RICOH @Remote Connector NX
Administration 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.

Document Number

CONNECTOR-ADMIN-A.0

Revision History

Date	Revision Number	Revision Details
	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

CHAPTER 1

Introduction

RICOH @Remote Connector NX provides connectivity to the @Remote Center System to maintain high device availability and efficiency. You can create discovery profiles to locate devices on the network that will be managed within @Remote Connector NX, or configure device discovery and status polling to keep the system current.

This guide is written for Administrators who are configuring @Remote Connector NX for the first time. Use this guide to perform initial configuration tasks and subsequent advanced customization of the management and monitoring aspects of the software.

Warning: Before you can complete the instructions in this guide, a Ricoh Customer Engineer must register @Remote Connector NX in the @Remote Center System.

1.1 Initial Configuration Workflow

If performing configuration of the @Remote Connector NX software for the first time, Administrators should follow the workflow outlined below to ensure the most predictable results. Some tasks rely upon instructions completed in a previous chapter, and therefore it is best to conform to the order shown whenever possible.

1 Create User Accounts	Page 21
Establish user accounts and assign system roles to limit access to the @Remote Connector NX system.	

↓

2 Add Devices to Manage	Page 27
Establish access accounts to allow @Remote Connector NX to contact devices on the network, and then configure automatic device discovery or manually import a list of devices for scheduled discovery.	

↓

3 Organize the Device List	Page 53
Establish custom categories and groups to separate a large fleet of devices into manageable groups reflective of your organization structure or distribution.	

↓

4 Change @Remote Connector NX Server Settings	Page 68
Change settings such as custom properties, date formats, proxy server addresses, and data management options. Also set your @Remote Connector NX password.	

↓

5 Configure @Remote Settings	Page 91
Establish the permission requirements for @Remote Tasks.	

1.2 Additional Information

To learn more about the advanced features and functionality of @Remote Connector NX, refer to the following product information.

Guide	Description
Installation Guide	Use this guide to install @Remote Connector NX.
Online Help Reference	Use the online help available through the Web Management Interface to answer questions about the individual screens and options that appear in the interface.

1.3 Important Terms and Definitions

This guide relies upon the following terms:

Guide	Description
Ricoh Customer Engineer	The Ricoh Customer Engineer who will perform the initial registration with the @Remote Center System.
@Remote Connector NX Administrator	The onsite Administrator who performs initial @Remote Connector NX configuration.
Managed Device	A device that is registered to the @Remote Center System. @Remote Connector NX can manage up to 5000 devices.
Monitored Device	A device that is included in the Device List, but is not registered to @Remote Center System.
@Remote task	An automatic task that occurs at the request of @Remote Connector NX to communicate with the @Remote Center System.
Device status information notification	An @Remote task that periodically provides managed device reporting status information to the @Remote Center System.

Guide	Description
Device counter information notification	An @Remote task that provides managed device reporting counter information to the @Remote Center System on or after a device closing date for meter reading.
Device List update	An @Remote task that updates the managed/ monitored device list registered on the @Remote Center System.

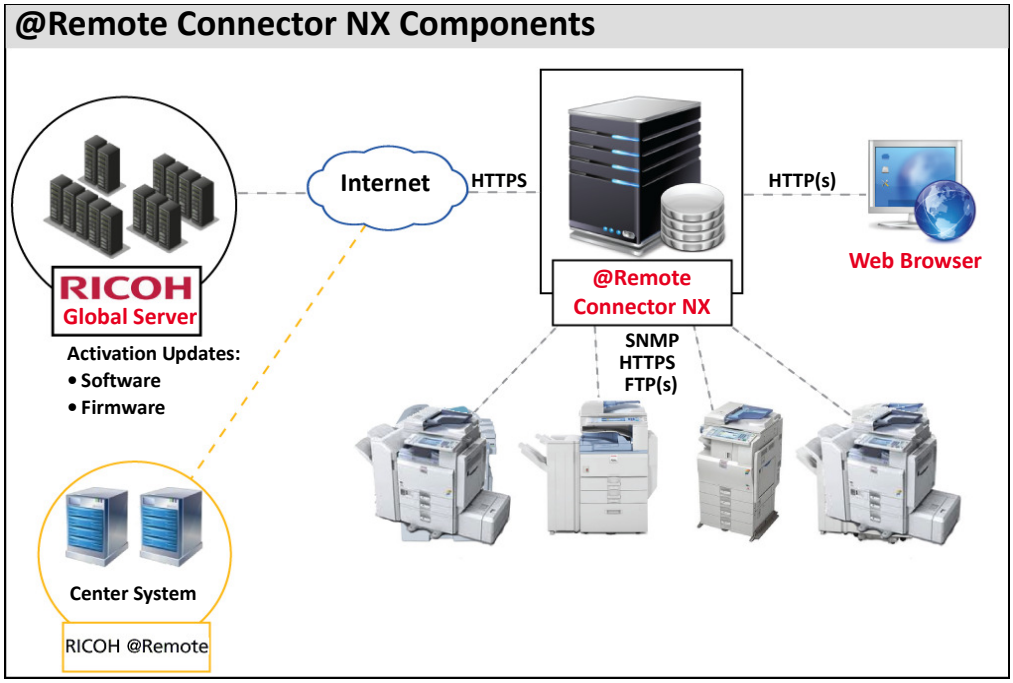
1.4 About RICOH @Remote Connector NX

@Remote Connector NX provides remote fleet management and monitoring of up to 5000 output devices on your network. @Remote Connector NX uses SNMP to remotely monitor devices from all manufacturers. Remote management capabilities include:

- Discover devices in the network and register them in the system
- Retrieve device information to track usage statistics
- Retrieve consumable data for supply tracking and proactive ordering

1.4.1 System Components

@Remote Connector NX requires internet access to communicate with the Ricoh Global Server when obtaining updates and to the Ricoh Activation Server to perform product activation.



- @Remote Connector NX communicates via HTTPS with the Ricoh Global Server to retrieve and apply software and firmware 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 13.

1.5 Supported Models

@Remote Connector NX identifies devices by MAC address, serial number and vendor name (converted from the model name). Although specific management and monitoring support is dependent upon the vendor and model, @Remote Connector NX classifies devices into the following categories:

	Supported Capabilities		
Device Type	**Discovery**	**Basic Device Info**	**Detailed Counters**
G1: Ricoh MFP (A3 size, 2000-2005 release date)	✓	✓	✓
G2: Ricoh MFP or printer (A3/A4 size, 2005-2011 release date)	✓	✓	✓
G3: Ricoh MFP or printer (A3/A4 size, 2012+ release date)	✓	✓	✓
R1: Ricoh MFP or printer (A4 size)	✓	△	✓
R2: Ricoh GelJet MFP or printer (A4 size)	✓	△	✓
R0: Other Ricoh MFP or printer	✓	△	△
Devices from other manufacturers	✓	△	△

△ = **Partial support**

1.6 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

1.7 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 the @Remote Connector NX.

1.8 Logging In

To access @Remote Connector NX, you must have a valid user name and password.

1. If you are accessing @Remote Connector NX from the local server, you can use the shortcut on the Start menu to access the software.

OR

1. If you are accessing @Remote Connector NX from across the network, open a web browser, and enter `http://<server_name>:8080/index.html` in the address field, where server_name is either the IP address or name of the @Remote Connector NX server. By default, @Remote Connector NX uses port 8080 to communicate. If you selected a different port when installing @Remote Connector NX, enter the correct port number instead.

   NOTE: If SSL is enabled, enter https instead of http in the address field. For information about enabling SSL, see *5.1.1 Enable the Proxy Server* on page 69.

2. On the Login screen, select the correct **profile** from the list.

NOTE: If this is your first time logging in after installation, use 'admin' as the user name, and leave the password field blank. Ensure that you change this password immediately. See *1.11 Changing A Password* on page 20.

3. Type your **User Name** and then your **Password**. The password is case-sensitive, so make sure you enter it correctly. Click **Login** to continue.

4. Select the language to apply to the @Remote Connector NX interface.

1.9 Activation

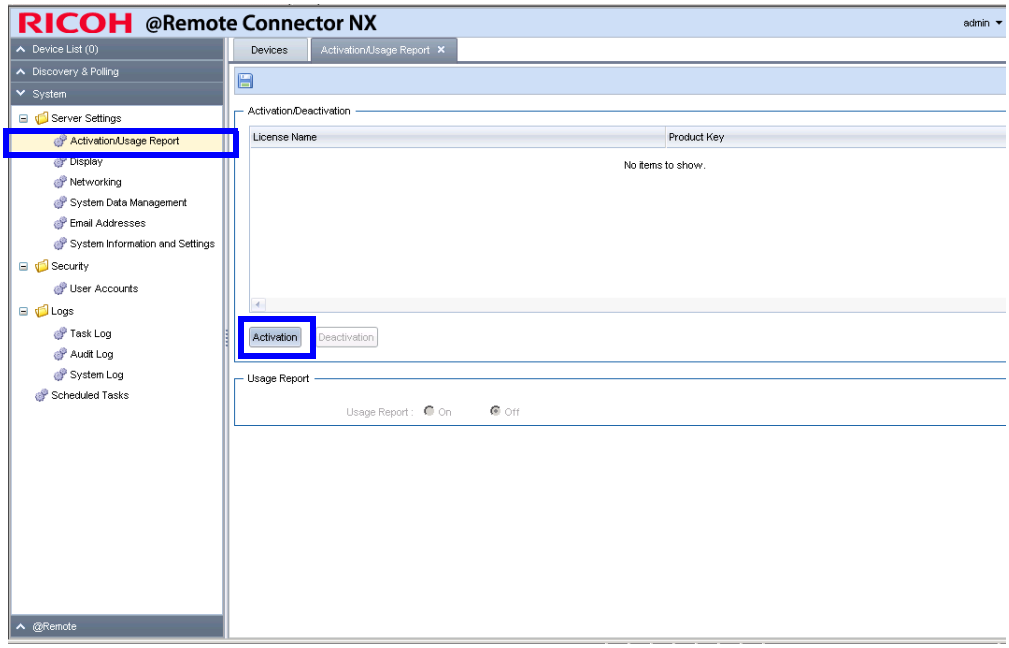
Activation can be accomplished online or offline. Online activation requires internet connectivity to allow @Remote Connector NX to contact the Ricoh Activation Server (https://licensemanagement.ricoh.com/aui). You require the Product Key provided to you at time of purchase.

NOTE: If your network uses a proxy server to hide IP Addresses, you need to set the proxy server information before you can perform activation. See *5.1.1 Enable the Proxy Server* on page 69 for instructions.

1.9.1 Online Activation

1. On the Navigation Tree, click **System**.

2. Under Server Settings, click **Activation/Deactivation/Usage Report**.



3. Click **Activation**.

4. To perform online activation, select **Online**, then enter the Product Key, and select the appropriate country.

NOTE: When @Remote Connector NX was installed, the installer referenced the Windows regional settings to determine the country settings. You may need to change this setting during activation because it determines the download location for external applications.

The product is now fully licensed and active.

1.9.2 Offline Activation

If you are unable to ensure internet connectivity on the server on which you installed @Remote Connector NX, follow these steps.

1. Contact Ricoh to obtain the license codes for @Remote Connector NX.

2. Use an internet-ready PC to enter the codes on the Ricoh Activation Server website at https://licensemanagement.ricoh.com/aui. The Activation Server will generate the required license information.

3. Copy the license information for each component carefully, then login to @Remote Connector NX to enter the codes.

4. On the Navigation Tree, click **System**.

5. Under Server Settings, click **Activation/Deactivation/Usage Report**.

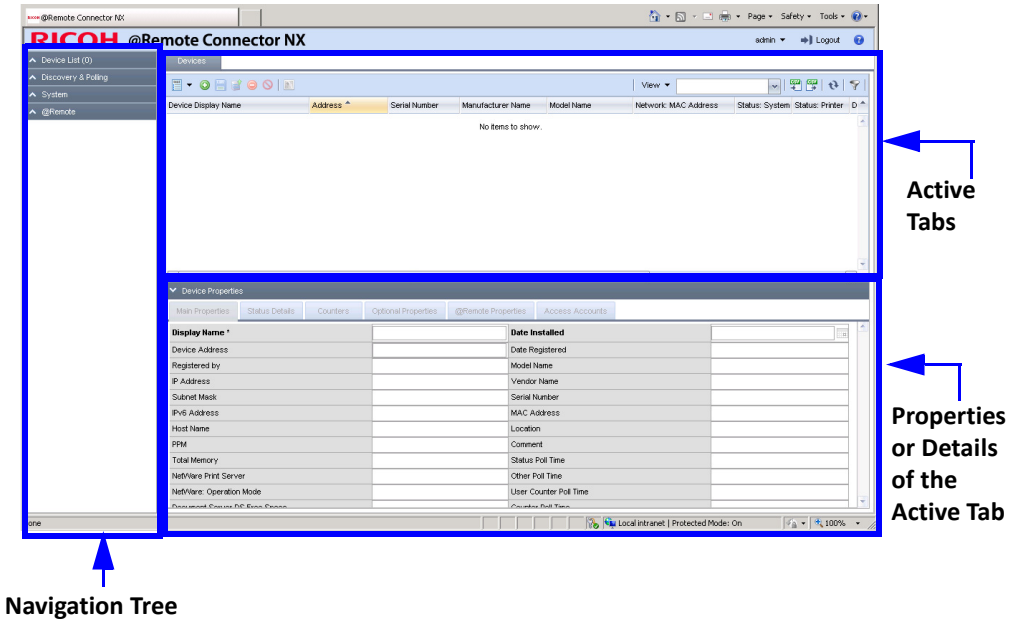
6. Click **Activation**, then enable **Offline**.

7. In the Activation field, enter the **License Code**, then click **OK.**

If the code was successful, the product is now fully licensed and active, and device monitoring and management can occur when internet connectivity is in place.

1.10 Getting Around the Interface

The @Remote Connector NX web management interface is divided into three main areas for easy navigation.



The Navigation Tree

The Navigation Tree is anchored to the left of the screen, and contains the following branches:

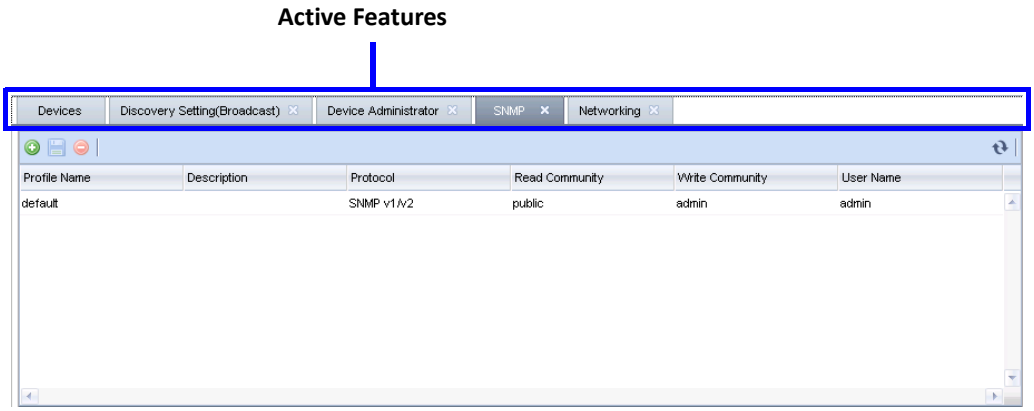
- Device List
- Discovery & Polling
- System
- @Remote

When you first launch @Remote Connector NX, the Device List branch is open at the top of the Navigation Tree. A branch is a collection of features that are grouped by function. If you click on a feature within a branch, the feature opens as new tab in the Active Tabs area.

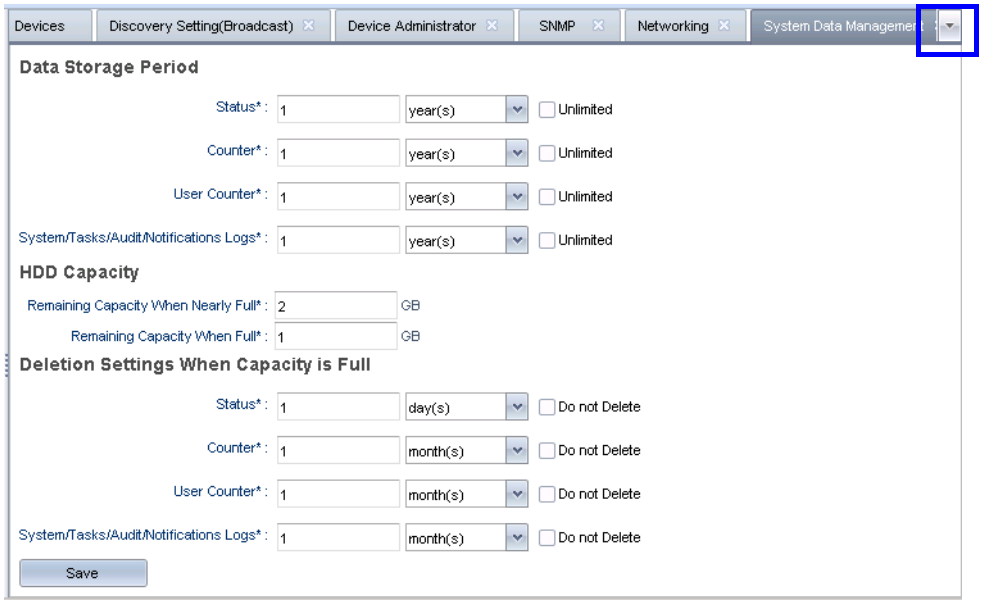
To open a branch, click on the branch name. The branch opens at the top of the Navigation Tree, hiding the Device List options. The branches are always shown in the same order for ease of access.

1.10.1 Active Features

When you click on a feature within a branch, the feature opens as a new tab in the Active Tabs area.



- To switch between features, simply click on the tab name.
- To close a tab, click on the X that appears to the right of the name.
- To close all tabs, right-click on any tab name, then choose Close All or Close All But Current from the menu.
- When you open more tabs than can fit on the screen, a drop-down arrow appears to the right of the tab names. Click on the arrow to view a list of all Active Tabs. The current tab is checked. Select another tab to make it the current view.

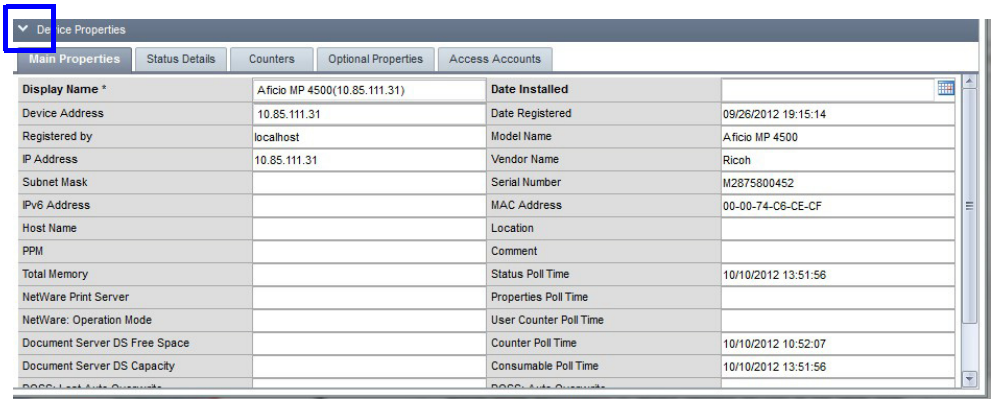


1.10.2 Options Bar

The Options bar contains various tools required for the active feature. Although the Options bar is always located in the same place on the active feature, the tools that are available may be slightly different depending on the requirements of the feature.

1.10.3 Properties/Details

Each active feature may use the Properties/Detail area located below the main feature items. For example, if you view a Devices list, the upper portion of the active feature lists the device, and the bottom portion of the screen is used to present individual device details. You can click on the up or down caret to hide or show this area as needed.



1.10.4 Time and Timezones

Within @Remote Connector NX, time is handled in different ways based on the following:

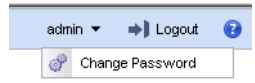
- All times for device activity stored in the database is reported in the @Remote Connector NX Server's local time.
- Time displayed in the @Remote Connector NX management interface is based on the browser settings.
- Tasks are run according to the @Remote Connector NX Server local time.

1.11 Changing A Password

If a user forgets their password, you can change the local account password at any time.

1. On the Navigation Tree, click **System**, then locate the **Security** folder.

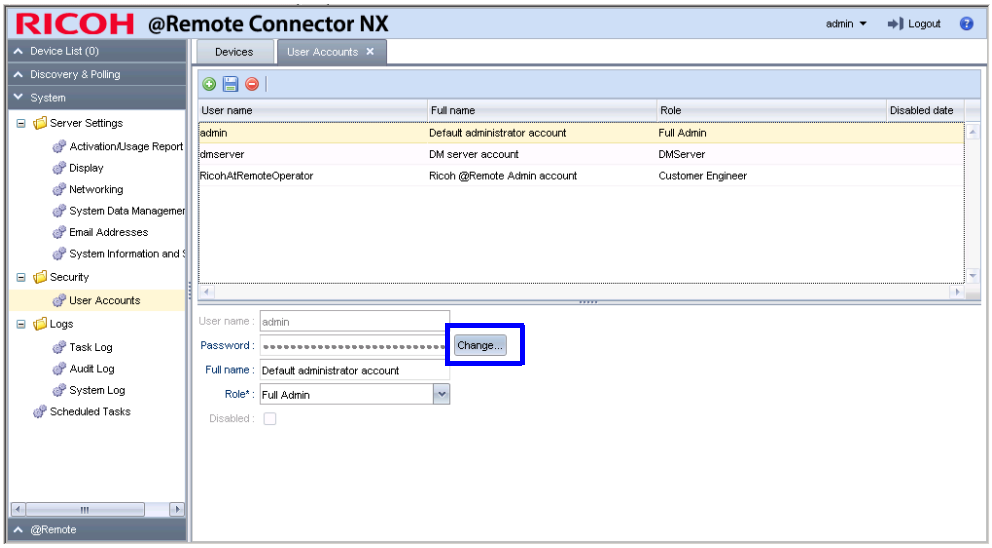
   TIP: Optionally, to change your own password, click on your login ID in the top right corner, and select Change Password. Skip to step 5 below to continue.



2. Click **User Accounts**.

3. Select your user account from the list to enable edits to the information at the bottom of the screen.

4. Click the **Change** button beside the Password field.



5. Type a new **password**, and then re- type the identical password to **confirm** it, then click **OK** to continue. The new password should use a combination of upper and lower case letters, plus at least one number for additional security. Passwords must be at least 6 characters in length.

6. On the User Accounts tab Options bar, click **Save**.

CHAPTER 2

Create User Accounts

Establishing user roles early in the configuration process is important because these settings control who can access the software, and determine the aspects of the software each user can see and modify.

This section includes information about the default security roles that you can use to limit access to features in @Remote Connector NX, and instructions to create users accounts. You will also find information about using the Audit Log to track user activity in this chapter.

2.1 Access Roles & Privileges

The features and functionality granted to a user are determined by the user access role that is assigned to their user account. When you create a user account, you are required to assign a user role to their account. Before you create user accounts, you should review the default access roles and corresponding privileges.

Three roles are included in @Remote Connector NX by default: DMServer, Full Admin, and Customer Engineer. However, only Full Admin and Customer Engineer should be assigned to users.

Role	Description	Associated Privileges
Customer Engineer	• Ricoh Customer Engineer • When a user logs into @Remote Connector NX with this privilege assigned to their user account, a screen will ask for confirmation before proceeding with the login	• View all information associated with a device • Create, update, and delete discovery profiles, polling profiles, and associated tasks • Modify device access accounts and custom properties • Update email address lists
Full Admin	• @Remote Connector NX administrator with responsibility for setup, configuration, and user account maintenance	• Full access to all privileges within @Remote Connector NX • Create, update, and delete security information including roles and user accounts
DM Server	• Full access to all privileges	• Reserved for communication between the internal @Remote Connector NX components – **should not be assigned to user accounts**

2.2 User Accounts

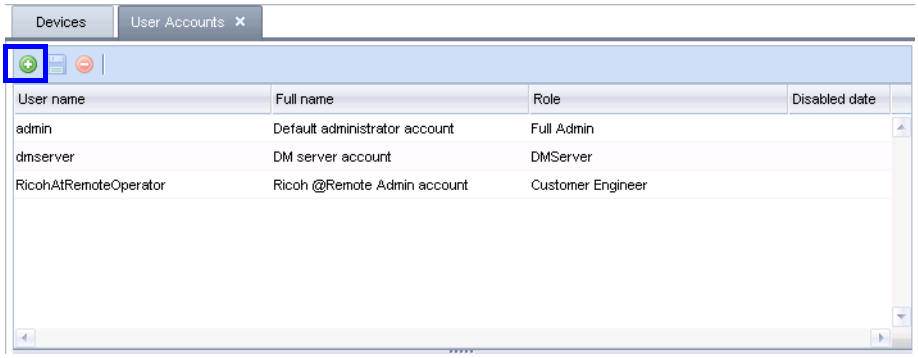
The @Remote Connector NX web management interface provides full account configuration, including password reset and role assignments.

2.2.1 Create a User Account

1. On the Navigation Tree, click **System**, then locate **Security**.

2. Click **User Accounts**.

3. On the Options bar, click **Add** to add a new account.



4. In the Properties area, set the following fields:

Field	Description
User name	• Type a unique name for the user account
Password	• Click the Change button to enter a password, then confirm the password in the Re-type field. The two fields must be identical to continue.
Full name	• Type the users first name and last name
Role	• Select the Access Role that will grant privileges to the user account

Field	Description
Disabled	• Enable this checkbox to temporarily disable an account. Use this option if you do not want to delete an account, but you want to temporarily ensure the user does not have access to the system. • When an account is disabled, the date and time the disable status was set is displayed.

5. On the Options bar, click **Save** to save the user account.

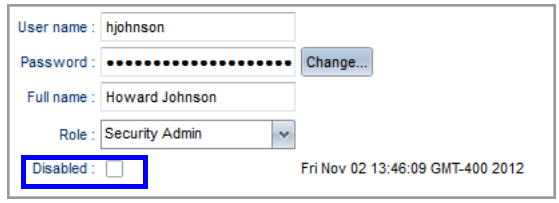
2.2.2 Delete or Disable User Accounts

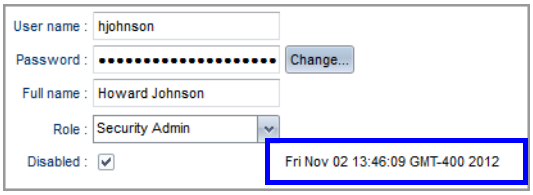
You can delete individual user accounts if necessary, or you can choose to temporarily disable an account if you want to leave account information in the database, but still prevent the user from accessing @Remote Connector NX.

- To delete an account, first click on the account to highlight it, then click Delete on the Options bar.

  NOTE: You cannot delete the Admin, the DMServer or the CustomerEngineer Account – these are system accounts and you will receive an error if you attempt to delete them. However, you can disable these accounts if necessary.

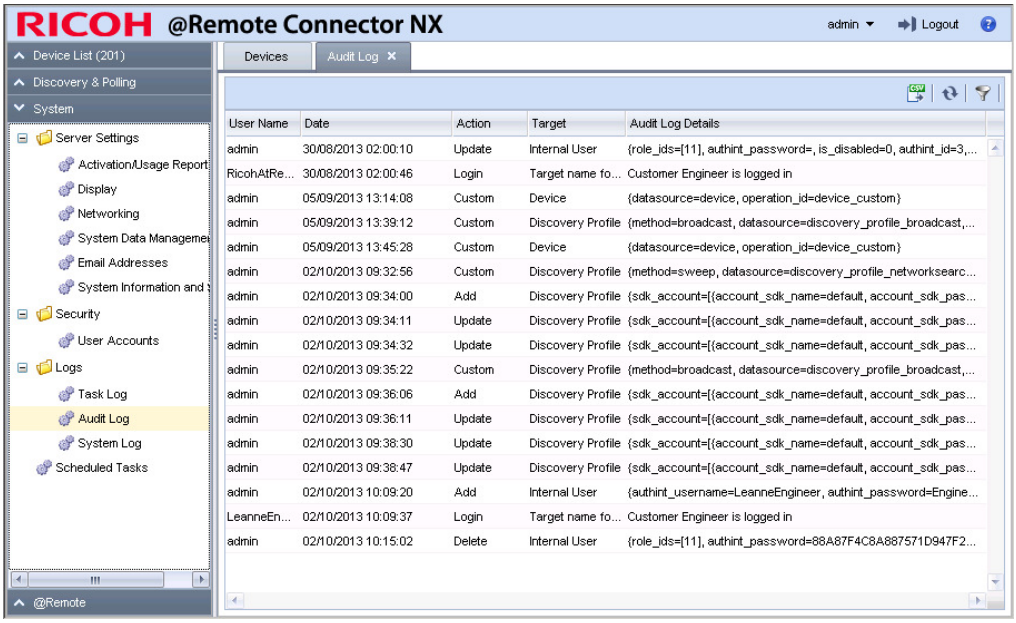
- To disable an account, first click on the account to enable the account properties, then complete the Disabled checkbox. Click Save on the Options bar to disable the account. The properties information will change to indicate the date and time that the account was disabled.





2.3 Tracking User Activity

The read-only Audit Log records all user activity and provides a trail to associate actions with a particular user. For example, in the log example below, you can see that the user "admin" added and updated Discovery Profiles on several dates.



In cases where you have multiple administrators working within the same system, this log can provide a valuable method to track changes made to the following user operations:

- Filter
- View
- Tasks
- Access Account
- System Settings
- Authentication and Accounts

To view the log, click **System** from the Navigation Tree, then click **Logs**. Click **Audit Log**.

This log contains the following fields:

Field	Description
User Name	• Login name of the user that made the change.
Date	• Date and time the change was made.
Action	• The action taken may include Add, Delete, Update, or Custom.
Target	• The location where the action was taken: Device, Discovery profile, Polling profile, SNMP profile, Role, User Account, Internal user.
Audit Log Details	• Specific information related to the Action taken, auto-generated by the system.

You can use the Filters button  on the Options bar to filter the data based on particular fields. You can also export the data to a .csv format file for analysis in third party software.

Next Steps:

- Establish a structure for the Device List before you perform discovery or manual import. See *Chapter 4: Organize the Device List* on page 53.

CHAPTER 3

Add Devices to Manage

There are several methods to locate devices on the network and register them in the system.

Migrate	• Migrate data from an existing RC Gate to @Remote Connector NX.
Import	• Import a list of devices from a text file.
Scheduled Discovery	• Network Search or Broadcast Search parameters use SNMP, Device Administrator or SDK/J Platform authentication to communicate with specified devices, devices present in an IP range or devices within an IP range or subnet. • Also allows you to find local USB-connected devices*
Manual Discovery	• Identify specific devices by IP Address that you want Device Manager to locate for monitoring.

NOTE: * To communicate with USB-connected devices, the @Remote Connector NX USB Agent must be installed on each workstation with USB-connected devices. @Remote Connector NX communicates with the USB Agent via SNMP to retrieve information about the attached devices. You must use an SNMP Access Account with a 'public' Read Community name. See *SNMP Account* on page 29 and to the @Remote Connector NX Installation Guide for USB Agent installation instructions.

3.1 Add Devices Workflow

If you are using previous Ricoh products, a Ricoh Customer Engineer will most likely migrate existing managed device data from the @Remote Center System to populate the Devices list for the first time. In this case, you might already see devices in your Devices list.

However, you now need to create a new discovery task that will locate any new devices that are added to the network (based on preset criteria). Typically, device discovery is used at some point after initial setup is complete to locate new additions to the fleet as they appear on the network.

Follow this workflow to add devices to the system:

Establish account information to allow @Remote Connector NX to communicate with devices	**Page 29**
For all devices, you need to enter the SNMP, Web Service and/or SDK account information that will allow @Remote Connector NX to locate the devices to manage.	

↓

Select <u>one</u> of the following methods:

1 Import device details from an external file	**Page 36**
Import a CSV file containing IP addresses and/or DNS names.	

OR

2 Set the discovery parameters and the run schedule for a network or broadcast search	**Page 38**
Set up a network or broadcast search to discover devices that will be managed, and determine a schedule when the search will run.	

OR

3 Set up a manual device discovery	**Page 48**
Force discovery of one or more devices by IP address.	

3.2 Establish Account Information

@Remote Connector NX attempts to communicate and authenticate with a device using three possible access profile types:

- SNMP
- Device Administrator
- SDK/J Platform

@Remote Connector NX uses a combination of all three profile types depending on the configuration task. In case of a pre-existing fleet, the profiles used may differ from those used by new devices.

For each profile, you must set the authentication information, or account profiles, that @Remote Connector NX can use to communicate with devices. You can configure as many access profiles per profile type as you require, and set priority on each profile. @Remote Connector NX attempts authentication according to the specified priority until authentication is successful.

3.2.1 SNMP Account

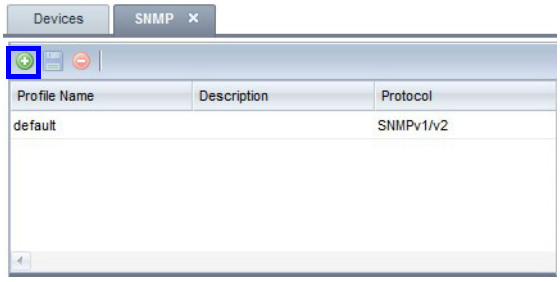
@Remote Connector NX can communicate with SNMP-enabled devices using SNMP v1, v2 and v3 and supports multiple community names for one or more device groups. To set up SNMP, you require the SNMP version, read and write community names (if specified separately), username and password.

NOTE: SNMP read access is required to allow @Remote Connector NX to discover and monitor the device. Communication with USB-connected local devices also uses SNMP v1/v2. Ensure the @Remote Connector NX USB Agent is installed on each local computer (which has a USB-connected device) prior to completing these instructions. See the *@Remote Connector NX Installation Guide* for installation instructions.

1. On the Navigation tree, click **Discovery & Polling,** then locate the **Access Profiles** folder.

2. Click on the **SNMP** option.

3. On the SNMP tab options bar, click **Add** to add a new SNMP Profile.



4. In the Details section at the bottom of the tab, enter the details outlined in the table below. Fields marked with an asterisk are required, and you can save the Profile only if all marked fields are completed. Fields specific to SNMPv3 profiles are not available until SNMPv3 is selected.

Field	Description
Profile Name*	A unique name to identify the profile in the Profile list.
Description	An optional description of the profile to further help identify the contents of this profile.

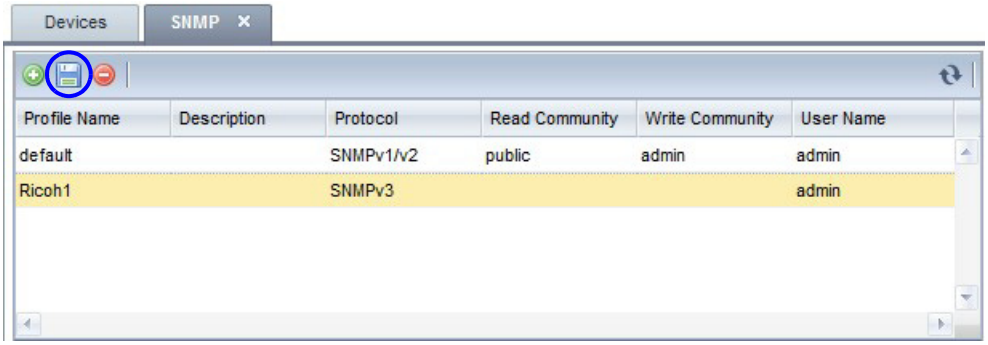
Field	Description
Retry*	The number of times @Remote Connector NX will retry any failed SNMP request, where a failed SNMP request is defined as any SNMP request that does not receive a response within the SNMP Timeout defined below.
Timeout*	The amount of time (in milliseconds) that @Remote Connector NX waits for a device to respond to the SNMP request for information. The default value is 2000 milliseconds.
Protocol	The SNMP protocol type that @Remote Connector NX should use to communicate with devices. **NOTE:** If you choose SNMP v3, an additional set of fields is available for completion. See Step 5 below.
Read Community Name*	Enter the Read Community names that will allow @Remote Connector NX to retrieve information from the SNMP agent. @Remote Connector NX is initially configured using the standard read and write community names of **public** and **admin**, respectively. If you are using different community names, change these default settings. This field is not applicable to SNMP v3.
Write Community Name*	Enter the Write Community name that will allow @Remote Connector NX to insert information into the SNMP agent. This field is not applicable to SNMP v3.

5. If you selected **SNMPv3**, also complete the following fields:

Field	Description
User Name*	Enter the name of the user (principal) on behalf of whom the message is being exchanged.

Field	Description
Password	Enter the password assigned to the user name. To change the password, click **Change**, then enter the new password in each of the fields. The passwords must match to proceed. The password change will not be made until you save the current authentication profile.
Authentication Algorithm	Select either MD5 or SHA1 as the authentication protocol and enter the corresponding password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
Context Name*	The SNMP context name identifying the collection of management information accessible by an SNMP entity. By default, the context name is set to **GWNCS**.
Encrypted Password	Enter the password for the selected encryption algorithm. To change the password, click **Change**, then enter the new password in each of the fields. The passwords must match to proceed. The password change will not be made until you save the current authentication profile.
Encryption Algorithm	Select either DES or AES128 encryption protocol.

6. On the Options bar, click **Save** . The Profile appears in the upper part of the screen.

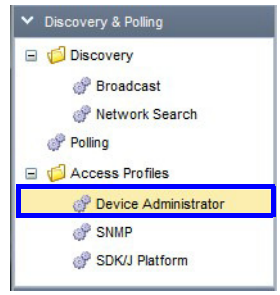


7. Continue adding additional SNMP profiles if required, then proceed to *3.4 Configure Automatic Device Discovery* on page 38.

3.2.2 Device Administrator Account

@Remote Connector NX can manually configure one or more access accounts for devices that require authentication. Once a device is discovered, @Remote Connector NX will attempt to authenticate with each of the specified Device Administrator profiles. When @Remote Connector NX succeeds with authentication, the software will store the access account information for the discovered device. You require the user name and password to configure this method.

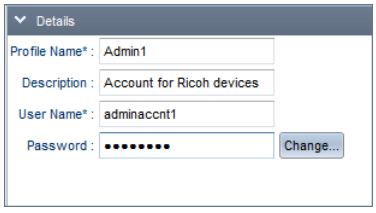
1. On the Navigation tree, click **Discovery & Polling,** then locate the **Access Profiles** folder.



2. Click on the **Device Administrator** option.

3. On the Device Administrator tab, click **Add** from the Options bar to add a new profile.

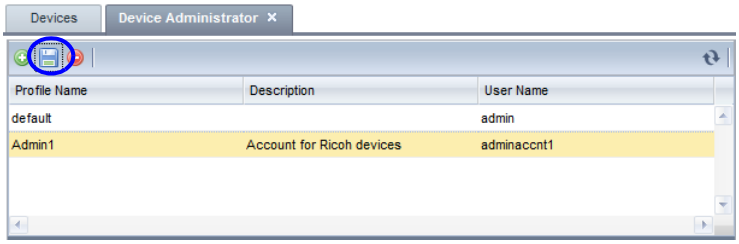
4. In the Detail section at the bottom of the tab, enter the following details. Fields marked with an asterisk are required, and you can save the Profile only if all marked fields are completed.



Field	Description
Profile Name*	A unique name to identify the profile in the Profile list.
Description	An optional description of the profile to further help identify the contents of this profile in the Profile list.
User Name*	Enter the name of the user (principal) on behalf of whom the message is being exchanged.

Field	Description
Password	Enter the password assigned to the user name. To change the password, click Change, then enter the new password in each of the fields. The passwords must match to proceed. The password change will not be made until you save the current authentication profile.

5. Click **Save** . The Profile appears in the upper part of the screen.

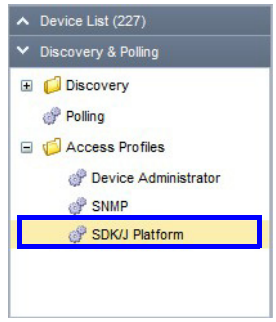


6. Continue adding additional profiles if required, then proceed to *3.4 Configure Automatic Device Discovery* on page 38.

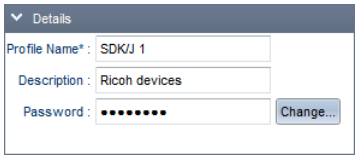
3.2.3 SDK/J Platform

Once @Remote Connector NX discovers a device, it tries the SDK/J platform accounts to identify credentials that can be used to manage the platform. In this case, you need to enter only the SDK password.

1. On the Navigation tree, click **Discovery & Polling,** then locate the **Access Profiles** folder.
2. Click on the **SDK/J Platform** option.
3. On the SDK/J Platform tab, click **Add** from the Options bar to add a new profile.

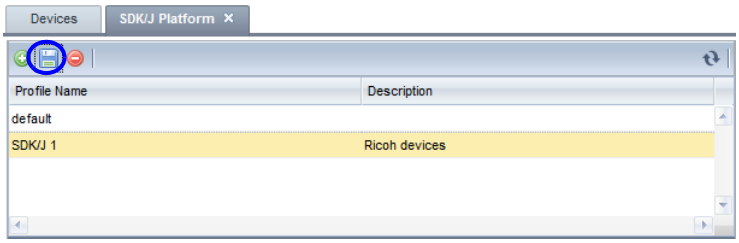


4. In the Detail section at the bottom of the tab, enter the following details. Fields marked with an asterisk are required, and you can save the profile only if all marked fields are completed.



Field	Description
Profile Name*	A unique name to identify the profile in the Profile list.
Description	An optional description of the profile to further help identify the contents of this profile in the Profile list.
Password	Enter the SDK password.

5. Click **Save** . The new profile appears in the upper part of the screen.



6. Continue adding additional SDK/J profiles if required, then proceed to *3.4 Configure Automatic Device Discovery* on page 38.

3.3 Import Device Information

When you perform an import, @Remote Connector NX imports the device information (i.e IP Address at a minimum) and adds the information to the Device list regardless of whether the devices are online and reachable. If the device is not currently reachable, full device information is added to the Device Properties when the device is successfully polled.

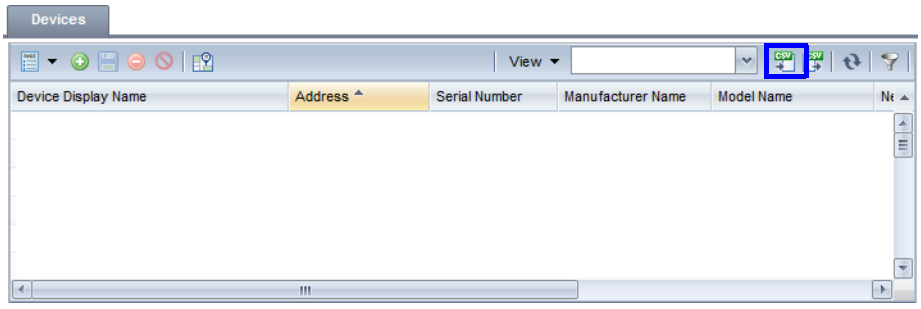
If you are working with a large fleet, you most likely have an external file or database containing a list of all IP addresses and/or DNS names of the devices within your fleet. In this case, you can import the device list from the external file, then set up a discovery task to locate any devices that are added to the fleet in the future.

Format the external file using the following values (in the order specified here). Only the Address field is mandatory. To view a sample, follow step three below.

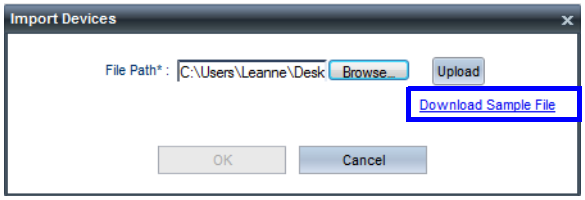
- Display Name
- Address (the IPv4 Address or the Hostname)
- Serial Number
- MAC Address
- Manufacturer
- Device Installation Date

The remaining five fields can be used for custom properties. See *5.4 Set Display Properties* on page 75.

1. On the Navigation tree, click **Devices list** to open the **Devices list** tab.
2. From the Options bar, click the Menu button and select **Import** from the menu.



3. In the Import CSV screen, click **Download Sample File**. Ensure your file is formatted according the sample before proceeding with the import.



4. Click **Browse** to locate your CSV file, then click **Upload**.

5. Click **OK** to proceed.

   The results will appear immediately in the Device List. Any missing properties for the imported devices will be completed once the device(s) are successfully polled.

3.4 Configure Automatic Device Discovery

Automatic device discovery locates devices that match parameters you specify and adds them to the Devices list.

There are two methods to discover devices:

- **Network Search** – sends an SNMP authentication message to a specified IP range. For instructions, see *3.4.1 Configure a Network Search Profile* on page 38.
- **Broadcast** – sends an SNMP authentication message to every client on the network, or to a specified subnet. For instructions, see *3.4.2 Configure a Broadcast Search* on page 43.

NOTE: If you are importing a list of devices from an external program, or are forcing a manual discovery, do not complete these instructions. Instead, refer to *3.3 Import Device Information* on page 36 or *3.5 Manual Device Discovery* on page 48.

You can set the parameters of both search types if needed.

3.4.1 Configure a Network Search Profile

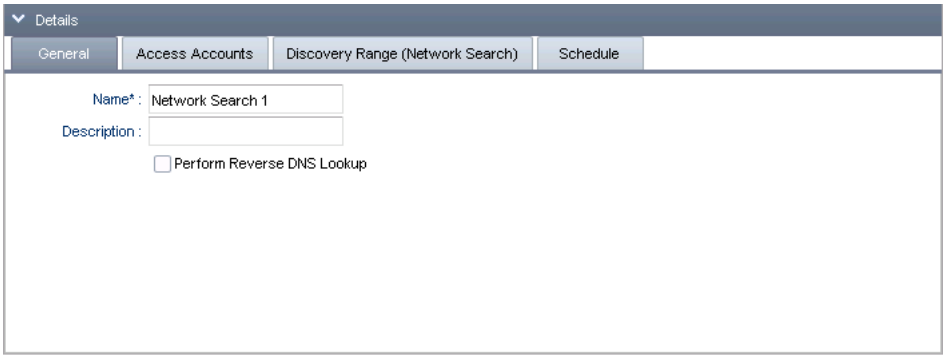
This task steps you through the configuration of a single network search discovery profile. If you prefer to implement broadcast searches, skip this step and see *3.4.2 Configure a Broadcast Search* on page 43. You might also choose to implement both a network and broadcast search that run on different schedules.

1. On the Navigation tree, click **Discovery & Polling,** then locate the **Discovery** folder.
2. Click on the **Network Search** option.
3. On the Discovery Setting (Network Search) tab, click **Add** from the Options bar to add a new network search profile.

   In the Details section at the bottom of the tab, you will see four tabs. Information is required on the General and Discovery Range tabs only.

   TIP: With the exception of the Discovery Range tab, you do not have to click Save between each tab - save the profile only after all options are selected.

4. On the **General** tab, complete the following options:



Field	Description
Name*	A unique name to identify the discovery profile in the Profile list.
Description	An optional description of the discovery profile to further help identify the contents of this profile in the Profile list.
Perform Reverse DNS Lookup	Enable this checkbox to perform a reverse lookup to identify the host name of a device. When an IP Address or host name is specified in the discovery target, the device(s) will be managed using the hostname, rather than IP address.

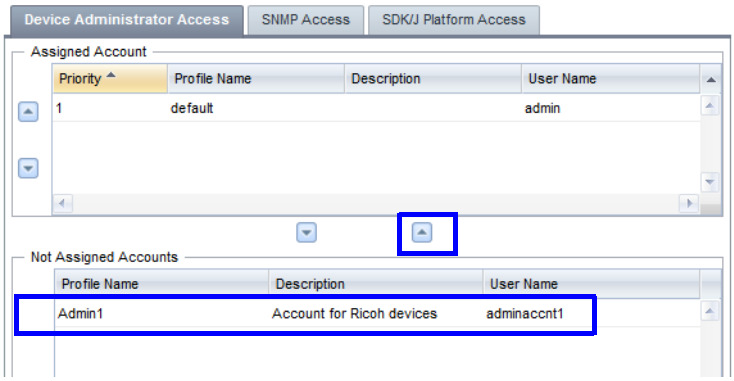
5. Switch to the **Access Accounts** tab.

   From the three subtabs, assign one or more access accounts (that you created in *3.2 Establish Account Information* on page 29) to this discovery network search profile. You should choose the best method to communicate with devices in the discovery range that you will identify in a later step. You must assign at least one or more Device Administrator, SNMP, or SDK/J Platform access profiles to each discovery profile. This example uses a Device Administrator access profile to search for devices within a specified IP range.

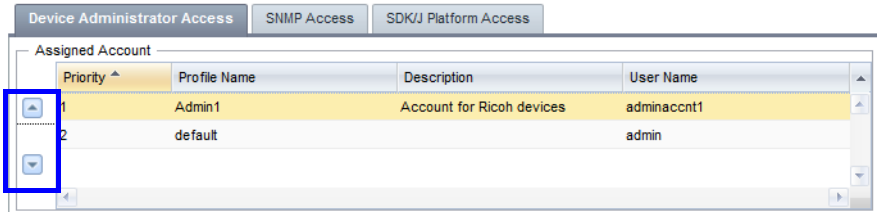
   When @Remote Connector NX runs the discovery, it will apply the access account profile in the priority order assigned on this tab.

   a. From the Not Assigned Accounts section, click on the **account you want to**

assign, then click the **Up arrow** to move it up to the assigned section.



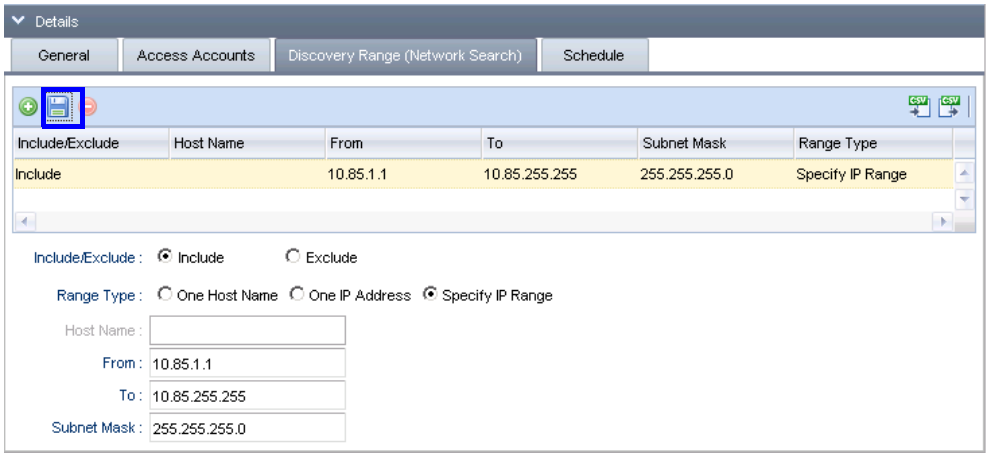
b. If you add more than one profile to the Assigned list, use the **Up/Down** arrow keys beside the Assigned Accounts to change the priority order. @Remote Connector NX will try to authenticate the device using each of the profiles in the order they appear here.



c. To configure full access to the device, switch to the SNMP Access and SDK/J Platform Access tabs to assign additional access profiles to this discovery profile.

6. On the **Discovery Range** tab, click **Add** to set the search parameters. You can limit or expand the search to an IP range, a single device, or within a particular host. The example below will search for all devices within the specified IP range, on the specified subnet mask.

TIP: To specify another IP range, click Add, and set the parameters for the next range. You can add as many search parameters as needed, but remember to click Save to save each new search.

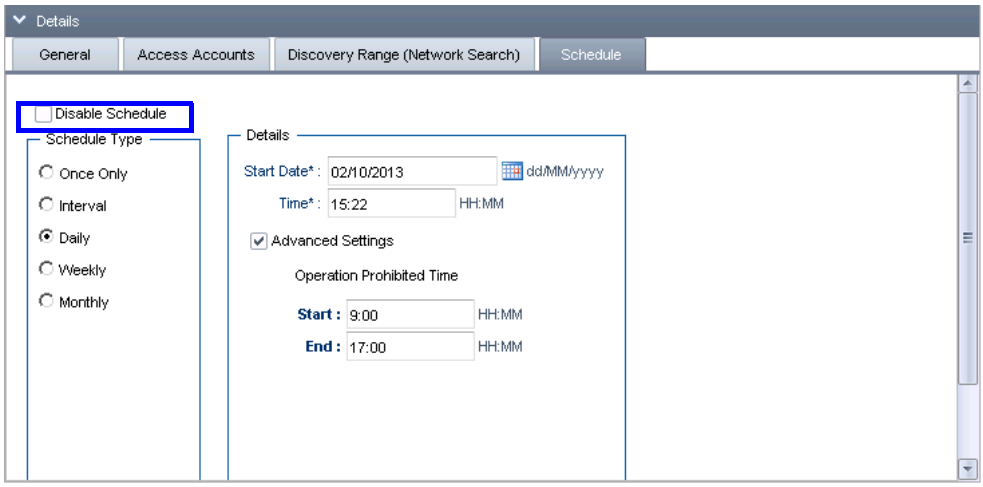


NOTE: You must click **Save** on this tab to save these parameters. If you do not save on this tab, you will see an error message when you try to save the discovery profile indicating that parameters are missing.

NOTE: When grouping, the hostname is only used if **One HostName** is selected and a hostname is entered in the **Host Name** field in the screen above.

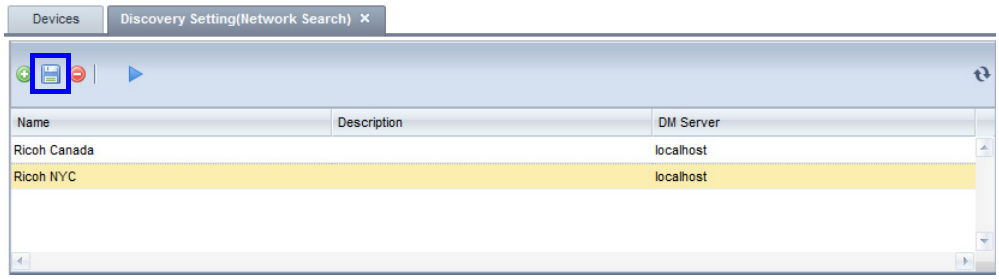
7. On the **Schedule** tab, clear the Disable Schedule checkbox to set the start date, time, and interval for this discovery profile. In this example, the discovery profile will run every day beginning at 17:00 hours.

TIP: If there are times when a search must not run, click Advanced Setting to view additional options that allow you to enter the times to prevent this discovery profile from running.



TIP: When Disable Schedule is checked, this discovery profile will not run as per the set schedule. Use this feature to temporarily disable the discovery profile. Use the Delete button on the Navigation bar to remove the discovery profile completely.

8. To save this discovery profile, click **Save** on the Options bar.



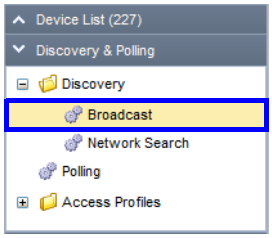
9. To **run this discovery profile immediately**, select the Profile from the list, then click the **Run** button. Otherwise, when the schedule parameters are met, this discovery profile will run and search for specified devices.

3.4.2 Configure a Broadcast Search

This task steps you through the configuration of a single broadcast discovery profile. This search broadcasts to all hosts specified in the search parameters.

Warning: If attempting to reach external network segments other than the segment to which the @Remote Connector NX server belongs, modify your router settings to enable broadcast.

1. On the Navigation tree, click **Discovery & Polling,** then locate the **Discovery** folder.



2. Click on the **Broadcast** option.
3. Click **Add** from the Options bar to add a new broadcast search profile.

   In the Detail section at the bottom of the tab, you will see five tabs. Information must be entered on the General tab, but you can leave the default settings on the remaining tabs if necessary.

4. On the **General** tab, complete the following fields:

Field	Description
Name*	A unique name to identify the discovery profile in the Profile list.
Description	An optional description of the discovery profile to further help identify the contents of this profile in the Profile list.
Perform Reverse DNS Lookup	Enable this checkbox to perform a reverse lookup to identify the host name of a device. If the reverse DNS lookup successfully identifies the host name for the device, the device is managed using the host name rather than the IP Address.

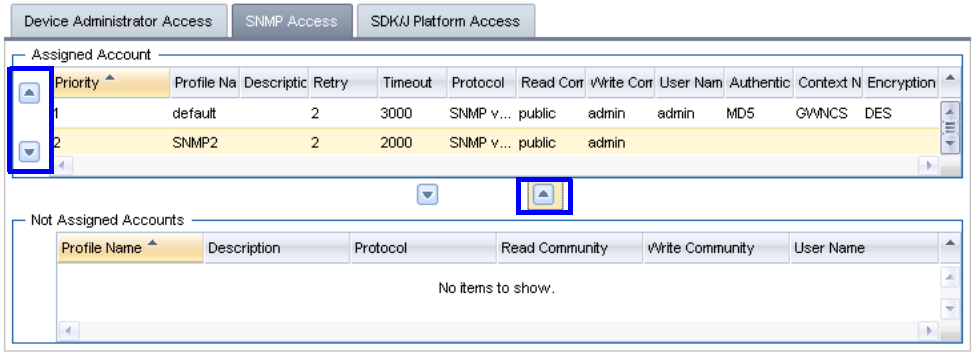
5. On the Access Accounts tab, assign one or more access accounts (that you created in *3.2 Establish Account Information* on page 29) to this broadcast discovery profile. You should choose the best method to communicate with devices in the discovery range that you will identify in a later step. You can assign one or more Device Administrator, SNMP, or SDK/J Platform access

profiles to each discovery profile. This example uses an SNMP access profile to search for devices on a specified local segment.

When @Remote Connector NX runs the discovery, it will apply the access account profiles in the priority order assigned on this tab.

a. From the Not Assigned Account section, click on the **account you want to assign**, then click the **Up arrow** to move it up to the assigned section.

b. If you add more than one profile to the Assigned list, use the **Up/Down** arrow keys beside the profiles to change the priority order.



c. If necessary, assign Device Administrator and SDK/J Platform access profiles to this discovery profile also.

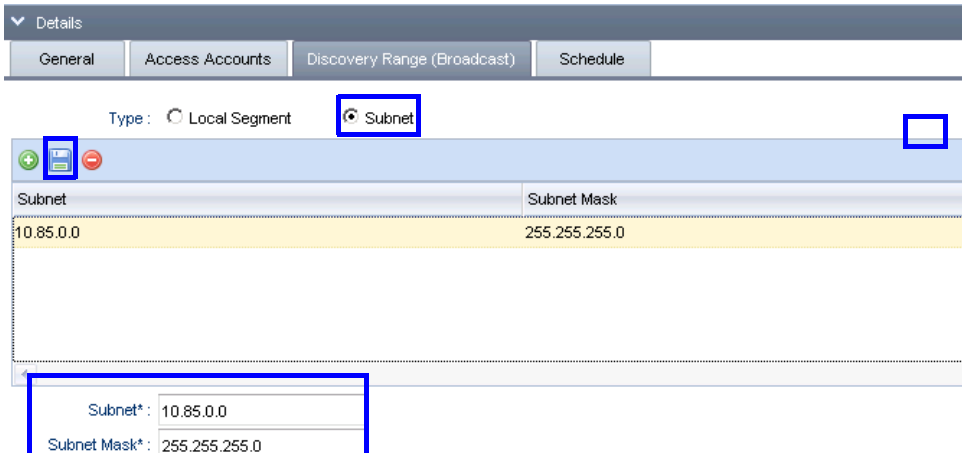
6. On the **Discovery Range** tab, set the search to either the local segment or a particular subnet.

a. If you select Local Segment, you can proceed to setting the schedule in Step 5 below. The search will be conducted on the same local segment as the selected DM Server and no further settings are required on this tab.

b. If you select Subnet, click **Add**, then type the Subnet and Subnet mask values.

Click **Save**. You can add additional subnets if necessary.

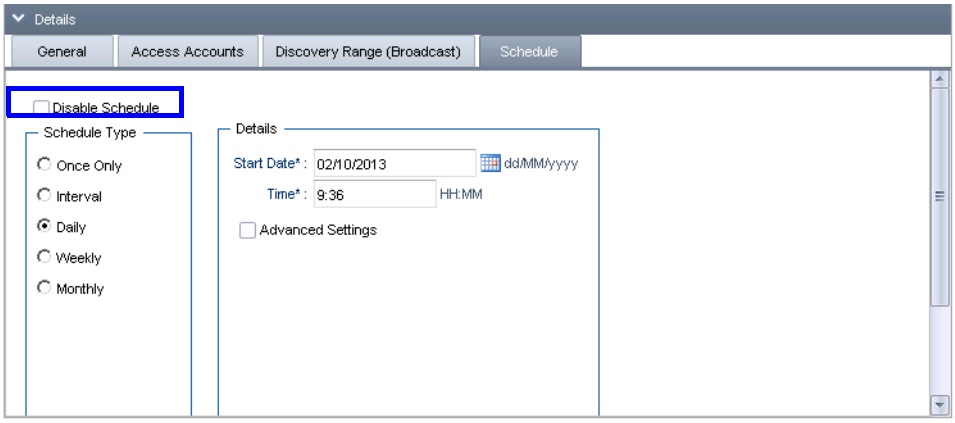
NOTE: You can also import a list of subnets from an external CSV file.



Warning: You must click Save on this tab to save these parameters. If you do not save on this tab, you will see an error message when you try to save the discovery profile indicating that parameters are missing.

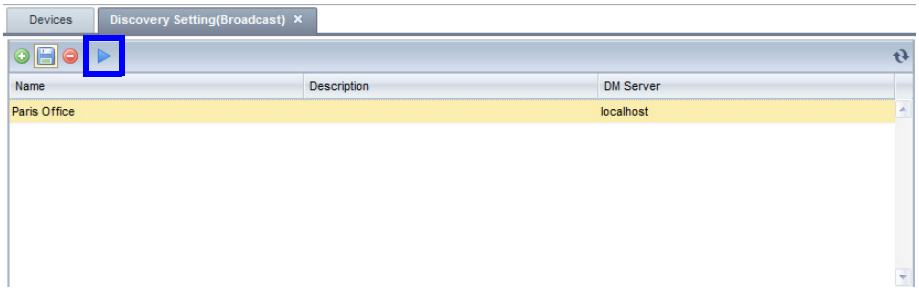
7. On the **Schedule** tab, clear the Disable Schedule checkbox to set the start date, time, and interval for this discovery profile. In this example, the discovery profile will run every day beginning at 09:36 hours.

TIP: If there are times when a search must not run, click Advanced Settings to view additional options that allow you to enter the times to prevent this discovery profile from running within the set time period.



TIP: When Disable Schedule is checked, this discovery profile will not run as per the set schedule. Use this feature to temporarily disable the discovery profile. Use the Delete button on the Navigation bar to remove the discovery profile completely.

8. To save this broadcast discovery profile, click **Save** on the Options bar.

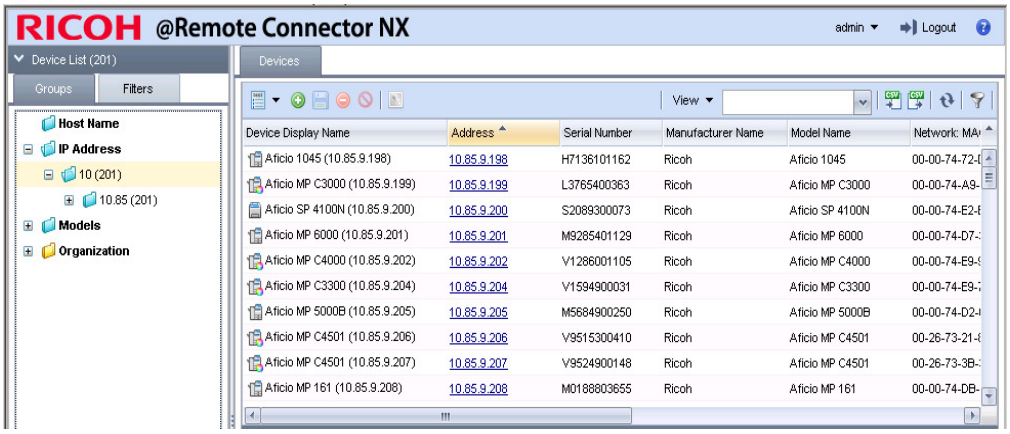


9. To **run this discovery profile immediately**, select the profile from the list, then click the **Run** button. Otherwise, when the schedule parameters are met, this discovery profile will run and search for specified devices.

3.4.3 View the Discovery Results

@Remote Connector NX adds devices to the Devices list automatically as they are discovered. To view the results, click Device List on the Navigation Tree, then view the devices by hostname, model or IP address.

In this example, a network discovery profile discovered devices within a specified IP range using an SNMP access account.



Next Steps:

- You can continue to set up additional discovery profiles as needed.
- You can force a manual device discovery if you have just a few devices to add for monitoring. See *3.5 Manual Device Discovery* on page 48.
- You can organize the Device List into custom categories and groups for easier navigation. See *4.1 Organize the Device List* on page 54.
- You can filter and view device details. See *4.2 Changing the Device List View* on page 64.

3.5 Manual Device Discovery

After initial population of the Device List, you may need to add just a few devices for monitoring when new devices are added to the fleet. Rather than waiting for automatic discovery (as per the schedules you created for broadcast or network search discovery profiles), you can run an immediate discovery based on the device IP Address or DNS name. After you specify one or more devices, a discovery task runs in the background immediately to locate the device data. Once the devices are discovered by @Remote Connector NX, the details are added to the entries in the Device List.

1. Click on the **Devices** tab.

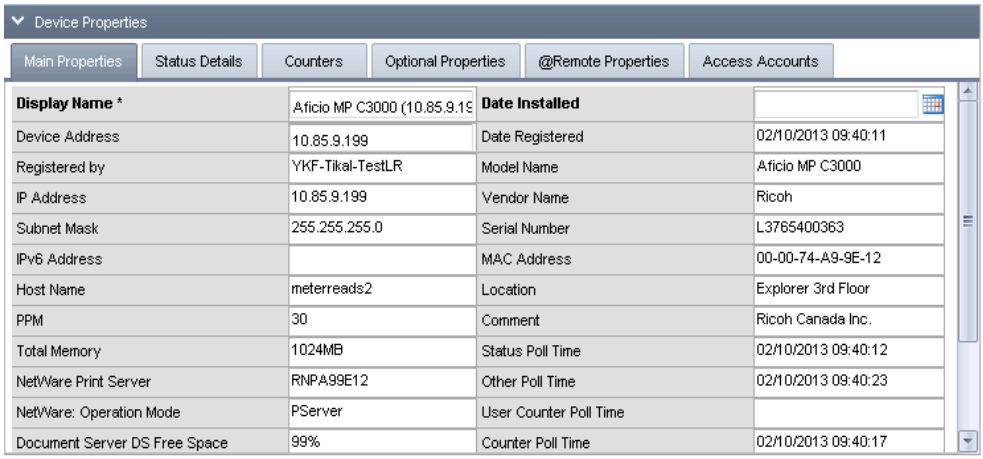
2. Click **Add** from the Options bar to add a new device.

3. In the Add Device window, enter the following:
   - **IP Address** of one or more devices
   - **Access Profiles – SNMP** or **Device Administrator** and **SDK/J** access profiles defined in *3.2.1 SNMP Account* on page 29, *3.2.2 Device Administrator Account* on page 33, or *3.2.3 SDK/J Platform* on page 34. Specify all profile types to ensure full device access.

4. Click **OK** to start the manual discovery.

5. In the Device Properties section at the bottom of the Device tab, the details for the device are shown. Any missing device properties will be retrieved from the

device after it is successfully polled. Each of the tabs are described in the table below.



Tab	Required Fields
Main Properties	Many of the fields on the Properties tab are filled automatically after @Remote Connector NX communicates with the device. There are two editable fields: • **Display Name**: Enter a unique name that will appear in the Display Name column of the Devices list. • **Date Installed:** Optionally, click on the calendar to set the Installation Date of the device.
Status Details	The Status Detail tab reports on the overall status of the device output functions. You can also switch to the Paper Tray, Toner/Ink or Output Tray subtabs for further details.
Counters	Full counter details including copy, printer, and fax output in both color (if applicable) and monochrome.
Optional Properties	Any Custom Properties, Installed Applications, Firmware and Platform information, and other Functions that are installed on the device. These properties are not editable.
@Remote Properties	Service Depot, connection type, and supply order information. See *Chapter 7: Configure @Remote Settings* on page 91 for details.

Tab	Required Fields
Access Accounts	This tab reports the details of the SNMP, Device Administrator, or SDK/J access accounts used to authenticate this device. This tab allows you to view the profiles only – you cannot change the values of the accounts on this tab. See *3.2 Establish Account Information* on page 29 for details.

6. If you made changes to an editable field, click **Save** on the Options bar.

3.6 View Device Properties

When you click on a device in the Device List branch, @Remote Connector NX retrieves the device properties from the database and reports this information under the Device Properties section of the Devices tab.

TIP: To see the latest information for a device, right click on the device in the Device List, and select Request Polling from the menu. You can select all polling types (Status, Supplies, Counter, Other, and User Counter), or check only specific Poll types as needed.

This table provides general descriptions of the tabs under the Device Properties section. For full reference information about these properties, refer to the @Remote Connector NX online help.

Tab	Description
Main Properties	The unique identifiers of the device, including the Display Name and IP Address. Other details include the device registration and installation date, model name, host name, serial number, MAC address, etc.
Status Details	Overall status of the device's output functions, with subtabs for paper tray, toner/ink and output tray status.
Counters	Full counter details including copy, printer, and fax output in both color (if applicable) and monochrome. **NOTE:** The Total counter provides the sum of all toner usage on this devices, and is a cumulative total of monochrome and color toner usage (if applicable).
Optional Properties	You can define up to ten custom device properties that will appear on this tab. See *Set Display Properties* on page 75 for instructions.
@Remote Properties	Reports the Connection Type, Service Depot information, and Supply order information as entered in the @Remote Settings by a Customer Engineer. See *Chapter 7: Configure @Remote Settings* on page 91 for details.

Tab	Description
Access Accounts	Details of the SNMP, Device Administrator, or SDK/J access accounts used to authenticate with this device. This tab allows you to view the profiles only – you cannot change the values of the accounts on this tab. See *3.2 Establish Account Information* on page 29 for steps to edit the account information.

CHAPTER 4

Organize the Device List

After your Device List is populated, you should consider a structure for the Device List that reflects the organization of your company.

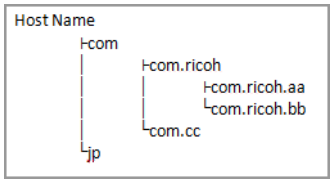
In this chapter, you will create custom categories and groups to organize the devices into a logical structure. At the same time, you can create filters that automatically add any new devices to specific groups based on defined criteria.

This chapter also includes information about sorting the devices in the Device List and using the Quickfilters to locate specific devices quickly.

4.1 Organize the Device List

When you first launch @Remote Connector NX, the Device List is expanded and the Device tab is the active feature by default. There are three system categories (indicated with a blue folder icon) to provide initial organization of the devices in the Device List:

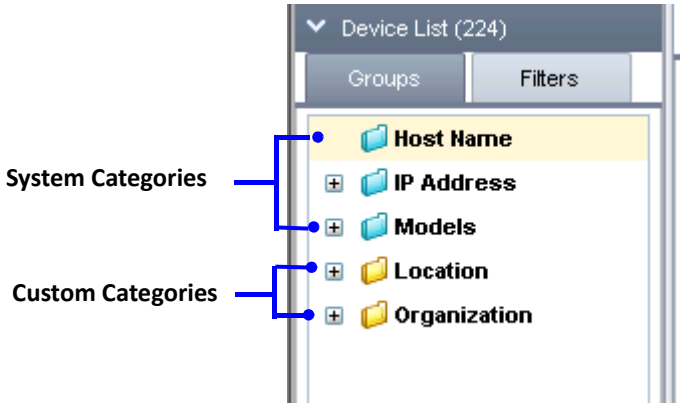
- **Host Name** – Devices are grouped based on domain hierarchies. When @Remote Connector NX identifies at least one dot within a domain hierarchy, it displays the host names in ascending order. If a domain hierarchy is not identified, the device are listed alphabetically by device display name until sorted otherwise.

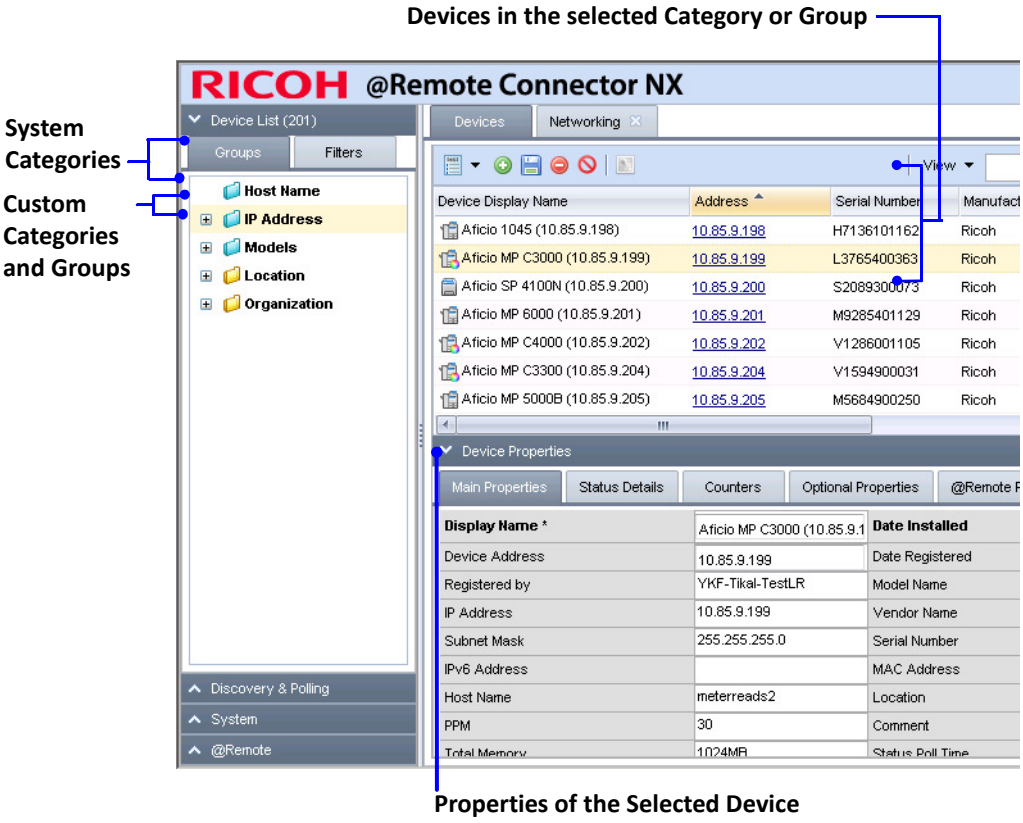


- **IP Address** – Devices are grouped by subnets (octects) with groups for each host. This applies to IPv4 devices only. IPv6 devices are not shown in the Navigation tree.
- **Models** – Devices are grouped by manufacturer, and groups further organize the devices by model name.

Each device appears in every system category. When you click on a category, the devices in that category are displayed in the Devices tab. However, if your fleet is large, you will find it very difficult to locate devices with only this minimal organization. Custom categories allow you to further group devices into categories and groups that make sense for your organization.

After you create the custom categories and groups, you can drag and drop devices from the system categories to the custom categories and groups as needed.



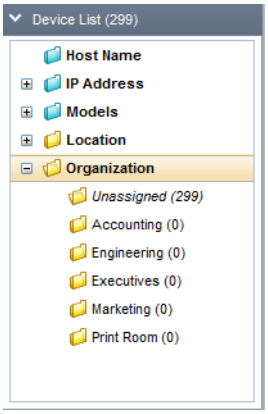


To implement a cohesive organizational scheme, @Remote Connector NX supports the creation of an unlimited number of custom categories and groups to suit your organizational needs. For example, you might prefer to group your devices by location or by organization (subsidiaries, divisions, departments, etc.).

To develop your own organization strategy, consider the following:

- A category is a method of classifying the devices within your organization. For example, you might categorize based on location (country, city, building, floor, etc.), by department (Accounting, Engineering, Marketing, etc.), or by cost centre, etc.

- You can use the structure to associate security roles with custom groups. For example, if you organize the structure based on Location, then create groups for various continents, and create further subgroups for countries and cities, your structure might look similar to Example B on the right.



Example A

Example B

In Example A, the structure is based on the organization of the business into groups such as accounting, engineering, etc.

The possibilities for organization are boundless, and it is up to you to use the information and instructions in this section as a guideline for establishing your own organization scheme.

The examples in this section create categories based on geographical location and require several subgroups per location.

4.1.1 Create Custom Categories

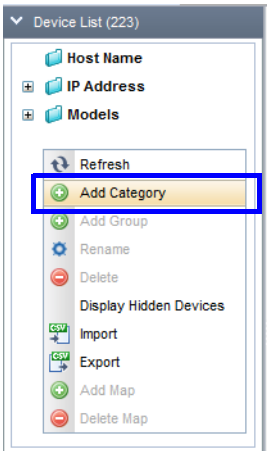
The examples in this section categorize devices by location, based on region, country and city. The fictitious company has devices installed across four continents, and has multiple sites on each continent. To categorize by location, the examples create a Location category, then groups and subgroups for Region, Country and City.

A **category** is always located at the top structure of the Navigation Tree.

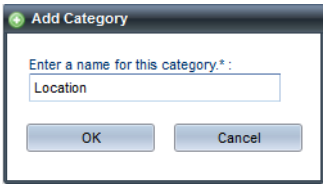
A **group** branches off a category. You can create unlimited groups to branch off from a single category. A device can appear in only one group within a category.

1. On the Navigation tree, click **Device List** to open the **Devices** tab and make it the active feature.

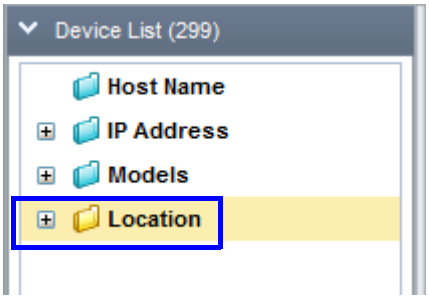
2. Right-click in a blank area of the Device List, and select **Add Category** from the menu.



3. Type a name for the category, then click **OK** to create the category.



The new custom category appears in the Device List beneath the system categories.



NOTE: A new category is always placed as a branch at the top of the Navigation Tree. You cannot nest categories, but you can nest groups.

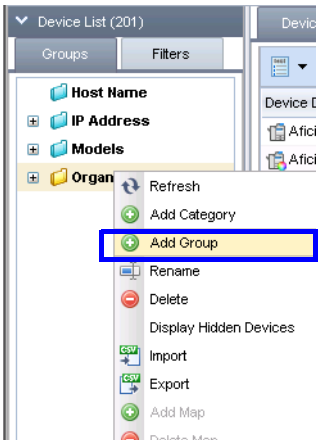
4. Repeat steps 2 and 3 to create additional categories if needed.

TIP: If there are already devices in your Device List, you can click on the + symbol beside the folder to expand the new categories. You should see a folder labeled *Unassigned ( ).* The number within the brackets refers to the number of devices that are not yet assigned to any custom category. If you have not yet performed discovery or device import, the categories are empty and you cannot expand them.

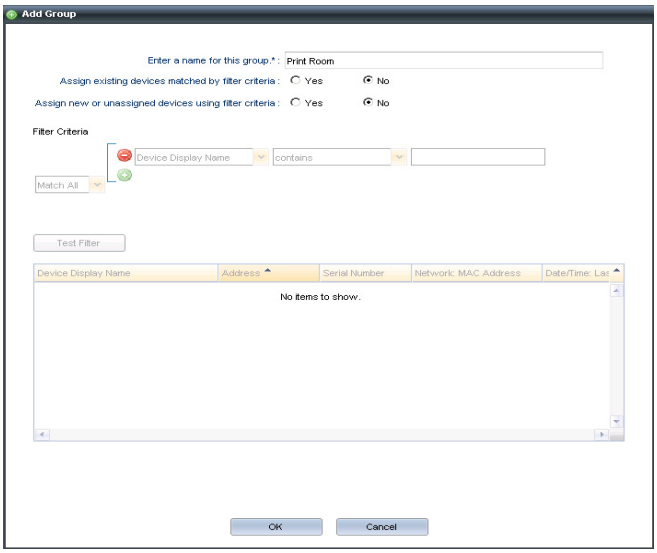
4.1.2 Create Custom Groups

Custom groups are nested within custom categories, and you can create an unlimited number of groups as needed. You can also nest groups within groups. When you add a custom group, you can create filter criteria that will automatically locate matching devices and add them to the specified group. Follow the instructions below to create a new group and set up filters.

1. To create a group that branches from a category, right-click on a category and select **Add Group** from the menu.



2. In the Add Group window, type a **name** for the group. This name must be unique within the selected category.



If you will use automatic filters to add devices to this group when performing a discovery or an import, set the following options. In this example, we are creating subgroups for the cities within each region, and therefore want to apply these filters only at the city level. See *Nesting Groups* on page 61 for a filter example.

Option	Settings
Assign existing devices matched by filter criteria	If there are already devices in the Device list from a previous discovery, import, or manual addition, the filter criteria will assess each device to determine if it matches the filter criteria you set here. If a match is found, the device is added to this group in the Navigation Tree.
Assign new or unassigned devices using filter criteria	When you perform a new discovery, import devices, or manually add individual devices to the Device List, this filter will assess each new device to determine if it matches the filter criteria you set here. If a match is found, the device is added to this group in the Navigation Tree.

Option	Settings
Filter Criteria	These fields are available only if you selected one of the filter criteria fields above. To set more than one filter, click the + button and select the additional criteria, type, and term. • **Match Term:** Match All, Match Any, Match None • **Match Parameter:** Select from over 40 device characteristics • **Match Condition:** Contains, does not contain, greater than, less than, equals, starts with, ends with. • **Match Criteria:** Type the information in the field.
Test Filter	Click this button to test the results of the filters you have created.

3. Click **OK** to add the custom group to the Navigation Tree.

The new group appears in the Device List nested beneath the selected category. Each group indicates the number of devices that belong to it in parentheses.

You will now see two groups in the category: the group you just added, plus a group called Unassigned. The unassigned folder is added to a category to indicate the number of devices that do not yet belong to a group. To resolve unassigned devices, you can create additional nested groups and set filters to assign the devices to the group, or you can simply drag and drop them to particular groups.

If your Device List is empty, you will see a (0) beside the groups until you perform a discovery, import, or a manual add. In this example, there were already devices in the Device List from a past discovery, so the Unassigned folder contains some devices.

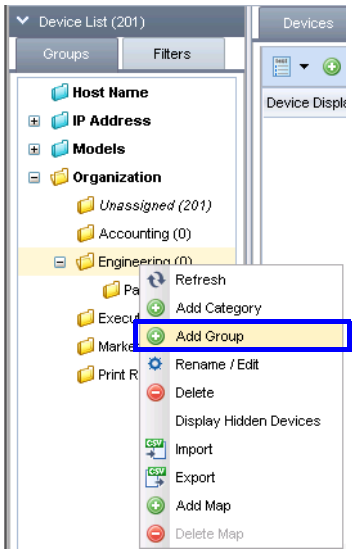
4. Repeat steps 1 through 3 to **continue adding additional groups** at this level to create your base structure.

In this example, we created additional groups for each function within the company organizational structure. To continue the structure, we might also add groups at this level in the Navigation Tree for the Sales team, IT group, etc.

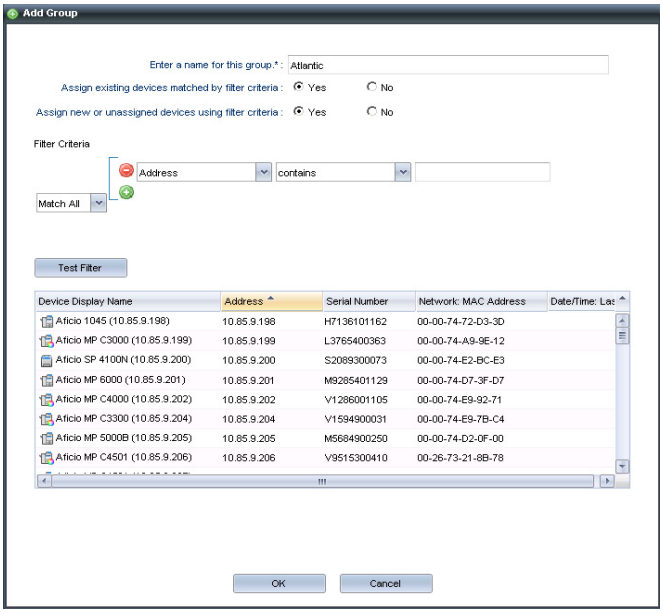
Nesting Groups

There is no limit to the number of levels you can nest custom groups. You should however, develop your filter strategy based on your structure. For example, if you organization has multiple offices, you could create a nested structure within each function based on city.

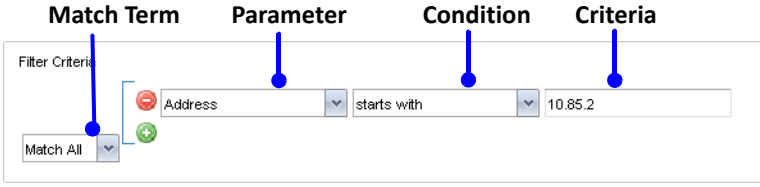
1. To create a nested group, right-click on any custom group and select **Add Group** from the menu.



2. In the Add Group window, type a **name** for the group. In this example, we are creating a group for the team in the Atlantic region

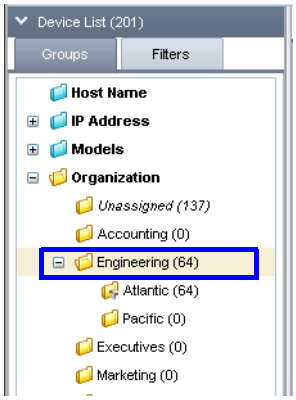


The filter criteria is set to add any existing or new device that starts with an Address of 10.85.2 to this group.



3. Click **OK** to save the group and apply the filter to any devices already in the Device List.

In this example, 64 devices were added to the Atlantic group because they matched the filter criteria.



4. Continue creating nested groups and applying filters until you are satisfied with your Navigation Tree structure.

5. If you did not set filters, you can simply drag and drop devices into this group as needed.

4.2 Changing the Device List View

Once the import, discovery, or manual device addition is complete, you can view and filter the Device List.

- Sort based on a particular column. See *4.2.1 Sort the Devices List* on page 64.
- Use the Quickfilters to resort the order of devices based on one or more columns. See *4.2.2 Use the Quickfilters* on page 65.

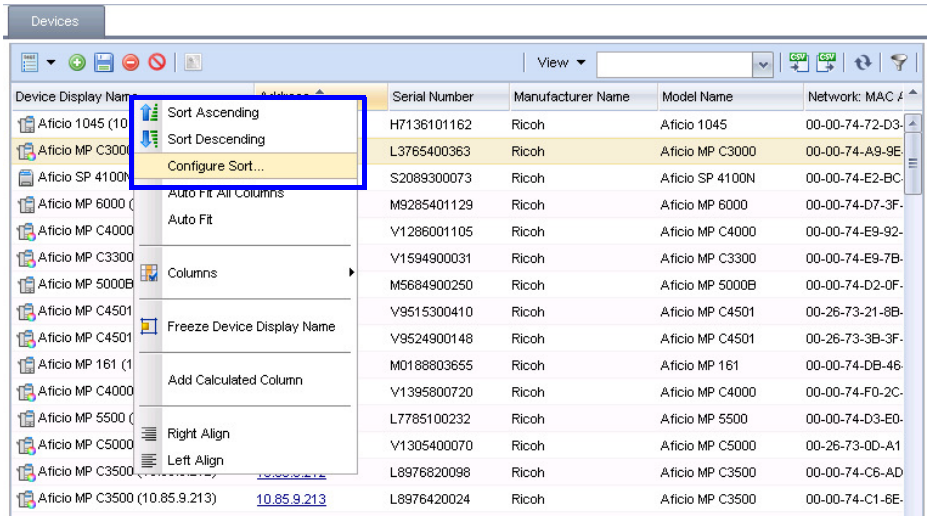
4.2.1 Sort the Devices List

You can sort the list based on a single column by Ascending or Descending alpha or numeric value.

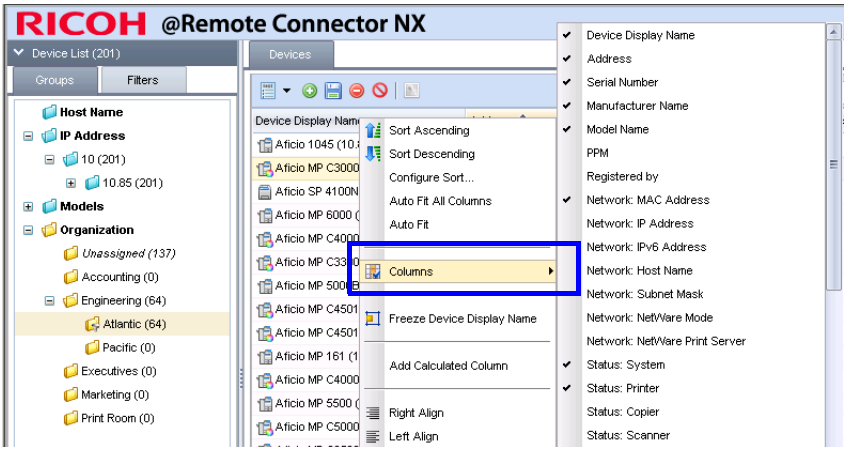
1. On the Navigation Tree, click the Device List branch.

2. On the Devices tab, select the **category** or **group** you wish to view.

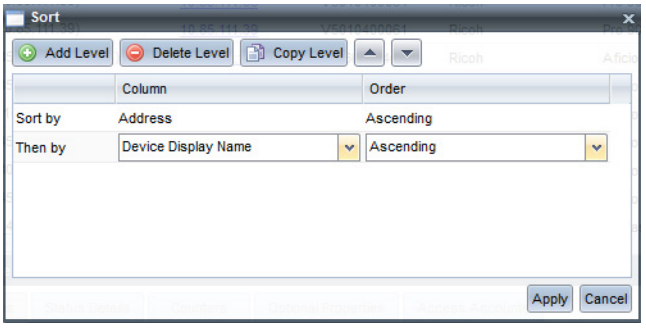
3. Click on the column name you want to sort, and select **Sort Ascending** or **Sort Descending** or **Configure Sort** from the menu.



TIP: To change the columns displayed on the Devices list for this category or group, select **Columns** from the right-click menu. Columns that appear in the display are checked. Check or uncheck any columns as you prefer.



4. If you selected Configure Sort, you can create sort levels, rather than just sorting on a single column. For example, you might want to sort based on IP address, then by device display name. You can add more levels as needed to sort this view of the Device List. Click OK to sort the Device List according to the criteria you set.

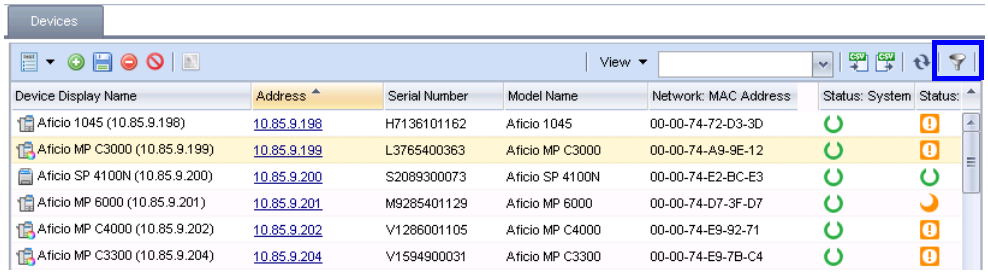


4.2.2 Use the Quickfilters

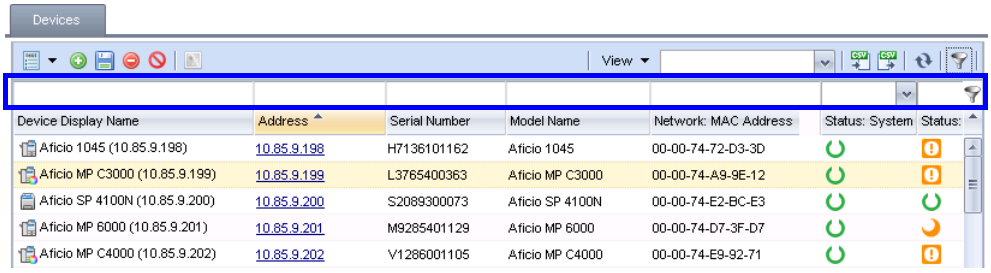
The Quickfilter option allows you to filter the list of devices based on the values you enter for one or more columns. This filter changes the devices in the Devices list based on the criteria you select. This feature can be used as a search tool when looking for specific devices.

1. From the Device List, select the **category** or **group** you wish to view in the Devices tab.

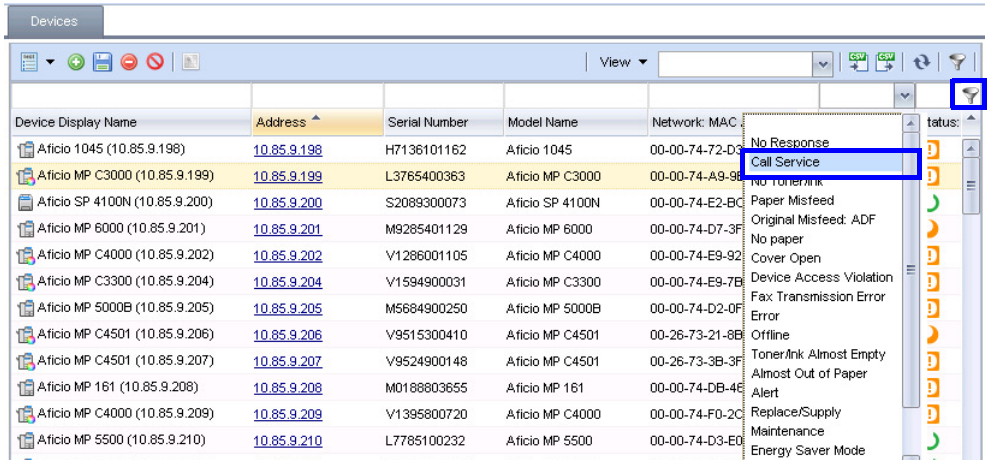
2. Click the **Filters** button on the Options bar.



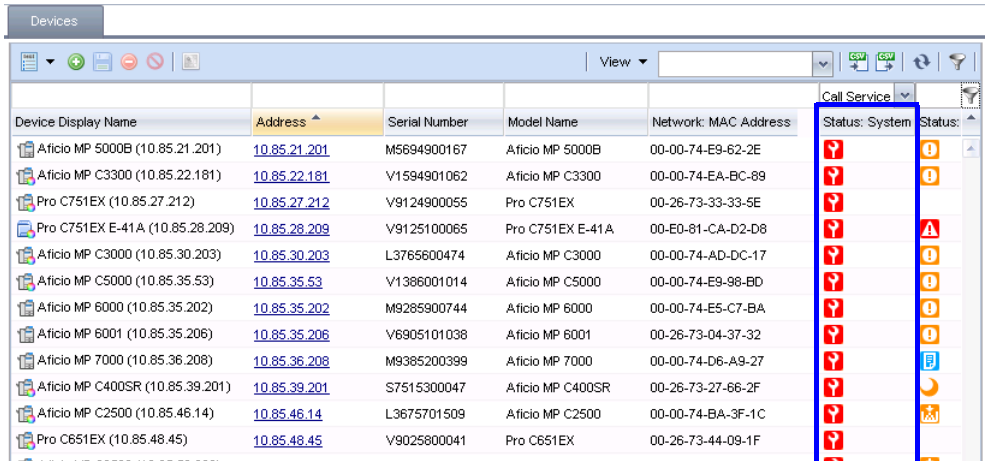
The Filter fields appear above the columns in the Devices list.



3. Type the filter criteria in the text entry fields (such as Display Name, Device Address, etc.), or click the drop-down list in any of the fields with pre-set criteria (such as System or Printer Status). Click the Filter button to force @Remote Connector NX to filter the current list of devices. In this example, we want to place devices that are waiting on a service call at the top of the Devices list.

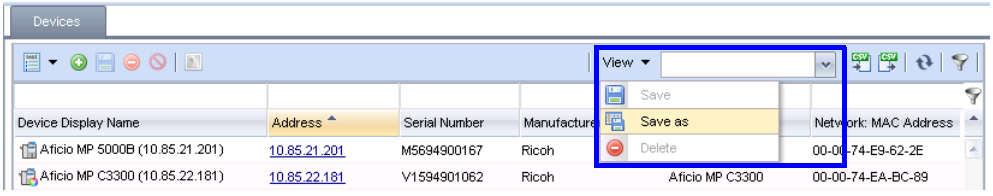


After the filter is applied, only devices awaiting a service call are shown in the list, as shown in the example below.

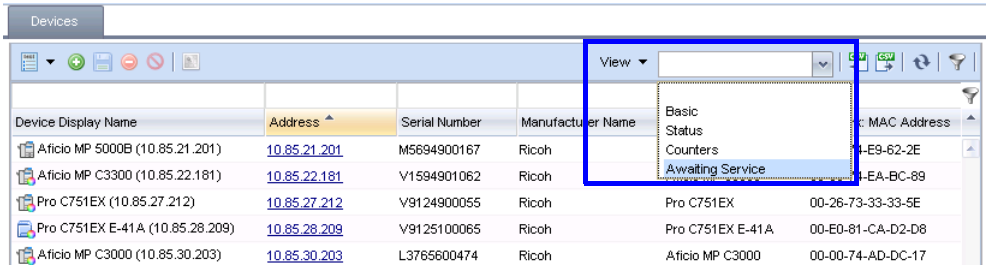


You can further filter the list by entering criteria in additional columns. For example, we could enter "C3500" to view only Aficio MP C3500 devices that are waiting for a service call.

4. To save this view as a Quickfilter for later use, drop the View list, and select Save As from the menu. Type a unique name for this View, then click **OK**. Saving a Quickfilter also saves the selected columns and the column widths to display.



When you view any device list, you can select this Quickfilter to filter the list of devices based on these pre-set selections.



CHAPTER 5

Change Server Settings

This section provides instructions to adjust server settings. These changes are optional; however, you should review these tasks to ensure you complete all necessary configuration changes for your deployment.

NOTE: For information about Activation/Deactivation/Usage Report, refer to *Chapter 1: Introduction* (see page 14).

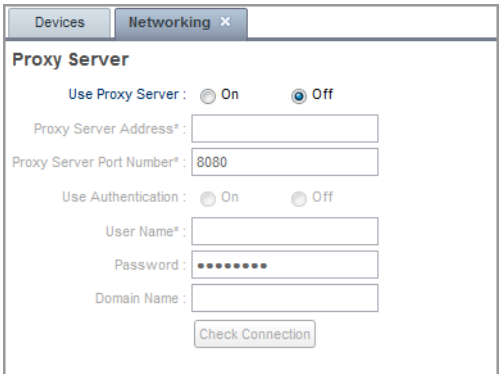
This chapter contains instructions to update the following server settings:

5.1 Network Settings

5.1.1 Enable the Proxy Server

By default, @Remote Connector NX does not enable a proxy server. However, if your deployment requires a proxy server, follow these instructions:

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder.
2. Click **Networking**.
3. Set the **Use Proxy Server** option to **On**.
4. Enter the **Proxy Server Address** and **Server Port Number** of the Proxy Server.
5. If the proxy server requires authentication, set the **Use Authentication** option to **On**, then enter the **User Name, Domain Name** and **Password**.
6. Optionally, click **Check Connection** to ensure these settings allow you to connect to the proxy server.



7. Click **Save** at the bottom of the Networking tab to finalize the changes.

5.1.2 Enable Secure Socket Layer (SSL)

You can enable SSL for communication between a web browser and @Remote Connector NX. SSL communication requires that the server provide the client with a set of credentials that are verified from a trusted source. @Remote Connector NX does not support self-signed certificates. Instead, acceptable certificates are those issued directly by a trusted certificate authority (CA) such as Verisign, Thawte, Entrust, etc or a combination of a CA-issued SSL certificate plus

an Intermediate CA certificate that is in turn validated/trusted by a certificate authority.

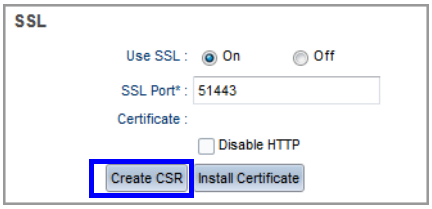
Complete the following instructions to generate the text that you can use to copy and paste into the Certificate Authority's SSL certificate request form.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder.

2. Click **Networking**.

3. Set the **Use SLL** option to **On**, then set the SSL Port number.

4. Click **Disable HTTP** to prevent access via HTTP only.



5. If you do not already have the SSL certificate, click **Create CSR** to enter the following information required for creating a certificate signing request (CSR): Server name, organization, State/Province, Organizational Unit, City or Locality, Country Code (two-character alphabetic field).

6. **Copy and paste** the information presented into the certificate authority's submission form.

When you have the completed certificate, copy the certificate to the @Remote Connector NX server. Note that these instructions will require a server restart.

1. Click **Install Certificate**.

2. Select the Certification type, then click **Browse** to find the certificate on the server or network.

3. Click **Upload** to complete the process.

4. Click **Save** at the bottom of the Networking tab to finalize the changes.

A dialog will inform you of a pending server restart. You will be logged out of the @Remote Connector NX management interface automatically, and after approximately 30 seconds, the browser will direct you to the new URL using SSL.

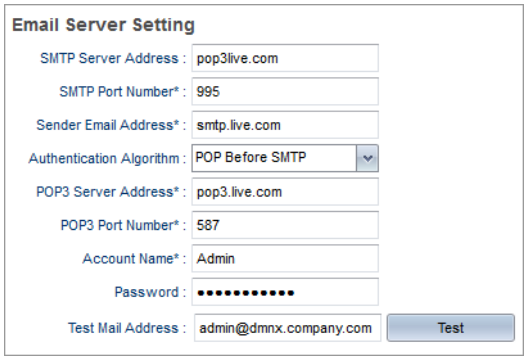
5.2 Email Server and Address Settings

5.2.1 Email Server Settings

To send system alert messages, you need to identify the SMTP Server information.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder and click **Networking**.

2. On the Networking tab, scroll down to the **Email Server Settings** and complete the fields. To send a test message, select your own email address, and click Test to review the message.



3. Click **Save**.

5.2.2 Email Addresses

Email Addresses are used in the @Remote Permission Settings if an @Remote Connector NX Administrator enabled the Confirm before running feature for an @Remote task. This feature will send an email message to a specified user indicating that they must login to the @Remote Connector NX web management interface to approve a task. See *7.3 Configure Permission Settings* on page 94 for more information.

The email addresses that appear in the @Remote Permission Settings tab are configured in **Server Settings →Email Addresses**. You can either enter individual email addresses, or you can use the import feature to import an existing list of email addresses from a specified (and correctly formatted).csv file.

To Add Individual Users

1. On the Navigation tree, click **System**, then locate the **Server Settings** folder and click **Email Addresses**.

2. To add a user, click **Add** from the Options Bar.

3. Under the Details area of the tab, enter a unique name for the user in the **Name** field, then enter an optional description.

4. Enter the email address in the **Address List** field, then click **Save** on the Options Bar to save the user.

5. **Repeat steps 2 through 4** to add more users.

To Import a List of Users

1. From the Options bar, click **Import CSV.**

2. In the Import CSV screen, click **Download Sample File**. Ensure your file is formatted according the sample before proceeding with the import.

3. Click **Browse** to locate your CSV file, then click **Upload**.

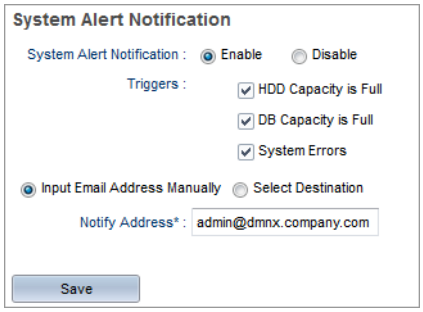
4. Click **OK** to proceed. The results will appear immediately in the Email Addresses list.

5.3 System Alert Notifications

This alert type sends an email alert to one or more email addresses when a system event occurs. Ensure you configure the settings in *Email Server and Address Settings* on page 72 before you set system alerts.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder and click **Networking**.

2. Under **System Alert Settings**, click **Enable** to enable the alerts. Set the following options:



Method	Description
Triggers	Select which events will cause the notification to be sent. Options includes HDD Capacity is Full, DB Capacity is Full, and System Errors.
Input Email Address Manually	Input the email address that the system alert will be sent to.
Select Destination	These destinations are defined in the Email Addresses tab. See *Email Addresses* on page 72 for instructions.

3. Scroll to the bottom of the screen, and click **Save**.

5.4 Set Display Properties

You can configure the following Display Properties. Instructions for each setting is provided on the following pages.

- Country Setting
- Date Display Format
- Custom Properties Fields
- Screen Lock and Timer
- Device Display Name Format

5.4.1 Change the Country Setting

When @Remote Connector NX was installed, the installer referenced the Windows regional settings to determine the country settings. However, you may need to change this setting because it determines the default value used during activation and when downloading external applications.

1. On the Navigation tree, click **System,** then locate the **Display** folder.
2. Select the correct **Country** from the list at the top of the screen, then click **Save** to save the change.

5.4.2 Define Custom Properties

@Remote Connector NX allows you to define up to five custom devices properties. When viewing device status detail, there may be additional properties that you want to see. For example, it may be beneficial to view an administration number or an asset number of the device that will be useful when deploying service personnel.

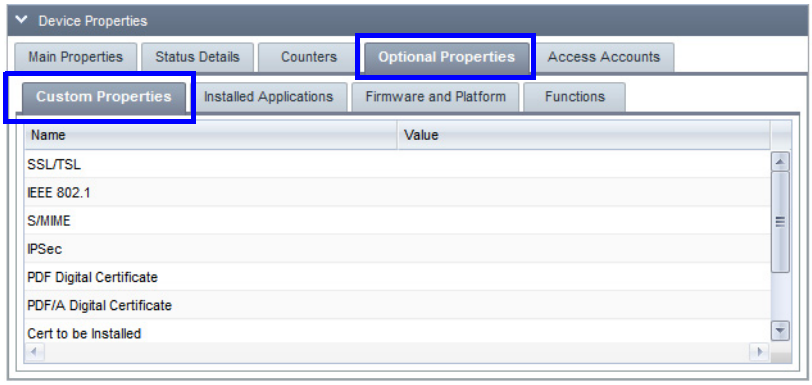
When viewing a device in the Device List, click on the Optional Properties tab to view the custom properties you define here.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder and click **Display**.

2. Enter the name of up to ten custom properties in the fields.

3. Click **Save** to save the changes.

To view the results: On the Navigation tree, switch to the Device List, then click on a device. Under Device Properties, click on Optional Properties, then click on Custom Properties. If the value was populated for the selected device, the Value column will be completed for the custom field.



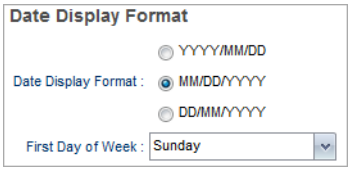
5.4.3 Change the Date Format

The default date region is set as follows:

- YYYY/MM/DD (Default for Japan and China)
- MM/DD/YYYY (Default for U.S and Canada.)
- DD/MM/YYYY (Default for all other countries)

Follow the instructions below to change the date format used throughout the @Remote Connector NX interface.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder.
2. Click **Display**.
3. Select the date format for your region.



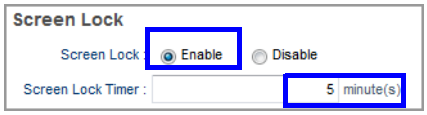
4. Set the first day of the week for your region. This setting is important when generating reports.
5. Click **Save**.

5.4.4 Enable Screen Lock

The screen lock feature logs the user out of the @Remote Connector NX management interface automatically after a set period of inactivity. This feature is a security measure to ensure that the system is not sitting open, yet unattended for a length of time.

Screen lock is enabled by default, and the timer is set to 5 minutes.

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder.
2. Click **Display**.
3. Under Screen Lock, select Enable, then enter the amount of idle time (in minutes) that will automatically cause a logout.



4. To disable Screen Lock, click **Disable**.
5. Click **Save** to save the changes.

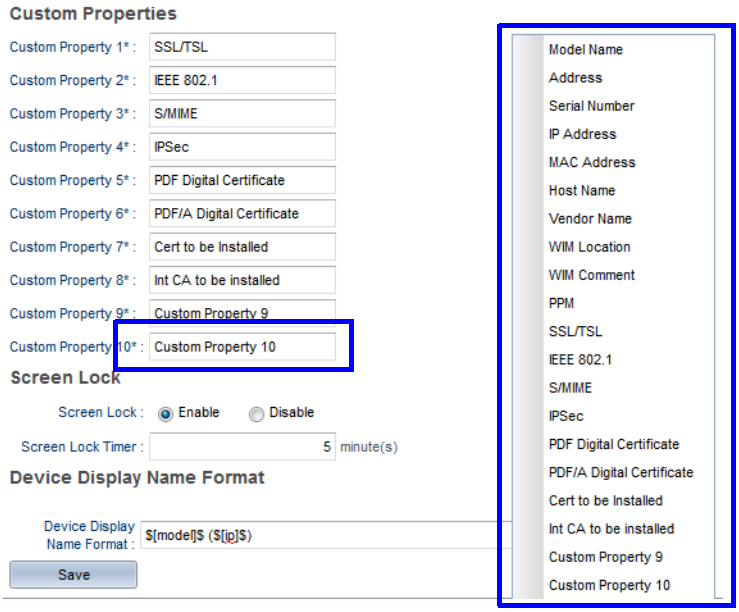
5.4.5 Set the Device Display Name Format

If you have configured device discovery to locate and add new devices to the system automatically, you can use the device display name setting to automatically update the device name that is assigned to the device in the @Remote Connector NX Device List. By default, the name is set to display the Model name, followed by the IP Address. This feature uses variables to determine the name format. You can select from the following variables:

Variable	Variable
Model Name	Address
Serial Number	IP Address
MAC Address	Host Name
Vendor Name	WIM Location
WIM Comment	PPM
Custom Property 1 - 10 (if defined)	

1. On the Navigation tree, click **System,** then locate the **Server Settings** folder.
2. Click **Display**.
3. Under Device Display Name Format, remove the variables you do not want to use, then right-click in the field to add new variables. In the example below, Custom Property 10 was right-clicked.

4. From the list that appears, select the variable that you want to use.



5. When finished, click **Save** to save the changes.

The Device tab will update automatically to display the new name format.

5.5 System Data Management

System Data Management settings address data storage periods, HDD and DB capacity settings, and deletion settings.

The Data Storage Periods determine the default storage period for the following:

- Device Status
- Device Counter
- User Counters
- Logs (including the System, Task, and Audit logs)

The retention period for each data set can be managed individually.

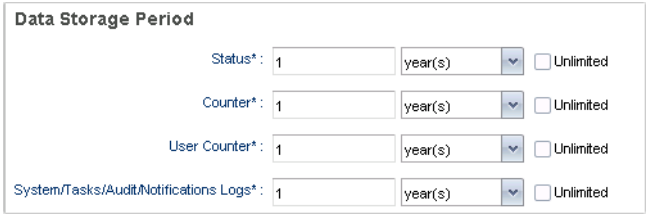
1. On the Navigation Tree, open the **System** branch**,** then select **System Data Management** from the **Server Settings** folder.

2. Under **Data Storage Period**, complete the following:

   a. Set the storage period for **Status**, **Counter**, **User Counter, and Logs**. By default, all status and counters are retained for 1 year.

   TIP: If you have sufficient storage capacity, you can enable the Unlimited checkbox beside any option to ensure that all status, counter, or user counter data is kept unless the HDD Capacity settings are met.

   b. Set the **System/Tasks/Notifications Logs** period. You can select a period of days, months, years, or click the Unlimited option to keep the data as long as the capacity settings are not exceeded.



3. Under **HDD Capacity** complete the following:

   a. In the **Remaining Capacity When Nearly Full** field, enter the number of free GB remaining on the hard disk that will trigger 'nearly full' status. By default, if free space falls below 2 GB, 'nearly full' status is triggered.

   b. In the **Remaining Capacity When Full** field, enter the number of GB that will trigger Full status. When this status is triggered, the **Deletion Settings**

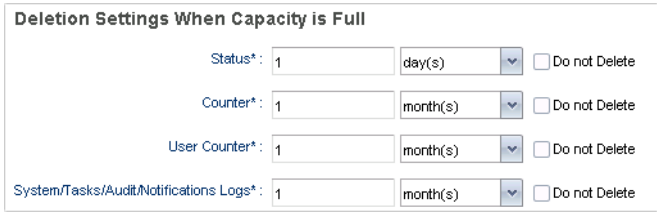
When Capacity is Full options are applied and data is deleted according to the settings.

NOTE: If the System Alert Notification is configured for HDD Capacity Full (on the Navigation Tree, see System → Server Settings → Networking), an alert is sent to the specified Email address regarding the capacity.

4. Under **Deletion Settings When Capacity is Full,** set the required options:

   By default, the status data for one day (the least recent data) will be deleted, and other data (Status, Counter, User Counter, and Logs) for one month (the least recent data) will be deleted. To prevent a particular log from deletion, enable **Do not Delete**.

   As an example, if you set the Deletion Setting for logs to 6 months and you have 24 months of log data currently on the disk, the LEAST recent 6 months of log data will be deleted to free up disk space.



5. Click **Save**.

5.6 View System Information

If you need to view the current @Remote Connector NX software version, you will find this information under the System Information options in the System → Server Settings folder. You will also find information about the number of registered devices, number of registered groups, and number of registered maps.

1. On the Navigation tree, click **System, then** locate the **Server Settings folder.**

2. Click **System Information and Settings**.

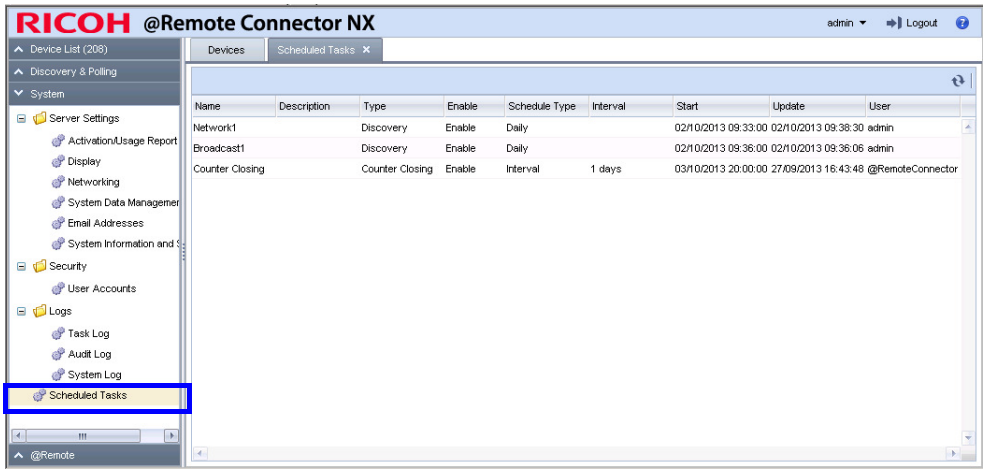
3. The current @Remote Connector NX server version information is displayed. This information is read-only.

4. To obtain debug log data about a customer environment (including device information), only a user with Admin privileges can download the logs to a specified location. If you are not logged in with sufficient privileges, you will see an 'Access Denied' message.

5.7 View Scheduled Tasks

A scheduled task is created when you configure a broadcast or network device discovery. If you set the discovery to occur at a future date and time, you can view the Scheduled Tasks list to see the list of tasks, the associated schedule per task, and the user who created the task.

1. On the Navigation Tree, open the **System** branch**,** then select the **Scheduled Tasks option**. The schedule will load as a read-only view.



CHAPTER 6

View Log Data

@Remote Connector NX offers three different log types to assist with audit and performance. At this point in initial configuration, you can configure the data retention settings for these logs.

Task Log	Use the Task log to track the status of user-initiated configuration tasks including scheduled device discovery tasks, and automated system tasks such as periodic device counter and information checks.
System Log	Records all system-related activities such as system activation/deactivation, hard disk space checks, software downloads, etc.
Audit Log	Use this log to view operations initiated by @Remote Connector NX users, including the operation performed and the time the action was initiated.

This section includes instructions to filter the log data to easily find what you need, and to export the data of any log to an external file.

For instructions to adjust the length of time that the log data is retained before it is deleted from the system, see *5.5 System Data Management* on page 80.

6.1 Task Log

A log entry is added to the task log each time a new task begins. While executing the task, @Remote Connector NX continuously updates the log. When the task is complete, the log is updated with the final result.

Each log entry appears in the upper portion of the screen. Columns include Start Date & Time, End Date & Time, Task Name, Category, Event, Progress, Result, Cause, Error Code, and Owner.

When you click on an entry from the upper area of the Task Log, additional details about specific devices are displayed in the Log Details area. The details listed depend on the task category:

- **Discovery**: Result Details are shown only for newly discovered devices.
- **Polling**: Result Details are shown only for failed devices.

Columns in the Result Details include Template Name, Start Date & Time, End Date & Time, Model Name, Address, Serial Number, Function (i.e. Network Device Discovery, Device Monitoring, Device Preference, etc.), Function Details (i.e. Status, Polling, Check, Apply, etc.), Result, Cause, and Error Code.

When viewing individual device details, the columns include Item Name, Template Value, Value Retrieved from Device, Result, Cause, and Error Code.

For information about filtering the log, see *6.4 Filtering Log Data* on page 89. For details about exporting the log data, see *6.5 Exporting Log Data* on page 90.

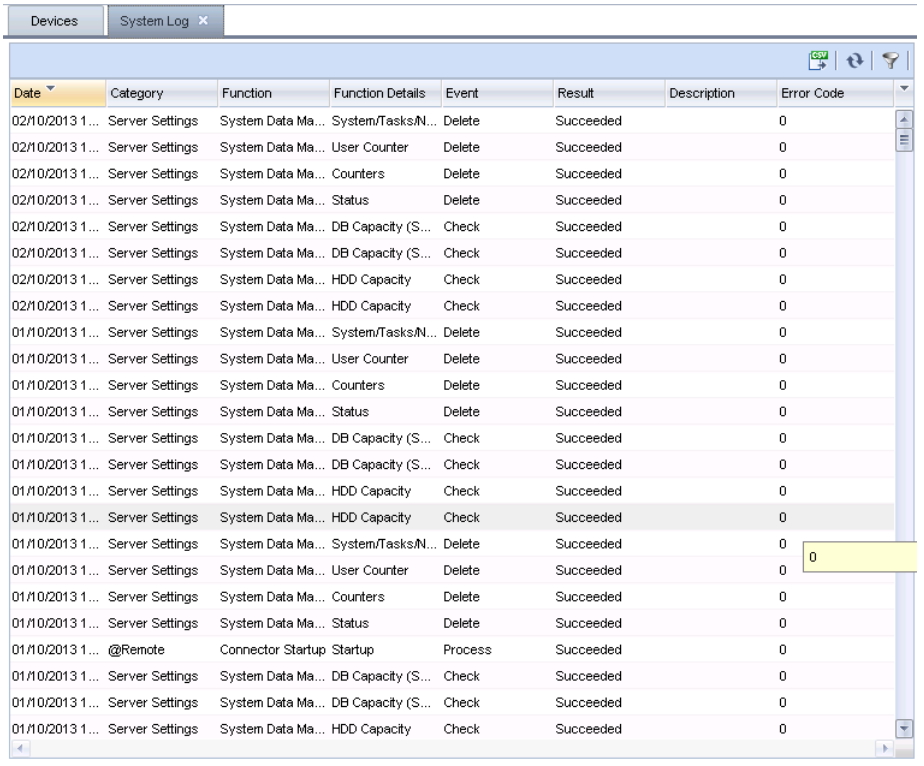
6.2 System Log

The System Log displays a record of internal system behavior. Each log entry includes information about the event category, function, details, event type, result, a description (if available), and the error code (if applicable). Click the Refresh button to obtain the most current log data.

The following events may be logged:

- Device Management/Monitoring: Device, Counter, User counters are added/updated/deleted into/from database*
- System Setting: Historical Data is deleted, Activation/Deactivation is performed, Usage report/Software update notification is performed
- System: System start up/shutdown
- Authentication: Login/Logout
- @Remote: Confirm communication, settings updates

** These entries are written only when the process failed.*



The following columns are included in the system log.

Column	Description
Date and Time	• Date and time when the log entry occurred.
Category	• Function category: discovery, device monitoring, device configuration, etc.
Function	• Function name: device configuration, SDK application management, etc.
Function Details	• Details of the function.
Event	• Event content: start, end, add.
Result	• Result of the function: started, failed, failed partially.
Description	• Details of the log: reasons of failure when execution failed.
Error code	• The specific error code if the execution failed.

For information about filtering the log, see *6.4 Filtering Log Data* on page 89. For details about exporting the log data, see *6.5 Exporting Log Data* on page 90.

6.3 Audit Log

The read-only Audit log records user actions made to the system, and provides a trail to associate actions with a particular user. In cases where you have multiple administrators working within the same system, this log can provide a valuable method to track changes made in the system.

This log contains the following columns:

Column	Description
User Name	• Login name of the user that made the change.
Date	• Date and time the change was made.
Action	• The action taken may include Add, Delete, Edit, or Update.

Column	Description
Target	• The location where the action was taken: •Discovery Profile •Device •Device Group •Device Category •System Settings •@Remote Settings •Authentication and Accounts
Audit Log Details	• Specific information related to the Action taken.

For information about filtering the log, see *6.4 Filtering Log Data* on page 89. For details about exporting the log data, see *6.5 Exporting Log Data* on page 90.

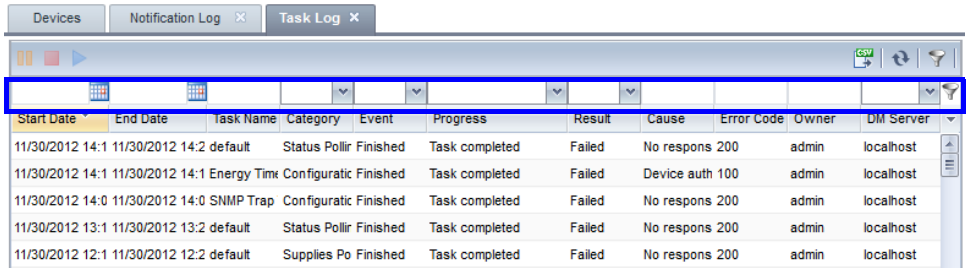
6.4 Filtering Log Data

The Quickfilter option allows you to filter the log entries based on the values you enter for one or more columns. Use this feature as a search tool when looking for specific log entries in the Task, Audit, or System Log.

1. Open the log you want to filter. This example filters the Task Log.

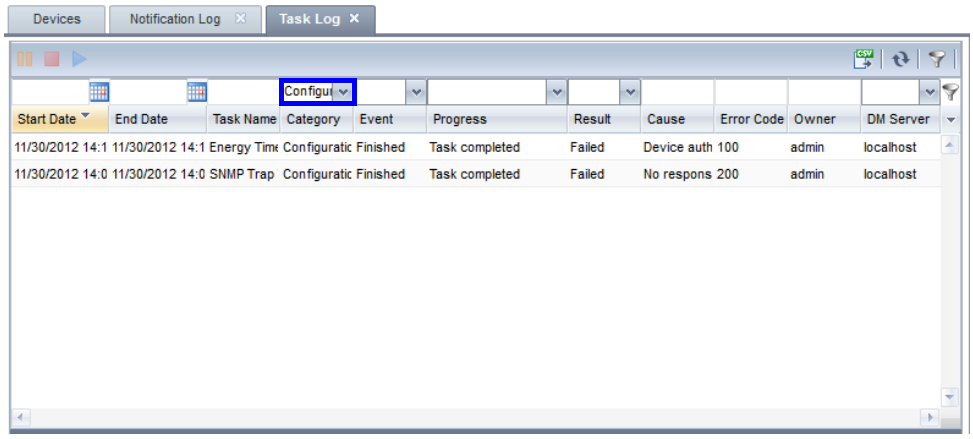
2. Click the **Filters** button on the Options bar.

The Filter fields appear above the columns in the log.



3. Type the filter criteria in the text entry fields, or click the drop-down list in any of the fields with pre-set criteria (such as Event or Category). Ensure you press the entry key after typing or making your selection to force the results to load.

In this example, we filtered the list to view only Configuration Notification entries.



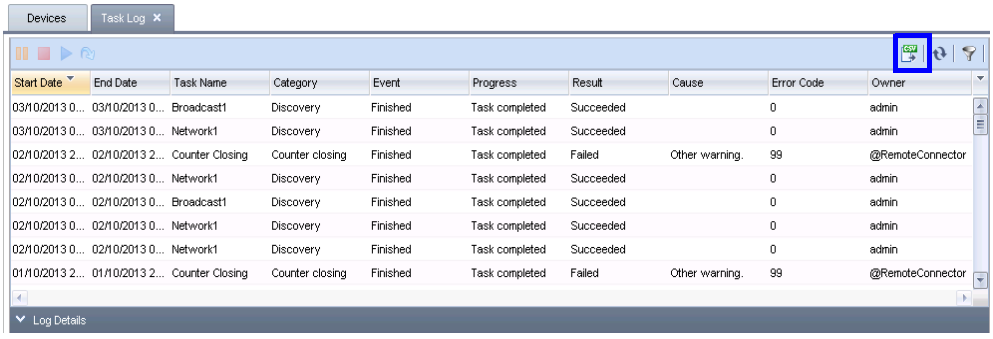
You can further filter the list by entering criteria in additional columns. For example, we could also filter based on the Result column if there were many entries still in the list to sort through.

6.5 Exporting Log Data

You can export the data from any log to a CSV file. The log is exported according the current view, so if you have applied any filters, the log exports only the filtered data, not all data in the log. The log includes the date and time generated, the log type (Task, Audit, or System) and columns appropriate to the log type.

1. Open the log you want to filter. This example filters the Task Log.

2. Click the **Export** button on the Options bar.



3. Select the location where you want to save the file, or open the file in the selected external application.

CHAPTER 7

Configure @Remote Settings

This chapter provides details about the options that are available to @Remote Connector NX Administrators in the @Remote branch of the Navigation Tree.

The settings described this chapter are available to any user that is assigned the Full Admin user role. See *2.1 Access Roles & Privileges* on page 22 for information about these roles.

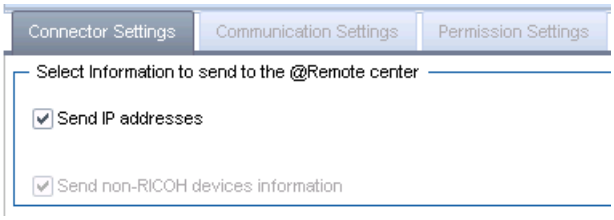
NOTE: Some options and entire tabs within the @Remote branch are available to Ricoh Customer Engineers only and are shown as gray text that is not editable to user logged in with the Full Admin user role. These options and tabs are not described in this chapter.

Warning: With the exception of the Connector Settings tab, the tabs in the @Remote Settings branch of the Navigation Tree are hidden from view until server registration with the @Remote Center System is complete.

7.1 View Connector Settings

The Connector Settings tabs provides the connection and registration information that enables @Remote Connector NX to communicate with the @Remote Center System.

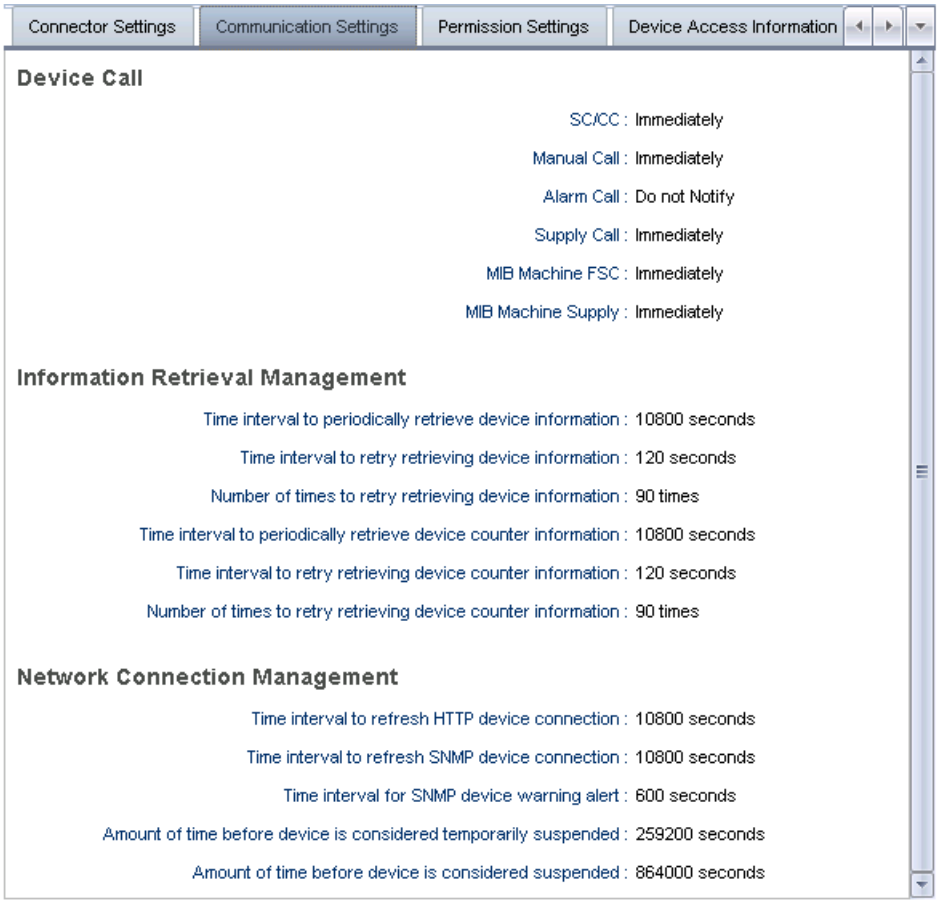
On this tab, the @Remote Connector NX can enable or disable the Send IP addresses option only.



Option	Description
Send Information to the @Remote Center	• **Send non-Ricoh devices information:** When enabled, sends the on-site device IP Addresses of non-Ricoh devices to Ricoh. This field is enabled by default and not editable for @Remote Connector NX. **Warning:** Deselecting this option can affect a number of functions. It is strongly recommended that you consult with a Ricoh Customer Engineer before deselecting.

7.2 View Communication Settings

This tab provides a read-only view of the settings currently applied within the @Remote Center System to achieve communication between @Remote Connector NX and the @Remote Center System.

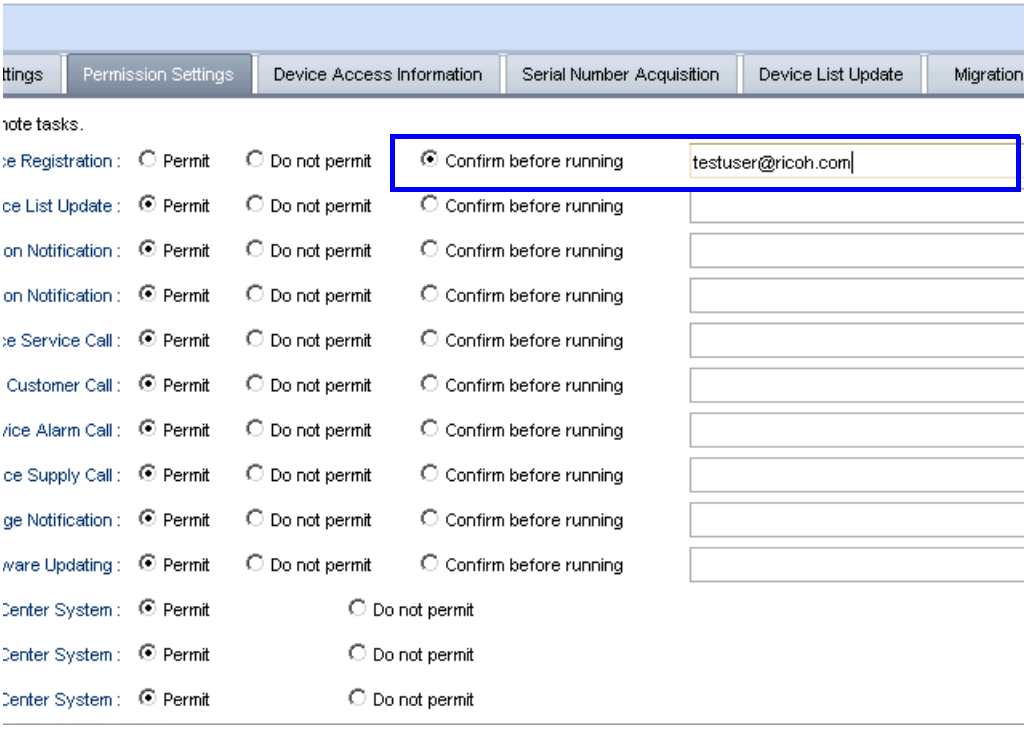


7.3 Configure Permission Settings

For each @Remote task on this tab, the Administrator can set **Permit**, **Do not permit**, or **Confirm before running**:

- **Permit:** Allows the task to execute automatically.
- **Do not permit:** The task will not be executed
- **Confirm before running:** When this option is selected, the Administrator must click **Select email address** to identify an email address that will receive a message to notify them that a task is awaiting their permission The user must login to @Remote Connector NX and confirm the task in the **Task Permit** area. See *Task Permit* on page 98 for details.

NOTE: The email addresses used to confirm before running are derived from **System →Server Settings →Email Addresses. See** *5.2.2 Email Addresses* on page 72 for details.



The Administrator can set individual permissions for each of these tasks:

- Device Registration
- Device List Update
- Device Status Information Notification

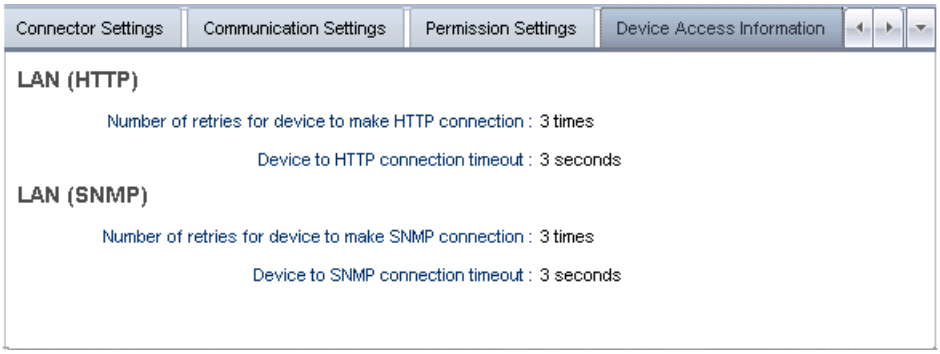
- Device Counter Information Notification
- Device Service Call
- Device Manual Call / Customer Call
- Device Alarm Call
- Device Supply Call
- Device Information Change Notification
- Device Firmware Update
- Device Registration from @Remote Center System *
- Information Setting Request from @Remote Center System *
- Information Getting Request from @Remote Center System *

** Confirm before running is not available for these options.*

If you make changes on this tab, ensure you click **Save** to apply the changes.

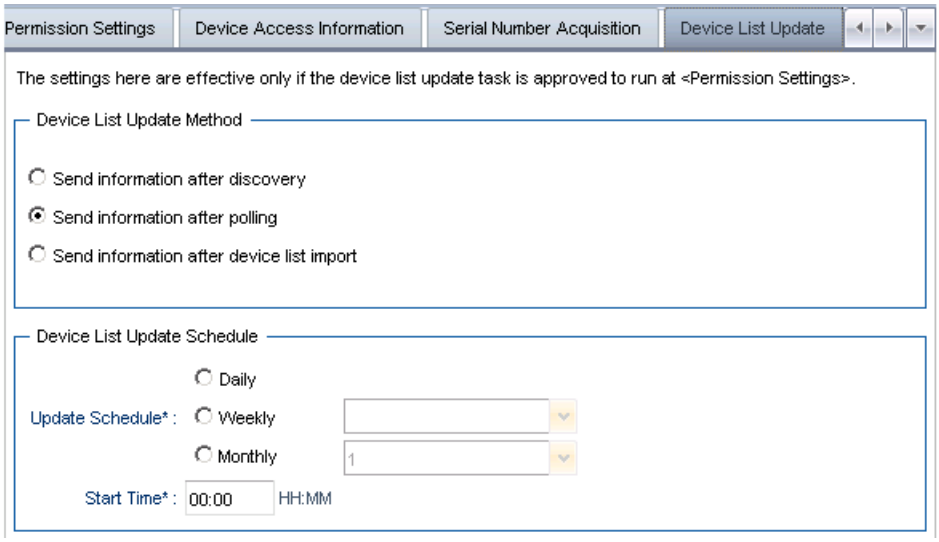
7.4 View Device Access Information

This tab provides read-only information about the HTTP and SNMP connection settings currently applied between @Remote Connector NX and the @Remote Center System.



7.5 Configure Device List Updates

The options on this tab determine how the device list is updated prior to sending data to the @Remote Center System. This tab allows you to set a single update method, and set the corresponding update schedule.



Update Method	Description
Send information after discovery	Discovery and polling are run before sending data to the @Remote Center System.
Send information after polling	Polling is run before sending data to the @Remote Center System, but Discovery is not performed. **NOTE:** If this option is selected, onsite discovery must be scheduled to run periodically in order to send new device information to the @Remote Center System. See *Chapter 3: Add Devices to Manage* on page 27 for instructions.
Send information after device list import	The device list is retrieved from Device Manager NX Pro or Device Manager NX Enterprise, and only devices within the list are polled before the data is sent to the @Remote Center System.

To determine how often the Device List is updated in the @Remote Center System, set the **Update Schedule**.

NOTE: If the time set on the @Remote Center System differs from the time set on the @Remote Connector NX, the value from the @Remote Center System is displayed.

Option	Description
Daily	If you enable Daily, also select the Start Time in hours and minutes when the update will be sent.
Weekly	To send updates only once per week, enable Weekly, then select the day of the week you prefer. Select the Start Time in hours and minutes when the update will be sent.
Monthly	To send updates only once per month, select the date you want to send the update (1 through 31). Select the Start Time in hours and minutes when the update will be sent.

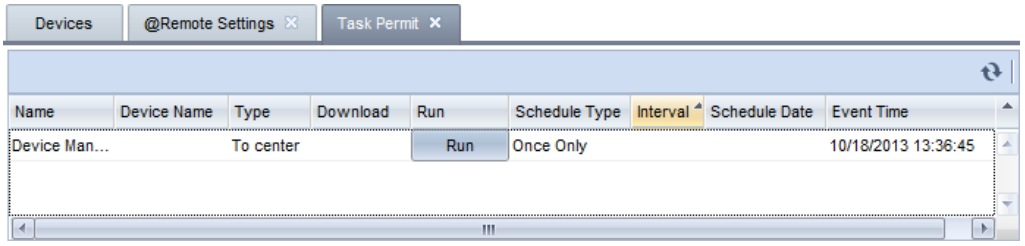
Click **Save**  on the Options Bar to save the schedule update.

7.6 Task Permit

If the @Remote Connector NX Administrator enabled any **Confirm before running** setting in the @Remote Settings Permission settings tab, they identified a user who received an email notification regarding a task awaiting in the @Remote Connector NX web management portal requiring their approval. Identified users are Administrators who are responsible for particular areas of the product, and have a valid Full Admin user role assigned to their user account.

NOTE: See *7.3 Configure Permission Settings* on page 94 for details about the tasks that can require approval.

After receiving the notification message, the user can login to the @Remote Connector NX web management portal with a valid account. On the Navigation Tree, click the **@Remote** branch, then click **Task Permit**.



The task remains in the Task Permit tab until the Administrator runs the task, or until an event occurs to match the automated delete condition, as described in the table below.

Task	Automatic Delete Condition	Schedule Type	Notes
Device Registration	On next update	Once Only	
Device List Update	On next update	Interval	
Device Status Information Notification	On next update	Interval	
Device Counter Information Notification	On next update	Interval	
Device Service Call	On next update	Once Only	Per Device

Task	Automatic Delete Condition	Schedule Type	Notes
Device Manual Call / Customer Call	On next update	Once Only	Per Device
Device Alarm Call	On next update	Once Only	Per Device
Device Supply Call	On next update	Once Only	Per Device
Device Information Change Notification	On next update	Interval	Per Device
Device Firmware Updating	Schedule Expired	Once Only	

Columns in the Task Permit tab include:

Column	Description
Name	Task name that is waiting for permission to run.
Device Name	For tasks that are applicable Per Device, the device name of IP Address of the target device.
Type	The task type (To Center or To Device). **NOTE:** Only the Device Updating Firmware Task is 'To Device' type.
Download	Click to download the data that will be sent to the @Remote Center System. **NOTE:** This option is not applicable to Device Firmware Updating tasks.
Run	Click Run to execute the task.
Schedule Type	The task schedule type (Interval or Once Only).
Interval	The task interval, shown in the NN hours/days/weeks/ months format **NOTE:** This option is not applicable to Device Firmware Updating tasks.
Schedule Date	The @Remote Center System specified schedule date.

Column	Description
Event Time	The date/time when the call or notification should be sent the @Remote Center System.


RICOH