NETGEAR®

NETGEAR ProSafe NMS200 Network Management Software

Quick Start Guide

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at
http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at
http://support.netgear.com/app/answers/detail/a_id/984

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10727-04	v1.0	September 2011	First publication

Contents

Before You Begin

1

Requirements for installation and use

This chapter provides an overview of the NETGEAR ProSafe NMS200 Network Management Software for managing your NETGEAR resources.

The following topics are discussed:

- *Network Management*
- *Compatible NETGEAR Devices*
- *System Requirements*
- *Update Your License*

Network Management

The NMS200 Network Management Software provides a browser interface to discover, configure, and monitor your NETGEAR resources across your entire network.
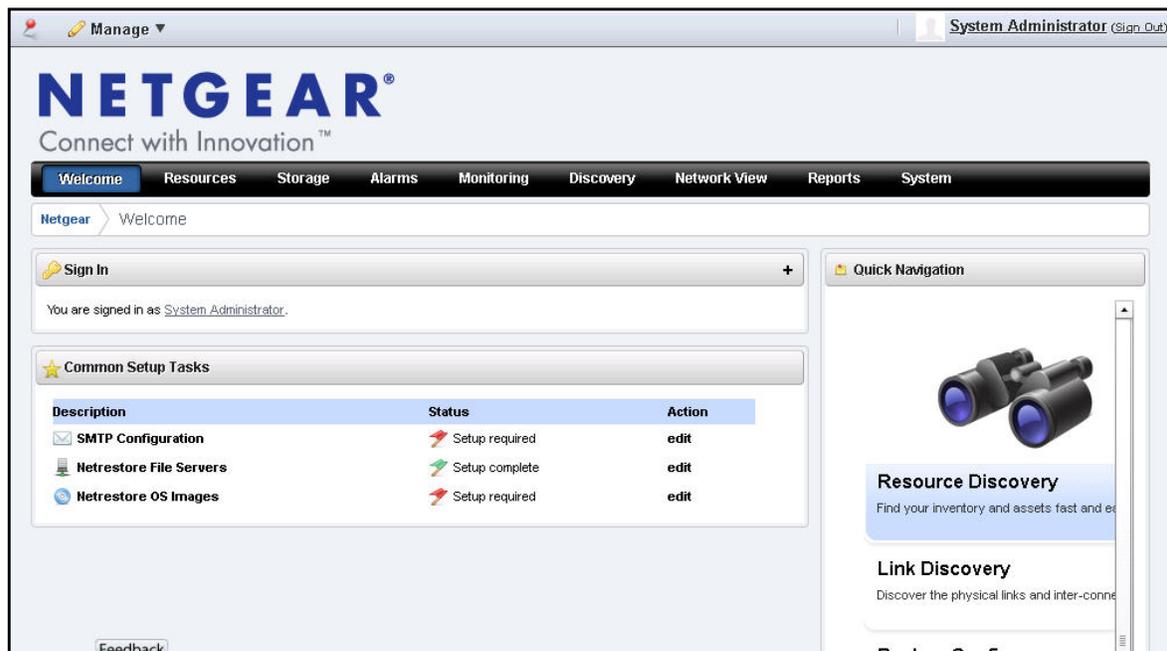
Discovery and Mapping

Once initiated, the NMS200 Network Management Software automatically discovers all NETGEAR-compatible equipment, interfaces, and physical and logical connectivity across your network using various protocols and centralized credentials.

Table 1. Discovery and Mapping

Capability	Purpose
Automated device discovery	Includes top-level components, subcomponents, interfaces, and ports as applicable.
Automated link discovery	Ethernet link discovery with LLDP.
Discovery protocol support	LLDP support.
Discovery scheduling	Ability to schedule discovery tasks at specified times and dates in the future.
Device resynchronization	System resynchronization with your device inventory.
Device resynchronization scheduling	Ability to schedule device resynchronization at a specified times and dates in the future.
SNMP MIB browser	Includes an SNMP MIB browser to view the attributes of all MIBs in a device.

Configuration

The NMS200 Network Management Software's configuration management capabilities let you automatically maintain, back up, restore, and compare network device configurations.

Table 2. Configuration

Capability	Purpose
Configuration file backup	Back up device configuration file; 1:1 and 1:many, immediately or scheduled.
Configuration file restoration	Restore device configuration file; 1:1, immediately or scheduled.
Device firmware update	Automated deployment of a selected version of firmware, either immediately or scheduled.
Firmware pre-load	Pre-load firmware versions into the application.
Configuration file comparison	Compare color-coded, line-adjusted text of two selected devices or stored files.
Device configuration	Direct access/cut-through (HTTP/Telnet/SSH).

Monitoring

The NMS200 Network Management Software's built-in monitors collect and analyze real-time conditions and performance metrics for NETGEAR managed equipment. The management platform also escalates any alarms that occur.

Table 3. Monitoring

Capability	Purpose
Topology mapping	Geographic and logical topology views, including filtering.
Event monitoring	SNMP trap reception with defined trap attribution, severity, and descriptions.
Alarm escalation	Alarm generation based on pre-defined event definitions.
Alarm propagation	Alarm propagation to alarm viewer and topology views.
Alarm/event actions	Event/alarm-initiated pre-defined or user-defined actions: notification or configuration operations.
Device performance key metrics	Real-time key performance metric collection and display for interfaces and ports of selected devices.
Active performance monitoring	Device and interface monitoring, historical data persistence, thresholding, and graphing.
Canned reports	Pre-defined reports for inventory, availability, and port status.

Compatible NETGEAR Devices

The NMS200 Network Management Software is compatible with the following NETGEAR devices (consult the Manage > Show Versions screen for the details).

NETGEAR Managed Switches

- FSM726-300
- GSM7224-200
- GSM7248-200
- GSM7228PS
- GSM7252PS
- GSM7328S-200
- GSM7352S-200
- GSM7328FS
- XSM7224S

- GSM7328S
- GSM7352S
- GSM7248
- GSM7224R
- GSM7248R
- GSM7224
- GSM7212
- GSM7312
- GSM7324

- FSM7328S
- FSM7352S
- FSM7328PS
- FSM7352PS
- FSM7326P
- FSM7226RS
- FSM7250RS
- XCM8806
- XCM8810

NETGEAR Smart Switches

- FS726T
- FS726TP
- FS728TP
- GS108T-200
- GS110TP

- GS716T-200
- GS724T-300
- GS748Tv3
- GS724TP
- GS748TP

- GS724TS
- GS748TS
- GS724TPS
- GS748TPS

NETGEAR Storage

- ReadyNAS 4200
- ReadyNAS 3200
- ReadyNAS 3100

- ReadyNAS 2100
- ReadyNAS Pro
- ReadyNAS Pro 2

- ReadyNAS Pro 4
- ReadyNAS Pro 6
- ReadyNAS NVX

NETGEAR Wireless Controllers

- WC7520

- WMS5316

System Requirements

System requirements vary depending how you use the application and the operational environment. Because NETGEAR does not know your specific network and devices, these recommendations are based on typical rather than definitive configurations.

> **Tip:** Base the minimum configuration of any system on its expected peak load. Your installation should spend 95 percent of its time idle and 5 percent of its time trying to keep pace with the resource demands.

Table 4. Operating Environment

Operation	Requirement
OS support	Windows Server 2003 32/64-bit.
	Windows Server 2008 32/64-bit.
	Windows XP 32-bit.
	Windows Vista® 32/64-bit.
	Windows 7 32/64-bit.
GUI-based installation	Automated (single server deployment—Windows).
Configurable installation location	Default install directory/path can be changed during installation process.
Management interface support	SNMP v1/v2/v3.
	CLI: Telnet/SSH.

Supported Operating System Versions

The following are supported operating system versions:

- Microsoft® Windows Server® 2003 (Standard, Enterprise, and Web), Server 2008 Enterprise.

  Windows Terminal Server is not supported. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server.

- Microsoft Windows XP (Professional) with current patches applied, including SP3.
- Microsoft Windows Vista (Business and above).
- Windows 7.

Disable user access control if you are installing on Vista, Windows Server 2008, or Windows 7. Also, this application cannot coexist with other installations of Cygwin on the same Windows computer.

Supported Web Browsers

- Internet Explorer 8
- Internet Explorer 9
- Google Chrome 10.x

Hardware Recommendations

The NMS200 Network Management Software contains an Application Server that runs continuously in the background. The minimum hardware recommendations are:

- 2.8 GHz dual core CPU
- 4G RAM (8G for 64-bit operating systems)
- 40G available disk space

Device monitoring stops when you stop the application server or turn off its host machine. Best practice is to install the application server to a host you do not turn off if you want constant monitoring of your devices.

Network Considerations

The system the NMS200 Network Management Software is on is required to be connected to a network for the application to start successfully.

Fixed IP Address

The NMS200 Network Management Software's application server is required to be installed on a host with a fixed IP address or a permanently assigned Dynamic Host Control Protocol (DHCP) lease. The fixed IP address is required for the application server to communicate with the managed devices.

> **Tip:** For trial purposes, you can rely on a dynamic IP address assignment with a long lease, but NETGEAR does not recommend this approach for production installations.

Firewalls

Firewalls, or SNMP management programs using the same port on the same machine where NMS200 Network Management Software is installed, can interfere with communication.

To deal with such barriers (such as initial device configuration to accept management, security measures, or firewalls), consult with your network administrator to ensure that the NMS200 Network Management Software has access to the devices you want to manage. The following protocols are used by the NMS200 Network Management Software:

- HTTP/S
- SNMP

- TCP/IP
- UDP Multicast

Authentication

For successful discovery of the resources on your network, the NMS200 Network Management Software requires authenticated management access to the device. To get this access, provide the correct SNMP community strings, WMI login credentials, and any other command-line (Telnet / SSH) or browser (HTTP/HTTPS) authentication. SNMP is required to be enabled (if that is not the device's default).

Some devices require pre-configuration to recognize this management software. Consult your network administrator for this information.

Name Resolution

The NMS200 Network Management Software server require resolution of device names to work correctly, whether by host files or the Domain Name System (DNS). The application server cannot respond to hosts with IP addresses alone. The application server might not even be in the same network, and therefore, the host would be unable to connect.

The NMS200 Network Management Software also supports installation only on the local file system. Avoid installing to shared drives.

Update Your License

If you have a limited license, then the NMS200 Network Management Software by default limits the number of devices that can be managed through the software to five devices. Go to *www.netgear.com/nms200* for more information about licenses.

Software Installation and Licenses 2

Get the NMS200 installed and running

This chapter describes how to get the NMS200 Network Management Software installed and running, along with how to manage your licenses and install software updates.

The following topics are discussed:

- *Initial Installation and Startup*
- *How to Manage Your Licenses*
- *How to Install Software Updates*

Initial Installation and Startup

Perform the following steps to install and start the NMS200 Network Management Software:

- *Step 1: Get the NMS200 Network Management Software*
- *Step 2: Select the Machine That Will Run the Software*
- *Step 3: Install the NMS200 Network Management Software*
- *Step 4: Log In to the NMS200 as the admin User*

Step 1: Get the NMS200 Network Management Software

The NETGEAR ProSafe NMS200 Network Management Software is downloadable at *www.netgear.com/nms200* and available on a CD (the size of the image exceeds 500 MB). This software is the fully functional version that includes a five-device test capability with no expiration date.

Various license packs are available when you are ready to expand beyond this five-device test capability. Go to *www.netgear.com/nms200* for more information about licenses.

Step 2: Select the Machine That Will Run the Software

The NMS200 Network Management Software contains an Application Server that runs continuously in the background. The minimum hardware recommendations are:

- 2.8 GHz dual core CPU
- 4G RAM (8G for 64-bit operating systems)

- 40G available disk space

Device monitoring stops when you stop the application server or turn off its host machine. Best practice is to install the application server to a host you do not turn off if you want constant monitoring of your devices.

For the operating system and hardware requirements to run the NMS200 Network Management Software, see *System Requirements* on page 9.

Step 3: Install the NMS200 Network Management Software

Perform the following steps to install the NMS200 Network Management Software.

- *Step A: Disable or Remove Conflicting Software (if necessary)*
- *Step B: Obtain a Fixed IP Address (if necessary)*
- *Step C: Install the Full NMS200 Software*

Step A: Disable or Remove Conflicting Software (if necessary)

Disable or remove conflicting software (see the following table).

Table 5. Conflicting Software

Software	Action
Cygwin	The NMS200 Network Management Software cannot co-exist with other installations of Cygwin on the same Windows computer. • Do not install the NMS200 Network Management Software where Cygwin is already installed, either separately or as part of another application. • If Cygwin is already installed, remove it before installing this application.
User access control	Disable user access control if you are installing on Vista, Windows Server 2008, or Windows 7. The installer might halt when pre-existing bash sessions or CMD sessions are open. Close all such sessions.

Also, make sure your network and the devices on the network are set up correctly. See *Network Considerations* on page 10.

⚠ **CAUTION:**

Windows also installs Internet Information Services (IIS) —formerly called Internet Information Server. That installation does not turn IIS on by default. Do not enable IIS on the host running NMS200.

Step B: Obtain a Fixed IP Address (if necessary)

The NMS200 Network Management Software has an application server that is required to be installed on a host that has a fixed IP address or a permanently assigned Dynamic Host Control Protocol (DHCP) lease.

> **Note:** For trial purposes, you can rely on a dynamic IP address assignment with a long lease, but NETGEAR does not recommend this approach for production installations.

To obtain a fixed IP address, consult with your network administrator or Windows help if you have questions.
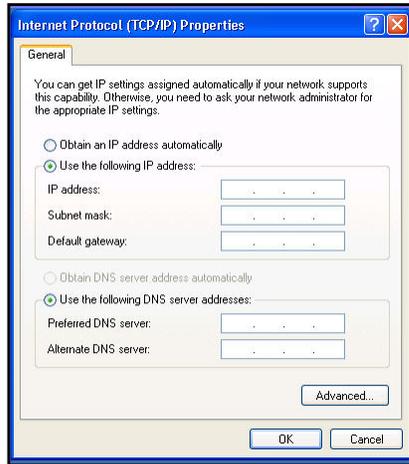
Step C: Install the Full NMS200 Software

The full NMS200 Network Management Software contains both the application server and Web server.

> **Note:** This software is a Java application. Virtual memory use increases when you install it. This is normal. If you monitor memory use over time it might appear that memory use is growing. This is a normal function of Java's memory management.

➢ **To install and start the NMS200 software:**

1. Unzip (decompress) the NETGEAR.*w.x.y.z*.zip file if you downloaded the application in .zip format, and close any applications that might interfere with this installation.

    Otherwise, insert the CD into the CD drive and open its associated directory.

    Be aware of the following requirements when selecting user names for the installation:

    • Install as a non-root user with the permission to create directories in the selected installation target path. Installing to a directory that requires root-level access fails.

- Do not use admin as the installing user account on your computer. Doing so wipes out any pre-configured admin permissions that come with the application (see *Step 4: Log In to the NMS200 as the admin User* on page 17).

2. Log in to your computer as an administrator-type user that can install software and run win_install.exe. Do not install as a user named "admin" or as the root user.
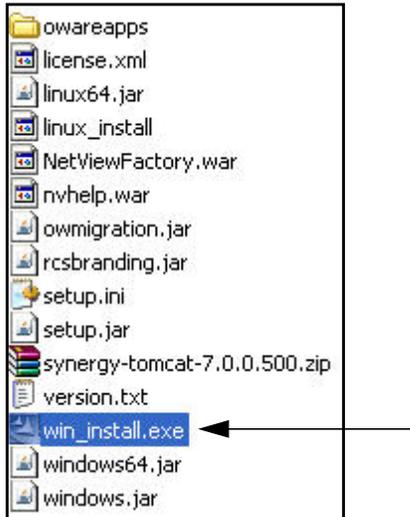
The following screen displays:
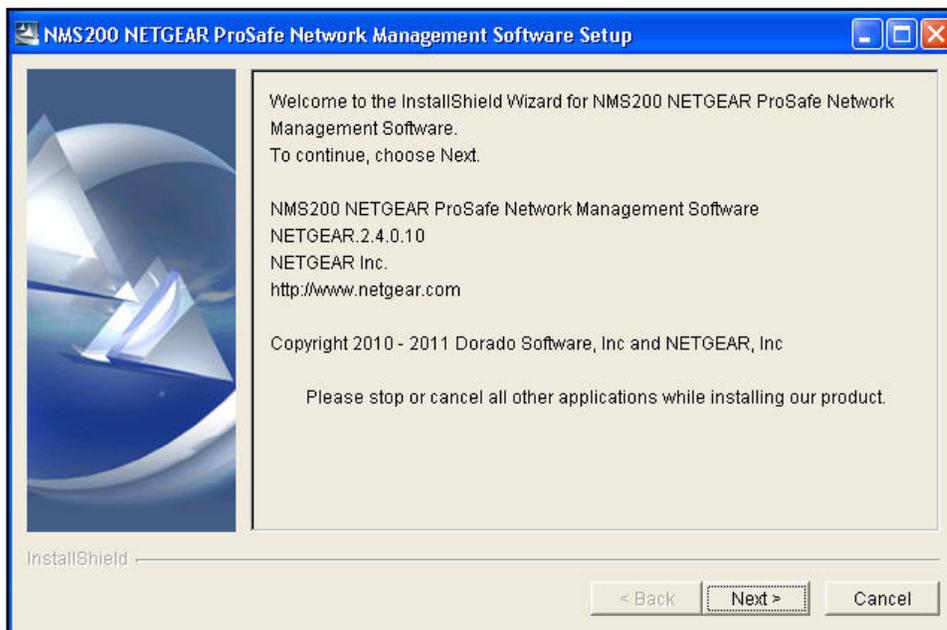
3. To initiate installation, click **Next**.

4. Confirm that your hardware meets the minimum system requirements, and click **Next**.

Minimum System Requirements

Dual core (2.8 Ghz)
4GB RAM - 32 Bit OS
or 6GB RAM - 64 Bit OS
40 GB available disk space

5. Accept the license agreement after reading it (otherwise, you cannot proceed), and click **Next**.

⦿ I accept the terms of the license agreement.
⦾ I do not accept the terms of the license agreement.

6. Confirm or alter the installation path, and click **Next**.

Directory Name:
C:\Program Files\NETGEAR\NETGEAR ProSafe NMS200

Browse

7. View the final confirmation of components to install, and click **Next**.

NMS200 NETGEAR ProSafe Network Management Software will be installed in the following location:

C:\Program Files\NETGEAR\NETGEAR ProSafe NMS200

with the following features:

Core Files
Database Server Configuration
Portal
Application Server Configuration
Mediation Server Configuration

for a total size:

2695.1 MB

Observe the progress bar as files are copied for installation. The database size typically defaults to 2 GB with unlimited expansion.

8. Click **Finish** to complete the installation.
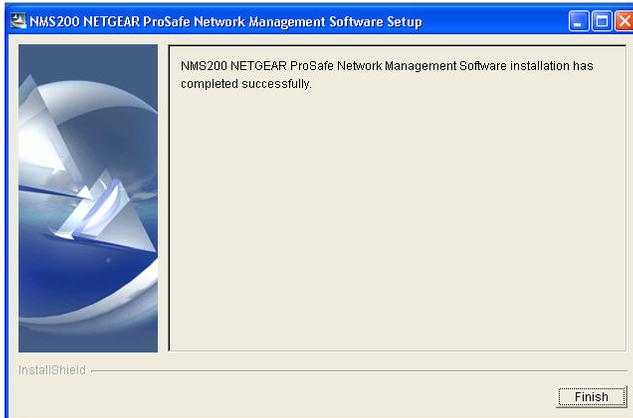
9. Reboot the machine.

When the Server Monitor icon (![icon]) in the system tray turns green (which might take several minutes), you can access the application server with a Web browser.

Note: The NMS200 Network Management Software also installs the Synergy Network Management Server icon (![icon]) in the system tray.

Step 4: Log In to the NMS200 as the admin User

The Server Monitor icon in the system tray indicates the application server's status.

- Red (![icon]) means that the application server is stopped.
- Yellow (![icon]) means that the application server is starting or stopping.
- Green (![icon]) means that the application server is running.

The application server monitors your devices even when you are not logged in to your machine. Best practice is to install the application server to a host you do not turn off if you want constant monitoring of your devices.

When the Server Monitor icon (![icon]) in the system tray turns green, you can access the application server with a Web browser.

➢ **To start and log in to the NMS200:**

1. Select **Start > All Programs > NETGEAR > NETGEAR ProSafe NMS200 > NETGEAR ProSafe NMS200** to invoke the NMS200 Network Management Software.

---

2. On the next screen, enter **netgear** for the Screen Name and **netgear** for the Password. Click **Sign In**.
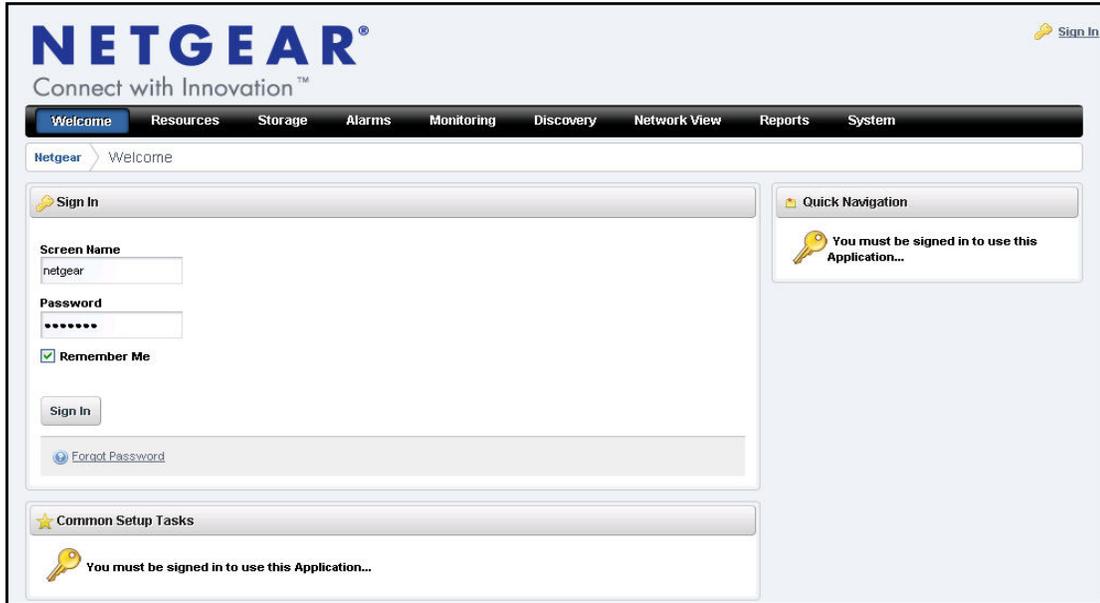
3. You will be asked to set up a password reminder query. Click **OK**. The main screen displays.
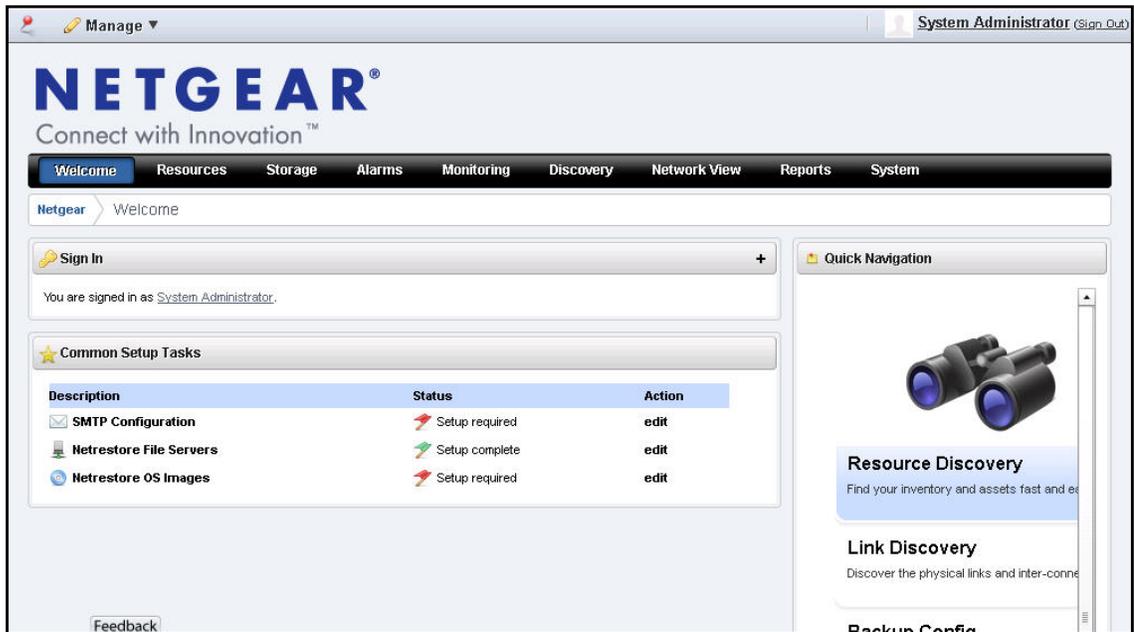
4. Go to *Chapter 3, How to Use the NMS200* to learn how to start managing your network.

How to Manage Your Licenses

Note: The NETGEAR ProSafe NMS200 Network Management Software comes with a five-device test capability that has no expiration date (this default limits the number of devices that can be managed through the software to five devices). Various license packs are available when you are ready to expand beyond this five-device test default. Go to *www.netgear.com/nms200* for more information about licenses.

Either restart the application server or wait up to 15 minutes before a license modification takes effect whenever you obtain licenses for more than the five-device default.

➢ **To activate additional licenses:**

1. Purchase your additional license pack from NETGEAR.

   a. Go to *www.netgear.com/nms200* and click **Buy netgear.com** (Buy netgear.com). Follow the instructions.

   b. Go to *www.doradosoftware.com/netgear* as directed for further instructions.

   You receive your license file when you are done with this step.

2. Click **License Management** on the Quick Navigation portlet.

The Register License portlet displays.
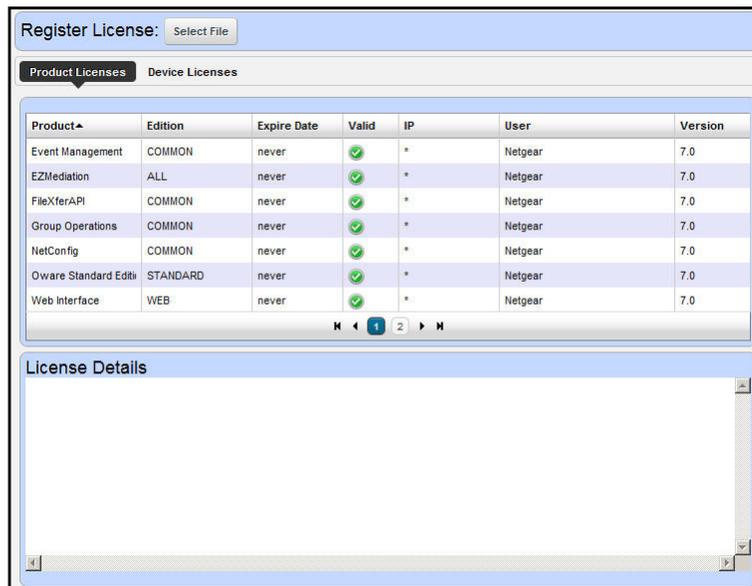
3. Either restart the application server or wait up to 15 minutes for the license modification to be effective.

How to Install Software Updates

Best practice is to perform a complete backup of your system and NMS200 Network Management Software database before performing an upgrade.

➢ **To install NMS200 Network Management Software updates:**

1. Download the new NMS200 Network Management Software.

2. Prepare your system:

    a. Back up your existing NMS200 Network Management Software database.

    b. Halt the NMS200 Network Management Software server.

    c. Export your NMS200 Network Management Software settings. Installation always re-seeds the settings. If you have changed the default settings, you might want to export these before proceeding.

    d. Set a Windows restore point.

3. Uninstall the existing NMS200 Network Management Software. Go to Add/Remove Programs in Windows' Control Panel and uninstall it as you would any other Windows program.

4. Install the new NMS200 Network Management Software.

5. Restart the NMS200 Network Management Software server.

6. Restore your NMS200 Network Management Software configuration:

    a. Refer to the release notes for the procedure to rebuild the NMS200 Network Management Software database. Some upgrades might require you to rebuild the database from scratch.

    b. If you have purchased additional NMS200 Network Management Software licenses, refer to *How to Manage Your Licenses* on page 19.

If your installation fails, see setup.log, db_setup.log, or app_setup.log in the destination directory for the installation for messages that might help fix the failure.

How to Use the NMS200

3

Keep your network running smoothly

This chapter describes how to manage your network starting from the NMS200 Network Management Software main screen using the default settings.
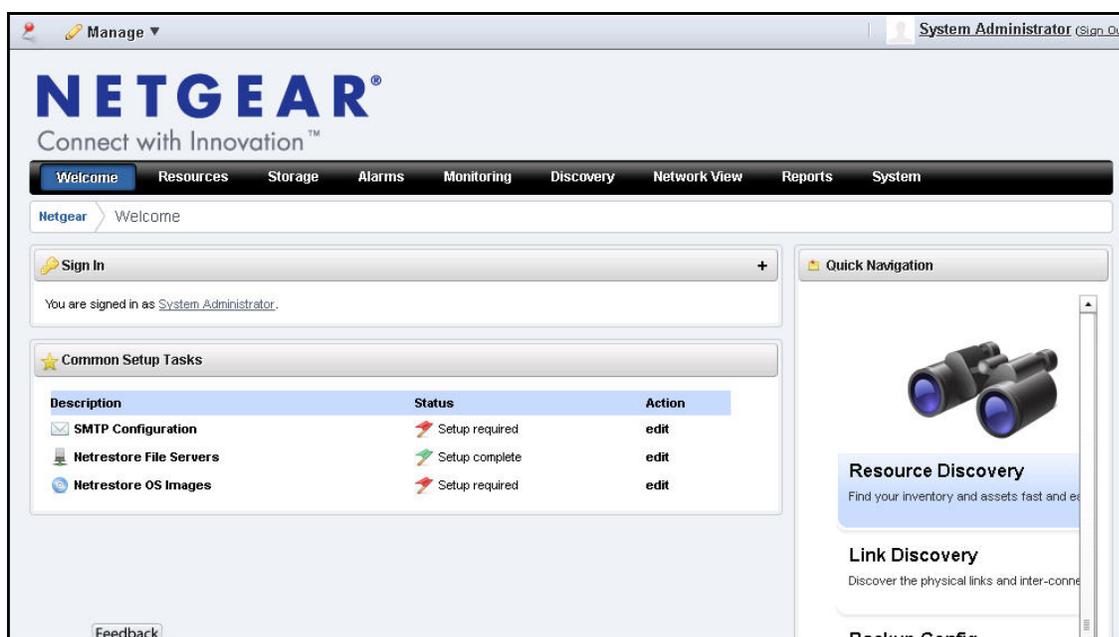
The following topics are discussed:

- *Common Setup Tasks at First-time Sign-in*
- *Quick Navigation Portlet*
- *Configure the NMS200 Groups and Locations*
- *Discover Your Network Resources and Devices*
- *Manage Your Network Resources and Devices*
- *Fault Management and Problem Diagnosis*
- *Performance Management and Troubleshooting*

Common Setup Tasks at First-time Sign-in

This portlet appears on the first page after you sign in.
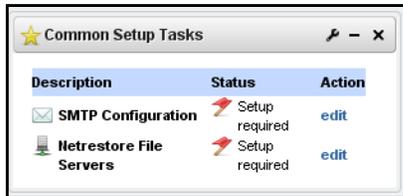
The portlet reminds you of the following common tasks:

- **SMTP Configuration**. This configures how NMS200 sends notification e-mails.
- **Netrestore File Servers**. See *FTP/TFTP Server* on page 27 for the setup instructions.

A red flag appears with the "Setup required" message in the Status column when these are not configured. Configuring them displays a green flag with the "Setup complete" message. Click the edit link in the Action column to open editors for each of these.

Quick Navigation Portlet

The Quick Navigation portlet lets you quickly click some links to basic tasks.

- **Resource Discovery**. Discover devices in your network. See *Discover Your Network Resources and Devices* on page 25.

- **Link Discovery**. After you have discovered resources, this discovers their connections.

- **Backup Config Files**. This lets you back up discovered devices' configuration files. Before you can use this feature, you must have servers configured as described in *Manage Your Network Resources and Devices* on page 27.

- **OS Image Upload**. Upload firmware updates for devices.

- **Deploy OS Image**. This deploys firmware updates. To deploy images, you must have File Servers configured, as described in *Configuration File Backup / Restore* on page 28.

- **License Management**. This lets you see and manage the licensed capabilities of NMS200, as described in *How to Manage Your Licenses* on page 19.

Configure the NMS200 Groups and Locations

As an Administrator, you can configure Users Groups to identify support teams (examples: administration, engineering and operations), and users to identify roles of team members.

Portal > Users

➢ **Add users with the following steps:**

1. Click *Manage > Control Panel > Portal Users.*

2. Click the *Add* tab under the *Users* heading at the top of the page.

3. Enter the details of the new user (*Name, Job Title*, and so on).

4. After you click *Save* notice that the right panel expands to include additional information. Make sure you specify a *Password. Organizations, Communities,* and *Roles* let you specify those for the new user.

5. After clicking the *Portal > Users* item on the left, click *Actions > Manage Pages* to the right of the user to specify which pages this user will see.

6. You can also click *Action > Permissions* to configure

7. You can also specify contact information and *Instant Messenger* information. The built-in instant messaging is available to users in NMS200 in addition to such instant messaging.

8. Finally, notice the *Miscellaneous* information that specifies *Announcements* to which this user subscribes, *Display Settings* and *Comments.*

Once you have configured a user, you can click the *View All* tab and use the *Action >* menu to the right of the user listed in *Portal > Users* on the *Control Panel* page to do the following:

- **Edit**—Re-configure the selected user.

- **Permissions**—Manage the user's access to and control over various parts of the portal.

- **Manage Pages—**Configure the *Public* or *Private* pages for a user, depending on the selected tab. Possible actions here include changing the look and feel of pages (for computers and mobile browsers), adding pages and child pages, and importing or exporting page configurations. Notice that you can configure meta tags, and javascript on these pages too.

Exports are in `.lar` format, and go to the download location configured in the browser you are using. The export screen lets you select specific features, and the date range of pages to export.

> **Tip:** If you want to set up several pages already configured elsewhere for another user, or even for an entire community of users, export those pages from their origin, then *Manage Pages* from the *Action* menu for the user or community.

- **Deactivate**—Retires a user configured on your system. You can also check users and click the *Deactivate* button above the listed users.

Your organization has a number of geographic locations and you plan to manage the network infrastructure for all these locations using RC7 Synergy. You can define the geographic locations to which devices can be associated. This will help you manage and view your network, grouped by location or branches.

> **Tip:** To edit your own information as a signed-in user, simply click your login name in the upper right corner of the portal screen.

Portal > Communities

➢ **Add Communities with the following steps:**

1. Click *Manage > Control Panel* and navigate to *Portal > Communities.*
2. Click the *Add* tab under the *Communities* heading at the top of the page.
3. Enter the details of the new community (*Name, Description*).
4. By clicking *Actions* to the right of any listed Community, you can also select its membership, permissions, viewable pages and so on.

> **Tip:** To see a portlet in Expanded rather than Summary mode, click + in the upper right corner.

Discover Your Network Resources and Devices

To begin managing resources in your network, you must discover them to store their information in the application database. This begins either with the Resource Discovery Quick Navigation button or the Discovery Profiles portlet. Discovery profiles configure equipment discovery for NMS200.

The summary view displays the Name, Description, Default (the green check indicates the default profile), whether the profile is Scheduled and Next Execution Date for scheduled discovery.

> ➢ **Follow these steps to start discovering equipment on your network.**

    1. Click **Resource Discovery** in Quick Navigation or right-click the Discovery Profiles list and select **New**. (If you have previously exported profiles, you can Import them. You can also Export Selection, or Export all profiles in this manager. Open an existing profile to edit it.)

    2. After this beginning, if you clicked **Resource Discovery**, the Quick Discovery screen appears where you can enter device identifiers (typically IP Address(es)), and authentications, then execute discovery. The Quick Discovery screen can also discover the default Discovery profile if you have configured one already.

    If you clicked **New** in the Discovery portlet, the *Discovery Profile Editor* appears, with a step-by-step set of screens to configure resource discovery, as described below.

    You can navigate through the Profile Editor by clicking the screen tab names at the top, or by clicking the Next button at the bottom of the page.

Discovery Profile Editor

Use this editor to configure discovery. Baseline discovery is the initial discovery to compare to later discoveries. Follow these steps to discover equipment on your network:

    3. **General Parameters**—Set the Name, Description and whether this profile is the baseline default.

    4. **Profile Options**—Select the Device Naming Format (how the device appears in lists, once discovered), whether to Manage by IP address or hostname, and check whether to Resolve Hostnames, ICMP Ping Device(s), Manage ICMP-only Device(s), or Manage Unclassified Device(s). This last checkbox determines whether NMS200 attempts to manage devices that have no device driver installed. Management may be possible, but more limited than for devices with drivers installed, provided this capability is one you have licensed.

Network

    5. After you click **Next**, the Network screen appears.

    Network Type and Addresses—Select the type of entry in the pick list (IP Address(es), CIDR Address, Hostname, SNMP Broadcast, Subnet).

       Tip: You can specify an IP Address range by separating the beginning and end with a dash. For example: 192.168.1.1 - 192.168.1.240.

    The tooltips in the data entry field describe what valid entries look like.

    6. **Authentication**—You can create new, or add existing authentications. Notice that authentications appear with Edit / Delete icons and Up / Down arrows on their right. The Edit icon opens the authentication editor. Click the arrows to arrange the order in which credentials are tried (top first). Ordering only applies when two credentials are of the same type.

Inspect

7. **Inspect**—This screen lets you preview the discovery profile's actions and access to devices. If you clicked Next rather than Inspect at the bottom of the previous screen, click **Start Inspection** in the top right corner of this screen to begin the inspection process that validates the device's credentials.

   Notice that the Inspection Status fields at the bottom of the screen indicate the success or failure of Ping, Hostname resolution, and Authentications.

   When authentications are unsuccessful, you can click **Previous** to go to the Network screen and remove or edit them.

8. **Save**—Click **Save** to preserve the profile. You can then right-click it to select Execute and begin discovery. If you select Execute from the profile editor, NMS200 does not save the profile to execute later.

Results

9. **Execute**—Click **Execute** to begin discovery, and the message traffic between NMS200 and the device appears on the Results screen. This is a standard Audit screen.

10. A message (Discovery Profile Execute is complete) appears in the Messages at the bottom left of the status bar.

   Tip: You can also schedule discovery profiles to run periodically, updating your NMS200 database with any network changes.

11. The devices in your network now appear in the *Manage Your Network Resources and Devices* portlet, and elsewhere (in Topology, for example).

Manage Your Network Resources and Devices

The Managed Resource portlet displays all the devices you have discovered. Right-clicking a listed resource displays a menu with options.

NMS200 lets you manage device configurations. Before you begin that management, you must first configure an *FTP/TFTP Server* to get or send such configurations from / to devices. After configuring the *FTP/TFTP Server*, you can do *Configuration File Backup / Restore* described below.

FTP/TFTP Server

➢ **Follow these steps to configure a server:**

1. Click either the *Common Setup Tasks at First-time Sign-in* portal Netrestore File Servers link, or right click and select **New** in the **Configuration Management > File Management** page's the File Servers portlet.

2. After entering all required details click **Save** to save new file server.

3. Optionally click **Test** to validate the new file server.

Configuration File Backup / Restore

Provided you have permissions, you can backup configuration file(s) for a single device or group of devices, either on demand or as scheduled.

➢ **Follow these steps:**

1. In the default NMS200 screen layout, go to **Configuration Management > Summary**.
2. In the Managed Resources portlet, select (click on) a Managed Resource of interest.
3. Right-click on selected resource in the Managed Resources portlet, and then click **File Management > Restore or Backup**.
4. Enter the information needed to create the backup or restoration.
5. Optionally click **Add Schedule** to schedule the backup task.
6. Click **Execute** to immediately do backup or **Save** to save the configured backup to run later.

Create Reports

Reporting combines defined device targets with a pre-configured report template. The report definition selects the resources to query and the (reusable) template selects which of the available attributes appear in the report.

If your want to automate month-end reports NMS200 lets you schedule either recurring reports or a single scheduled occurrence. With the correct permissions, you can run Inventory Reports on demand or as scheduled. You can use the Reports to troubleshoot and monitor performance and historical data that has been collected during the operation of the network.

Most users create reports about discovered resources with the included report templates. To create a report with an existing template, open the Reports portlet and right-click a report listed there and select Execute.

➢ **Follow these steps:**

1. Click **Reports** in the portal and scroll down to find the Reports portlet.
2. Click to select a Report of interest.
3. Right-click, and then click **Execute** to run report.
4. Report generation runs in the background. When it is complete, you a message appears in the Messages tab at the bottom left corner.
5. Click **Messages** to open, then click on the Report of interest and click **View Details** at the right end of entry, to view completed report.

You can also automate report generation. If you want to have a recurring report, scheduling is the most convenient way to arrange it. Automatically generated reports are archived, and appear in the history snap panel of the expanded portlet.

Fault Management and Problem Diagnosis

NMS200 lets you diagnose network problems with its *Alarms* viewer, and lets you monitor performance with its *Performance Management and Troubleshooting* capabilities, as described below. The following briefly outlines these capabilities:

Alarms

Alerts about network performance issues can include alarms about the following:

- Excessive interface utilization
- Unexpectedly high CPU load
- Loss of available memory
- Slow response time
- Excessive interface errors

When you receive an alarm you can take any of the following action on the alarm itself, or the target of the alarm:

- Assign User
- Acknowledge Alarm
- Unacknowledge Alarm
- Clear Alarm
- Show Performance

➢ **Follow these steps to get started:**

1. Click **Alarms > Summary** from the default screens.
2. In the Alarms portlet, click on an Alarm of interest.
3. Right-click on the selected alarm, and then click **Acknowledge Alarm** to take ownership of the alarm.
4. Right-click then click **Assign User** to select a user owner for the alarm.
5. Right-click then click **Clear Alarm** to remove the alarm from list.
6. Click the plus (**+**) in the upper right corner of the Alarms portlet to go into Expanded mode where you can view more details about an alarm.

Performance Management and Troubleshooting

In addition to troubleshooting faults, you can also monitor device performance with NMS200.

Monitors

Monitors display some critical performance metrics for devices on the network, including:

- Network availability
- Bandwidth capacity utilization
- Buffer usage and errors
- CPU and memory utilization
- Interface errors and discards
- Network latency
- Node and interface status

➢ **To get started using monitors, follow these steps:**

1. Click **Performance Management > Summary**, and find the Resource Monitors portlet on that page.
2. Hover the cursor over a Monitor of interest to see a tooltip of details about it.
3. Click to select a Monitor of interest.
4. Right-click the selected monitor in the Resource Monitors portlet, and then click **Open** to edit its details, including enabling/disabling it.

Dashboard Views

With permissions, you can view the performance data collected by the monitors, in graphical and tabular form including:

- Excessive interface utilization
- Unexpectedly high CPU load
- Loss of available memory
- Slow response time
- Excessive interface errors

➢ **To view this data, follow these steps:**

1. Click **Performance Management > Summary** and find the Top Problem Nodes portlet.
2. Hover the cursor over a Device/Interface of interest to see a tooltip of details about its status.
3. Right-click and select **Show Key Metrics**, or **Show Performance**, which opens a dashboard.

Troubleshooting

This appendix presents links to the NETGEAR site for more information.

- The NMS200 Network Management Software product page is at *www.netgear.com/nms200*. Consult this page for the latest product information.

- The NMS200 Network Management Software FAQs are at *support.netgear.com/app/answers/detail/a_id/16861*. Consult this page for the latest support information.

Index