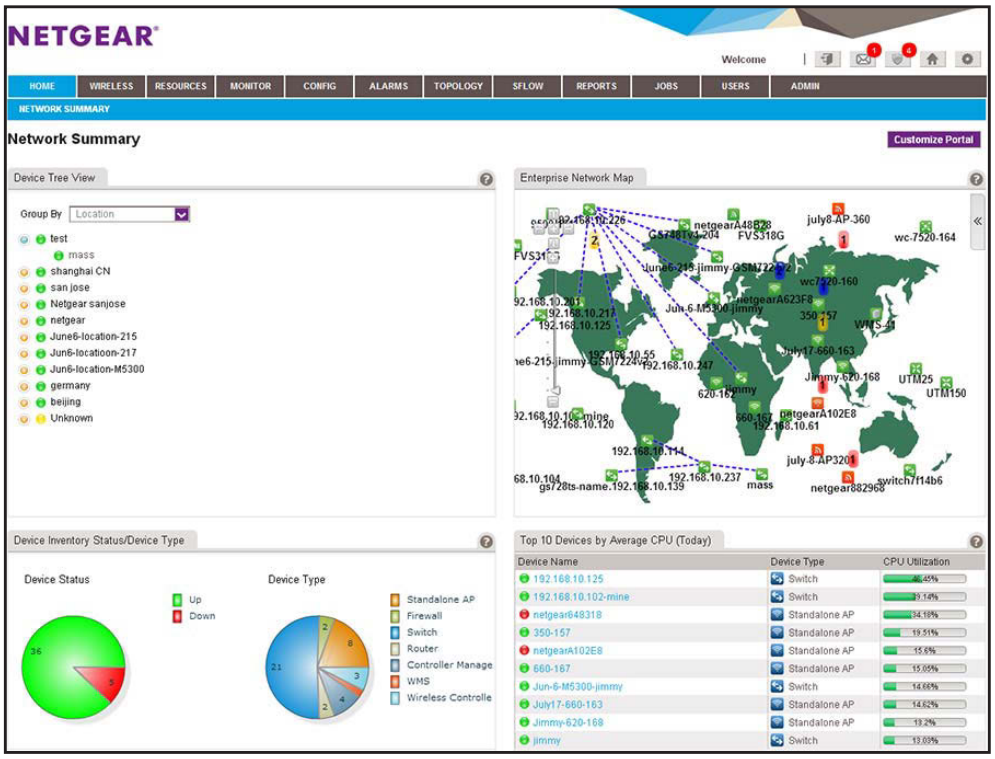
NETGEAR®

NMS300 Network Management System Application

Quick Start Guide



December 2014
202-11288-04

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product.

After installing your device, locate the serial number on the label of your product and use it to register your product at https://my.netgear.com. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website.

For product updates, additional documentation, and support, visit 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/general/contact/default.aspx.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11289-04	December 2014	• Added support for the following platforms: - M6100 managed switch, including blades and supervisors inserted in the chassis: XCM8944, XCM8944-POE+, XCM8944-uPOE, XCM8948, XCM8948-POE+, XCM8948-uPOE, XCM8944F, and XCM8924X - S3300 smart switch: S3300-28X, S3300-28X-PoE+, S3300-52X, and S3300-52X-PoE+ - FVS336Gv3 firewall - WN370 wireless access point • Added the option to display the slot list for an M6100 managed switch. (For more information, see the user manual.) • Added the option to enter an email address for notification of file backup results (see *Add a Backup Profile and Execute a Backup Job* on page 66). • Added an option to send an SMS message when an alarm is triggered (see *Configure the SMS Server for Alerts and Alarm Notifications* on page 22 and *Add an Alarm Notification Profile* on page 61). However, this option is supported for a particular SMS gateway in the People's Republic of China only. • Added sampled flow (sFlow) for managed switches. (For more information, see the user manual.) • Added support for an external file storage server on which you can store backup files. (For more information, see the user manual.) • Added the capacity to support Chinese characters for device names.
202-11289-03	January 2014	• Added support for storage systems. • Added support for additional firewalls. • Added support for additional switches and wireless devices. • Removed devices that are no longer supported (EOL).
202-11289-02	October 2013	• Revised many procedures for more clarity. • Added support for wireless devices. • Added support for firewalls.
202-11289-01	June 2013	First publication.

Contents

Chapter 5 Manage Configurations and Firmware

Install the NMS300 Application

1

Install the application and prepare your network

The NETGEAR Network Management System 300 (NMS300) is a centralized and comprehensive management application that enables you to discover, monitor, configure, and report on enterprise-class networks with NETGEAR and third-party network devices.

This *Quick Start Guide* is intended for network administrators and describes how to install the software and get up and running quickly. For a complete description of the features and capabilities of the NMS300, see the *NMS300 Network Management System Application User Manual*, which is available at *downloadcenter.netgear.com*.

This chapter covers the following topics:

- *Computer Requirements*
- *Compatible Devices*
- *Download, Install, and Run the Application*
- *Prepare the Network Devices for Discovery*

Note: In this guide, the NMS300 application is referred to as the application. The server on which the application is installed is referred to as the NMS300 server.

For more information about the topics covered in this manual, visit the support website at *support.netgear.com*.

For more information about this NMS300 release, see the *NMS300 Release Notes*, which are available on *downloadcenter.netgear.com*.

Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Computer Requirements

For this release of the application, the computer that functions as the NMS300 server must meet the following requirements:

- 2.8 GHz dual-core CPU
- 4 G RAM (32-bit OS) or 8 G RAM (64-bit OS)
- 20 G storage
- Static IP address

This release of the application supports the following operating systems:

- Microsoft Windows XP (Professional) 32-bit and 64-bit with SP3 or later
- Windows Server 2003 (Standard, Enterprise, and Web), 32-bit and 64-bit
- Windows Server 2008 (Enterprise), 32-bit and 64-bit
- Microsoft Windows 7 (Professional, Enterprise, and Ultimate), 32-bit and 64-bit
- Microsoft Windows 8 (Enterprise), 64-bit
- Microsoft Windows Server 2012 (Standard), 64-bit

This release of the application supports the following browsers:

- Internet Explorer 9 or 10
- Firefox 20.0.1 or a later version
- Chrome 26.0.1410.64 m or a later version

Compatible Devices

This release of the application supports the following features:

- Support for NETGEAR managed and smart switches
- Support for NETGEAR wireless devices
- Support for NETGEAR firewalls
- Support for ReadyNAS and ReadyDATA storage devices
- Support for discovery and node status monitoring of third-party devices

Products that reached their end of life (EOL) are not included in the following lists.

NETGEAR Managed Switches

This release supports the following NETGEAR managed switches:

- GSM5212P
- GSM7212F
- GSM7212P
- GSM7224P
- JGSM7224
- M4100-12G-POE+
- M4100-12GF
- M4100-24G-POE+
- M4100-26-POE+
- M4100-26G
- M4100-26G-POE
- M4100-50-POE
- M4100-50G
- M4100-50G-POE+
- M4100-D10-POE
- M4100-D12G
- M4100-D12G-POE+
- M5300-28G
- M5300-28G-POE+
- M5300-28G3
- M5300-28GF
- M5300-52G
- M5300-52G-POE+
- M5300-52G3
- M6100, including blades and supervisors inserted in chassis:
  - XCM8944
  - XCM8944-POE+
  - XCM8944-uPOE
  - XCM8948
  - XCM8948-POE+
  - XCM8948-uPOE
  - XCM8944F
  - XCM8924X
- M7100 XSM7224
- M7100 XSM7224S

NETGEAR Smart Switches

This release supports the following NETGEAR smart switches:

- FS526Tv2
- FS726Tv2
- FS728TLP
- FS728TPv2
- FS728TP-200
- GS108T-200
- GS110TP
- GS510TP
- GS516TP
- GS724T-400
- GS716T-300
- GS748T-500
- GS728TP
- GS728TPP
- GS728TPS
- GS728TS
- GS728TXS
- GS748T-400
- GS752TP
- GS752TPS
- GS752TS
- GS752TXS
- S3300-28X
- S3300-28X-PoE+
- S3300-52X
- S3300-52X-PoE+
- XS712T

NETGEAR Firewalls

This release supports the following NETGEAR firewalls:

- FVS318G
- FVS318N
- FVS336Gv2
- FVS336Gv3
- SRX5308

NETGEAR Wireless Access Points

This release supports the following NETGEAR wireless access points:

- WG103
- WN203
- WN203-200
- WN370
- WNAP210
- WNAP320
- WNAP370
- WNDAP350
- WNDAP360
- WNDAP380R
- WNDAP380Rv2
- WNDAP620
- WNDAP660

NETGEAR Wireless Management Systems and Controllers

This release supports the following NETGEAR wireless management systems and wireless controllers:

- WMS5316
- WC7520
- WC7600
- WC9500

NETGEAR Storage Systems

This release supports the following NETGEAR ReadyNAS and ReadyDATA storage systems:

- RN2120
- RN312
- RN314
- RN316
- RN3220
- RN4220
- RN516
- RDD516
- RD5200

Download, Install, and Run the Application

The application must reside on a server at a static IP address on the local area network.

➢ **To download, install, and run the application:**

1. Review the supported Windows computer operating systems (see *Computer Requirements* on page 6).
2. Visit *downloadcenter.netgear.com* and download the application zip file that corresponds to your Windows computer operating system.
3. Make sure that the Windows computer on which you intend to install the application is assigned a static IP address.

   The application binds itself to the static IP address of the host computer, which is the NMS300 server.
4. Unzip the file you downloaded to obtain the executable installer file.
5. Launch the installer wizard by double-clicking the executable file.
6. Follow the installer wizard prompts.

   The installer wizard guides you through the default settings and allows you to customize them.

   - If another application is already using port number 8080 on the Windows computer, modify this default setting to a different port number.
   - Other settings can be customized as well.
   - If your Windows computer includes multiple network interface cards (NICs), select the appropriate NIC in the NIC selection screen of the wizard.

   Once the installer finishes executing, you are prompted to reboot the computer.

7. Reboot your computer.

   NETGEAR recommends that you reboot your computer.

   After the reboot, for Windows 7 and Windows XP operating systems, the application is already running as a service.

8. For Windows 2008 and Windows 2003 operating systems, use either of the following methods to start the application manually.
   - Select **NMS300 > Service > Start Server**.
   - Navigate to the directory that you selected for the application installation and under that directory, navigate to the NMS300\StartService.bat folder.

   You do not need to enter a license key for the application.

Prepare the Network Devices for Discovery

To manage the devices on your network, you must prepare them for the application. By default, the application lets you manage up to 200 devices. For information about managing more than 200 devices, contact your NETGEAR sales contact.

➢ **To prepare the devices on your network:**

1. Upgrade your devices to their latest released firmware.

   To upgrade the firmware, use the web management interface of the device.

   Each device must run the latest firmware before the application can discover and manage the device. Once you perform this one-time upgrade, the application can centrally manage future device firmware upgrades.

2. Create the credentials for your devices.

   The application uses a combination of SNMP, HTTP, and Telnet protocols to interact with the devices on your network. You must configure the application with the device credentials to authenticate with the devices over the following protocols:

   - **Telnet and HTTP protocols**. If the devices are not configured with the default password for the admin user, create two new credentials in the application.

     Create one credential for the Telnet protocol and another credential for the HTTP protocol that contain either the admin user credential or the credential of another user of the device with administrative privileges.

   - **SNMP community strings**. If the devices are not configured with the default SNMP community strings, create a credential in the application for the SNMP protocol that contains the matching community strings.

   For more information, see *Add a Device Credential* on page 30.

3. Make sure that each device on your network is configured to send SNMPv1 or SNMPv2 traps to the IP address of the NMS300 server.

   The application listens for SNMPv1 and SNMPv2 traps.

2 Get Started

Log in and perform basic configuration tasks

After you logged in to the application, you can change your password and account information and configure the email server.

This chapter covers the following topics:

- *Log In to the Application*
- *Change Your Password and Account Information*
- *Add a User Profile to the User Base*
- *Configure the Email Server for Alerts and Alarm Notifications*
- *Configure the SMS Server for Alerts and Alarm Notifications*

Log In to the Application

The application uses a browser server architecture. Administrators and other types of users can access the application from any supported browser. Before you log in to the application, check the following items:

- Make sure that the application is installed on a server with a static IP address.
- Clear your browser cache before you use the application.

CAUTION:

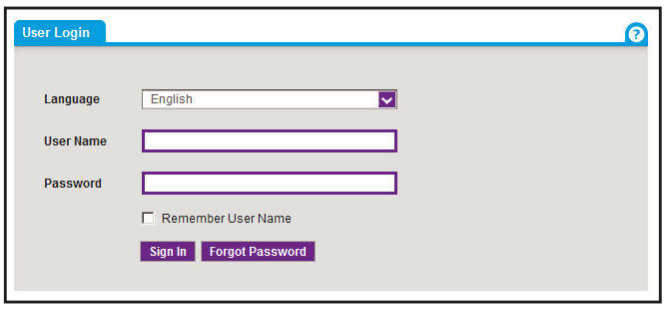
The application supports multiple concurrent users. NETGEAR recommends that different user coordinate their application activities so that modifications to a screen made by one user are not inadvertently changed by another user.

➢ **To select your language and log in to the application:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.
   - To connect to the application from the same NMS300 server on which you installed the application, enter the URL **http://localhost:8080**.

     If you entered a different port number for the NMS300 server during the application installation, replace *8080* in this URL with the port number that you provided during installation.
   - To connect to the application from a remote computer, replace *localhost* with the IP address of the NMS300 server. For example, enter **http://203.0.113.56:8080**, in which 203.0.113.56 is the IP address of the NMS300 server and 8080 is the port number for the NMS300 server.

   After you connect to the application, the User Login screen displays.



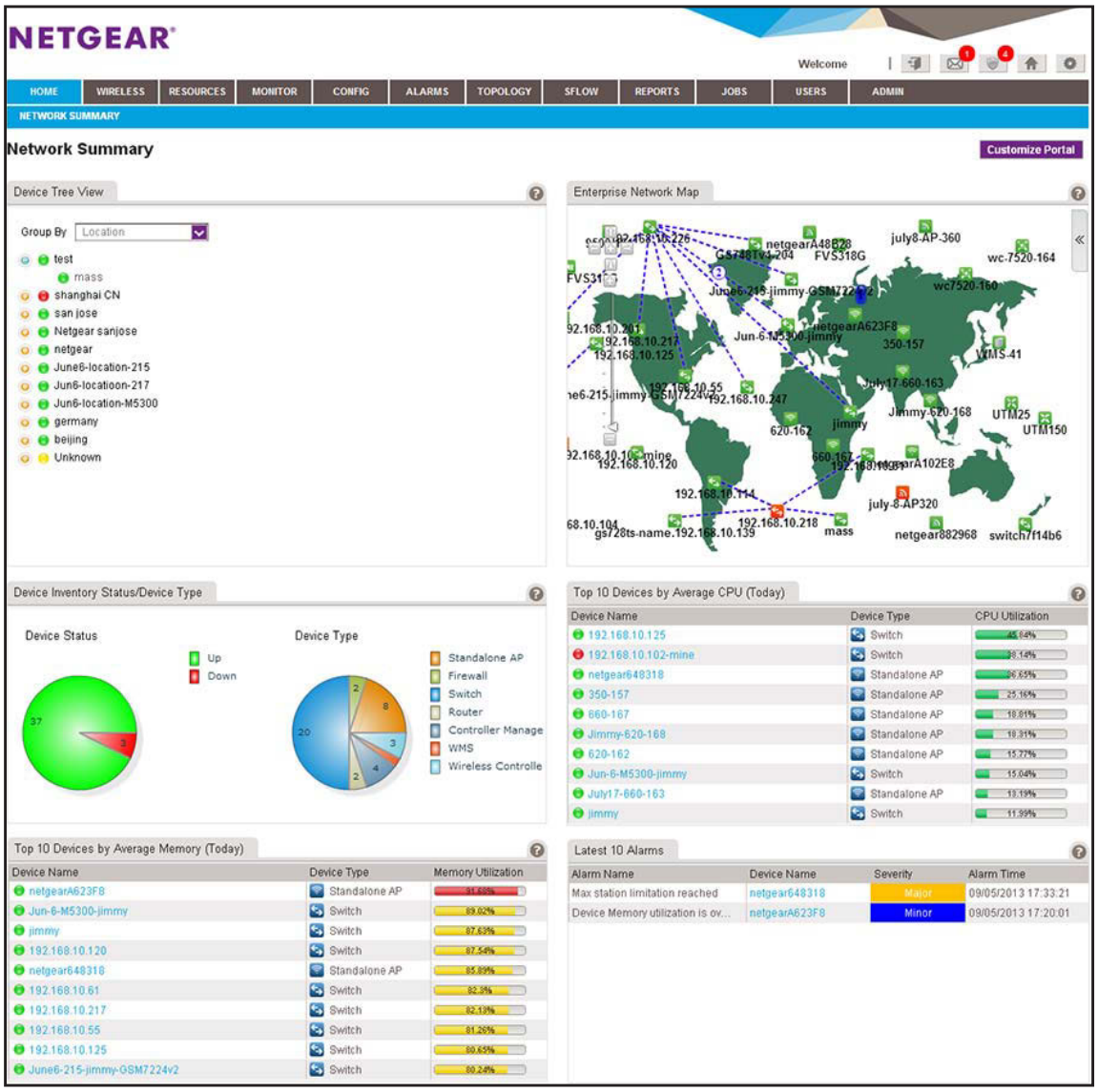
2. From the **Language** menu, select your language.

   The default language is English. You can also select Chinese.
3. Enter your user name and password.

   When the application is initially installed, the default administrator user name is **admin** and the default administrator password is also **admin**.

You must be an administrator (admin user, that is, a user with a security profile that is set to Admin) to be able to create user names and passwords for other types of users.

4. Click the **Sign In** button.



For more information about the Network Summary screen, see *View the Default Network Summary* on page 54.

Change Your Password and Account Information

NETGEAR recommends that you change your password to a more secure password. This recommendation applies to admin users only because nonadministrative users such as users with a security profile set to Operator or Observer cannot change their password.

As an admin user, you can also change your account information. Items that you can change include your email address, real name, and telephone number. You cannot change your user name but you can add a second admin account with a different user name. For more information, see the *NMS300 Network Management System Application User Manual*.

Change Your Password

When the application is initially installed, the default administrator user name is admin and the default administrator password is admin. As an admin user, you can create user names and passwords for other types of users.

➢ **To change your password:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

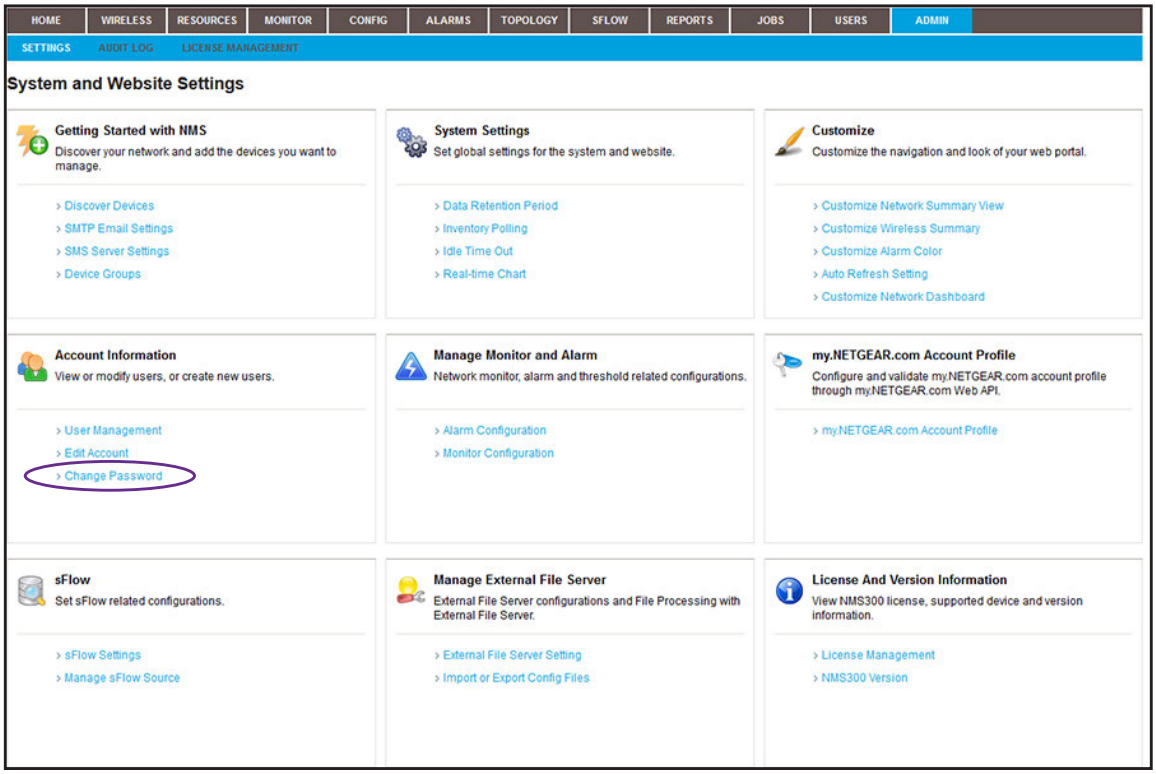
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

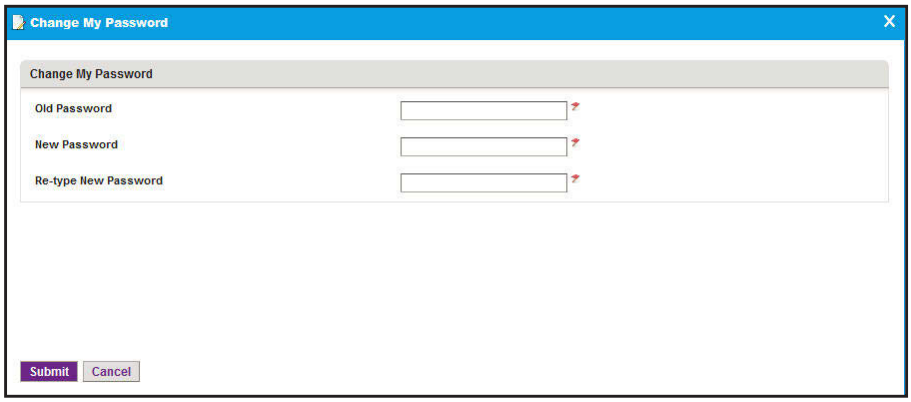
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under Account Information, click the **Change Password** link.



6. Enter your old and new passwords
7. Click the **Submit** button.

   Your password is updated.

Change Your Account Information

You can change your general account settings such as your email address and telephone number.

➢ **To change your account information:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

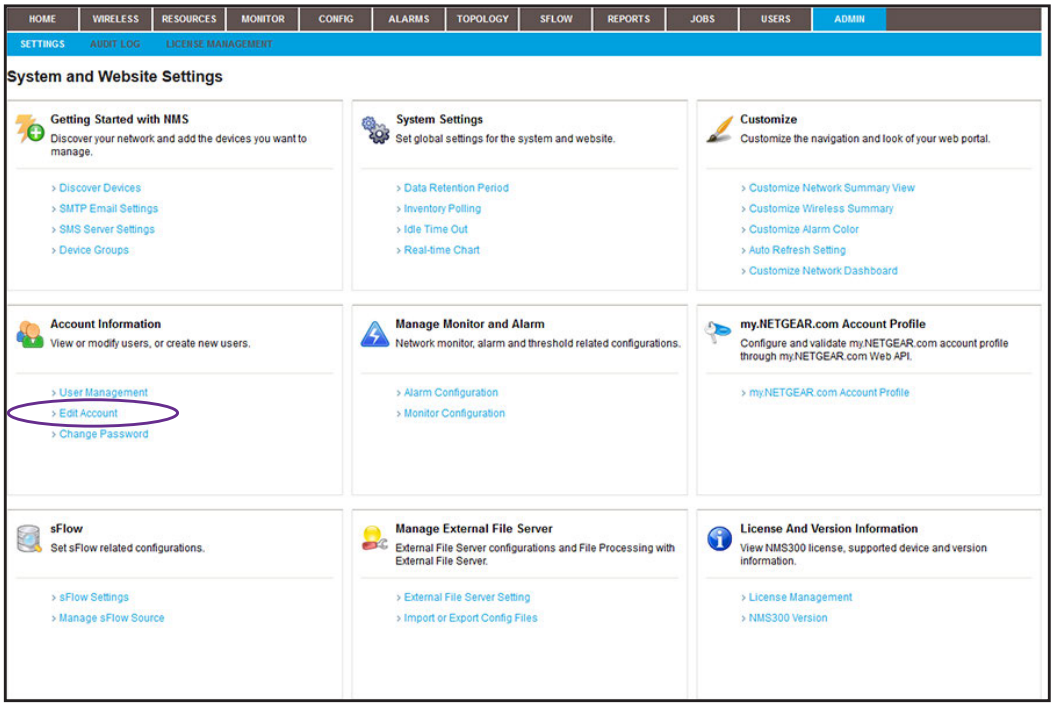
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

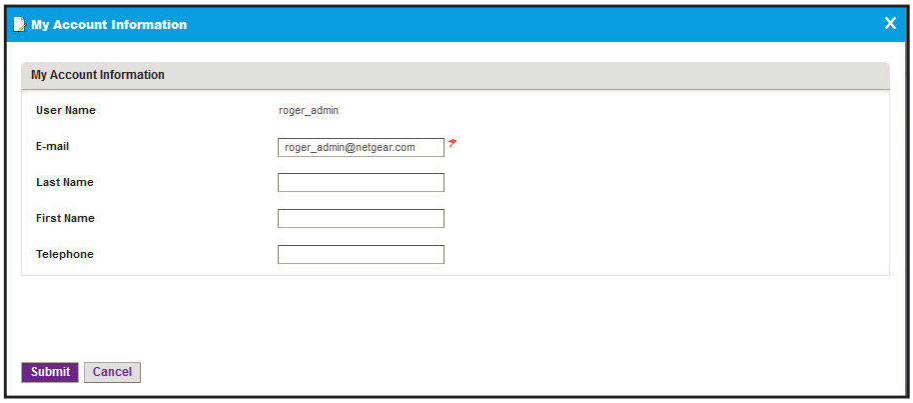
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under Account Information, click the **Edit Account** link.



6. Modify the information as needed.
7. Click the **Submit** button.

   Your account information is updated.

Add a User Profile to the User Base

The application provides the following default user security profiles:

- **Admin**. A user who can perform *all* functions of the application, including management of users and security profiles.
- **Operator**. A user who can manage the network functions, but cannot manage users or security profiles, or perform administrative tasks.
- **Observer**. A user who can only monitor and view network functions.

As an admin user, you can modify and delete these security profiles and you can define new security profiles. For example, you can add a security profile for someone who can only run and view network reports but is not authorized to perform any other tasks. For more information, see the *NMS300 Network Management System Application User Manual*.

➢ **To add a user profile:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

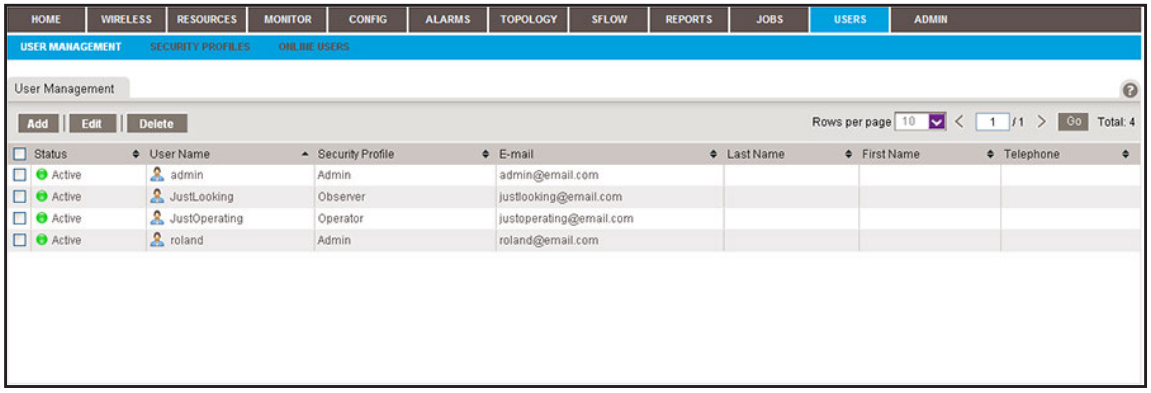
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

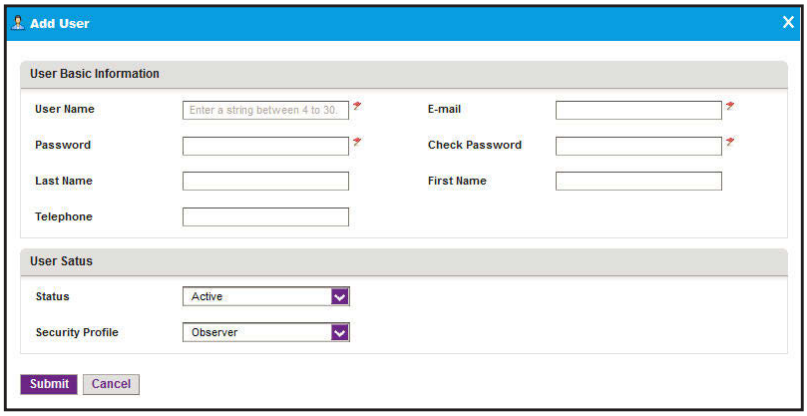
4. Select **USERS > USER MANAGEMENT**.



   The Status column displays whether the user is active and the user can log in.

5. Click the **Add** button.

The Add User screen displays.



6. Specify the following information:
   - In the User Basic Information section, enter the user name, password, and email address for the user. The first and last name and telephone number are optional.
   - In the User Status section, select whether the user profile is active and select the security profile that applies to the user.
7. Click the **Submit** button.

   The screen closes and the new user is added to the User Management table.

Configure the Email Server for Alerts and Alarm Notifications

Before the application can send email updates and alarm notifications, you must configure the email server settings. Only an admin user can configure the email server settings.

Note: For information about adding an alarm notification profile with an email address to which the application can send a notification, see *Add an Alarm Notification Profile* on page 61.

Configure the General Email Server Settings

The following procedure describes how to configure the general email server settings.

➢ **To configure the email server:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

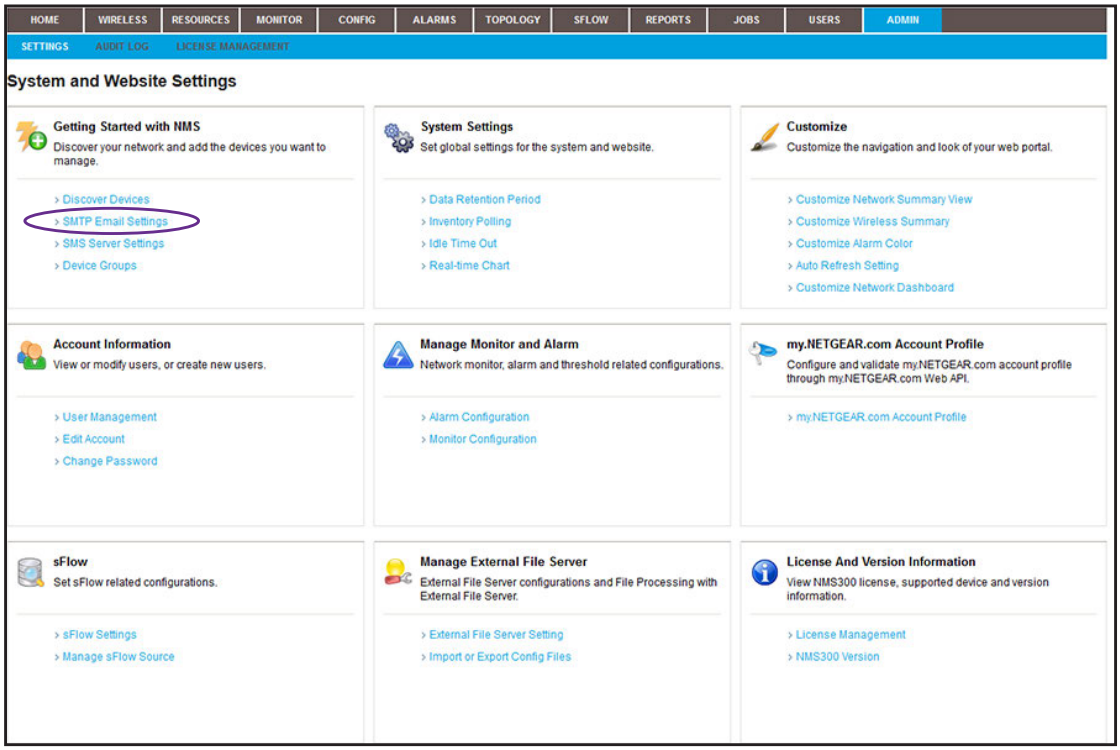
   For more information, see *Log In to the Application* on page 13.
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

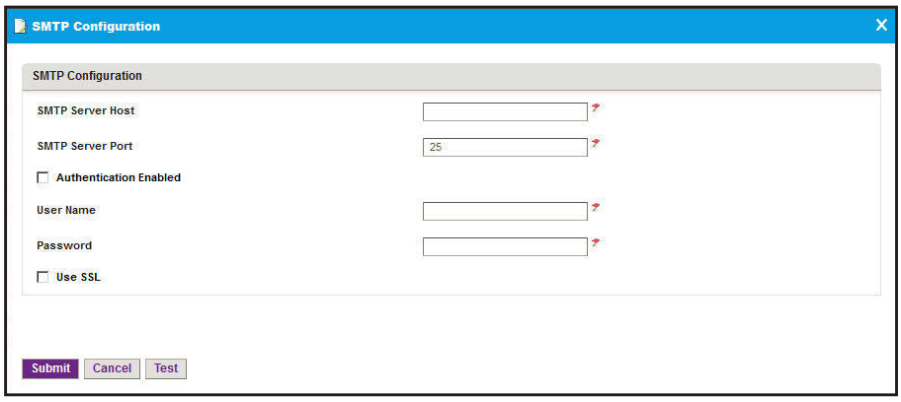
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under Getting Started with NMS, click the **SMTP Email Settings** link.



6. Enter your SMTP configuration settings.
7. If your SMTP server requires authentication, select the **Authentication Enabled** check box.
8. In the **User Name** field, enter the user name for your email account.

   Note: You must enter the email user name entirely, that is with the at sign (@) and domain name. For example, username@domain.com. The SMTP server also uses the entire user name as the address from which email is sent.

9. In the **Password** field, enter the password for your email account.
10. To use a secure email connection, select the **Use SSL** check box, and in the **SMTP Server Port** field, enter the port number for the SSL connection.
11. Click the **Test** button.

    Your SMTP configuration settings are verified.
12. Click the **Submit** button.

    Your changes are saved.

Configure Email Server Settings for a Gmail Account

The following procedure describes how to configure the email server for a Gmail account.

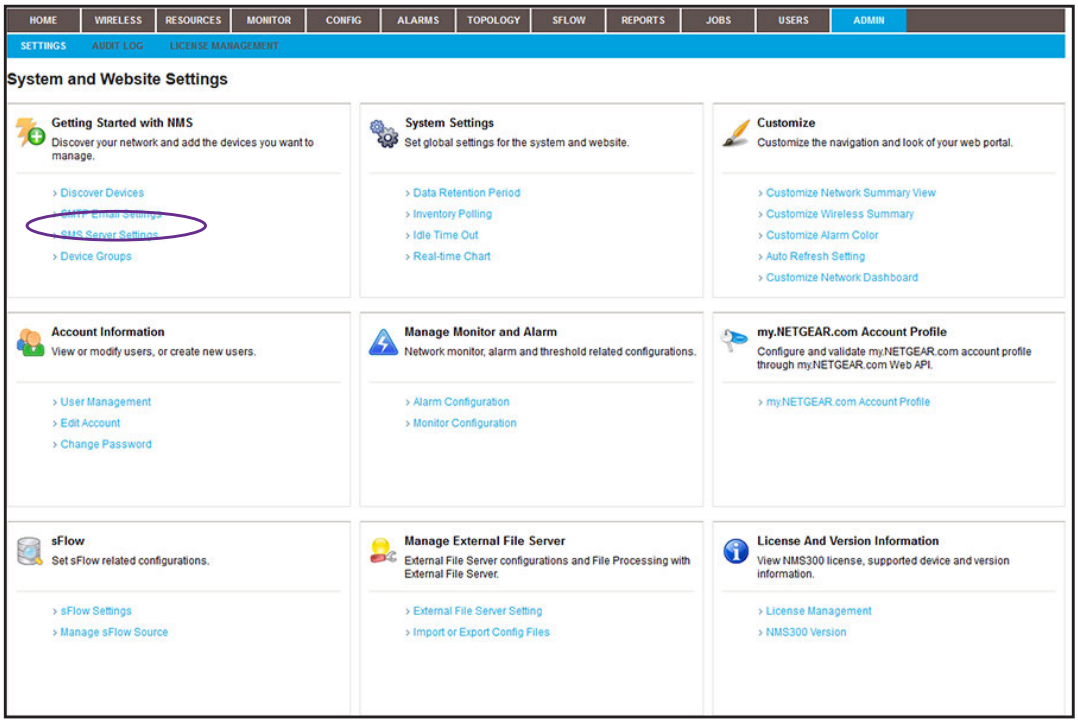
➢ **To configure the email server for a Gmail account:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

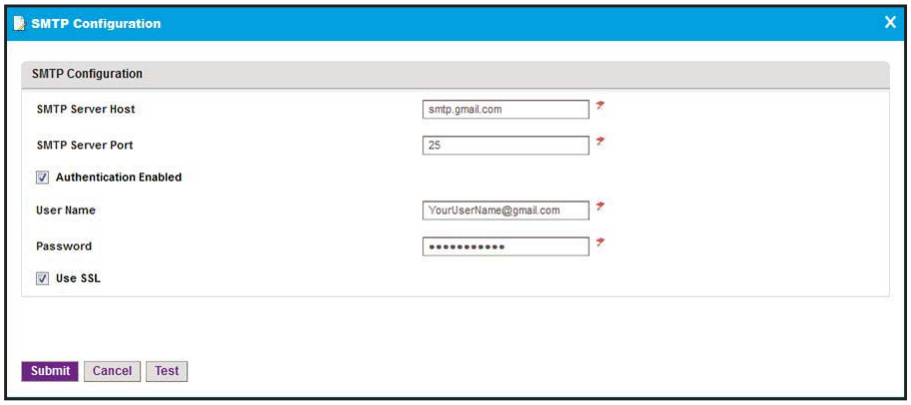
   For more information, see *Log In to the Application* on page 13.
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.
3. Click the **Sign In** button.

   The Network Summary screen displays.
4. Select **ADMIN > SETTINGS**.



5. Under Getting Started with NMS, click the **SMTP Email Settings** link.



6. Enter the following settings and select the following check boxes:
   - In the **SMTP Server Host** field, enter **smtp.gmail.com**.
   - In the **SMTP Server Port** field, enter **25**.
   - Select the **Authentication Enabled** check box.
   - In the **User Name** field, enter the user name for your Gmail account.

   Note: You must enter the email user name entirely, that is with the at sign (@) and domain name. For example, username@gmail.com. The SMTP server also uses the entire user name as the address from which email is sent.

   - In the **Password** field, enter the password for your Gmail account.
7. To use a secure email connection, select the **Use SSL** check box, and in the **SMTP Server Port** field, enter **465**.
8. Click the **Test** button.

   Your SMTP configuration settings are verified.
9. Click the **Submit** button.

   Your changes are saved.

Configure the SMS Server for Alerts and Alarm Notifications

Note: The SMS server option is supported for a particular SMS gateway in the People's Republic of China only. No other SMS servers are supported in this release.

Before the application can send SMS updates and alarm notifications, you must configure the SMS server settings. Only an admin user can configure the SMS server settings.

For information about adding an alarm notification profile with an SMS telephone number to which the application can send a notification, see *Add an Alarm Notification Profile* on page 61.

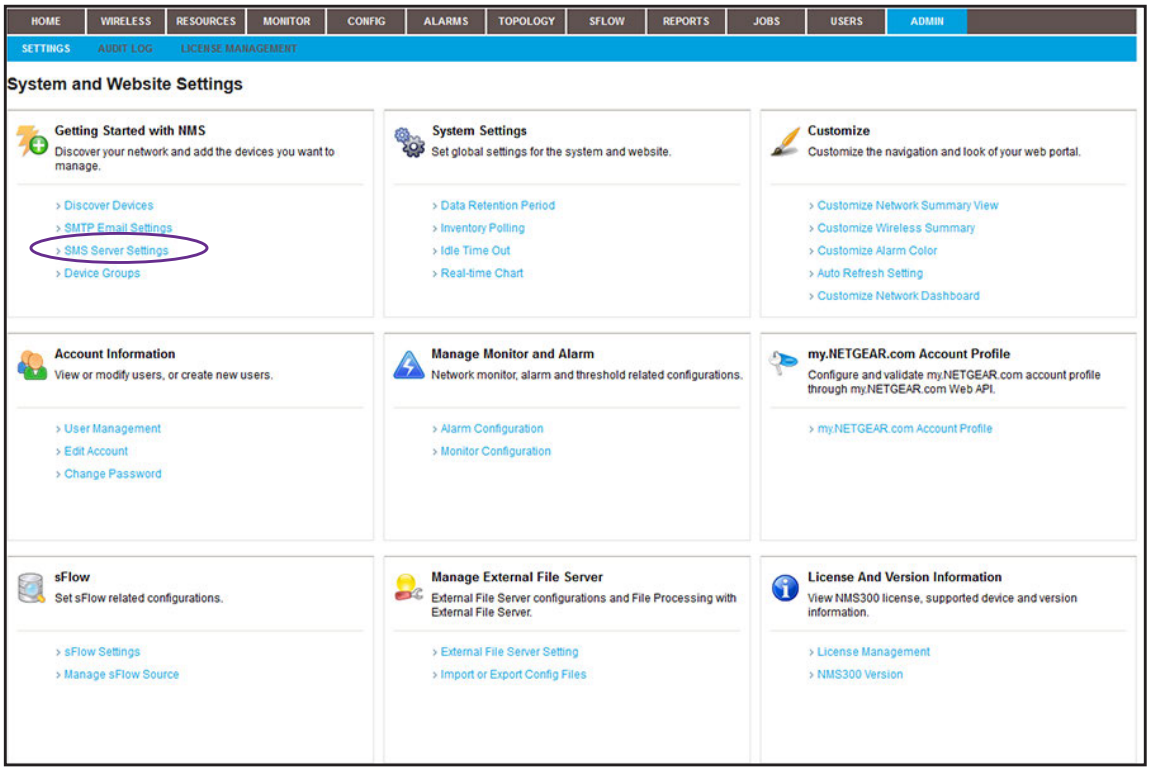
➢ **To configure the SMS server:**

1. Contact NETGEAR support to obtain the corporation ID and password for the Chinese SMS server that is supported.
2. Open a browser and connect to the application through the static IP address of the NMS300 server.

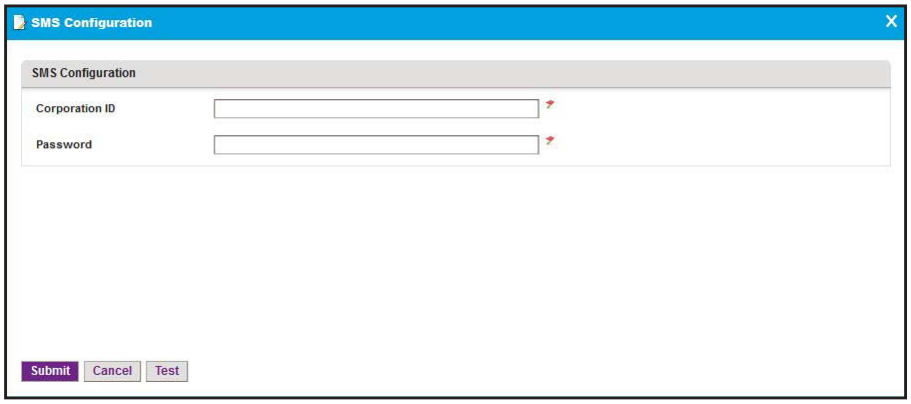
   For more information, see *Log In to the Application* on page 13.
3. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.
4. Click the **Sign In** button.

   The Network Summary screen displays.
5. Select **ADMIN > SETTINGS**.



6. Under Getting Started with NMS, click the **SMS Server Settings** link.



7. Enter the corporation ID.

   The corporation ID specifies the SMS gateways that the application must use. This is the corporation ID that NETGEAR support gave you.

8. Enter the password for accessing the SMS gateway.

   This is the password that NETGEAR support gave you.

9. Click the **Test** button.

   Your SMS configuration settings are verified.

10. Click the **Submit** button.

    Your changes are saved.

Discover Resources

3

Discover your devices and add device groups

Before you can manage your network, you must let the application find the devices that are on your network and perform other setup tasks that could simplify the management of your network.

This chapter covers the following topics:

- *Discovery Concepts*
- *Use Quick Discovery to Discover Devices on Your Network*
- *Use a Discovery Profile to Discover Devices on Your Network*
- *Add Device Groups*

Note: For more information about the topics that are described in this chapter, see the *NMS300 Network Management System Application User Manual*.

Discovery Concepts

You can discover devices on your network by using the following methods:

- **Quick discovery**. Discovers devices without using a discovery profile. This method is a quick and easy discovery method but gives you limited control over the discovery process.
- **Regular discovery**. Filters the devices on your network through a discovery profile that you must configure first. This method gives you more control than the quick discovery method but is a bit more complicated.

With both methods, the application can discover wired devices, wireless devices, NETGEAR devices, and third-party devices that support standard SNMP MIBs.

The application can discover and monitor NETGEAR firewalls over the WAN. Firewalls can use a static WAN IP address, dynamic WAN IP address, or WAN host name. If a firewall uses a WAN host name, the firewall must also use DNS.

Note: By default, the application lets you discover up to 200 devices. For information about discovering more than 200 devices, contact your NETGEAR sales contact.

For wireless access points (APs), the nature of the AP determines whether the application can discover the AP:

- **Standalone AP**. An AP that is not controlled by another device and that operates in standalone mode. This type of AP is also referred to as a Fat AP. The application can discover and manage standalone APs just like any other network device that the application supports.
- **Controller-managed AP**. An AP that a NETGEAR WC7520 or WC9500 wireless controller manages. This type of AP is also referred to as a Fit AP. After the application discovers a wireless controller, it displays the controller-managed APs in the device table. In this indirect way, the application can discover the controller-managed APs but cannot manage them. You cannot back up or restore the configuration, upgrade the firmware, or delete the access points from the application. Controller-managed APs are not subtracted from the number of devices that the license of the application supports. The license of the application ignores the controller-managed APs.

Use Quick Discovery to Discover Devices on Your Network

Quick Discovery is a quick and easy discovery method but gives you limited control over the discovery process.

➢ **To discover the devices on your network:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

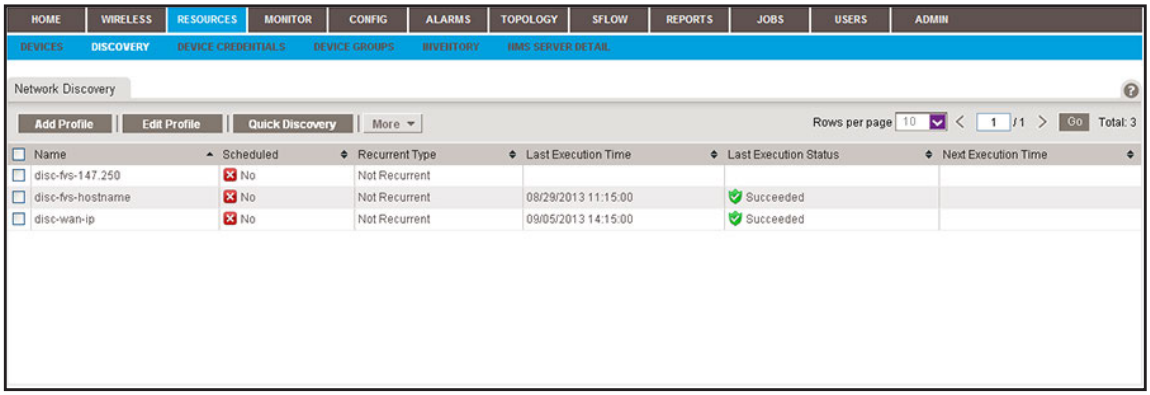
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

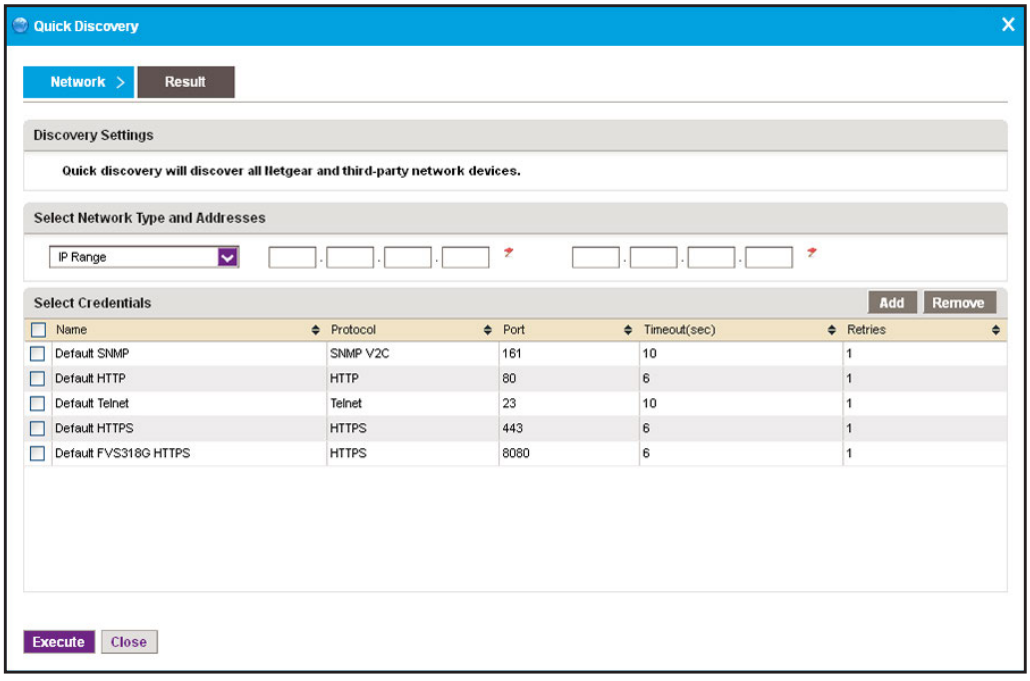
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **RESOURCES > DISCOVERY**.



5. Click the **Quick Discovery** button.



6. From the menu on the upper left of the screen, select one of the following network types and enter the applicable address information in the fields to the right of the menu:
   - **IP Range**
   - **Subnet**
   - **Single IP**
   - **IP Address(es)**
   - **Hostname**
7. Specify the credentials that pertain to the devices on your network by select one of the following types of credentials:
   - **Default SNMP**
   - **Default HTTP**
   - **Default Telnet**
   - **Default HTTPS**
   - **Default FVS318G HTTPS**

   Note: For the NETGEAR FVS318N, FVS336Gv2, FVS336Gv3, and SRX5308 firewalls, use the default SNMP device credentials. For the NETGEAR FVS318G firewall, use the default FVS381G HTTPS device credential.

8. If the credential that you need is not listed in the table, do the following:
   a. Click the **Add** button.

      The Select Credentials screen displays. In addition to the default credentials, the screen displays the device credentials that you added. For more information, see *Add a Device Credential* on page 30.

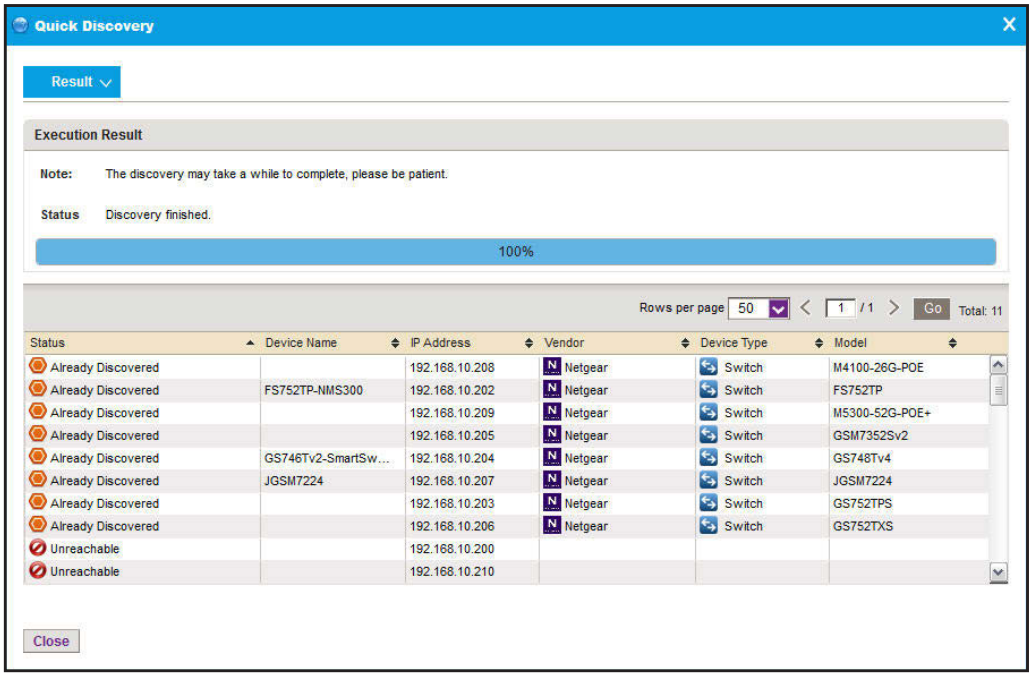
   b. Select one or more credentials and click the **Add Selection** button.

      To add all credentials, click the **Add All** button.

      The Select Credentials screen closes and the selected credentials are added to the credentials table.

   c. Select the credential or credentials that you added.
9. Click the **Execute** button.

When the quick discovery process completes, the Quick Discovery screen displays the results.



Note: If a credential failure occurs, a common reason is that the device login information changed from its default. When a credential failure occurs, add or modify the credential and run the discovery job again. For more information, see *Add a Device Credential* on page 30.

10. Click the **Close** button.

    The Quick Discovery screen closes.

Use a Discovery Profile to Discover Devices on Your Network

A discovery profile gives you more control over the discovery process than the quick discovery method but is a bit more complicated. The following sections describe how you can use a discovery profile to discover devices:

1. *Add a Device Credential*
2. *Add a Discovery Profile*
3. *Execute a Discovery Job*

Add a Device Credential

During the discovery process, the application must log in to devices to obtain the information to discover and manage the devices. A device credential includes the user name, password, and SNMP community string that allows the application to log in to the device. The user name and password are the same user information that you use to log in to the device to perform system configuration. The application provides default device credentials for discovery over HTTP, HTTPS, SNMP, and Telnet, and for discovery of the NETGEAR FVS318G firewall over HTTPS.

You must configure the correct device credentials for any device that you want the application to manage. If a device is not configured with its default credentials, do the following:

- If a device is not configured with its default admin user password, create two new credentials in the application, one for Telnet and another for the HTTP protocol. These credentials contain either the admin user credential or the credential of another user with administrative privileges.
- If a device is not configured with its default SNMP community strings, create a credential in the application for the SNMP protocol that contains the matching community strings.

➢ **To add a device credential:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

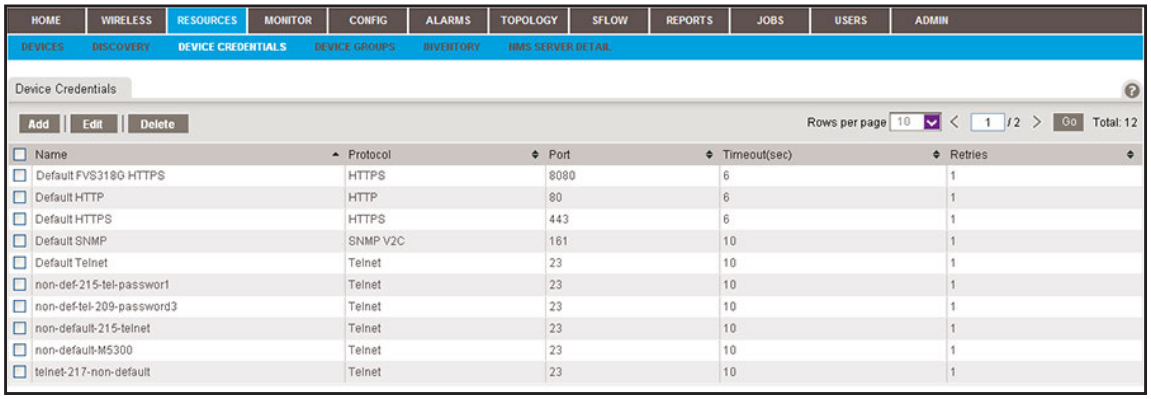
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

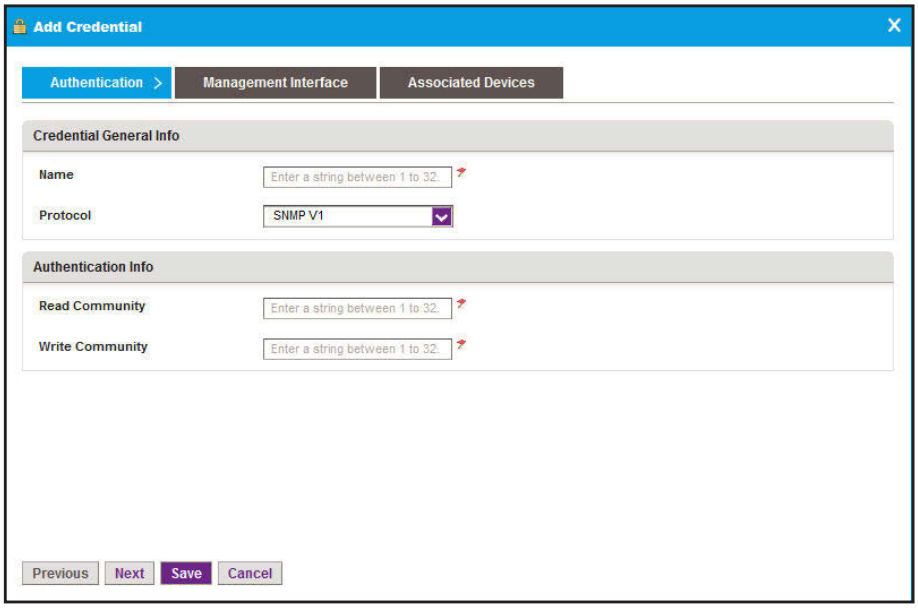
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **RESOURCES > DEVICE CREDENTIALS**.



5. Click the **Add** button.

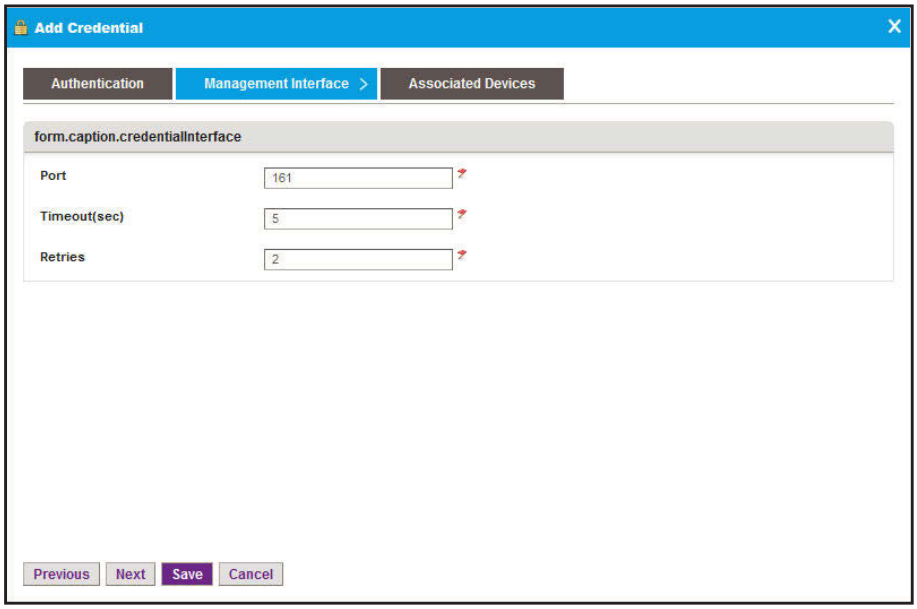


6. In the Credential General Info section, enter the name for the credential.
7. From the **Protocol** menu, select one of the following protocols:
   - **SNMP V1**
   - **SNMP V2C**
   - **SNMP V3**
   - **Telnet**
   - **SSH**
   - **HTTP**
   - **HTTPS**

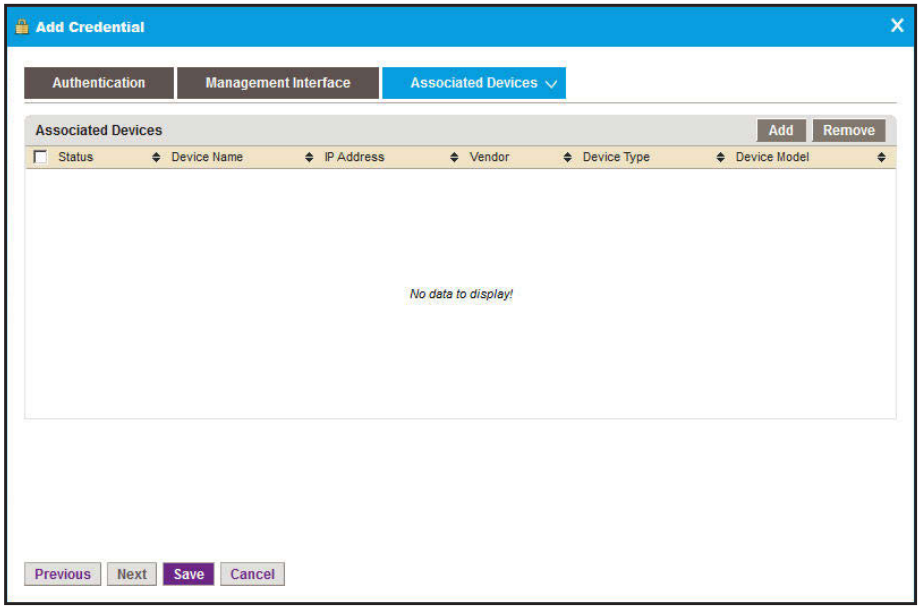
   Depending on your protocol selection, the screen might adjust to display other fields and menus.
8. In the Authentication Info section, enter the information for the selected protocol.

Note: If you are setting up a Telnet device credential for a managed switch for which the privileged EXEC password was changed (on the Enable Password Configuration screen of the switch web management interface), enter the privileged EXEC password in the **Enable Password** field. The **Enable Password** field displays when you select **Telnet** from the **Protocol** menu.

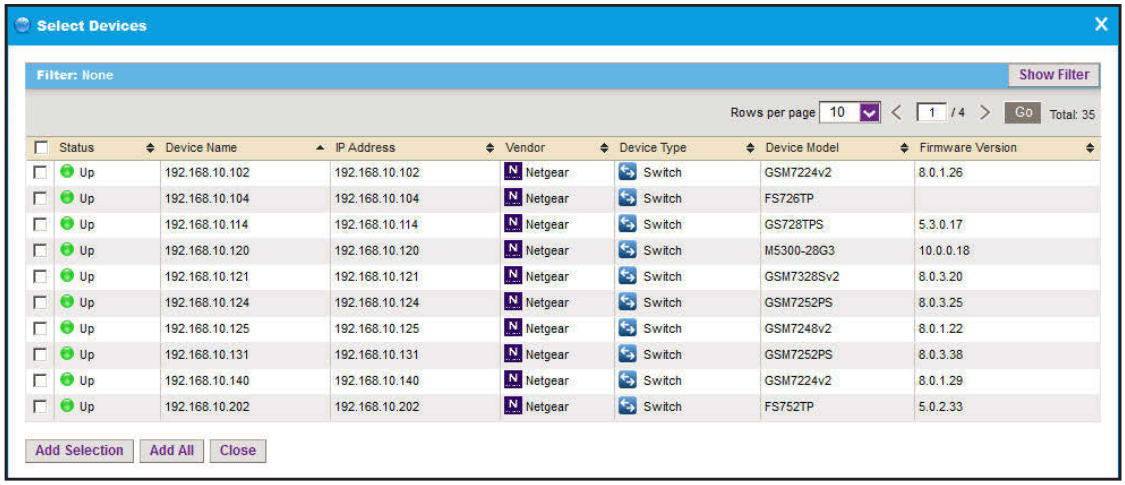
9. Click the **Management Interface** tab.



10. Enter the port number, time-out period in seconds, and the number of retries.
11. Click the **Associated Devices** tab.



12. Click the **Add** button.



13. Select one or more devices and click the **Add Selection** button.

    To add all devices to the device credential, click the **Add All** button.

    The Select Devices screen closes and the selected devices are added to the Associated Devices table.

14. Click the **Save** button.

    The screen closes and the new or modified device credential displays in the Device Credentials table.

Add a Discovery Profile

A discovery profile filters the network device information that the application can detect. The application can discover devices through an IP address range, IP subnet address, a single IP address, a list of IP addresses, or device host name.

➢ **To add a discovery profile:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

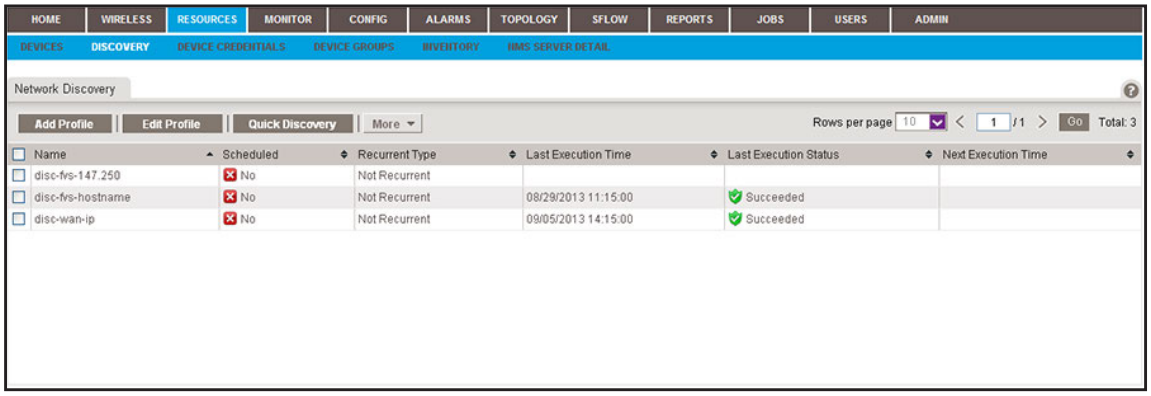
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

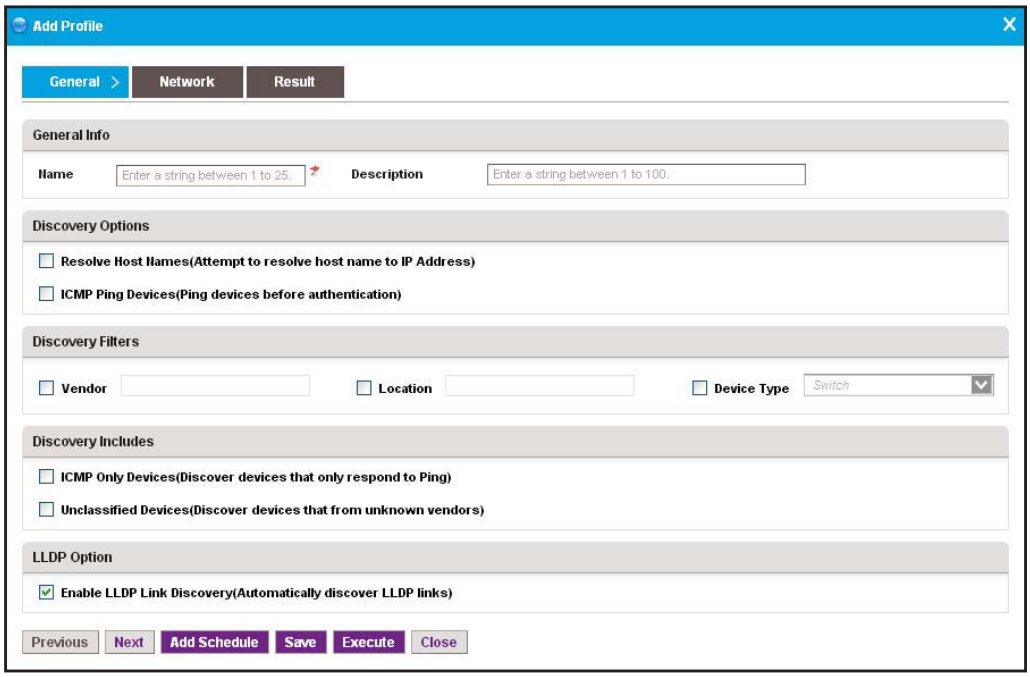
   The Network Summary screen displays.

4. Select **RESOURCES > DISCOVERY**.



The screen displays the existing discovery profiles.

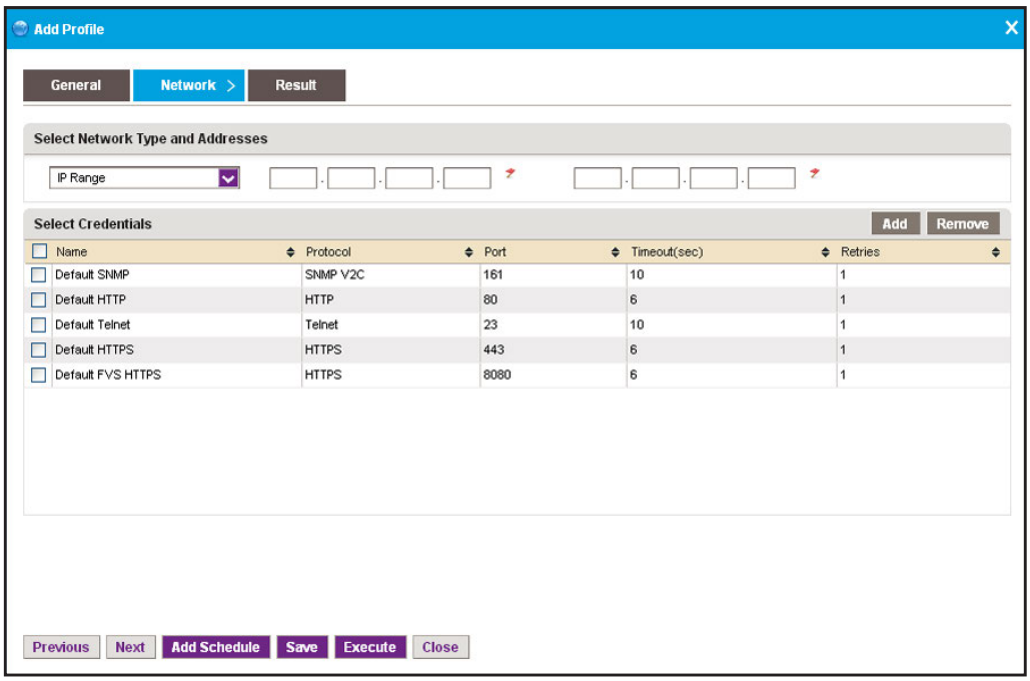
5. Click the **Add Profile** button.



6. Enter the information in the following sections:
   - **General Info**. Enter the name and description of the profile.
   - **Discovery Options**:
     - **Resolve Host Names**. To attempt to resolve a host name to an IP address, select the **Resolve Host Names (Attempt to resolve host name to IP address)** check box.
     - **ICMP Ping Devices**. To monitor the node status of third-party non-SNMP devices, select the **ICMP Ping Devices (Ping devices before authentication)** check box.
   - **Discovery Filters**. Select the discovery filters you want by vendor, location, and device type.

- **Discovery Includes**. Select whether to include ICMP-only devices or unclassified devices.
- **LLDP Option**. To monitor the node status of third-party non-SNMP devices, select the **Enable LLDP Link Discovery (Automatically discover LLDP links)** check box.

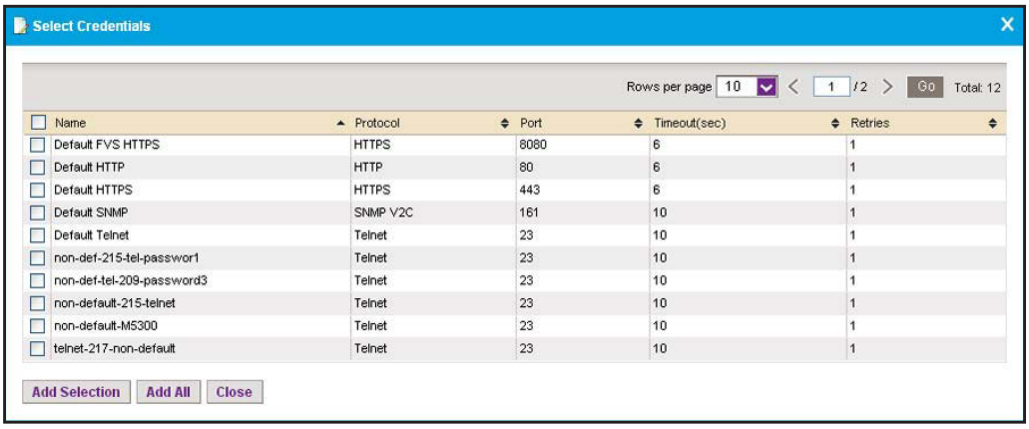
7. Click the **Network** tab.



8. From the menu on the upper left of the screen, select one of the following network types and enter the applicable address information in the fields to the right of the menu:
   - **IP Range**
   - **Subnet**
   - **Single IP**
   - **IP Address(es)**
   - **Hostname**
9. Specify the credentials that pertain to the devices on your network by selecting one of the following types of credentials:
   - **Default SNMP**
   - **Default HTTP**
   - **Default Telnet**
   - **Default HTTPS**
   - **Default FVS318G HTTPS**

10. If the credential that you need is not listed in the table, do the following:

    a. Click the **Add** button.



    In addition to the default credentials, the screen displays the device credentials that you added. For more information, see *Add a Device Credential* on page 30.

    b. Select one or more credentials and click the **Add Selection** button.

    To add all credentials, click the **Add All** button.

    The Select Credentials screen closes and the credentials are added to the Select Credentials table on the Network subscreen (the figure that is shown in *Step 7*).

    c. On the Network subscreen, select the credential or credentials that you added.

11. Click the **Save** button.

    The screen closes and the new or modified discovery profile displays in the Network Discovery table.

Execute a Discovery Job

You can execute a one-time discovery job immediately. For information about scheduling a one-time or recurring discovery job, see the *NMS300 Network Management System Application User Manual*.

➢ **To execute a discovery job:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

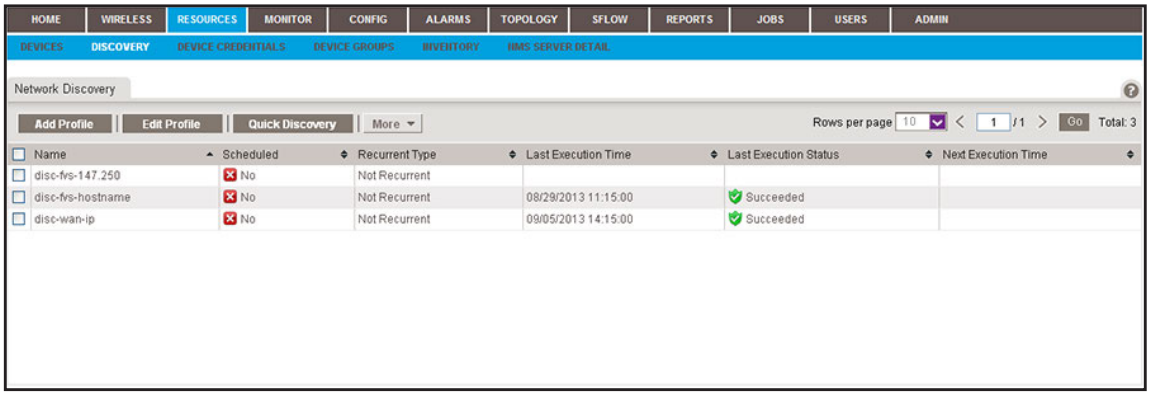
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

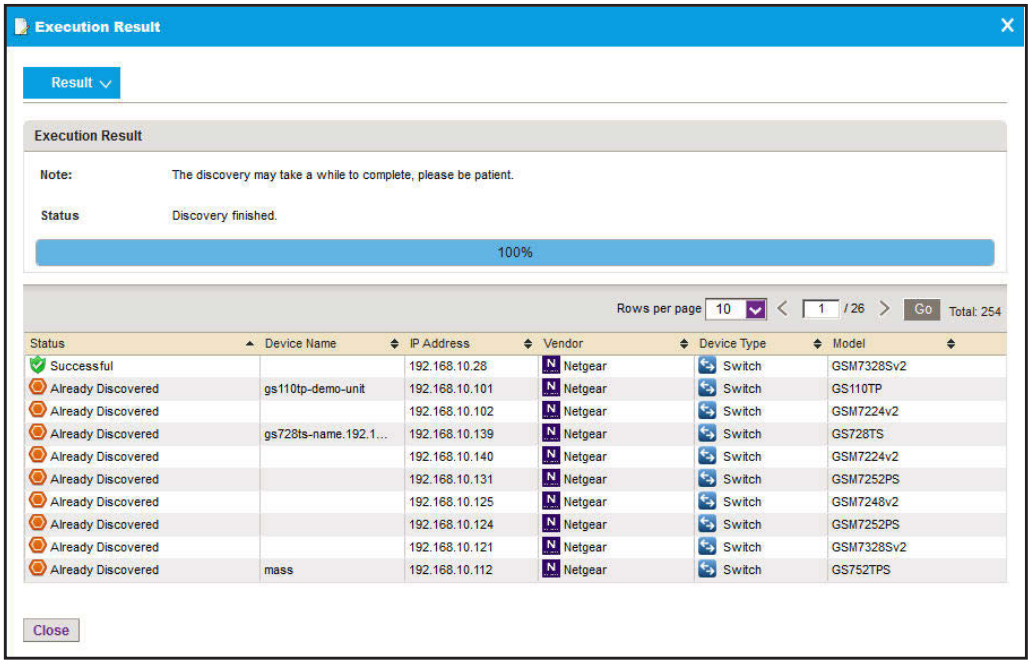
   The Network Summary screen displays.

4. Select **RESOURCES > DISCOVERY**.



5. Select the discovery profile.
6. From the **More** menu, select **Execute**.

   When discovery completes, the Execution Results screen displays the discovered devices that the application adds to its inventory database.



7. Click the **Close** button.

   The screen closes.

Note: Output files from completed resource discovery jobs are saved for the data retention period. For more information, see the *NMS300 Network Management System Application User Manual*.

Add Device Groups

To simplify the management of networks with many devices, you can create device groups. Once they are discovered, you can group the devices on your network by location, device type, and other criteria.

You can create static and dynamic device groups:

- **Static device group**. A fixed group of specific devices that you add manually. For more information, see *Add a Static Device Group* on page 38.
- **Dynamic device group**. A dynamic list of devices that are selected automatically based on your filter selection criteria. For more information, see *Add a Dynamic Device Group* on page 40.

Add a Static Device Group

A static group is a fixed list of specific devices. You must add devices manually.

➢ **To add a static device group:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

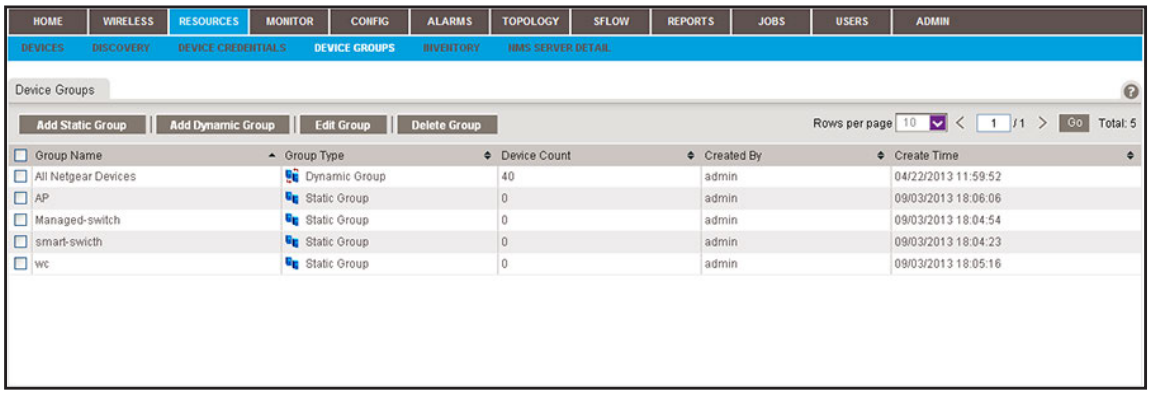
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

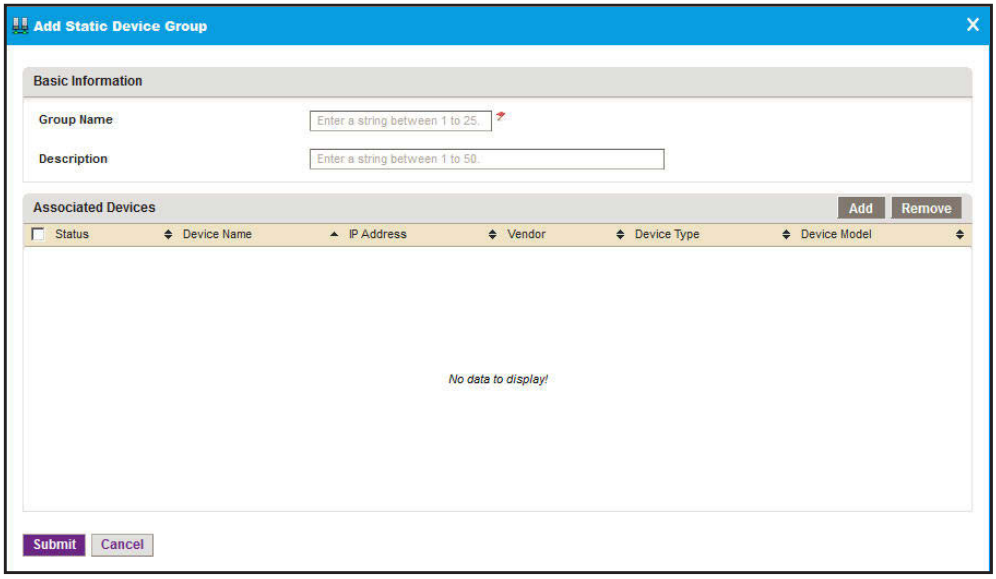
3. Click the **Sign In** button.

   The Network Summary screen displays.

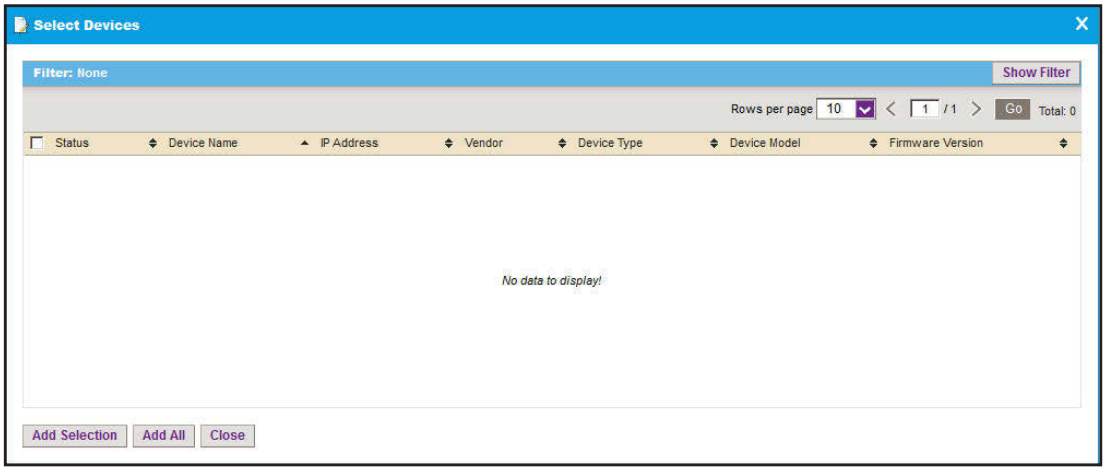
4. Select **RESOURCES > DEVICE GROUPS**.



5. Click the **Add Static Group** button.



6. Enter a group name.
7. Enter a description.
8. Click the **Add** button.



9. To filter the devices that display on the screen, click the **Show Filter** button.

   You can filter the devices by criteria such as device type, device name and IP address, location, device model, and status.

   To hide the device filter, click the **Hide Filter** button.
10. On the Select Devices screen, select devices for the group.
11. Click the **Add Selection** button.

    To add all devices, click the **Add All** button.
12. Click the **Submit** button.

    The screen closes. The devices are added to the static device group, and the group is displayed in the Device Groups table.

Add a Dynamic Device Group

A dynamic group is a dynamic list of devices that are selected automatically based on your filter selection criteria. The list changes automatically as devices that meet the filter criteria are added to and removed from the network.

➢ **To add a dynamic device group:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

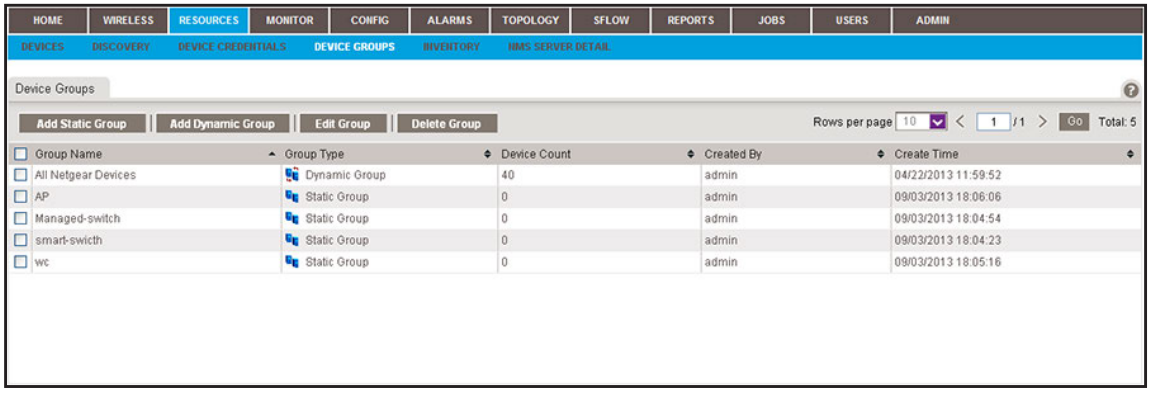
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

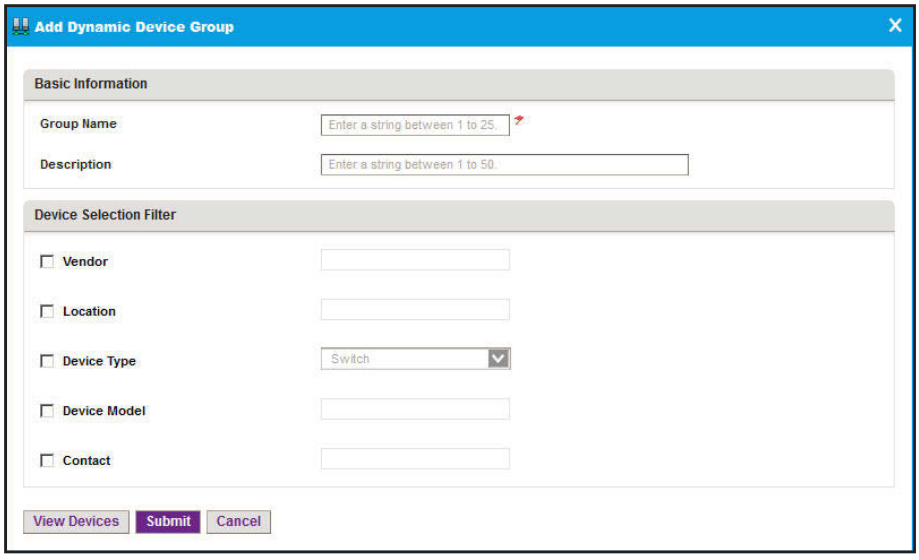
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **RESOURCES > DEVICE GROUPS**.



5. Click the **Add Dynamic Group** button.



6. Enter a group name.
7. Enter a description.
8. Enter the criteria for the device selection filter.

   You can filter by device vendor, device location, device type, device model, and device contact. You can select more than one filter. To filter by device type, make a selection from the **Device Type** menu.
9. To view the devices in the group before you save the group, select the **View Devices** button.

   The devices that meet the selection criteria are displayed.
10. Click the **Submit** button.

    The screen closes. The devices are added to the dynamic device group, and the group is displayed in the Device Groups table.

Monitor Your Network

4

Monitor devices and alarms

You can view summary and detailed information about the network, devices, and interfaces, including real-time and historical information and performance statistics. You can also enable and disable the configuration monitors and manage alarms.

This chapter covers the following topics:

- *Monitor Device and Network Information*
- *Manage the Configuration Monitors*
- *Manage Device Alarms and Alerts*

Note: For more information about the topics that are described in this chapter, see the *NMS300 Network Management System Application User Manual*.

Monitor Device and Network Information

The network monitor lets you view device and interface information, network summary information, performance statistics, real-time information, and historical information.

The application provides the following types of views:

- **Inventory and interface view**. View the devices that the application discovered and the interfaces that are associated with the devices. For more information, see *View and Export the Inventory Table and Interface List Table* on page 43.
- **Device view**. View and manage the information for devices that the application discovered. For more information, see *View Device Information and Device Details* on page 45.
- **Wireless device view**. View and manage the information for wireless devices that the application discovered. For more information, see *View Wireless Device Information Only* on page 48.
- **Wireless client view**. View and manage the information for wireless clients of wireless devices that the application discovered. For more information, see *View Wireless Client Information* on page 51
- **Network summary view**. Display a network overview with a device tree, an enterprise network map, and the status of and statistics for the devices that the application discovered. For more information, see *View the Default Network Summary* on page 54.

The application provides several more views that you first must configure before they display useful information: the topology map view, network topology view, and dashboard views that you can display on the network dashboard. For information about these views and dashboards, see the *NMS300 Network Management System Application User Manual*.

The following sections describe the tasks that you can perform:

- *View and Export the Inventory Table and Interface List Table*
- *View Device Information and Device Details*
- *View Wireless Device Information Only*
- *View Wireless Client Information*
- *View the Default Network Summary*

View and Export the Inventory Table and Interface List Table

You can view the table of wired and wireless devices and interfaces that the application manages, and export this table to an Excel or PDF file.

➢ **To view and export the Inventory table and Interface List table:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

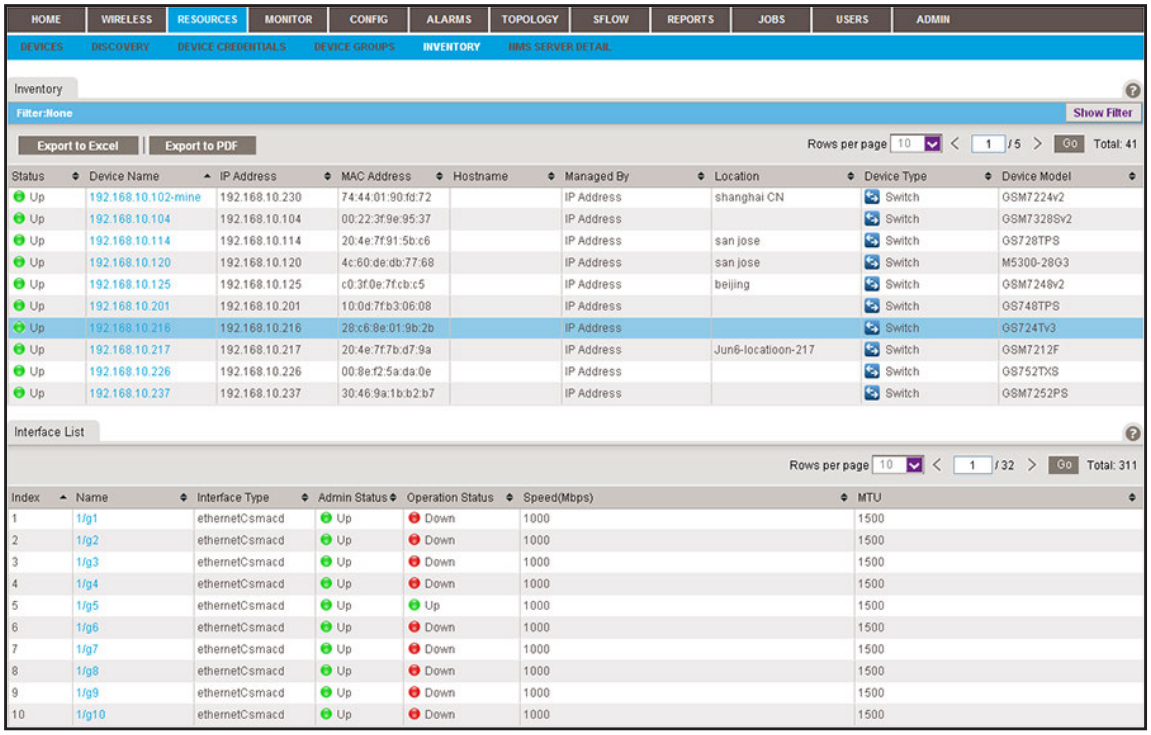
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **RESOURCES > INVENTORY**.



5. To add columns to or remove them from the Inventory table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, Device Model, Device Type, Firmware Version, Serial Number, MAC Address, Last Update Time, Location, Registered, Hostname, Managed By, Date of Purchase, Vendor, Country of Purchase, Hardware Version, Configuration Version, Contact, Discover Time, and Description.

6. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as device type, device name and IP address, device model, and status.

   To hide the filter, click the **Hide Filter** button.

7. To view interfaces for a specific device, click the table row for a device anywhere but in the Device Name column.
8. To view details about an individual device or interface, in the Device Name column, click a device name (or IP address), or, in the Name column, click an interface name.

For information about viewing device details, see *View Device Information and Device Details* on page 45.

9. Click the **Export to Excel** button or the **Export to PDF** button.
10. To save the device information on your computer, follow the directions of your browser.

View Device Information and Device Details

You can see a table of devices that the application discovered in your network.

➢ **To view the Devices table:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

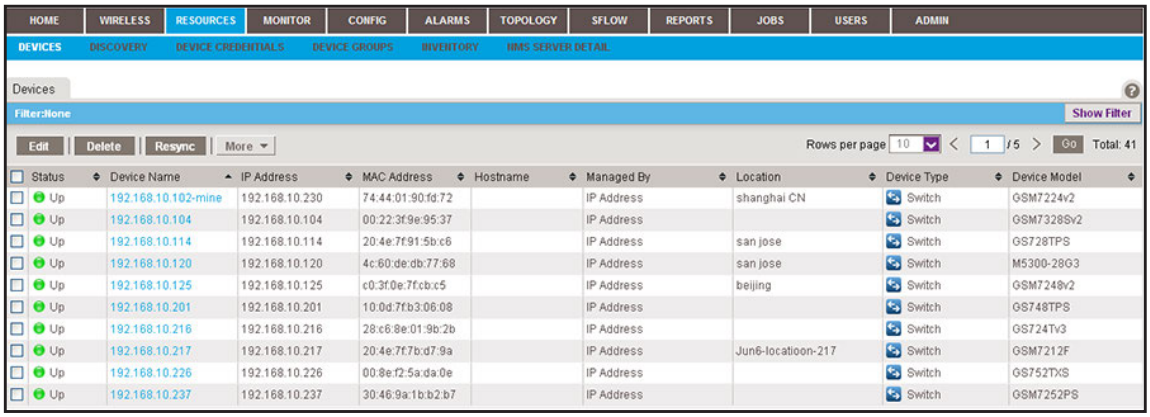
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **RESOURCES > DEVICES**.



   The screen displays the devices that the application discovered.

5. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, Device Model, Device Type, Firmware Version, Serial Number, MAC Address, Last Update Time, Location, Registered, Hostname, Managed By, Date of Purchase, Vendor, Country of Purchase, Hardware Version, Configuration Version, Contact, Discover Time, and Description.

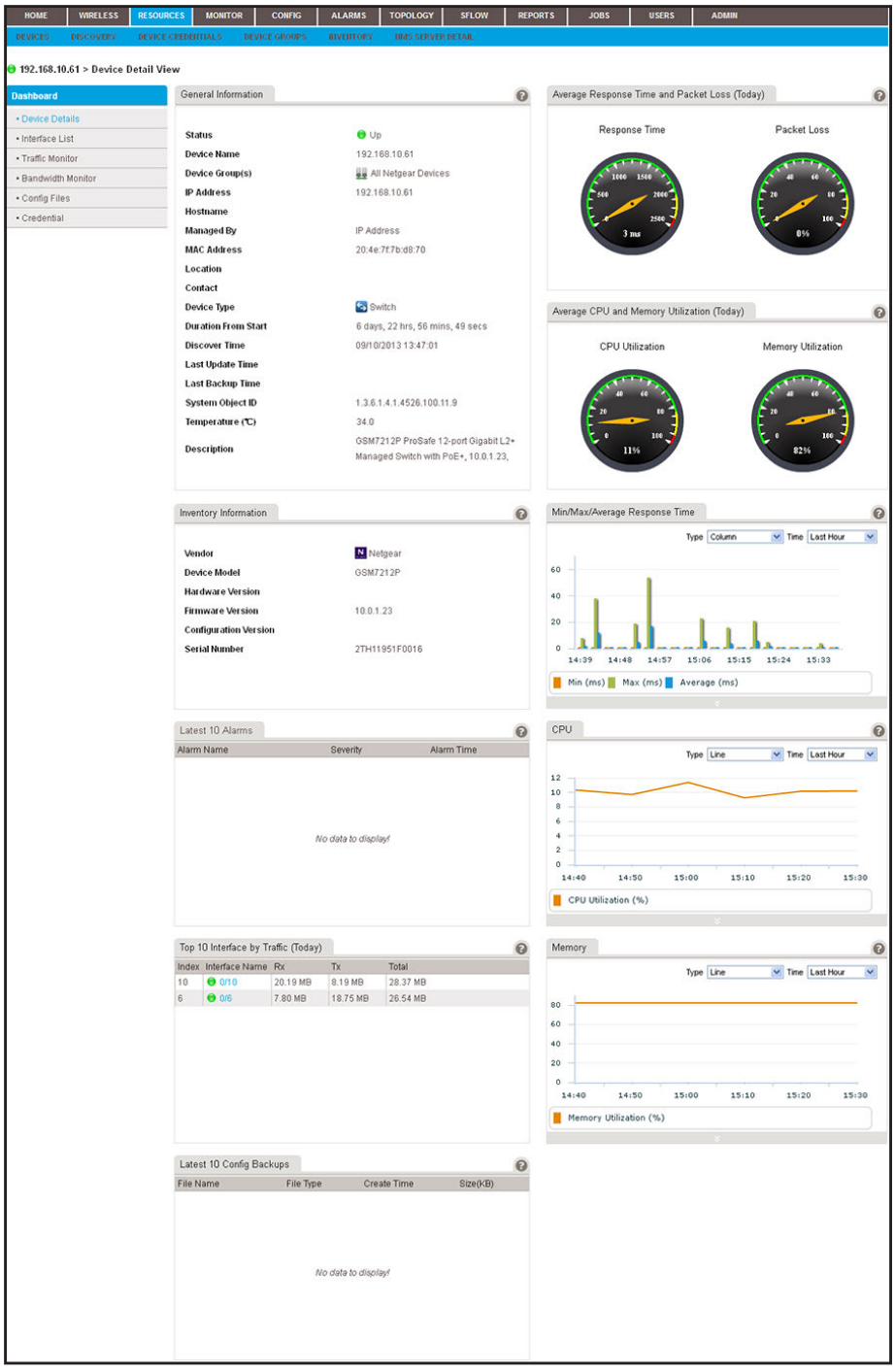
6. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, vendor, model, and status.

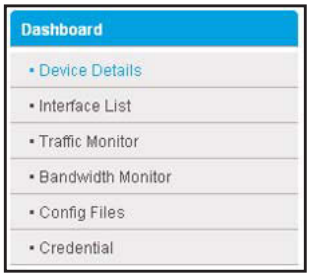
To hide the filter, click the **Hide Filter** button.

7. To view details about a device, click the device name (or IP address) for the device.

   The following figure shows the screen that displays when the device that you select is a switch.



The following figure shows the **Dashboard** menu for a switch.



Note: If the device that you select is an M6100 managed switch, the Dashboard also displays the Slot List option.

8. From the **Dashboard** menu, select a menu option.

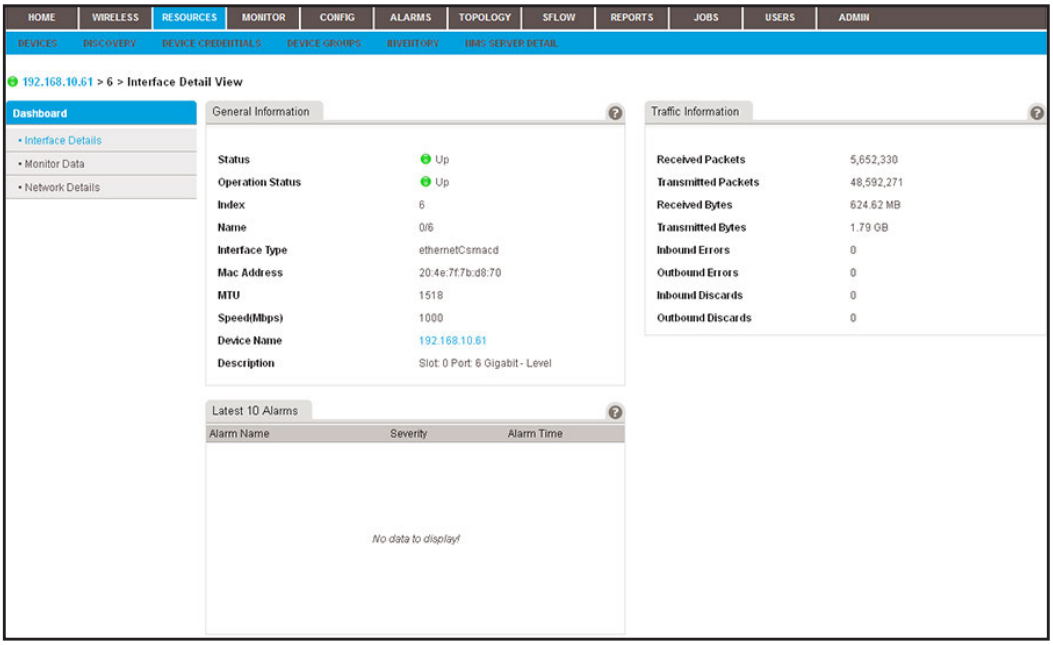
   The screen adjusts to display information that corresponds to your menu option.

   For switches, wireless controllers, wireless management systems, and routers, you can display interface details.

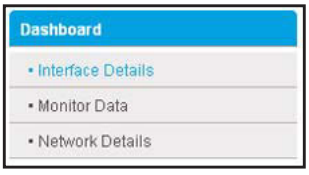
9. To display interface details:

   a. Select **Interface List**.

      A screen similar to the following displays.



   The following figure shows the **Dashboard** menu for an interface:



b. From the **Dashboard** menu, select a menu option.

The screen adjusts to display information that corresponds to your menu option.

View Wireless Device Information Only

You can easily monitor your wireless network by displaying wireless controllers, wireless access point (APs), wireless management systems, and active wireless clients.

Because of the nature of controller-managed APs, the application can provide only limited information for controller-managed APs, compared to standalone APs.

Note: For information about viewing wireless clients of wireless controllers, APs, and management systems, see *View Wireless Client Information* on page 51.

View Wireless Controller Information Only

You can display only the wireless controllers that the application manages.

➢ **To view wireless controller information:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

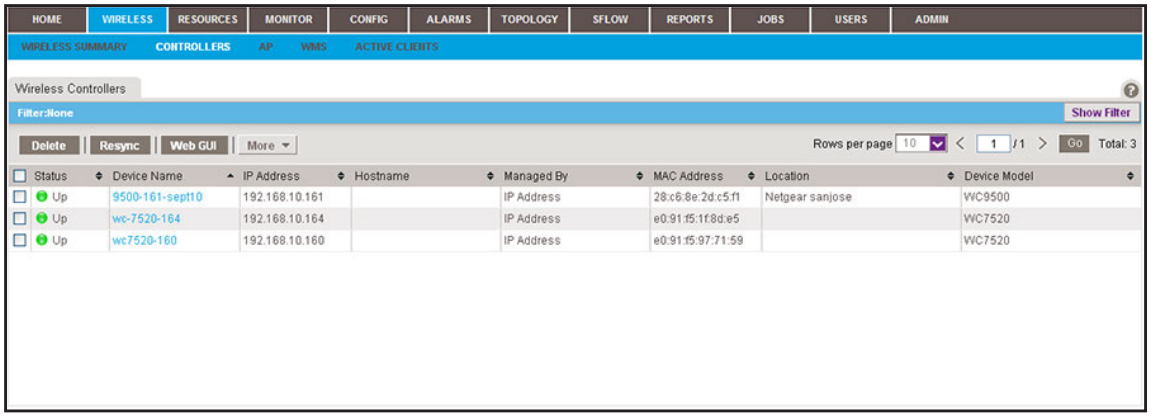
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **WIRELESS > CONTROLLERS**.



5. To add columns to or remove them from the Wireless Controllers table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, Hostname, Managed By, MAC Address, Location, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, and Discover Time.

6. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as name, IP address, location, model, and status.

   To hide the filter, click the **Hide Filter** button.

7. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Information and Device Details* on page 45.

View Wireless Access Point Information Only

You can display only the standalone APs and controller-managed APs. The application manages the standalone APs. The controller-managed APs are managed by their wireless controllers and display for information only.

➢ **To view wireless access point information:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

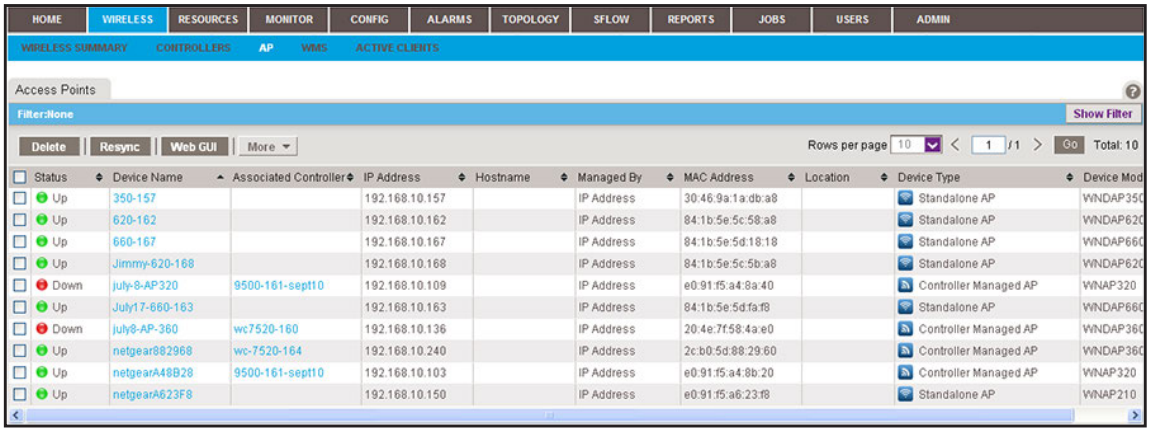
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **WIRELESS > AP**.



5. To add columns to or remove them from the Access Points table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

6. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as device name, device IP address, controller name, location, device model, and status.

   To hide the filter, click the **Hide Filter** button.

7. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Information and Device Details* on page 45.

View Wireless Management System Information Only

You can display only the wireless management systems that the application manages.

➢ **To view wireless management system information:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

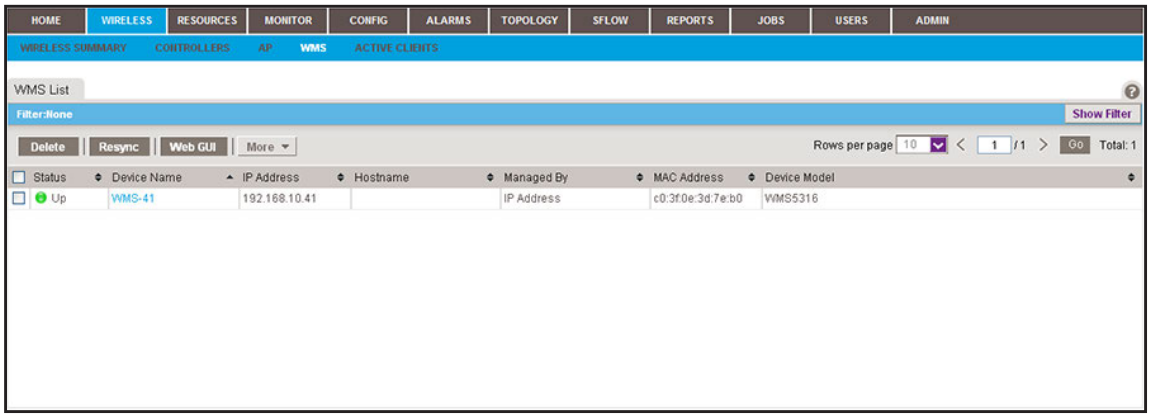
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **WIRELESS > WMS**.



5. To add columns to or remove them from the WMS List table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

You can choose from the following columns: Status, Device Name, IP Address, Hostname, Managed By, MAC Address, Device Model, Vendor, Location, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial, Number, Contact, and Discover Time.

6. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

7. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Information and Device Details* on page 45.

View Wireless Client Information

The application lets you monitor the active wireless clients by wireless controller, standalone AP, controller-managed AP, or SSID.

You can display various wireless details for each client.

➢ **To monitor wireless clients and view details for a single client:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

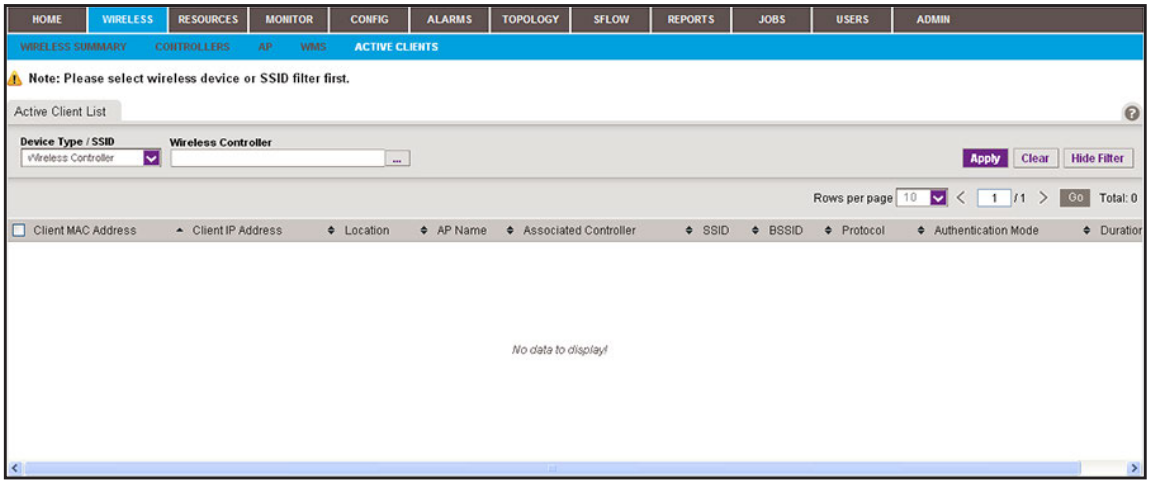
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **WIRELESS > ACTIVE CLIENTS**.

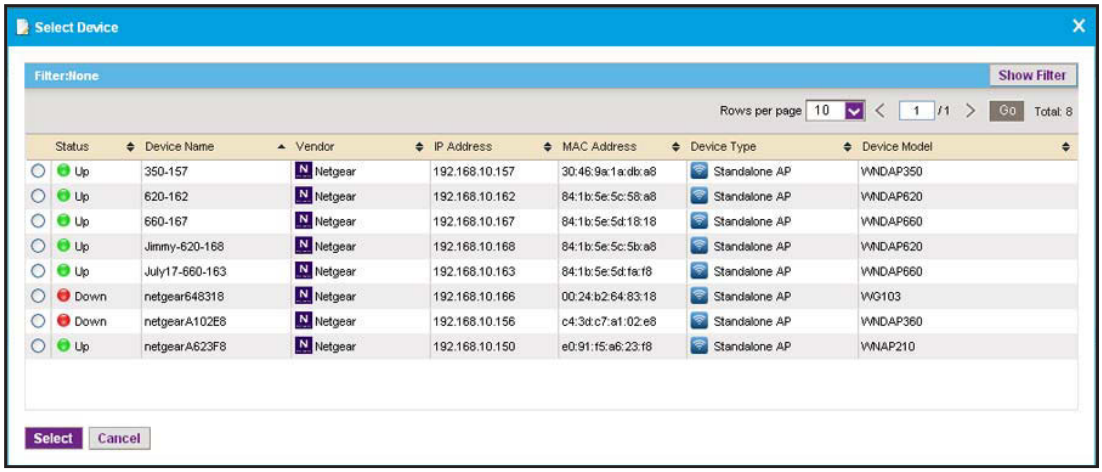


By default, the filter is active because the Active Client List table can display many wireless clients.

5. To hide the filter for active clients, click the **Hide Filter** button and go to *Step 12*.
6. From the **Device Type / SSID** menu, select **Wireless Controller**, **Standalone AP**, **Controller Managed AP**, or **SSID**.

   The name of the field to the right of the **Device Type / SSID** menu adjusts according to your selection from the menu.
7. Click the dots next to the field to the right of the **Device Type / SSID** menu.

   A screen similar to the following displays.

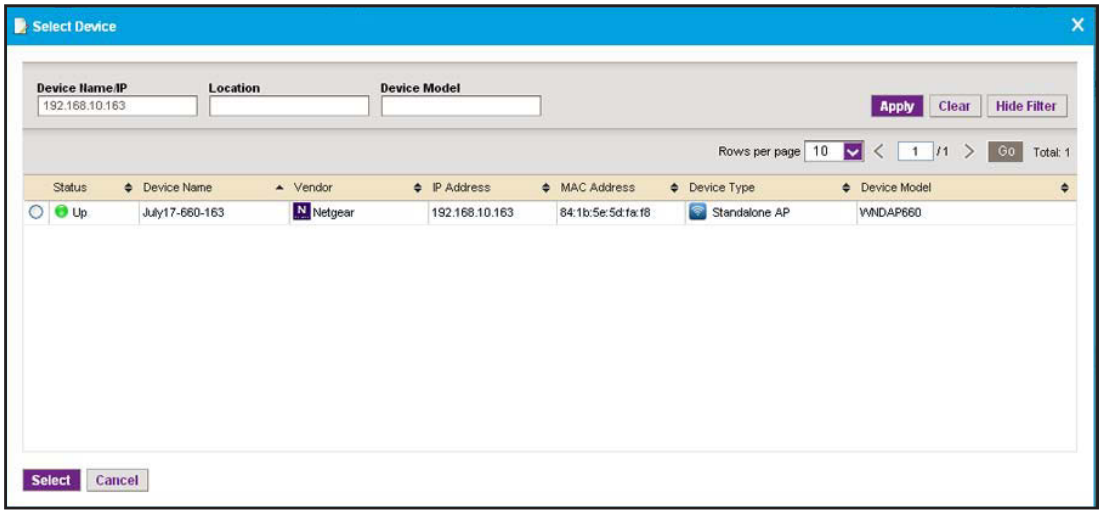


8. To filter the devices or SSIDs that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as name, IP address, location, and model. You can filter the SSIDs by criteria such as SSID name, device name, and device IP address.

   To hide the filter for devices or SSIDs, click the **Hide Filter** button.

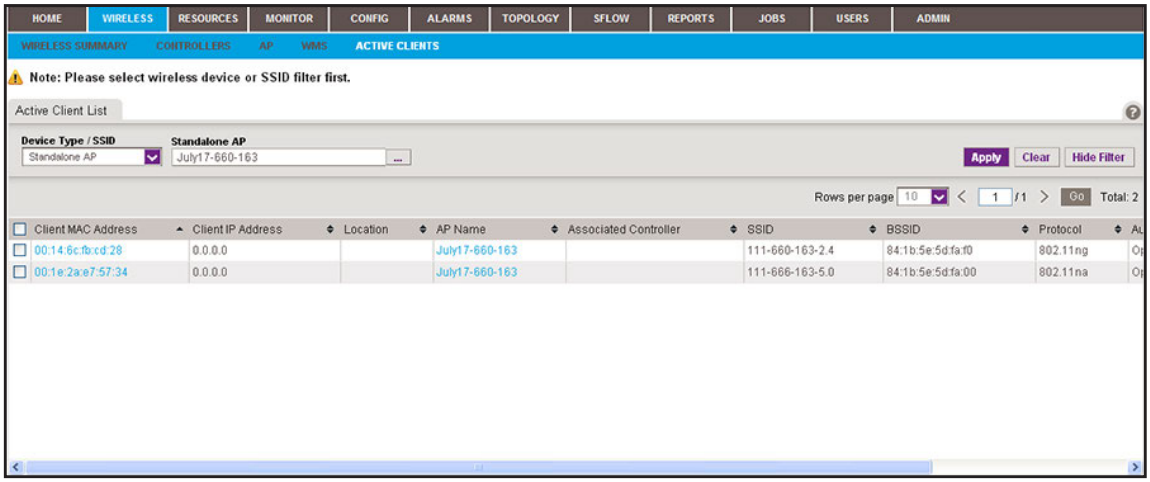
   The following figure shows a sample of a screen that displays when you filter by device IP address:



9. Select the device or SSID.
10. Click the **Select** button.

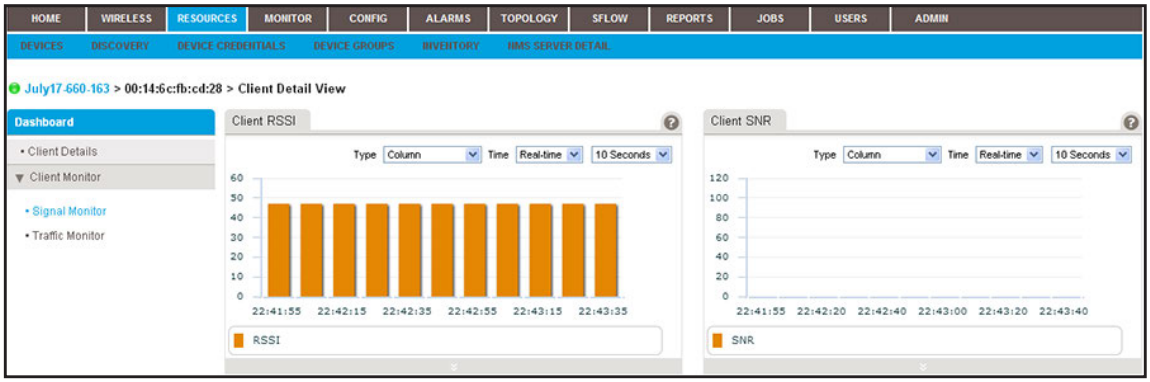
    The screen closes and the empty Active Client List table displays.
11. Click the **Apply** button.

    The application populates the Active Client List table with the wireless clients of the selected device or SSID.



12. To add columns to or remove them from the Active Client List table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

    You can choose from the following columns: Client MAC Address, Client IP Address, Location, AP Name, Associated Controller, SSID, BSSID, Protocol, Authentication Mode, Duration, Channel, RSSI, SNR, Transmit Power, Transmitted, Rate (Mbps), Received Rate (Mbps), Transmitted Bytes, Received Bytes, Transmitted Packets, Received Packets, and Status.
13. To view details for an individual wireless client, in the Client MAC Address column, click a MAC address. A screen similar to the following displays.



14. From the **Dashboard** menu, select a menu option.

    By default, the screen displays the **Signal Monitor** menu option. If you select the **Traffic Monitor** menu option, the screen adjusts.

View the Default Network Summary

The Network Summary screen displays a device tree, an enterprise network map, a physical representation of the status and device type of the inventory, and various top 10 widgets.

➢ **To view the default network summary:**

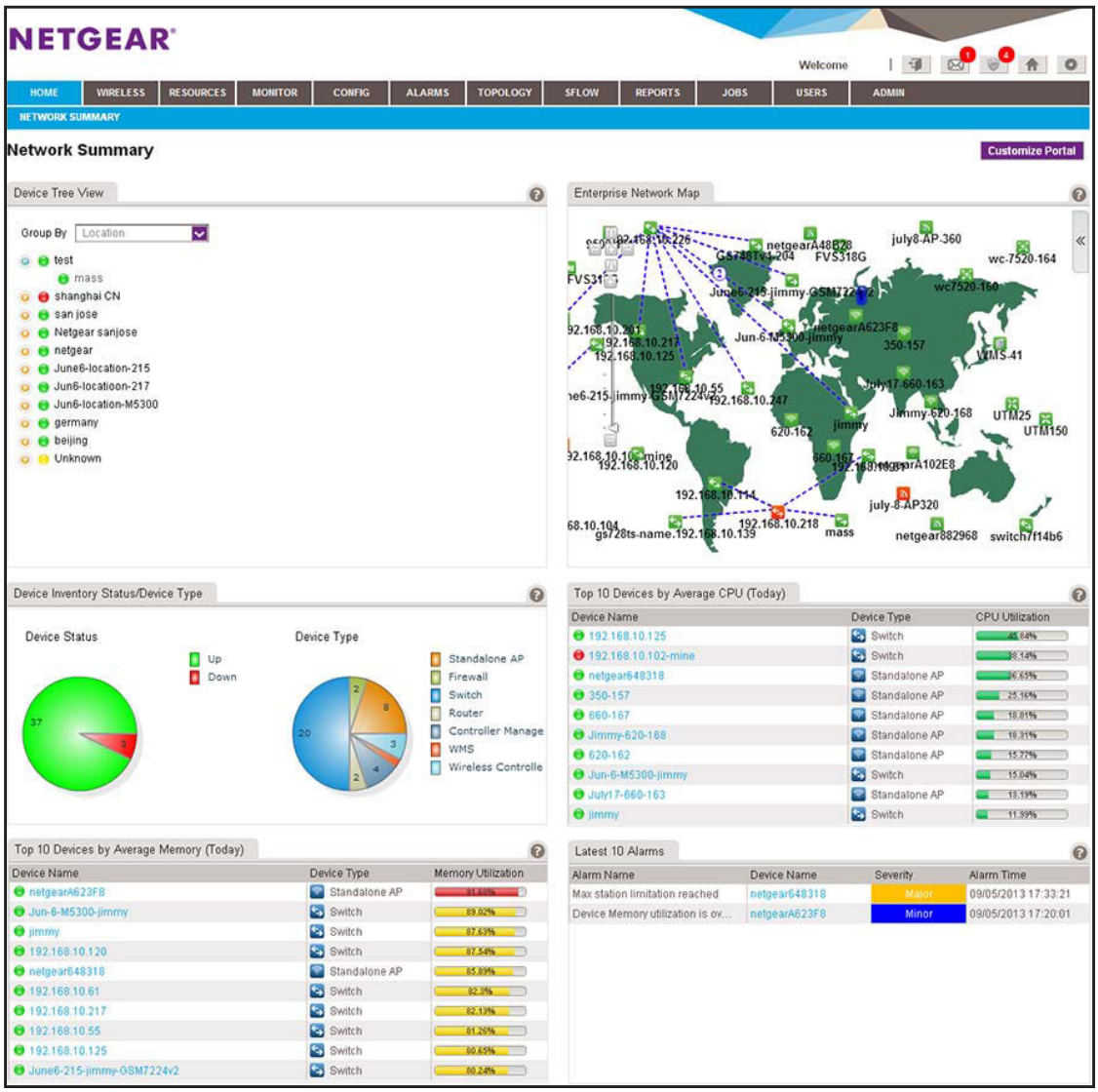
1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.



By default, the following widgets display onscreen.

Widget	Description	Information
Device Tree View	A tree of all discovered and managed devices in the network. You can expand the tree.	Group devices by: • Location (the default setting) • Vendor • Device Type • Device Group
Enterprise Network Map	A world map that displays the location of each device and its connections to other devices	• Manual link • LLDP link • < 1.5 Mbps link • >= 1.5 Mbps < 10 Mbps link • >= 10 Mbps < 100 Mbps link • >= 100 Mbps < 1 Gbps link • >= 1 Gbps < 10 Gbps link • >= 10 Gbps link • Link of unknown speed
Device Inventory Status/Device Type	A slice graph displaying the device status (Up or Down) and a slice graph displaying the network breakdown per device type.	
Top 10 Devices by Average CPU (Today)	Top 10 devices by average CPU utilization for today	• Device status • Device name • Device type • CPU utilization in percentage
Top 10 Devices by Average Memory (Today)	Top 10 devices by average memory utilization for today	• Device status • Device name • Device type • Memory utilization in percentage
Latest 10 Alarms		• Alarm Name • Device Name • Severity • Alarm Time

4. To view details about a device, click the device name.

   For more information, see *View Device Information and Device Details* on page 45.

Manage the Configuration Monitors

The application provides monitors for the following device metrics:

- Status
- ICMP ping
- CPU
- Memory
- Temperature
- Disk (for storage devices)
- IP traffic
- ICMP traffic
- TCP traffic
- UDP traffic
- SNMP traffic
- Interface traffic

In addition, the application provides monitors for the following server, wireless device, and storage system metrics:

- NMS system server
- Radio statistics
- WLAN utilization
- VAP statistics (wireless performance statistics of the WLAN network based on SSID)
- Wired Ethernet statistics (wired performance statistics of standalone APs)
- Storage temperature
- Storage disk temperature
- Storage disk capacity

By default, all monitors are enabled. You can disable or reenable individual monitors and specify the information and devices that are monitored.

For each individual monitor, you can modify the information and devices that are monitored.

➢ **To configure an individual monitor:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

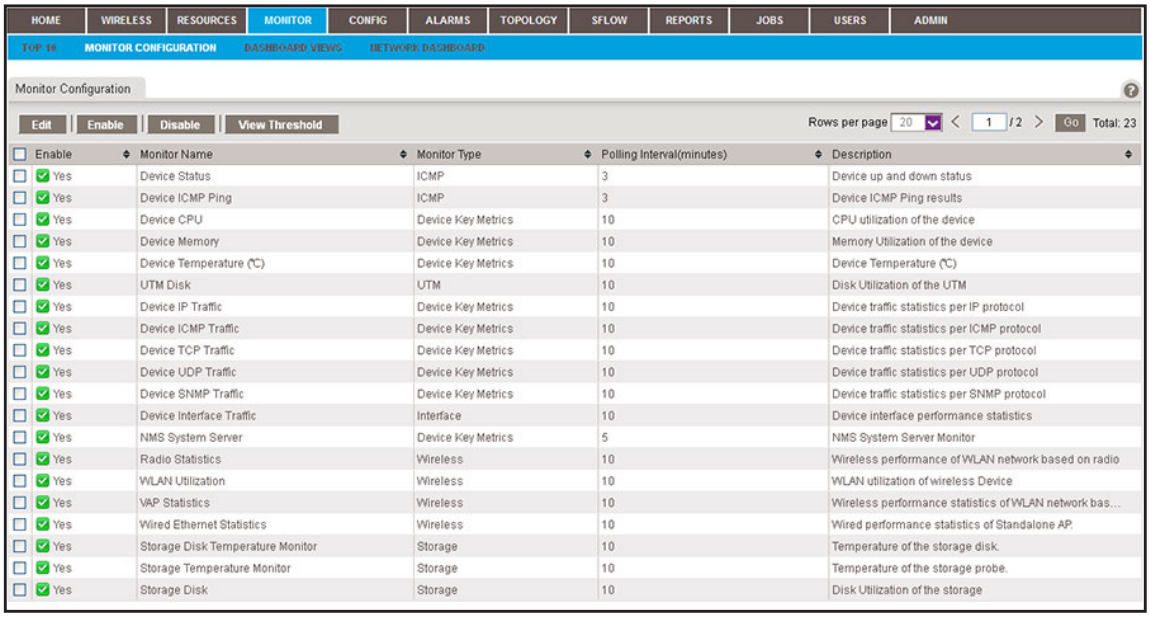
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

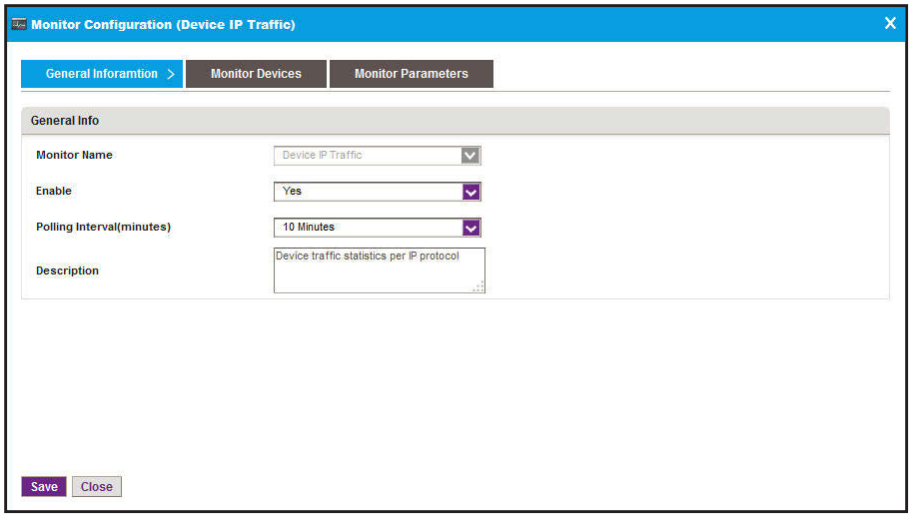
   The Network Summary screen displays.

4. Select **MONITOR > MONITOR CONFIGURATION**.



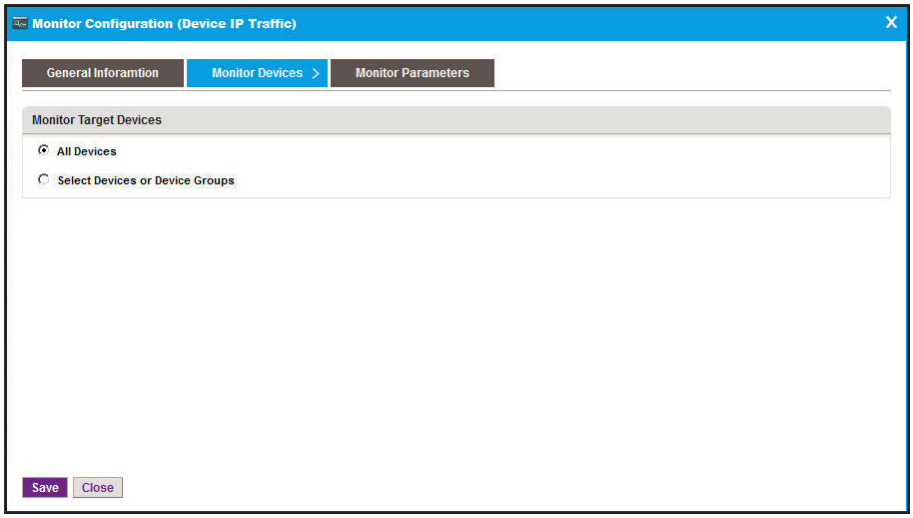
Enable	Monitor Name	Monitor Type	Polling Interval(minutes)	Description
Yes	Device Status	ICMP	3	Device up and down status
Yes	Device ICMP Ping	ICMP	3	Device ICMP Ping results
Yes	Device CPU	Device Key Metrics	10	CPU utilization of the device
Yes	Device Memory	Device Key Metrics	10	Memory Utilization of the device
Yes	Device Temperature (℃)	Device Key Metrics	10	Device Temperature (℃)
Yes	UTM Disk	UTM	10	Disk Utilization of the UTM
Yes	Device IP Traffic	Device Key Metrics	10	Device traffic statistics per IP protocol
Yes	Device ICMP Traffic	Device Key Metrics	10	Device traffic statistics per ICMP protocol
Yes	Device TCP Traffic	Device Key Metrics	10	Device traffic statistics per TCP protocol
Yes	Device UDP Traffic	Device Key Metrics	10	Device traffic statistics per UDP protocol
Yes	Device SNMP Traffic	Device Key Metrics	10	Device traffic statistics per SNMP protocol
Yes	Device Interface Traffic	Interface	10	Device interface performance statistics
Yes	NMS System Server	Device Key Metrics	5	NMS System Server Monitor
Yes	Radio Statistics	Wireless	10	Wireless performance of WLAN network based on radio
Yes	WLAN Utilization	Wireless	10	WLAN utilization of wireless Device
Yes	VAP Statistics	Wireless	10	Wireless performance statistics of WLAN network bas...
Yes	Wired Ethernet Statistics	Wireless	10	Wired performance statistics of Standalone AP
Yes	Storage Disk Temperature Monitor	Storage	10	Temperature of the storage disk.
Yes	Storage Temperature Monitor	Storage	10	Temperature of the storage probe.
Yes	Storage Disk	Storage	10	Disk Utilization of the storage

5. Select the monitor.
6. Click the **Edit** button.



7. (Optional) In the General Information screen, modify the following settings:
   - From the **Polling Interval** menu, select a polling interval.
   - Enter a description.

8. Click the **Monitor Devices** tab.



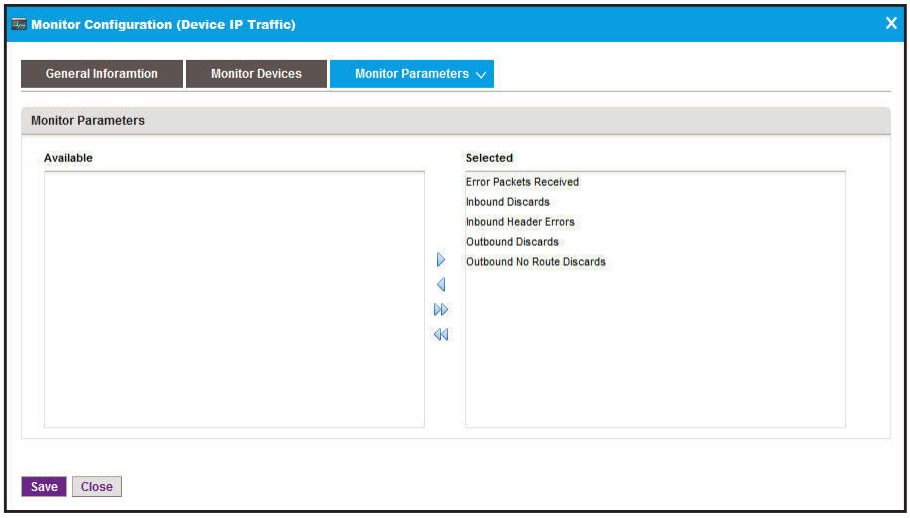
9. (Optional) In the Monitor Devices screen, select one of the following radio buttons:
   - **All Devices**. Monitors all devices.
   - **Select Devices or Device Groups**. The screen adjusts to let you select devices, device groups, or both to monitor:
     a. Click the **Add Device** button.
     b. Either select individual devices and click the click **Add Selection** button, or click the **Add All** button.

        The device or devices are added to the table on the Monitor Devices screen.

     c. Click the **Add Group** button.
     d. Either select individual devices and click the click **Add Selection** button, or click the **Add All** button.

        The device groups or groups are added to the table on the Monitor Devices screen.

10. Click the **Monitor Parameters** tab.



11. (Optional) In the Monitor Devices screen, move parameters between the Available Fields table and Selected Fields table by using the **>**, **<**, **>>**, and **<<** buttons.
    a. In the Available Fields table, select a parameter.
    b. Click the **>** button.

       The parameter moves to the Selected Fields table.

    c. To move another parameter, repeat *Step a* and *Step b*.
12. Click the **Save** button.

    Your changes are saved.

Manage Device Alarms and Alerts

The application provides many default alarms, including status alarms, monitor alarms, and trap alarms. If an upper or lower threshold is exceeded, an alarm configuration generates an alarm.

The application provides the following four severity levels for alarms:

- Critical (by default, red color indication)
- Major (by default, yellow color indication)
- Minor (by default, blue color indication)
- Info (by default, no color indication)

You can view and manage the current alarms and use optional alarm notification profiles to specify criteria that enable the application to generate and send a notification email message if an alarm occurs.

For more about how to view and manage the alarm history and how to add custom alarm configurations that are based on existing configuration monitors, see the *NMS300 Network Management System Application User Manual*.

View and Manage Current Alarms

The Current Alarms table shows the active alarms for the entire network. You can acknowledge alarms, display details about alarms, clear alarms, and export alarms.

➢ **To view and manage the current alarms:**

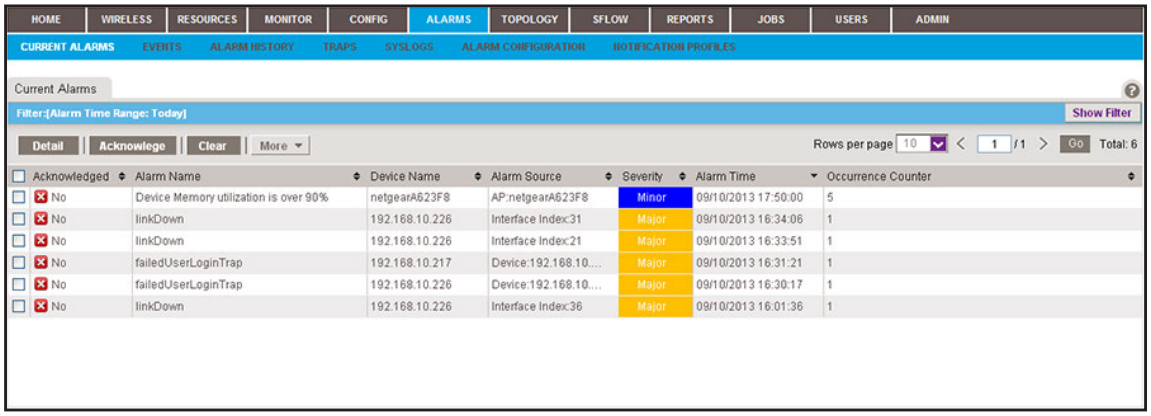
1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **ALARMS > CURRENT ALARMS**.



5. To add columns to or remove them from the Current Alarms table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Acknowledged, Alarm Name, Device Name, Alarm Source, Severity, Alarm Time, Occurrence Counter, Alarm Type, Device IP, Acknowledge By, Acknowledge Time, and Notification OID.

6. To filter the alarm entries that are listed, click the **Show Filter** button.

   You can filter the alarm entries by criteria such as time range, device name, device IP address, alarm name, severity level, and acknowledgment. By default, the alarm entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

7. Take one of the following actions:
   - View details for an alarm:
     a. Select the alarm.
     b. Click the **Detail** button.

     c. To close the Alarm Detail screen, click the **Close** button.
   - Acknowledge an alarm:
     a. Select the alarm.
     b. Click the **Acknowledge** button.

        Acknowledging an alarm means that you take ownership of the issue.

- Clear an alarm:
  a. Select the alarm.
  b. Click the **Clear** button.

     Clearing an alarm means that the fault that the alarm indicates no longer exists.
- Acknowledge a batch of alarms:
  a. Select multiple alarms.
  b. From the **More** menu, select **Batch Acknowledge**.
- Clear a batch of alarms:
  a. Select multiple alarms.
  b. From the **More** menu, select **Batch Clear**.
- Export the entire Current Alarms table to an Excel spreadsheet:
  a. From the **More** menu, select **Export to Excel**.
  b. To save the alarms on your computer, follow the directions of your browser.
- Export the entire Current Alarms table to a PDF:
  a. From the **More** menu, select **Export to PDF**.
  b. To save the alarms on your computer, follow the directions of your browser.

Add an Alarm Notification Profile

By default, the application does not include any alarm notification profiles. To be notified if an alarm occurs, you need to add an alarm notification profile.

Before the application can generate email and SMS messages, you must provide email server settings and SMS server settings. For more information, see *Configure the Email Server for Alerts and Alarm Notifications* on page 19 and *Configure the SMS Server for Alerts and Alarm Notifications* on page 22.

➢ **To add an alarm notification profile:**

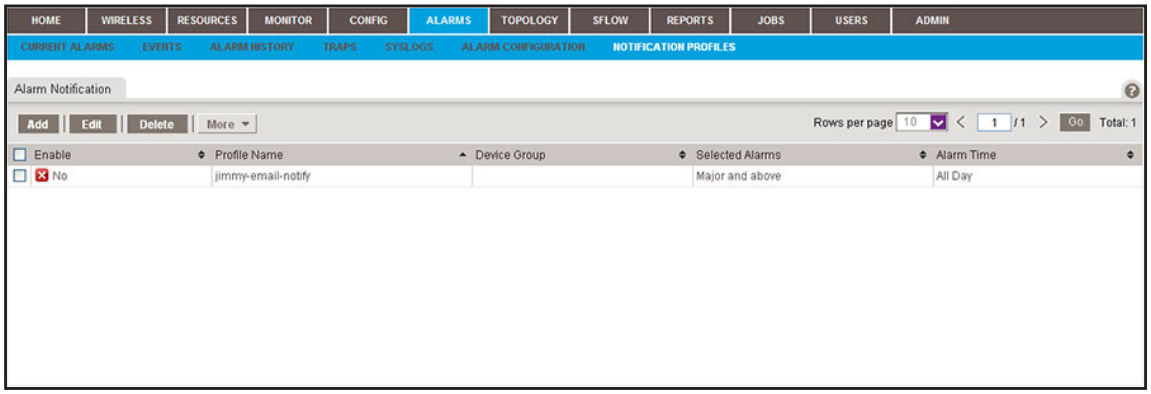
1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.
2. Enter your user name and password.

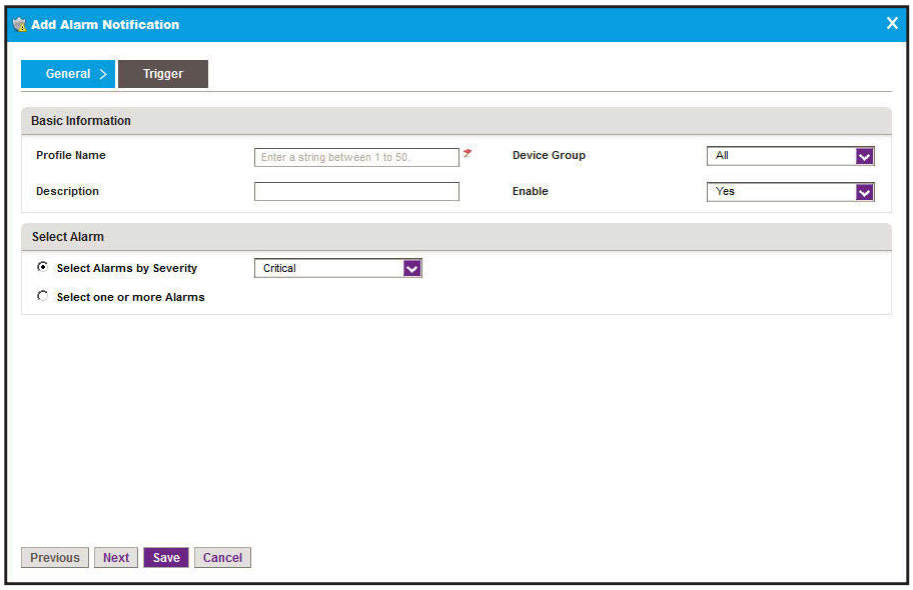
   The default administrator user name is **admin** and the default administrator password is also **admin**.
3. Click the **Sign In** button.

   The Network Summary screen displays.

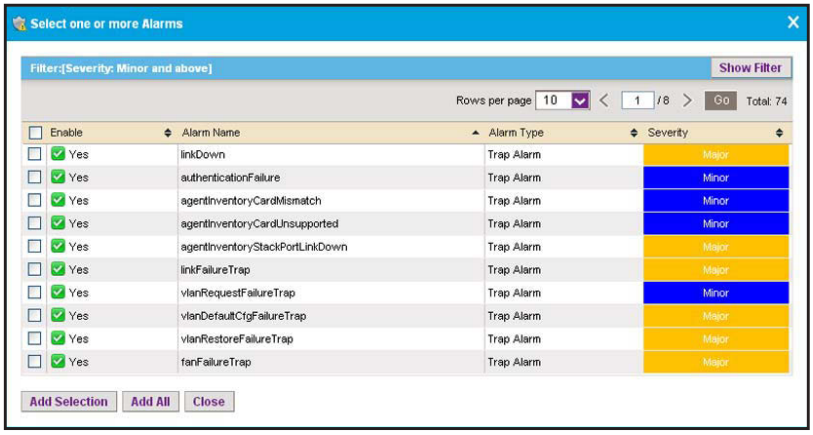
4. Select **ALARMS > NOTIFICATION PROFILES**.



5. Click the **Add** button.



6. In the Basic Information section, specify the following information:
   - **Profile Name**. Enter the name for the profile.
   - **Description**. Enter the description for the profile.
   - **Device Groups**. Select whether to apply the profile to all device groups or to a particular device group.
   - **Enable**. Select whether to enable the alarm notification profile.
7. In the Select Alarm section, select one of the following radio buttons:
   - **Select Alarms by Severity**. Select the alarms by severity by selecting a severity level from the menu.
   - **Select one or more Alarms**. The appearance of the screen changes, enabling you to add alarms:
     a. Click the **Add** button.



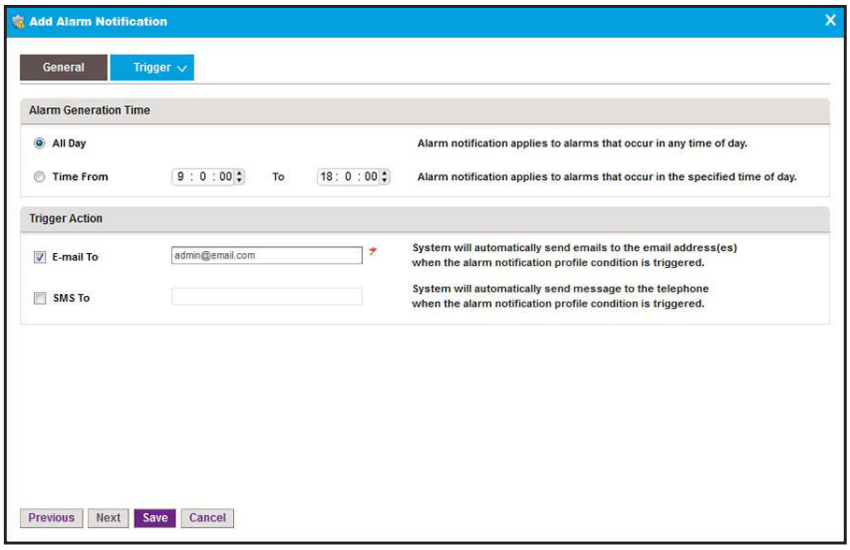
b. Select the alarms that you want to include in the alarm notification profile.

c. Click the **Add Selection** button.

To add all alarms, click the **Add All** button.

The alarms are added to the Add Alarm Notification screen.

8. Click the **Trigger** tab.



9. Specify the following information:

- **Alarm Generation Time**. Select one of the following radio buttons:
  - **All Day**. The alarm notification applies to alarms that occur in any time of the day.
  - **Time Frame**. From the menus, select a time frame. The alarm notification applies only to alarms that occur in the specified time frame.
- **Trigger Action**. Select one or both check boxes:
  - **E-mail To**. Enter the email address to send the notification to if the alarm notification condition is triggered.
- **SMS To**. Enter the telephone number to send the notification to if the alarm notification condition is triggered.

Note: The SMS notification option is supported for a particular SMS gateway in the People's Republic of China only. For more information, see *Configure the SMS Server for Alerts and Alarm Notifications* on page 22.

10. Click the **Save** button.

    The Add Alarm Notification screen closes. The alarm profile notification displays in the Alarm Notification table.

Manage Configurations and Firmware

5

Keep your device firmware current

You can back up and restore device configurations. You can also upgrade device firmware.

This chapter covers the following topics:

- *Add a Backup Profile and Execute a Backup Job*
- *Restore the Configuration of a Single Device*
- *Upgrade Firmware for One or More Devices*

Note: For more information about the topics that are described in this chapter, see the *NMS300 Network Management System Application User Manual*.

Add a Backup Profile and Execute a Backup Job

A backup profile defines the devices that are included in a backup job, and as an option, the schedule with which the backup job occurs. For information about scheduling a backup job, see the *NMS300 Network Management System Application User Manual*.

You must create a backup profile before you can back up the configuration of one or more devices. After you executed a backup job, you can use the backup file to restore device configurations for the devices on your network. For more information, see *Restore the Configuration of a Single Device* on page 69.

To a single backup profile, you can add devices, device groups, or both.

➢ **To add a backup profile and execute a backup job:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

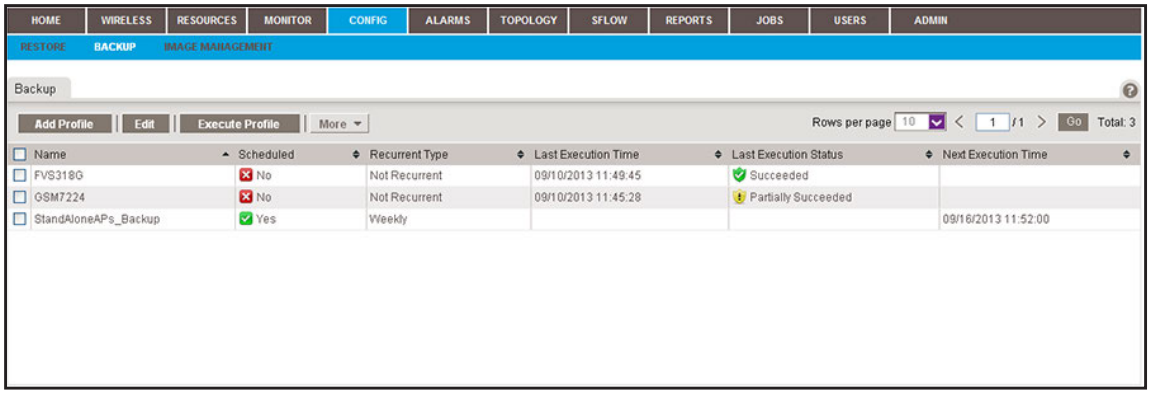
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **CONFIG > BACKUP**.

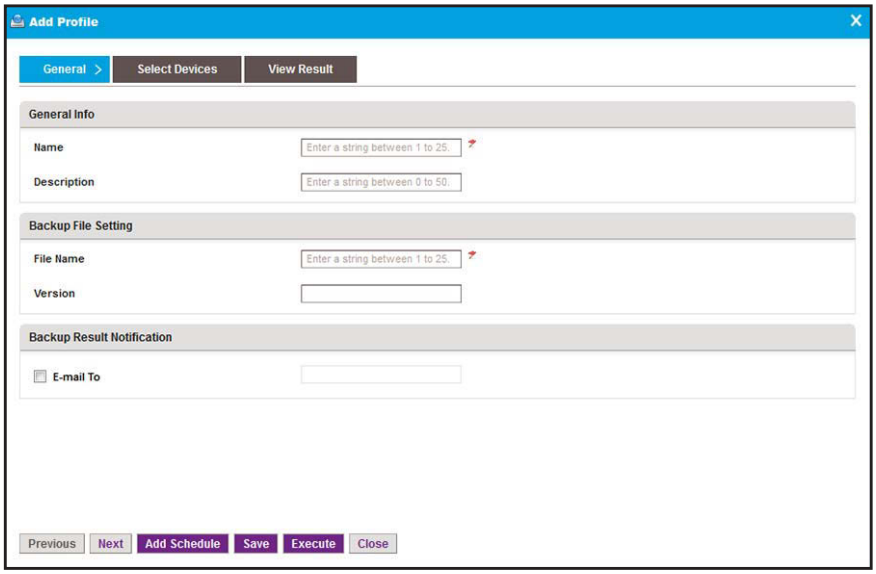


   The Backup screen displays the existing backup profiles.

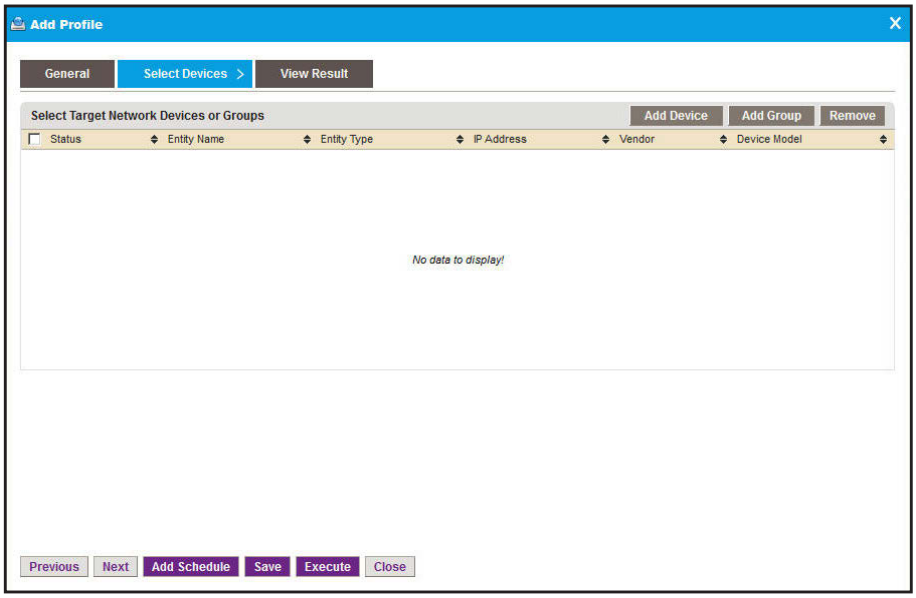
5. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

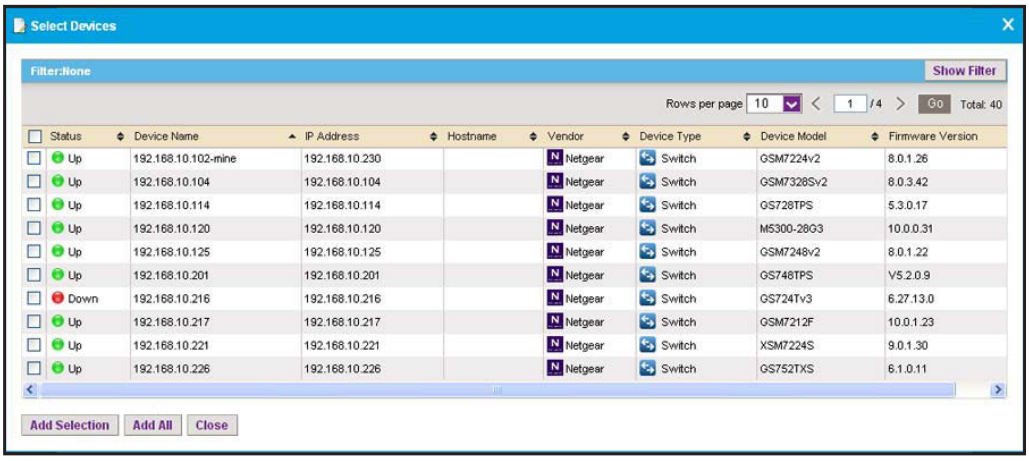
Click the **Add Profile** button.



6. Enter or modify the following information:
   - **General Info**. Enter a name and description for the new profile.
   - **Backup File Setting**. Enter a file name and version for the backup file.
   - **Backup Result Notification**. To enable the application to send an email message with the backup results, select the **E-mail To** check box and enter an email address.
7. Click the **Select Devices** tab.



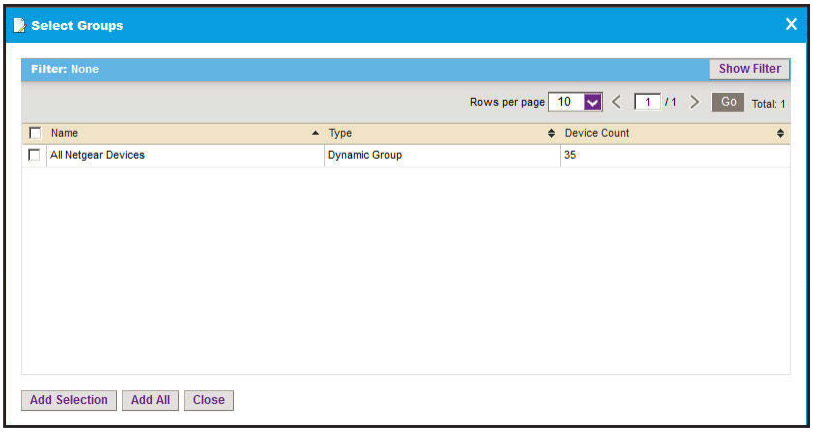
8. Add devices, device groups, or both:
   a. Click the **Add Device** button.



   b. Select devices to add and click the **Add Selection** button.

      To add all the devices in the table, click the **Add All** button.

   c. Click the **Add Group** button.



   d. Select device groups to add and click the **Add Selection** button.

      To add all the device groups in the table, click the **Add All** button.

   The selected devices, groups, or both, display in the Select Target Network Devices or Groups table.

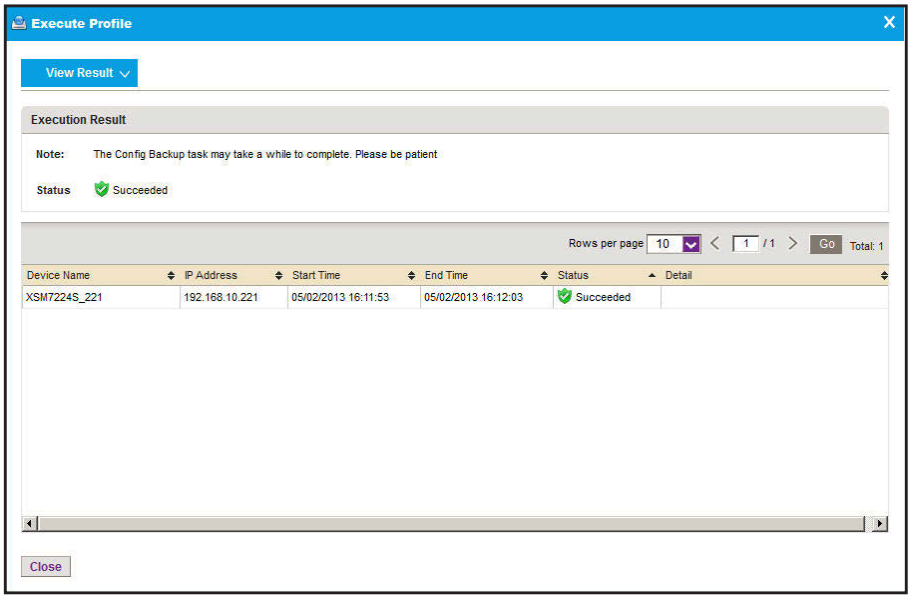
9. Click the **Save** button.

   The new or modified backup profile is saved and displays in the Backup screen.

10. Click the **Execute** button.

    Your backup profile is executed immediately.

A screen similar to the following displays.



The **Status** field displays the progress of the backup job. After the job completes successfully, the **Status** field displays **Succeeded**.

11. Click the **Close** button.

    The screen closes.

Restore the Configuration of a Single Device

You can restore the configurations of the devices that the application manages on your network, as follows:

- **Single device**. You can restore the configuration of a single device on your network. This procedure is described in this section.
- **Several identical devices**. You can use the configuration of one of the devices on your network to create a configuration template for several identical devices on your network. For more information, see the *NMS300 Network Management System Application User Manual*.

The Restore table (which you access by selecting **CONFIG > RESTORE**) displays the backup configuration files that the application adds after it backed up a configuration.

The application saves backup configuration files for the data retention period. For more information, see the *NMS300 Network Management System Application User Manual*.

If the configuration file that you need does not display in the Restore table, you can import the file into the application. For more information, see the *NMS300 Network Management System Application User Manual*.

CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that you select both the correct device type and correct device model for the configuration file that you upload to the application. If you provide the wrong configuration file, the application pushes the incorrect configuration file when it executes the configuration restore job and you can damage the device.

➢ **To restore a configuration to a single device:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

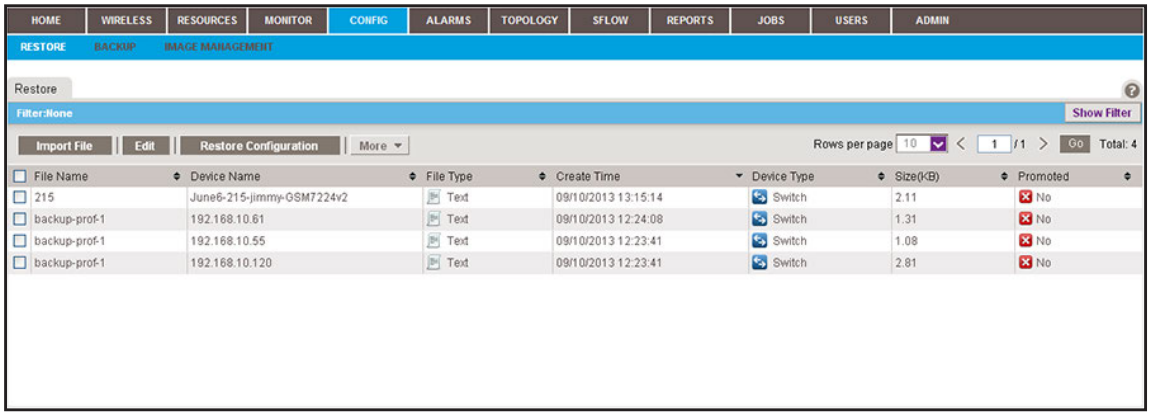
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **CONFIG > RESTORE**.



5. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

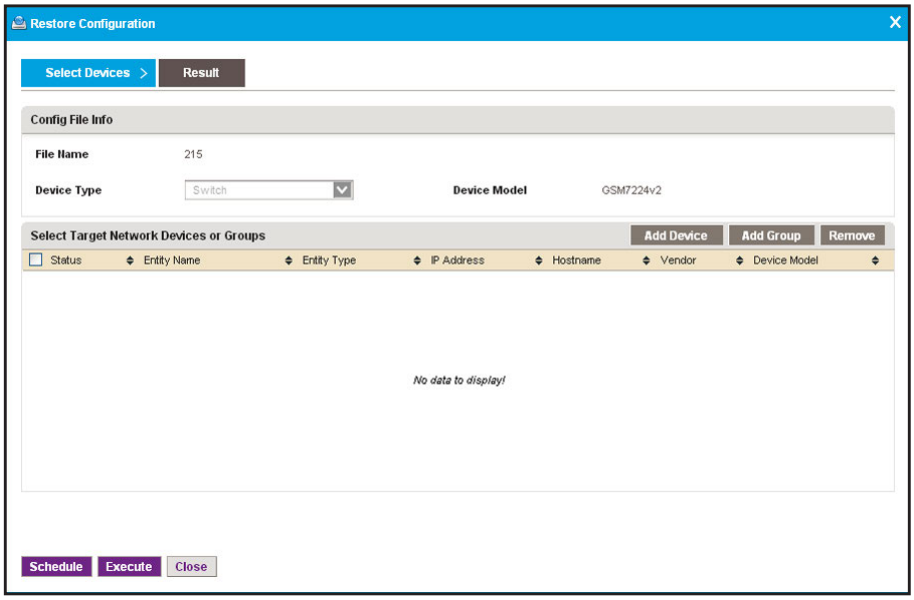
6. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

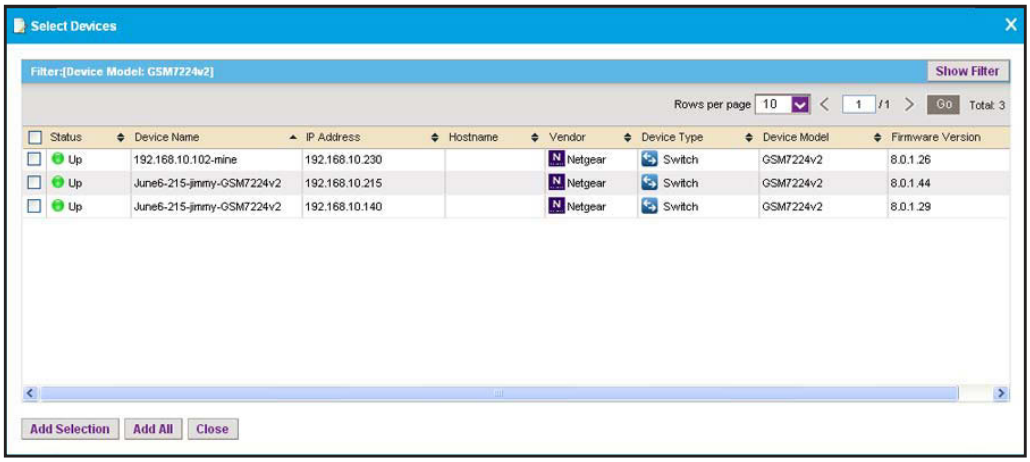
   To hide the filter, click the **Hide Filter** button.

7. Select the configuration file.

8. Click the **Restore Configuration** button.

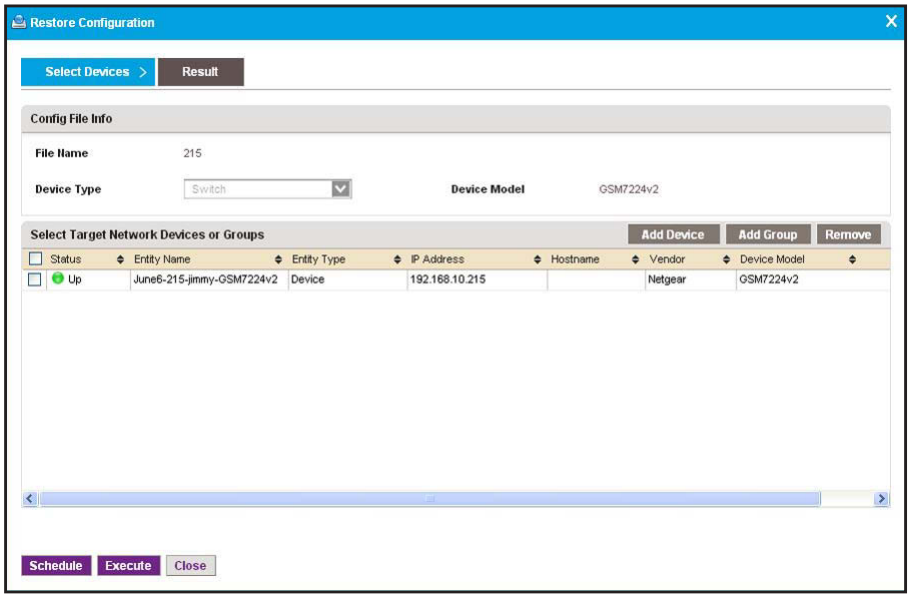


9. Click the **Add Device** button.



10. Select the device.
11. Click the **Add Selection** button.

The screen closes and the selected device is listed on the Restore Configuration screen.



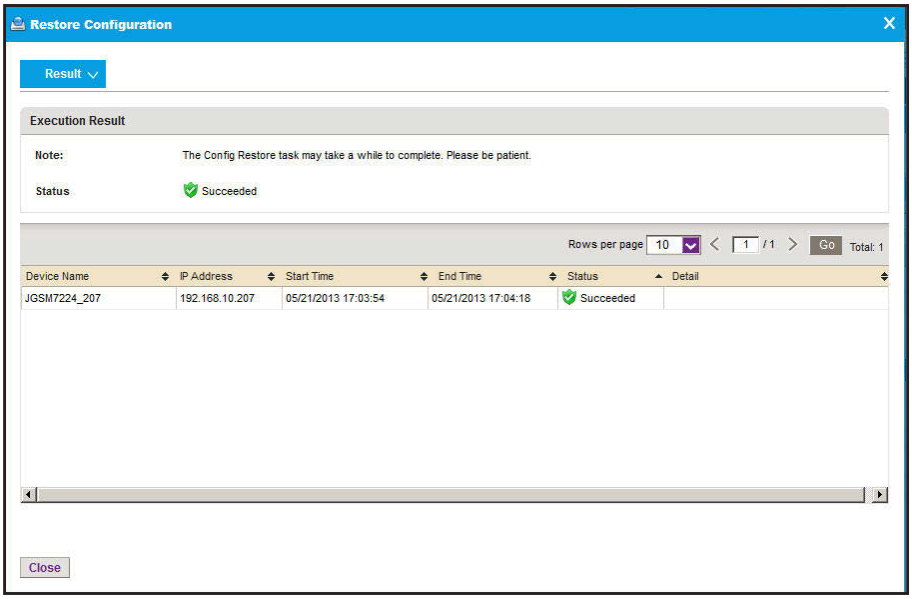
CAUTION:

Make sure that you select the correct device. Selecting the wrong device for the selected configuration file can damage the device.

12. Specify whether to restore the configuration file immediately or later by clicking one of the following buttons:

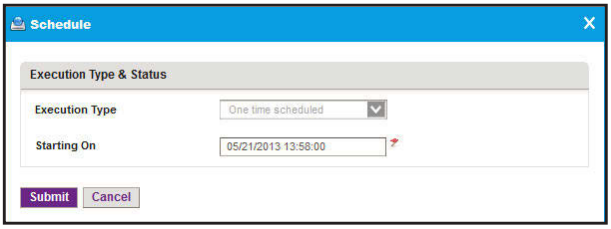
    - **Execute**. Restores the configuration file immediately.

      When the job completes, a screen similar to the following displays.



- **Schedule**. Lets you set up a schedule to restore the configuration file later.

  A screen similar to the following displays.



  a. Specify the time that you want the procedure to start.
  b. Click the **Submit** button.

     The restore procedure is executed once at the specified time.

Upgrade Firmware for One or More Devices

NETGEAR posts the latest firmware for each NETGEAR device on *support.netgear.com*. NETGEAR recommends that you visit this site regularly to see if new firmware is available.

CAUTION:

When you update the firmware of a device, you must provide the correct firmware file. Make sure that you select both the correct device type and correct device model for the firmware file that you upload to the application. If you provide the wrong firmware file, the application pushes out the incorrect firmware file while it executes the firmware upgrade and you can damage the device.

CAUTION:

When you update the firmware of stacked switches, make sure that all of the switches in the stack support the firmware that you select to update on the stack master.

The following sections describe the tasks that are related to firmware upgrades:

- *Import a Firmware File*
- *Execute or Schedule a Firmware Upgrade*

Import a Firmware File

After you download device firmware (an image) from the NETGEAR website at *support.netgear.com* to your computer, you can load the firmware file onto the NMS300 server.

If you want to use an MD5 file for error checking during the import process, first use an MD5 tool to generate an MD5 file that is based on the firmware file that you want to import.

➢ **To load a firmware file onto the NMS300 server:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.

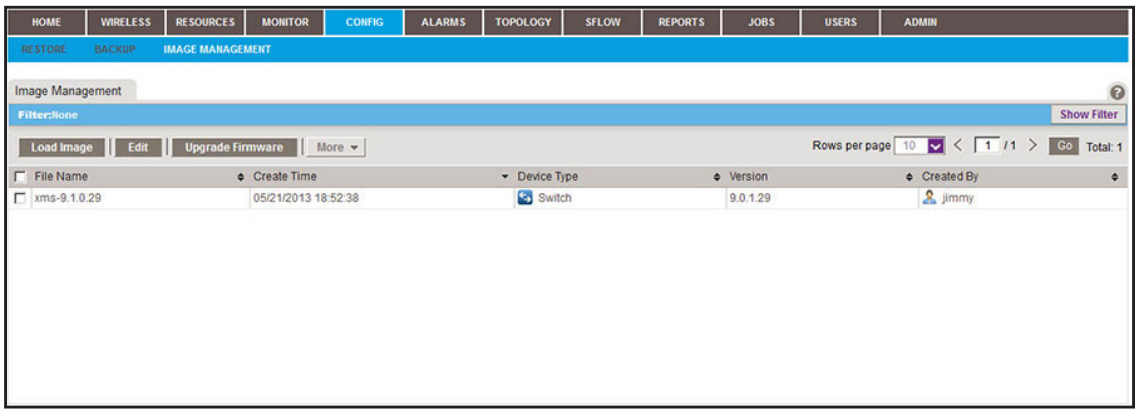
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.

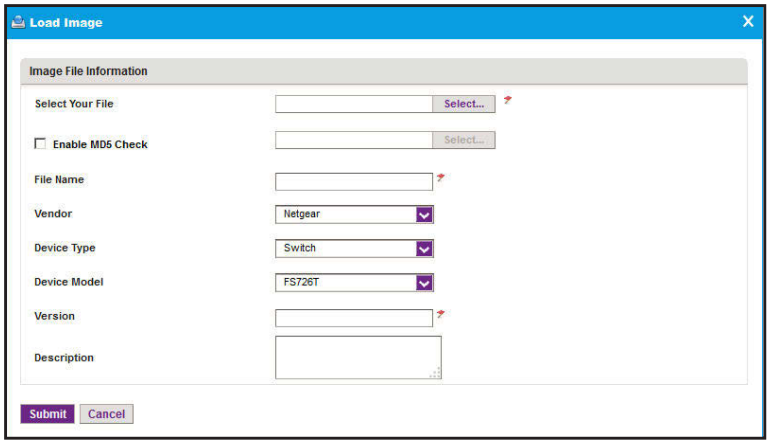
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **CONFIG > IMAGE MANAGEMENT**.



5. Click the **Load Image** button.



6. Specify the following information:
   - **Select Your File**. Click the **Select** button.

     To select the firmware from your computer, follow the directions of your browser.
   - **Enable MD5 Check**. To enable file validation with the Message Digest 5 algorithm, select this check box and click the **Select** button.

     To select the MD5 file from your computer, follow the directions of your browser.
   - **File Name**. Enter the name of the firmware file.
   - **Vendor**. Select the vendor of the device.
   - **Device Type**. Select the device type.
   - **Device Model**. Select the device model.
   - **Version**. Enter the version of the firmware file.
   - **Description**. Enter a description for the firmware file.
7. Click the **Submit** button.

   The firmware file is transferred from your computer to the NMS300 server.

   The imported firmware file is saved for the data retention period. For more information, see the *NMS300 Network Management System Application User Manual*.

Execute or Schedule a Firmware Upgrade

After you import a firmware file into the NMS300 server (see *Import a Firmware File* on page 74), you can execute a firmware upgrade immediately or schedule the application to execute a firmware upgrade later.

➢ **To execute or schedule a firmware upgrade:**

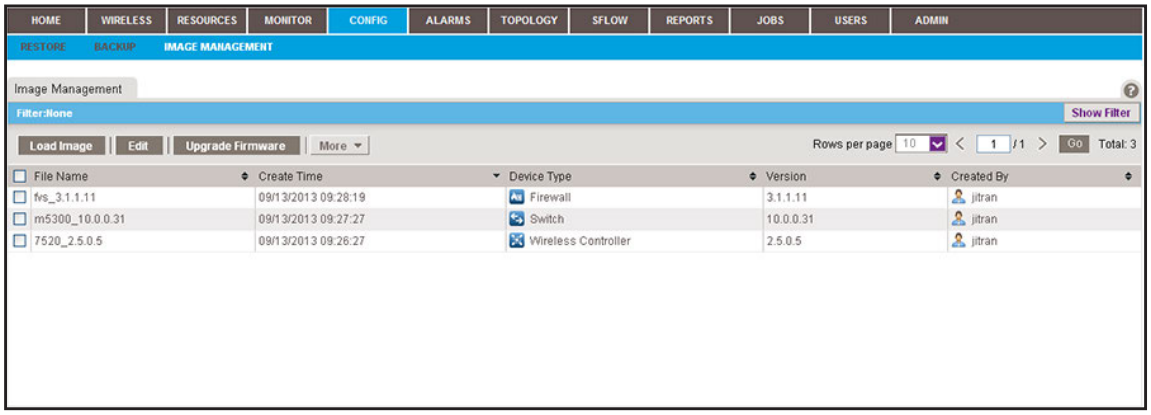
1. Open a browser and connect to the application through the static IP address of the NMS300 server.

   For more information, see *Log In to the Application* on page 13.
2. Enter your user name and password.

   The default administrator user name is **admin** and the default administrator password is also **admin**.
3. Click the **Sign In** button.

   The Network Summary screen displays.

4. Select **CONFIG > IMAGE MANAGEMENT**.



5. To add columns to or remove them from the Image Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

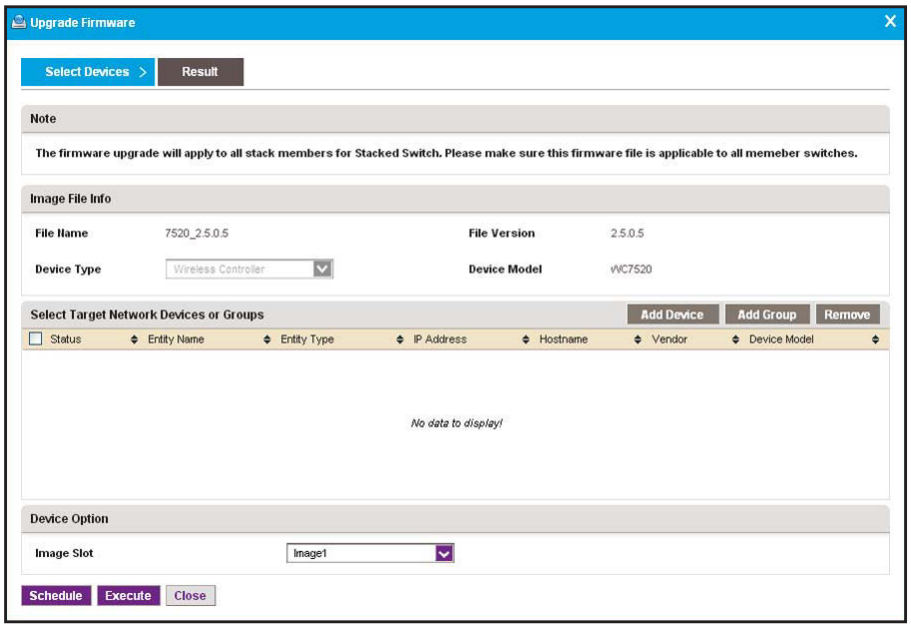
   You can choose from the following columns: File Name, Create Time, Device Type, Version, Created By, Vendor, Device Model, Size (MB), and Description.

6. To filter the firmware files that are listed, click the **Show Filter** button.

   You can filter the firmware files by criteria such as time range, device type, device model, and file name.

   To hide the filter, click the **Hide Filter** button.

7. Select the firmware file.
8. Click the **Upgrade Firmware** button.

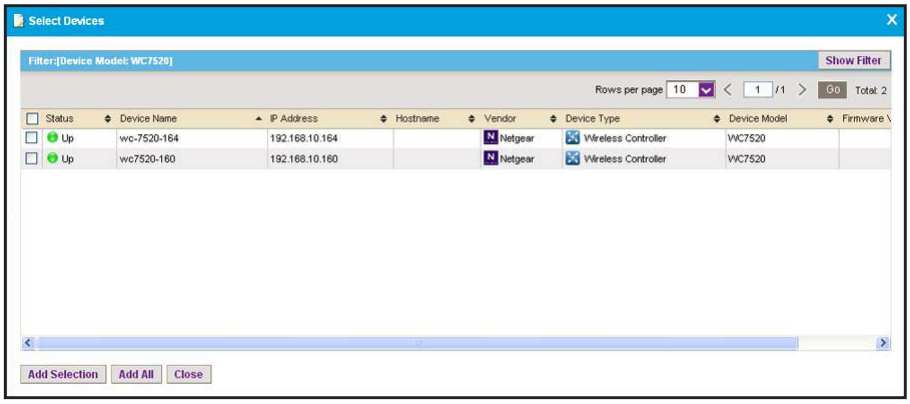


9. Select the target network devices or groups:

CAUTION:

Make sure that you select the correct devices or device groups. Selecting the wrong devices or device groups for the selected firmware file can damage the devices.

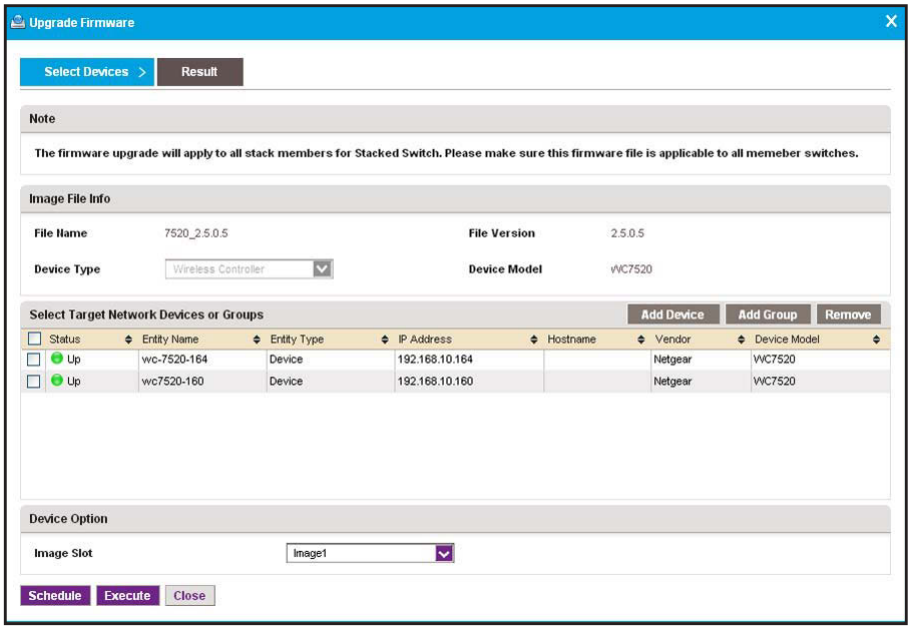
- To specify individual devices:
  a. Click the **Add Device** button.



  b. Select devices and click the **Add Selection** button.

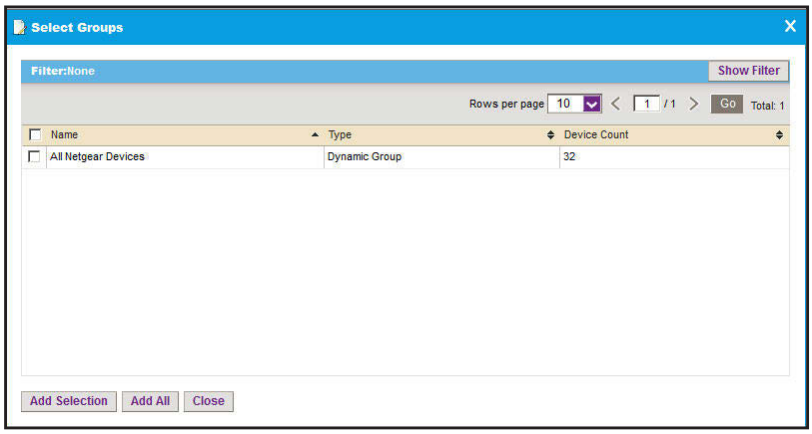
  To add all devices, click the **Add All** button.

  The screen closes and the selected device or devices are listed on the Upgrade Firmware screen.



- To specify device groups:

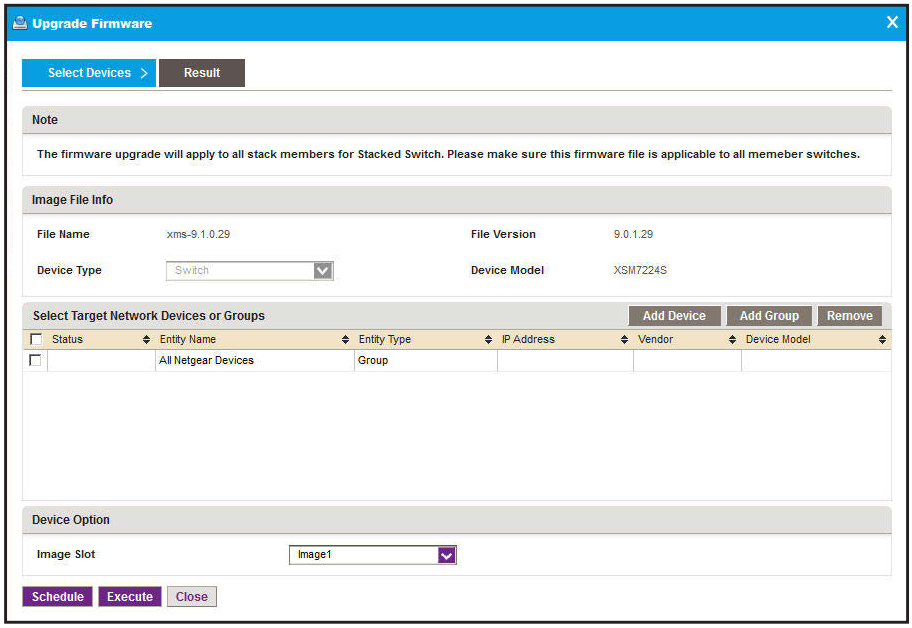
  a. Click the **Add Group** button.



  b. Select groups and click the **Add Selection** button.

  To add all groups, click the **Add All** button.

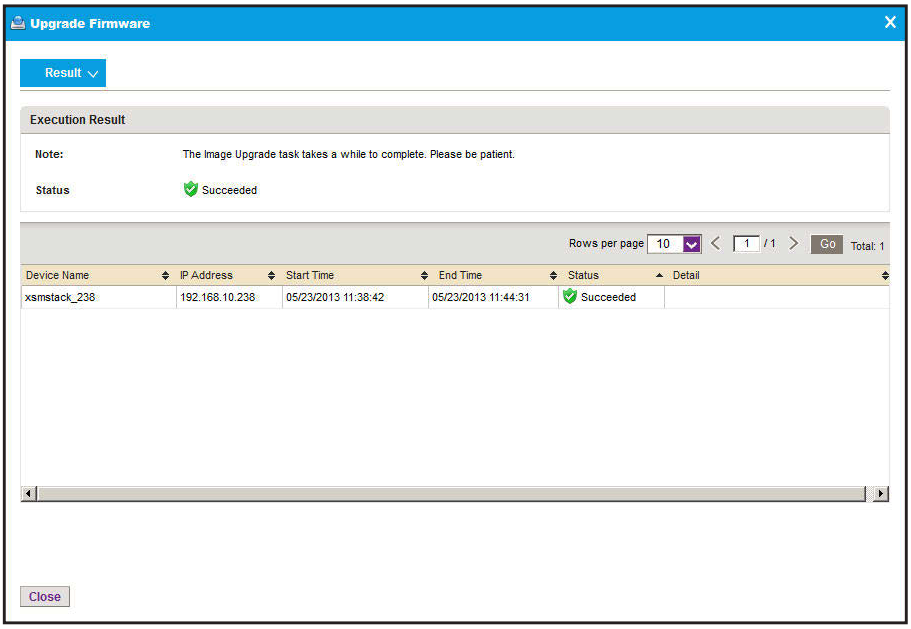
  The screen closes and the selected group or groups are listed on the Upgrade Firmware screen.



10. Specify whether to execute the firmware upgrade immediately or later by clicking one of the following buttons:

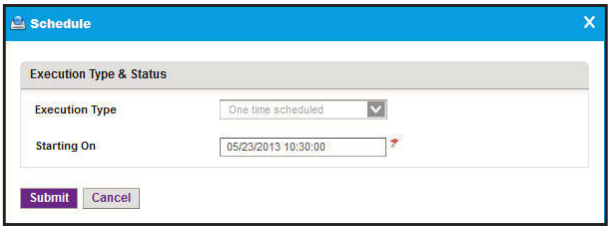
    - **Execute**. Upgrades the firmware immediately.

When the job completes, a Result screen similar to the following displays.



- **Schedule**. Lets you set up a schedule to upgrade the firmware later.

  A screen similar to the following displays.



  a. Specify the time that you want the upgrade to occur.

  b. Click the **Submit** button.

  The upgrade procedure is executed once at the specified time.