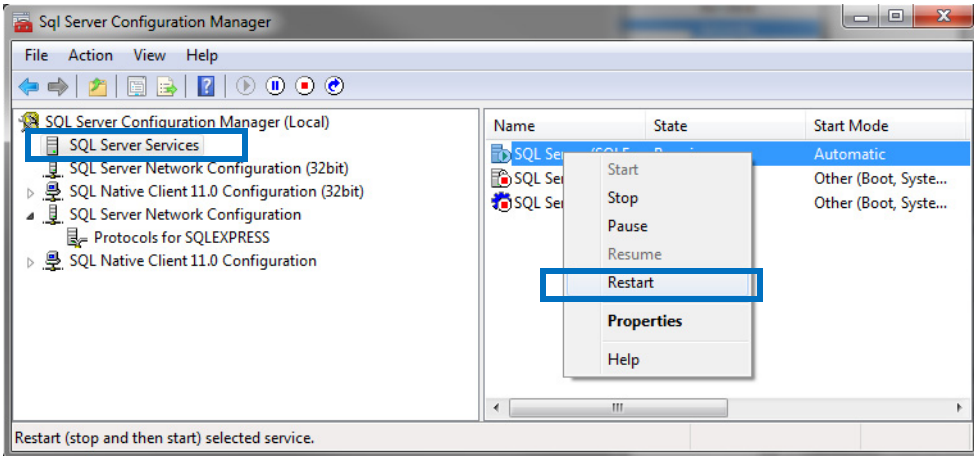
3. In the TCP/IP Properties screen, Protocol tab, set **Enabled** to **Yes** and ensure the IP addresses are active on the IP Addresses tab. To use the default SQL Server port, s**et the TCP ports to 1433**.





4. Click **OK** to save the changes. You will receive a message indicating the changes will be applied only when the service is stopped and started. Click **OK** again to clear the message.

5. Select the **SQL Server Services option** from the list on the left. From the list on the right, right click on **SQL Server** and select **Restart** from the menu.



You are now ready to install @Remote Connector NX.

2.3 Install @Remote Connector NX

There are two installers available to install the product:

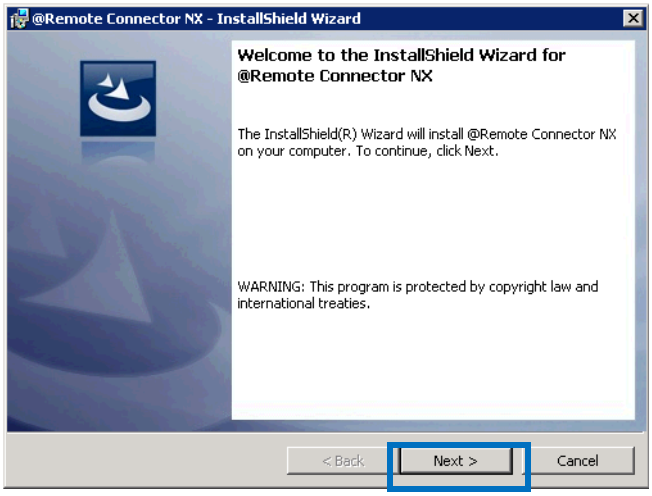
- Setup-x64.exe
- Setup-x86.exe

Ensure you run the installer that corresponds to the architecture of the machine you are installing @Remote Connector NX on.

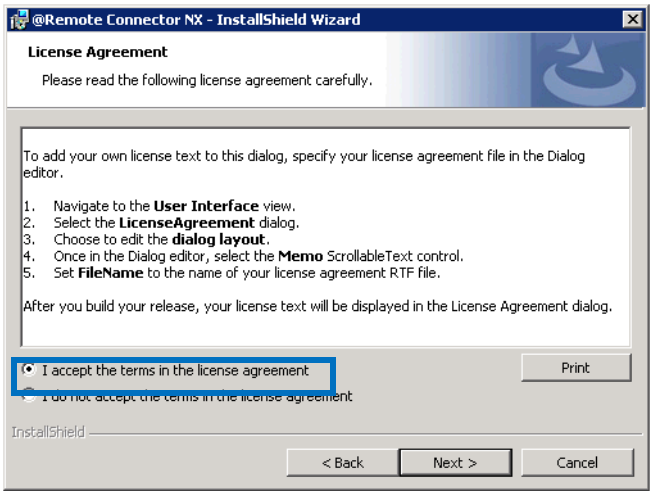
Warning: You must have Administrator rights on the machine to install this software.

1. Double-click the .exe file to launch the installer.
2. @Remote Connector NX checks for the Java Runtime Environment, a required piece of software. If the JRE is not found, you will be prompted to install it:

   Click **Install** to proceed.
3. After the JRE install is complete (or if it was already installed), the installer extracts the MSI and you can select the components to install. Click **Next** to continue.

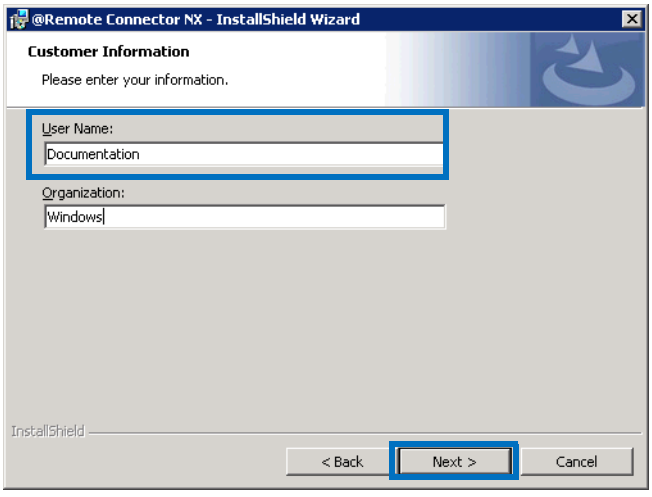


4. In the **License Agreement** screen, read the license text, or click **Print** to print out the full agreement and read it offline. Click **I accept the terms in the license agreement**, then click **Next**.

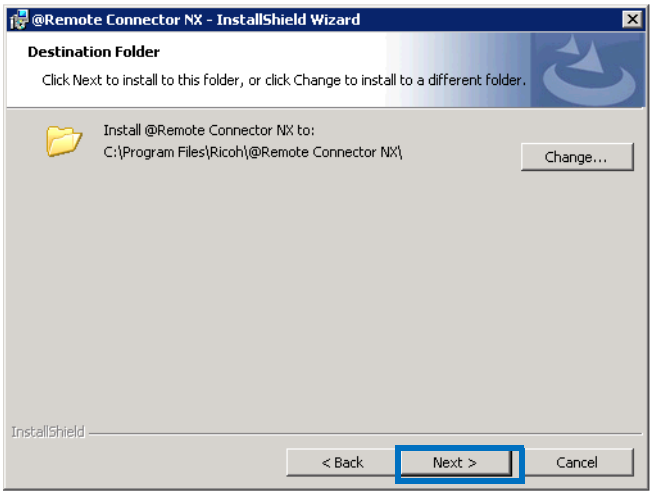


Warning: You cannot proceed with the install until you accept this agreement.

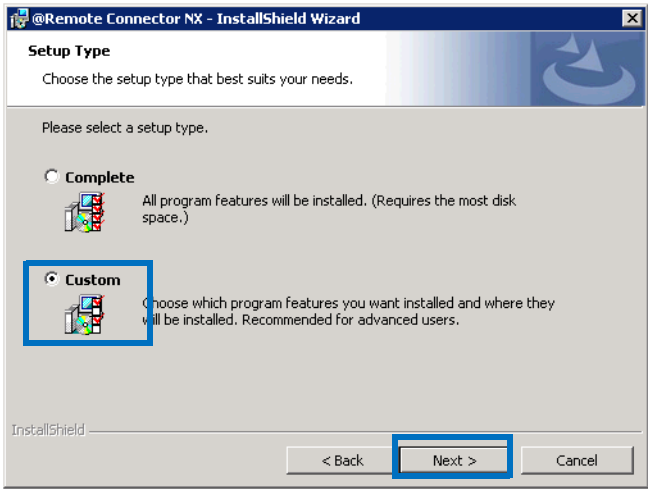
5. In the **Customer Information** screen, type your **User Name** (for this machine) and the name of your organization, then click **Next**.



6. In the **Destination Folder** screen, choose the location where you will install the software. You can accept the default, or click **Change** to select another location. Click **Next** to continue.



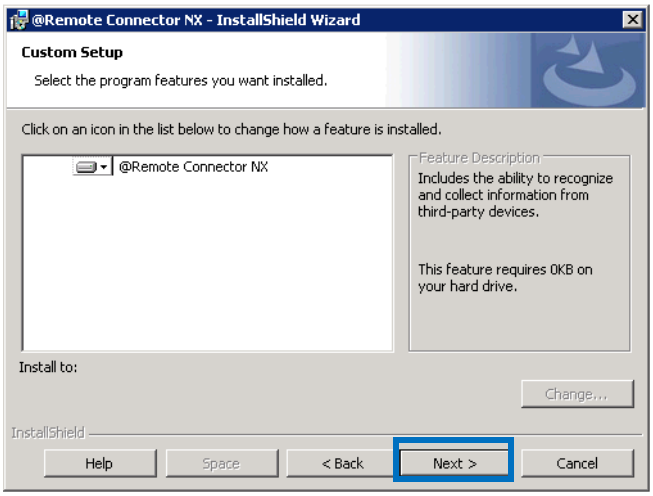
7. In the **Setup Type** screen, select **Complete** to install all components on this machine, or click **Custom** to choose the individual components.



8. Click **Next** to Continue.

9. In the Custom Setup screen, verify the components to install, then click **Next** to continue.

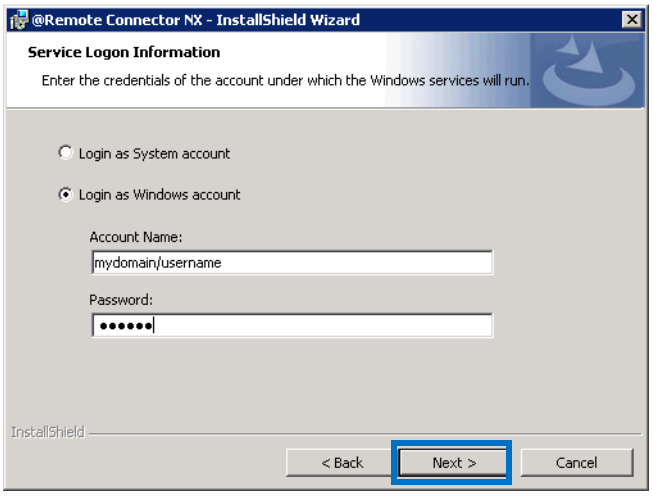
NOTE: This screen appears only if you chose Custom setup.



TIP: To determine space requirements for a selected feature, click **Space**.

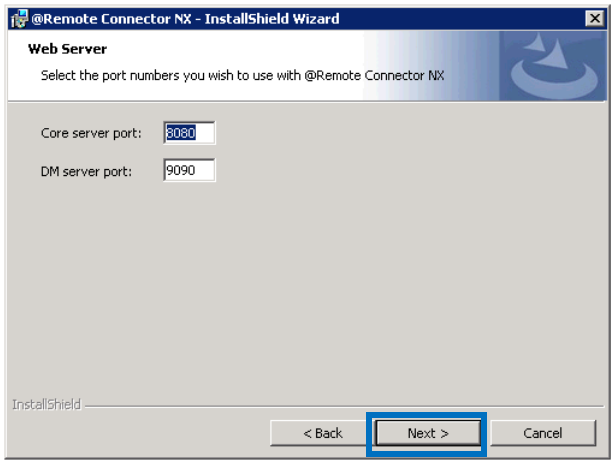
10. In the **Service Logon Information** screen, choose the account under which the @Remote Connector NX service(s) will run. Click **Next** to continue.

NOTE: If using Windows Authentication Mode with SQL Server, you must use a Windows account.



@Remote Connector NX will validate the credentials before proceeding.

11. In the **Web Server** screen, verify the communication ports for the DM Server and Core Server. The defaults are port 8080 for the Core Server, and port 9090 for the DM Server. Click **Next** to continue.

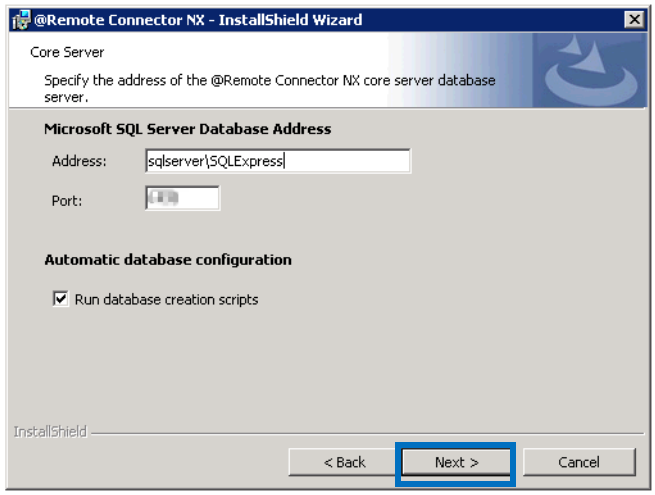


NOTE: The DM Server port is used to communicate with the devices. The Core Server port is used to communicate with the @Remote Connector NX database. If you are using IIS, the Core Server port will also be used when IIS communicates with the Core Server.

12. In the **Core Server** screen, enter the SQL Server address and instance.

    For example, if 'sqlserver' is the location and 'SQLExpress' is the database instance, enter `'sqlserver\SQLExpress'`.

13. Also in the Core Server screen, the **Run database creation scripts** option is checked by default to allow the Installer to automatically create and configure the database tables, then start the services.



    If you are using an external database, and SQL Server is already installed and configured with the instance you want, the information you provide for connecting to the database

will be used to run the script when automatically installing the database from the installer.

You should uncheck the Run database creation scripts option if:

- You have not installed SQL Server on the server where it will be run and plan to do so as your next step
- You want to run the create script yourself instead of letting the installer do it.
- You are reinstalling the software

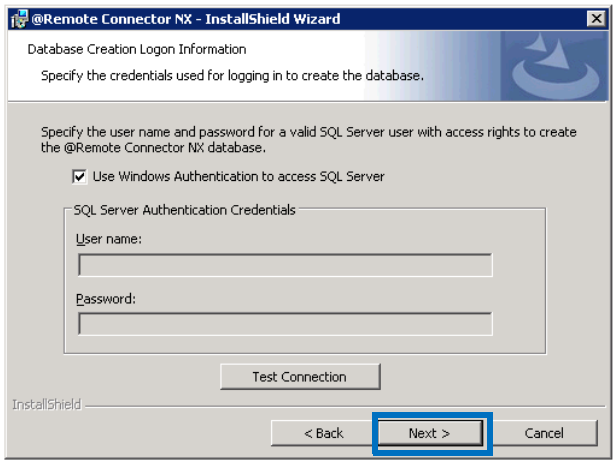
Warning: If you uncheck the option, complete the instructions in *Prepare the Database* on page 21 to ensure the software is ready for first use.

Click **Next** to continue.

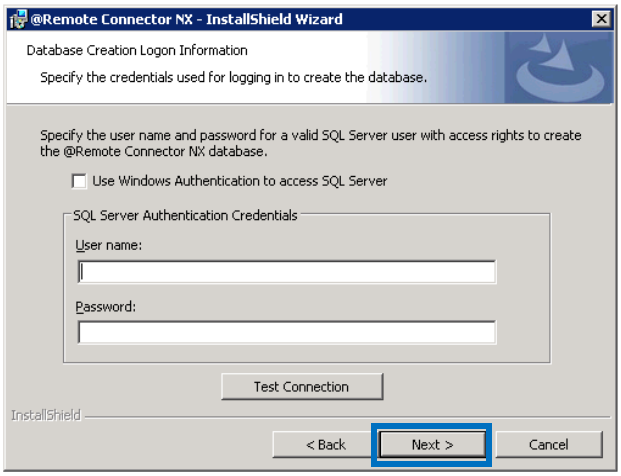
14. In the **Database Creation Logon Information** screen, provide the credentials that the Core Server will use to connect to the database.

    If you previously provided Windows credentials under which the services will run, the 'Use Windows Authentication to access SQL Server' checkbox will be available. Enable the option to check for Windows Authentication to SQL Server, or leave the option unchecked to provide SQL Authentication username and password credentials.

    Click **Next** to continue, then wait while the database is created.



15. In the **Database Creation Logon Information** screen, enter the credentials that will be used to access the SQL database.



16. The installation is now ready to proceed. Click **Install** to continue.

17. When the installation is complete, click **Finish** to complete the process.

Warning: The Central Manager Service is started automatically only if you left the 'Run database creation scripts checkbox' enabled in the installer. If you disabled this checkbox, see *Configure the @Remote Connector NX Database* on page 21 for further instructions.

2.4 Configure the @Remote Connector NX Database

Complete these instructions if both of the following conditions apply:

- If you unchecked the 'Run database creation scripts' option during the install, the database was not automatically configured.
- If you are using an external SQL Server database (as opposed to SQL Express).

Create and configure the database tables using the script installed on the machine where you installed @Remote Connector NX. Afterward, you can start the Central Manager service and the software will be ready for first use.

2.4.1 Prepare the Database

1. Launch the **SQL Server Management Studio**.
2. From the **File** menu, select **Open**, then **File** from the submenu.
3. Browse to the following location:
\Program Files\Ricoh\@Remote Connector NX\data\database

Warning: If the SQL Server Management Studio instance used to manage the database is not installed on the same server as @Remote Connector NX, then copy CreateDMNX_DB.sql to the system running the management tool before completing these instructions.

4. Select **CreateDMNX_DB.sql** to open the file.
5. Click **Execute** to create the default configuration for the database.
6. When the process is complete, close **SQL Server Management Studio**.

2.4.2 Start the Central Manager Service

After the database is successfully configured, start the Central Manager Service (also called the Core Server in the installer):

1. Launch the Windows **Control Panel**.
2. From **Administrative Tools**, launch the **Services** applet.

3. Right-click the **Ricoh_DMNX Central Manager Service** and select **Start** from the menu.

4. Close the Services applet.

The software is now ready for use. You can access the Web Management interface via a web browser at:

http://<coreserveraddress>:8080/index.html

NOTE: If you changed Core Server port during the install, enter that port instead of 8080.

To access the web management interface for the first time, enter the default username 'Admin', and leave the password field blank. Remember to change the password immediately after you login. Refer to the *RICOH @Remote Connector NX Administration Guide* for instructions.

2.4.3 Backup the Database

It is important to backup the <install_dir>\data directory. All information required to restore the database is in this directory. If you restore the database, also restore this directory; however, do not backup or restore the data/database directory.

In addition, you may also need to backup the following files:

- configuration\gc.properties-default – Backup this file if the database connection string was modified after the backup
- configuration\core\config.ini – Backup this file if SSL was enabled or disabled after backup

Backup the Software

1. Using the OS tool, stop the following services:
   - Ricoh_DMNX Central Manager Service
   - Ricoh_DMNX Device Manager Service

2. Make a backup of the database with backup tools that are included with the database.

3. Copy and keep all the data in the data folder that is directly under the install path of the product.

Restore the Software

1. Using the OS tool, stop the following services:
   - Ricoh_DMNX Central Manager Service
   - Ricoh_DMNX Device Manager Service
2. Using the restore tool that comes with the database, restore the database from the backup data.
3. Erase the entire data folder that is directly under the install path of the product and replace it with the data folder copied during the backup process.

2.5 Activation

You must license the software prior to first use. For additional details, refer to the *RICOH @Remote Connector NX Administration Guide*.

RICOH

3

Installing the Software in a Cluster Environment

This chapter describes the process for installing and configuring @Remote Connector NX within an existing Windows cluster environment. This guide assumes that you have already created, configured and tested your Windows cluster or clusters. For information on creating Windows server clusters, refer to your Microsoft documentation.

Before you install in a cluster environment, you must first plan the machines that will be used, and the IP addresses and shared disks that will be assigned.

3.1 Cluster Installation Workflow

When installing in a cluster environment, follow the workflow outlined below.

Note that some steps reference instructions provided in the *Chapter 2: Installing the Software*.

These steps assume that the SQL Server database is already configured on a cluster with high availability.

1 Install @Remote Connector NX on each node **Page 14**

Install @Remote Connector NX on each node, ensuring that you perform the install exactly the same way on every node that will be used as a failover destination.

↓

2 Edit the @Remote Connector NX Configuration **Page 26**

Change the RICOH services start-up type from Automatic to Manual, and edit the gc.properties-default file and add the ports to the firewall.

↓

3 Configure the Core Server Cluster Resources **Page 28**

Run the Failover Cluster Manager to configure the Core Server resource.

↓

4 Configure the DM Server in the Core Cluster Resource **Page 31**

Configure the DM Server in the cluster resource in which Core was configured.

↓

5 Activation **Page 23**

Register licenses to complete software activation.

3.2 Edit the @Remote Connector NX Configuration

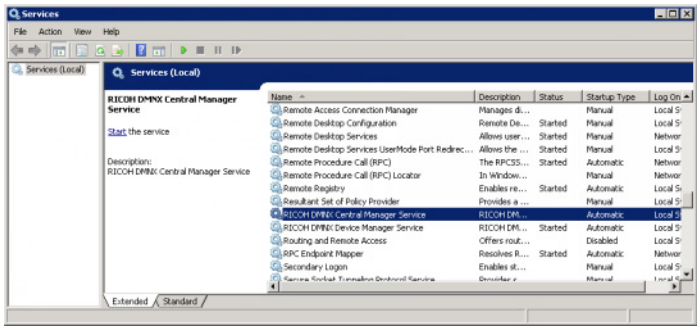
Before completing the instructions below, ensure that you have installed @Remote Connector NX on each node, as outlined in step 1 in the *Cluster Installation Workflow* on page 25.

NOTE: The examples below show the RICOH DMNX Central Manager Service, but also apply to the RICOH DMNX Device Manager Service.

Edit the Service Startup Type

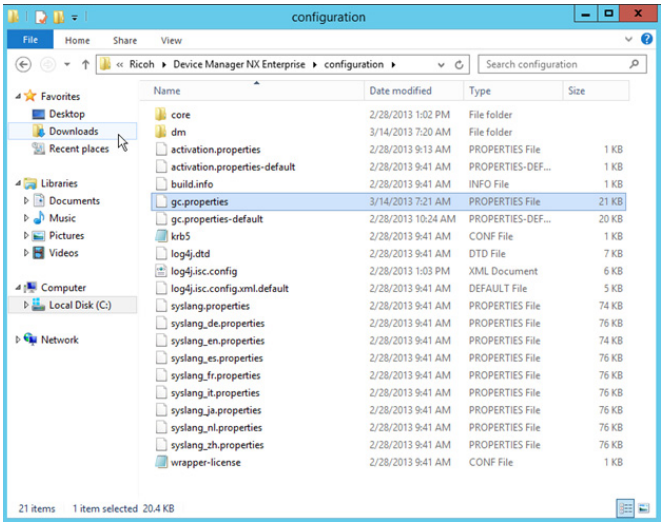
1. On each node where you installed @Remote Connector NX, run the services applet to stop the RICOH services. Change the **start-up type** from Automatic to **Manual**.

   NOTE: The services will not be stopped or started from this applet going forward.



Modify the Properties File

1. Under the installation path, locate the '**configuration**' subfolder.



2. On each node:
   - Delete the gc.properties file
   - Edit the gc.properties-default file in notepad:
     - Search for the setting "core.address" and set it to the address or name of the cluster resource or server on which Core will be running:
       `core.address=192.168.56.21`

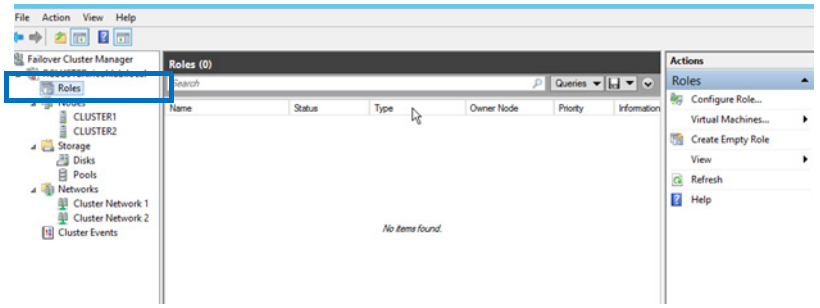
Port Configuration

1. Add the ports configured during the installers as exceptions in the firewall.

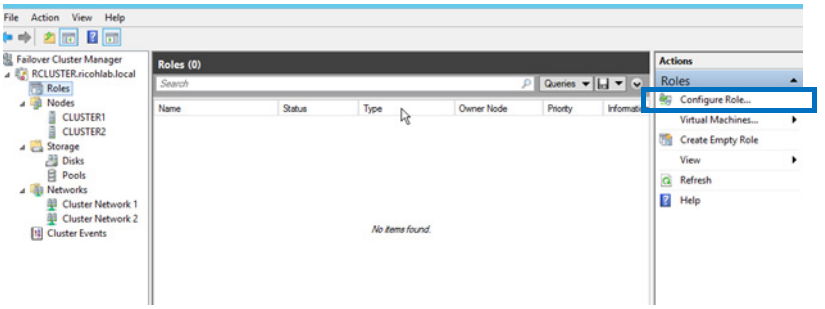
3.3 Configure the Core Server Cluster Resources

1. Run the **Failover Cluster Manager** and connect to the cluster.

2. Select **Roles** from the Navigation tree on the left.

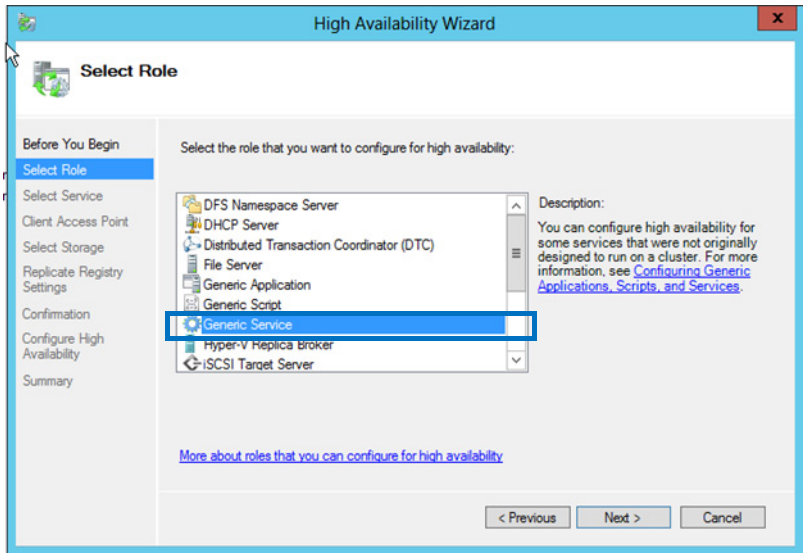


3. From the Action list on the right, click **Configure Role.**

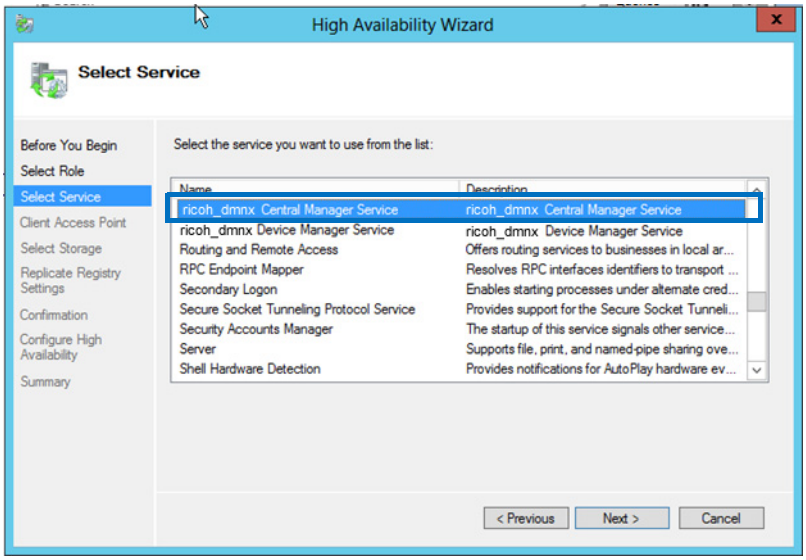


4. On the Before You Begin screen, click **Next**.

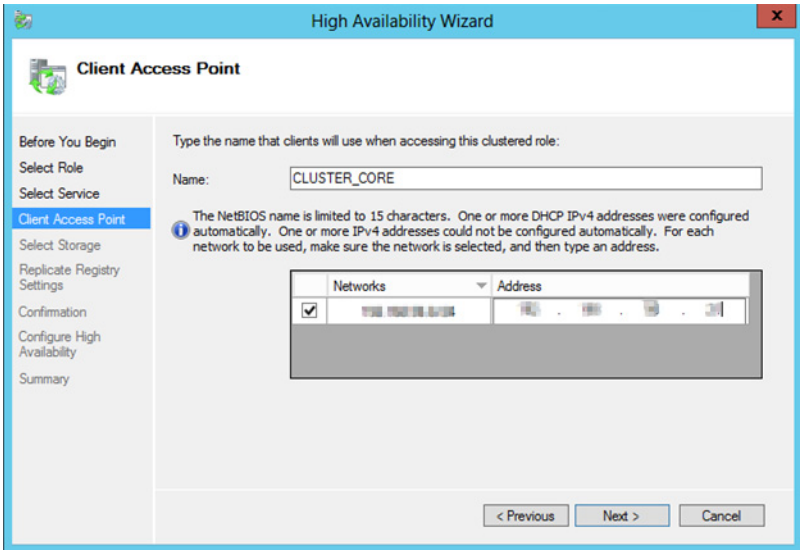
5. On the Select Role screen, select the **Generic Service** role, then click **Next**.



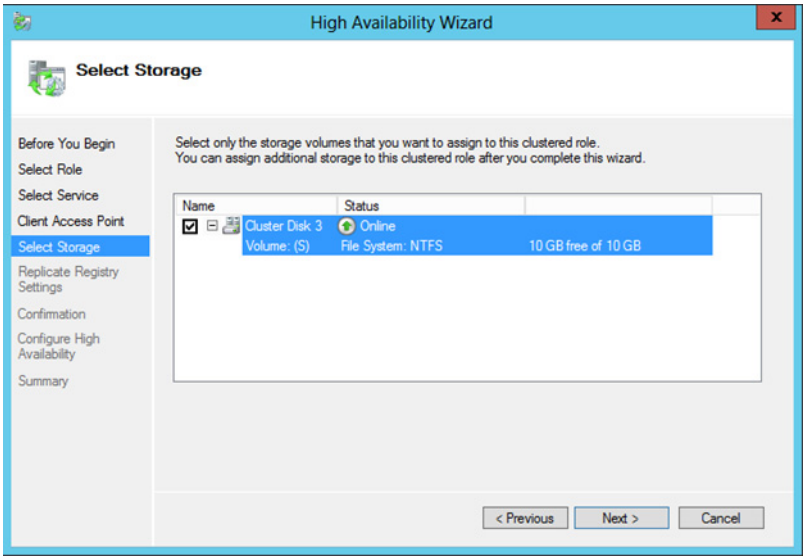
6. In the Select Service screen, select the **RICOH DMNX Central Manager Service**, then click **Next**.



7. In the Client Access Point screen, type the **name of the access point** that client machines will connect through to communicate with the Core Service. Click **Next** to continue.



8. In the Select Storage screen, choose the **storage location** where the Core will store its file repository. This storage disk will failover with the cluster role, so it is always accessible by the Core regardless of the node on which it is running.



9. In the Replicate Registry Settings screen, no registry replication is required. Click **Next** to continue.

10. Review the configuration and click **Next** to complete the wizard.

11. Take the Core Service offline if it was automatically started.

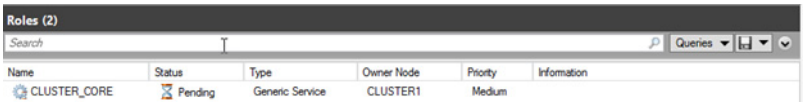
12. On each node, under the installation directory, browse to `Device Manager NX Enterprise\configuration\core` and **edit the wrapper.conf file** to add the following line to the Java Additional Parameters section:

    ```
    wrapper.java.additional.3=-Dconf.datastoragepath=S:\core
    ```

    where 'S' is the drive letter of the cluster storage disk configured in step 8 above.

13. **Bring the S: drive online** (or the appropriate drive letter) on one of the nodes. On the same drive, create a folder named 'core'.

14. Bring the **Core cluster resource online**.



15. Connect via a supported web browser to the Core Server to verify correct configuration.

16. Failover the Core cluster role to all nodes and ensure they work as expected.

3.4 Configure the DM Server in the Core Cluster Resource

1. On each node, under the installation directory, browse to `Device Manager NX\configuration\dm` and **edit the wrapper.conf file** to add the following line to the Java Additional Parameters section:

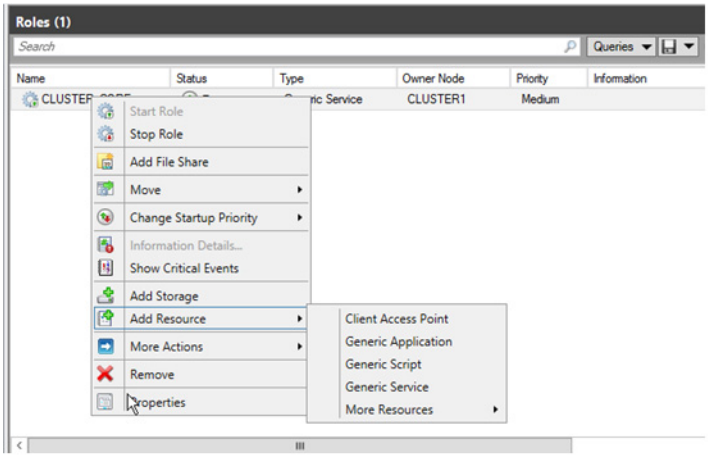
   ```
   wrapper.java.additional.5=-Dderby.system.home=S:\dm
   ```

   where 'S' is the drive letter of the cluster storage disk configured in step 8 above.

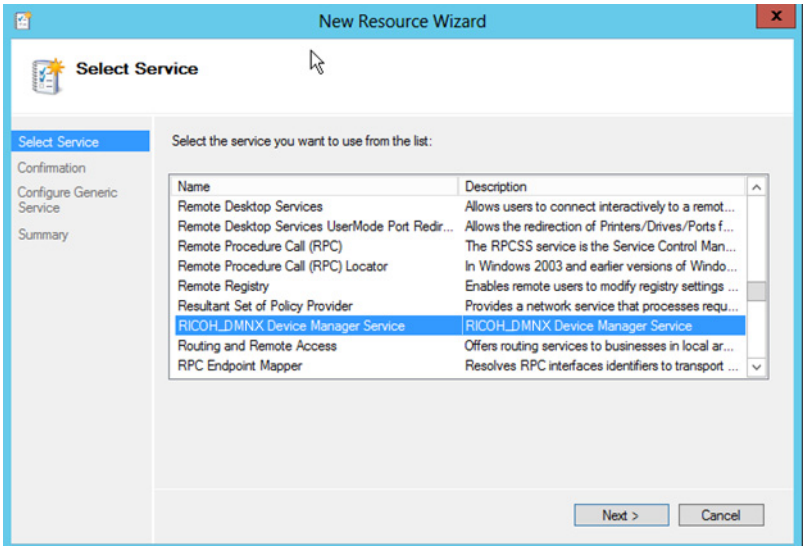
2. **Bring the S: drive online** (substitute the appropriate drive letter) on one of the nodes. On the same drive, **create a folder named 'dm'**.

3. Run the **Failover Cluster Manager** and connect to the cluster.

4. Select **Roles** in the left pane, then right-click on the existing cluster resource for Core and select **Add Resource→Generic Service**.

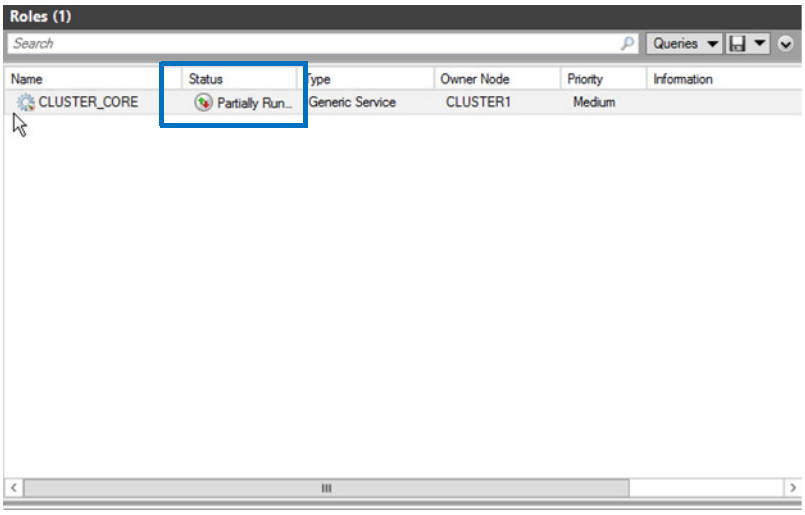


5. Select the **RICOH_DMNX Device Manager Service**.

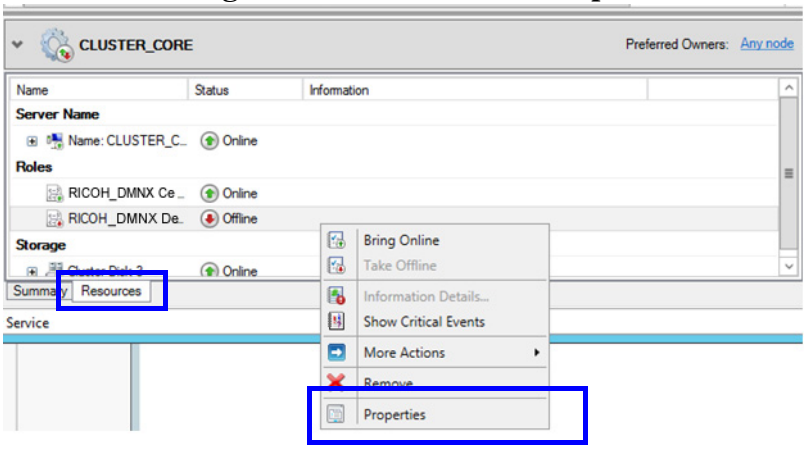


6. Review the configuration and click **Next** to complete the wizard.

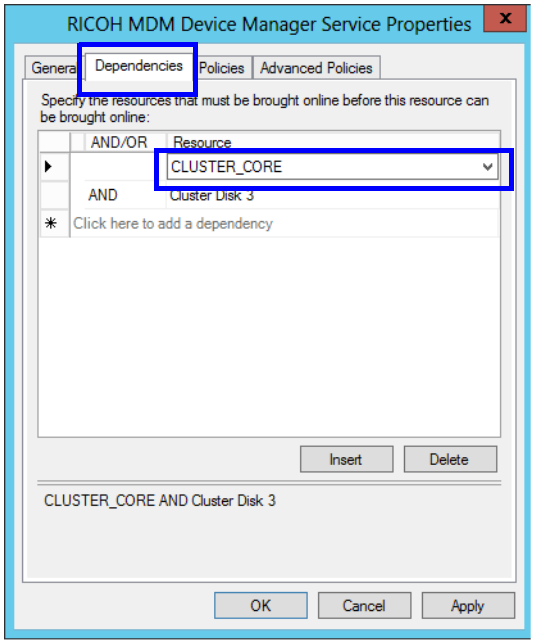
The Cluster Resource should indicate a status of 'Partially Running'.



7. At the bottom of the screen, switch to the **Resources** tab, then right-click on the **Device Manager Resource**, and select **Properties**.



8. Switch to the Dependencies tab, and add the Cluster Server Name and Cluster Storage disk as dependencies.



9. Bring the cluster resource completely online.

10. Failover the cluster resource to all nodes to ensure it comes online properly.

RICOH

4

Uninstalling, Modifying, or Reparing the Install

If you run the installer on the machine where you have installed @Remote Connector NX, you have the option of repairing, modifying or uninstalling the software.

Repair	• Fix missing or corrupt files, shortcuts or registry entries.
Modify	• Change the installed @Remote Connector NX components on the machine.
Uninstall	• Remove all @Remote Connector NX program files on the machine.

4.1 Uninstall Workflow

The uninstall process automatically removes all @Remote Connector NX programs files on the machine. You must run the uninstall on each machine that @Remote Connector NX is currently deployed on.

The uninstall process does not uninstall the SQL Server or SQL Express database. For database uninstall instructions, refer to the Microsoft website for full documentation.

Ensure that you close all other programs before you run the uninstall. The process may require a reboot to completely remove the files.

Warning: If @Remote Connector NX is running in a clustered environment, remove the Core and DM cluster resources before uninstalling from the nodes.

1. Launch the **Windows Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Locate and then double-click @Remote Connector NX.
4. Click **Yes** to confirm that you want to uninstall the software.

   The uninstall will proceed in minimal UI mode. To confirm the uninstall, verify that @Remote Connector NX no longer appears in the Programs list.
5. If you installed the product in a cluster configuration, you can now remove the shared resource folders (Core and DM) from the machine where the product was installed.

NOTE: Alternatively, you can run the @Remote Connector NX installer and choose the Remove option to remove the components. However, if the installer is not available, follow these instructions to uninstall using the Windows Control Panel instead.

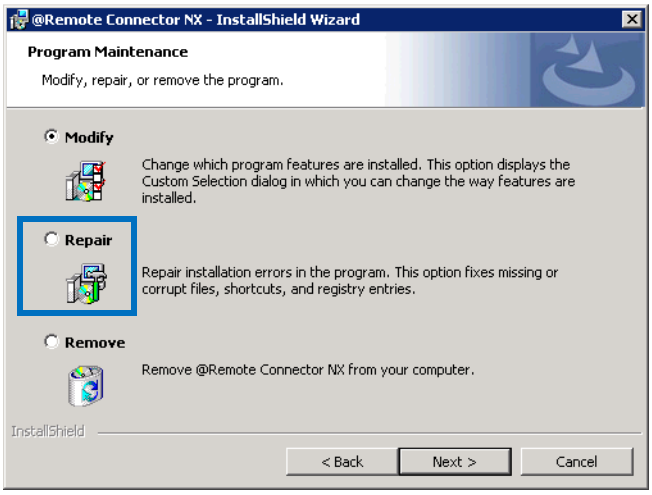
4.2 Repair Workflow

If you are experiencing a problem after you install @Remote Connector NX, you can try re-running the installer and using the Repair option to fix missing or corrupt file, shortcuts or registry entries.

1. Run the @Remote Connector NX Installer. The Installer will detect that one or more @Remote Connector NX components are already installed on the machine.

2. Click **Next** at the Welcome screen.

3. From the Program Maintenance screen, select **Repair** and then click **Next**.



4. Click **Install** to begin the process. The Installer will install any missing or corrupt files.

5. Click **Finish** when complete to close the Installer.

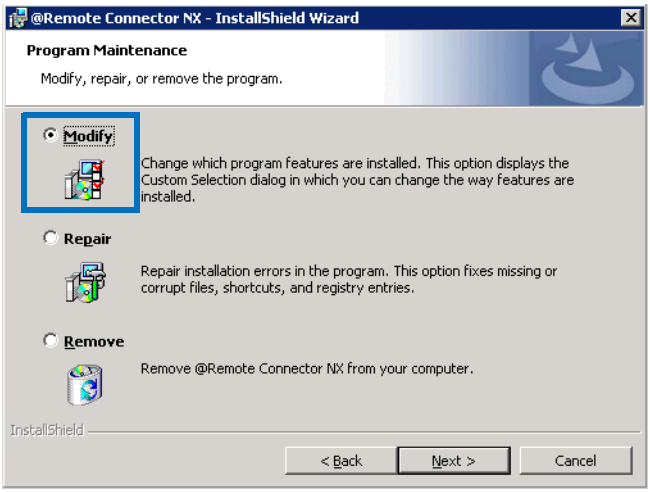
4.3 Modify Components Workflow

If you previously installed one or more components on a particular computer, and you want to add or remove a component, you can run the installer to modify the install.

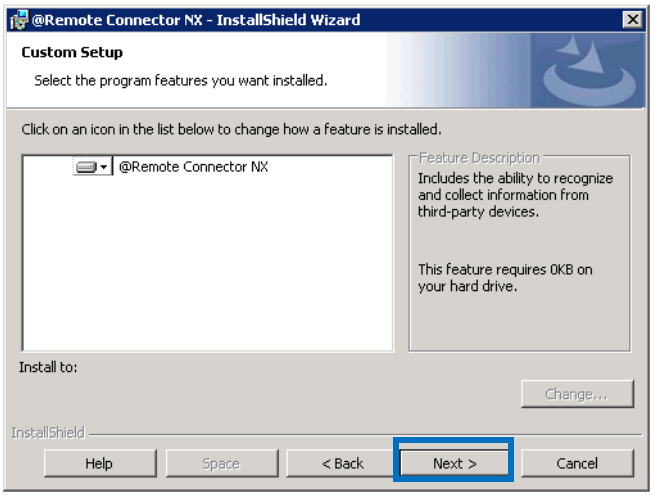
1. Run the @Remote Connector NX Installer. The Installer will detect that one or more @Remote Connector NX components are already installed on the machine.

2. Click **Next** at the Welcome screen.

3. From the Program Maintenance screen, select **Modify** and then click **Next**.

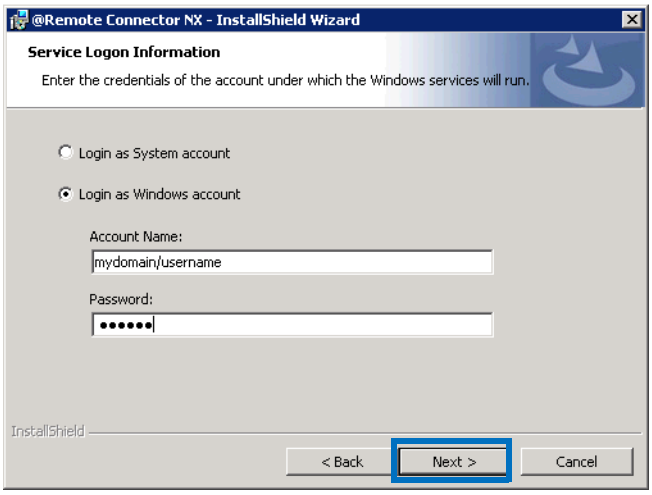


4. From the Custom Setup screen, deselect the components you do NOT want to install on the device, then click **Next**.



5. In the **Service Logon Information** screen, choose the account under which the @Remote Connector NX service(s) will run. Click **Next** to continue.

   NOTE: If using Windows Authentication Mode with SQL Server, you must use a Windows account.



   @Remote Connector NX will validate the credentials before proceeding.

6. Identify the Core server port (by default 8080). Click **Next** to continue.

7. Click **Install** to begin the process.

8. Click **Finish** when complete to close the Installer.

Appendix A: SQL Database Migration

If you have an existing @Remote Connector NX installation and wish to migrate the database, you can migrate the following versions:

- From Microsoft® SQL Server® 2012 Express to Microsoft® SQL Server® 2008 or 2008 R2, or Microsoft® SQL Server® 2012
- From Microsoft® SQL Server® 2008 or 2008 R2 to Microsoft® SQL Server® 2012

Warning: Ricoh recommends creating a new database instance (on the same machine or on another machine) whenever possible, rather than attempting to upgrade SQL Server in place. This will decrease down time and make it easier to revert in the event of an error.

1. Before performing the migration, ensure that you backup the database.
2. Stop the @Remote Connector NX Central Manager Service:
   a. Launch the Windows **Control Panel**.
   b. From **Administrative Tools**, launch the **Services** applet.
   c. Right-click the **RICOH DMNX Central Manager Service** and select **Stop** from the menu.
3. Use Microsoft's migration tools to move the database instance from one version to the other.
4. If the database connection information changed, update the information stored in the gc.properties file. This file is located in the Ricoh/@Remote Connector NX/Configuration folder where @Remote Connector NX is installed.
5. Modify the following line (following the example below):

   core.database.url=jdbc:sqlserver://
   <ServerName>\\<InstanceName>:<port>;DatabaseName=ricoh_dmnx;integratedSecurity=true;

   Example:

   core.database.url=jdbc:sqlserver://localhost\\sqlexpress:51416;DatabaseName=Ricoh_dmnx;integratedSecurity=true;

Entry	Used in the Example
<ServerName>	localhost

Entry	Used in the Example
<InstanceName>	sqlexpress
<Port>	51416

d. In the Windows Services applet, start the @Remote Connector NX Core Server service. Right-click the **RICOH DMNX Central Manager Service** and select **Start** from the menu.

Appendix B: IIS Configuration

Perform the steps below to configure an IIS server to redirect IIS requests to Jetty if you prefer to expose IIS. The following requirements must be met:

- IIS v7.0 or later is required
- IIS Application Request Routing version 2.5 is installed via the Web Platform Installer (see http://www.iis.net/downloads/microsoft/application-request-routing)

  The following ARR components must be installed:

  - URL Rewrite 2.0
  - Web Farm Framework 1.1
  - Application Request Routing 2.5
  - External Cache 1.0

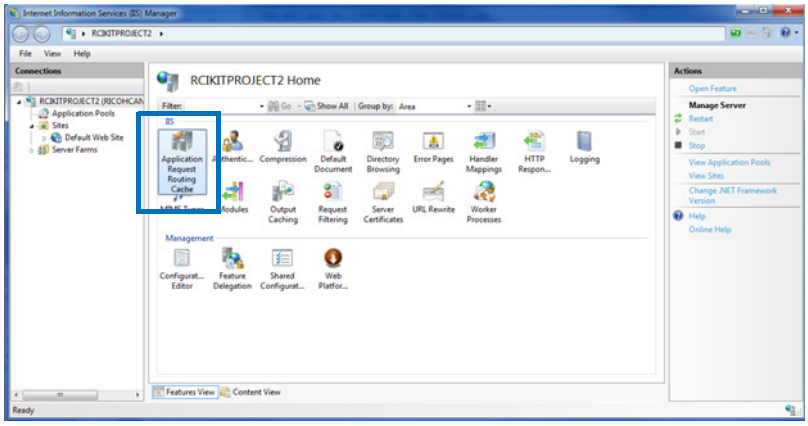
Configuring @Remote Connector NX with IIS

After installing @Remote Connector NX with IIS on the same server, launch IIS Manager or use the command line to configure IIS to work with @Remote Connector NX. If using the command line, open the command prompt as the Administrator, and navigate to `%windir%\system32\inetsrv`.

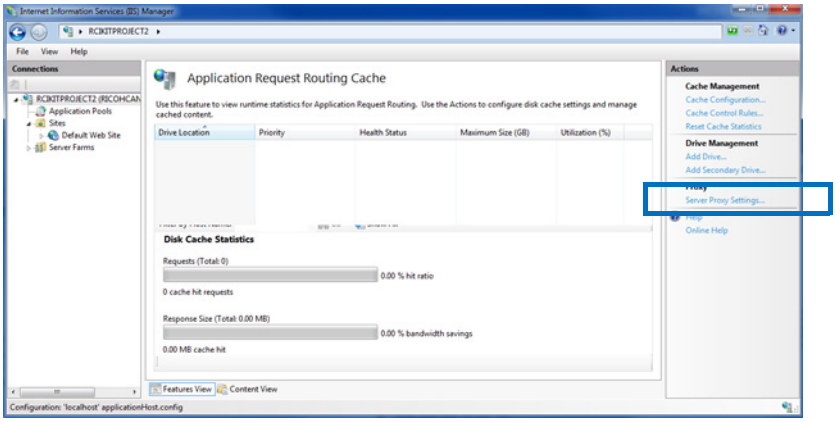
Configure IIS as a Proxy Server

IIS will be configured to forward HTTP requests to @Remote Connector NX using a proxy.

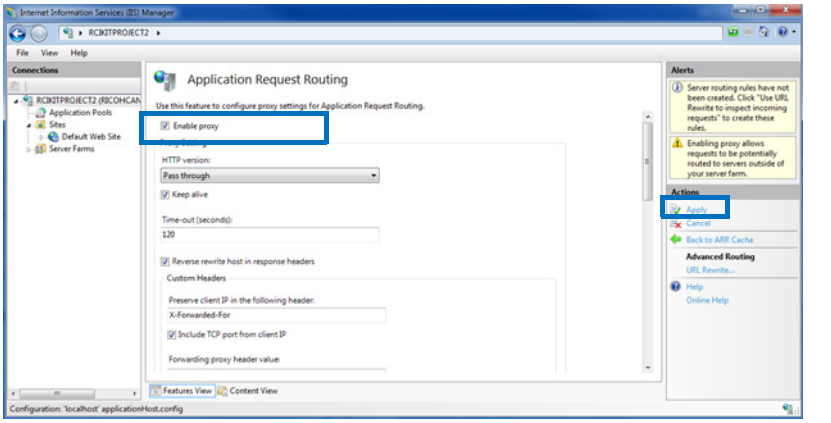
1. Select **Application Request Routing Cache**.



2. In the Actions pane, click **Server Proxy Settings**.



3. Select the **Enable proxy** checkbox, and leave the remainder of the changes at the defaults. Click **Apply** from the Actions on the right side of the screen.



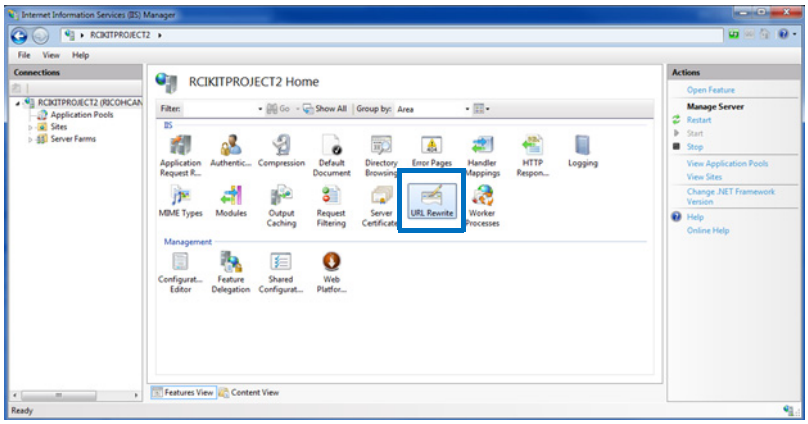
NOTE: To perform these steps from the command line rather than within the IIS Manager, run the following command:

```
appcmd.exe set config -section:system.webServer/proxy /
enabled:"True" /commit:apphost
```

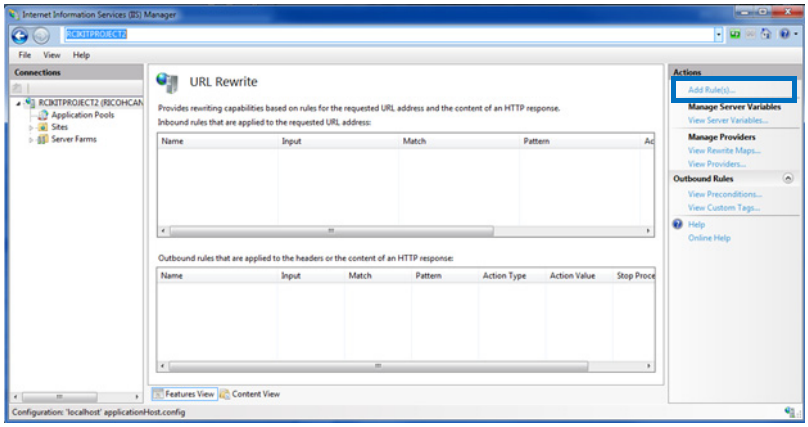
Redirect Configuration

To configure the redirection of IIS to @Remote Connector NX, the first step is to add a configuration to rewrite the IIS URL to the @Remote Connector NX URL.

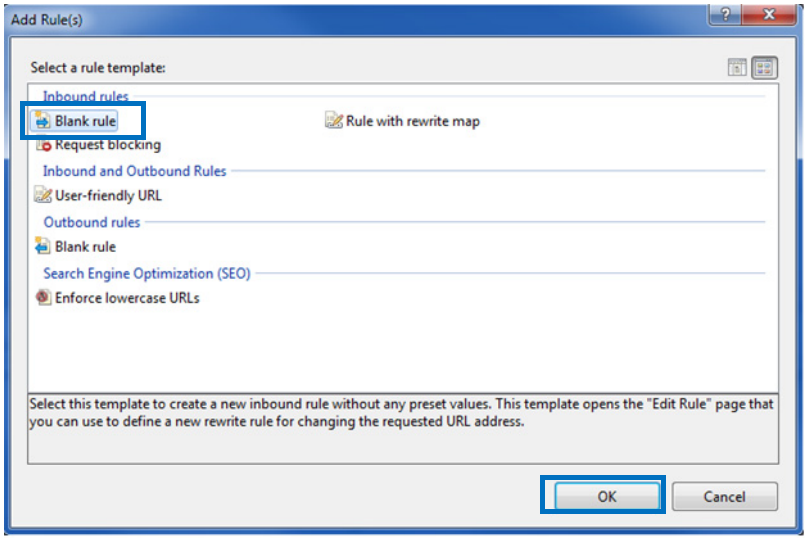
1. Select **URL Rewrite**.



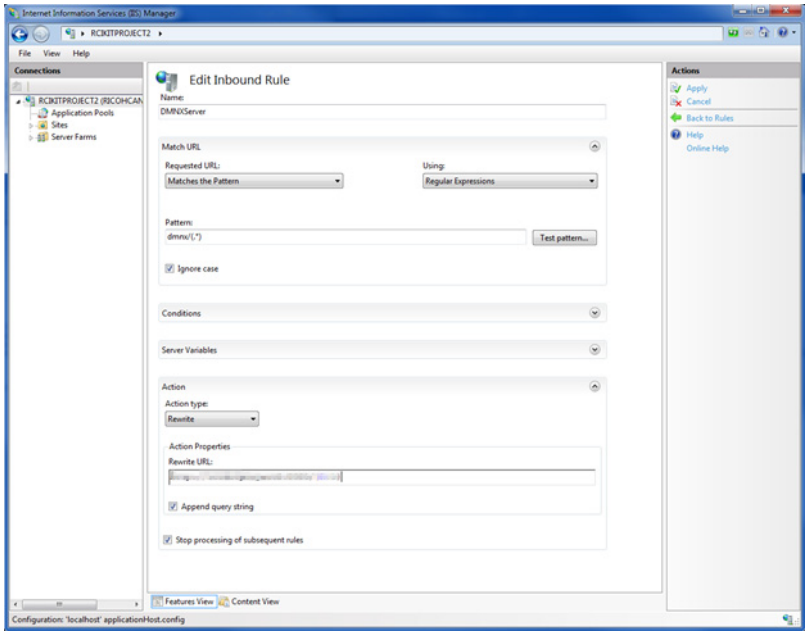
2. In the Actions pane, click **Add Rule(s)**.



3. Select **Blank rule** under Inbound rules, and click **OK**.



4. Configure the rule to redirect the IIS URL to the @Remote Connector NX URL.



Set the following options:

- **Name:** Specify a name for the rule
- **Requested URL:** Matches the Pattern
- **Using:** Regular Expressions

- **Pattern:** Specify the alias to use for the IIS URL followed by a wildcard pattern - "alias/(.*)". For this example, "DMNX" is used.
- **Action Type:** Rewrite
- **Rewrite URL:** The URL to @Remote Connector NX, using the port specified during installation of @Remote Connector NX. The trailing {R:1} indicates that the URL is to use a back-reference to the rule pattern (i.e. Whatever the IIS URL contains after the "dmnx/" will be passed through to the rewrite rule).

5. In the Actions pane, click **Apply** to save the changes.

NOTE: To perform this action from the command line, run the following commands, replacing the %1 value with the alias used (in this example the alias is DMNX), and %2 with the write URL (in this example the rewrite URL is http://rcikitproject2:8080/):

```
appcmd.exe set config -section:system.webServer/rewrite/
globalRules /+"[name='DMNXServer',stopProcessing='True']" /
commit:apphost

appcmd.exe set config -section:system.webServer/rewrite/
globalRules /
[name='DMNXServer',stopProcessing='True'].match.url:"%1/(.*)" /
commit:apphost

appcmd.exe set config -section:system.webServer/rewrite/
globalRules /
[name='DMNXServer',stopProcessing='True'].action.type:"Rewrite"
/[name='DMNXServer',stopProcessing='True'].action.url:"%2/{R:1}"
/commit:apphost
```

Update the Configuration to Indicate IIS is Enabled

1. Under the installation path, located the **configuration** subfolder.

2. Edit the **gc.properties file** and look for the property `system.option.iis`. Update this option to: `system.option.iis = 1`

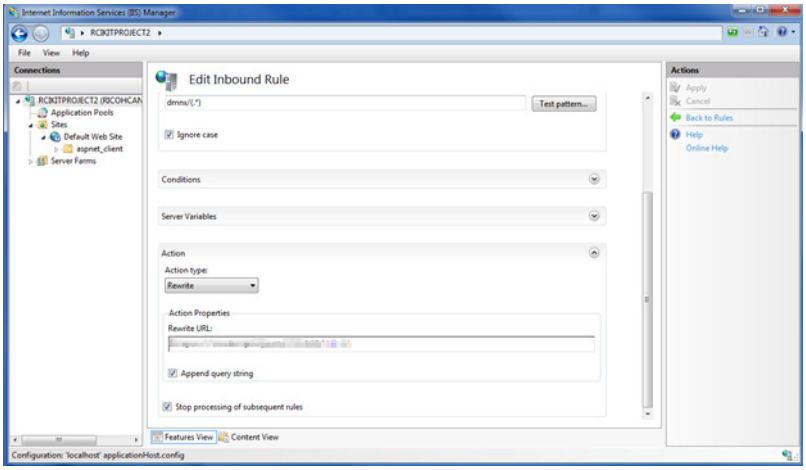
3. Test the redirect using the IIS URL.

Configuring SSL

1. Configure SSL on @Remote Connector NX (see *Change Server Settings* in the *@Remote Connector NX Administration Guide* for instructions).

2. Import the SSL certificate into IIS.

3. Update the redirect URL to be the SSL URL to the @Remote Connector NX server using the port configured for SSL.




RICOH