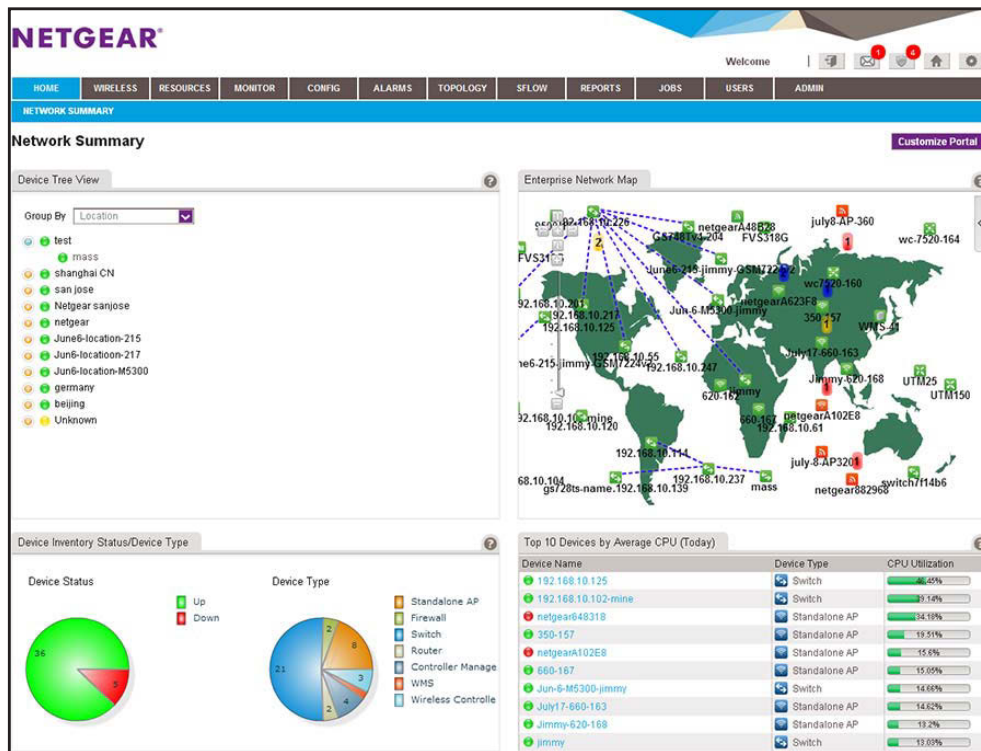




NMS300 Network Management System Application

User Manual



December 2014
202-11289-04

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

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 and web 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

© NETGEAR, Inc. NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-11289-04	December 2014	<ul style="list-style-type: none"> • Added support for the following platforms: <ul style="list-style-type: none"> - 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 (see View Device Details and Interface Details on page 85). • Added the option to enter an email address for notification of file backup results (see Add or Modify a Backup Profile on page 112). • 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 26 and Add or Modify an Alarm Notification Profile on page 171). 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 (see Chapter 8, Manage sFlow). • Added support for an external file storage server on which you can store backup files (see Set Up an External File Server on page 246 and Import and Export Configuration Files to an External File Server on page 145). • Added the capacity to support Chinese characters for device names.
202-11289-03	January 2014	<ul style="list-style-type: none"> • 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). • Added Chapter 14, Register Devices. • Added an Index.

NMS300 Network Management System Application

202-11289-02	October 2013	<ul style="list-style-type: none">• Revised the structure of the manual entirely.• Added support for wireless devices.• Added support for the FVS318G firewall.
202-11289-01	June 2013	First publication.

Contents

Chapter 1 Introduction

Network Environment Concepts	10
Device Groups	11
Types of Users	11
Compatible Devices	12
NETGEAR Managed Switches	12
NETGEAR Smart Switches	13
NETGEAR Firewalls	14
NETGEAR Wireless Access Points	14
NETGEAR Wireless Management Systems and Controllers	15
NETGEAR Storage Systems	15
Prepare the Network Devices for Discovery	15
What to Do Next	16

Chapter 2 Get Started

Log In to the Application	18
Change Your Password and Account Information	20
Change Your Password	20
Change Your Account Information	22
Configure the Email Server for Alerts and Alarm Notifications	23
Configure the General Email Server Settings	23
Configure Email Server Settings for a Gmail Account	25
Configure the SMS Server for Alerts and Alarm Notifications	26

Chapter 3 Discover and Manage Resources

Discovery Concepts	30
Use Quick Discovery to Discover Devices on Your Network	31
Use a Discovery Profile to Discover Devices on Your Network	33
Add or Modify a Device Credential	34
Add or Modify a Discovery Profile	37
Execute a Discovery Job	40
Schedule or Reschedule an Existing Discovery Job	42
Remove a Device Credential	45
Remove a Discovery Profile	46
View and Manage the Wired and Wireless Devices on Your Network	47
View Device Information	47
View Wireless Device Information Only	48
Modify the Name, Location Information, and Contact Information	52
Remove Device Information	53

Synchronize a Network Device	54
Log In to a Device	56
Ping, Perform a Traceroute, or Reboot a Device	57
Use the SNMP MIB Browser	59
View and Export the Inventory Table and Interface List Table	62
Manage Device Groups	63
Add or Modify a Static Device Group	63
Add or Modify a Dynamic Device Group	65
Remove a Device Group	67

Chapter 4 Monitor Devices and the Network

Monitor the Network	69
View the Default Network Summary	69
Customize the Network Summary Screen	70
Monitor the Top 10 Widgets for All Devices	74
View the Default Top 10 Widgets	74
Customize the Top 10 Screen	77
View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices	80
View the Wireless Summary and Default Top 10 Wireless Widgets	81
Customize the Wireless Summary Screen	83
View Device Details and Interface Details	85
Monitor Wireless Clients and View Client Details	89
Manage the Configuration Monitors	92
Configure an Individual Monitor	93
Disable a Monitor	95
Reenable a Monitor	96
View or Modify the Polling Interval for a Monitor	96
Customize the Optional Network Dashboard	97
Create or Modify a Dashboard View and Launch the Dashboard View	98
Remove a Dashboard View	102
Customize the Network Dashboard	103
View and Export Audit Logs	105
View Firmware Version Information	106
View the NMS300 Server Information	107
View Application Notifications	109

Chapter 5 Manage Configurations and Firmware

Back Up Your Device Configurations	112
Add or Modify a Backup Profile	112
Execute a Backup Job	115
Schedule a Backup Job	117
View the Execution Status of a Backup Job	120
Remove a Backup Profile	121
Restore Your Device Configurations	122
Restore the Configuration of a Single Device	123
Customize and Promote a Configuration File	127

Promote a Configuration File for an FVS318G Firewall	130
Restore the Configuration of Several Identical Devices	134
Import a Configuration File	138
Export a Configuration File	140
Modify a Configuration File	141
Remove a Configuration File	143
Compare Two Configuration Files	144
Import and Export Configuration Files to an External File Server	145
Upgrade Firmware for One or More Devices	148
Import a Firmware File	148
Execute or Schedule a Firmware Upgrade	150
Modify the File Name, Version Information, and Description for a Firmware File	154
Export a Firmware File	155
Remove a Firmware File	156

Chapter 6 Manage Alarms and Logs

View and Manage Alarms, Triggers, and Notification Profiles	159
View and Manage Current Alarms	159
View and Manage the Alarm History	161
View and Manage Alarm Configurations	163
Add a Custom Alarm Configuration	165
Modify an Alarm Configuration	168
View and Manage Alarm Notification Profiles	169
Add or Modify an Alarm Notification Profile	171
Customize Alarm Colors	174
View and Manage Network Event Notifications	176
View and Manage Device Traps	177
View and Manage Device System Logs	179

Chapter 7 Manage Maps and Topologies

View and Manage Maps	183
View a Hierarchical Map and Locate a Device	183
Manage a Hierarchical Map	186
Add a Childmap	188
Add Devices to a Map	191
Add a Link Between Devices on a Map	193
Customize the Style of a Link on a Map	196
View and Manage Network Topologies	198
Add a Topology View	199
View a Network Topology and Details About a Device	201
Manage a Topology View	203
Add a Link Between Devices on a Topology View	206
Customize the Style of a Node and Link on a Topology View	209
Remove a Topology View	212

Chapter 8 Manage sFlow

Set Up the sFlow Collection Server and Manage the sFlow Settings	215
Manage sFlow Sources	216
View and Export the Results of sFlow Monitoring	218

Chapter 9 Generate and View Reports

Manage Report Templates	221
Add or Modify a Report Template	221
Remove a Report Template	225
Generate and Schedule Reports	226
Generate a One-Time Report Immediately	226
Schedule a Report	228
View and Remove Saved Reports	230
View a Saved Report	230
Remove a Saved Report	231

Chapter 10 Manage Jobs

Schedule Jobs	234
View and Manage Jobs	234

Chapter 11 Manage Users and Security Profiles

Security Profile Concepts	238
Add a Security Profile	238
Modify or Remove a Security Profile	239
Add a User Profile to the User Base	241
Modify or Remove a User Profile	242
View and Log Off Online Users	244

Chapter 12 Customize Global Settings

Set Up an External File Server	246
Set the Data Retention Period	247
Set the Inventory Polling	249
Set the Idle Time-Out	251
Set the Real-time Chart	252
Change the Auto Refresh Setting	254

Chapter 13 Manage Licenses

View License Information	257
Register a License	258
Deregister a License	259

Chapter 14 Register Devices

Registration Concepts	262
---------------------------------	-----

Set Up and Validate Your Account Profile in the Application.	262
Set Up Your Account Profile for Device Registration	262
Validate and Retrieve Your Customer Account Information	264
Register One or More Devices.	265
Register All Devices.	268
Resynchronize Previously Registered Devices	270

Appendix A Technical Specifications

Appendix B Device Details

Switch Details.	275
Firewall Details.	276
Standalone AP Details.	277
Controller-Managed AP Details	278
Wireless Controller Details.	279
Wireless Managements System Details	280
Storage System Details.	281
Router Details.	282
Unknown Device Details.	283
Interface Details	283

Index

Introduction

1

Streamline network management tasks

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 manual is intended for network administrators.

This chapter covers the following topics:

- *Network Environment Concepts*
- *Compatible Devices*
- *Prepare the Network Devices for Discovery*
- *What to Do Next*

Note: In this manual, 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.

Network Environment Concepts

The application resides on the NMS300 server at a static IP address on the local area network. The application monitors the NETGEAR and third-party devices on the network.

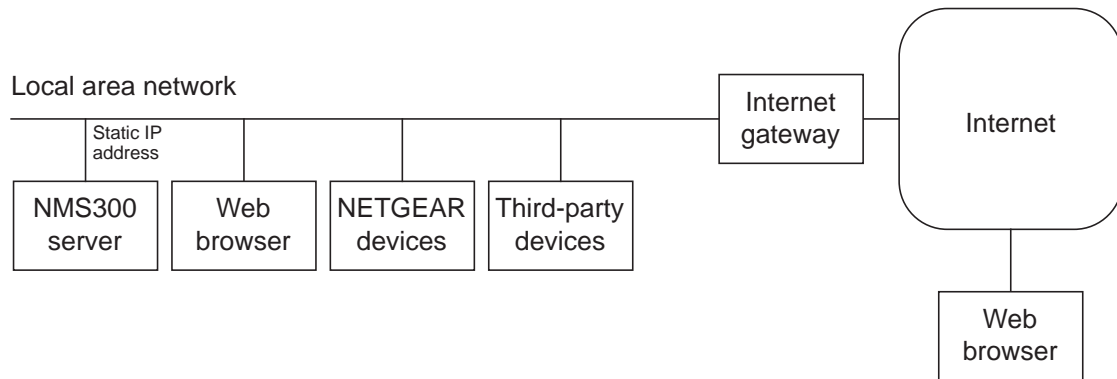


Figure 1. The Network Management System 300

You access the application through a web browser. The IP address for a web browser that is located outside the Internet gateway must be permitted to access the network.

The application supports the following devices:

- NETGEAR devices
 - For detailed information about the supported NETGEAR devices, including model numbers, see [Compatible Devices](#) on page 12.
- Third-party (non-NETGEAR) devices, including the following:
 - Routers
 - VoIP gateways
 - Hosts
 - Virtualization servers
- The managed NMS300 server

The application displays whether third-party devices are up or down. If a third-party device supports SNMP, the application uses SNMP MIBs to gather and present health and status information about the device.

Device Groups

To simplify the management of networks with many devices, you can create device groups. Group devices by vendor, location, device type, device model, and contact. Device groups are optional.

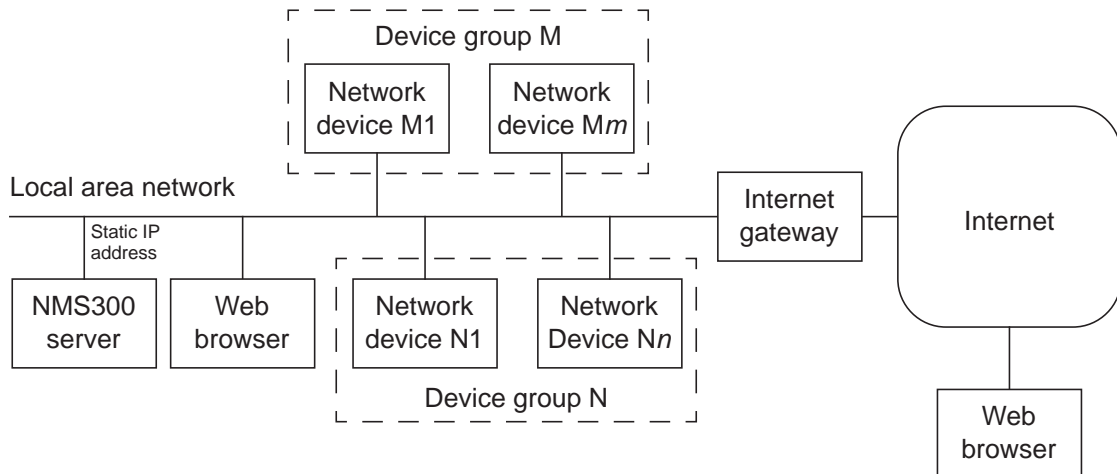


Figure 2. Device groups

You can create two types of device groups:

- **Static device groups.** A static group is a fixed list of specific devices. You must configure this list manually. For more information, see [Add or Modify a Static Device Group](#) on page 63.
- **Dynamic device groups.** A dynamic group is a dynamic list of devices that filter selection criteria determine. The list changes automatically as devices that meet the filter criteria are added to and removed from the network. For more information, see [Add or Modify a Dynamic Device Group](#) on page 65.

Types of Users

The application includes the following default user security profiles:

- **Admin.** A user who can perform administration-related functions. An admin user is authorized to perform all application functions. Only an admin user can modify and delete the default security profiles, can define new security profiles, and can add or remove user profiles.

For more information, see [Chapter 11, Manage Users and Security Profiles](#).

- **Operator.** A user who can manage the enterprise network functions, but cannot perform administration-related functions.
- **Observer.** A user who can only monitor and view enterprise network functions.

This manual is written for the admin user but also contains information that is useful for operators and observers.

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

Note: 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

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 or Modify a Device Credential](#) on page 34.

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.

What to Do Next

Before you can manage your network, you must perform certain basic configuration tasks and let the application find the devices that are on your network. These tasks are described in the following chapters:

- [Chapter 2, Get Started](#)
- [Chapter 3, Discover and Manage Resources](#)

2

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*
- *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. For more information about installing the application, see the *NMS300 Network Management Quick Start Guide*, which is available at downloadcenter.netgear.com.

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.

The screenshot displays the NETGEAR NMS300 Network Management System interface. The top navigation bar includes links for HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. The main content area is titled 'Network Summary' and contains several widgets:

- Device Tree View:** A tree structure showing devices grouped by location, including test, mass, shanghai CN, san jose, Netgear sanjose, netgear, Jun6-location-215, Jun6-location-217, Jun6-location-M5300, germany, beijing, and Unknown.
- Enterprise Network Map:** A world map showing the geographical distribution of network devices with labels for various devices and their IP addresses.
- Device Inventory Status/Device Type:** Two charts showing device status (Up/Down) and device types (Standalone AP, Firewall, Switch, Router, Controller Manage, WMS, Wireless Controller).
- Top 10 Devices by Average CPU (Today):** A table listing the top 10 devices by CPU utilization.

Device Name	Device Type	CPU Utilization
192.168.10.125	Switch	46.64%
192.168.10.102-mine	Switch	38.14%
netgear648318	Standalone AP	28.63%
350-157	Standalone AP	25.16%
660-167	Standalone AP	18.81%
Jimmy-620-168	Standalone AP	18.31%
620-162	Standalone AP	15.72%
Jun-6-M5300-jimmy	Switch	15.04%
July17-660-163	Standalone AP	13.19%
Jimmy	Switch	11.99%
- Top 10 Devices by Average Memory (Today):** A table listing the top 10 devices by memory utilization.

Device Name	Device Type	Memory Utilization
netgearA623F8	Standalone AP	91.85%
Jun-6-M5300-jimmy	Switch	89.62%
jimmy	Switch	87.63%
192.168.10.120	Switch	87.54%
netgear648318	Standalone AP	85.89%
192.168.10.61	Switch	82.3%
192.168.10.217	Switch	82.13%
192.168.10.55	Switch	81.26%
192.168.10.125	Switch	80.65%
June6-215-jimmy-GSM7224v2	Switch	80.24%
- Latest 10 Alarms:** A table showing recent alarms.

Alarm Name	Device Name	Severity	Alarm Time
Max station limitation reached	netgear648318	Major	09/05/2013 17:33:21
Device Memory utilization is ov...	netgearA623F8	Minor	09/05/2013 17:20:01

For more information about the Network Summary screen, see [Monitor the Network](#) on page 69.

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 *Chapter 11, Manage Users and Security Profiles*.

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 18.

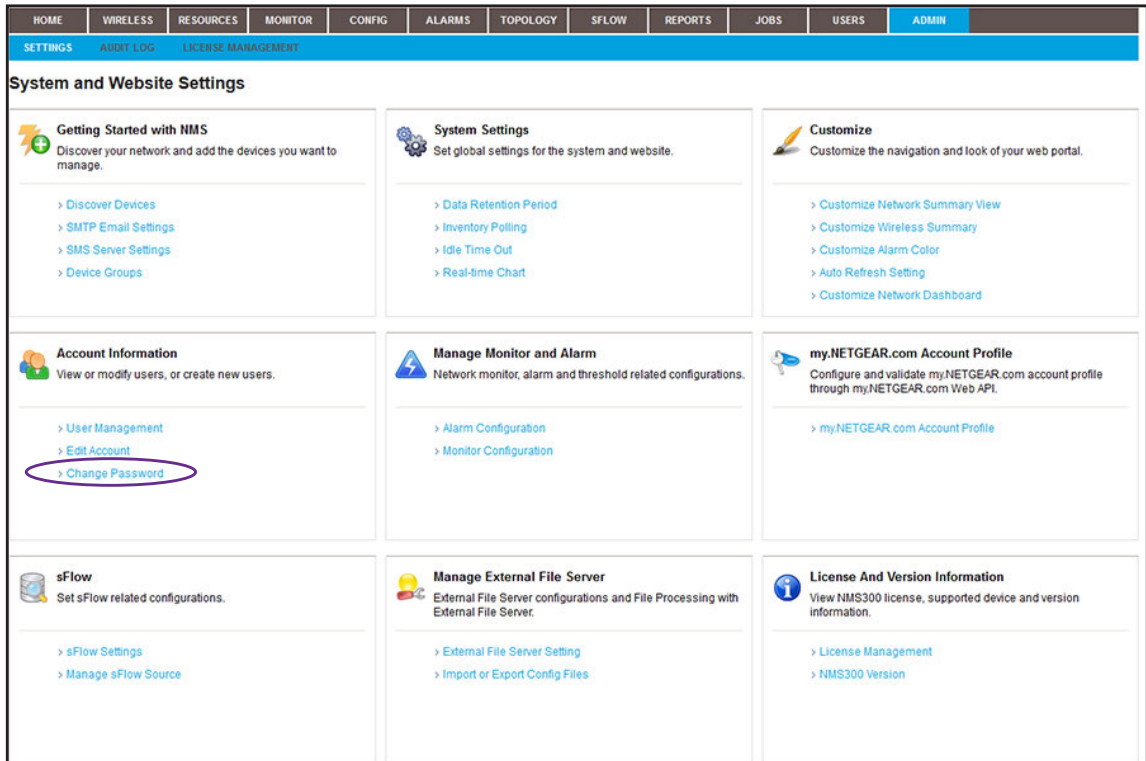
2. Enter your user name and password.

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.

The screenshot shows the "Change My Password" dialog box. It has a title bar with "Change My Password" and a close button (X). The main area contains three input fields:

- Old Password
- New Password
- Re-type New Password

At the bottom, there are two buttons: "Submit" and "Cancel".

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 18.

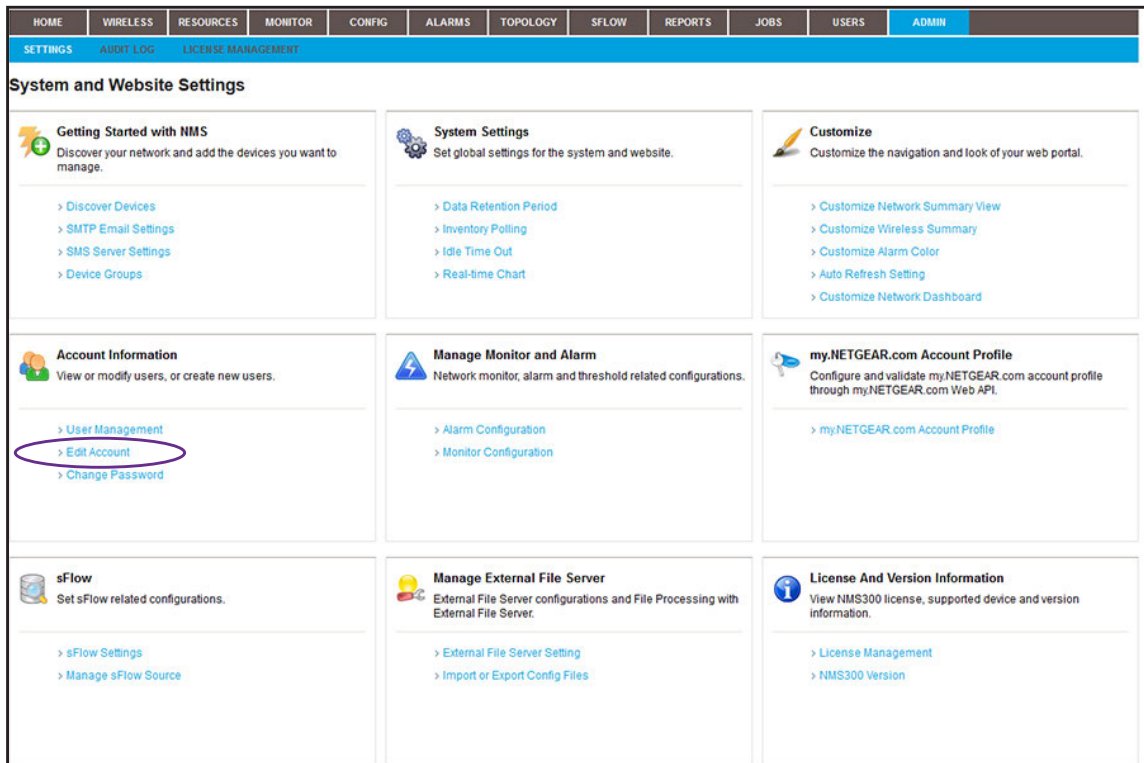
2. Enter your user name and password.

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.

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.

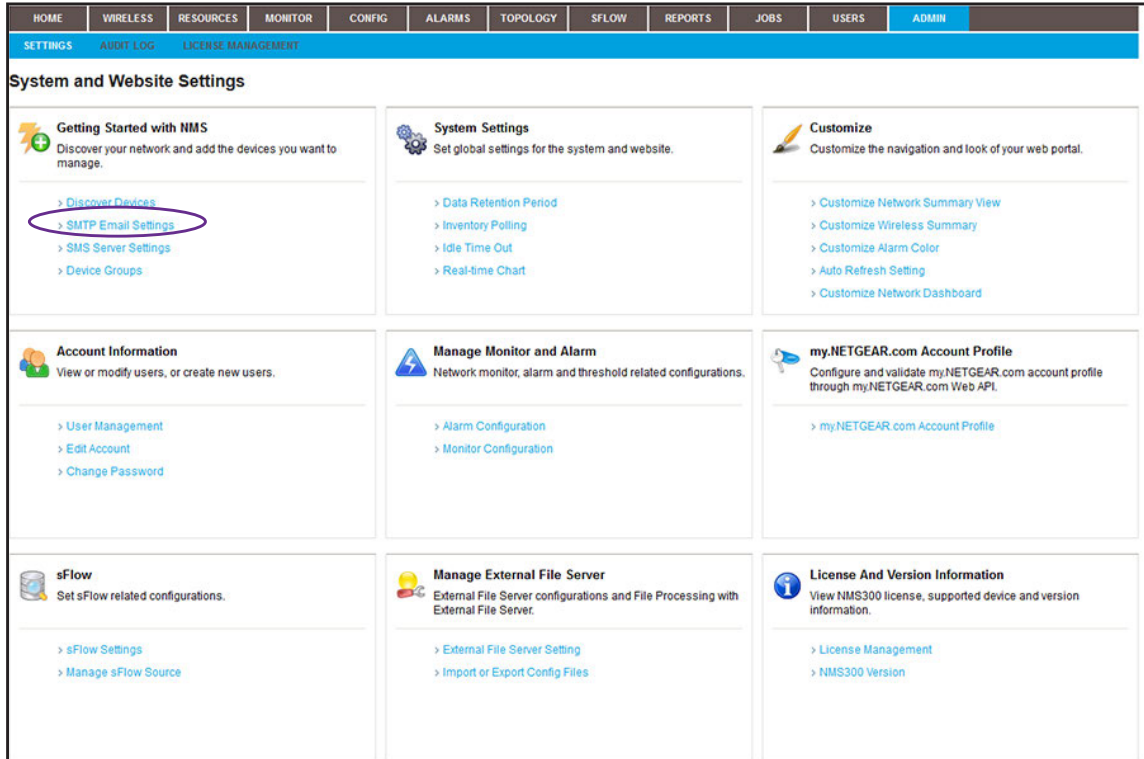
Note: For information about adding an alarm notification profile with an email address to which the application can send a notification, see [Add or Modify an Alarm Notification Profile](#) on page 171.

Configure the General Email Server Settings

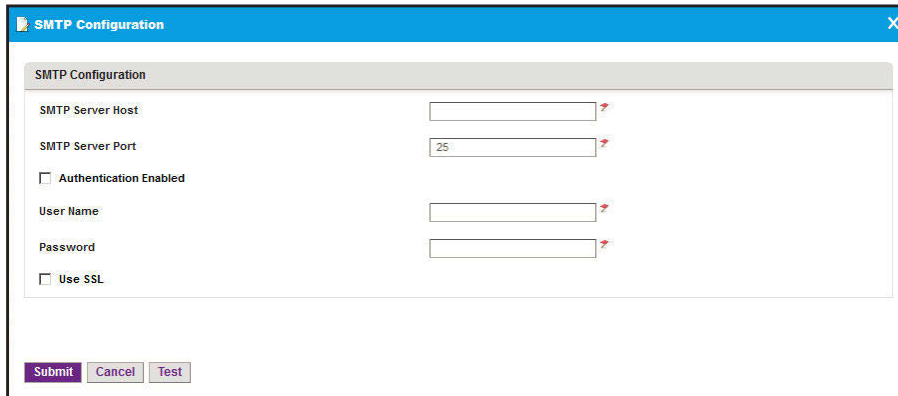
The following procedure describes how to configure the general email server settings.

- **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 18.
 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.

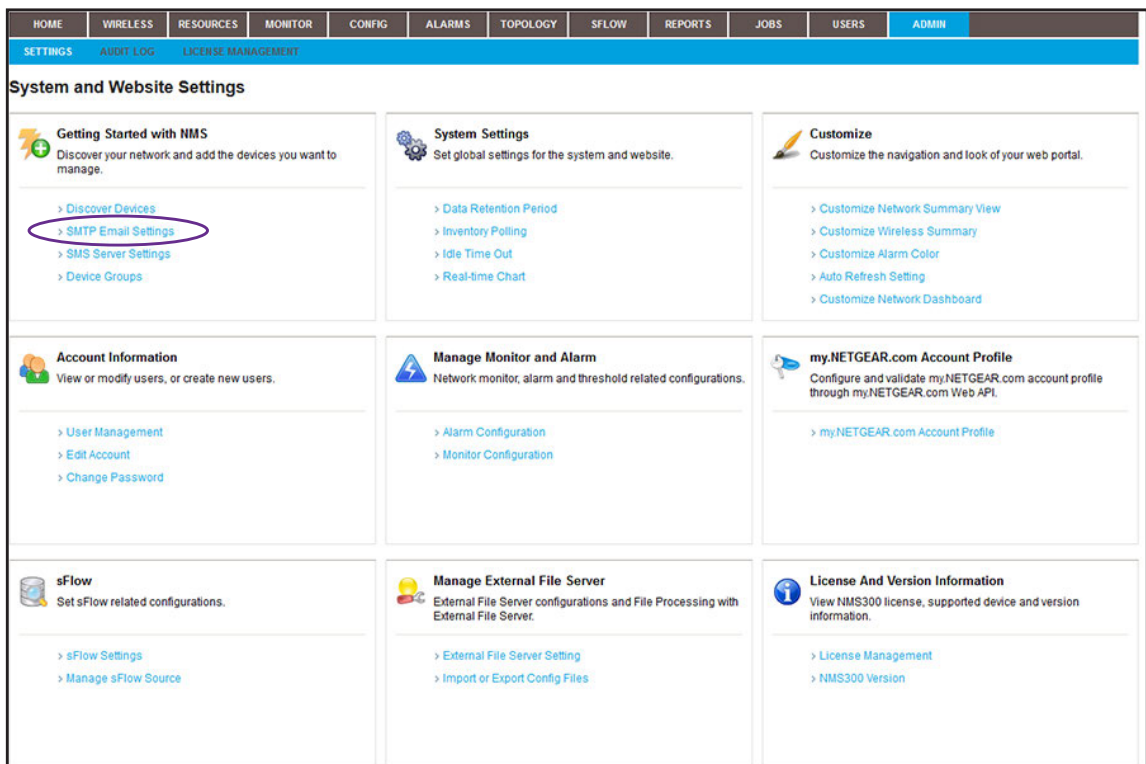
10. To use a secure email connection, select the **Use SSL** check box, and in the **SMTP Server Port** field, enter the port number for the SSL connection.
11. Click the **Test** button.
Your SMTP configuration settings are verified.
12. Click the **Submit** button.
Your changes are saved.

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 18.
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**.



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

- 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.
- To use a secure email connection, select the **Use SSL** check box, and in the **SMTP Server Port** field, enter **465**.
- Click the **Test** button.
Your SMTP configuration settings are verified.
- 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 or Modify an Alarm Notification Profile](#) on page 171.

➤ **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 18.

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.

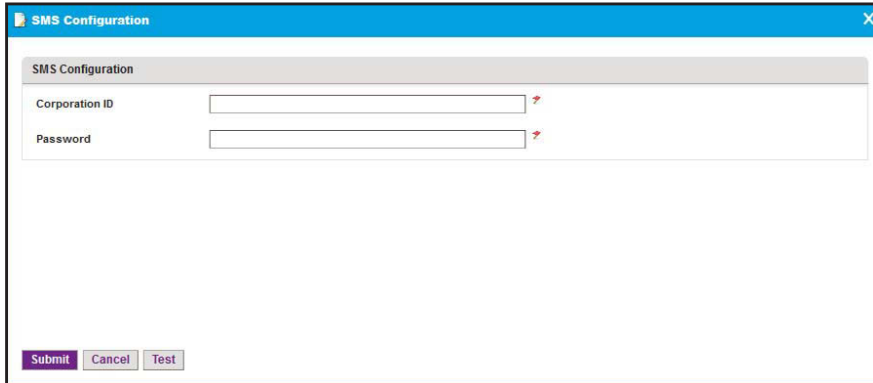
The Network Summary screen displays.

5. Select **ADMIN > SETTINGS**.

The screenshot shows the NMS300 Network Management System Application interface. The top navigation bar includes tabs for HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. The ADMIN tab is selected. Below the navigation bar, the 'SETTINGS' section is active, and the 'SYSTEM MANAGEMENT' sub-section is visible. The main content area is titled 'System and Website Settings' and is organized into a grid of nine panels:

- Getting Started with NMS:** Discover your network and add the devices you want to manage. Links include Discover Devices, SMTP Email Settings (circled in red), SMS Server Settings (circled in red), and Device Groups.
- System Settings:** Set global settings for the system and website. Links include Data Retention Period, Inventory Polling, Idle Time Out, and Real-time Chart.
- Customize:** Customize the navigation and look of your web portal. Links include Customize Network Summary View, Customize Wireless Summary, Customize Alarm Color, Auto Refresh Setting, and Customize Network Dashboard.
- Account Information:** View or modify users, or create new users. Links include User Management, Edit Account, and Change Password.
- Manage Monitor and Alarm:** Network monitor, alarm and threshold related configurations. Links include Alarm Configuration and Monitor Configuration.
- my.NETGEAR.com Account Profile:** Configure and validate my.NETGEAR.com account profile through my.NETGEAR.com Web API. Link includes my.NETGEAR.com Account Profile.
- sFlow:** Set sFlow related configurations. Links include sFlow Settings and Manage sFlow Source.
- Manage External File Server:** External File Server configurations and File Processing with External File Server. Links include External File Server Setting and Import or Export Config Files.
- License And Version Information:** View NMS300 license, supported device and version information. Links include License Management and NMS300 Version.

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



The screenshot shows a window titled "SMS Configuration" with a close button in the top right corner. The window contains a form with two input fields: "Corporation ID" and "Password". Each input field has a red question mark icon to its right. At the bottom of the window, there are three buttons: "Submit", "Cancel", and "Test".

- 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.
- Enter the password for accessing the SMS gateway.
This is the password that NETGEAR support gave you.
- Click the **Test** button.
Your SMS configuration settings are verified.
- Click the **Submit** button.
Your changes are saved.

3

3. Discover and Manage Resources

Find and manage the devices on your network

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*
- *View and Manage the Wired and Wireless Devices on Your Network*
- *Manage Device Groups*

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 18.

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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
disc-frs-147.250	No	Not Recurrent			
disc-frs-hostname	No	Not Recurrent	08/29/2013 11:15:00	Succeeded	
disc-wan-ip	No	Not Recurrent	09/05/2013 14:15:00	Succeeded	

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

Name	Protocol	Port	Timeout(sec)	Retries
Default SNMP	SNMP V2C	161	10	1
Default HTTP	HTTP	80	6	1
Default Telnet	Telnet	23	10	1
Default HTTPS	HTTPS	443	6	1
Default FVS3180 HTTPS	HTTPS	8080	6	1

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 selecting 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.

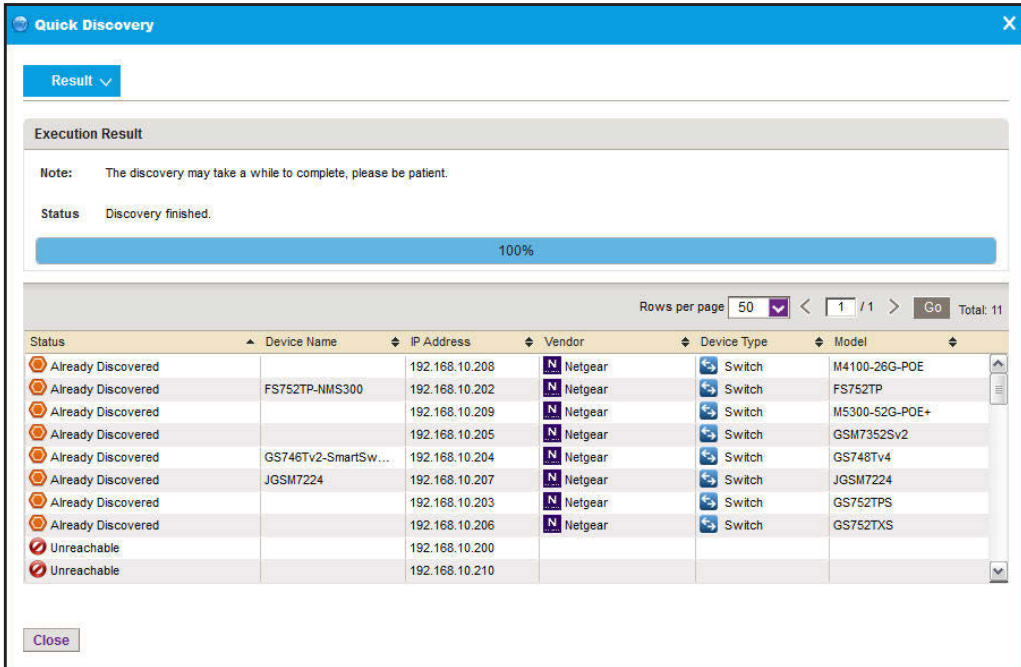
8. If the credential that you need is not listed in the table, do the following:
 - a. Click the **Add** button.

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 or Modify a Device Credential](#) on page 34.
 - 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 or Modify a Device Credential](#) on page 34.

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 or Modify a Device Credential](#)
2. [Add or Modify a Discovery Profile](#)
3. [Execute a Discovery Job](#) or [Schedule or Reschedule an Existing Discovery Job](#)

Add or Modify 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 a NETGEAR FVS318G firewall over HTTPS. (The NETGEAR FVS318N, FVS336Gv2, FVS336Gv3, and SRX5308 firewalls use an SNMP device credential.)

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 or modify an existing 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 18.

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**.

Name	Protocol	Port	Timeout(sec)	Retries
Default FVS318G HTTPS	HTTPS	8080	6	1
Default HTTP	HTTP	80	6	1
Default HTTPS	HTTPS	443	6	1
Default SNMP	SNMP V2C	161	10	1
Default Telnet	Telnet	23	10	1
non-def-215-tel-password1	Telnet	23	10	1
non-def-tel-209-password3	Telnet	23	10	1
non-default-215-telnet	Telnet	23	10	1
non-default-M5300	Telnet	23	10	1
telnet-217-non-default	Telnet	23	10	1

5. Add a device credential or modify an existing device credential:
 - To add a device credential, click the **Add** button.
 - To modify an existing device credential:
 - a. From the Device Credentials table, select a device credential.
 - b. Click the **Edit** button.

For a new device credential, the Add Credential screen displays. For an existing device credential, the Edit Credential screen displays.

6. In the Credential General Info section, enter or modify 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 or modify 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.

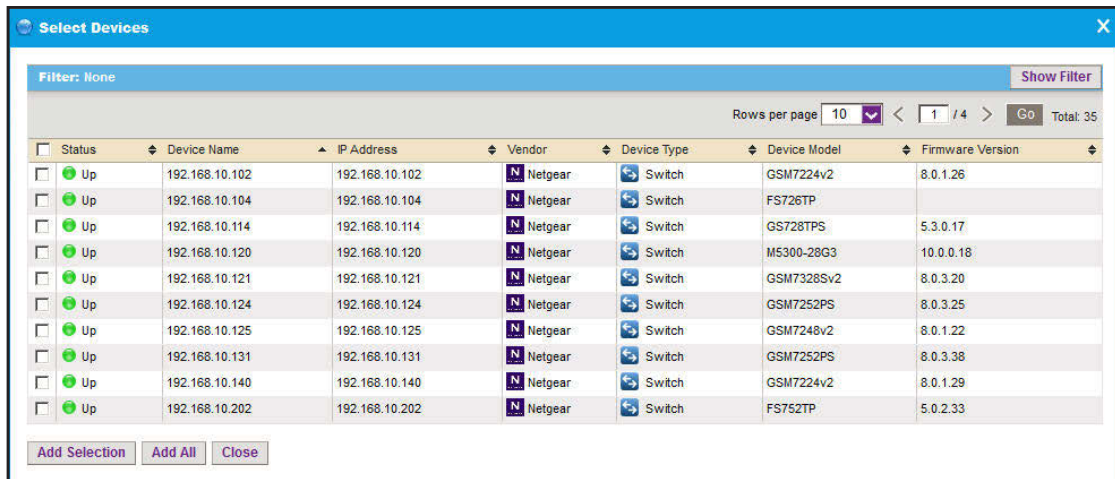
The screenshot shows the 'Add Credential' dialog box with the 'Management Interface' tab selected. The dialog has three tabs: 'Authentication', 'Management Interface', and 'Associated Devices'. The 'Management Interface' tab is active, showing a form with three input fields: 'Port' (value: 161), 'Timeout(sec)' (value: 5), and 'Retries' (value: 2). Each field has a red arrow icon to its right. At the bottom of the dialog are four buttons: 'Previous', 'Next', 'Save', and 'Cancel'.

10. Enter or modify the port number, time-out period in seconds, and the number of retries.

11. Click the **Associated Devices** tab.

The screenshot shows the 'Add Credential' dialog box with the 'Associated Devices' tab selected. The dialog has three tabs: 'Authentication', 'Management Interface', and 'Associated Devices'. The 'Associated Devices' tab is active, showing a table with columns: 'Status', 'Device Name', 'IP Address', 'Vendor', 'Device Type', and 'Device Model'. There are 'Add' and 'Remove' buttons to the right of the table header. The table is currently empty, displaying the message 'No data to display!'. At the bottom of the dialog are four buttons: 'Previous', 'Next', 'Save', and 'Cancel'.

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. If you are modifying an existing device credential, to remove devices:

- a. Select the devices.
- b. Click the **Remove** button.

The devices are removed from the Associated Devices table.

15. Click the **Save** button.

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

Add or Modify 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 or modify an existing 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 18.

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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> disc-fvs-147.250	<input checked="" type="checkbox"/> No	Not Recurrent			
<input type="checkbox"/> disc-fvs-hostname	<input checked="" type="checkbox"/> No	Not Recurrent	08/29/2013 11:15:00	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> disc-wan-ip	<input checked="" type="checkbox"/> No	Not Recurrent	09/05/2013 14:15:00	<input checked="" type="checkbox"/> Succeeded	

The screen displays the existing discovery profiles.

5. Add a discovery profile or modify an existing discovery profile:

- To add a discovery profile, click the **Add Profile** button.
- To modify an existing discovery profile:
 - a. From the Network Discovery table, select a discovery profile.
 - b. Click the **Edit Profile** button.

For a new discovery profile, the Add Profile screen displays. For an existing discovery profile, the Edit Profile screen displays.

Add Profile

General > Network Result

General Info

Name: Description:

Discovery Options

Resolve Host Names (Attempt to resolve host name to IP Address)

ICMP Ping Devices (Ping devices before authentication)

Discovery Filters

Vendor: Location: Device Type: Switch

Discovery Includes

ICMP Only Devices (Discover devices that only respond to Ping)

Unclassified Devices (Discover devices that from unknown vendors)

LLDP Option

Enable LLDP Link Discovery (Automatically discover LLDP links)

Previous Next Add Schedule Save Execute Close

6. Enter or modify 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.

Select Network Type and Addresses

IP Range

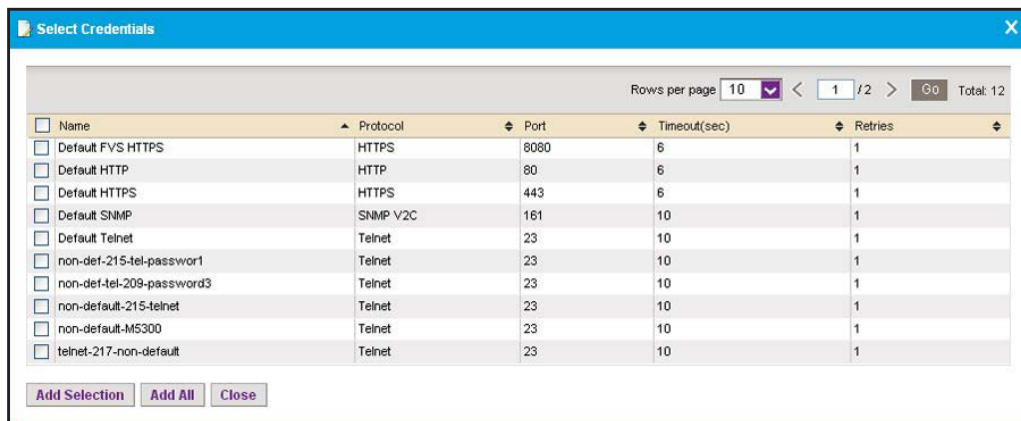
Select Credentials

<input type="checkbox"/> Name	Protocol	Port	Timeout(sec)	Retries
<input type="checkbox"/> Default SNMP	SNMP V2C	161	10	1
<input type="checkbox"/> Default HTTP	HTTP	80	6	1
<input type="checkbox"/> Default Telnet	Telnet	23	10	1
<input type="checkbox"/> Default HTTPS	HTTPS	443	6	1
<input type="checkbox"/> Default FVS HTTPS	HTTPS	8080	6	1

Buttons: Previous, Next, Add Schedule, Save, Execute, Close

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 or modify 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 or Modify a Device Credential](#) on page 34.

- 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.

➤ 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 18.

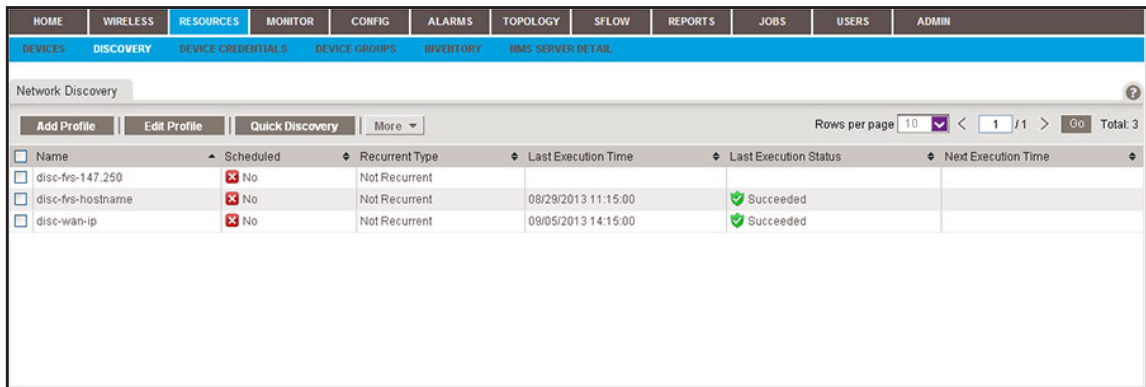
2. Enter your user name and password.

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

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

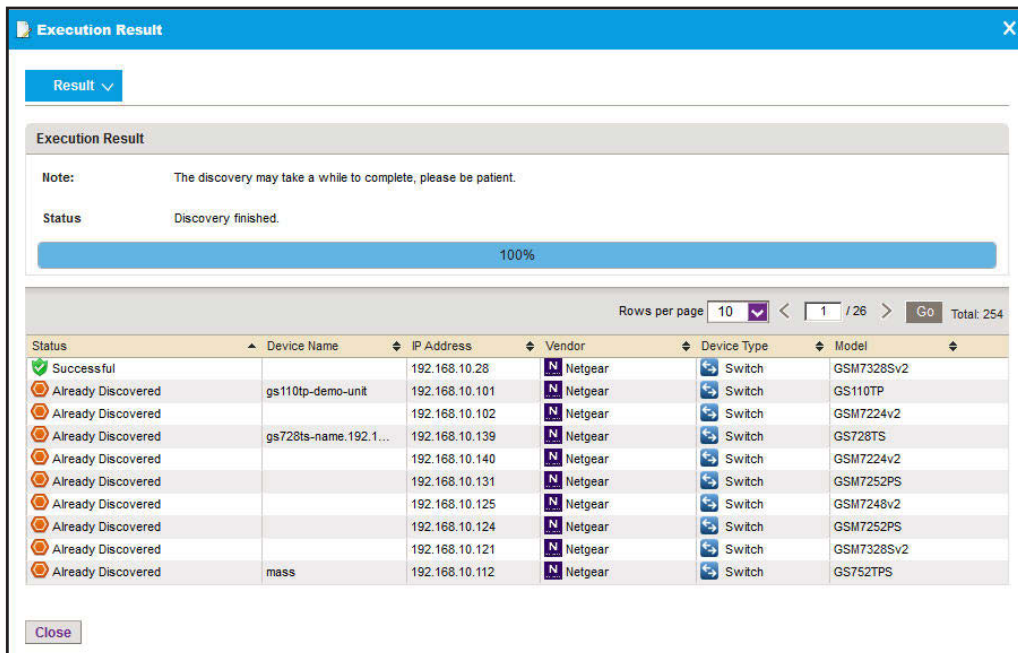
The Network Summary screen displays.

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 [Set the Data Retention Period](#) on page 247.

Schedule or Reschedule an Existing Discovery Job

You can schedule or reschedule an existing discovery job to occur later. This discovery job can be one time or recurrent.

➤ **To schedule or reschedule an existing discovery job for future execution:**

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 18.

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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> disc-fvs-147.250	<input checked="" type="checkbox"/> No	Not Recurrent			
<input type="checkbox"/> disc-fvs-hostname	<input checked="" type="checkbox"/> No	Not Recurrent	08/29/2013 11:15:00	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> disc-wan-ip	<input checked="" type="checkbox"/> No	Not Recurrent	09/05/2013 14:15:00	<input checked="" type="checkbox"/> Succeeded	

The screen lists the existing discovery profiles in the application.

5. Select the discovery profile.

- Click the **Edit Profile** button.

- Take one of the following actions:
 - To add a new schedule, click the **Add Schedule** button.
 - To modify an existing schedule, click the **Edit Schedule** button.

- From the **Enable** menu, select **Yes**.

The screen adjusts to display more fields.

The screenshot shows a 'Schedule' dialog box with the following fields:

- Execution Type & Status:**
 - Enable: Yes (dropdown)
 - Execution Type: One time scheduled (dropdown)
- Starting On:**
 - Starting On: 09/27/2013 18:01:00 (calendar icon)
- Buttons:** Submit, Cancel

9. Specify whether the application executes the discovery job once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering or modifying the corresponding information:

- **One time scheduled.** This is the default selection.

In the **Starting On** field, enter or modify the date and time.

- **Recurrent.** The screen adjusts to display more fields.

The screenshot shows a 'Schedule' dialog box with the following fields:

- Execution Type & Status:**
 - Enable: Yes (dropdown)
 - Execution Type: Recurrent (dropdown)
- Starting On:**
 - Starting On: 04/30/2013 14:59:00 (calendar icon)
- Recurrence:**
 - Recurrence Type: Weekly (dropdown)
 - Day of the Week: Monday Tuesday Wednesday Thursday Friday Saturday Sunday
- Stopping On:**
 - End Time: []
 - Never
- Buttons:** Submit, Cancel

Enter or modify the following information:

- a. In the **Starting On** field, enter or modify the date and time.
- b. From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.

- c. Select the **End Time** radio button and enter or modify the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.

10. Click the **Submit** button.

The Schedule screen closes. The discovery job schedule becomes part of the discovery profile.

11. On the Edit Profile screen, click the **Save** button.

Your discovery job is executed according to the schedule that you set.

Note: Output files from completed resource discovery jobs are saved for the data retention period. For more information, see [Set the Data Retention Period](#) on page 247.

Remove a Device Credential

You can remove a device credential that you no longer need.

➤ **To remove 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 18.

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**.

Name	Protocol	Port	Timeout(sec)	Retries
<input type="checkbox"/> Default FVS318G HTTPS	HTTPS	8080	6	1
<input type="checkbox"/> Default HTTP	HTTP	80	6	1
<input type="checkbox"/> Default HTTPS	HTTPS	443	6	1
<input type="checkbox"/> Default SNMP	SNMP V2C	161	10	1
<input type="checkbox"/> Default Telnet	Telnet	23	10	1
<input type="checkbox"/> non-def-215-tel-password1	Telnet	23	10	1
<input type="checkbox"/> non-def-tel-209-password3	Telnet	23	10	1
<input type="checkbox"/> non-default-215-telnet	Telnet	23	10	1
<input type="checkbox"/> non-default-M5300	Telnet	23	10	1
<input type="checkbox"/> telnet-217-non-default	Telnet	23	10	1

5. Select the device credential.

6. Click the **Delete** button.
A pop-up confirmation screen displays.
7. Click the **Yes** button.
The device credential is removed from the Device Credentials table and deleted.

Remove a Discovery Profile

If you delete a discovery job from the Jobs table, the application deletes the discovery profile for the job automatically. For more information, see [View and Manage Jobs](#) on page 234. You can also remove a discovery profile manually.

➤ **To remove a discovery profile manually:**

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 18.
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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
disc-fvs-147.250	No	Not Recurrent			
disc-fvs-hostname	No	Not Recurrent	08/29/2013 11:15:00	Succeeded	
disc-wan-ip	No	Not Recurrent	09/05/2013 14:15:00	Succeeded	

5. Select the discovery profile.
6. From the **More** menu, select **Delete**.
A pop-up confirmation screen displays.
7. Click the **Yes** button.
The discovery profile is removed from the Network Discovery table and deleted.

View and Manage the Wired and Wireless Devices on Your Network

After the application discovers the wired and wireless devices on your network and adds them to the inventory database, you can view and test the devices. The following sections describe the tasks that you can perform:

- *View Device Information*
- *View Wireless Device Information Only*
- *Modify the Name, Location Information, and Contact Information*
- *Remove Device Information*
- *Synchronize a Network Device*
- *Log In to a Device*
- *Ping, Perform a Traceroute, or Reboot a Device*
- *Use the SNMP MIB Browser*
- *View and Export the Inventory Table and Interface List Table*

The application polls the devices to make sure that they are still on the network. You can change how frequently the device inventory is polled. For more information, see *Set the Inventory Polling* on page 249.

View Device Information

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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:f0:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c8:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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.

For more information, see [View Device Details and Interface Details](#) on page 85.

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.

Note: For information about viewing wireless clients of wireless controllers, APs, and management systems, see [Monitor Wireless Clients and View Client Details](#) on page 89.

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 18.

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**.

Status	Device Name	IP Address	Hostname	Managed By	MAC Address	Location	Device Model
Up	9500-161-sept10	192.168.10.161		IP Address	28:c6:8e:2d:c5:f1	Netgear sanjose	WC9500
Up	wc-7520-164	192.168.10.164		IP Address	e0:91:f5:1f:8d:e5		WC7520
Up	wc7520-160	192.168.10.160		IP Address	e0:91:f5:97:71:59		WC7520

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 Details and Interface Details](#) on page 85.

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 18.

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**.

Status	Device Name	Associated Controller	IP Address	Hostname	Managed By	MAC Address	Location	Device Type	Device Model
Up	350-157		192.168.10.157		IP Address	30.46.9a.1a:db:a8		Standalone AP	WNDAP350
Up	620-162		192.168.10.162		IP Address	84.1b.5e.5c:5b:a8		Standalone AP	WNDAP620
Up	660-167		192.168.10.167		IP Address	84.1b.5e.5d:18:18		Standalone AP	WNDAP660
Up	Jimmy-620-168		192.168.10.168		IP Address	84.1b.5e.5c:5b:a8		Standalone AP	WNDAP620
Down	July-8-AP320	9500-161-sept10	192.168.10.109		IP Address	e0.91.f5.a4.8a.40		Controller Managed AP	WNAP320
Up	July17-660-163		192.168.10.163		IP Address	84.1b.5e.5d:fa:f9		Standalone AP	WNDAP660
Down	July8-AP-360	wc7520-160	192.168.10.136		IP Address	20.4e.7f:58.4a:e0		Controller Managed AP	WNDAP360
Up	netgear982968	wc-7520-164	192.168.10.240		IP Address	2c:b0.5d:88:29.60		Controller Managed AP	WNDAP360
Up	netgearA48B28	9500-161-sept10	192.168.10.103		IP Address	e0.91.f5.a4.8b.20		Controller Managed AP	WNAP320
Up	netgearA623F8		192.168.10.150		IP Address	e0.91.f5.a6:23:f8		Standalone AP	WNAP210

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 Details and Interface Details* on page 85.

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 18.

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**.

Status	Device Name	IP Address	Hostname	Managed By	MAC Address	Device Model
Up	WMS-41	192.168.10.41		IP Address	c0:3f:0e:3d:7e:b0	WMS5316

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 Details and Interface Details* on page 85.

Modify the Name, Location Information, and Contact Information

You can modify the device name, location information, and contact information that the application displays for a wired or wireless device.

➤ **To modify information for a 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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:fd:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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. Select the device.
8. Click the **Edit** button.

Edit Information			
Device Name	192.168.10.213		
Location	GS724Tv3_loc		
Contact	GS724Tv3_con		
Description	GS724Tv3		
Other Information			
Status	Up	Device Type	Switch
IP Address	192.168.10.213	MAC Address	28:c6:8e:01:9b:31
Discover Time	05/21/2013 17:28:32		
System Object ID	1.3.6.1.4.1.4526.100.4.17		

9. Modify the device information.
10. Click the **Submit** button.

The device information is updated and the screen closes.

Remove Device Information

You can remove all information that the application displays for a wired or wireless device. However, when you run another discovery job, the application might rediscover the device and add it again to its inventory database.

➤ To remove information for a 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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:f6:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328Sv2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TxS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

The screen displays the devices that the application discovered.

- 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.

- 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.

- Select the device.
- Click the **Delete** button.

A pop-up confirmation screen displays.

- Click the **Yes** button.

The device is removed from the Devices table and deleted.

Synchronize a Network Device

You can time-synchronize a wired or wireless network device to the NMS300 server.

➤ **To synchronize a device:**

- 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 18.

- 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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:fd:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724TV3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TKS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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. Select the device.

8. Click the **Resync** button.

A pop-up confirmation screen displays.

9. Click the **Yes** button.

The device is synchronized and the confirmation screen closes.

Log In to a Device

You can log in to a wired or wireless device on your network using either the web management interface or Telnet.

You can log in to a device when your web browser can be routed to the device. Generally, your web browser must be on the local network side of the Internet gateway.

➤ **To log in to a 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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:fd:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724TV3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS7527XS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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. Select the device.
8. Take one of the following actions:
 - Log in over the web management interface:
 - a. From the **More** menu, select **Web GUI**.

A login screen for the web management interface displays.
 - b. Enter the user name and password.

For most NETGEAR products, the user name is **admin** and the password is **password**.
 - c. Click the button that lets you log in to the device.

The name of the button depends on the device. For most NETGEAR products, the button is called the **Login** button.
 - Log in over a Telnet connection:
 - a. From the **More** menu, select **Telnet**.

A login screen for the CLI displays.
 - b. Enter the user name and password.

For most NETGEAR products, the user name is **admin** and the password is **password**.

Ping, Perform a Traceroute, or Reboot a Device

You can ping, perform a traceroute, or reboot a wired or wireless network device from the LAN or WAN. Your web browser must be routed to the NMS300 server to conduct these tasks.

➤ To test or reboot a 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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:f0:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c8:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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. Select the device.

8. Take one of the following actions:

- Ping the device. From the **More** menu, select **Ping**.

When the ping completes, a screen displays the results.

- Trace a route. From the **More** menu, select **TraceRoute**.

When the traceroute completed, a screen displays the results.

- Reboot the device. From the **More** menu, select **Reboot**.

Even though you reboot the device, the device remains in the inventory of the application.

Use the SNMP MIB Browser

The SNMP MIB browser lets you retrieve information about SNMP-enabled devices directly. The application supports SNMPv1, SNMPv2c, and SNMPv3 and all supported standard and private MIBs. The SNMP MIB browser lets you select one of several MIB databases and navigate a MIB tree to select a specific MIB trap. The application displays the data that the MIB trap collects, information about the selected MIB trap, and information about the SNMP credentials.

➤ **To select a MIB database and a MIB trap, collect data for a device, and view information about the MIB trap and SNMP credentials:**

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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74.44.01.90:fd.72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00.22.3f.9e.95.37		IP Address		Switch	GSM7328Sv2
Up	192.168.10.114	192.168.10.114	20.4e.7f.91.5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c.60.de.db.77.68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0.3f.0e.7f.cb:c5		IP Address	beijing	Switch	GSM7249v2
Up	192.168.10.201	192.168.10.201	10.0d.7f.b3.0e.08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28.c6.8e.01.9b.2b		IP Address		Switch	GS724TV3
Up	192.168.10.217	192.168.10.217	20.4e.7f.7b:d7.9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00.8e.f2.5a.da.0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30.46.9a.1b.b2.b7		IP Address		Switch	GSM7252PS

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.

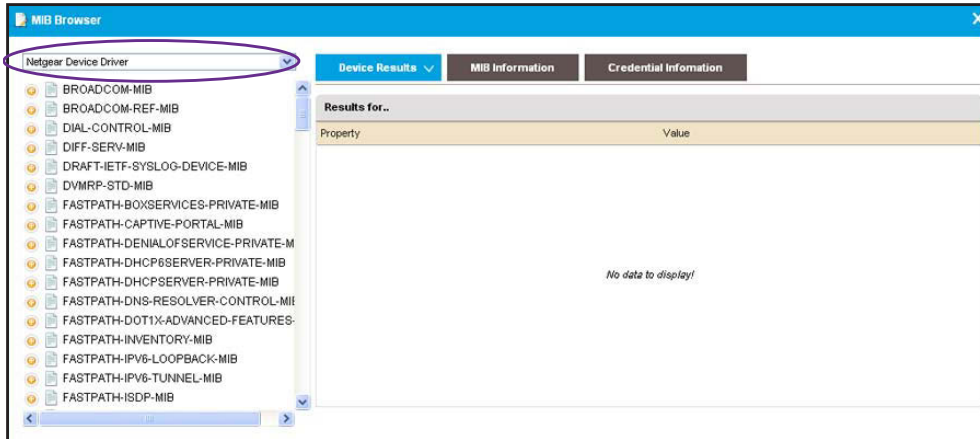
You can choose from the following columns: Status, Device Name, IP Address, Device Model, Device Type, Firmware Version, Serial Number, MAC Address, Last Update Time, Location, Registered, Hostname, Managed By, Date of Purchase, Vendor, Country of Purchase, Hardware Version, Configuration Version, Contact, 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. Select the device.
8. From the **More** menu, select **MIB Browser**.

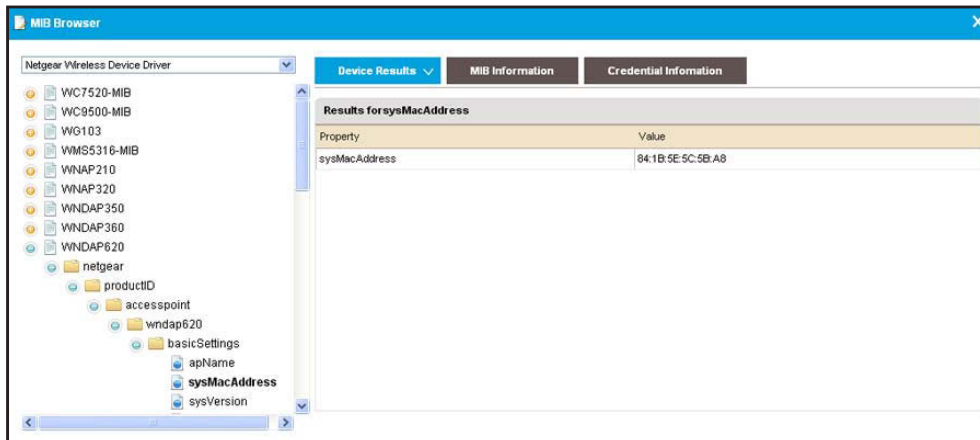


9. From the menu in the upper left of the screen, select the MIB database.

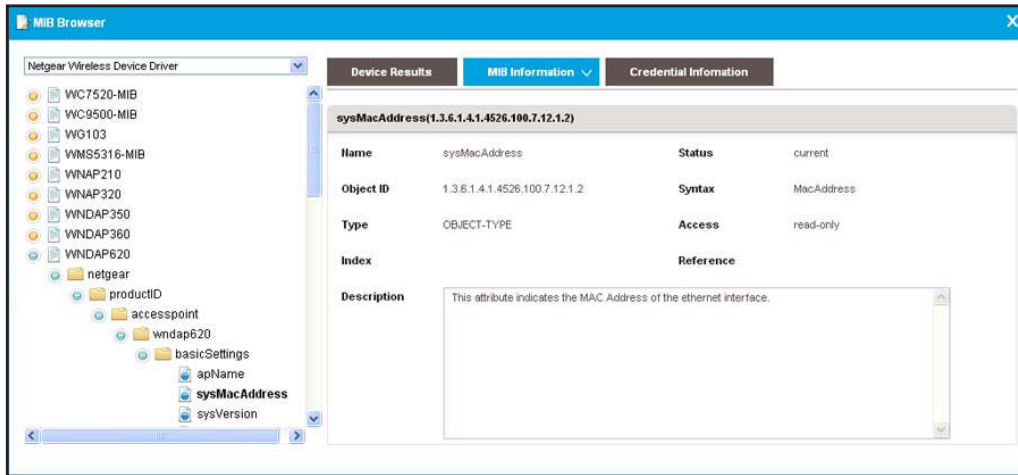
A MIB tree populates the screen.

10. Navigate to the MIB trap and click the MIB trap.

The Device Results section of the screen displays the property and value that the MIB trap collects:

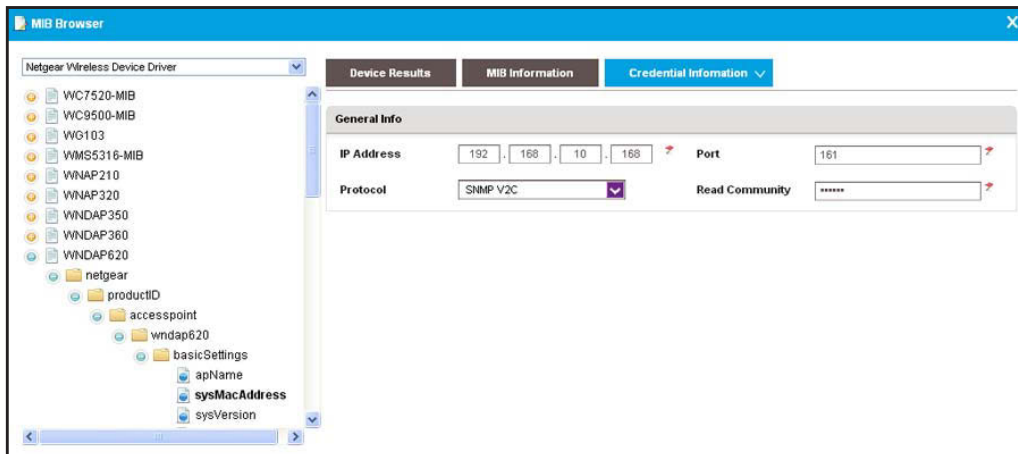


- To view information about the selected MIB or MIB trap, click the **MIB Information** tab.



The screen displays the name and object ID of the selected MIB or MIB trap, along with a description and other information.

- To view information about the SNMP credentials for the selected device, click the **Credential Information** tab.



The screen displays the IP address and SNMP port for the device, along with SNMP protocol and read community or SNMP user information.

- To display the information for another SNMP protocol, select another protocol from the **Protocol** menu.

The information onscreen adjusts.

- To close the MIB browser, click the **X** (✕) in the upper right of the screen.

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 18.

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**.

The screenshot shows the NMS300 application interface. The top navigation bar includes tabs for HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. The 'RESOURCES' tab is active, and the 'INVENTORY' sub-tab is selected. Below the navigation bar, there are options to 'Export to Excel' and 'Export to PDF'. The 'Inventory' table has columns for Status, Device Name, IP Address, MAC Address, Hostname, Managed By, Location, Device Type, and Device Model. The 'Interface List' table has columns for Index, Name, Interface Type, Admin Status, Operation Status, Speed(Mbps), and MTU.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:fd:72		IP Address	shanghai CN	Switch	GSM7224V2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248V2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724TV3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

Index	Name	Interface Type	Admin Status	Operation Status	Speed(Mbps)	MTU
1	1/g1	ethernetCsmacd	Up	Down	1000	1500
2	1/g2	ethernetCsmacd	Up	Down	1000	1500
3	1/g3	ethernetCsmacd	Up	Down	1000	1500
4	1/g4	ethernetCsmacd	Up	Down	1000	1500
5	1/g5	ethernetCsmacd	Up	Up	1000	1500
6	1/g6	ethernetCsmacd	Up	Down	1000	1500
7	1/g7	ethernetCsmacd	Up	Down	1000	1500
8	1/g8	ethernetCsmacd	Up	Down	1000	1500
9	1/g9	ethernetCsmacd	Up	Down	1000	1500
10	1/g10	ethernetCsmacd	Up	Down	1000	1500

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 the device anywhere but in the Device Name column.
8. To view details about an individual device or interface, in the Device Name column, click the device name (or IP address), or, in the Name column, click the interface name.
For information about viewing device details, see [View Device Details and Interface Details](#) on page 85.
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.

Manage 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 or Modify a Static Device Group](#) on page 63.
- **Dynamic device group.** A dynamic list of devices that are selected automatically based on your filter selection criteria. For more information, see [Add or Modify a Dynamic Device Group](#) on page 65.

For general information about device groups, see [Device Groups](#) on page 11.

Add or Modify 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 or modify an existing 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 18.
 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**.

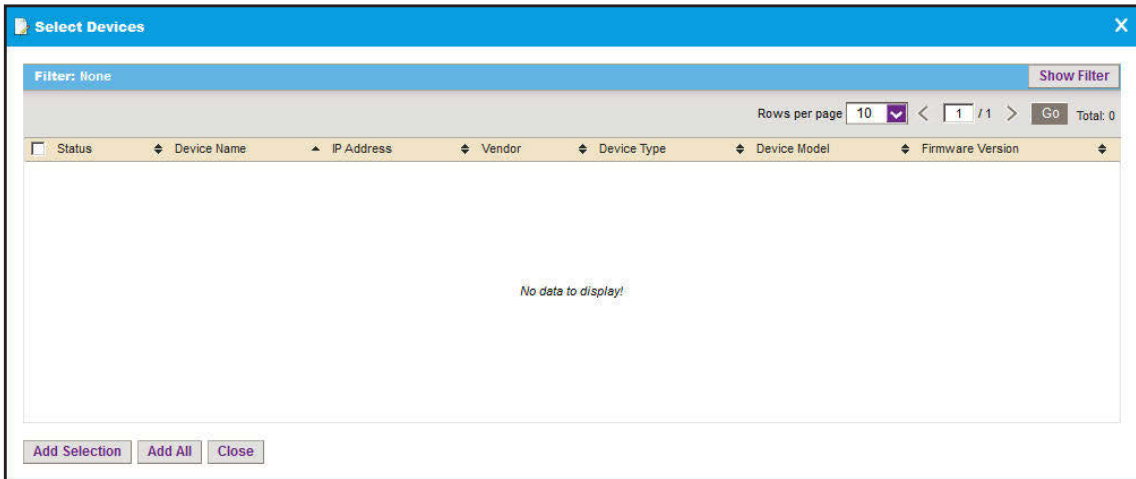
Group Name	Group Type	Device Count	Created By	Create Time
All Netgear Devices	Dynamic Group	40	admin	04/22/2013 11:59:52
AP	Static Group	0	admin	09/03/2013 18:06:06
Managed-switch	Static Group	0	admin	09/03/2013 18:04:54
smart-switch	Static Group	0	admin	09/03/2013 18:04:23
wc	Static Group	0	admin	09/03/2013 18:05:16

5. Add a static device group or modify an existing static device group:
- To add a static device group, click the **Add Static Group** button.
 - To modify an existing static device group:
 - a. From the Device Groups table, select the static device group.
 - b. Click the **Edit Group** button.

For a new static device group, the Add Static Device Group screen displays. For an existing static device group, the Edit Static Device Group screen displays.

6. Enter or modify the group name.
7. Enter or modify the 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. If you are modifying an existing static device group, to remove devices:
 - a. Select the devices.
 - b. Click the **Remove** button.
 The devices are removed from the Associated Devices table.
13. 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 or Modify 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 or modify an existing 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 18.
 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**.

Group Name	Group Type	Device Count	Created By	Create Time
<input type="checkbox"/> All Netgear Devices	Dynamic Group	40	admin	04/22/2013 11:59:52
<input type="checkbox"/> AP	Static Group	0	admin	09/03/2013 18:06:06
<input type="checkbox"/> Managed-switch	Static Group	0	admin	09/03/2013 18:04:54
<input type="checkbox"/> smart-switch	Static Group	0	admin	09/03/2013 18:04:23
<input type="checkbox"/> wc	Static Group	0	admin	09/03/2013 18:05:16

5. Add a dynamic device group or modify an existing dynamic device group:
 - To add a dynamic device group, click the **Add Dynamic Group** button.
 - To modify an existing dynamic device group:
 - a. From the Device Groups table, select the dynamic device group.
 - b. Click the **Edit Group** button.

For a new dynamic device group, the Add Dynamic Device Group screen displays. For an existing dynamic device group, the Edit Dynamic Device Group screen displays.

6. Enter or modify the group name.
7. Enter or modify the description.
8. Enter or modify 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.

- 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.

- 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.

Remove a Device Group

You can remove a device group that you no longer need.

➤ To remove a device group:

- 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 18.

- Enter your user name and password.

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

- Click the **Sign In** button.

The Network Summary screen displays.

- Select **RESOURCES > DEVICE GROUPS**.

Group Name	Group Type	Device Count	Created By	Create Time
<input type="checkbox"/> All Netgear Devices	Dynamic Group	40	admin	04/22/2013 11:59:52
<input type="checkbox"/> AP	Static Group	0	admin	09/03/2013 18:06:06
<input type="checkbox"/> Managed-switch	Static Group	0	admin	09/03/2013 18:04:54
<input type="checkbox"/> smar-switch	Static Group	0	admin	09/03/2013 18:04:23
<input type="checkbox"/> wc	Static Group	0	admin	09/03/2013 18:05:16

- Select the device group.
- Click the **Delete Group** button.

A pop-up confirmation screen displays.

- Click the **Yes** button.

The device group is removed from the Device Groups table and deleted.

4

4 Monitor Devices and the Network

Monitor how devices and the network perform

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, view and export the audit logs, view firmware versions, and view NMS300 server information.

This chapter covers the following topics:

- *Monitor the Network*
- *Monitor the Top 10 Widgets for All Devices*
- *View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices*
- *View Device Details and Interface Details*
- *Monitor Wireless Clients and View Client Details*
- *Manage the Configuration Monitors*
- *Customize the Optional Network Dashboard*
- *View and Export Audit Logs*
- *View Firmware Version Information*
- *View the NMS300 Server Information*
- *View Application Notifications*

Monitor the Network

You can monitor the network by various criteria and you can customize the information that displays on the Network Summary screen.

View the Default Network Summary

If you did not customize the Network Summary screen, the 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:**

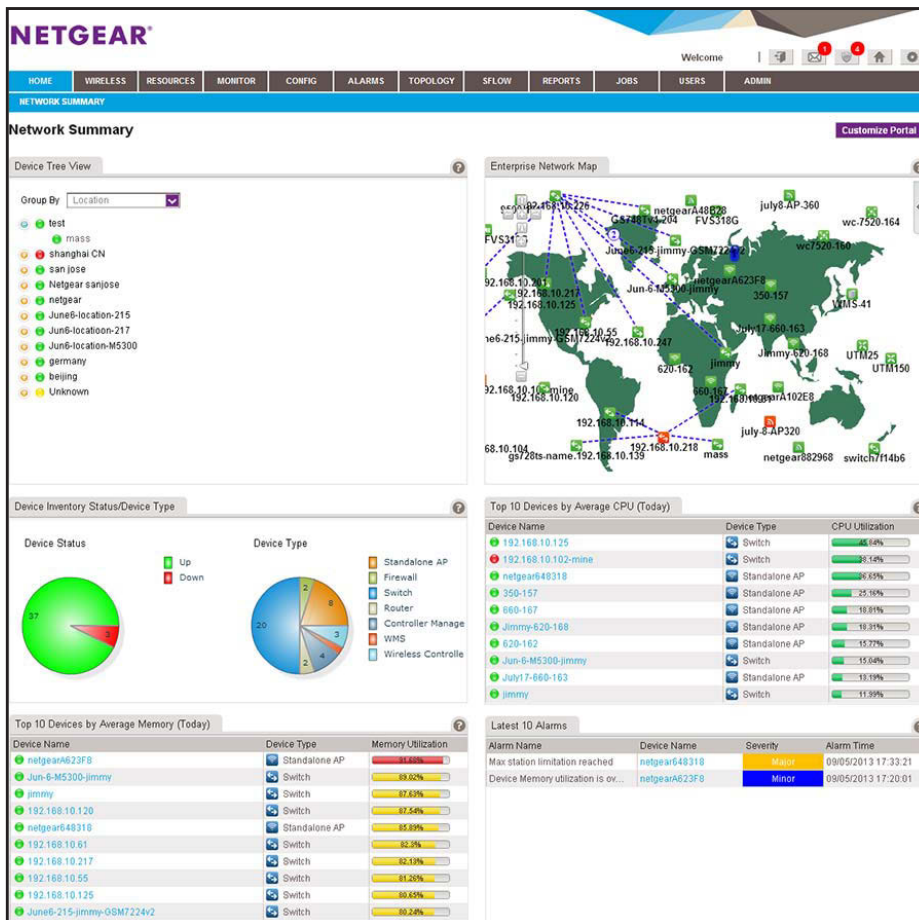
1. Open a browser and connect to the application through the static IP address of the NMS300 server.

For more information, see [Log In to the Application](#) on page 18.

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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Device status • Device name • Device type • Memory utilization in percentage
Latest 10 Alarms		<ul style="list-style-type: none"> • Alarm Name • Device Name • Severity • Alarm Time

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

For more information, see [View Device Details and Interface Details](#) on page 85.

Customize the Network Summary Screen

You can customize the items that display on the Network Summary screen. You do not need to be an admin user to customize the Network Summary screen.

In addition to the default widgets that are shown in the table in [View the Default Network Summary](#) on page 69, you can add the optional widgets that are listed in the following table.

Table 1. Optional widgets for the Network Summary screen

Widget	Description	Information
Devices		
Top 10 Devices by Average Response Time (Today)	Top 10 devices by average response time for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Average response time in ms
Top 10 Devices by Average Packet Loss (Today)	Top 10 devices by average packet loss percentage for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Average packet loss in percentage
Interfaces		
Top 10 Interfaces by Utilization (Today)	Top 10 interfaces by interface utilization for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Ingress (Rx) utilization in percentage • Egress (Tx) utilization in percentage • Total utilization in percentage
Top 10 Interfaces by Traffic Rate (Today)	Top 10 interfaces by traffic rate for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic rate • Egress (Tx) traffic rate • Total traffic rate <p>Note: Traffic rate is stated in bps, Kbps, or Mbps.</p>
Top 10 Interfaces by Traffic (Today)	Top 10 interfaces by total traffic for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>

Table 1. Optional widgets for the Network Summary screen (continued)

Widget	Description	Information
Top 10 Interfaces by Errors (Today)	Top 10 interfaces by total errors for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Number of ingress (Rx) errors • Number of egress (Tx) errors • Total number of errors
Top 10 Interfaces by Discards (Today)	Top 10 interfaces by total discarded packets for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Number of discarded egress (Tx) packets • Number of discarded ingress (Rx) packets • Total number of discarded packets

➤ **To customize the Network Summary screen:**

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 18.

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 **HOME > NETWORK SUMMARY**.

The Network Summary screen displays.

5. Click the **Customize Portal** button.

The screenshot shows the NMS300 Network Management System Application dashboard. At the top, there is a navigation bar with tabs: HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, ADMIN. Below the navigation bar is a "NETWORK SUMMARY" header. The main content area is divided into several widgets:

- Available Widgets:** A sidebar menu on the left with the following items: Enterprise Network Map (expanded), Enterprise Network Map, Device Tree View, Device Inventory, Alarm, Top 10 Device, and Interface.
- Device Tree View:** A widget showing a tree structure of devices grouped by location. The "Group By" dropdown is set to "Location". The tree shows:
 - ShangHai
 - ShangHai AP
 - GuangDong
 - s
 - unknown
 - ShangHai AC
 - gs110tp_eltecom
 - asd
 - netgearA0FCCB
- Enterprise Network Map:** A world map showing device locations. Labels include "San Jose", "asd", and IP addresses "192.168.0.157" and "192.168.0.137".
- Device Inventory Status/Device Type:** A widget with two circular gauges. The left gauge is green and labeled "Up", and the right gauge is orange and labeled "Switch".
- Top 10 Devices by Average CPU (Today):** A table showing the top 10 devices by CPU utilization.

Device Name	Device Type	CPU Utilization(%)
192.168.0.118	Switch	1%
GSM7212F-2	Switch	10.22%
M4100-26-POE_111	Switch	3.48%
M5300-28G-POE+_111333	Switch	7.56%
192.168.0.124	Switch	4.84%
- Top 10 Devices by Average Memory (Today):** A table showing the top 10 devices by memory utilization.

Device Name	Device Type	Memory Utilization(%)
192.168.0.124	Switch	32%
192.168.0.118	Switch	35%
M5300-28G-POE+_111333	Switch	37%
M4100-26-POE_111	Switch	31%
GSM7212F-2	Switch	31%
- Latest 10 Alarms:** A table showing the latest 10 alarms.

Alarm Name	Device Name	Severity	Alarm Time
Interface Trasmitted p...	GS748T_1	Minor	04/10/2013
Interface recived pack...	GS748T_1	Minor	04/10/2013
Interface recived pack...	GS728TXS_1	Minor	04/10/2013
Interface Trasmitted p...	GS728TXS_1	Minor	04/10/2013
Interface Trasmitted p...	GS752TXS_1	Minor	04/10/2013
Interface recived pack...	GS752TXS_1	Minor	04/10/2013
Interface Trasmitted p...	M5300-28G-F...	Minor	04/10/2013
Interface recived pack...	GS752TP_1	Minor	04/10/2013
Interface Trasmitted p...	GS752TP_1	Minor	04/10/2013
Interface recived pack...	M5300-28G-F...	Minor	04/10/2013
- Widget Area:** Two empty widget slots at the bottom with the text "Drag the widget from left to here".

The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.

The "Available Widgets" menu is shown in a close-up view. It contains the following items:

- Enterprise Network Map (expanded)
- Enterprise Network Map
- Device Tree View
- Device Inventory
- Alarm
- Top 10 Device
- Interface

6. Customize the Network Summary screen by performing one of the following tasks:
 - **Add a widget.** From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
Table 1 on page 71 describes the optional widgets that you can add.
 - **Remove a widget.** In a widget area that is populated by a widget, click the **X** (X) in the upper right of the widget area.
 - **Adjust the widget order.** To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
 - **Remove all widgets.** Click the **Remove All** button.
 - **Reset the Network Summary screen to its defaults.** Click the **Default** button.
7. Repeat [Step 6](#) until you selected all widgets that you want to display on the Network Summary screen.
8. If you are not content with your selections, click the **Reset** button and repeat [Step 6](#) and [Step 7](#).
9. Click the **Save** button.
The settings are saved for your account.
10. (Optional) Select **HOME > NETWORK SUMMARY**.
The screen displays its customized settings.

Monitor the Top 10 Widgets for All Devices

You can monitor the status and top 10 widgets for devices on the network by various criteria and you can customize the information that displays on the Top 10 screen.

View the Default Top 10 Widgets

If you did not customize the Top 10 screen, the screen displays the default top 10 widgets.

- **To monitor the default top 10 widgets and view device details:**
 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 18.
 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 > TOP 10.**

The screenshot shows the 'TOP 10' monitoring dashboard with the following data:

Device Name	Device Type	CPU Utilization
192.168.10.125	Switch	46.49%
192.168.10.102-mine	Switch	33.77%
netgear648318	Standalone AP	34.18%
350-157	Standalone AP	19.89%
netgearA102E8	Standalone AP	15.85%
660-167	Standalone AP	15%
Jun-6-M5300-jimmy	Switch	14.66%
July17-660-163	Standalone AP	14.5%
jimmy	Switch	13.09%
Jimmy-620-168	Standalone AP	13.09%

Device Name	Device Type	Memory Utilization
netgearA623F8	Standalone AP	91.6%
Jun-6-M5300-jimmy	Switch	88.93%
jimmy	Switch	87.78%
192.168.10.120	Switch	87.45%
netgear648318	Standalone AP	86.65%
192.168.10.61	Switch	82.3%
192.168.10.217	Switch	82.13%
192.168.10.55	Switch	81.26%
192.168.10.125	Switch	80.88%
June6-215-jimmy-GSM7224v2	Switch	78.45%

Device Name	Interface Name	Rx Util	Tx Util	Total
192.168.10.216	g11	0.00%	18.21%	18.21%
192.168.10.216	g13	18.19%	0.00%	18.19%
192.168.10.237	1/0/23	0.16%	0.14%	0.30%
192.168.10.237	1/0/48	0.10%	0.14%	0.24%
192.168.10.226	1/g39	0.13%	0.06%	0.19%
June6-215-jimmy-GSM7224v2	0/13	0.03%	0.03%	0.06%
192.168.10.237	1/0/21	0.01%	0.04%	0.05%
WMS-41	eth0	0.04%	0.00%	0.04%
192.168.10.226	1/g18	0.00%	0.03%	0.03%
UTM150	eth0	0.03%	0.00%	0.03%

Device Name	Interface Name	Rx(bps)	Tx(bps)	Total
192.168.10.216	g11	2,206	182,126,565	182,128,771
192.168.10.216	g13	181,929,625	40,831	181,970,456
192.168.10.237	1/0/23	165,344	137,805	303,149
192.168.10.237	1/0/48	96,244	144,357	240,601
192.168.10.226	1/g39	126,711	63,875	190,586
192.168.10.226	1/g46	13,813	92,244	106,057
192.168.10.226	1/g25	34,713	62,457	97,170
June6-215-jimmy-GSM7224v2	0/13	29,709	34,304	64,013
192.168.10.201	1/g5	41,727	14,918	56,645
192.168.10.226	1/g23	14,888	41,620	56,507

Device Name	Interface Name	Tx	Rx	Total
192.168.10.216	g11	489.80 GB	6.08 MB	489.81 GB
192.168.10.216	g13	112.45 MB	489.27 GB	489.38 GB
192.168.10.226	1/g39	514.63 MB	1020.87 ...	1.50 GB
192.168.10.226	1/g46	742.51 MB	111.19 MB	853.70 MB
192.168.10.237	1/0/23	378.49 MB	454.13 MB	832.63 MB
192.168.10.237	1/0/48	396.49 MB	264.34 MB	660.84 MB
June6-215-jimmy-GSM7224v2	0/13	276.38 MB	239.36 MB	515.74 MB
192.168.10.226	1/g23	335.32 MB	119.95 MB	455.27 MB
192.168.10.201	1/g5	119.76 MB	334.96 MB	454.72 MB
June6-215-jimmy-GSM7224v2	0/17	168.79 MB	209.06 MB	377.85 MB

Device Name	Interface Name	Tx Errors	Rx Errors	Total
192.168.10.237	1/0/48	0	4	4
192.168.10.237	1/0/21	0	3	3
192.168.10.237	1/0/23	0	1	1

By default, the following widgets display onscreen.

Widget	Description	Information
Top 10 Devices by Average CPU (Today)	Top 10 devices by average CPU utilization for today	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Device status Device name Device type Memory utilization in percentage
Top 10 Interfaces by Utilization (Today)	Top 10 interfaces by interface utilization for today	<ul style="list-style-type: none"> Device status Device name Interface status Interface name Ingress (Rx) utilization in percentage Egress (Tx) utilization in percentage Total utilization in percentage

Widget	Description	Information
Top 10 Interfaces by Traffic Rate (Today)	Top 10 interfaces by traffic rate for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic rate • Egress (Tx) traffic rate • Total traffic rate <p>Note: Traffic rate is stated in bps, Kbps, or Mbps.</p>
Top 10 Interfaces by Traffic (Today)	Top 10 interfaces by total traffic for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>
Top 10 Interfaces by Errors (Today)	Top 10 interfaces by total errors for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Number of ingress (Rx) errors • Number of egress (Tx) errors • Total number of errors

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

For more information, see [View Device Details and Interface Details](#) on page 85.

6. To view details about an interface, click the interface name.

For more information, see [View Device Details and Interface Details](#) on page 85.

Customize the Top 10 Screen

You can customize the information that displays on the Top 10 screen by adding and removing widgets. You can also reset the screen to its default information.

In addition to the default widgets that are shown in the table in [View the Default Top 10 Widgets](#) on page 74, you can add the optional widgets that are listed in the following table.

Table 2. Optional widgets for the Top 10 screen

Widget	Description	Information
Top 10 Device		
Top 10 Devices by Average Response Time (Today)	Top 10 devices by average response time for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Average response time in ms
Top 10 Devices by Average Packet Loss (Today)	Top 10 devices by average packet loss percentage for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Average packet loss in percentage
Top 10 Interface		
Top 10 Interfaces by Discards (Today)	Top 10 interfaces by total discarded packets for today	<ul style="list-style-type: none"> • Device status • Device name • Interface status • Interface name • Number of discarded egress (Tx) packets • Number of discarded ingress (Rx) packets • Total number of discarded packets
Top 10 Standalone AP		
Top 10 Standalone AP by CPU Utilization (Today)	Top 10 wireless standalone APs by total CPU utilization for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • CPU utilization in percentage
Top 10 Standalone AP by WLAN Utilization (Today)	Top 10 wireless standalone APs by total WLAN utilization for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • WLAN utilization in percentage
Top 10 AP by Client Count (Current)	Top 10 wireless standalone APs and controller-managed APs by number of current clients	<ul style="list-style-type: none"> • Device status • Device name • Device type • Total number of clients

Table 2. Optional widgets for the Top 10 screen (continued)

Widget	Description	Information
Top 10 Standalone AP by Wired traffic (Today)	Top 10 wireless standalone APs by traffic volume over a wired connection for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>
Top 10 SSID		
Top 10 SSID by Client Count (Current)	Top 10 SSIDs by number of current clients	<ul style="list-style-type: none"> • SSID • Device status • Device name • Radio • Total number of clients
Top 10 SSID by Traffic (Today)	Top 10 SSIDs by traffic volume for today	<ul style="list-style-type: none"> • SSID • Device status • Device name • Radio • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>
Top 10 Radio		
Top 10 Radio by Client Count (Current)	Top 10 radios by number of current clients	<ul style="list-style-type: none"> • Radio • Device status • Device name • Device type • Total number of clients
Top 10 Radio by Traffic (Today)	Top 10 radios by traffic volume for today	<ul style="list-style-type: none"> • Radio • Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>

➤ **To customize the Top 10 screen:**

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 18.

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 > TOP 10**.

The Top 10 screen displays.

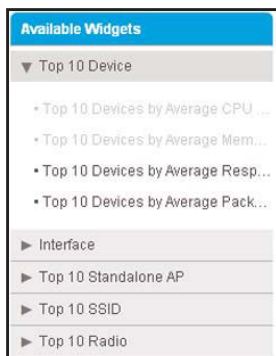
5. Click the **Customize Portal** button.

The screenshot displays the NMS300 Network Management System Application interface. At the top, there is a navigation menu with tabs: HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. Below the menu, the main dashboard is titled 'TOP 10' and includes sub-tabs for MONITOR CONFIGURATION, DASHBOARD VIEWS, and NETWORK DASHBOARD. On the left, an 'Available Widgets' sidebar lists various monitoring options. The main area contains six data widgets:

- Top 10 Devices by Average CPU (Today)**: A table showing CPU utilization for various devices.
- Top 10 Devices by Average Memory (Today)**: A table showing memory utilization for various devices.
- Top 10 Interfaces by Utilization (Today)**: A table showing interface utilization metrics (Rx Util, Tx Util, Total).
- Top 10 Interfaces by Traffic Rate (Today)**: A table showing interface traffic rates (Rx(bps), Tx(bps), Total(bps)).
- Top 10 Interfaces by Traffic (Today)**: A table showing interface traffic volumes (Tx(KB), Rx(KB), Total(KB)).
- Top 10 Interface by Errors (Today)**: A table showing interface error counts (Tx Errors, Rx Errors, Total).

At the bottom of the screen, there are two empty 'Widget Area' boxes with the instruction 'Drag the widget from left to here'.

The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.



6. Customize the Top 10 screen by performing one of the following tasks:
 - **Add a widget.** From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.

Table 2 on page 77 describes the optional widgets that you can add.
 - **Remove a widget.** In a widget area that is populated by a widget, click the **X** (X) in the upper right of the widget area.
 - **Adjust the widget order.** To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
 - **Remove all widgets.** Click the **Remove All** button.
 - **Reset the Top 10 screen to its defaults.** Click the **Default** button.
7. Repeat *Step 6* until you selected all widgets that you want to display on the Top 10 screen.
8. If you are not content with your selections, click the **Reset** button and repeat *Step 6* and *Step 7*.
9. Click the **Save** button.

Your changes are saved.

10. (Optional) Select **MONITOR > TOP 10**.

The screen displays its customized settings.

View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices

You can monitor the wireless inventory and top 10 widgets for wireless devices on the network by various criteria and you can customize the information that displays on the Wireless Summary screen.

View the Wireless Summary and Default Top 10 Wireless Widgets

If you did not customize the Wireless Summary screen, the screen displays the wireless inventory and default top 10 widgets for wireless devices.

➤ **To monitor the wireless inventory, monitor the default top 10 widgets for wireless devices, and view wireless device details:**

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 18.

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 > WIRELESS SUMMARY**.

Wireless Summary

Wireless Inventory

Wireless AP Status: Up (Green), Down (Red)

Wireless Device Type: Standalone AP (Orange), Controller Manage (Green), WMS (Blue), Wireless Controlle (Yellow)

Top 10 SSID by Client Count (Current)

SSID	Device Name	Radio	Client Count
1-210-150	netgearA623F8	2.4GHz	1
350-157-5ghz	350-157	5GHz	1

Top 10 AP by Client Count (Current)

Device Name	Device Type	Client Count
350-157	Standalone AP	1
netgearA623F8	Standalone AP	1

Top 10 Standalone AP by CPU Utilization (Today)

Device Name	Device Type	CPU Utilization
netgear648318	Standalone AP	34.19%
350-157	Standalone AP	19.52%
netgearA102E8	Standalone AP	15.8%
660-167	Standalone AP	14.88%
July17-660-163	Standalone AP	14.55%
Jimmy-620-168	Standalone AP	12.35%
620-162	Standalone AP	11.35%
netgearA623F8	Standalone AP	9.96%

Top 10 Standalone AP by Wired Traffic (Today)

Device Name	Device Type	Rx	Tx	Total
350-157	Standalone AP	245.95 MB	127.51 MB	373.46 MB
netgearA623F8	Standalone AP	236.12 MB	40.94 MB	277.06 MB
July17-660-163	Standalone AP	235.68 MB	16.55 MB	252.23 MB
620-162	Standalone AP	232.93 MB	11.14 MB	244.06 MB
Jimmy-620-168	Standalone AP	230.78 MB	12.87 MB	243.65 MB
660-167	Standalone AP	230.83 MB	12.49 MB	243.32 MB
netgear648318	Standalone AP	205.86 MB	11.18 MB	217.04 MB
netgearA102E8	Standalone AP	187.72 MB	10.88 MB	198.60 MB

Latest 10 Wireless Alarms

Alarm Name	Device Name	Severity	Alarm Time
60% utilization	350-157	Minor	09/06/2013 18:55:01
60% utilization	netgearA623F8	Minor	09/06/2013 18:55:00
Node is down	netgear648318	Critical	09/06/2013 16:06:20
Max station limitation reached	netgear648318	Major	09/06/2013 16:03:17
Rogue AP detect	netgearA623F8	Minor	09/06/2013 15:10:20
Node is down	netgearA102E8	Critical	09/06/2013 15:03:20
Node is down	July8-AP-360	Critical	09/06/2013 15:03:14
Node is down	netgear662968	Critical	09/06/2013 15:03:14
Max station limitation reached	July17-660-163	Major	09/05/2013 17:38:08

By default, the following widgets display onscreen.

Widget	Description	Information
Wireless Inventory	Status of the wireless APs and distribution of wireless devices in the network	<ul style="list-style-type: none"> Wireless AP status: <ul style="list-style-type: none"> Number of APs that are up Number of APs that are down Wireless device type: <ul style="list-style-type: none"> Number of standalone APs Number of controller-managed APs Number of wireless management systems (WMSs) Number of wireless controllers
Top 10 SSID by Client Count (Current)	Top 10 SSIDs by number of current clients	<ul style="list-style-type: none"> SSID Device status Device name Radio Total number of clients
Top 10 AP by Client Count (Current)	Top 10 wireless standalone APs and controller-managed APs by number of current clients	<ul style="list-style-type: none"> Device status Device name Device type Total number of clients
Top 10 Standalone AP by CPU Utilization (Today)	Top 10 wireless standalone APs by total CPU utilization for today	<ul style="list-style-type: none"> Device status Device name Device type CPU utilization in percentage
Top 10 Standalone AP by Wired traffic (Today)	Top 10 wireless standalone APs by traffic volume over a wired connection for today	<ul style="list-style-type: none"> Device status Device name Device type Ingress (Rx) traffic volume Egress (Tx) traffic volume Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>
Latest 10 Wireless Alarms		<ul style="list-style-type: none"> Alarm name Device name Severity Alarm time

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

For more information, see [View Device Details and Interface Details](#) on page 85.

Customize the Wireless Summary Screen

You can customize the information that displays on the Wireless Summary screen by adding and removing widgets. You can also reset the screen to its default information.

In addition to the default widgets that are shown in the table in [View the Wireless Summary and Default Top 10 Wireless Widgets](#) on page 81, you can add the optional widgets that are listed in the following table.

Table 3. Optional widgets for Wireless Summary screen

Widget	Description	Information
Top 10 Standalone AP		
Top 10 Standalone AP by Memory Utilization (Today)	Top 10 wireless standalone APs by total memory utilization for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • Memory utilization in percentage
Top 10 Standalone AP by WLAN Utilization (Today)	Top 10 wireless standalone APs by total WLAN utilization for today	<ul style="list-style-type: none"> • Device status • Device name • Device type • WLAN utilization in percentage
Top 10 SSID		
Top 10 SSID by Traffic (Today)	Top 10 SSIDs by traffic volume for today	<ul style="list-style-type: none"> • SSID • Device status • Device name • Radio • Egress (Tx) traffic volume • Ingress (Rx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>
Top 10 Radio		
Top 10 Radio by Client Count (Current)	Top 10 radios by number of current clients	<ul style="list-style-type: none"> • Radio • Device status • Device name • Device type • Total number of clients
Top 10 Radio by Traffic (Today)	Top 10 radios by traffic volume for today	<ul style="list-style-type: none"> • Radio • Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume <p>Note: Traffic volume is stated in KB, MB, or GB.</p>

➤ To customize the Wireless Summary screen:

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 18.

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 > WIRELESS SUMMARY**.

The Wireless Summary screen displays.

5. Click the **Customize Portal** button.

The screenshot shows the 'WIRELESS SUMMARY' page in the NMS300 application. The navigation bar includes: HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, ADMIN. The main content area is titled 'WIRELESS SUMMARY' and contains several widgets:

- Available Widgets:** A list of widgets that can be added to the dashboard, including 'Top 10 Standalone AP', 'Top 10 Standalone AP by CPU U...', 'Top 10 Standalone AP by VLAN...', 'Top 10 AP by Client Count(Current)', 'Top 10 Standalone AP by Wired...', 'Top 10 SSID', 'Top 10 Radio', 'Device Inventory', and 'Alarm'.
- Wireless Inventory:** A widget with two charts: 'Wireless AP Status' (a green circle with '11' inside) and 'Wireless Device Type' (a pie chart showing 9 Standalone AP, 2 Controller Manage, 2 WMS, and 1 Wireless Controlle).
- Top 10 SSID by Client Count (Current):** A table showing the top 10 SSIDs and their client counts.

SSID	Device Name	Radio	Client Count
NETGEAR_620-97	netgearSC47E8	2.4GHz	3
NETGEAR_11ng_97	netgearSC47E8	2.4GHz	1
NETGEAR_11ng_99	netgearSC7D68	2.4GHz	1
WG103_229	netgear3E23B8	2.4GHz	1
- Top 10 AP by Client Count(Current):** A table showing the top 10 APs by client count.

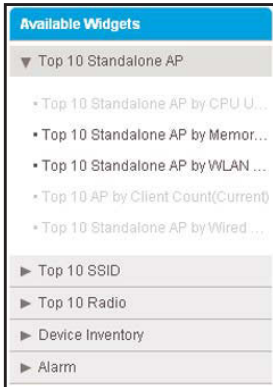
Device Name	Device Type	Client Count
netgearA9FC8	Controller Mana...	13
NTR-660-96	Standalone AP	13
NTR-620-94	Standalone AP	7
netgear5FF7B8	Controller Mana...	6
NTR-350-237	Standalone AP	6
NTR-WG103-229	Standalone AP	5
NTR-WG103-134	Standalone AP	5
NTR-620-97	Standalone AP	4
NTR-320-99	Standalone AP	3
netgear5FF238	Standalone AP	3
- Top 10 Standalone AP by CPU Utilization (Today):** A table showing the top 10 standalone APs by CPU utilization.

Device Name	Device Type	CPU Utilization
NTR-WG103-134	Standalone AP	34.35%
NTR-WG103-229	Standalone AP	32.45%
NTR-620-94	Standalone AP	19.0%
NTR-620-97	Standalone AP	11.52%
NTR-660-96	Standalone AP	3.29%
NTR-350-237	Standalone AP	7.41%
netgear5FF238	Standalone AP	7.16%
WIDAP36992	Standalone AP	5.1%
NTR-320-99	Standalone AP	4.6%
- Top 10 Standalone AP by Wired Traffic (Today):** A table showing the top 10 standalone APs by wired traffic.

Device Name	Device Type	Rx	Tx	Total
WIDAP36992	Standalone AP	51.42 MB	4.69 MB	56.11 MB
NTR-350-237	Standalone AP	50.71 MB	3.87 MB	54.59 MB
NTR-620-97	Standalone AP	50.16 MB	4.30 MB	54.46 MB
netgear5FF238	Standalone AP	50.41 MB	3.55 MB	53.97 MB
NTR-320-99	Standalone AP	50.31 MB	3.45 MB	53.77 MB
NTR-660-96	Standalone AP	49.34 MB	4.34 MB	53.68 MB
NTR-620-94	Standalone AP	49.12 MB	4.12 MB	53.23 MB
NTR-WG103-134	Standalone AP	49.03 MB	3.49 MB	52.53 MB
NTR-WG103-229	Standalone AP	49.03 MB	3.49 MB	52.53 MB
- Latest 10 Wireless Alarms:** A table showing the latest 10 wireless alarms.

Alarm Name	Device Name	Severity	Alarm Time
Device Memory utilization is over...	wanquan	Minor	06/24/2013 09:50:01
Rogue AP detect	netgear3E23B8	Minor	06/23/2013 17:14:21
- Widget Area:** Two empty boxes with the text 'Drag the widget from left to here'.

The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.



6. Customize the Wireless Summary screen by performing one of the following tasks:
 - **Add a widget.** From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.

Table 3 on page 83 describes the optional widgets that you can add.
 - **Remove a widget.** In a widget area that is populated by a widget, click the **X** (X) in the upper right of the widget area.
 - **Adjust the widget order.** To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
 - **Remove all widgets.** Click the **Remove All** button.
 - **Reset the Wireless Summary screen to its defaults.** Click the **Default** button.
7. Repeat [Step 6](#) until you selected all widgets that you want to display on the Wireless Summary screen.
8. If you are not content with your selections, click the **Reset** button and repeat [Step 6](#) and [Step 7](#).
9. Click the **Save** button.

Your changes are saved.
10. (Optional) Select **WIRELESS > WIRELESS SUMMARY**.

The screen displays its customized settings.

View Device Details and Interface Details

You can view many details for a device and its interfaces. The detailed information that the application can provide depends on the type of device. The Devices table can list the following devices in the Device Type column:

- Switch
- Firewall

- Standalone AP
- Controller-Managed AP
- Wireless Controller
- WMS
- Storage
- Router
- Unknown

For information about the details that the application can provide for each type of device, see [Appendix B, Device Details](#). For information about NETGEAR products that the application supports, see [Compatible Devices](#) on page 12.

➤ **To view the detailed information for a device and an interface:**

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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:f0:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM73285v2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	G8728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-2803
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	G8748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	G8724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:9e:f2:5a:da:0e		IP Address		Switch	G8752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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.

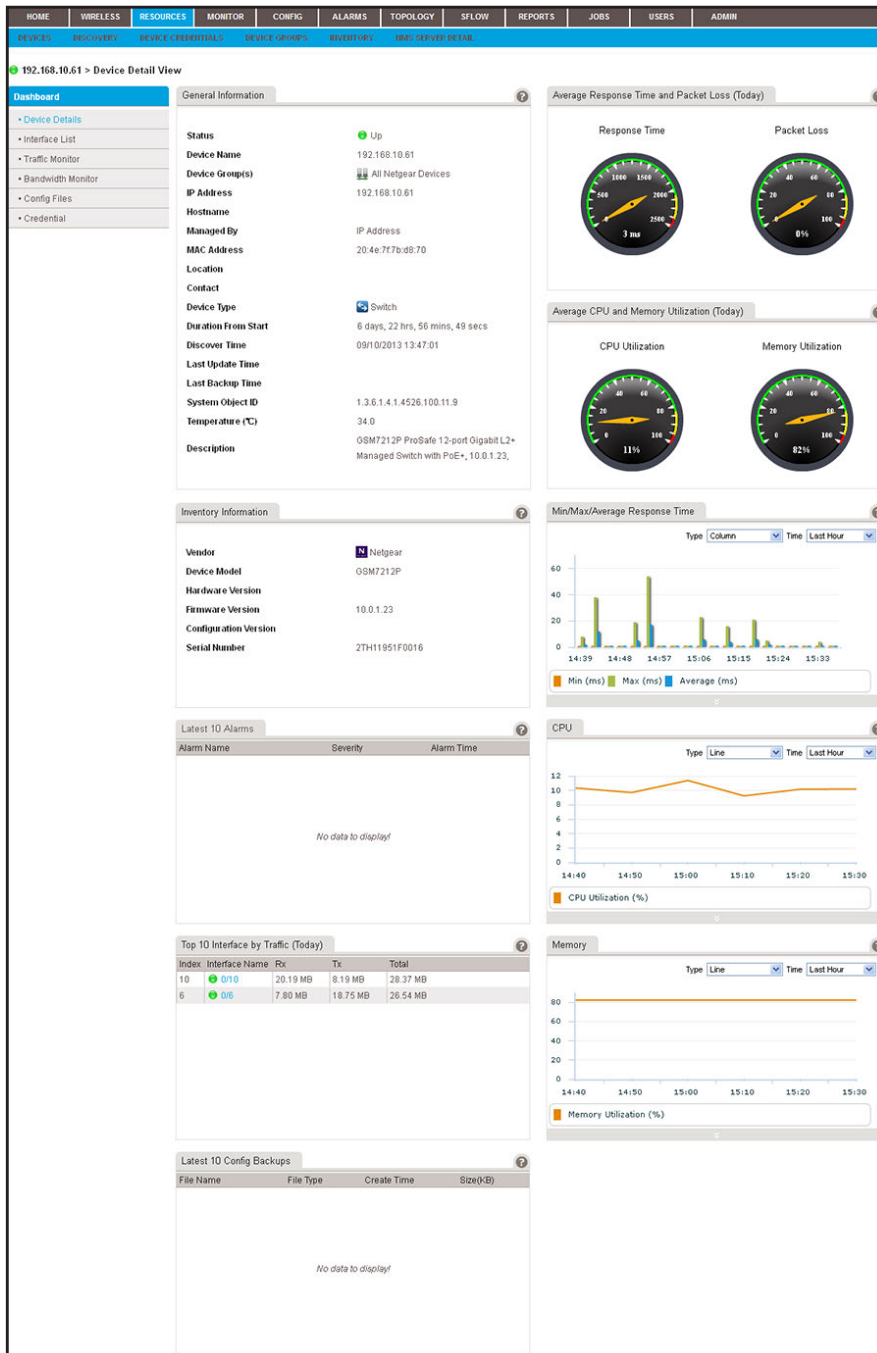
- To filter the devices that are listed, click the **Show Filter** button.

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

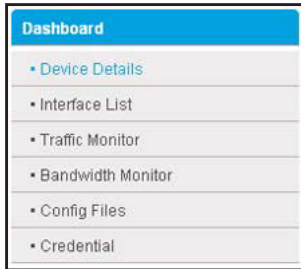
To hide the filter, click the **Hide Filter** button.

- Click the name of 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 that displays when the device that you select is a switch.



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

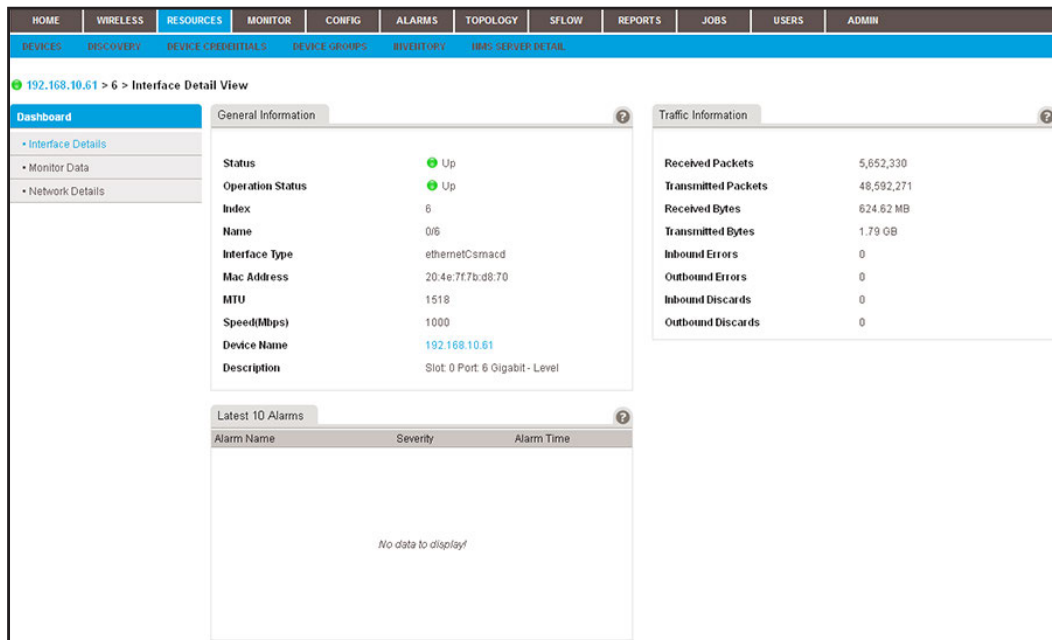
- From the **Dashboard** menu, select a menu option.

The screen adjusts to display information that corresponds to your menu option. For information about the details that the application can provide for each type of device, see [Appendix B, Device Details](#).

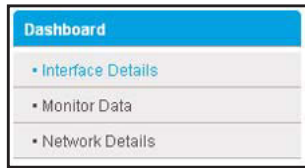
For switches, wireless controllers, wireless management systems, and routers, you can display interface details.

- To display interface details:

- Select **Interface List**.



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.

For more information about the details that the application can provide for an interface, see [Appendix B, Device Details](#).

Monitor Wireless Clients and View Client Details

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 18.

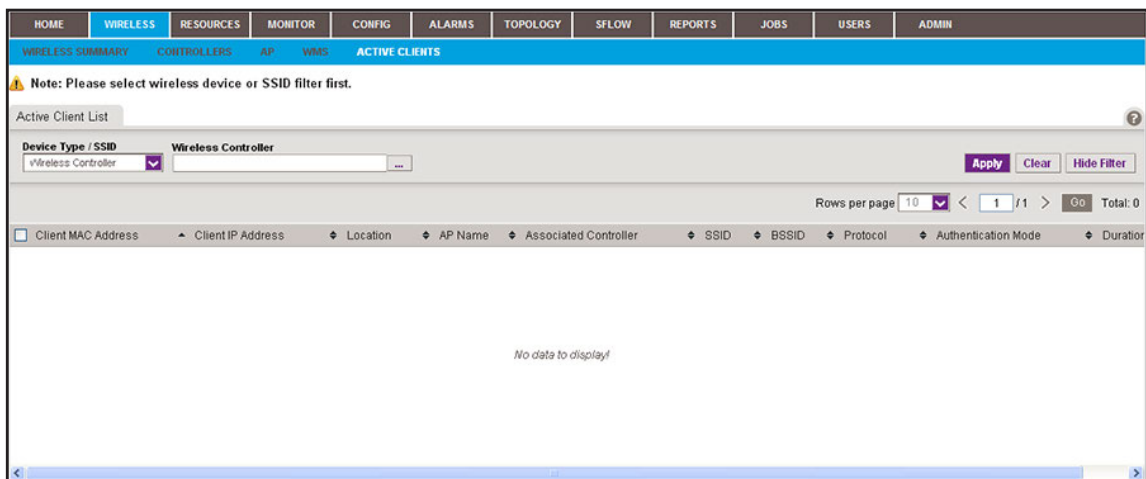
2. Enter your user name and password.

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**.



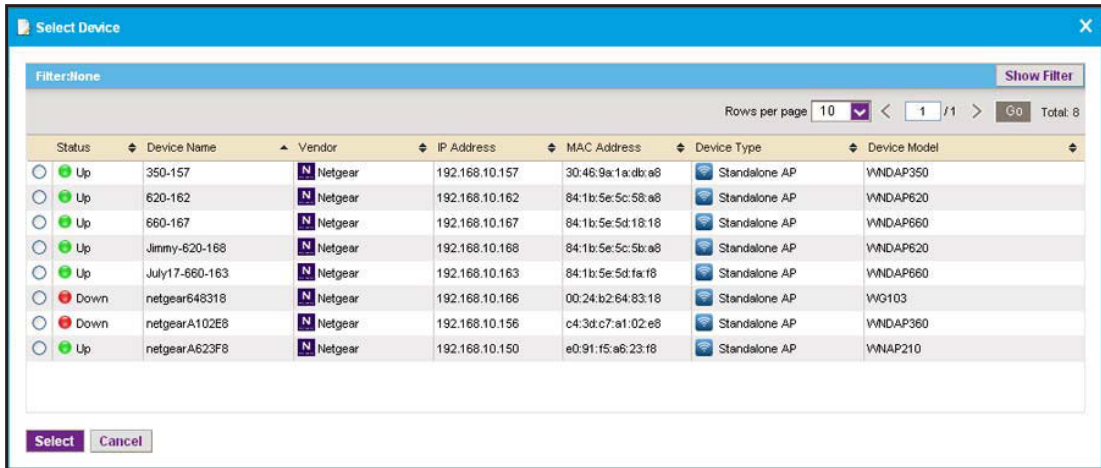
By default, the filter for active clients is active because the Active Client List table can display many wireless clients.

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.

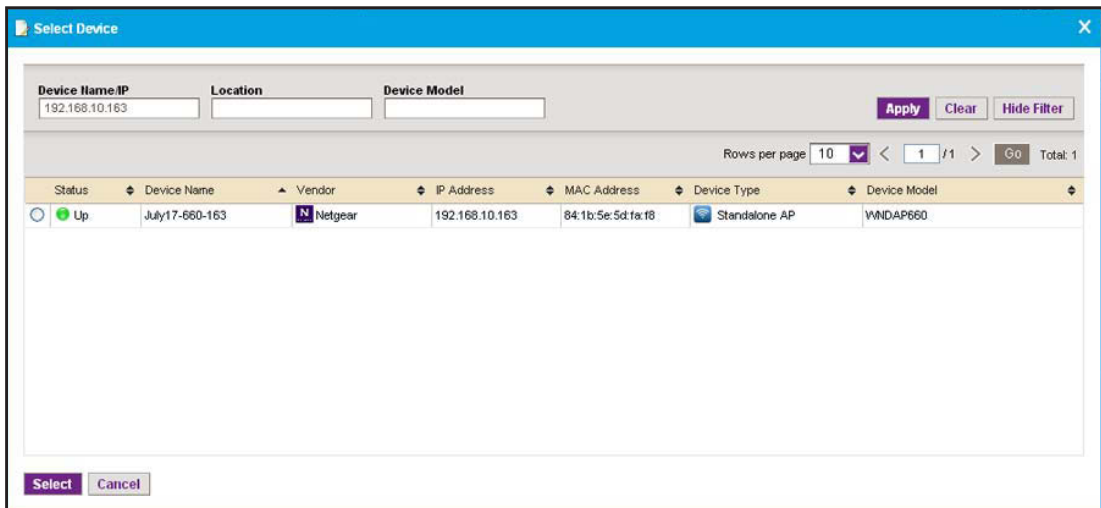


8. To filter the devices or SSIDs that are listed, click the **Show Filter** button.

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 SSIDs or devices, click the **Hide Filter** button.

The following figure shows an example 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.

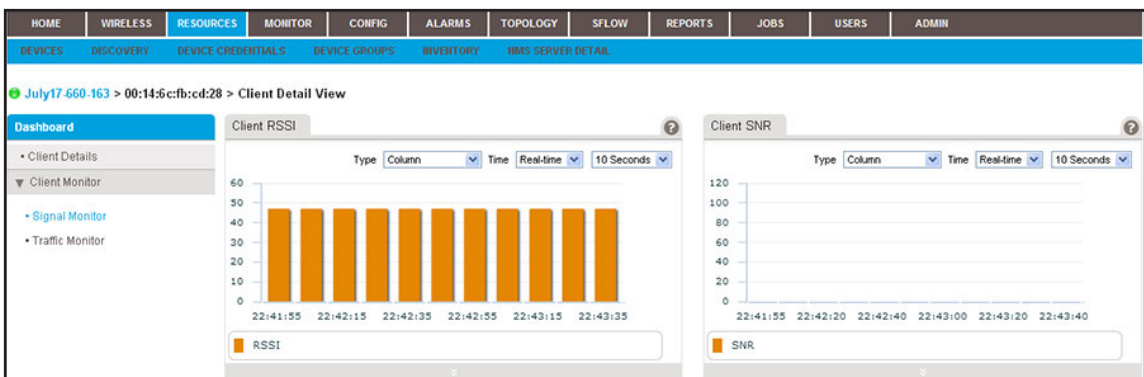
Client MAC Address	Client IP Address	Location	AP Name	Associated Controller	SSID	BSSID	Protocol	Authentication Mode
<input type="checkbox"/> 00:14:6c:fb:cd:28	0.0.0.0		July17-660-163		111-660-163-2.4	84:1b:5e:5d:fa:f0	802.11ng	...
<input type="checkbox"/> 00:1e:2a:e7:57:34	0.0.0.0		July17-660-163		111-660-163-5.0	84:1b:5e:5d:fa:f0	802.11na	...

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.

The following table lists some of the dashboard options and widgets or tables that are available for a wireless client.

Dashboard Option	Widget or Table
Signal Monitor	Client RSSI
	Client SNR
Traffic Monitor	Client Received/Transmitted Bytes
	Client Data Rate

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 information about how to configure alarm trigger settings for these monitors, see [Add a Custom Alarm Configuration](#) on page 165.

The following sections describe the tasks that you can perform for the configuration monitors:

- [Configure an Individual Monitor](#)
- [Disable a Monitor](#)
- [Reenable a Monitor](#)
- [View or Modify the Polling Interval for a Monitor](#)

Configure an Individual Monitor

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 18.

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
<input checked="" type="checkbox"/>	Device Status	ICMP	3	Device up and down status
<input checked="" type="checkbox"/>	Device ICMP Ping	ICMP	3	Device ICMP Ping results
<input checked="" type="checkbox"/>	Device CPU	Device Key Metrics	10	CPU utilization of the device
<input checked="" type="checkbox"/>	Device Memory	Device Key Metrics	10	Memory Utilization of the device
<input checked="" type="checkbox"/>	Device Temperature (°C)	Device Key Metrics	10	Device Temperature (°C)
<input checked="" type="checkbox"/>	UTM Disk	UTM	10	Disk Utilization of the UTM
<input checked="" type="checkbox"/>	Device IP Traffic	Device Key Metrics	10	Device traffic statistics per IP protocol
<input checked="" type="checkbox"/>	Device ICMP Traffic	Device Key Metrics	10	Device traffic statistics per ICMP protocol
<input checked="" type="checkbox"/>	Device TCP Traffic	Device Key Metrics	10	Device traffic statistics per TCP protocol
<input checked="" type="checkbox"/>	Device UDP Traffic	Device Key Metrics	10	Device traffic statistics per UDP protocol
<input checked="" type="checkbox"/>	Device SNMP Traffic	Device Key Metrics	10	Device traffic statistics per SNMP protocol
<input checked="" type="checkbox"/>	Device Interface Traffic	Interface	10	Device interface performance statistics
<input checked="" type="checkbox"/>	NMS System Server	Device Key Metrics	5	NMS System Server Monitor
<input checked="" type="checkbox"/>	Radio Statistics	Wireless	10	Wireless performance of WLAN network based on radio
<input checked="" type="checkbox"/>	WLAN Utilization	Wireless	10	WLAN utilization of wireless Device
<input checked="" type="checkbox"/>	VAP Statistics	Wireless	10	Wireless performance statistics of WLAN network bas...
<input checked="" type="checkbox"/>	Wired Ethernet Statistics	Wireless	10	Wired performance statistics of Standalone AP.
<input checked="" type="checkbox"/>	Storage Disk Temperature Monitor	Storage	10	Temperature of the storage disk.
<input checked="" type="checkbox"/>	Storage Temperature Monitor	Storage	10	Temperature of the storage probe.
<input checked="" type="checkbox"/>	Storage Disk	Storage	10	Disk Utilization of the storage

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

The screenshot shows the 'Monitor Configuration (Device IP Traffic)' dialog box with the 'General Information' tab selected. The 'Monitor Name' is set to 'Device IP Traffic', 'Enable' is 'Yes', and 'Polling Interval' is '10 Minutes'. The 'Description' field contains 'Device traffic statistics per IP protocol'. 'Save' and 'Close' buttons are at the bottom left.

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.

The screenshot shows the 'Monitor Configuration (Device IP Traffic)' dialog box with the 'Monitor Devices' tab selected. Under 'Monitor Target Devices', the 'All Devices' radio button is selected. 'Save' and 'Close' buttons are at the bottom left.

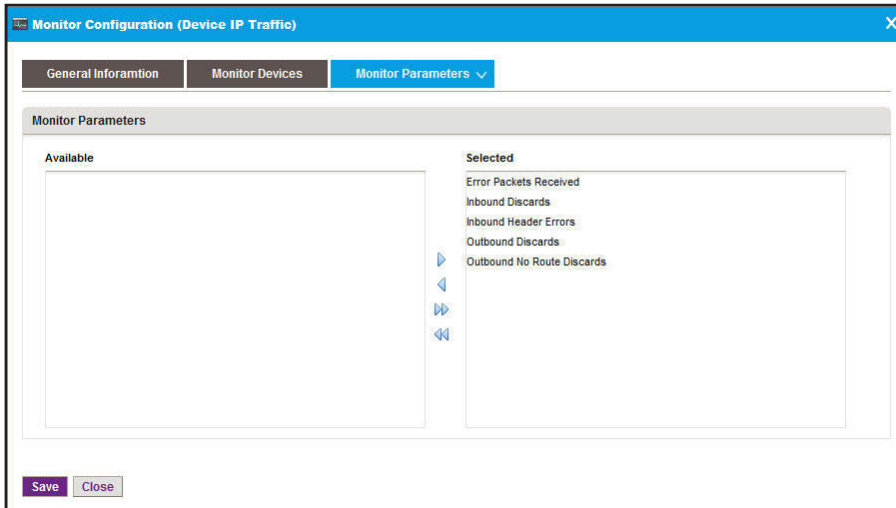
9. (Optional) In the Monitor Devices screen, select one of the following radio buttons:
 - **All Devices.** Monitors all devices.
 - **Select Devices or Device Groups.** The screen adjusts to let you select devices, device groups, or both to monitor:
 - a. Click the **Add Device** button.
 - b. Either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

Disable a Monitor

By default, all monitors are enabled.

➤ **To disable a 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 18.

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

A pop-up confirmation screen displays.

7. Click the **Yes** button.

The monitor is disabled. In the Monitor Configuration table, the Enable column displays No for the monitor.

Reenable a Monitor

➤ **To reenable a monitor after you disabled it:**

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 18.

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

A pop-up confirmation screen displays.

The monitor is reenabled. In the Monitor Configuration table, the Enable column displays Yes for the monitor.

View or Modify the Polling Interval for a Monitor

You can view and modify the polling interval for a monitor to control how frequently the device and network information is updated.

➤ **To view and modify the polling interval for a 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 18.

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
<input checked="" type="checkbox"/>	Device Status	ICMP	3	Device up and down status
<input checked="" type="checkbox"/>	Device ICMP Ping	ICMP	3	Device ICMP Ping results
<input checked="" type="checkbox"/>	Device CPU	Device Key Metrics	10	CPU utilization of the device
<input checked="" type="checkbox"/>	Device Memory	Device Key Metrics	10	Memory Utilization of the device
<input checked="" type="checkbox"/>	Device Temperature (°C)	Device Key Metrics	10	Device Temperature (°C)
<input checked="" type="checkbox"/>	UTM Disk	UTM	10	Disk Utilization of the UTM
<input checked="" type="checkbox"/>	Device IP Traffic	Device Key Metrics	10	Device traffic statistics per IP protocol
<input checked="" type="checkbox"/>	Device ICMP Traffic	Device Key Metrics	10	Device traffic statistics per ICMP protocol
<input checked="" type="checkbox"/>	Device TCP Traffic	Device Key Metrics	10	Device traffic statistics per TCP protocol
<input checked="" type="checkbox"/>	Device UDP Traffic	Device Key Metrics	10	Device traffic statistics per UDP protocol
<input checked="" type="checkbox"/>	Device SNMP Traffic	Device Key Metrics	10	Device traffic statistics per SNMP protocol
<input checked="" type="checkbox"/>	Device Interface Traffic	Interface	10	Device interface performance statistics
<input checked="" type="checkbox"/>	NMS System Server	Device Key Metrics	5	NMS System Server Monitor
<input checked="" type="checkbox"/>	Radio Statistics	Wireless	10	Wireless performance of WLAN network based on radio
<input checked="" type="checkbox"/>	WLAN Utilization	Wireless Device	10	WLAN utilization of wireless Device
<input checked="" type="checkbox"/>	WAP Statistics	Wireless	10	Wireless performance statistics of WLAN network bas...
<input checked="" type="checkbox"/>	Wired Ethernet Statistics	Wireless	10	Wired performance statistics of Standalone AP.
<input checked="" type="checkbox"/>	Storage Disk Temperature Monitor	Storage	10	Temperature of the storage disk.
<input checked="" type="checkbox"/>	Storage Temperature Monitor	Storage	10	Temperature of the storage probe.
<input checked="" type="checkbox"/>	Storage Disk	Storage	10	Disk Utilization of the storage

The current polling interval for each metric is listed on the screen in the Polling Interval (minutes) column.

5. Select the monitor.
6. Click the **Edit** button.
7. In the General Information screen, from the **Polling Interval** menu, select a polling interval.
8. Click the **Save** button.

Your changes are saved.

Customize the Optional Network Dashboard

By default, the network dashboard does not display any information. If you want to use the network dashboard, you must create and customize network views and select one or more of these views on the network dashboard.

The following sections describe the network dashboard tasks:

- *Create or Modify a Dashboard View and Launch the Dashboard View*
- *Remove a Dashboard View*
- *Customize the Network Dashboard*

Create or Modify a Dashboard View and Launch the Dashboard View

You can create dashboard views, including dashboard views that let you monitor performance in real time.

➤ **To create a dashboard view or modify an existing dashboard view and launch the dashboard view:**

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 18.

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 > DASHBOARD VIEWS**.

Name	Time Frame	Created By	Created Time
AP_RadioStatistics	Real-time	roland	09/28/2013 11:45:22
SwitchPingResponseTime	Real-time	roland	09/28/2013 11:43:37

By default, the application does not include any dashboard views.

5. Create a dashboard view or modify an existing dashboard view:
 - To create a dashboard view, click the **Add** button.
 - To modify an existing dashboard view:
 - a. From the Dashboard Views table, select the dashboard view.
 - b. From the **More** menu, select **Edit**.

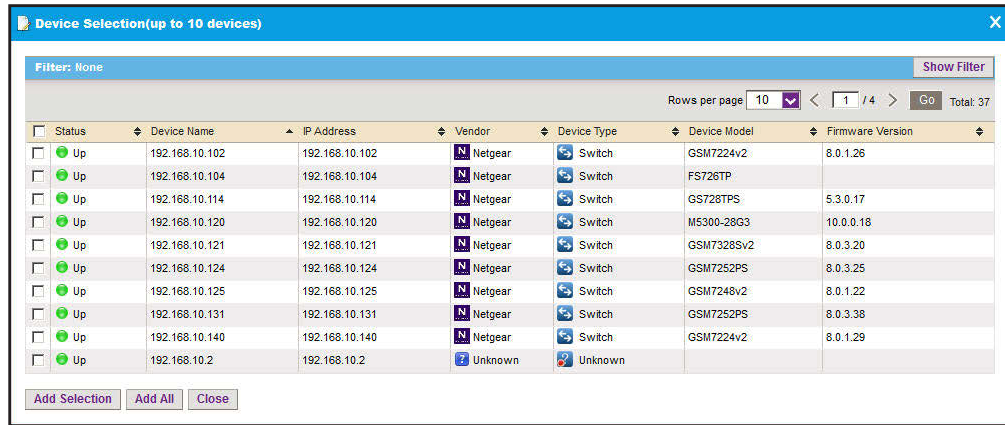
For a new dashboard view, the Add Dashboard displays. For an existing dashboard view, the Edit Dashboard screen displays.

6. In the **Name** field, enter or modify the name for the dashboard view.
7. From the **Time Frame** menu, select the time frame over which you want to view the performance:
 - **Real-time**. View the performance in real time. (This is the default setting.) From the **Intervals (sec)** menu, select the period in seconds or minutes over which you want to view the performance:
 - **10 Seconds** (This is the default setting.)
 - **30 Seconds**
 - **1 Minute**
 - **2 Minutes**
 - **5 Minutes**
 - **Last Hour**
 - **Last 24 Hours**
 - **Last 7 Days**
 - **Last 30 Days**
8. If you select Real Time from the **Time Frame** menu, select a predefined period in seconds or minutes from the **Interval** menu.
9. From the **Default Chart Type** menu, select one of the following types:
 - **Line**
 - **Column**
 - **Column Stacked**
 - **Area**
 - **Area Stacked**

10. From the **Source Type** menu, select either **Device** or **Interface**:

- **Device.** Create or modify a dashboard view of devices:
 - a. Click the **Add Device** button.

The Device Selection screen displays.



- b. To filter the devices that display in the table, click the **Show Filter** button.
- c. Select up to 10 devices and click the **Add Selection** button.

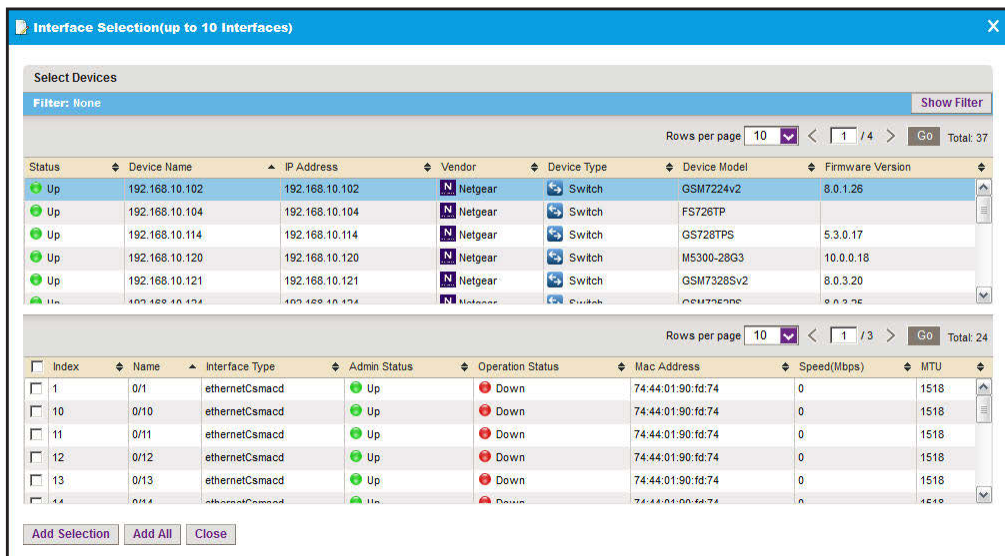
To add the first 10 devices that display in the table, click the **Add All** button.

- d. If you are modifying an existing dashboard view, to remove devices, select the devices, and click the **Remove** button.

The devices are removed from the Device Selection table.

- **Interface.** Create or modify a dashboard view of interfaces:
 - a. Click the **Add Interface** button.

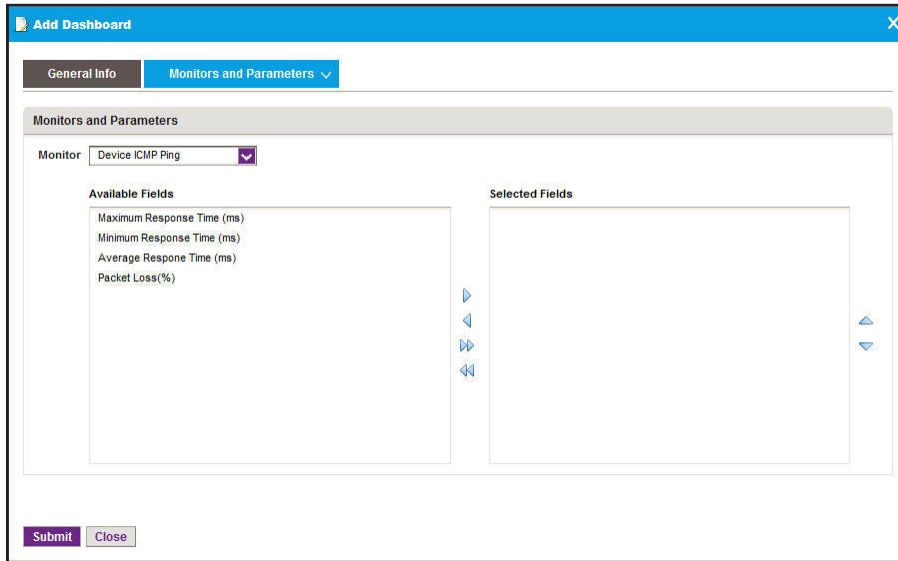
The Interface Selection screen displays.



- b. To filter the devices that appear in the table, click the **Show Filter** button.
- c. From the upper table, select a device for which you want to monitor interfaces.
- d. From the lower table, select the interfaces, and click the **Add Selection** button.
To add the first 10 interfaces that display in the table, click the **Add All** button.
- e. To add interfaces for another device, repeat *Step a* through *Step d*.
- f. If you are modifying an existing dashboard view, to remove interfaces, select the interfaces, and click the **Remove** button.

The interfaces are removed from the Interface Selection table.

11. Click the **Monitors and Parameters tab.**



12. From the **Monitor menu, select a monitor.**

The **Monitor** menu displays only common monitors that apply to the device types that you select in *step 10* on page 100. Your selection from the **Monitor** menu determines the options that display in the Available Fields section.

13. Specify the fields and their order.

To select the fields, use the left and right arrows. To arrange their order, use the up and down arrows.

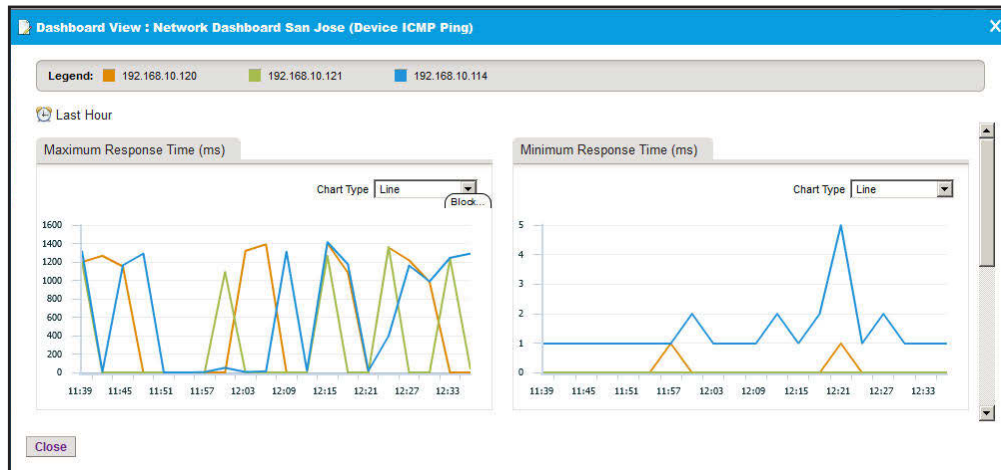
14. Click the **Submit button.**

The screen closes. The new or modified dashboard displays in the Dashboard Views table.

15. Select the new or modified dashboard view.

16. Click one of the following buttons:

- **Launch (Popup).** A pop-up screen similar to the following displays.



To close the screen, click the **X** (X) button.

- **Launch (New).** A screen opens in a new browser window.

The information that displays if you click the **Launch (New)** button is identical to the information that displays if you click the **Launch (Popup)** button.

Remove a Dashboard View

You can remove a dashboard view that you no longer need.

➤ To remove a dashboard view:

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 18.

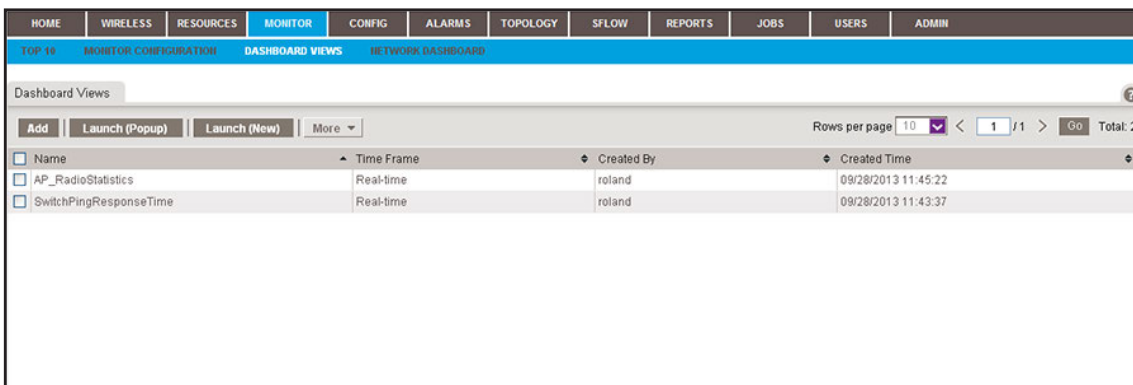
2. Enter your user name and password.

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 > DASHBOARD VIEWS**.



5. Select the dashboard view.
6. From the **More** menu, select **Delete**.
A pop-up confirmation screen displays.

7. Click the **Yes** button.

The dashboard view is removed from the Dashboard Views table and deleted.

Customize the Network Dashboard

If you did not add any dashboard views (see *Create or Modify a Dashboard View and Launch the Dashboard View* on page 98), the network dashboard does not display any information. After you added one or more dashboard views, you can select a dashboard view to display on the network dashboard.

➤ To customize the network dashboard:

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 18.

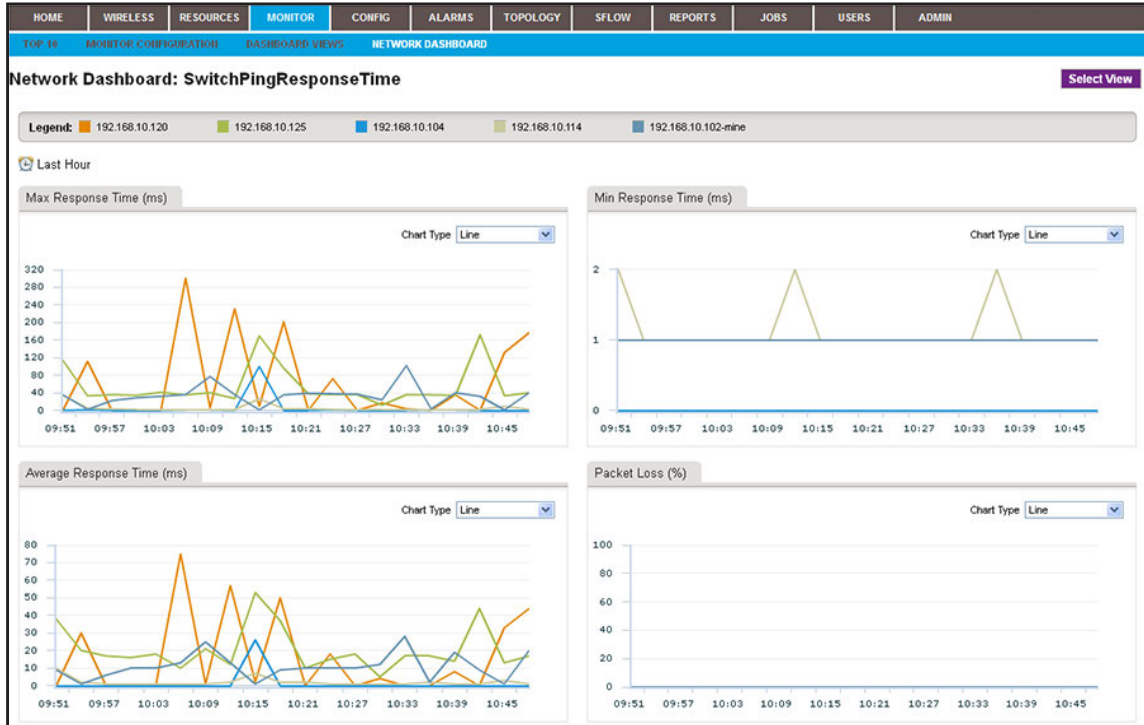
2. Enter your user name and password.

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 > NETWORK DASHBOARD**.



5. Click the **Select View** button.

The screenshot shows the 'Select View' dialog box. It contains a table with the following data:

Name	Time Frame	Source Type	Created By	Created Time
Controllers	Last 24 Hours	Device	roland	09/10/2013 10:33:31
StandAloneAPs	Real-time	Device	roland	09/10/2013 10:31:53
SwitchPingResponseTime	Last Hour	Device	roland	09/10/2013 10:48:26

At the bottom of the dialog box, there are 'Select View' and 'Close' buttons.

If the table does not display any dashboard views, you did not create any. For information about creating a dashboard view, see [Create or Modify a Dashboard View and Launch the Dashboard View](#) on page 98.

6. In the table, click the dashboard view.

7. Click the **Select View** button.

The screen closes and the selected network dashboard view displays.

View and Export Audit Logs

The system audit logs provide information about the tasks that you performed on the network or on the NMS300 server.

Audit logs are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 247.

➤ **To view and export the application audit logs:**

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 18.

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 > AUDIT LOG**.

User Name	Category	Operation	Target	Status	Operation Time
roland	Users	Login to System	NMS System	✔ Succeeded	09/10/2013 10:57:45
roland	Users	Exit System	NMS System	✔ Succeeded	09/10/2013 10:57:34
roland	Monitor	Set Network Dashboard: SwitchPingResponseTime	NMS System	✔ Succeeded	09/10/2013 10:48:37
roland	Monitor	Add Dashboard View: SwitchPingResponseTime	NMS System	✔ Succeeded	09/10/2013 10:48:26
roland	Monitor	Add Dashboard View: SwitchPingResponseTime	NMS System	✘ Failed	09/10/2013 10:48:17
roland	Monitor	Update Dashboard View: Controllers	NMS System	✔ Succeeded	09/10/2013 10:45:15
roland	Monitor	Update Dashboard View: Controllers	NMS System	✔ Succeeded	09/10/2013 10:44:30
roland	Monitor	Update Dashboard View: Controllers	NMS System	✔ Succeeded	09/10/2013 10:44:02
roland	Monitor	Update Dashboard View: Controllers	NMS System	✔ Succeeded	09/10/2013 10:43:30
roland	Users	Exit System	NMS System	✔ Succeeded	09/10/2013 10:42:24

5. To filter the log entries that display in the System Audit Log table, click the **Show Filter** button.

You can filter the log entries in the System Audit Log table by criteria such as user name, category, and operation time span.

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

6. Click the **Export to Excel** button or the **Export to PDF** button.
7. To save the audit logs on your computer, follow the directions of your browser.

View Firmware Version Information

You can view the firmware version information for the application and for all NETGEAR switches, NETGEAR wireless devices, and NETGEAR firewalls that the application discovered.

➤ **To view firmware version 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 18.

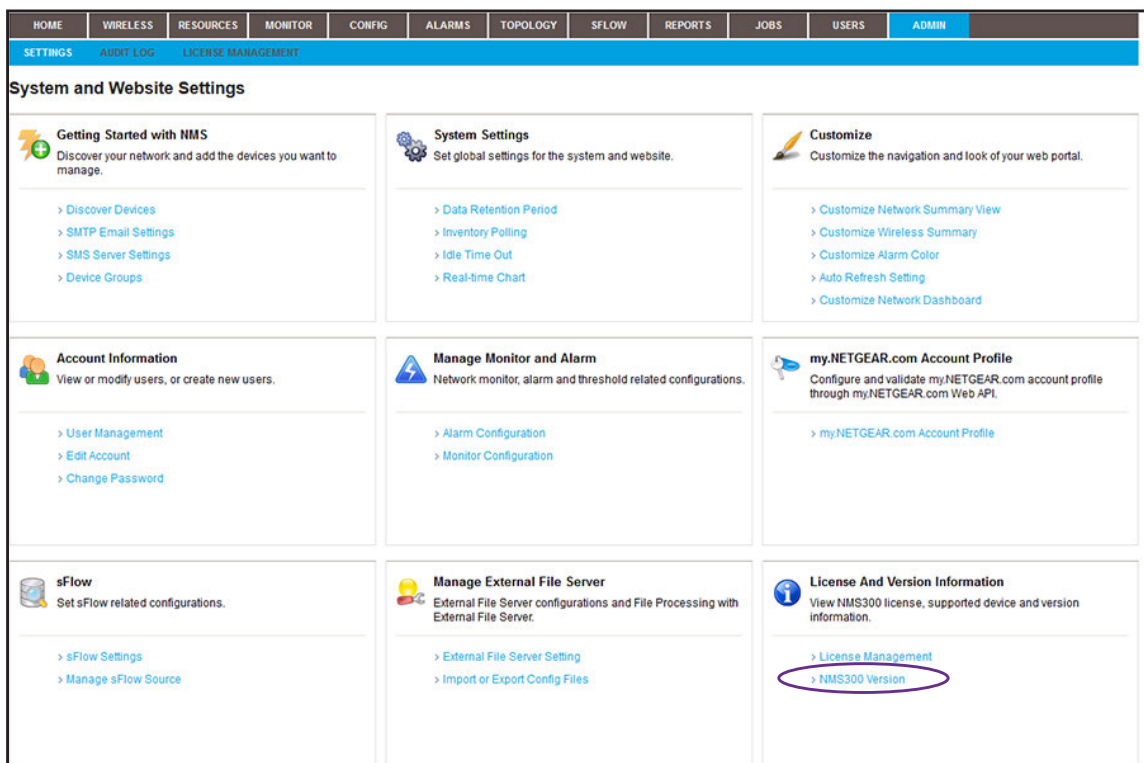
2. Enter your user name and password.

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

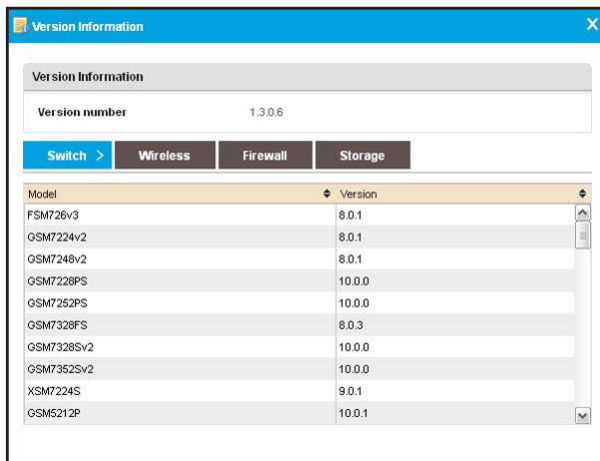
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under License And Version Information, click the **NMS300 Version** link.



Under Version Information, the firmware version of the application displays in the **Version number** field.

6. To view firmware versions of NETGEAR devices that the application discovered, click the **Switch**, **Wireless**, **Firewall**, or **Storage** tab.
7. Click the **X** (X) button.
The screen closes.

View the NMS300 Server Information

You can monitor the performance information of the NMS300 server.

➤ To view the NMS300 server 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 18.

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** > **NMS SERVER DETAIL**.

HOME WIRELESS **RESOURCES** MONITOR CONFIG ALARMS TOPOLOGY SFLOW REPORTS JOBS USERS ADMIN

DEVICES DISCOVERY DEVICE CREDENTIALS DEVICE GROUPS INVENTORY **NMS SERVER DETAIL**

NMS Server Detail View

General Information

Operating System	Microsoft Windows 7 Professional
Duration From Start	7 hrs, 54 mins, 43 secs
IP address	192.168.10.4
MAC address	64-31-50-36-20-13
Total Memory	3.97 GB
Free Memory	1.28 GB
JVM Total Memory	994.88 MB
JVM Free Memory	639.38 MB
JVM Memory Utilization (Current)	35.73 %
Total Disk Space	453.34 GB
Free Disk Space	257.51 GB

Average CPU and Memory Utilization (Today)

OS CPU Utilization

11%

OS Memory Utilization

54%

System Health

FTP Service	Up
TFTP Service	Up
Trap Service	Up
Syslog Service	Up
DB	Normal
Monitor Polling Service	Normal

Disk Utilization History

Type: Column Time: Last Hour

Server Disk Utilization(%)

CPU

Type: Column Time: Last Hour

Server CPU Utilization(%)

JVM Memory Utilization History

Type: Column Time: Last Hour

Server JVM Memory Utilization(%)

Memory

Type: Column Time: Last Hour

Server Memory Utilization(%)

Latest 10 Alarms

Alarm Name	Severity	Alarm Time
No data to display		

View Application Notifications

The application generates a notification when a task is completed. For example, if you initiated a firmware upgrade for one or more devices, the application generates a notification when the upgrade is completed. The notification includes details about whether the task completed successfully.

When the application generates one or more notifications, a small red-colored circle displays on top of the **Envelope** button in the top bar at the upper right of the screen. A number in the circle indicates the number of notifications that the application generated.

➤ **To view application notifications:**

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

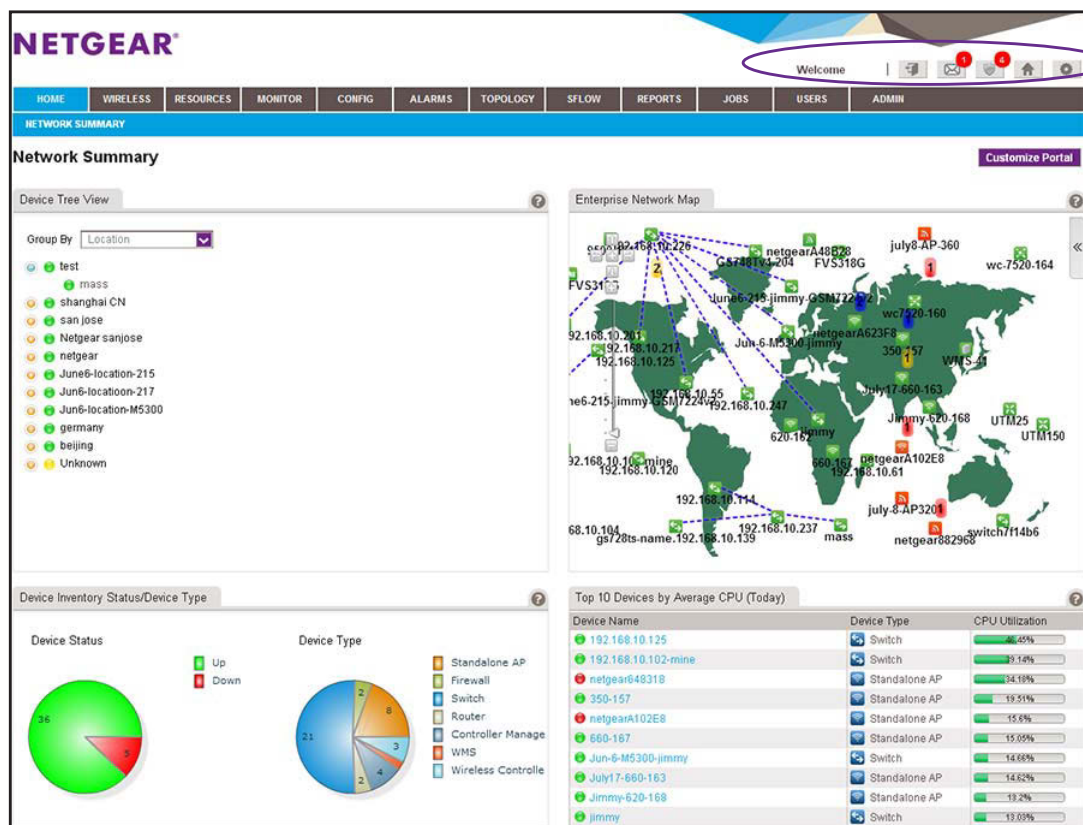
For more information, see *Log In to the Application* on page 18.

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.

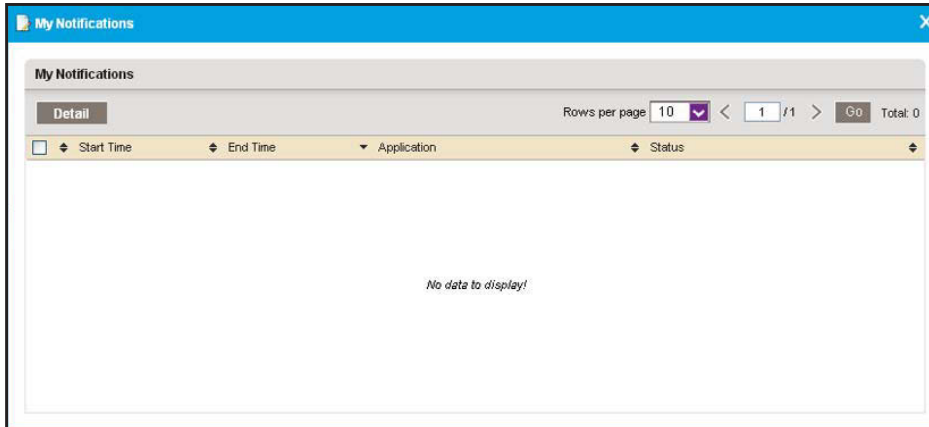
The Network Summary screen displays.



4. In the top bar at the upper right of the screen, click the **Envelope** button.



The My Notifications screen displays.



5. To view details about a notification, select the notification and click the **Details** button.
6. To close the screen, click the **X** (X) button.

5

5. Manage Configurations and Firmware

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:

- *Back Up Your Device Configurations*
- *Restore Your Device Configurations*
- *Import and Export Configuration Files to an External File Server*
- *Upgrade Firmware for One or More Devices*

Back Up Your Device Configurations

You can back up the configurations of the NETGEAR devices on your network.

You can schedule configuration backup jobs for future execution on a recurrent basis for batch operations.

The following sections describe the backup tasks:

- *Add or Modify a Backup Profile*
- *Execute a Backup Job*
- *Schedule a Backup Job*
- *View the Execution Status of a Backup Job*
- *Remove a Backup Profile*

Add or Modify a Backup Profile

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. You must create a backup profile before you can back up the configuration of one or more devices.

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

➤ To add a backup profile or modify an existing backup 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 18.

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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> FVS3180	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:49:45	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> OSM7224	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:45:28	<input checked="" type="checkbox"/> Partially Succeeded	
<input type="checkbox"/> StandAloneAPs_Backup	<input checked="" type="checkbox"/> Yes	Weekly			09/16/2013 11:52:00

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.

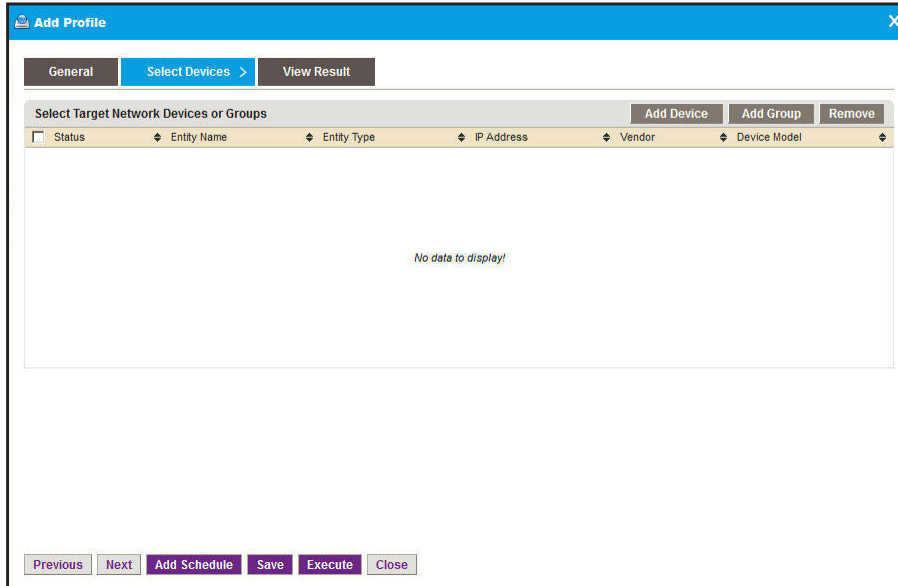
You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

6. Add a backup profile or modify an existing backup profile:
 - To add a backup profile, click the **Add Profile** button.
 - To modify an existing backup profile:
 - a. From the Backup table, select a backup profile.
 - b. Click the **Edit** button.

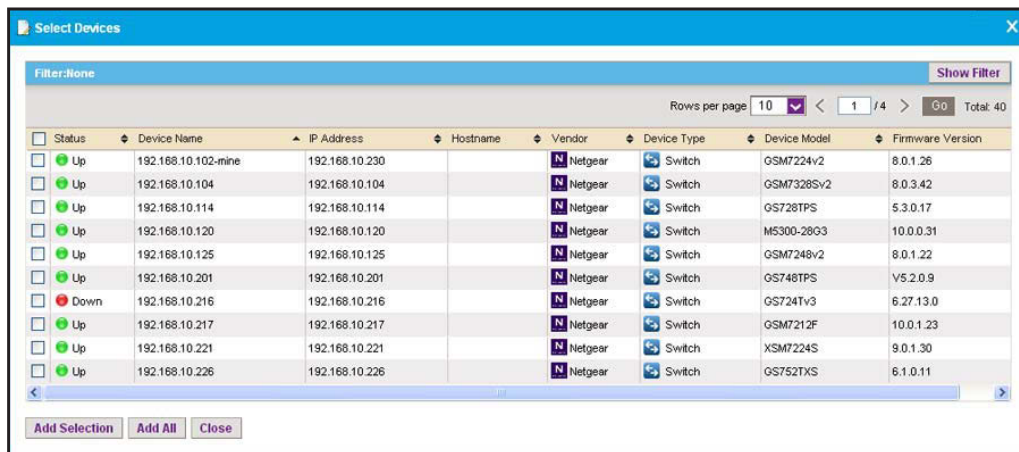
For a new backup profile, the Add Profile screen displays. For an existing backup profile, the Edit Profile screen displays.

7. 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.

8. Click the **Select Devices** tab.

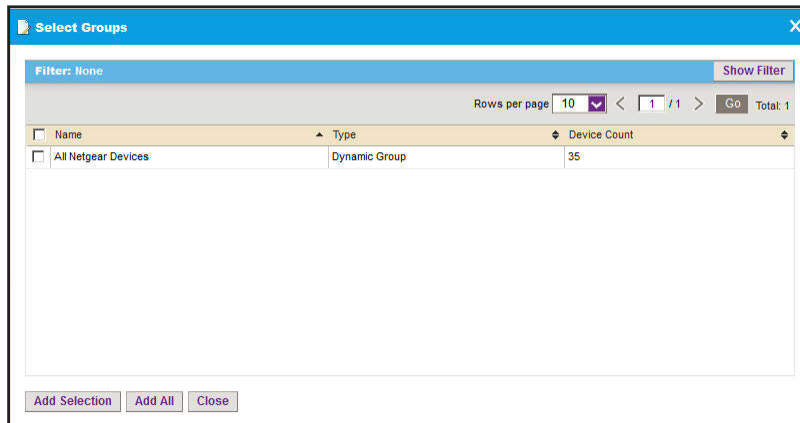


9. Add devices, device groups, or both:
 - a. Click the **Add Device** button.



- b. Select devices to add and click the **Add Selection** button.
To add all of 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 of 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.

10. If you are modifying an existing backup profile, to remove devices or groups:

- a. Select the devices or groups.
- b. Click the **Remove** button.

The devices or groups are removed from the Select Target Network Devices or Groups table.

11. To add a schedule, click the **Add Schedule** button.

You can schedule the generation of the report for a later time or let it recur automatically. For more information, see [Schedule a Backup Job](#) on page 117.

12. Click the **Save** button.

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

13. To execute the backup job, click the **Execute** button.

Your backup profile is executed immediately.

Execute a Backup Job

You can execute a one-time backup profile immediately. Executing a backup profile is referred as a backup job.

The application saves the backup configuration files on the NMS300 server and lists them on the Restore screen. You can use the backup files to restore device configurations for the devices on your network. For more information, see [Restore Your Device Configurations](#) on page 122.

The application saves configuration files from completed backup jobs for the data retention period. For more information, see [Set the Data Retention Period](#) on page 247.

➤ **To execute a backup profile immediately:**

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 18.

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**.

<input type="checkbox"/>	Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/>	FVS318G	No	Not Recurrent	09/10/2013 11:49:45	Succeeded	
<input type="checkbox"/>	GSM7224	No	Not Recurrent	09/10/2013 11:45:28	Partially Succeeded	
<input type="checkbox"/>	StandAloneAPs_Backup	Yes	Weekly			09/16/2013 11:52:00

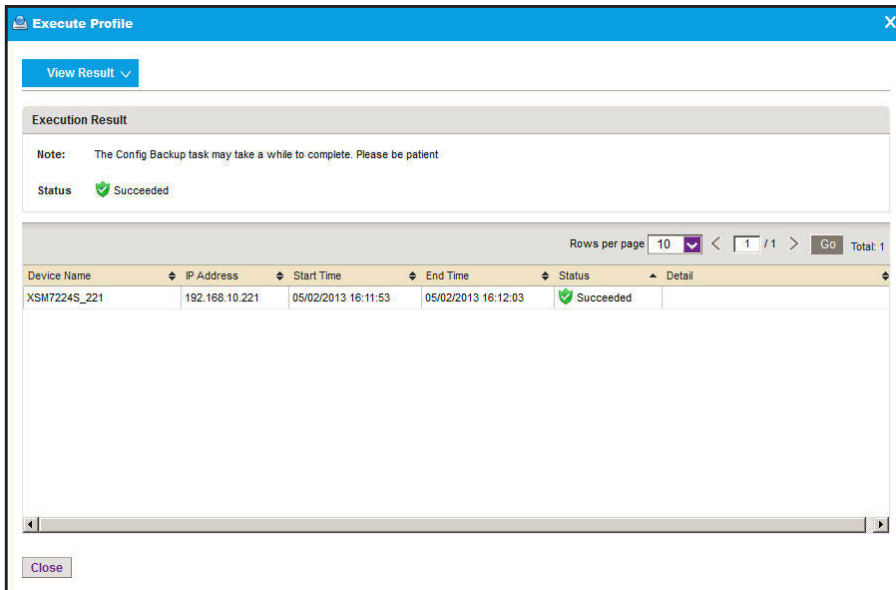
The Backup screen displays the existing backup profiles in the application.

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.

6. Select the backup profile.

- Click the **Execute Profile** button.



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

- Click the **Close** button.

The screen closes.

Schedule a Backup Job

You can schedule a backup job to occur later, either once or on a recurring basis.

➤ To schedule a backup job:

- 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 18.

- Enter your user name and password.

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

- Click the **Sign In** button.

The Network Summary screen displays.

4. Select **CONFIG > BACKUP**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> FVS318G	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:49:45	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> OSM7224	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:45:28	<input checked="" type="checkbox"/> Partially Succeeded	
<input type="checkbox"/> StandAloneAPs_Backup	<input checked="" type="checkbox"/> Yes	Weekly			09/16/2013 11:52:00

The Backup screen displays the existing backup profiles in the application.

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.

6. Select the backup profile.

7. Click the **Edit** button.

8. Click the **Add Schedule** button.

The screenshot shows a 'Schedule' dialog box with a blue header. Below the header is a section titled 'Execution Type & Status'. It contains two dropdown menus: 'Enable' is set to 'No' and 'Execution Type' is set to 'One time scheduled'. At the bottom of the dialog are two buttons: 'Submit' and 'Cancel'.

9. From the **Enable** menu, select **Yes**.
10. Specify whether the application executes the backup job once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering the corresponding information:
 - **One time scheduled.** This is the default selection.
In the **Starting On** field, enter a date and time.
 - **Recurrent.** The screen adjusts to display more fields.

The screenshot shows the 'Schedule' dialog box with more fields visible. In the 'Execution Type & Status' section, 'Enable' is now 'Yes' and 'Execution Type' is 'Recurrent'. Below this is the 'Starting On' section with a text field containing '04/30/2013 14:59:00'. The 'Recurrence' section shows 'Recurrence Type' set to 'Weekly' and 'Day of the Week' with 'Monday' checked. The 'Stopping On' section has two radio buttons: 'End Time' (unselected) and 'Never' (selected). 'Submit' and 'Cancel' buttons are at the bottom.

Enter the following information:

- a. In the **Starting On** field, enter a date and time.
 - b. From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.
 - c. Select the **End Time** radio button and enter the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.
11. Click the **Submit** button.

The Schedule screen closes. The backup job schedule becomes part of the backup profile.

- On the Edit Profile screen, click the **Save** button.

The backup job is executed according to the schedule that you set.

The application saves the backup configuration files on the NMS300 server and lists them on the Restore screen. You can use the backup files to restore device configurations for the devices on your network. For more information, see [Restore Your Device Configurations](#) on page 122.

The application saves configuration files from completed backup jobs for the data retention period. For more information, see [Set the Data Retention Period](#) on page 247.

View the Execution Status of a Backup Job

You can view the execution status of a backup job to ensure that a device configuration was backed up as scheduled.

➤ To view the status of a backup job:

- 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 18.

- Enter your user name and password.

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

- Click the **Sign In** button.

The Network Summary screen displays.

- Select **CONFIG > BACKUP**.

The screenshot shows the 'Backup' screen in the NMS300 application. The navigation bar at the top includes HOME, WIRELESS, RESOURCES, MONITOR, CONFIG (selected), ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. Below the navigation bar, there are tabs for RESTORE, BACKUP (selected), and IMAGE MANAGEMENT. The main content area is titled 'Backup' and contains a table with columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, and Next Execution Time. The table lists three backup profiles: FVS318G, OSM7224, and StandAloneAPe_Backup. The FVS318G profile is not scheduled and has a 'Succeeded' status. The OSM7224 profile is not scheduled and has a 'Partially Succeeded' status. The StandAloneAPe_Backup profile is scheduled for weekly backups and has a 'Succeeded' status.

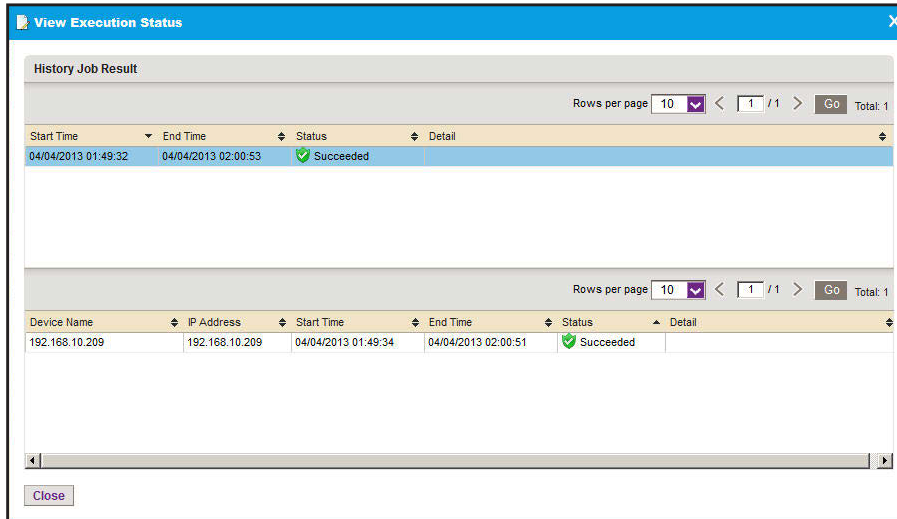
Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> FVS318G	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:49:45	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> OSM7224	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:45:28	<input checked="" type="checkbox"/> Partially Succeeded	
<input type="checkbox"/> StandAloneAPe_Backup	<input checked="" type="checkbox"/> Yes	Weekly			09/16/2013 11:52:00

The Backup screen displays the existing backup profiles in the application.

- 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.

6. Select the backup profile.
7. From the **More** menu, select **View Execution Status**.



The screen displays the execution history of a job and whether the job succeeded or failed.

8. Click the **Close** button.
The screen closes.

Remove a Backup Profile

If you delete a backup job from the Jobs table, the application deletes the backup profile for the job automatically. For more information, see [View and Manage Jobs](#) on page 234. You can also remove a backup profile manually.

➤ To remove a backup profile manually:

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 18.

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**.

Name	Scheduled	Recurrent Type	Last Execution Time	Last Execution Status	Next Execution Time
<input type="checkbox"/> FVS318G	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:49:45	<input checked="" type="checkbox"/> Succeeded	
<input type="checkbox"/> OSM7224	<input checked="" type="checkbox"/> No	Not Recurrent	09/10/2013 11:45:28	<input checked="" type="checkbox"/> Partially Succeeded	
<input type="checkbox"/> StandAloneAPs_Backup	<input checked="" type="checkbox"/> Yes	Weekly			09/16/2013 11:52:00

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.

6. Select the backup profile.
7. From the **More** menu, select **Delete Profile**.

A pop-up confirmation screen displays.

8. Click the **Yes** button.

The backup profile is removed from the Backup table and deleted.

Restore Your Device Configurations

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. For more information, see [Restore the Configuration of a Single Device](#) on page 123.
- **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 [Customize and Promote a Configuration File](#) on page 127 or [Promote a Configuration File for an FVS318G Firewall](#) on page 130 and [Restore the Configuration of Several Identical Devices](#) on page 134.

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 [Set the Data Retention Period](#) on page 247.

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 [Import a Configuration File](#) on page 138. The Restore table also displays the configuration files that you imported.

**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.

The following sections describe the tasks that you can perform with device configuration files:

- *Restore the Configuration of a Single Device*
- *Customize and Promote a Configuration File*
- *Promote a Configuration File for an FVS318G Firewall*
- *Restore the Configuration of Several Identical Devices*
- *Import a Configuration File*
- *Export a Configuration File*
- *Modify a Configuration File*
- *Remove a Configuration File*
- *Compare Two Configuration Files*

Restore the Configuration of a Single Device

You can restore the configuration of a single device immediately or schedule the application to restore the configuration later.

➤ **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 18.

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**.

File Name	Device Name	File Type	Create Time	Device Type	Size (KB)	Promoted
215	June6-215-jimmy-GSM7224v2	Text	09/10/2013 13:15:14	Switch	2.11	No
backup-prof-1	192.168.10.61	Text	09/10/2013 12:24:08	Switch	1.31	No
backup-prof-1	192.168.10.55	Text	09/10/2013 12:23:41	Switch	1.08	No
backup-prof-1	192.168.10.120	Text	09/10/2013 12:23:41	Switch	2.81	No

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.

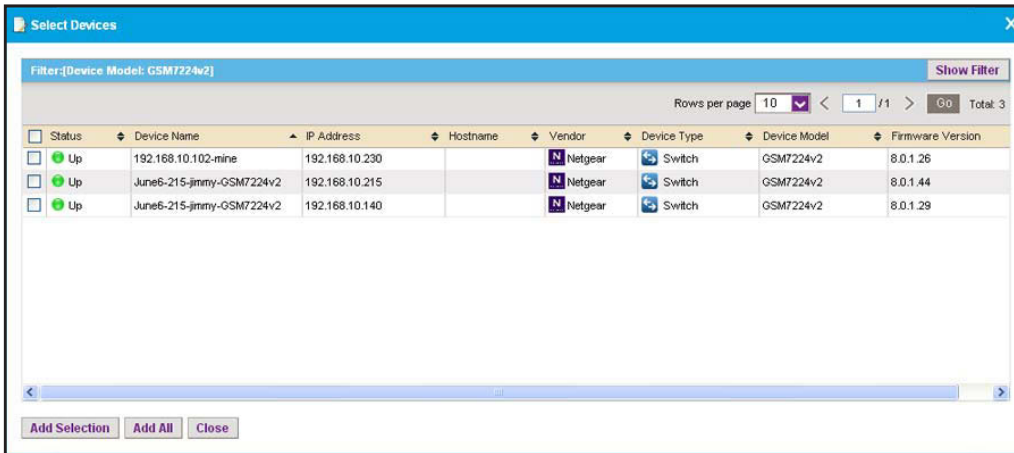
You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

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

7. Select the configuration file.

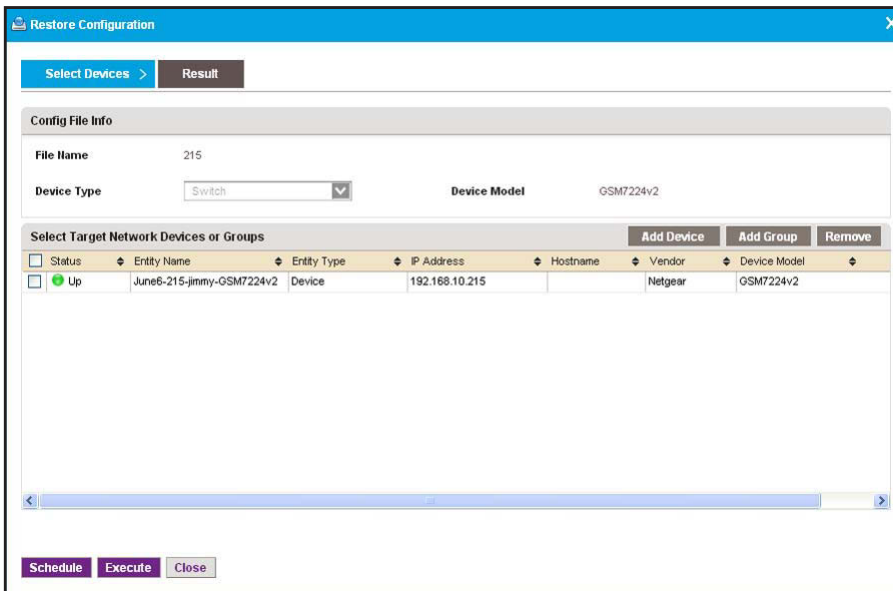
8. Click the **Restore Configuration** button.

- Click the **Add Device** button.



- Select the device.
- Click the **Add Selection** button.

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



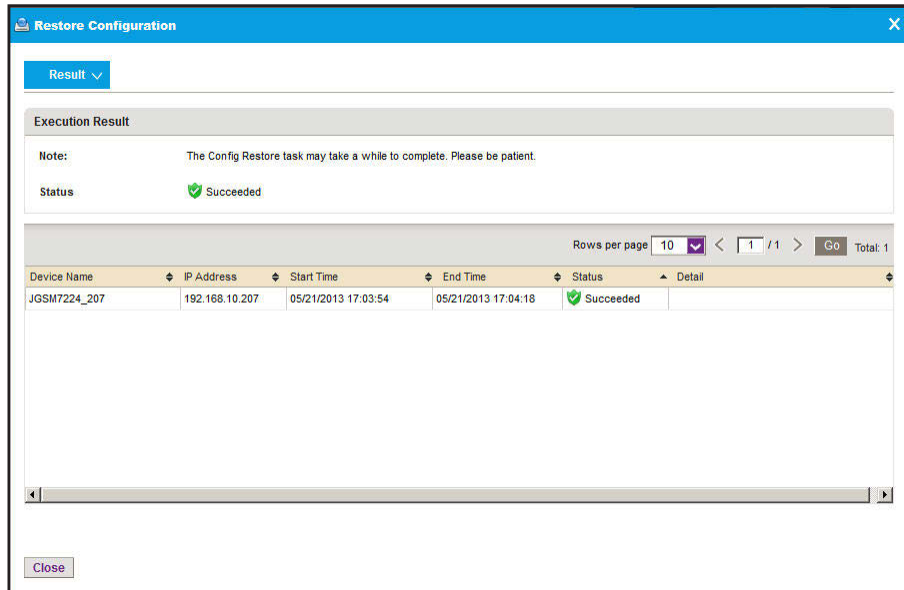
CAUTION:

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:

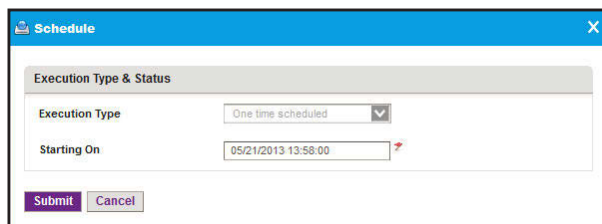
- **Execute.** Restores the configuration file immediately.

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.



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

The restore procedure is executed once at the specified time.

Customize and Promote a Configuration File

To use the configuration file of a device as a template to configure a collection of devices (see *Restore the Configuration of Several Identical Devices* on page 134), you first must customize the file for your network configuration and promote the file.

You cannot use a promoted file to configure the following types of devices and firewall models:

- Wireless controllers
- Wireless management systems
- Storage devices
- Any compatible NETGEAR device that does not support a text-based configuration file
- FVS318N firewall
- FVS336Gv2 firewall
- FVS336Gv3 firewall
- SRX5308 firewall

Note: For information about using a configuration file as a template to configure several NETGEAR FVS31G firewalls, see *Promote a Configuration File for an FVS318G Firewall* on page 130.



CAUTION:

NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➤ **To customize and promote a configuration file:**

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 18.

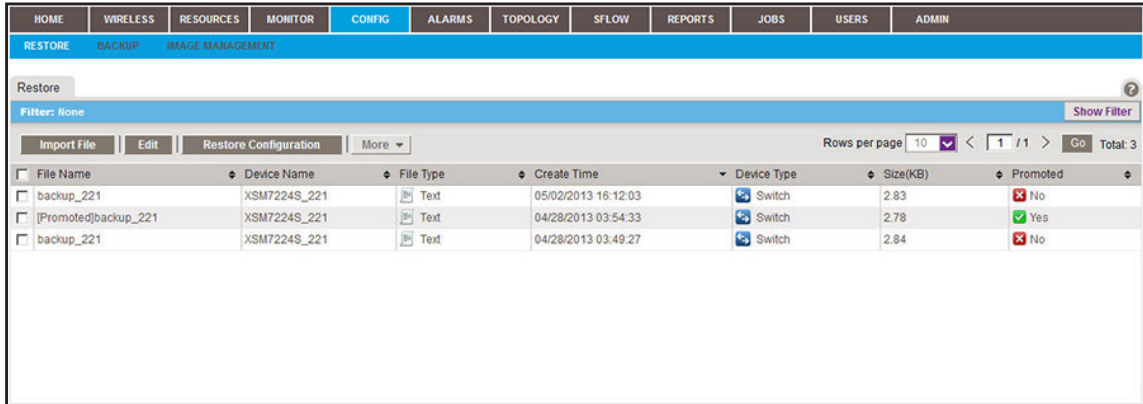
2. Enter your user name and password.

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.

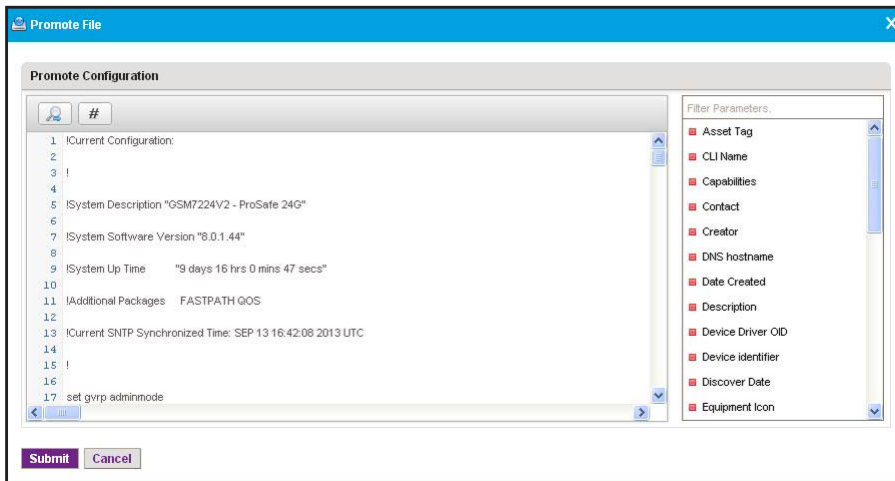
You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

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. From the **More** menu, select **Promote File**.



9. Modify the configuration file by inserting a preconfigured parameter in the configuration file.

The application substitutes the parameter that you insert with the actual value that it obtains from the device through monitoring.

- a. Select the line of code that you want to modify.

The following figure shows an example of a line of code.

```
network parms 192.168.10.202 255.255.255.0 192.168.10.1
```

- b. Erase the value and leave the cursor positioned where you want the parameter inserted in the line of code.

The following figure shows the example of *Step a* after you erased 192.168.10.202 from the line of code.

```
network parms 255.255.255.0 192.168.10.1
```

- c. Double-click a parameter in the Filter Parameters table.

The following figure shows the preconfigured IP Address parameter that you can select from the Filter Parameters table.

```
IP Address
```

The application inserts the parameter at the position of the cursor in the line of code.

The following figure shows the example of *Step a* after you inserted the IP Address parameter in the line of code.

```
network parms $IPAddress$ 255.255.255.0 192.168.10.1
```

10. Repeat *Step 9* until you made all your changes in the configuration file.



CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that any changes that you make on the Promote Configuration screen do not corrupt the configuration file. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file when it executes the configuration restore job and you can damage the device.

11. Click the **Submit** button.

The Promote File screen closes and the promoted configuration file is listed in the Restore table.

Promote a Configuration File for an FVS318G Firewall

To use the configuration file of a single NETGEAR FVS318G firewall as a template to configure a collection of NETGEAR FVS318G firewalls (see *Restore the Configuration of Several Identical Devices* on page 134), you must promote the configuration file but can retain the existing configurations for the following features:

- ISP login and type of ISP
- WAN Internet (IP) address and DNS servers
- Dynamic DNS configuration
- SNMP configuration
- Time Zone

For each of these features, you can decide to either retain the existing configuration on the firewalls or overwrite the configuration for the feature with the one from the promoted configuration file. The firewalls obtain all other features that are not stated in the previous list from the promoted configuration file.

Note: You cannot promote a configuration file for the FVS318N, FVS336Gv2, FVS336Gv2, or SRX5308 firewall.



CAUTION:

NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➤ To promote a configuration file for an FVS318G firewall:

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 18.

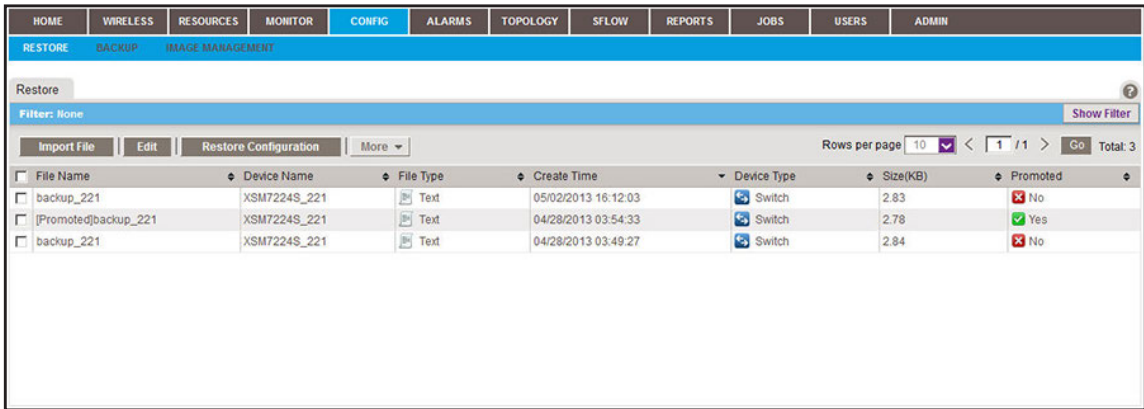
2. Enter your user name and password.

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.

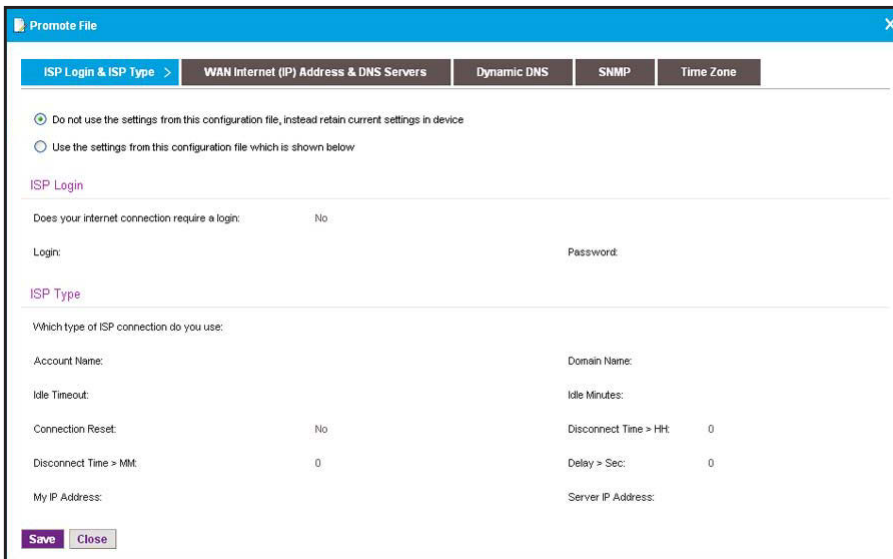
6. To filter the configuration files that are listed, click the **Show Filter** button.

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 for an FVS318G firewall.

8. From the **More** menu, select **Promote File**.



9. Select one of the following radio buttons:

- **Do not use the settings from this configuration file, instead retain current settings in device.**
- **Use the settings from this configuration file which is shown below.**

10. Click the **WAN Internet (IP) Address Servers** tab.

Promote File

ISP Login & ISP Type | **WAN Internet (IP) Address & DNS Servers** > | Dynamic DNS | SNMP | Time Zone

Do not use the settings from this configuration file, instead retain current settings in device
 Use the settings from this configuration file which is shown below

Internet (IP) Address

Get Dynamically from ISP/Use Static IP Address: Use Static IP Address

Client Identifier Checkbox: Client Identifier Name:

Vendor Class Identifier:

IP Address: 66.166.147.252 IP Subnet Mask: 255.255.255.0

Gateway IP Address: 66.166.147.249

Domain Name Server (DNS) Servers

Get Automatically from ISP/Use These DNS Servers: Use These DNS Servers

Primary DNS Server: 8.8.8.8 Secondary DNS Server: 0.0.0.0

Save Close

11. Select one of the following radio buttons:

- **Do not use the settings from this configuration file, instead retain current settings in device.**
- **Use the settings from this configuration file which is shown below.**

12. Click the **Dynamic DNS** tab.

Promote File

ISP Login & ISP Type | WAN Internet (IP) Address & DNS Servers | **Dynamic DNS** > | SNMP | Time Zone

Do not use the settings from this configuration file, instead retain current settings in device
 Use the settings from this configuration file which is shown below

Dynamic DNS

DNS Type: Not Set Domain Name:

User Name/Email: Password/Key:

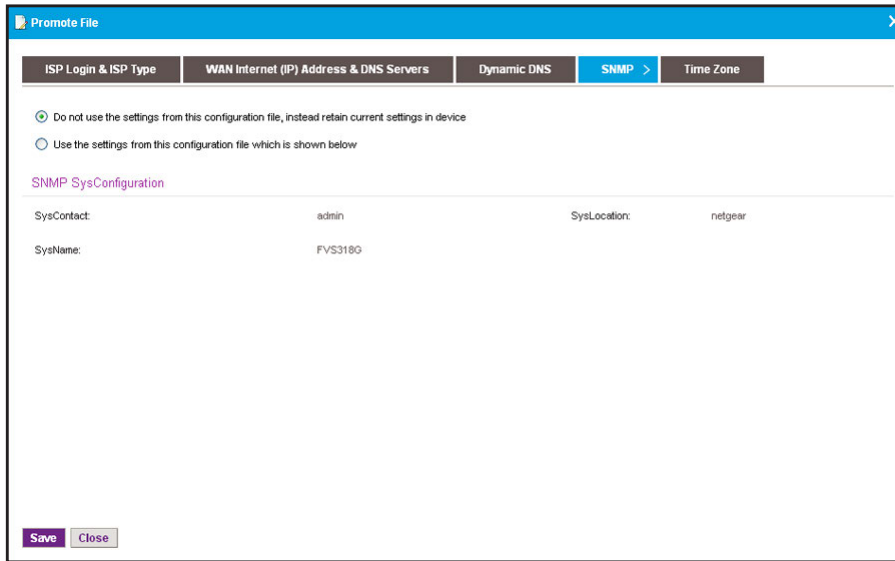
Use wildcards: No Update every 30 days: No

Save Close

13. Select one of the following radio buttons:

- **Do not use the settings from this configuration file, instead retain current settings in device.**
- **Use the settings from this configuration file which is shown below.**

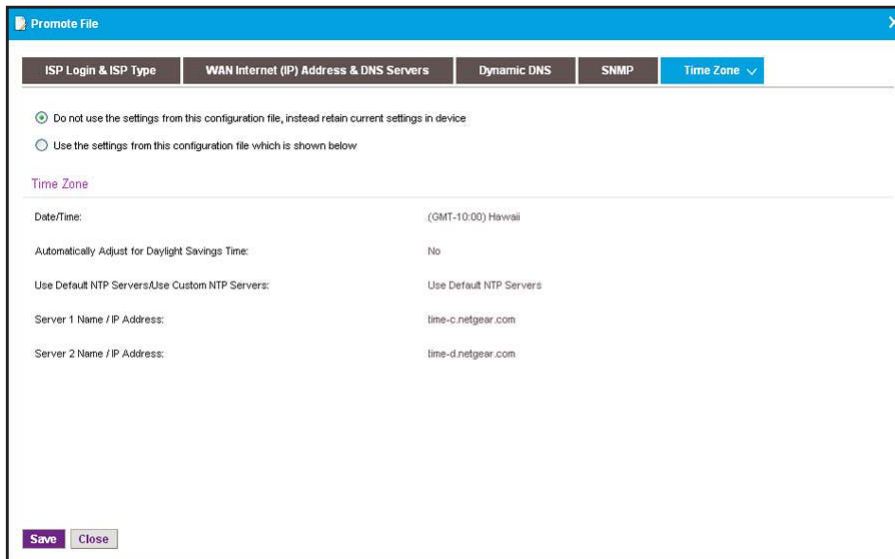
14. Click the **SNMP** tab.



15. Select one of the following radio buttons:

- **Do not use the settings from this configuration file, instead retain current settings in device.**
- **Use the settings from this configuration file which is shown below.**

16. Click the **Time Zone** tab.



**CAUTION:**

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that you configure the configuration file correctly. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file when it executes the configuration restore job and you can damage the device.

17. Click the **Save** button.

The Promote File screen closes and the promoted configuration file is listed in the Restore table.

Restore the Configuration of Several Identical Devices

You can use the configuration file of one of the devices on your network to create a template configuration for several identical devices on your network. You must promote this template configuration file before you can use it to restore the configuration of several devices (see *Customize and Promote a Configuration File* on page 127 or *Promote a Configuration File for an FVS318G Firewall* on page 130). Otherwise, the restore procedure fails.

You can restore the configuration of several devices immediately or schedule the application to restore the configuration later.

**CAUTION:**

NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➤ **To configure several identical devices:**

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 18.

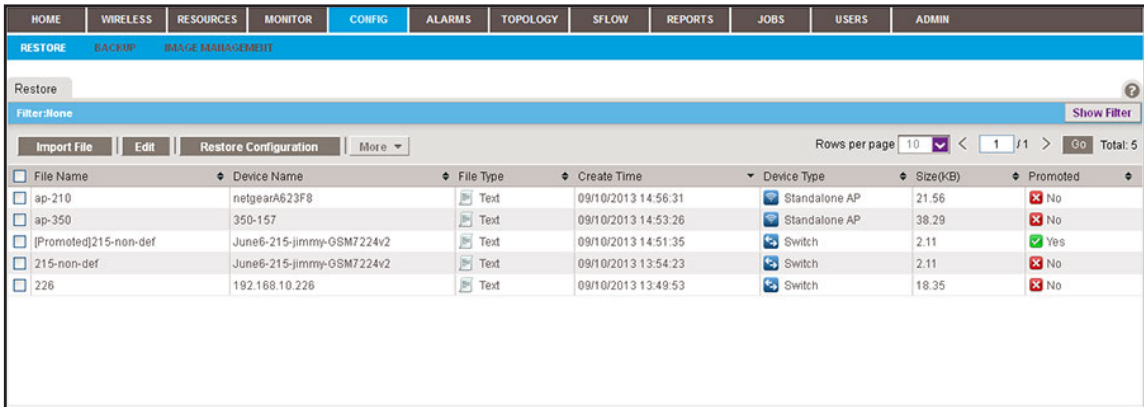
2. Enter your user name and password.

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.

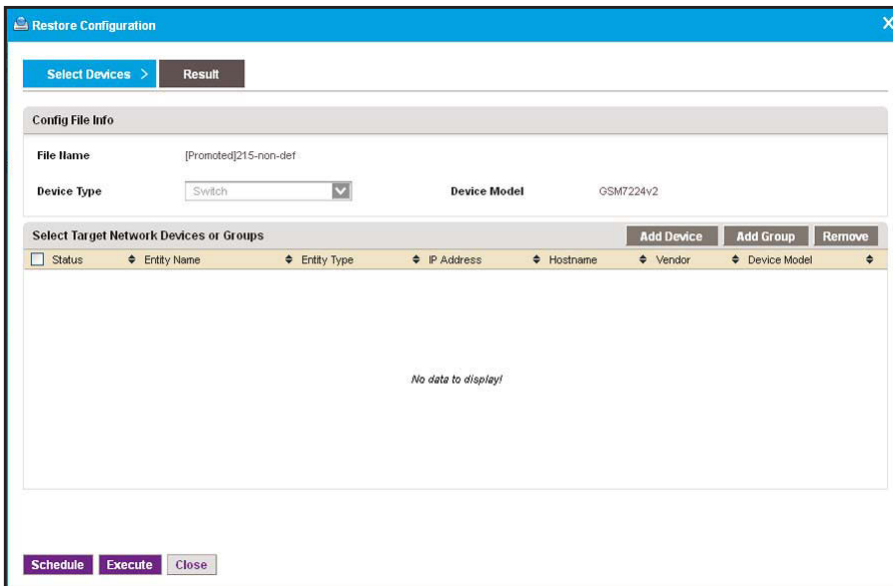
You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

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 promoted configuration file.
 8. Click the **Restore Configuration** button.



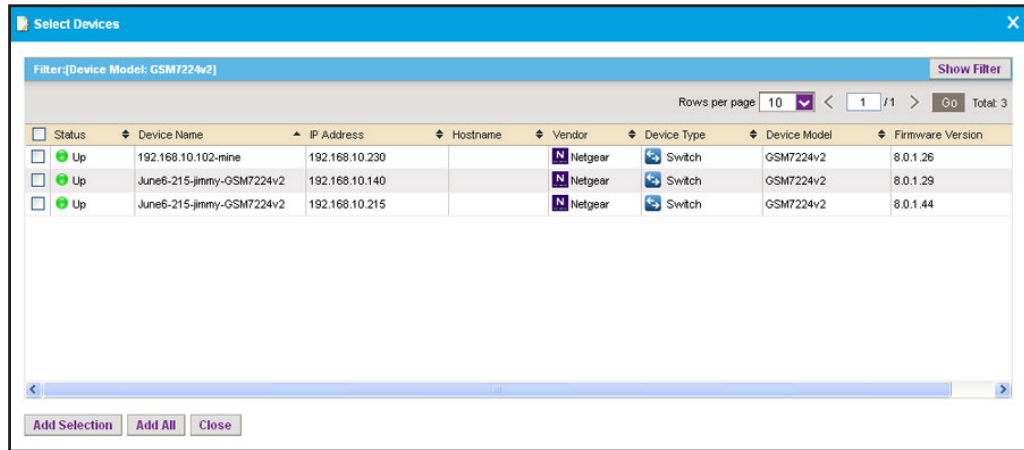
9. Select the target network devices or groups.



CAUTION:

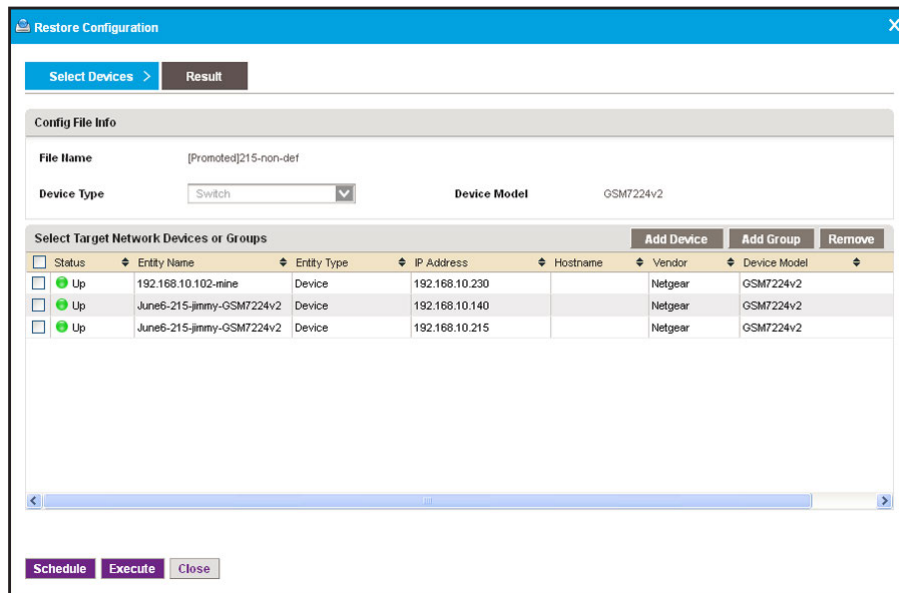
Make sure that you select the correct devices or device groups. Selecting the wrong devices or device groups for the selected configuration file can damage the devices.

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

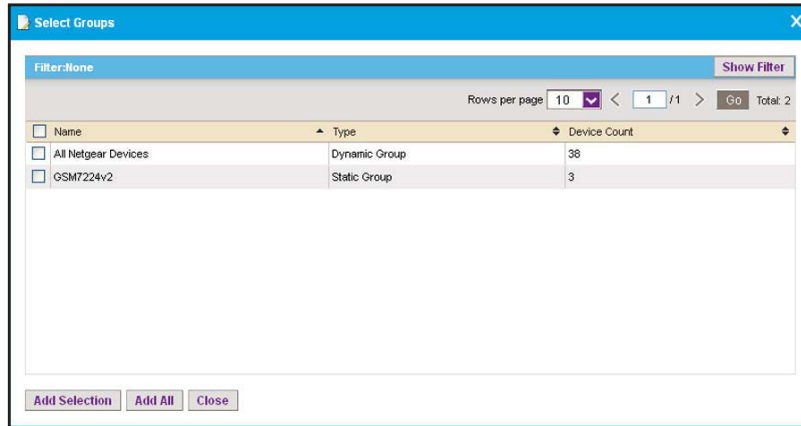


- b. Select the devices you want to add and click the **Add Selection** button.
To add all devices, click the **Add All** button.

The screen closes and the selected devices are listed on the Restore Configuration screen.

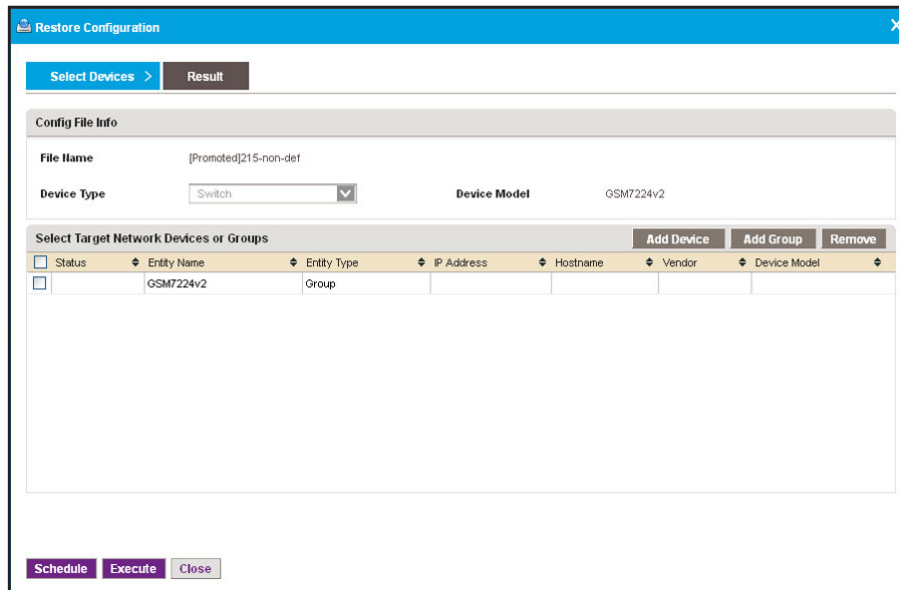


- To add device groups:
 - a. Click the **Add Group** button.



- b. Select the groups you want to add and click the **Add Selection** button.
To add all groups, click the **Add All** button.

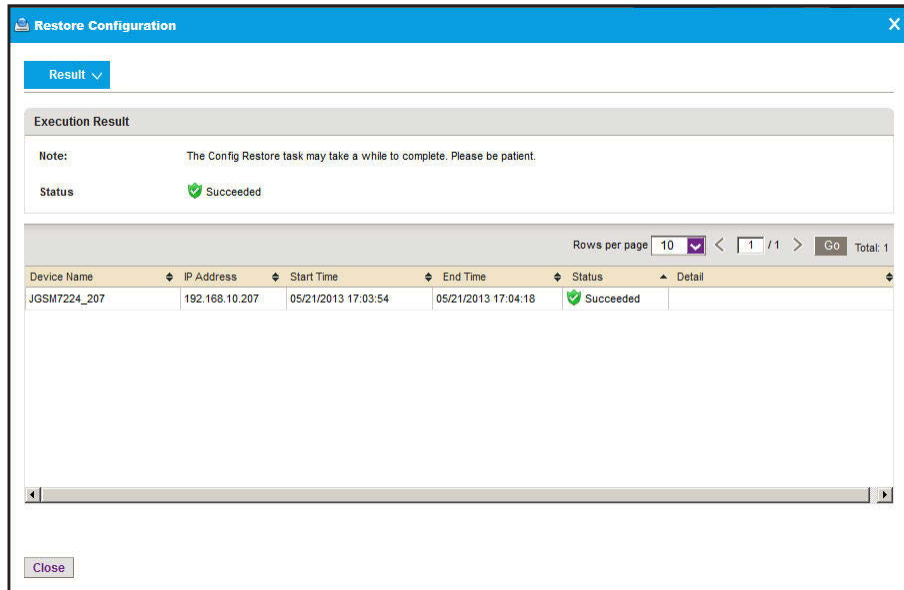
The screen closes and the selected groups are listed on the Restore Configuration screen.



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

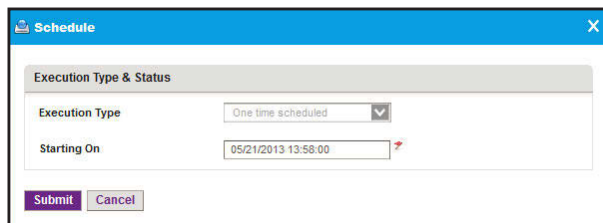
- **Execute.** Restores the configuration file immediately.

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.



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

The restore procedure is executed once at the specified time.

Import a Configuration File

You can import a configuration file for a device. 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 configuration file that you want to import.

➤ To import a configuration file for a 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 18.

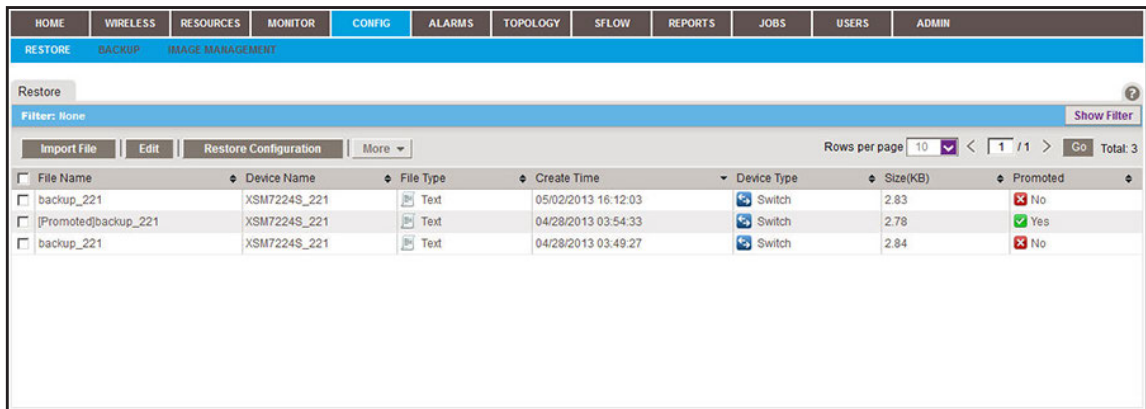
2. Enter your user name and password.

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

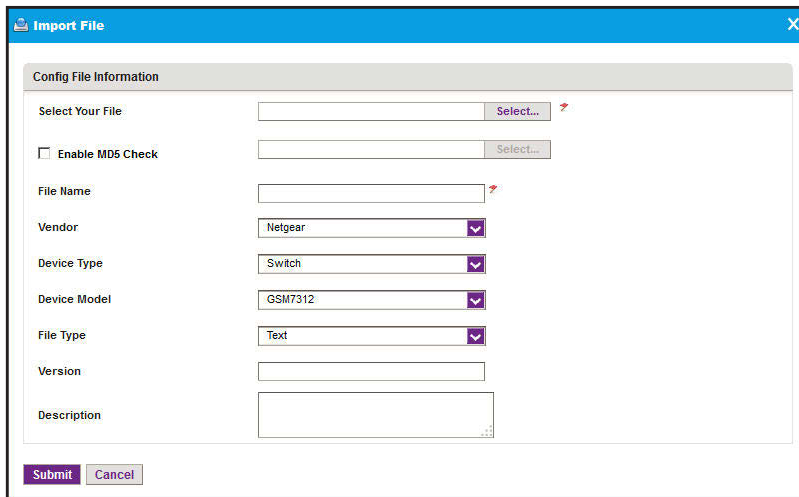
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **CONFIG > RESTORE**.



5. Click the **Import File** button.



6. Specify the following information:

- **Select Your File.** Click the **Select** button.

Select the image file 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 configuration file that you want to use.
- **Vendor.** Select the vendor of the device.
- **Device Type.** Select the device type.

- **Device Model.** Select the device model.
 - **File Type.** Select the file type.
 - **Version.** Enter the version of the configuration file.
 - **Description.** Enter a description of the configuration file.
7. Click the **Submit** button.
- The Import File screen closes and the imported file is listed in the Restore table.

Export a Configuration File

You can export a configuration file for a device.

➤ **To export a configuration file for a 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 18.

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**.

File Name	Device Name	File Type	Create Time	Device Type	Size(KB)	Promoted
<input type="checkbox"/> backup_221	XSM7224S_221	Text	05/02/2013 16:12:03	Switch	2.83	<input type="checkbox"/> No
<input type="checkbox"/> [Promoted] backup_221	XSM7224S_221	Text	04/28/2013 03:54:33	Switch	2.78	<input checked="" type="checkbox"/> Yes
<input type="checkbox"/> backup_221	XSM7224S_221	Text	04/28/2013 03:49:27	Switch	2.84	<input type="checkbox"/> No

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. From the **More** menu, select **Export File**.
9. To save the file on your computer, follow the directions of your browser.

Modify a Configuration File

You can modify a configuration file except for the configuration file for a NETGEAR firewall. The configuration file of a NETGEAR firewall includes content in hexadecimal format.



CAUTION:

NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➤ To modify a configuration file:

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 18.

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**.

File Name	Device Name	File Type	Create Time	Device Type	Size(KB)	Promoted
<input type="checkbox"/> backup_221	XSM7224S_221	Text	05/02/2013 16:12:03	Switch	2.83	<input type="checkbox"/> No
<input type="checkbox"/> [Promoted]backup_221	XSM7224S_221	Text	04/28/2013 03:54:33	Switch	2.78	<input checked="" type="checkbox"/> Yes
<input type="checkbox"/> backup_221	XSM7224S_221	Text	04/28/2013 03:49:27	Switch	2.84	<input type="checkbox"/> No

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.

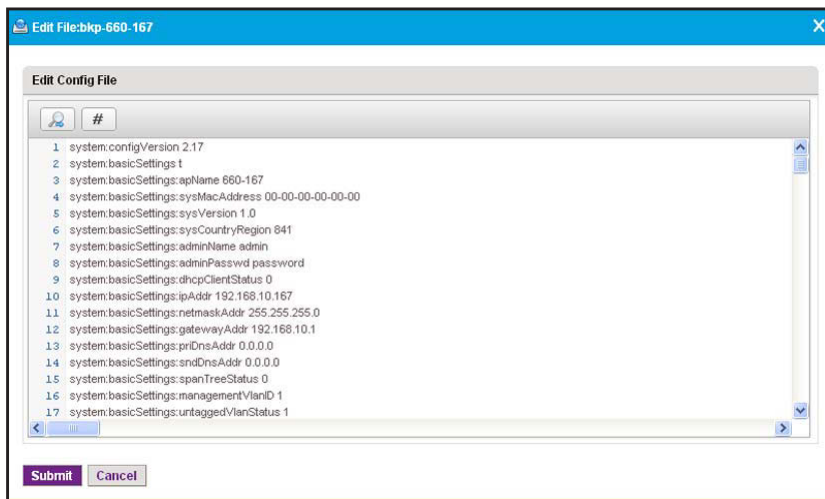
You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

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 **Edit** button.



9. Modify the configuration file by changing, inserting, deleting, or overwriting information.

The following tools are at your disposal:

- **Looking glass icon.** Displays the Find/Replace pop-up screen.
- **Number sign icon.** Displays the Jump to Line pop-up screen.



CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that any changes that you make to the configuration file do not corrupt the file. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file while it executes the configuration restore job and you can damage the device.

10. Click the **Submit** button.

The modified file is saved and the screen closes.

Remove a Configuration File

You can remove a configuration file that you no longer need.

➤ To remove a configuration file:

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 18.

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**.

File Name	Device Name	File Type	Create Time	Device Type	Size(KB)	Promoted
<input type="checkbox"/> backup_221	XSM7224S_221	Text	05/02/2013 16:12:03	Switch	2.83	No
<input type="checkbox"/> [Promoted]backup_221	XSM7224S_221	Text	04/28/2013 03:54:33	Switch	2.78	Yes
<input type="checkbox"/> backup_221	XSM7224S_221	Text	04/28/2013 03:49:27	Switch	2.84	No

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. From the **More** menu, select **Delete File**.

A pop-up confirmation screen displays.

9. Click the **Yes** button.

The file is removed from the Restore table and deleted.

Compare Two Configuration Files

You can compare two configuration files. The files must be text files. You cannot compare binary files.

➤ **To compare two configuration files:**

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 18.

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**.

File Name	Device Name	File Type	Create Time	Device Type	Size(KB)	Promoted
backup_221	XSM7224S_221	Text	05/02/2013 16:12:03	Switch	2.83	No
Promoted backup_221	XSM7224S_221	Text	04/28/2013 03:54:33	Switch	2.78	Yes
backup_221	XSM7224S_221	Text	04/28/2013 03:49:27	Switch	2.84	No

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.

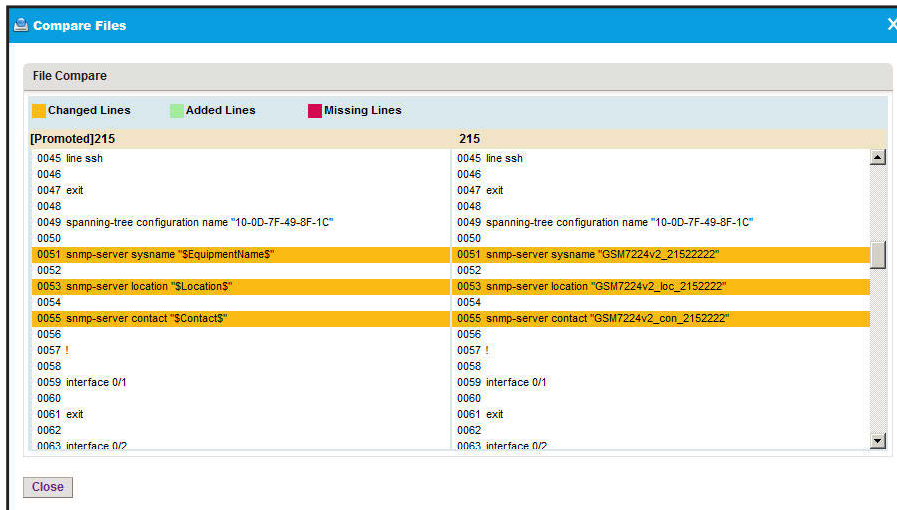
To hide the filter, click the **Hide Filter** button.

7. Select the two configuration files that you want to compare.

Both files must be text files.

8. From the **More** menu, select **Compare Files**.

A screen similar to the following one displays.



The left and right side of the screen each display one of the selected files. The screen highlights changed lines in yellow, added lines in green, and missing lines in red.

9. Click the **Close** button.

The screen closes.

Import and Export Configuration Files to an External File Server

By default, the application saves and retrieves configuration files from the NMS300 server. However, if you set up an external file server (see [Set Up an External File Server](#) on page 246), you can retrieve (import) and save (export) configuration files, including backup files, to the external file server.

For each type of device, you can transfer only the entire file directory that includes all configuration files for the type of device. You cannot transfer individual configuration files. For example, if you export the file directory for switches, *all* configuration files for *all* switches are exported. Similarly, if you import the file directory for standalone APs, *all* configuration files for *all* standalone APs are imported.

Note: After file directories are transferred from the NMS300 server to an external file server (that is, the directories are exported), the application deletes the file directories from the NMS300 server. Similarly, after file directories are transferred from the external file server to the NMS300 server (that is, the directories are imported), the application deletes the file directories from the external file server.

➤ **To import or export configuration file directories to an external file 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 18.

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.

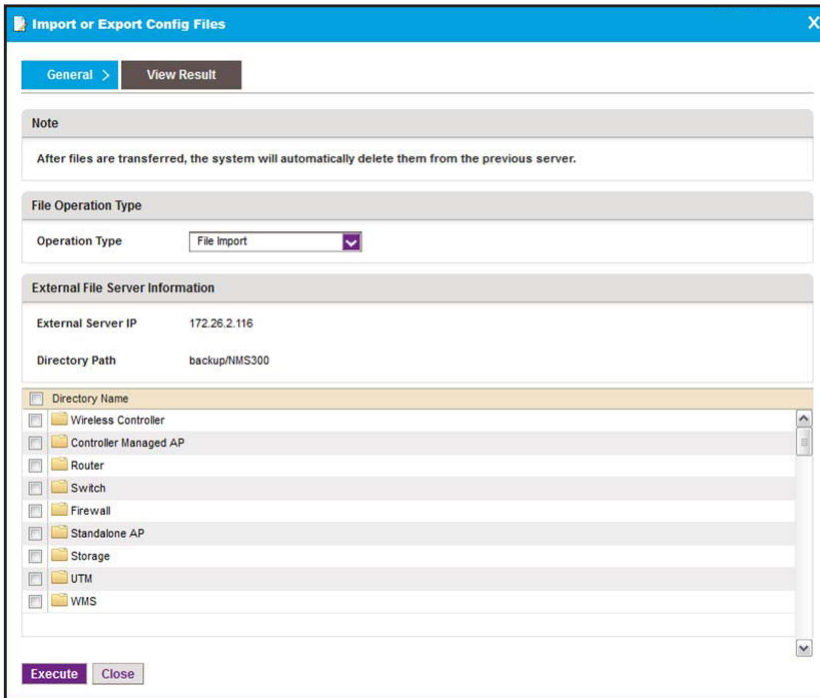
The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.

The screenshot shows the 'ADMIN > SETTINGS' page. The navigation bar includes: HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. Below the navigation bar, there are sub-sections: SETTINGS, AUDIT LOG, and LICENSE MANAGEMENT. The main content area is titled 'System and Website Settings' and contains several configuration panels:

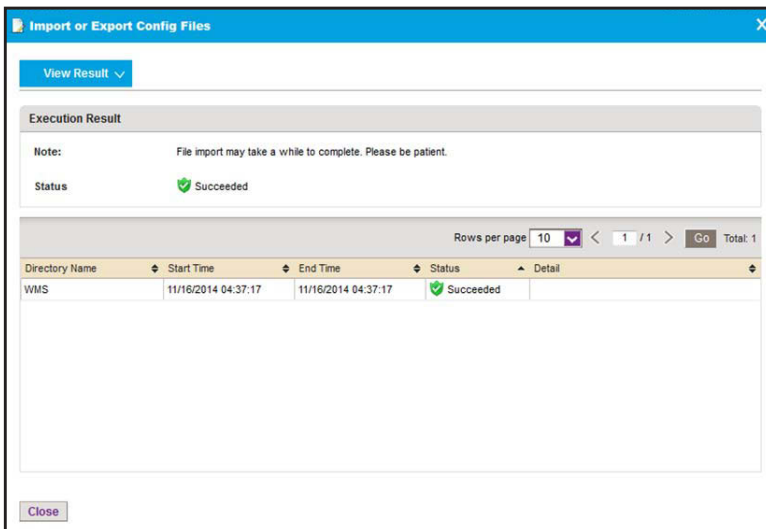
- Getting Started with NMS:** Discover your network and add the devices you want to manage.
 - > Discover Devices
 - > SMTP Email Settings
 - > SMS Server Settings
 - > Device Groups
- System Settings:** Set global settings for the system and website.
 - > Data Retention Period
 - > Inventory Polling
 - > Idle Time Out
 - > Real-time Chart
- Customize:** Customize the navigation and look of your web portal.
 - > Customize Network Summary View
 - > Customize Wireless Summary
 - > Customize Alarm Color
 - > Auto Refresh Setting
 - > Customize Network Dashboard
- Account Information:** View or modify users, or create new users.
 - > User Management
 - > Edit Account
 - > Change Password
- Manage Monitor and Alarm:** Network monitor, alarm and threshold related configurations.
 - > Alarm Configuration
 - > Monitor Configuration
- my.NETGEAR.com Account Profile:** Configure and validate my.NETGEAR.com account profile through my.NETGEAR.com Web API.
 - > my.NETGEAR.com Account Profile
- sFlow:** Set sFlow related configurations.
 - > sFlow Settings
 - > Manage sFlow Source
- Manage External File Server:** External File Server configurations and File Processing with External File Server.
 - > External File Server Setting
 - > Import or Export Config Files (circled in red)
- License And Version Information:** View NMS300 license, supported device and version information.
 - > License Management
 - > NMS300 Version

- Under Manage External File Server, click the **Import or Export Files** link.



- From the **Operation Type** menu, select **File Import** or **File Export**.
- In the **Directory Name** table, select the check boxes for the individual directories, or select the check box in the table heading for all directories.
- Click the **Execute** button.

The directories transfer to or from the external file server and the results display.



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](#)
- [Modify the File Name, Version Information, and Description for a Firmware File](#)
- [Export a Firmware File](#)
- [Remove a Firmware File](#)

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 18.

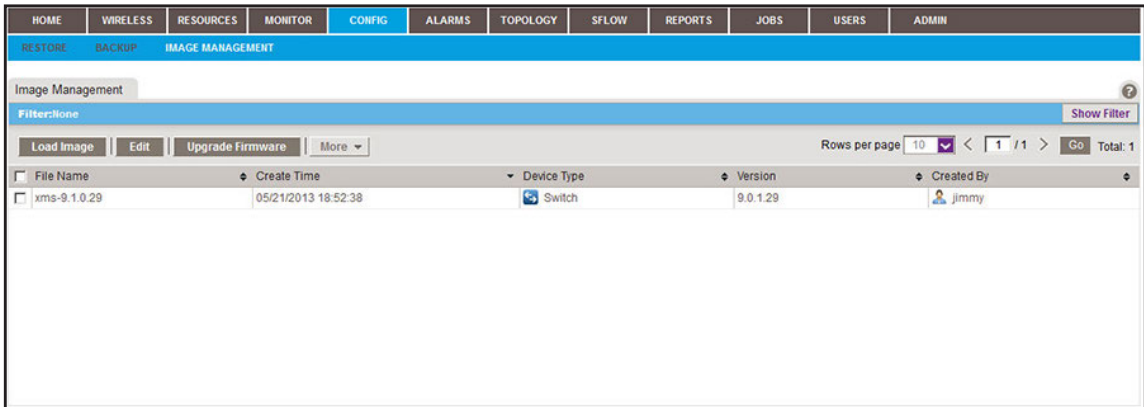
2. Enter your user name and password.

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

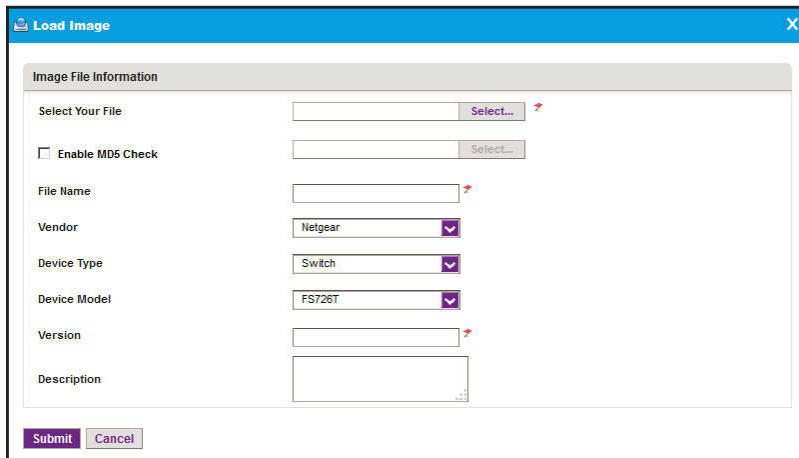
3. Click the **Sign In** button.

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 file 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 *Set the Data Retention Period* on page 247.

Execute or Schedule a Firmware Upgrade

After you import a firmware file into the NMS300 server (see *Import a Firmware File* on page 148), 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 18.

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**.

The screenshot shows the 'IMAGE MANAGEMENT' section of the NMS300 application. It features a navigation menu at the top with options like HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. Below the menu, there are tabs for RESTORE, BACKUP, and IMAGE MANAGEMENT. The main area contains a table with columns for File Name, Create Time, Device Type, Version, and Created By. The table lists three files: 'fns_3.1.1.11' (Firewall), 'm5300_10.0.0.31' (Switch), and '7520_2.5.0.5' (Wireless Controller). A 'Show Filter' button is visible in the top right corner of the table area.

File Name	Create Time	Device Type	Version	Created By
<input type="checkbox"/> fns_3.1.1.11	09/13/2013 09:28:19	Firewall	3.1.1.11	jitrn
<input type="checkbox"/> m5300_10.0.0.31	09/13/2013 09:27:27	Switch	10.0.0.31	jitrn
<input type="checkbox"/> 7520_2.5.0.5	09/13/2013 09:26:27	Wireless Controller	2.5.0.5	jitrn

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.

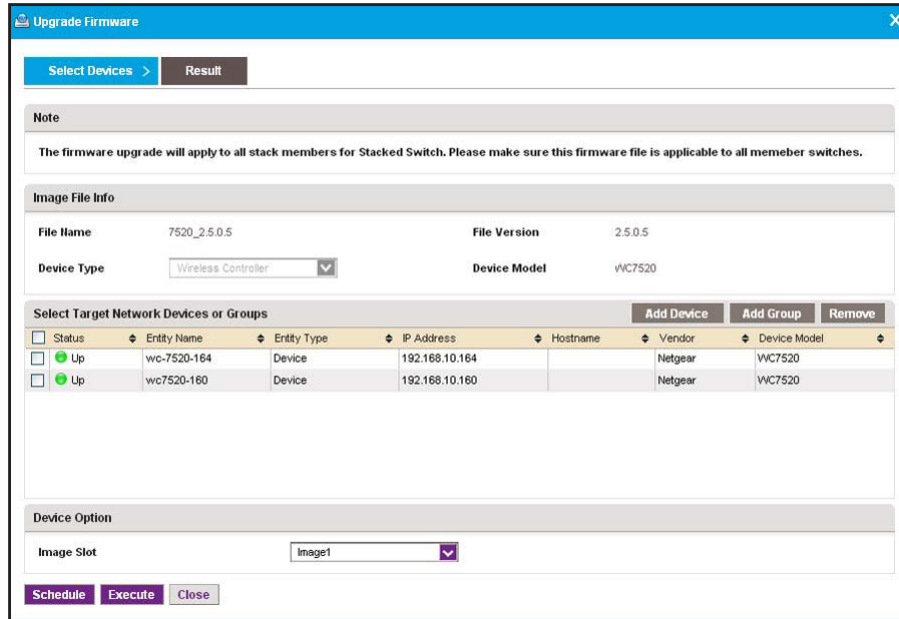
- To specify individual devices:
 - a. Click the **Add Device** button.

Status	Device Name	IP Address	Hostname	Vendor	Device Type	Device Model	Firmware
Up	wc-7520-164	192.168.10.164		Netgear	Wireless Controller	WC7520	
Up	wc7520-160	192.168.10.160		Netgear	Wireless Controller	WC7520	

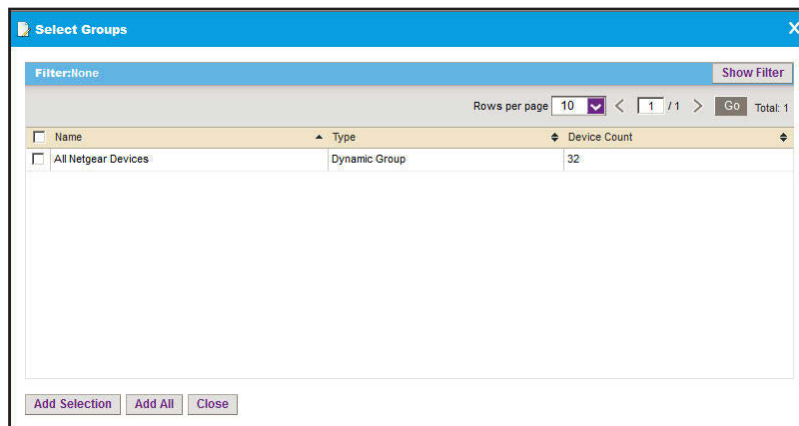
- b. Select devices and click the **Add Selection** button.

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

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



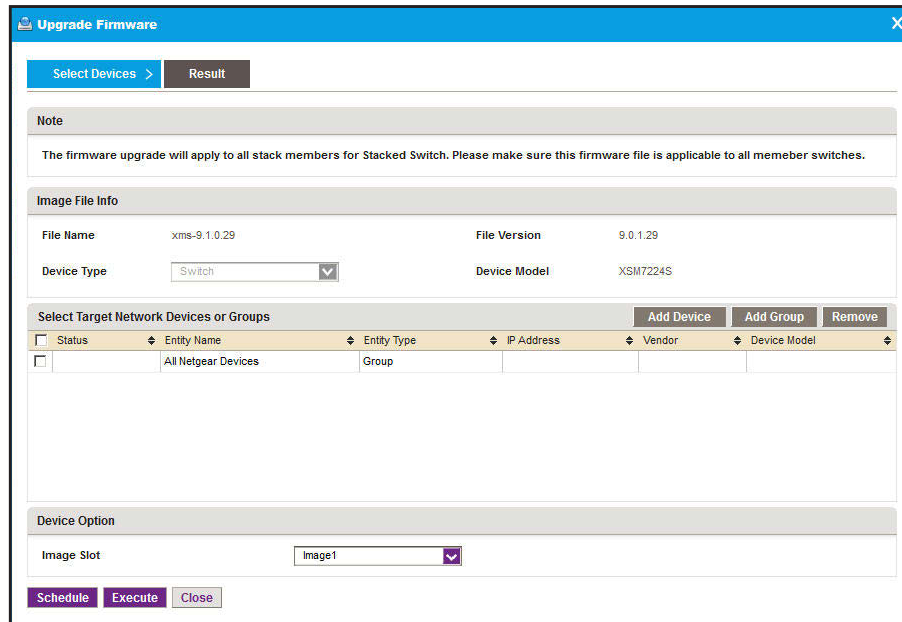
- To specify device groups:
 - a. Click the **Add Group** button.



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

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

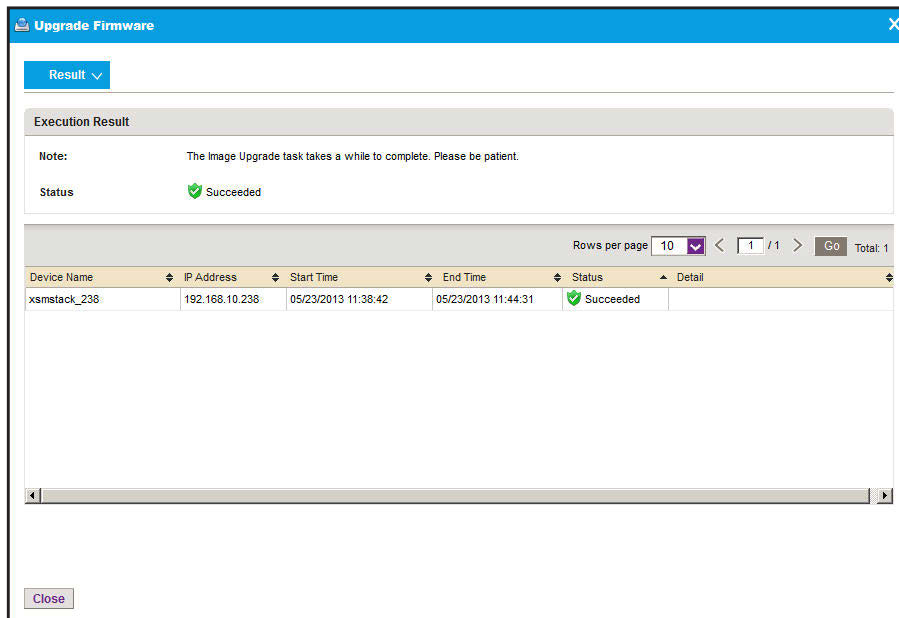
The screen closes and the selected group or groups are listed on the Upgrade Firmware screen.



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.

- Specify the time that you want the upgrade to occur.
- Click the **Submit** button.

The upgrade procedure is executed once at the specified time.

Modify the File Name, Version Information, and Description for a Firmware File

You can modify the file name, version information, and description for a firmware file. You cannot modify the vendor information, device type, and device model for a firmware file.

➤ To modify information for a firmware file:

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 18.

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**.

File Name	Create Time	Device Type	Version	Created By
xms-9.1.0.29	05/21/2013 18:52:38	Switch	9.0.1.29	jimmy

- 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.

- 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.

- Select the firmware file.
- Click the **Edit** button.

- Modify the information in the **File Name** field, **Version** field, or **Description** field, or in a combination of these fields.
- Click the **Submit** button.

The modified firmware file is saved and the screen closes.

Export a Firmware File

You can export a firmware file.

➤ To export a firmware file:

- 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 18.

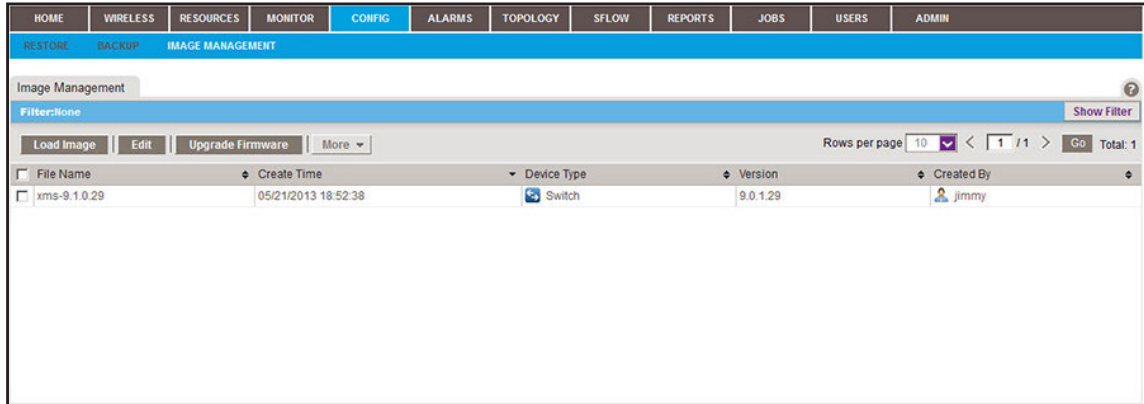
- Enter your user name and password.

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

- 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. From the **More** menu, select **Export Image**.
 9. To save the firmware file on your computer, follow the directions of your browser.

Remove a Firmware File

You can remove a firmware file that you no longer need.

➤ **To remove a firmware file:**

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 18.

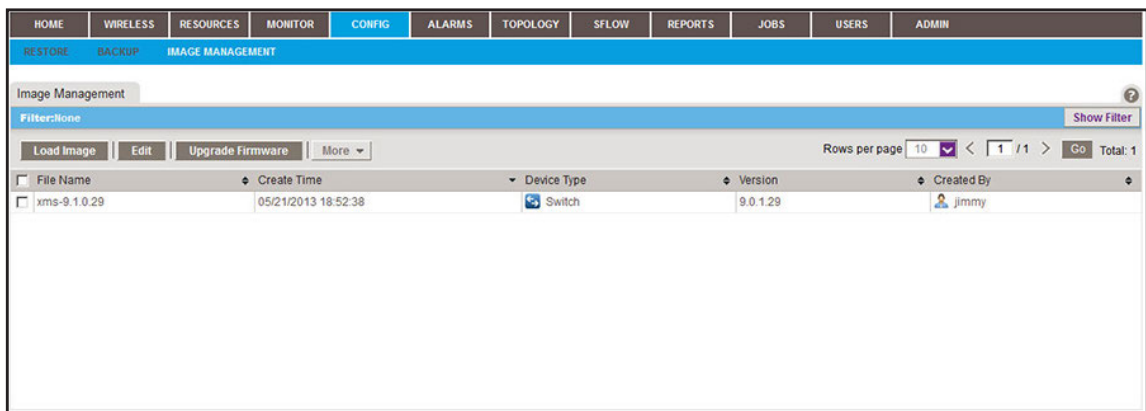
2. Enter your user name and password.

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. From the **More** menu, select **Delete Image**.

A pop-up confirmation screen displays.

9. Click the **Yes** button.

The firmware file is removed from the Image Management table and deleted.

6

6 Manage Alarms and Logs

Get alerts if something goes wrong

You can receive alarm notifications when conditions are suboptimal and view current and previous alarms using various filter options. As an option, you can receive these alarm notifications by email. In addition, you can view and manage network event notifications, device traps, and device system logs.

This chapter covers the following topics:

- *View and Manage Alarms, Triggers, and Notification Profiles*
- *View and Manage Network Event Notifications*
- *View and Manage Device Traps*
- *View and Manage Device System Logs*

View and Manage Alarms, Triggers, and Notification Profiles

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.

You can view and manage the current alarms, and you can view and manage the alarm history. You can also add custom alarm configurations that are based on existing configuration monitors.

One or more optional alarm notification profiles let you specify criteria that enable the application to generate and send a notification email message if an alarm occurs.

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)

The following sections describe the alarm-related tasks:

- *View and Manage Current Alarms*
- *View and Manage the Alarm History*
- *View and Manage Alarm Configurations*
- *Add a Custom Alarm Configuration*
- *Modify an Alarm Configuration*
- *View and Manage Alarm Notification Profiles*
- *Add or Modify an Alarm Notification Profile*
- *Customize Alarm Colors*

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 18.

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**.

Acknowledged	Alarm Name	Device Name	Alarm Source	Severity	Alarm Time	Occurrence Counter
<input type="checkbox"/> No	Device Memory utilization is over 90%	netgearA623F8	AP:netgearA623F8	Minor	09/10/2013 17:50:00	5
<input type="checkbox"/> No	linkDown	192.168.10.226	Interface Index:31	Major	09/10/2013 16:34:06	1
<input type="checkbox"/> No	linkDown	192.168.10.226	Interface Index:21	Major	09/10/2013 16:33:51	1
<input type="checkbox"/> No	failedUserLoginTrap	192.168.10.217	Device:192.168.10...	Major	09/10/2013 16:31:21	1
<input type="checkbox"/> No	failedUserLoginTrap	192.168.10.226	Device:192.168.10...	Major	09/10/2013 16:30:17	1
<input type="checkbox"/> No	linkDown	192.168.10.226	Interface Index:36	Major	09/10/2013 16:01:36	1

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.

Acknowledged	No	Alarm Name	Node is down
Device Name	FS752TP-NMS300	Device IP	192.168.10.202
Alarm Source	Device:FS752TP-NMS300	Severity	Critical
Alarm Type	Status Alarm	Notification OID	
Alarm Time	04/09/2013 02:06:10	Acknowledge By	
Acknowledge Time		Occurrence Counter	1

- 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.

View and Manage the Alarm History

The Alarm History table shows the previous alarms for the entire network. You can remove alarms from this table to reduce the amount of disk space that the application requires on the server. You can also export alarms.

➤ To view and manage the alarm history:

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 18.

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 > ALARM HISTORY**.

Alarm Name	Device Name	Device IP	Alarm Source	Severity	Alarm Time	Cleared Time
<input type="checkbox"/> Node is down	FVS3180	66.166.147.252	Device:FVS3180	Critical	09/10/2013 18:05:11	09/10/2013 18:06:31
<input type="checkbox"/> Node is down	66.166.147.250	66.166.147.250	Device:66.166.147.250	Critical	09/10/2013 18:05:11	09/10/2013 18:06:05
<input type="checkbox"/> Node is down	FVS3180	66.166.147.252	Device:FVS3180	Critical	09/10/2013 17:57:34	09/10/2013 17:58:26
<input type="checkbox"/> Node is down	FVS3180	66.166.147.252	Device:FVS3180	Critical	09/10/2013 17:48:13	09/10/2013 17:51:02
<input type="checkbox"/> Node is down	66.166.147.250	66.166.147.250	Device:66.166.147.250	Critical	09/10/2013 17:48:13	09/10/2013 17:51:00
<input type="checkbox"/> Node is down	Jimmy-620-168	192.168.10.168	AP:Jimmy-620-168	Critical	09/10/2013 16:39:21	09/10/2013 16:54:03
<input type="checkbox"/> Node is down	192.168.10.217	192.168.10.217	Device:192.168.10.217	Critical	09/10/2013 16:36:22	09/10/2013 16:37:49
<input type="checkbox"/> Node is down	Jun-6-M5300-jimmy	192.168.10.209	Device:Jun-6-M5300-jimmy	Critical	09/10/2013 16:36:21	09/10/2013 16:37:49
<input type="checkbox"/> linkDown	192.168.10.226	192.168.10.226	Interface Index:36	Major	09/10/2013 14:31:30	09/10/2013 15:58:06
<input type="checkbox"/> Node is down	wc-7520-164	192.168.10.164	Controller:wc-7520-164	Critical	09/10/2013 15:50:35	09/10/2013 15:53:08

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

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

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

You can filter the alarm history entries by criteria such as time range, device name, device IP address, severity level, and alarm name. By default, the alarm history 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.

Alarm Time	04/10/2013 09:45:06	Alarm Name	Node is down
Device Name	192.168.10.218	Device IP	192.168.10.218
Alarm Source	Device:192.168.10.218	Alarm Type	Status Alarm
Severity	Critical	Notification OID	
Acknowledge By	System	Acknowledge Time	
Cleared By	System	Cleared Time	04/10/2013 10:36:01
Occurrence Counter	1		

To close the History Alarm Detail screen, click the **Close** button.

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

The alarm is removed from the database.

- Delete a batch of alarms:
 - a. Select multiple alarms.
 - b. Click the **Batch Delete** button.

The alarms are removed from the database.

- Export the entire Alarm History 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 Alarm History 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.

View and Manage Alarm Configurations

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

The default status alarms include the following critical alarms:

- FTP service is down
- Node is down
- Performance management (PM) collection service error
- Syslog service is down
- TFTP service is down
- Trap service is down

The default monitor alarms include alarms for memory and CPU utilization of devices and disk, CPU, and memory utilization of the NMS300 server. The application provides multiple default trap alarms.

You can view, disable, reenable, remove, and export alarm configurations. For information about how to add a custom alarm configuration, see [Add a Custom Alarm Configuration](#) on page 165. For information about how to modify an existing alarm configuration, see [Modify an Alarm Configuration](#) on page 168.

➤ To view and manage the alarms configurations:

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 18.

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 > ALARM CONFIGURATION**.

Enable	Alarm Name	Alarm Type	Trap Name	Notification OID	Severity
<input checked="" type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.11.3.2.0.1	Info
<input checked="" type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.10.3.2.0.1	Info
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.11.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.10.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.11.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.10.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.11.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.10.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.11.13.0.3	Info
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.10.13.0.3	Info

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

You can choose from the following columns: Enable, Alarm Name, Alarm Type, Trap Name, Notification OID, Severity, MIB Name, and Description.

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

You can filter the alarm configuration by criteria such as alarm name, enabled status, alarm type, and severity.

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

7. Take one of the following actions:

- Disable an alarm configuration:
 - a. Select the alarm configuration.
 - b. From the **More** menu, select **Disable**.
 - c. Click the **Yes** button.

A pop-up confirmation screen displays. The alarm configuration is disabled and can no longer generate an alarm. In the Alarm Configuration table, the Enable column displays No for the alarm configuration.

- Enable an alarm configuration:
 - a. Select the alarm configuration.
 - b. Select the **Enable** button.

The alarm configuration is enabled and can generate an alarm. In the Alarm Configuration table, the Enable column displays Yes for the alarm configuration.

- Remove an alarm configuration:
 - a. Select the alarm configuration.
 - b. From the **More** menu, select **Delete**.
A pop-up confirmation screen displays.
 - c. Click the **Yes** button.
The alarm configuration is removed from the Alarm Configuration table and deleted.
- Export the entire Alarm Configuration table to an Excel spreadsheet:
 - a. From the **More** menu, select **Export to Excel**.
 - b. To save the alarm configurations on your computer, follow the directions of your browser.
- Export the entire Alarm Configuration table to a PDF:
 - a. From the **More** menu, select **Export to PDF**.
 - b. To save the alarm configurations on your computer, follow the directions of your browser.

Add a Custom Alarm Configuration

You can define your own alarms, including alarms for all configuration monitors (see *Manage the Configuration Monitors* on page 92).

A custom alarm configuration that you add is always based on an existing configuration monitor and includes a threshold. The configuration monitor determines the polling interval for the alarm configuration. For more information, see *Manage the Configuration Monitors* on page 92.

➤ To add one or more custom alarm configurations:

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 18.

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 > ALARM CONFIGURATION**.

Enable	Alarm Name	Alarm Type	Trap Name	Notification OID	Severity
<input checked="" type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.11.3.2.0.1	Info
<input checked="" type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.10.3.2.0.1	Info
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.11.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.10.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.11.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.10.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.11.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.10.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.11.13.0.3	Info
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.10.13.0.3	Info

5. Click the **Add** button.

Add Threshold Alarm

Monitor Package

Monitor Name: Device ICMP Ping
 Description: Device ICMP Ping results
 Polling Interval(minutes): 3 Minutes
 Enable: Yes

Threshold List

Rows per page: 10 / 1 / 1
 Total: 0

Paramter Enable Alarm Name Upper/Lower Count Threshold Severity

No data to display!

Close

6. From the **Monitor Name** menu, select the monitor.

7. In the **Description** field, enter a new description, or use the default description.

The configuration monitor determines the polling interval for the alarm configuration. For more information, see [Manage the Configuration Monitors](#) on page 92.

The **Enable** field shows whether the configuration monitor is enabled. However, you can enable an alarm configuration even if the configuration monitor is disabled.

8. Click the **Add** button.

9. Enter the following threshold information:

- **General Info:**
 - **Alarm Name.** Enter a name for the alarm.
 - **Description.** Enter a description for the alarm.
 - **Parameter.** Select a parameter. The parameters that are displayed in the menu depend on the monitor that you select in [Step 6](#).
 - **Enable.** Select whether to enable the threshold.
 - **Calculation Type.** Select a consecutive or average calculation.
 - **Count.** Select the number of times that a particular event must occur before the threshold is met.
- **Threshold Alarm Info:**
 - **Upper/Lower.** Select an upper or lower threshold.
 - **Threshold.** Enter the threshold. If this threshold is exceeded, the application triggers an alarm.
 - **Severity.** Select whether the alarm is considered critical, major, minor, or informational.

10. Click the **Submit** button.

The Add Threshold screen for the selected monitor screen closes and the alarm configuration is added to the Threshold List table.

11. To add another alarm configuration, repeat [Step 8](#) through [Step 10](#).

Before you add a new alarm configuration to the Alarm Configuration table, you can still modify or remove the alarm configuration.

12. To close the general Add Threshold screen, click the **Close** button.

All new alarm configurations are added to the Alarm Configuration table.

Modify an Alarm Configuration

You can modify a default or custom alarm configuration.

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 18.

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 > ALARM CONFIGURATION**.

Enable	Alarm Name	Alarm Type	Trap Name	Notification OID	Severity
<input type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.11.3.2.0.1	Info
<input checked="" type="checkbox"/>	aciTrapRuleLogEvent	Trap Alarm	aciTrapRuleLogEvent	1.3.6.1.4.1.4526.10.3.2.0.1	Info
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.11.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardMismatch	Trap Alarm	agentInventoryCardMismatch	1.3.6.1.4.1.4526.10.13.0.1	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.11.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryCardUnsupported	Trap Alarm	agentInventoryCardUnsupported	1.3.6.1.4.1.4526.10.13.0.2	Minor
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.11.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkDown	Trap Alarm	agentInventoryStackPortLinkDown	1.3.6.1.4.1.4526.10.13.0.4	Major
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.11.13.0.3	Info
<input checked="" type="checkbox"/>	agentInventoryStackPortLinkUp	Trap Alarm	agentInventoryStackPortLinkUp	1.3.6.1.4.1.4526.10.13.0.3	Info

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

You can choose from the following columns: Enable, Alarm Name, Alarm Type, Trap Name, Notification OID, Severity, MIB Name, and Description.

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

You can filter the alarm configuration by criteria such as alarm name, enabled status, alarm type, and severity.

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

7. Select the alarm configuration.

8. Click the **Edit** button.

9. Modify the following threshold information as needed:

- **General Info:**
 - **Alarm Name.** Modify the name for the alarm.
 - **Description.** Modify the description for the alarm.
 - **Parameter.** You cannot modify the parameter.
 - **Enable.** Select whether to enable the threshold.
 - **Calculation Type.** You cannot modify the type of calculation.
 - **Count.** Select the number of times that a particular event must occur before the threshold is met.
- **Threshold Alarm Info:**
 - **Upper/Lower.** You cannot modify the type of threshold.
 - **Threshold.** Modify the threshold. If this threshold is exceeded, the application triggers an alarm.
 - **Severity.** Select whether the alarm is considered critical, major, minor, or informational.

10. Click the **Submit** button.

The modified alarm configuration displays in the Alarm Configuration table.

View and Manage Alarm Notification Profiles

An alarm notification profile specifies criteria that enable the application to generate and send a notification email message if an alarm occurs. By default, the application does not include any alarm notification profiles.

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 23 and [Configure the SMS Server for Alerts and Alarm Notifications](#) on page 26.

➤ **To view and manage alarm notification profiles:**

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 18.

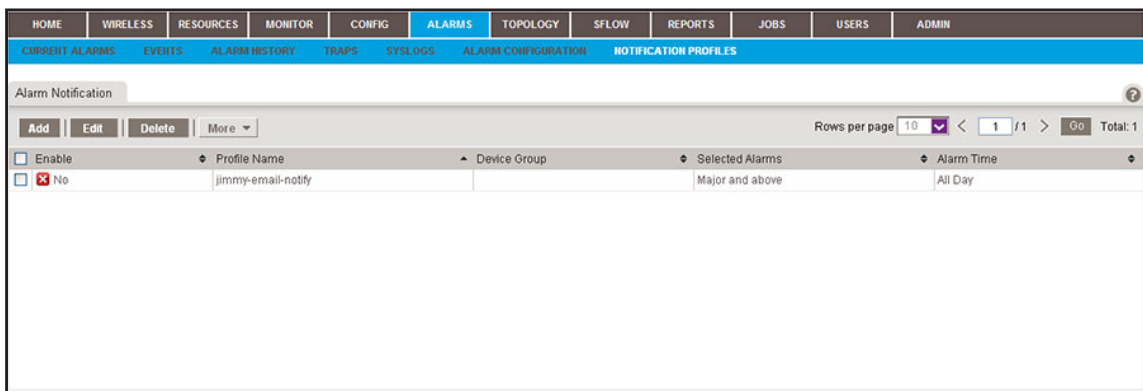
2. Enter your user name and password.

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**.



If you did not yet add any alarm notification profiles (see *Add or Modify an Alarm Notification Profile* on page 171), the Alarm Notification table is empty.

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

You can choose from the following columns: Enable, Profile Name, Device Group, Selected Alarms, Alarm Time, Created By, and Create Time.

6. Select an alarm notification profile.

7. Take one of the following actions:

- Disable the alarm notification profile:
 - a. From the **More** menu, select **Disable**.
A pop-up confirmation screen displays.
 - b. Click the **Yes** button.

The alarm notification profile is disabled and can no longer generate an email message. In the Alarm Notification table, the Enable column displays No for the alarm notification profile.

- Reenable the alarm notification profile. From the **More** menu, select **Enable**.
The alarm notification profile is enabled and can generate an email message. In the Alarm Notification table, the Enable column displays Yes for the alarm notification profile.
- Remove the alarm notification profile:
 - a. Select the **Delete** button.
A pop-up confirmation screen displays.
 - b. Click the **Yes** button.
The alarm notification profile is removed from the Alarm Notification table and deleted.

Add or Modify an Alarm Notification Profile

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

➤ **To add an alarm notification profile or modify an existing 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 18.

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**.

Enable	Profile Name	Device Group	Selected Alarms	Alarm Time
<input type="checkbox"/> No	jimmy-email-notify		Major and above	All Day

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

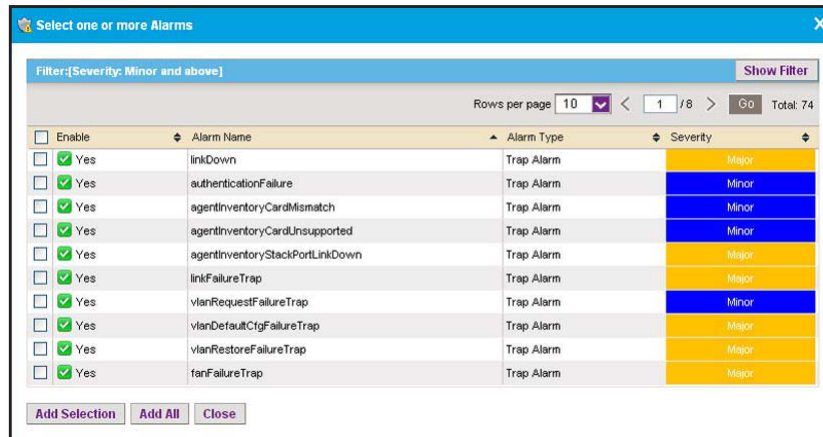
You can choose from the following columns: Enable, Profile Name, Device Group, Selected Alarms, Alarm Time, Created By, and Create Time.

6. Add an alarm notification profile or modify an existing alarm notification profile:
 - To add an alarm notification profile, click the **Add** button.
 - To modify an existing alarm notification profile:
 - a. From the Alarm Notification table, select the alarm notification profile.
 - b. Click the **Edit** button.

For a new alarm notification profile, the Add Alarm Notification screen displays. For an existing alarm notification profile, the Edit Alarm Notification screen displays.

7. In the Basic Information section, specify or modify the following information:
 - **Profile Name.** Enter or modify the name for the profile.
 - **Description.** Enter or modify 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.
8. 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.

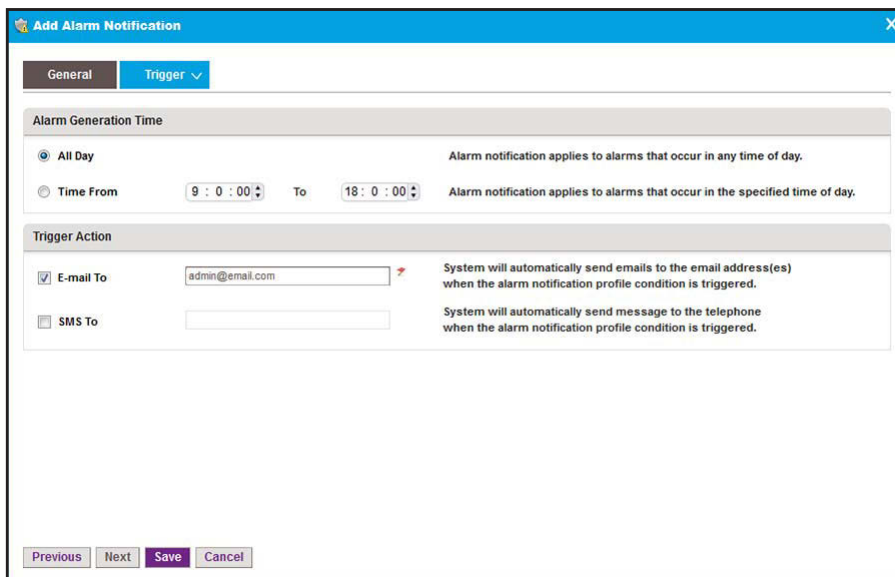
To add all alarms, click the **Add All** button.

The alarms are added to the Add Alarm Notification screen (or, if you are modifying an existing alarm notification profile, to the Edit Alarm Notification screen).

- d. If you are modifying an existing alarm notification profile, to remove alarms, select the alarms, and click the **Remove** button.

The alarms are removed from the Edit Alarm Notification screen.

9. Click the **Trigger** tab.



10. Specify or modify the following information:

- **Alarm Generation Time.** Select one of the following radio buttons:
 - **All Day.** The alarm notification applies to alarms that occur at 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 which the application can send a notification if the alarm notification condition is triggered.
 - **SMS To.** Enter the telephone number to which the application can send a notification 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 26.

11. Click the **Save** button.

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

Customize Alarm Colors

You can change the colors of the alarms.

➤ To customize the color of an alarm:

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 18.

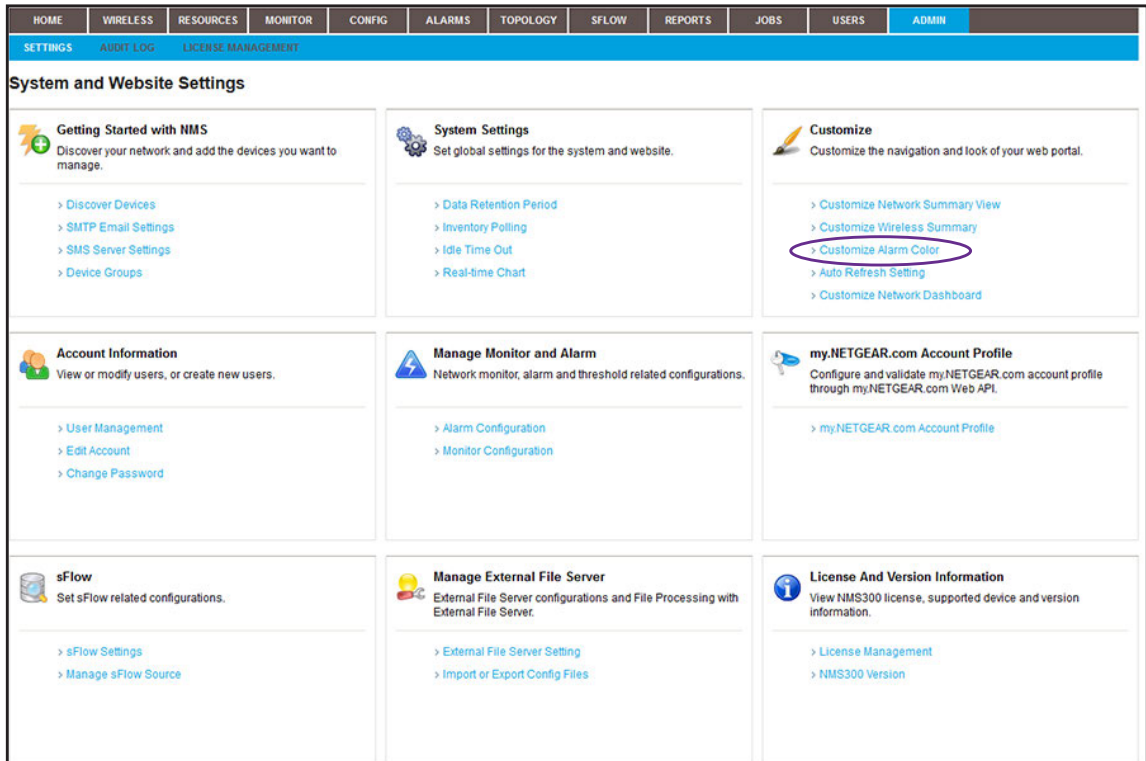
2. Enter your user name and password.

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

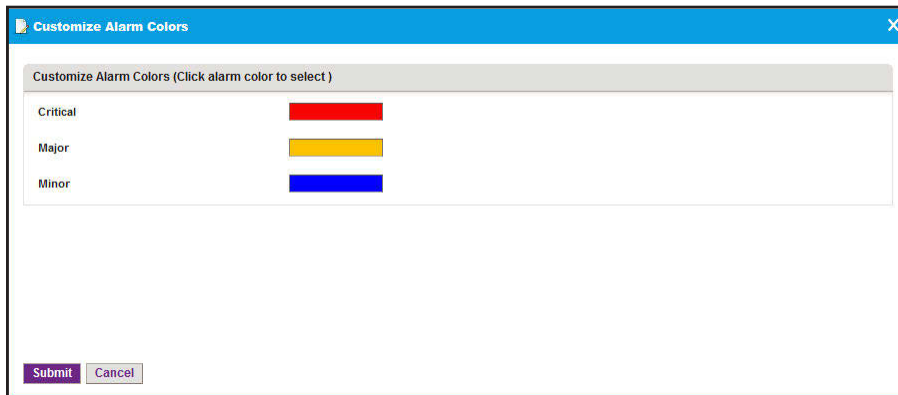
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.

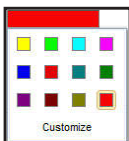


5. Under Customize, click the **Customize Alarm Color** link.



6. Click the alarm color.

7. Select another color.



8. Click the **Submit** button.

Your changes are saved.

View and Manage Network Event Notifications

The Events table shows the events for the entire network, including events for devices and interfaces. You can display details about network events, remove network events, and export network events.

➤ **To view and manage network events:**

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 18.

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 > EVENTS**.

Event Name	Device Name	Device IP	Event Source	Event Type	Event Time
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:36	Trap Alarm	09/10/2013 15:58:06
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:32	Trap Alarm	09/10/2013 15:49:42
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:32	Trap Alarm	09/10/2013 15:49:24
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:30:04
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:29:51
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:29:15
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:28:38
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:14:35
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:14:22
<input type="checkbox"/> linkUp	192.168.10.226	192.168.10.226	Interface Index:27	Trap Alarm	09/10/2013 15:13:46

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

You can choose from the following columns: Event Name, Device Name, Device IP, Event Source, Event Type, Event Time, and Notification OID.

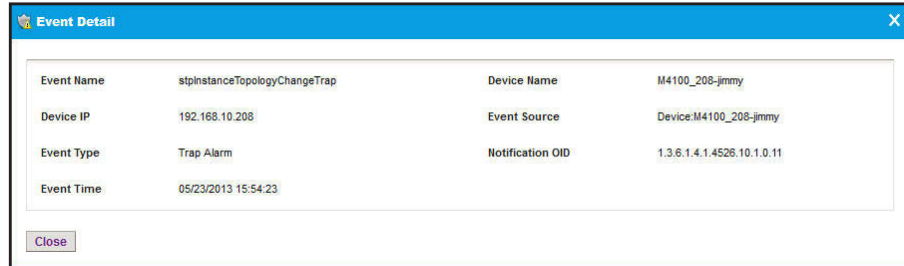
6. To filter the event entries that are listed, click the **Show Filter** button.

You can filter the event entries by criteria such as time range, device name, device IP address, and severity level. By default, the event 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 event:
 - a. Select the event.
 - b. Click the **Detail** button.



- c. To close the Event Detail screen, click the **Close** button.
- Delete an event:
 - a. Select the event.
 - b. Click the **Delete** button.

The event is removed from the database.
 - Delete a batch of events:
 - a. Select multiple events.
 - b. Click the **Batch Delete** button.

The events are removed from the database.
 - Export the entire Events table to an Excel spreadsheet:
 - a. From the **More** menu, select **Export to Excel**.
 - b. To save the events on your computer, follow the directions of your browser.
 - Export the entire Events table to a PDF:
 - a. From the **More** menu, select **Export to PDF**.
 - b. To save the events on your computer, follow the directions of your browser.

View and Manage Device Traps

The Traps table shows the device trap events. You can display details about device trap events, remove device trap events, and export device trap events.

➤ To view and manage device traps:

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 18.
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 > TRAPS**.

Source IP	Trap Type	Notification OID	Receive Time	Trap Detail
192.168.10.226	linkDown	1.3.6.1.6.3.1.1.5.3	09/10/2013 16:34:05	1.3.6.1.2.1.2.2.1.1.31.31; 1.3.6.1.2.1.2.2.1.7.31.1; 1.3.6.1.2.1.2.2.1.8.31.2
192.168.10.226	linkDown	1.3.6.1.6.3.1.1.5.3	09/10/2013 16:33:51	1.3.6.1.2.1.2.2.1.1.21.21; 1.3.6.1.2.1.2.2.1.7.21.1; 1.3.6.1.2.1.2.2.1.8.21.2
192.168.10.217	failedUserLoginTrap	1.3.6.1.4.1.4526.10.1.0.13	09/10/2013 16:31:21	
192.168.10.226	failedUserLoginTrap	1.3.6.1.4.1.4526.11.1.0.13	09/10/2013 16:30:17	
192.168.10.226	linkDown	1.3.6.1.6.3.1.1.5.3	09/10/2013 16:01:36	1.3.6.1.2.1.2.2.1.1.36.36; 1.3.6.1.2.1.2.2.1.7.36.1; 1.3.6.1.2.1.2.2.1.8.36.2
192.168.10.226	linkUp	1.3.6.1.6.3.1.1.5.4	09/10/2013 15:58:06	1.3.6.1.2.1.2.2.1.1.36.36; 1.3.6.1.2.1.2.2.1.7.36.1; 1.3.6.1.2.1.2.2.1.8.36.1
192.168.10.226	linkUp	1.3.6.1.6.3.1.1.5.4	09/10/2013 15:49:42	1.3.6.1.2.1.2.2.1.1.32.32; 1.3.6.1.2.1.2.2.1.7.32.1; 1.3.6.1.2.1.2.2.1.8.32.1
192.168.10.226	linkDown	1.3.6.1.6.3.1.1.5.3	09/10/2013 15:49:38	1.3.6.1.2.1.2.2.1.1.32.32; 1.3.6.1.2.1.2.2.1.7.32.1; 1.3.6.1.2.1.2.2.1.8.32.2
192.168.10.226	linkUp	1.3.6.1.6.3.1.1.5.4	09/10/2013 15:49:24	1.3.6.1.2.1.2.2.1.1.32.32; 1.3.6.1.2.1.2.2.1.7.32.1; 1.3.6.1.2.1.2.2.1.8.32.1
192.168.10.226	linkDown	1.3.6.1.6.3.1.1.5.3	09/10/2013 15:49:18	1.3.6.1.2.1.2.2.1.1.32.32; 1.3.6.1.2.1.2.2.1.7.32.1; 1.3.6.1.2.1.2.2.1.8.32.2

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

You can choose from the following columns: Source IP, Trap Type, Notification OID, Receive Time, Trap Detail, Trap Version, and Time Stamp.

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

You can filter the trap entries by criteria such as time range, device IP address, and trap type. By default, the trap 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 a trap:
 - a. Select the trap.
 - b. Click the **Detail** button.

Source IP	192.168.10.208
Trap Version	V2c
Notification OID	1.3.6.1.2.1.17.0.2
Trap Type	1.3.6.1.2.1.17.0.2
Time Stamp	3 days, 6 hours, 58 minutes, 07 seconds
Receive Time	05/23/2013 15:54:25
Trap Detail	

- c. To close the Trap Detail screen, click the **Close** button.

- Delete a trap:
 - a. Select the trap.
 - b. Click the **Delete** button.

The trap is removed from the database.
- Delete a batch of traps:
 - a. Select multiple traps.
 - b. Click the **Batch Delete** button.

The traps are removed from the database.
- Export the entire Traps table to an Excel spreadsheet:
 - a. From the **More** menu, select **Export to Excel**.
 - b. To save the traps on your computer, follow the directions of your browser.
- Export the entire Traps table to a PDF:
 - a. From the **More** menu, select **Export to PDF**.
 - b. To save the traps on your computer, follow the directions of your browser.

View and Manage Device System Logs

The Syslog table shows the device system log entries. You can display details about log entries, remove log entries, and export log entries.

➤ To view and manage the device system log entries:

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 18.

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 > SYSLOGS**.

Receive Time	Device IP	Facility	Severity	Message
09/10/2013 18:41:15	192.168.10.162	daemon	Info	Jan 1 02:51:44 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:14	192.168.10.168	daemon	Info	Jan 1 02:01:08 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:06	192.168.10.162	daemon	Info	Jan 1 02:51:35 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:02	192.168.10.162	daemon	Info	Jan 1 02:51:30 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:02	192.168.10.168	daemon	Info	Jan 1 02:00:55 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:58	192.168.10.162	daemon	Info	Jan 1 02:51:27 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:54	192.168.10.162	daemon	Info	Jan 1 02:51:23 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:45	192.168.10.162	daemon	Info	Jan 1 02:51:13 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:44	192.168.10.168	daemon	Info	Jan 1 02:00:37 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:36	192.168.10.162	daemon	Info	Jan 1 02:51:05 lldpd[685]: lldpd_decode: unable to guess frame type

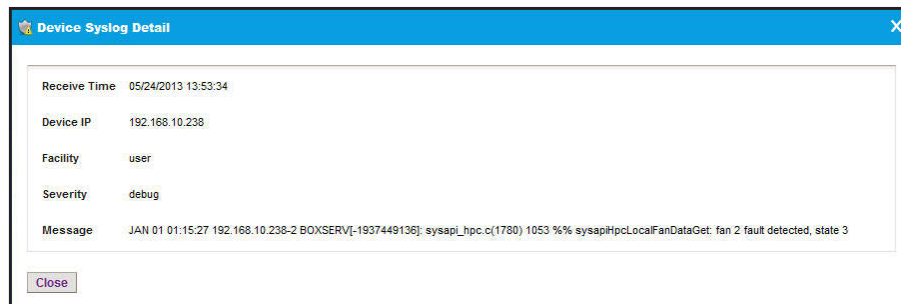
5. To filter the syslog entries that are listed, click the **Show Filter** button.

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

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

6. Take one of the following actions:

- View details for a log entry:
 - a. Select the log entry.
 - b. Click the **Detail** button.



- c. To close the Device Syslog Detail screen, click the **Close** button.
- Delete a log entry:
 - a. Select the log entry.
 - b. Click the **Delete** button.

The log is removed from the database.

- Delete a batch of log entries:
 - a. Select multiple log entries.
 - b. Click the **Batch Delete** button.

The log entries are removed from the database.

- Export the entire Syslogs table to an Excel spreadsheet:
 - a. From the **More** menu, select **Export to Excel**.
 - b. To save the log entries on your computer, follow the directions of your browser.
- Export the entire Syslogs table to a PDF:
 - a. From the **More** menu, select **Export to PDF**.
 - b. To save the log entries on your computer, follow the directions of your browser.

7

7. Manage Maps and Topologies

View the topology of your network

You can create hierarchical maps and topological views of your network.

This chapter covers the following topics:

- *View and Manage Maps*
- *View and Manage Network Topologies*

View and Manage Maps

The application provides a default world map. This map is the root map for any child map that you add.

The following sections describe the tasks that relate to maps:

- *View a Hierarchical Map and Locate a Device*
- *Manage a Hierarchical Map*
- *Add a Childmap*
- *Add Devices to a Map*
- *Add a Link Between Devices on a Map*
- *Customize the Style of a Link on a Map*

View a Hierarchical Map and Locate a Device

You can view a hierarchical map of your network, locate devices on the map, and view details about the devices, including alarms.

➤ **To view a hierarchical map, locate a device on the map, and view details about the 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 18.

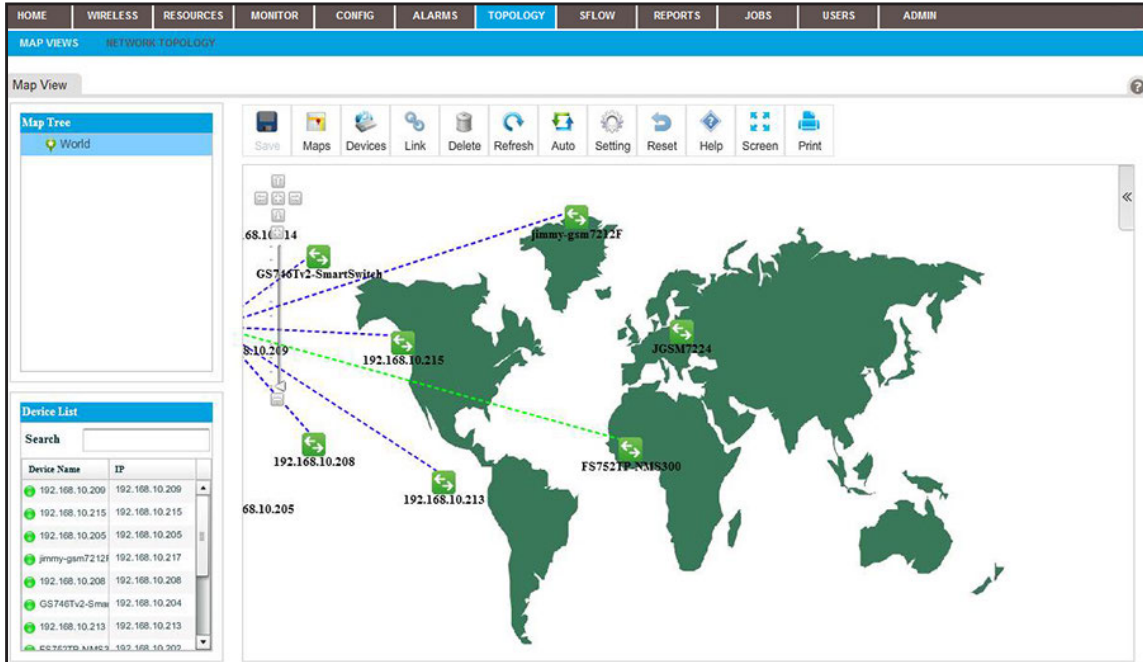
2. Enter your user name and password.

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

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

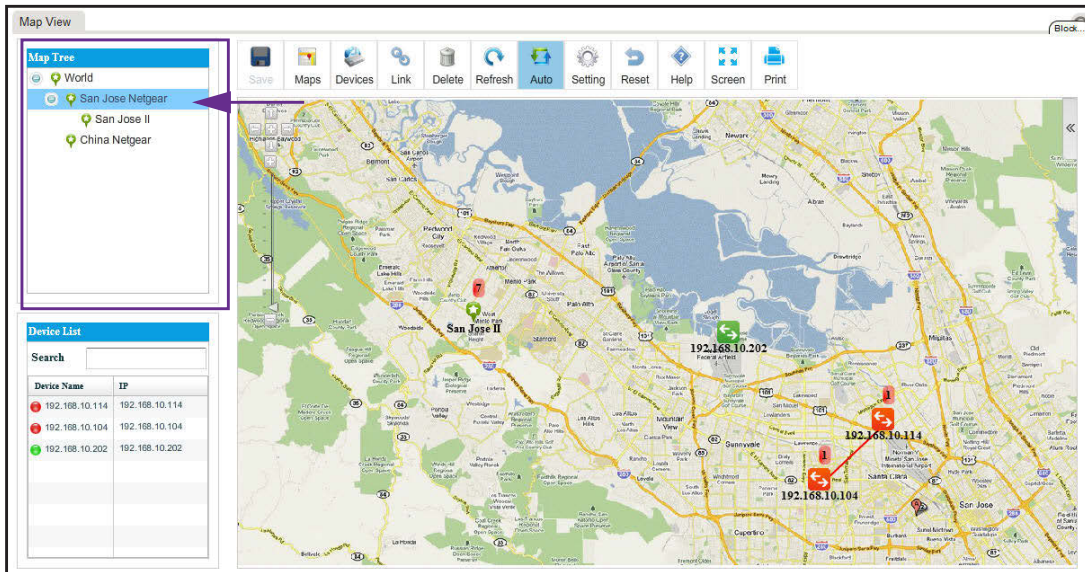
The Network Summary screen displays.

4. Select **TOPOLOGY > MAP VIEWS**.



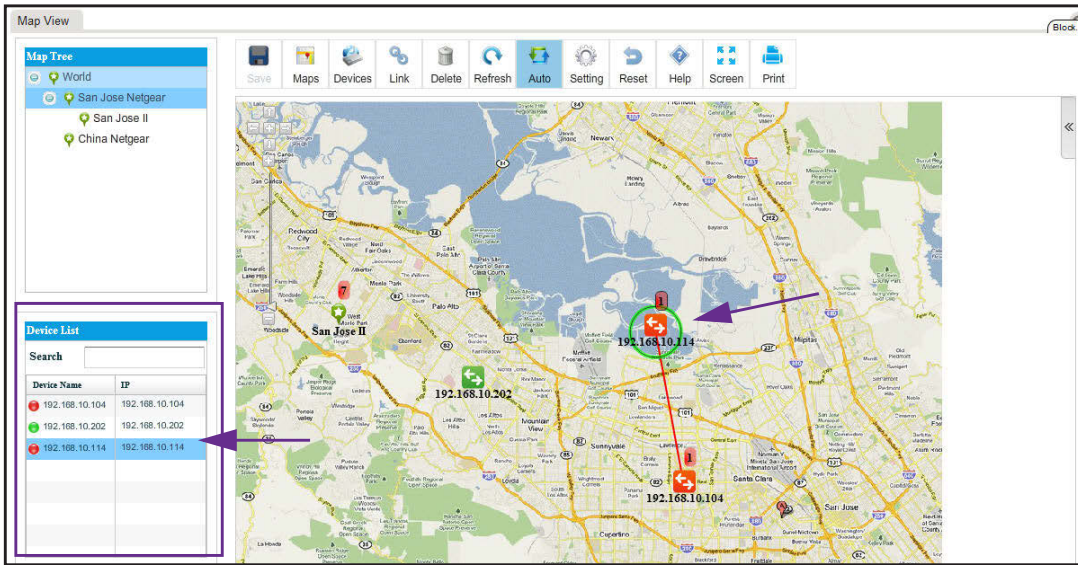
5. From the Map Tree, select the map.

The selected map displays.



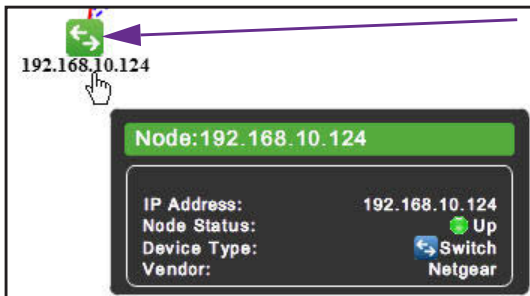
6. From the Device List table, select the device that you want to locate on the map.

A circle displays around the selected device.



- To view information about the device (node), point to the device on the map.

A pop-up screen similar to the following displays.

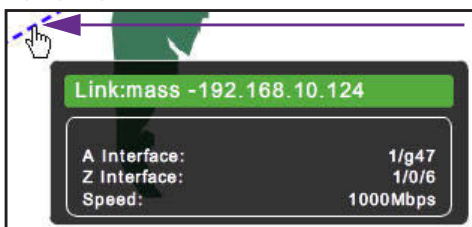


- To see detailed information and the Dashboard menu for the device, double-click the device on the map.

For more information, see [View Device Details and Interface Details](#) on page 85.

- To view the details for a link, point to the link on the map.

A pop-up screen similar to the following displays.



- To view the summary for an alarm, point to the alarm summary on the map.

An alarm summary is displayed as a red-colored rectangular with a number.

A pop-up screen similar to the following displays.



Manage a Hierarchical Map

On the Map Views screen, the icons that display above a map let you perform various tasks.

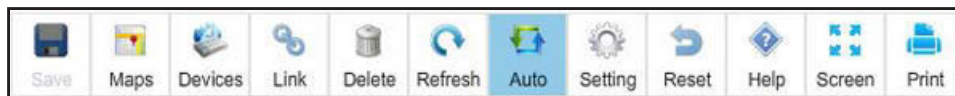


Figure 3. Icons on the Map Views screen

The following procedure describes the tasks that you can perform for a hierarchical map. For complicated tasks, the procedure points to a section that provides detailed information.

➤ To manage a hierarchical map:

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 18.

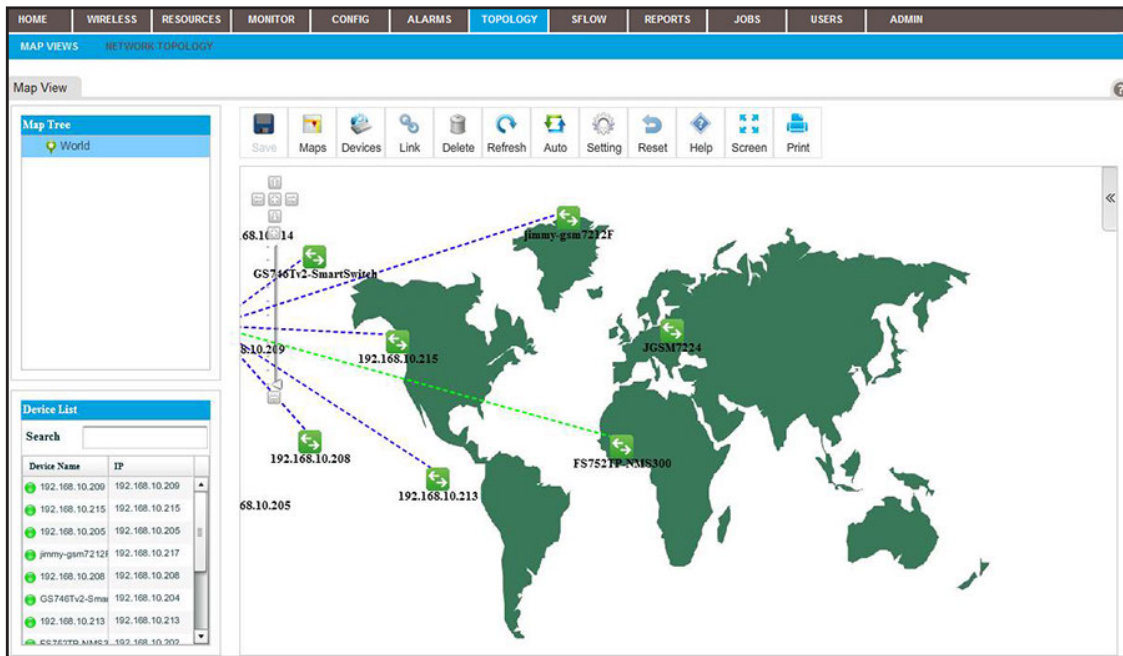
2. Enter your user name and password.

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

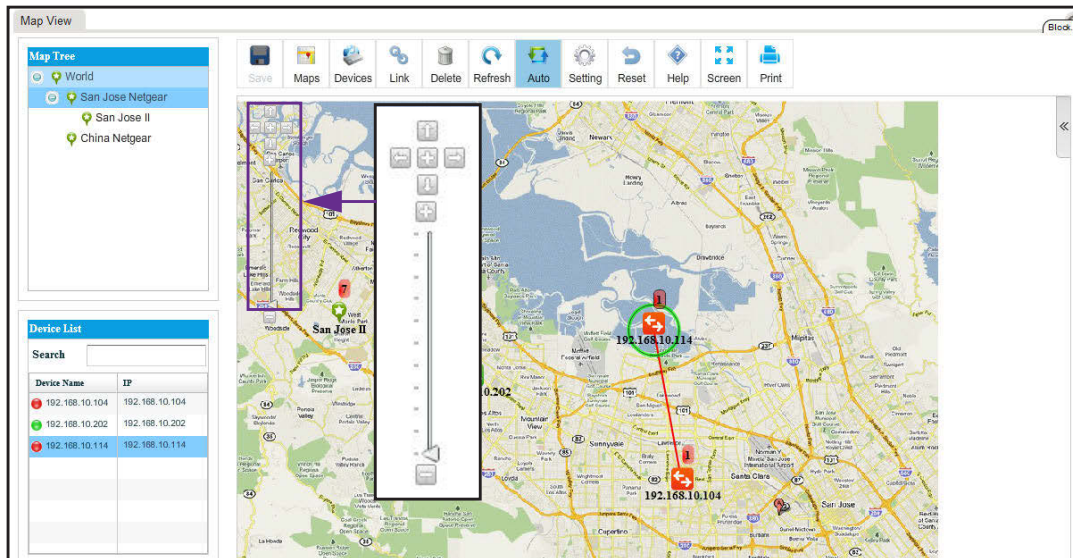
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **TOPOLOGY > MAP VIEWS**.



5. From the Map Tree, select the map.
6. To rescale the map, use the scaling tool that displays on the left of the map.



7. To reposition the map, hold your cursor on the map and drag the map to a new position.
8. Take one of the following actions:
 - Let the application refresh the map automatically. Click the **Auto** icon.
The map refreshes automatically every two minutes. Automatic refreshment is the default setting.
 - Refresh the map manually. Click the **Refresh** icon.
The map refreshes once immediately.

- Add a childmap. Click the **Maps** icon.
For more information, see [Add a Childmap](#) on page 188.
- Add devices to a map. Click the **Devices** icon.
For more information, see [Add Devices to a Map](#) on page 191.
- Add a link between devices on a map. Click the **Link** icon.
For more information, see [Add a Link Between Devices on a Map](#) on page 193.
- Customize the link style settings. Click the **Setting** icon.
For more information, see [Customize the Style of a Link on a Map](#) on page 196.
- Remove a childmap, device, or link from the map:
 - a. Select the item.
 - b. Click the **Delete** icon.
The item is removed.
- Undo unsaved changes. Click the **Reset** icon.
The unsaved changes are reset.
- Save changes. Click the **Save** icon.
Your changes are saved. When the Save icon is grayed out, everything is saved.
- Open the Help screen. Click the **Help** icon.
The Help pop-up screen displays.
- Enter full-screen mode. Click the **Screen** icon.
The screen displays in full-screen mode. To return to the regular screen display, either press the **Esc** key, or from the full screen, click the **Screen** icon.
- Print the screen. Click the **Print** icon.
The map is printed.

Add a Childmap

You can add a childmap (submap) to a hierarchical map. The hierarchical map functions as the parent map to the childmap. The application provides default childmaps. You can also import your own childmaps.

➤ To add a childmap:

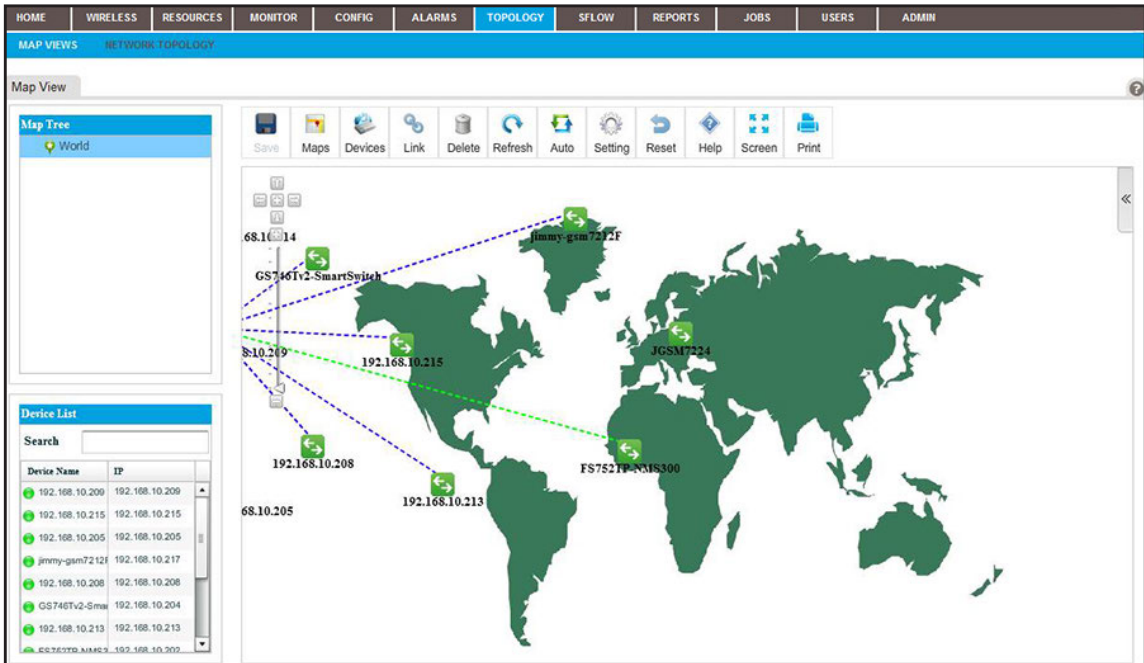
1. Open a browser and connect to the application through the static IP address of the NMS300 server.
For more information, see [Log In to the Application](#) on page 18.
2. Enter your user name and password.

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 **TOPOLOGY > MAP VIEWS**.

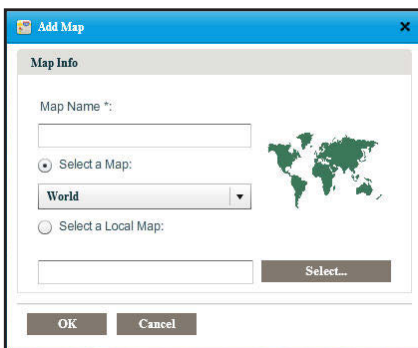


5. From the Map Tree, select the map.

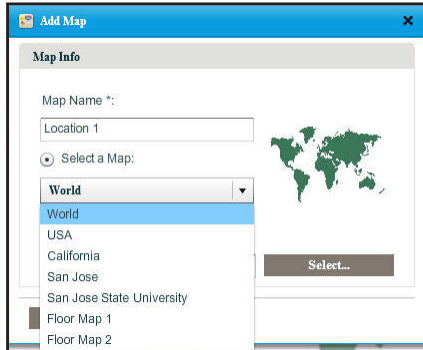
6. Click the **Maps** icon.



The Add Map screen displays.



7. Enter a name for the childmap.

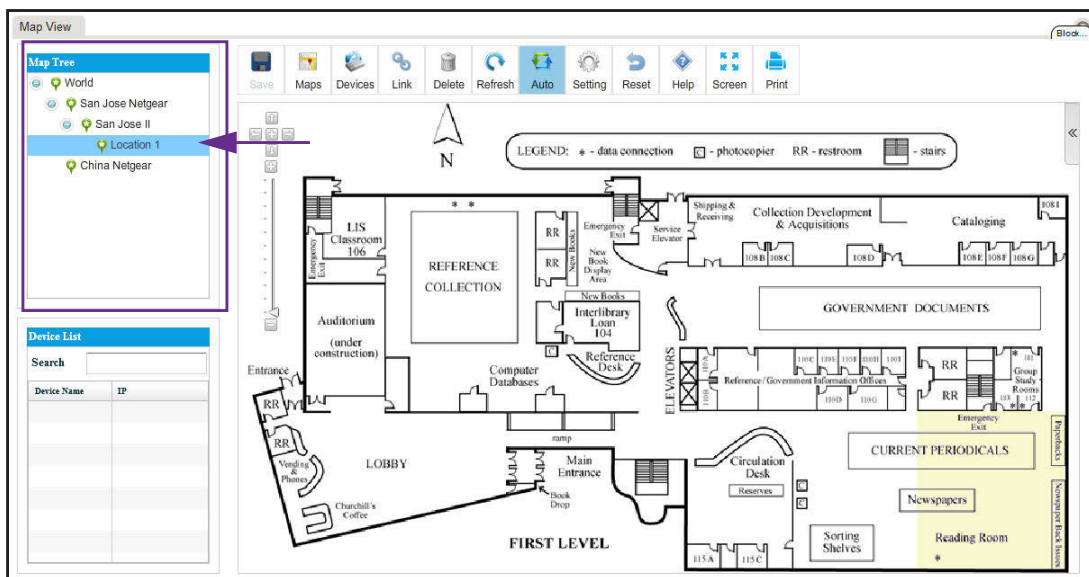


8. Either select a default childmap or import a map from your computer by selecting one of the following radio buttons:

- **Select a Map.** Select a default map from the menu.
- **Select a Local Map.** Take the following action:
 - a. Click the **Select** button.
 - b. Locate and select a map on your computer.

9. Click the **OK** button.

The map that you selected or imported displays as a childmap below the parent map and the name of the map you selected displays in the Map Tree.



Add Devices to a Map

You can add devices to a map.

➤ **To add devices to a map:**

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 18.

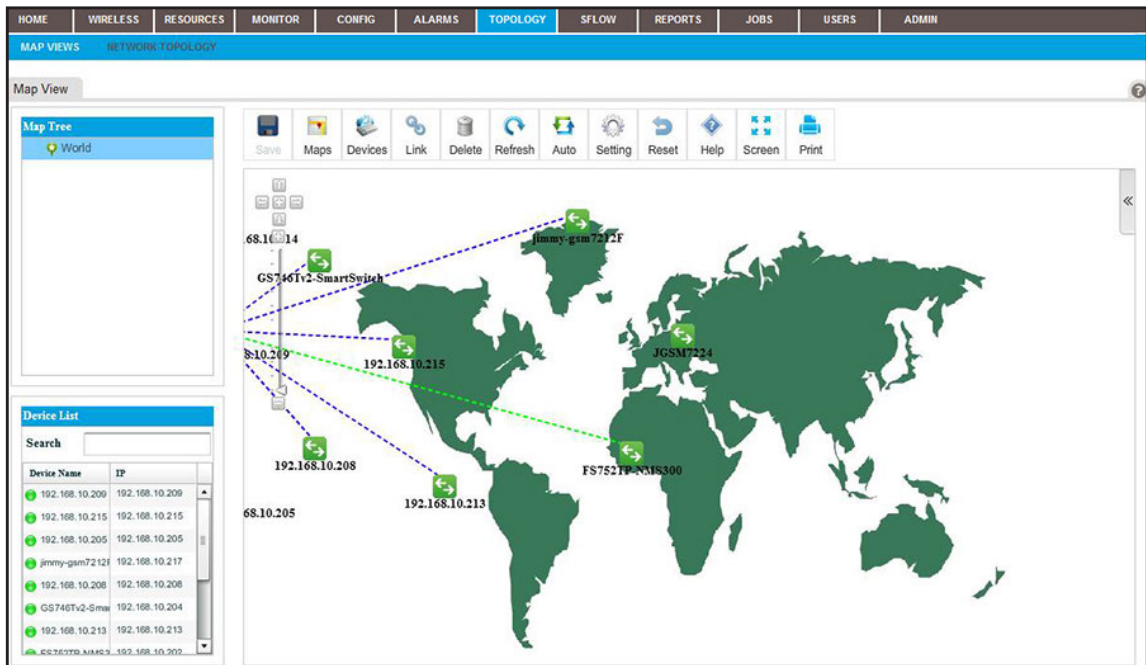
2. Enter your user name and password.

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.

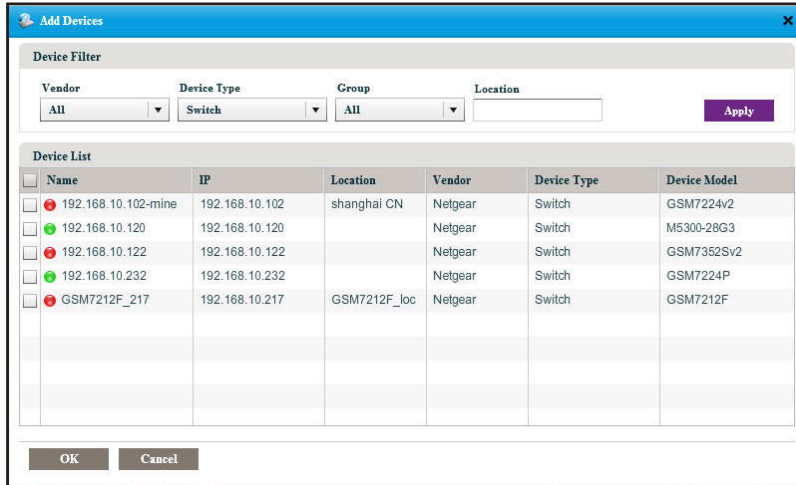
4. Select **TOPOLOGY > MAP VIEWS**.



5. From the Map Tree, select the map.
6. Click the **Devices** icon.

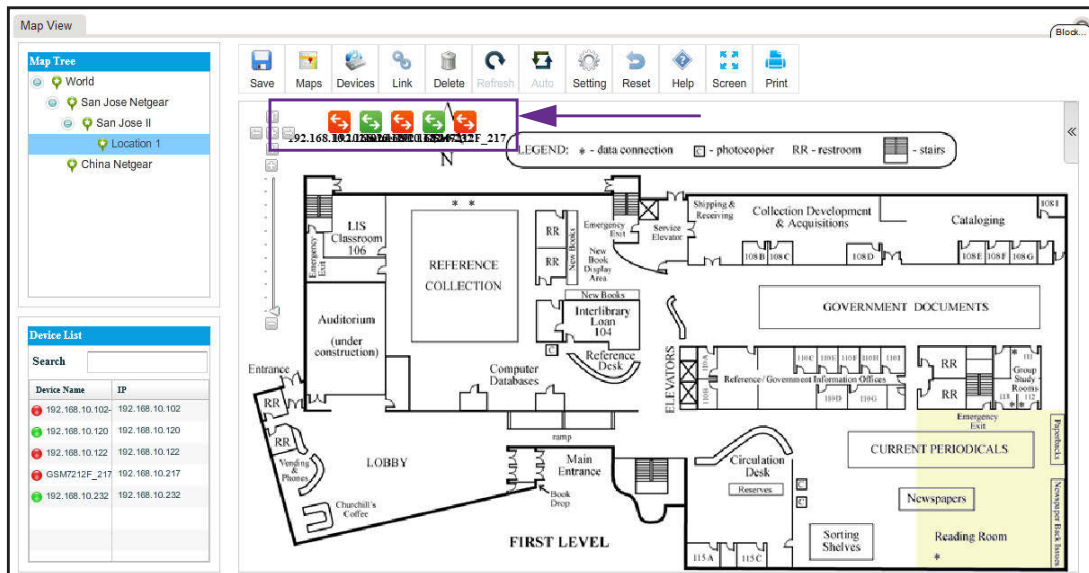


The Add Devices screen displays.



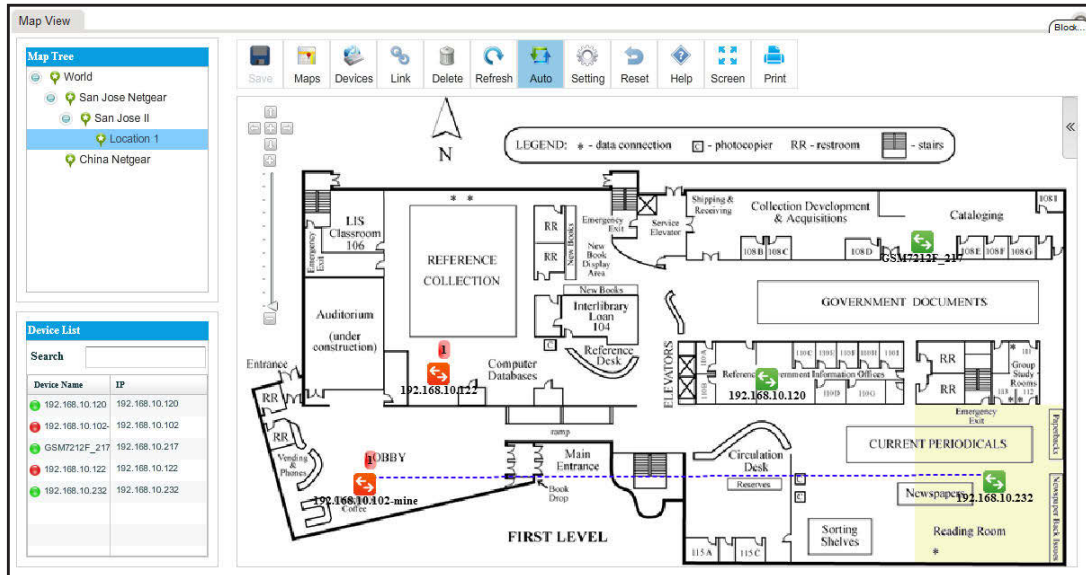
7. Select one or more devices.
8. Click the **OK** button.

The devices display on the map.



9. For each device, select the device and drag it to where you want it on the map.
10. Click the **Save** button.

The devices display at their locations on the map. The map also displays the existing links between the devices.



Add a Link Between Devices on a Map

You can add a link between devices. For devices that do not support link discovery through Link Layer Discovery Protocol (LLDP), you can manage links manually. When you know that physical connections exist for the non-LLDP devices, you can draw these links manually and also update them manually when the physical connections are reconfigured.

➤ To add a link between devices on a map:

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 18.

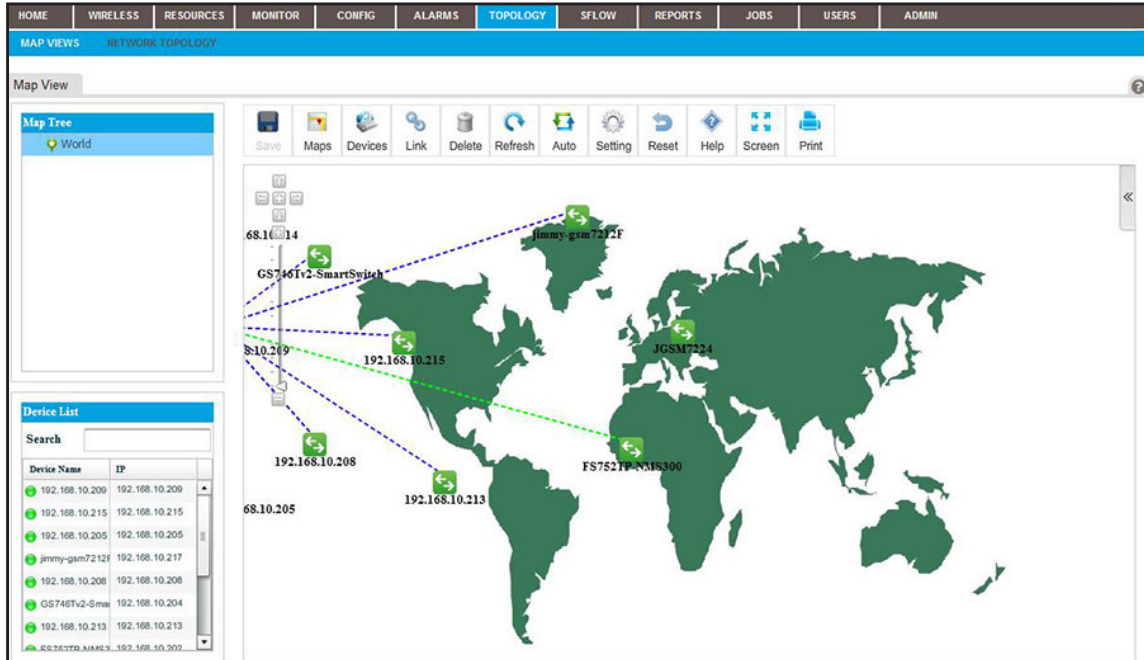
2. Enter your user name and password.

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

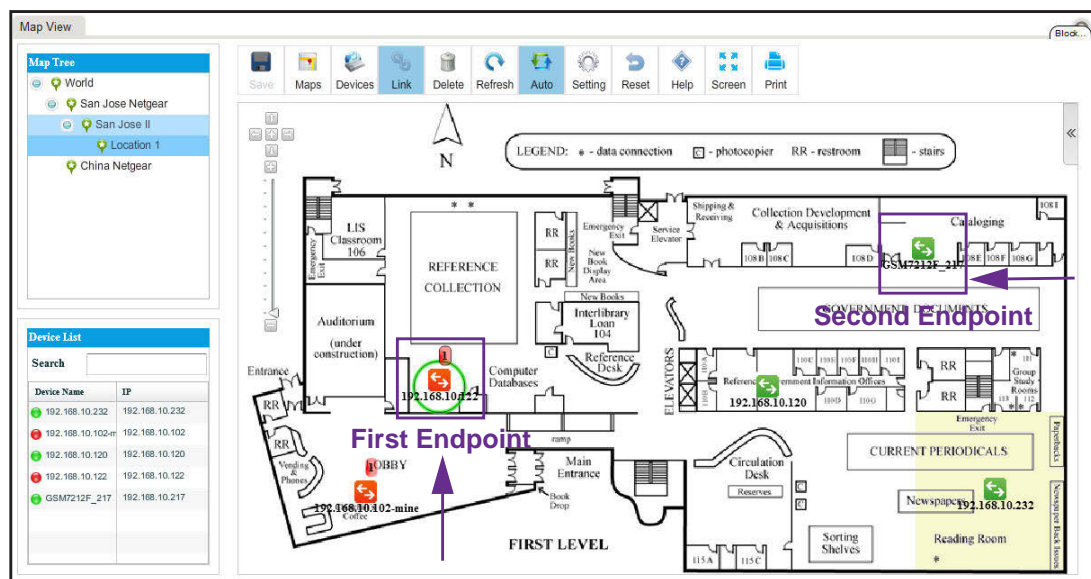
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **TOPOLOGY > MAP VIEWS**.



- From the Map Tree, select the map.
- Select the device that is the first endpoint of the link.



7. Click the **Link** icon.



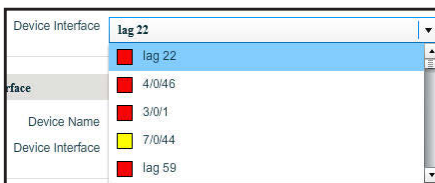
- Drag your cursor from the device that you selected in *Step 6* to the device that is the second endpoint of the link.

- Release the mouse button.

The Add Link screen displays.



- From the menus, select the device interface for each end of the link.

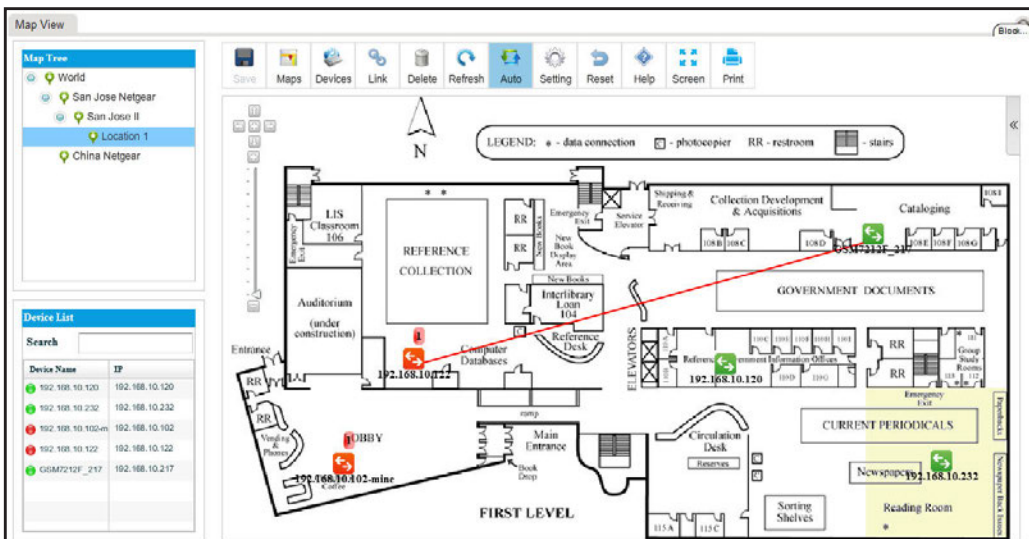


- Click the **OK** button.

The Add Link screen closes.

- Click the **Save** button.

The link is added.



Customize the Style of a Link on a Map

You can customize the way that a link displays.

➤ **To customize the style of a link:**

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 18.

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.

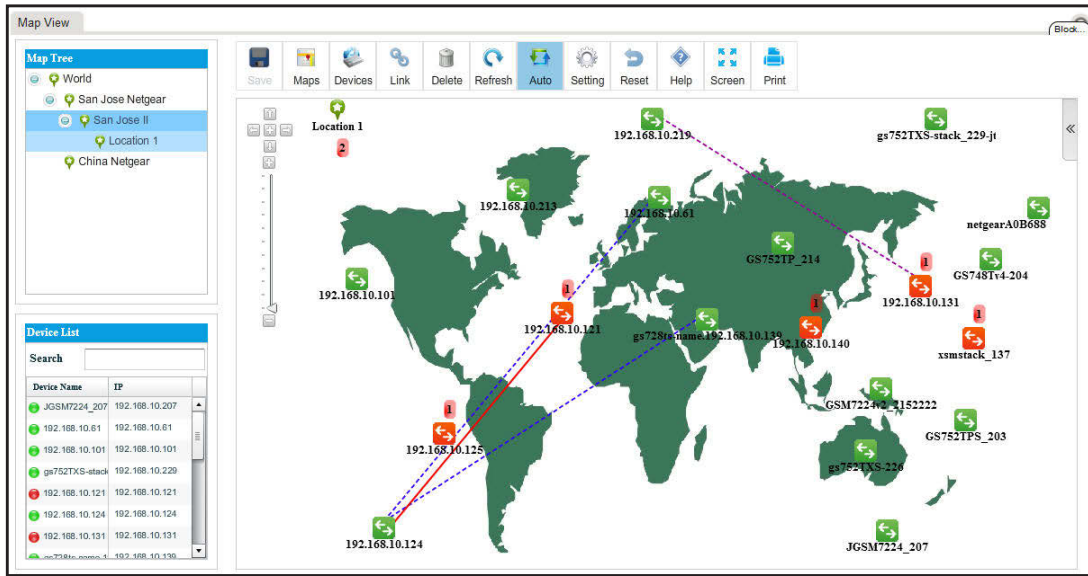
The Network Summary screen displays.

4. Select **TOPOLOGY > MAP VIEWS**.

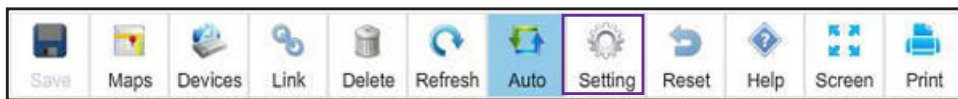
The screenshot shows the 'Map Views' interface in the NMS300 application. The top navigation bar includes 'HOME', 'WIRELESS', 'RESOURCES', 'MONITOR', 'CONFIG', 'ALARMS', 'TOPOLOGY', 'SFLOW', 'REPORTS', 'JOBS', 'USERS', and 'ADMIN'. The 'TOPOLOGY' menu is selected, and the 'MAP VIEWS' sub-menu is active. The main area displays a world map with several network devices connected by links. The devices are labeled with IP addresses and names, such as 'GS7461v2-SmartSwitch', 'jimmy-gsm727F', 'JGSM7224', and 'FS7521v2-NMS300'. A 'Device List' table is visible on the left side of the map view.

Device Name	IP
192.168.10.200	192.168.10.200
192.168.10.215	192.168.10.215
192.168.10.205	192.168.10.205
jimmy-gsm7212f	192.168.10.217
192.168.10.208	192.168.10.208
GS7461v2-Smar	192.168.10.204
192.168.10.213	192.168.10.213
68.10.205	68.10.205
68.10.214	68.10.214
192.168.10.202	192.168.10.202

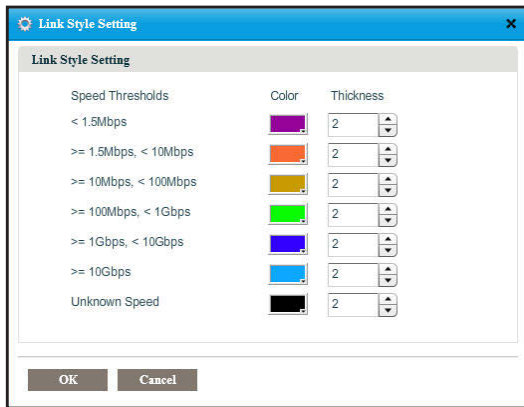
- From the Map Tree, select the map.



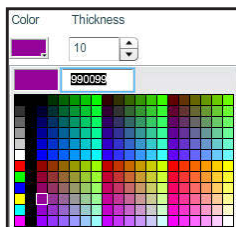
- Click the **Setting** icon.



The Link Style Setting screen.

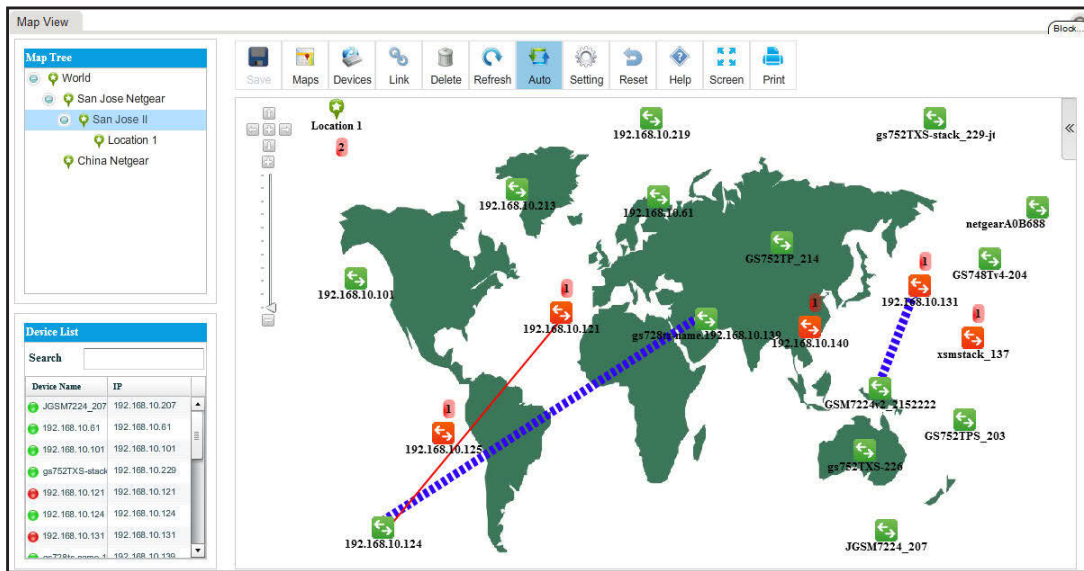


- Select the color and thickness of the links:



- Click the **OK** button.

The links on the map display the modified link styles.

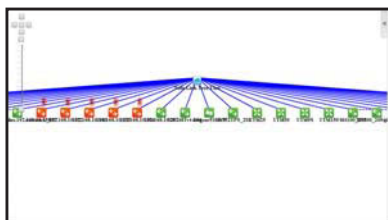


9. Click the **Save** button.
Your changes are saved.

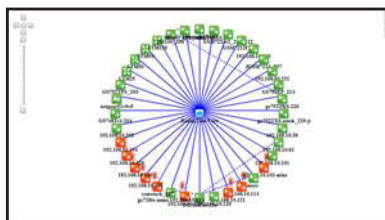
View and Manage Network Topologies

A network topology displays the structure of your network as a link tree view, radial view, or spring view:

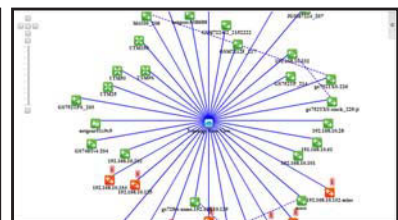
- **Link tree view.** The network nodes are displayed as a hierarchical organization chart.
- **Radial view.** The network nodes are displayed in an outwardly expanding radial pattern.
- **Basic spring view.** The network nodes are displayed in a pattern in which children nodes are in circles with parent nodes.



Link tree view



Radial view



Basic spring view

Figure 4. Network topology views

The following sections describe the tasks that relate to network topology views:

- *Add a Topology View*
- *View a Network Topology and Details About a Device*
- *Manage a Topology View*
- *Add a Link Between Devices on a Topology View*
- *Customize the Style of a Node and Link on a Topology View*
- *Remove a Topology View*

Add a Topology View

You can add a topology view of your network.

➤ To add a topology view of 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 18.

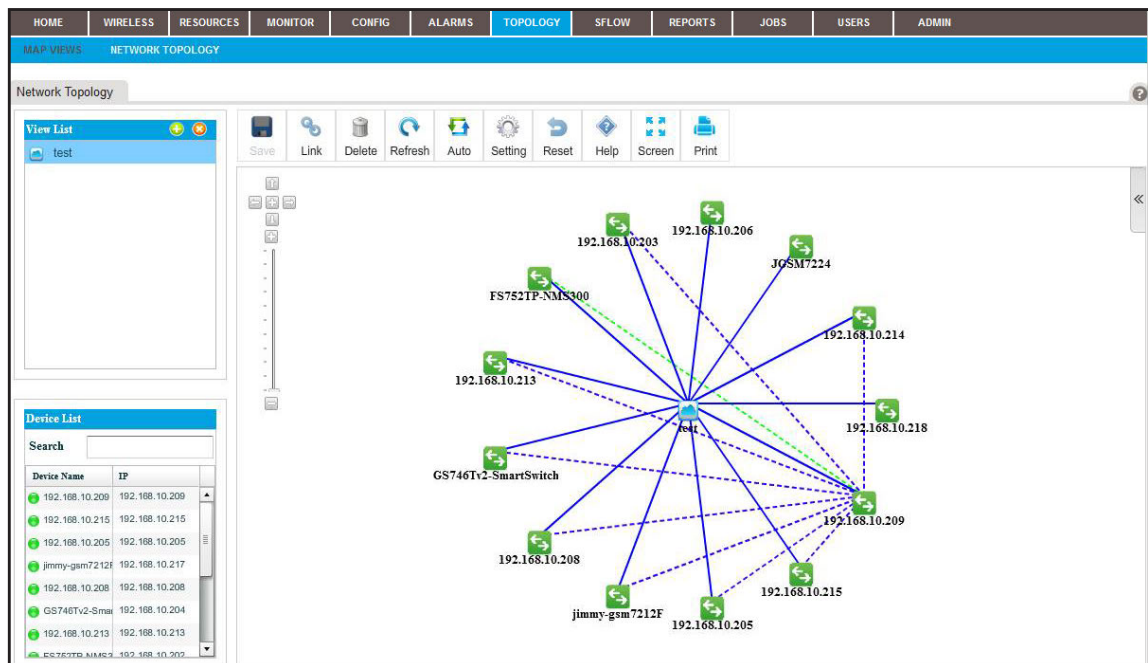
2. Enter your user name and password.

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

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

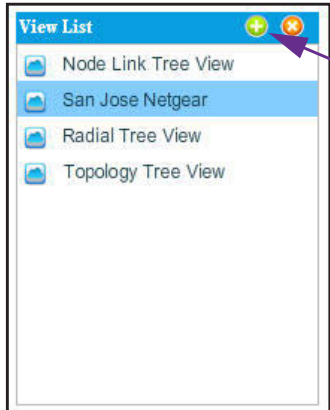
The Network Summary screen displays.

4. Select **TOPOLOGY > NETWORK TOLOPOGY**.

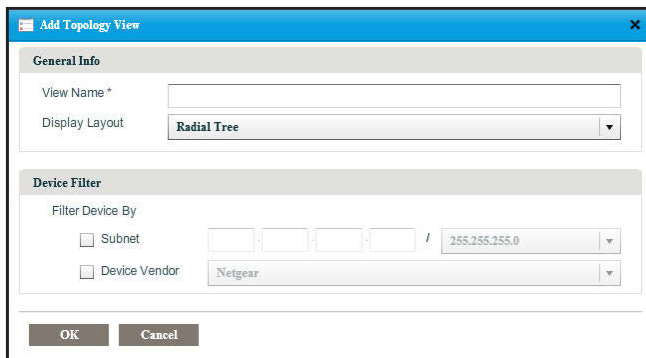


Note: If you did not yet add any topology views for your network, the screen does not display any.

- Next to View List, click the + (+) button.



The Add Topology View screen displays.



- Specify the following information:
 - General Info:**
 - View Name.** Enter a name for the topology view.
 - Display Layout.** From the menu, select **Radial**, **Node Tree**, or **Basic Spring**.
 - Device Filter.** Select one of the following check boxes and specify the corresponding information:
 - Subnet.** Enter an IP address and select a subnet from the menu.
 - Device Vendor.** Select a vendor from the menu.

- Click the **OK** button.

The Add Topology View screen closes.

- To view the new topology view, select it from the View List table.

The topology view displays.

View a Network Topology and Details About a Device

You can view a network topology and view details about the devices, including alarms.

➤ **To display a network topology and details about a device in the 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 18.

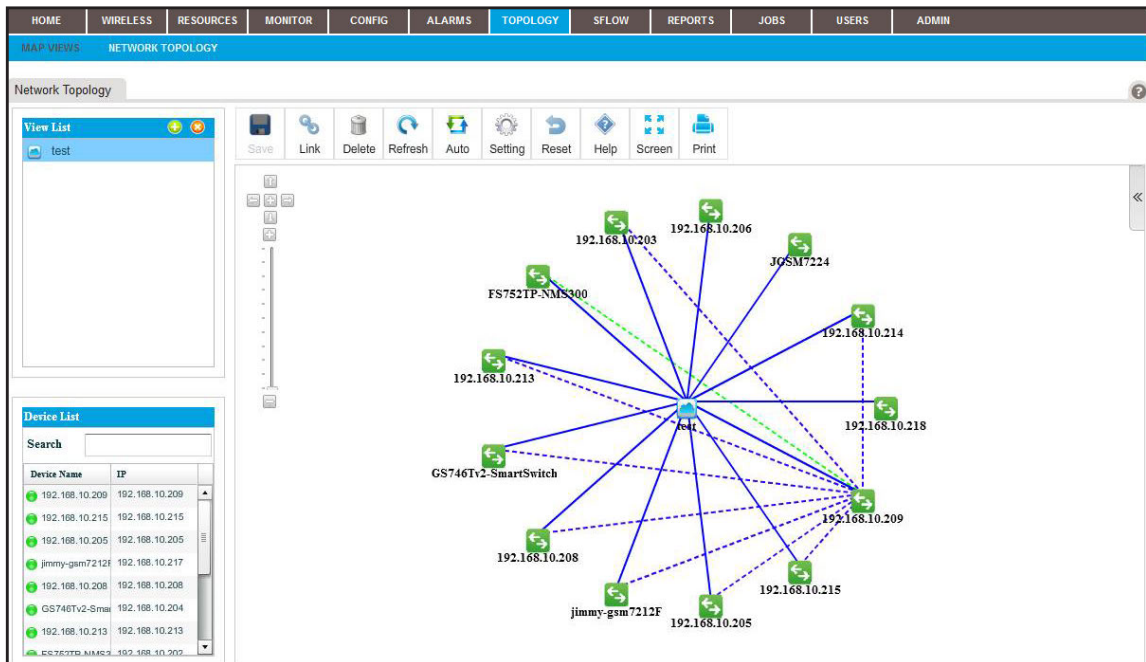
2. Enter your user name and password.

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.

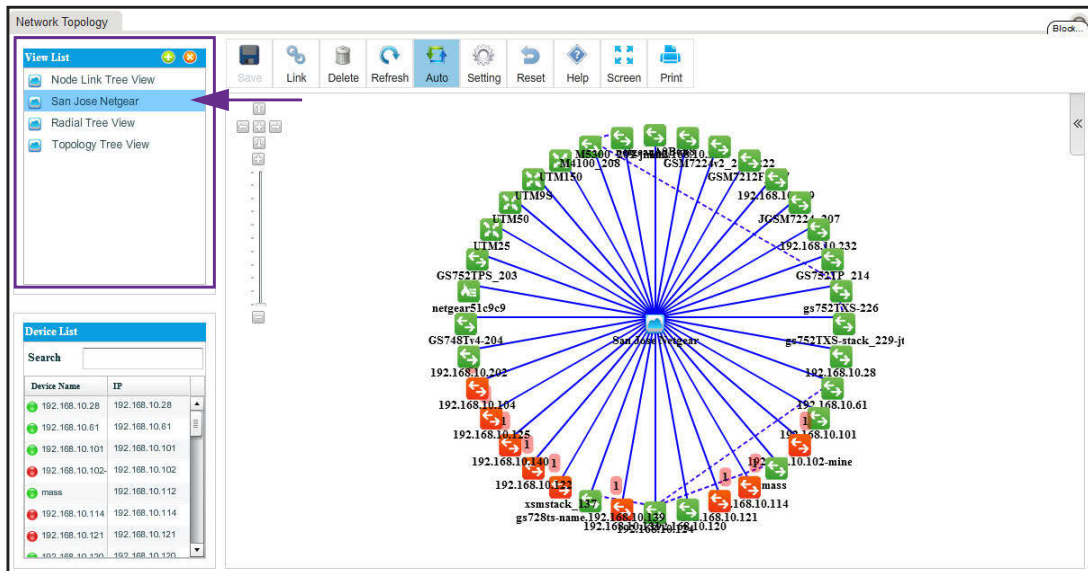
4. Select **TOPOLOGY > NETWORK TOPOLOGY**.



5. From the View List table, select the topology view.

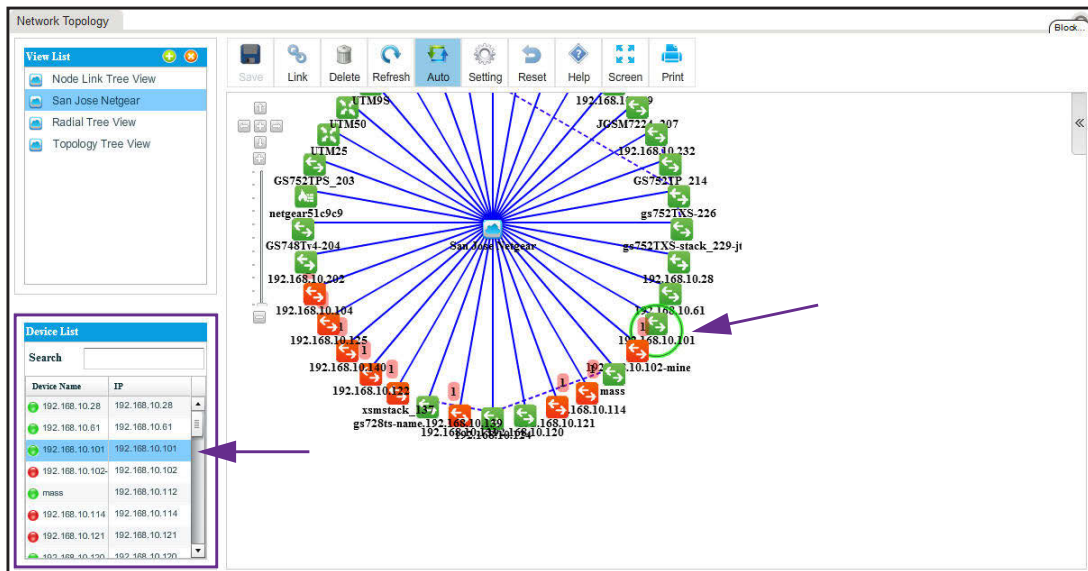
For information about adding a topology view, see *Add a Topology View* on page 199.

The selected view displays.



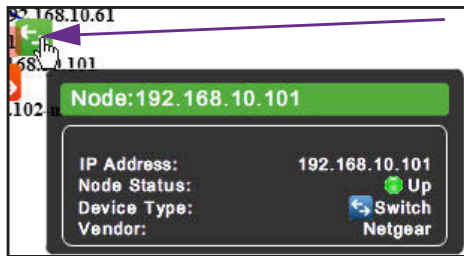
- From the Device List table, select a device.

A circle displays around the selected device.



- To view information about the device (node), point to the device on the map.

A pop-up screen similar to the following displays.

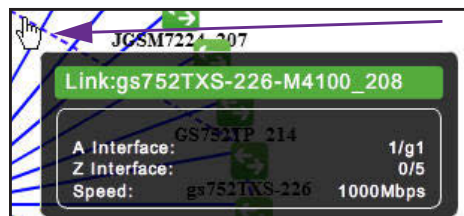


8. To see detailed information and the Dashboard menu for the device, double-click the device on the map.

For more information, see [View Device Details and Interface Details](#) on page 85.

9. To view the details for a link, point to the link on the map.

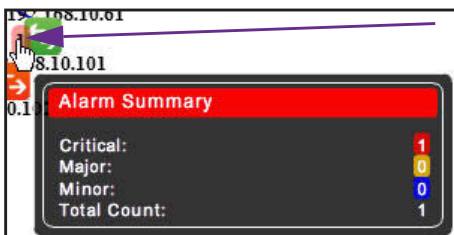
A pop-up screen similar to the following displays.



10. To view the summary for an alarm, point to the alarm summary on the map.

An alarm summary is displayed as a red-colored rectangular with a number.

A pop-up screen similar to the following displays.



Manage a Topology View

On the Network Topology screen, the icons that display above a topology view let you perform various tasks.



Figure 5. Icons on the Network Topology screen

The following procedure describes the tasks that you can perform for a topology view. For complicated tasks, the procedure points to a section that provides detailed information.

➤ **To manage a topology view:**

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 18.

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.

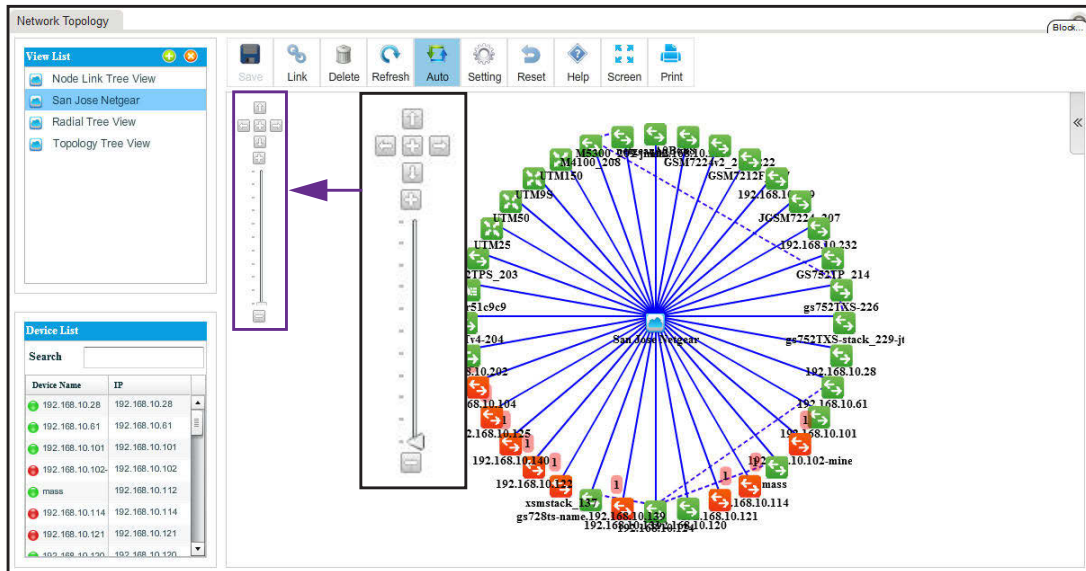
The Network Summary screen displays.

4. Select **TOPOLOGY > NETWORK TOPOLOGY**.

The screenshot displays the 'Network Topology' interface. On the left, there is a 'View List' table with a search bar and a list of device names and IP addresses. The main area shows a network diagram with a central hub labeled 'NMS300' connected to various peripheral devices like 'FS7521P-NMS300', 'GS746T2-SmartSwitch', and 'jimmy-gsm7212F'. The interface also includes a navigation menu at the top and a toolbar with icons for Save, Link, Delete, Refresh, Auto, Setting, Reset, Help, Screen, and Print.

5. From the View List table, select the topology view.

- To rescale the topology view, use the scaling tool that displays on the left of the topology view.



- To reposition the topology view, hold your cursor on the topology view and drag the topology view to a new position.
- Take one of the following actions:
 - Let the application refresh the topology view automatically. Click the **Auto** icon.
The topology view refreshes automatically every two minutes. Automatic refreshment is the default setting.
 - Refresh the topology view manually. Click the **Refresh** icon.
The topology view refreshes once immediately.
 - Add a link between devices on a topology view. Click the **Link** icon.
For more information, see [Add a Link Between Devices on a Topology View](#) on page 206.
 - Customize the link style settings. Click the **Setting** icon.
For more information, see [Customize the Style of a Node and Link on a Topology View](#) on page 209.
 - Remove a link from the topology view:
 - Select the link.
 - Click the **Delete** icon.
The link is removed.
 - Undo unsaved changes. Click the **Reset** icon.
The unsaved changes are reset.

- Save changes. Click the **Save** icon.
Your changes are saved. When the Save icon is grayed out, everything is saved.
- Open the Help screen. Click the **Help** icon.
The Help pop-up screen displays.
- Enter full-screen mode. Click the **Screen** icon.
The screen displays in full-screen mode. To return to the regular screen display, either press the **Esc** key, or from the full screen, click the **Screen** icon.
- Print the screen. Click the **Print** icon.
The topology view is printed.

Add a Link Between Devices on a Topology View

You can add a link between devices. For devices that do not support link discovery through Link Layer Discovery Protocol (LLDP), you can manage links manually. When you know that physical connections exist for the non-LLDP devices, you can draw these links manually and also update them manually when the physical connections are reconfigured.

➤ To add a link between devices on a topology view:

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 18.

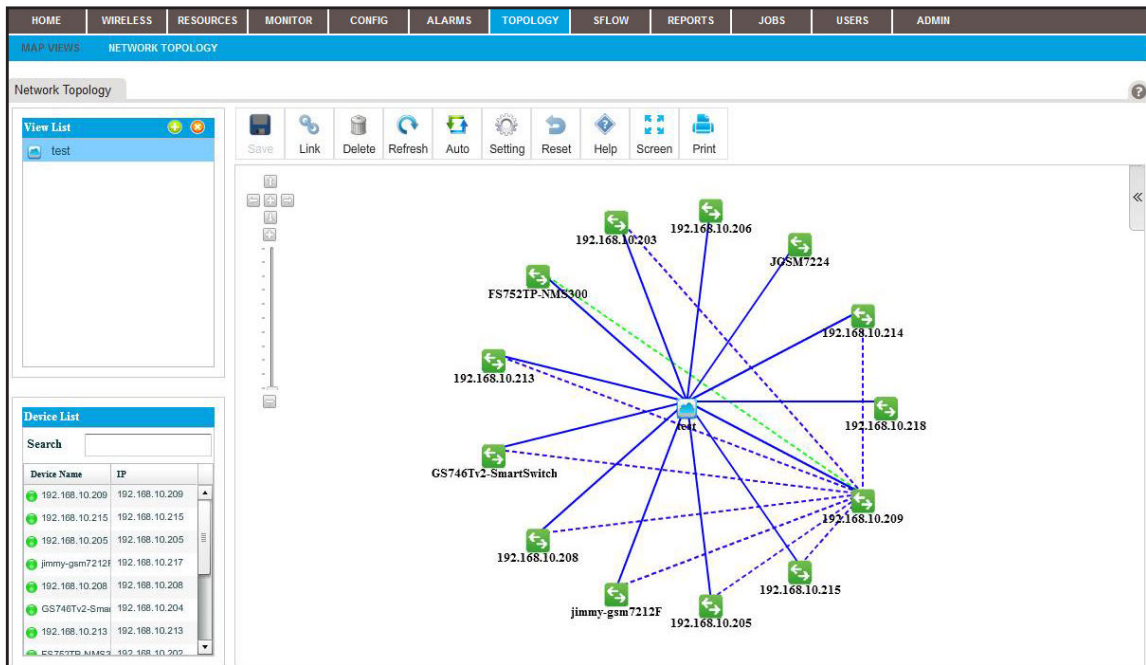
2. Enter your user name and password.

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

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

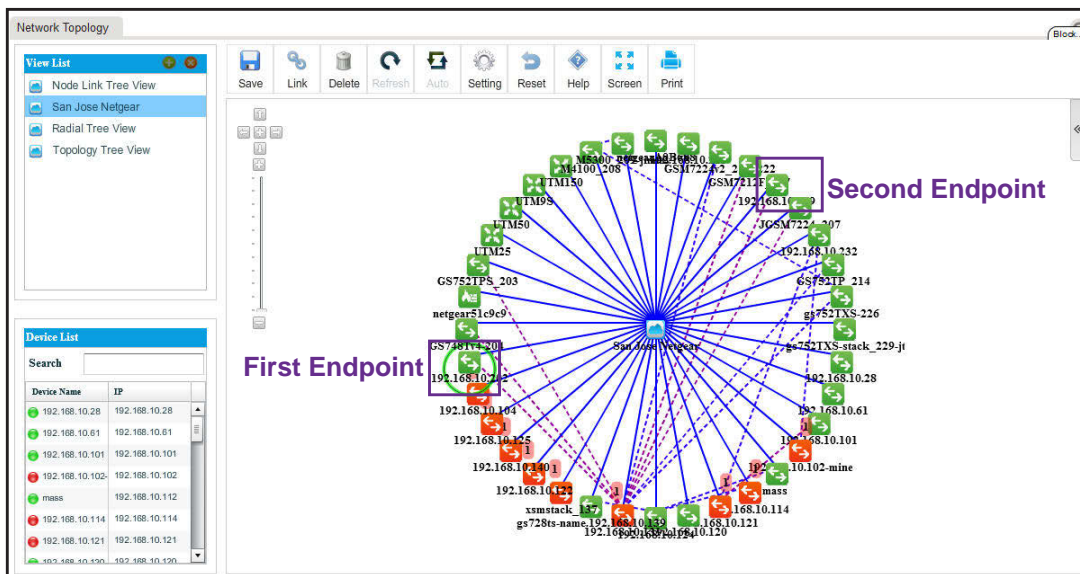
The Network Summary screen displays.

4. Select **TOPOLOGY > NETWORK TOPOLOGY**.



5. From the View List table, select the topology view.

6. Select the device that is the first endpoint of the link:



7. Click the **Link** icon.



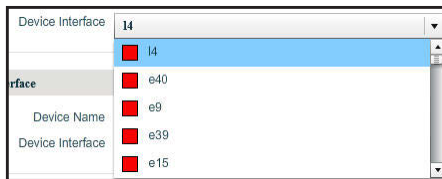
8. Drag your cursor from the device that you selected in *Step 6* to the device that is the other endpoint of the link.

9. Release the mouse button.

The Add Link screen displays.



10. From the menus, select the device interface for each end of the link.

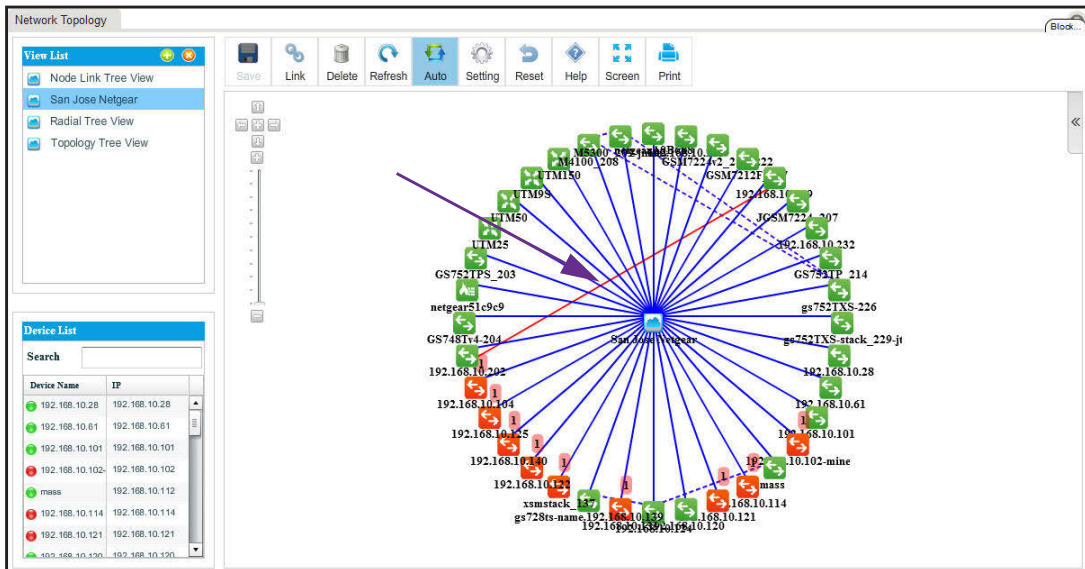


11. Click the **OK** button.

The Add Link screen closes.

12. Click the **Save** button.

The link is added between the two devices.



Customize the Style of a Node and Link on a Topology View

You can customize the way that a node and a link display.

➤ **To customize the style of a node and link:**

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 18.

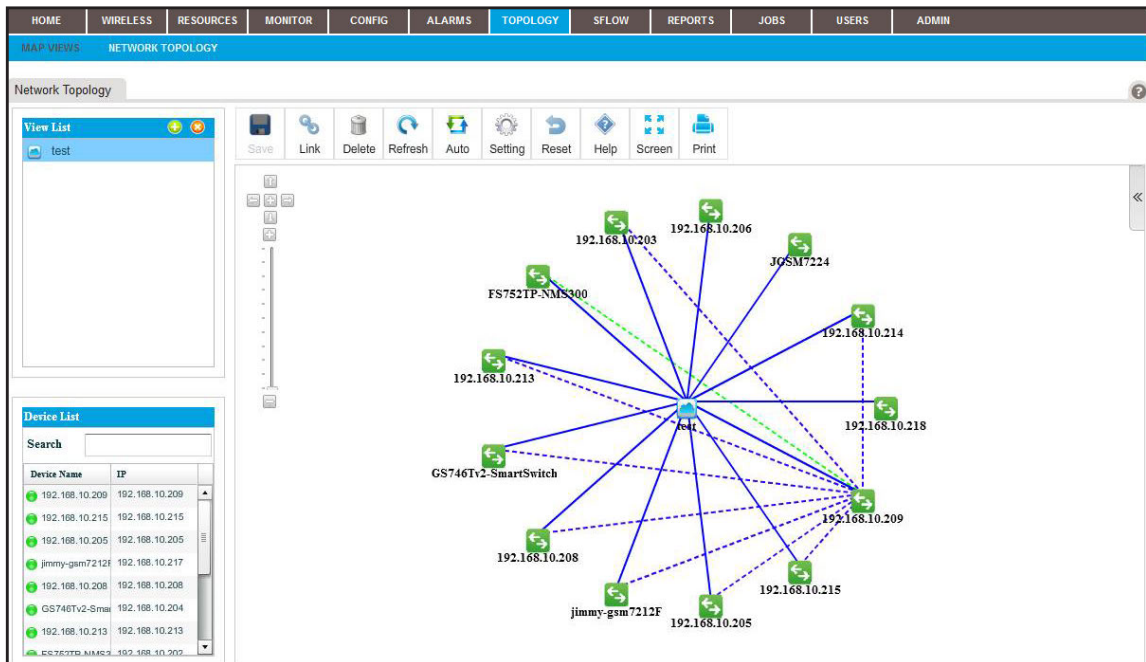
2. Enter your user name and password.

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

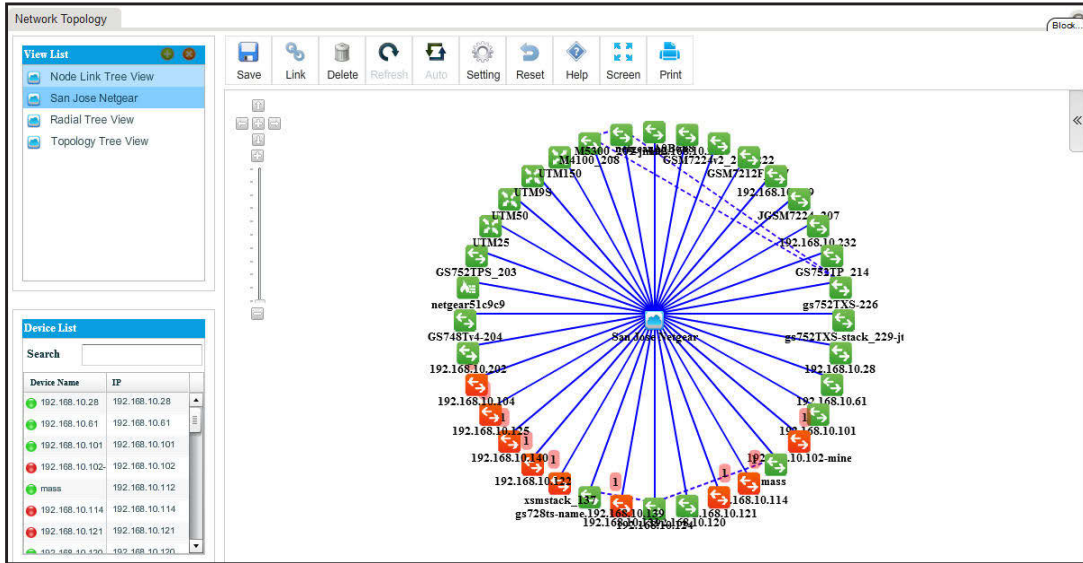
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **TOPOLOGY > NETWORK TOPOLOGY**.



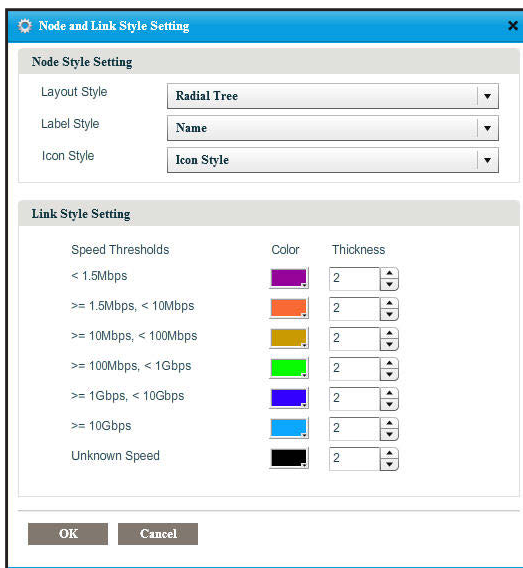
- From the View List table, select the topology view.



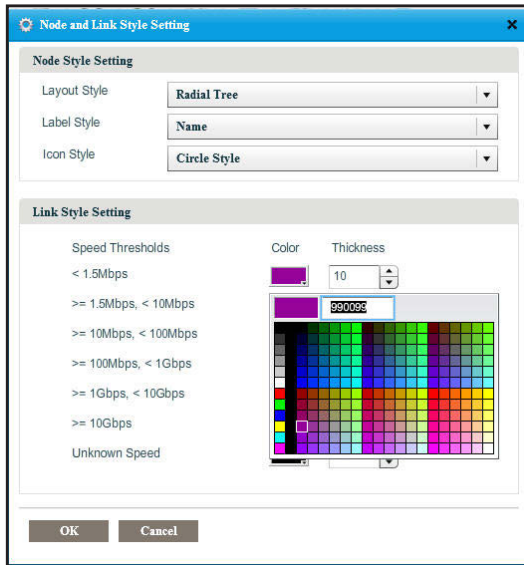
- Click the **Setting** icon.



The Node and Link Style Settings screen displays.

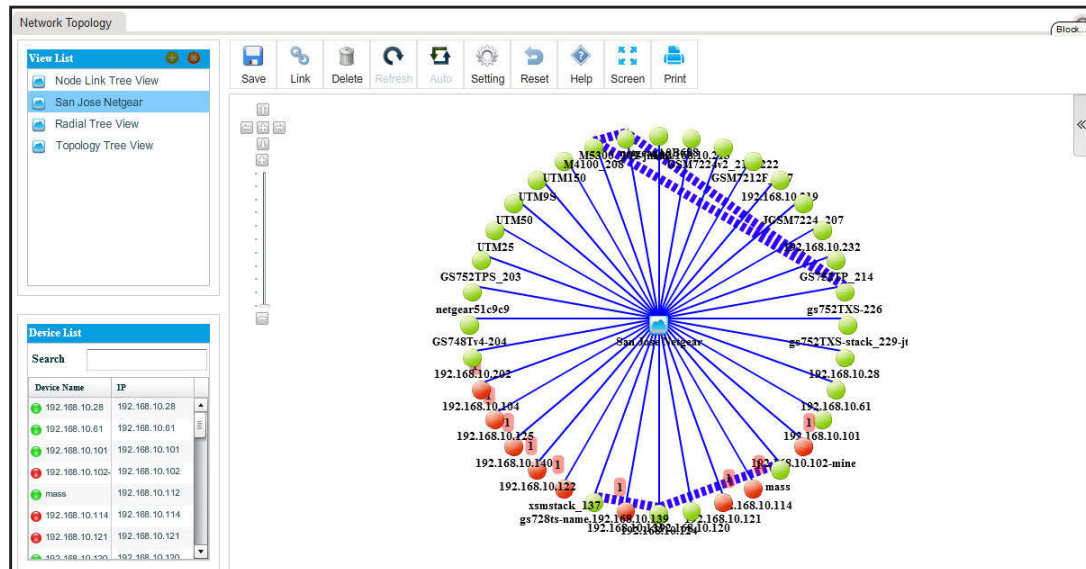


7. Select the node style settings and link style settings:



8. Click the **OK** button.

The nodes and links on the view display the modified node and link styles.



9. Click the **Save** button.

Your changes are saved.

Remove a Topology View

You can remove a topology view that you no longer need.

➤ **To remove a topology view:**

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 18.

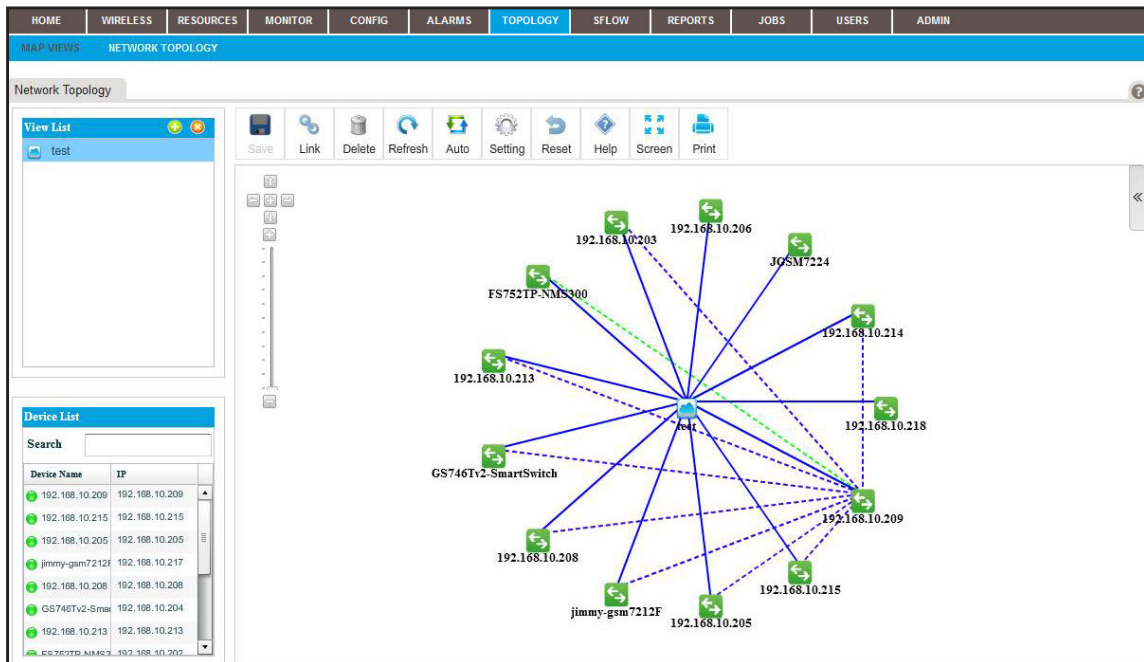
2. Enter your user name and password.

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

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

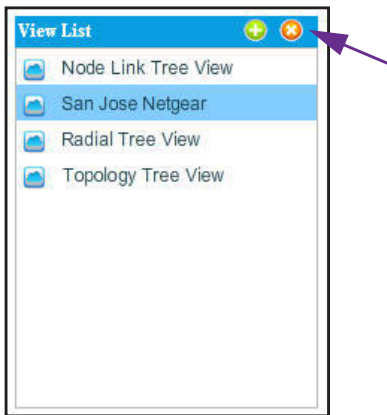
The Network Summary screen displays.

4. Select **TOPOLOGY > NETWORK TOPOLOGY**.



5. From the View List table, select the topology view.

- Next to View List, click the **X** button.



A pop-up confirmation screen displays.

- Click the **Yes** button.

The topology view is removed from the View List table and deleted.

8

8. Manage sFlow

Manage sFlow sources and view the sFlow summary

Using packet sampling, sampled flow (sFlow) lets you monitor managed switches in high-speed switched networks.

This chapter covers the following topics:

- *Set Up the sFlow Collection Server and Manage the sFlow Settings*
- *Manage sFlow Sources*
- *View and Export the Results of sFlow Monitoring*

Set Up the sFlow Collection Server and Manage the sFlow Settings

➤ **To configure the SMS 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 18.

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**.

The screenshot shows the NMS300 web interface with the 'ADMIN' menu selected. The 'SETTINGS' page is displayed, showing a grid of configuration options. The 'sFlow' section is circled in red, highlighting the 'sFlow Settings' link.

HOME	WIRELESS	RESOURCES	MONITOR	CONFIG	ALARMS	TOPOLOGY	SFLOW	REPORTS	JOBS	USERS	ADMIN
SETTINGS AUDIT LOG LICENSE MANAGEMENT											
System and Website Settings											
Getting Started with NMS Discover your network and add the devices you want to manage. <ul style="list-style-type: none"> > Discover Devices > SMTP Email Settings > SMS Server Settings > Device Groups 				System Settings Set global settings for the system and website. <ul style="list-style-type: none"> > Data Retention Period > Inventory Polling > Idle Time Out > Real-time Chart 				Customize Customize the navigation and look of your web portal. <ul style="list-style-type: none"> > Customize Network Summary View > Customize Wireless Summary > Customize Alarm Color > Auto Refresh Setting > Customize Network Dashboard 			
Account Information View or modify users, or create new users. <ul style="list-style-type: none"> > User Management > Edit Account > Change Password 				Manage Monitor and Alarm Network monitor, alarm and threshold related configurations. <ul style="list-style-type: none"> > Alarm Configuration > Monitor Configuration 				my.NETGEAR.com Account Profile Configure and validate my.NETGEAR.com account profile through my.NETGEAR.com Web API. <ul style="list-style-type: none"> > my.NETGEAR.com Account Profile 			
sFlow Set sFlow related configurations. <ul style="list-style-type: none"> > sFlow Settings > Manage sFlow Source 				Manage External File Server External File Server configurations and File Processing with External File Server. <ul style="list-style-type: none"> > External File Server Setting > Import or Export Config Files 				License And Version Information View NMS300 license, supported device and version information. <ul style="list-style-type: none"> > License Management > NMS300 Version 			

- Under sFlow, click the **sFlow Settings** link.

- Enter the sFlow settings:
 - **History Data Save in (days)**. From the menu, select how long sFlow data is saved. By default, the data is saved for 15 days. You can also select 3, 5, or 7 days.
 - **sFlow Collection Server**. Enter the IP address of the sFlow collection server.
 - **sFlow Collection Server Port**. Enter the port number for the sFlow collection server. By default, the port number is 6343.
 - **Sampling Rate**. Enter the rate at which the data is sampled. By default, the rate is 1024, which means that 1 in 1024 packets is sampled. You can set a higher sampling rate, which might result in a higher accuracy but increases the sFlow traffic. You can set the sampling rate from 1024 to 65536 packets.
 - **Max Header Size**. Enter the maximum size of the header. By default, the size is 128, which means that a maximum of 128 bytes is sampled from a packet. You can set the maximum header size from 20 to 256 bytes.
- Click the **Submit** button.
Your changes are saved.

Manage sFlow Sources

An sFlow system consists of multiple devices performing two types of sampling:

- Random sampling of packets or application-layer operations
- Time-based sampling of counters

The sampled packet and operation information, referred to as flow samples, and the sampled counter information, referred to as counter samples, are sent as sFlow datagrams to the application, which functions as the sFlow collector.

sFlow is supported for managed switches only (see *NETGEAR Managed Switches* on page 12) and for a maximum of 16 interfaces at a time.

➤ **To enable interfaces of managed switches as sFlow sources:**

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 18.

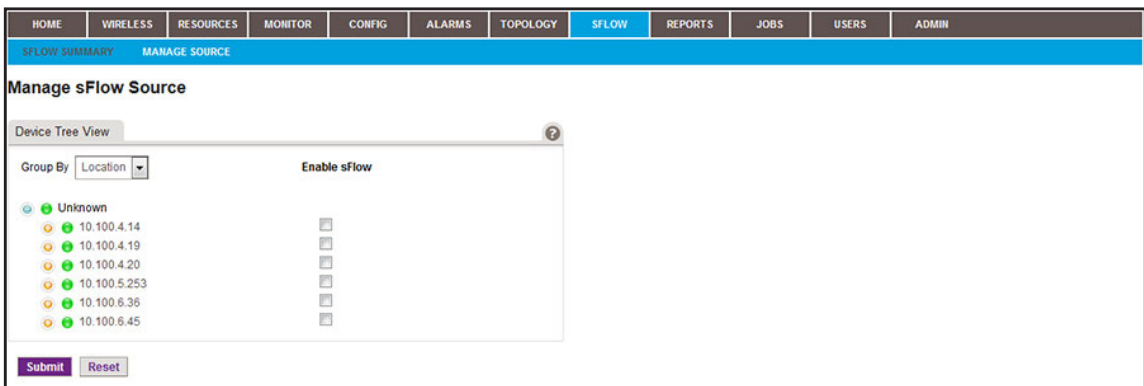
2. Enter your user name and password.


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

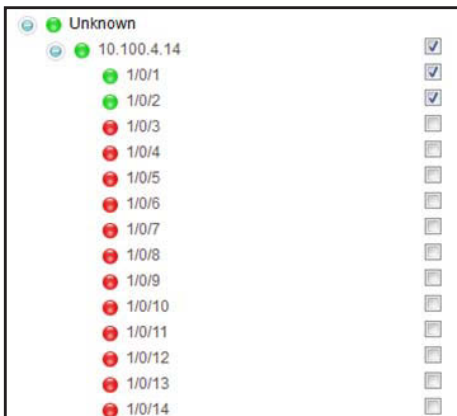
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **SFLOW > MANAGE SOURCE**.



5. Click the  icon to the left of the IP address of a managed switch.



6. Select the check boxes for active interfaces (displayed with green icons) that must be included as sFlow sources.
7. To add interfaces of another managed switch, scroll down and repeat [Step 5](#) and [Step 6](#).

Note: You can select a maximum of 16 interfaces from the same or different managed switches.

8. Click the **Submit** button.

Your changes are saved.

View and Export the Results of sFlow Monitoring

If you specify the sFlow sources, and traffic is present for these sources, you can view the results of sFlow monitoring.

The application provides the following defaults and filter options for viewing the results:

- **Source.** You can select to display the source switch. By default, the application displays information about the source switch with the lowest IP address.
- **Interface.** You can select to display the source interface. By default, the application displays information about all source interfaces for the selected source switch.
- **Date time range.** You can select to display a time range or customize a time range. By default, the application displays the sFlow information that is collected today.
- **Top.** You can select to display the top 10 or top 20 active sFlow streams. By default, the application displays information about the top 10 active sFlow streams.

➤ To view the results of sFlow monitoring:

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 18.

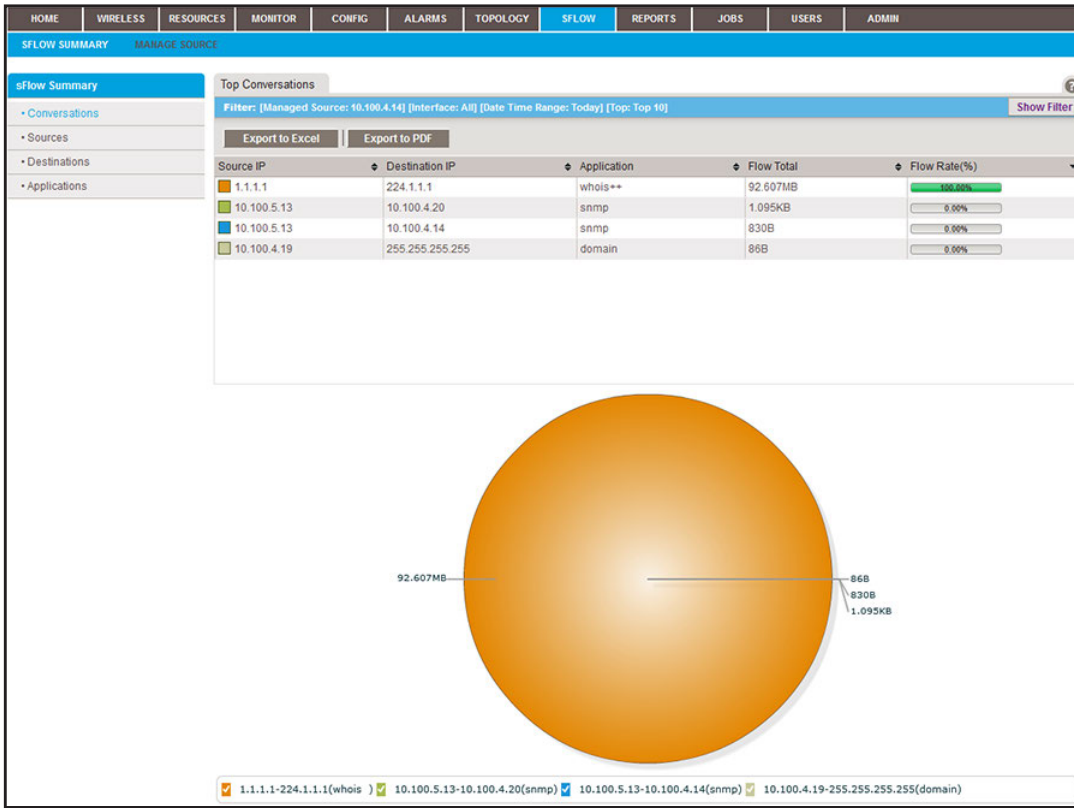
2. Enter your user name and password.

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 **SFLOW > SFLOW SUMMARY**.



By default, the table and associated pie chart show the sFlow conversations (that is, application traffic streams) between source and destination IP addresses, their total flow traffic, and their flow rate in percentage.

By default, the application displays the top 10 streams that sFlow collected today for the device with the lowest IP address.

5. To view a table and pie chart of IP sources, destinations, or applications, click one of the following **Show Summary** menu links:
 - **Sources.** The table and associated pie chart show the sFlow source IP addresses and the total flow traffic and flow rate in percentage for these addresses.
 - **Destinations.** The table and associated pie chart show the sFlow destination IP addresses and the total flow traffic and flow rate in percentage for these addresses.
 - **Applications.** The table and associated pie chart show the sFlow applications and the total flow traffic and flow rate in percentage for these applications.
6. To filter the event entries that are listed, click the **Show Filter** button.

You can filter the event entries by criteria such as managed source IP address, interface number, time range, and top active interfaces.

To hide the filter, click the **Hide Filter** button.
7. Click the **Export to Excel** button or the **Export to PDF** button.
8. To save the sFlow information on your computer, follow the directions of your browser.

9

9. Generate and View Reports

Record how your network performs

You can generate reports from either built-in or customized report templates, and you can view them at any time. You can create new report templates that generate one-time reports or regular reports automatically on a schedule.

This chapter covers the following topics:

- *Manage Report Templates*
- *Generate and Schedule Reports*
- *View and Remove Saved Reports*

Manage Report Templates

The application provides default report templates that are based on inventory, devices, wireless devices, wireless clients, traffic, and storage device components. You can generate and view a report based on such templates. You can also add a new report template based on an existing template, modify an existing template, and remove a report template.

The following figure shows the types of reports that the templates are based on.

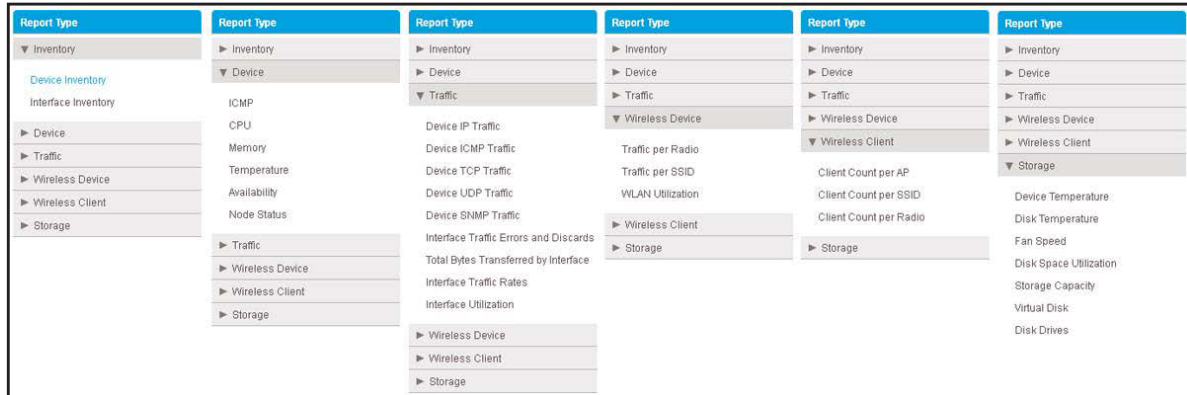


Figure 6. Overview of the types of reports

Add or Modify a Report Template

To generate reports for your particular network and situation, you can add a report template that is based on a default report template or modify a default report template.

➤ To select a report style and add a report template or modify an existing report template:

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 18.

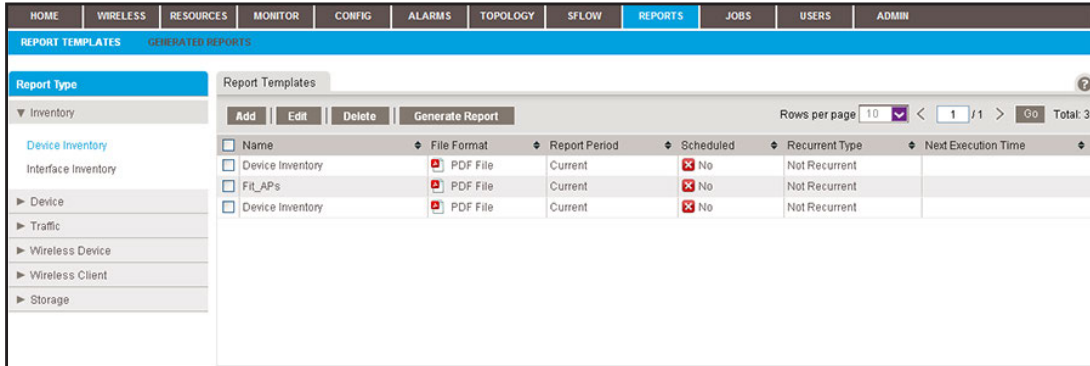
2. Enter your user name and password.

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 **REPORTS > REPORT TEMPLATES**.



5. To add columns to or remove them from the Report Templates 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, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

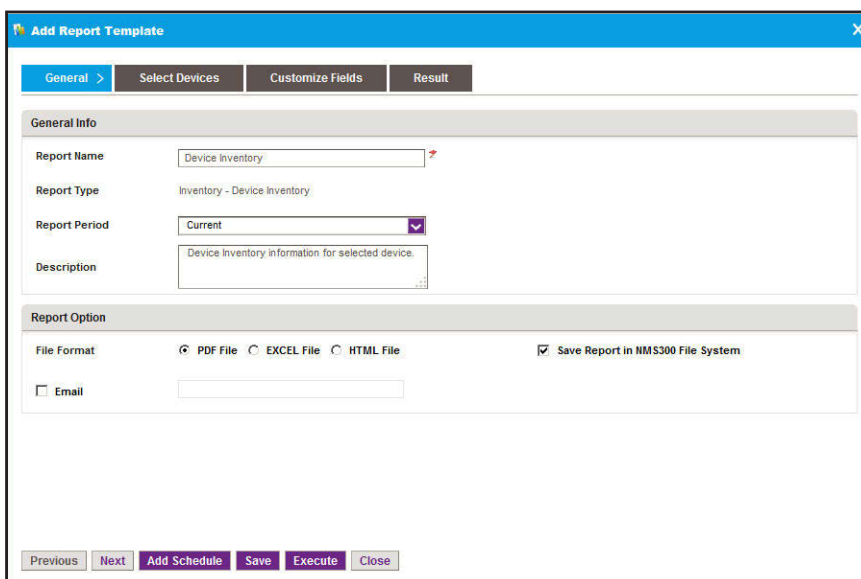
6. From the **Report Type** menu, select the report type.

For some report types, the application provides one or more default report templates. For other report types, the application does not provide any default report templates and you must add a report template.

7. Add a report template or modify an existing report template:

- To add a report template, click the **Add** button.
- To modify an existing report template:
 - a. From the Report Templates table, select the report template.
 - b. Click the **Edit** button.

For a new report template, the Add Report Template screen displays. For an existing report template, the Edit Report Template screen displays.



Depending on your type of report selection, a different Add Report Template screen or Edit Report Template screen might display.

8. Enter or modify the following general report information:

- **General Info:**
 - **Report Name.** Enter or modify the name for the report template.
 - **Report Type.** Your selection in *Step 6* determines the content of this field.
 - **Report Period.** Select the period to which the report template applies.
 - **Description.** Enter or modify the description for the report template.

- **Report Option:**

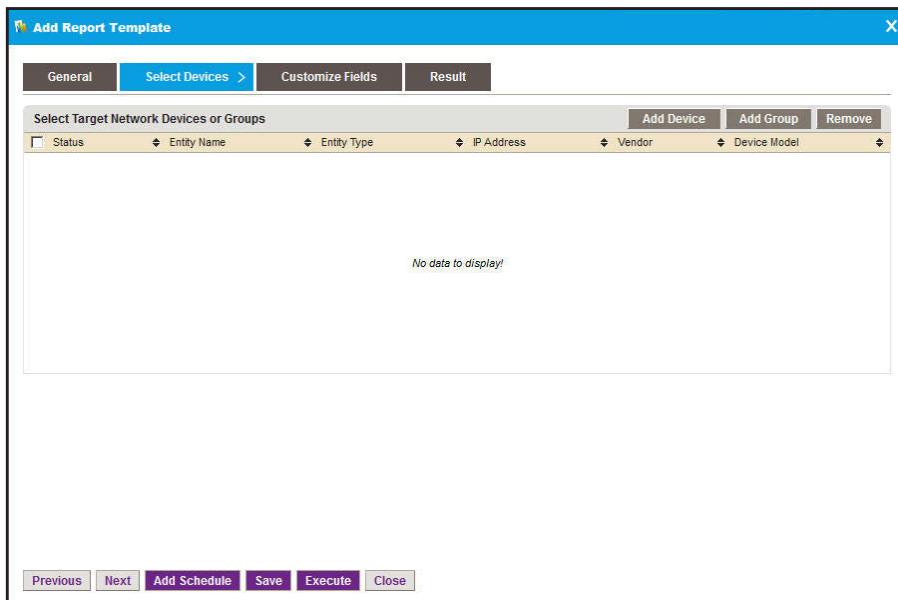
- **File Format.** Select the **PDF File**, **EXCEL File**, or **HTML file** radio button.

To save generated reports, select the **Save Reports in NMS300 File System** check box.

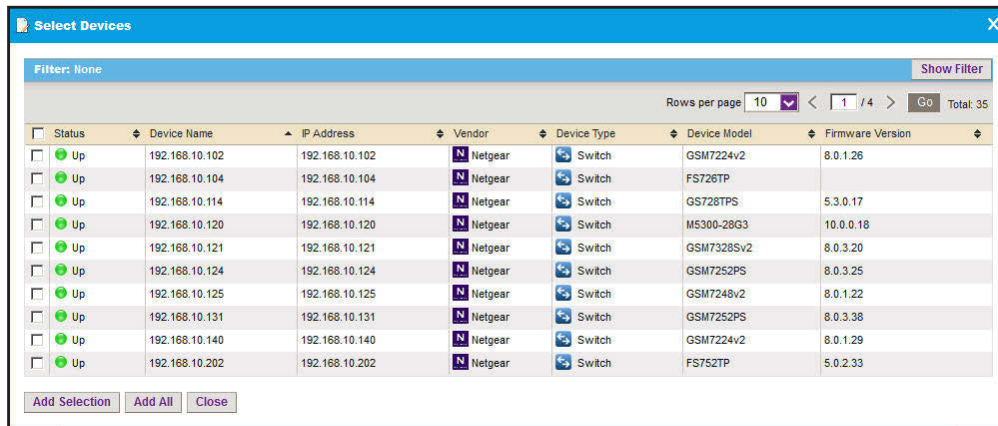
For information about how to view reports that were generated previously, see *View and Remove Saved Reports* on page 230.

- **Email.** To let the application send a copy of the report to your email address, select the **Email** check box and enter or modify your email address.

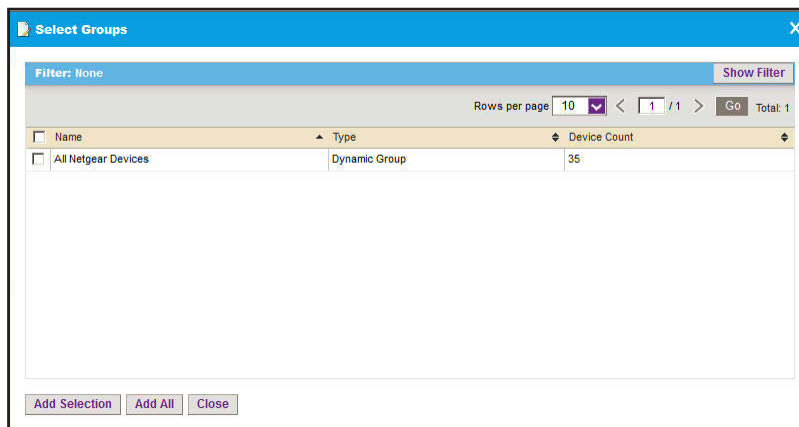
9. Click the **Select Devices** tab.



10. 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 of 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 of 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.
 - e. If you are modifying an existing report template, to remove devices or groups, select the devices or groups, and click the **Remove** button.
The devices or groups are removed from the Select Target Network Devices or Groups table.

11. Click the **Customize Fields** tab.

Depending on your type of report selection, a different Customize Fields screen might display.

- a. In the Customize Report Fields section, specify the fields and the order in which you want them to appear in your report template.

To select the fields, use the >, <, >>, and << buttons. To arrange their order, use the up and down buttons.

- b. In the Data Sort section, specify how you want the information sorted.

You can sort by device and by descending or ascending order.

12. Click the **Save** button.

The report template is saved and added to the Report Template table.

Remove a Report Template

When you delete a report generation job from the Jobs table, the application deletes the report template for the job automatically. For more information, see [View and Manage Jobs](#) on page 234. You can also remove a report template manually.

➤ To remove a report template manually:

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

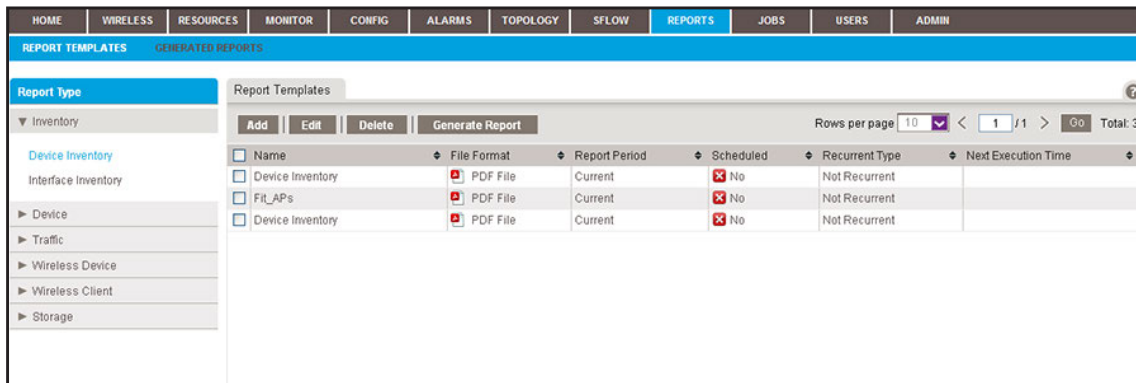
For more information, see [Log In to the Application](#) on page 18.

2. Enter your user name and password.

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

- Click the **Sign In** button.
The Network Summary screen displays.

- Select **REPORTS > REPORT TEMPLATES**.



- To add columns to or remove them from the Report Templates 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, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.
- From the **Report Type** menu, select the report type.
- Select the report template.
- Click the **Delete** button.
A pop-up confirmation screen displays.
- Click the **Yes** button.
The report template is removed from the Report Templates table and deleted.

Generate and Schedule Reports

You can generate reports from an existing report template. You can create one-time reports manually that are generated immediately or schedule one-time reports that are generated later. You can also schedule recurring reports that are generated automatically.

Generate a One-Time Report Immediately

You can generate a new report immediately from an existing template. For information about how to schedule the generation of a one-time report later, see [Schedule a Report](#) on page 228.

➤ To generate and view a report:

- 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 18.

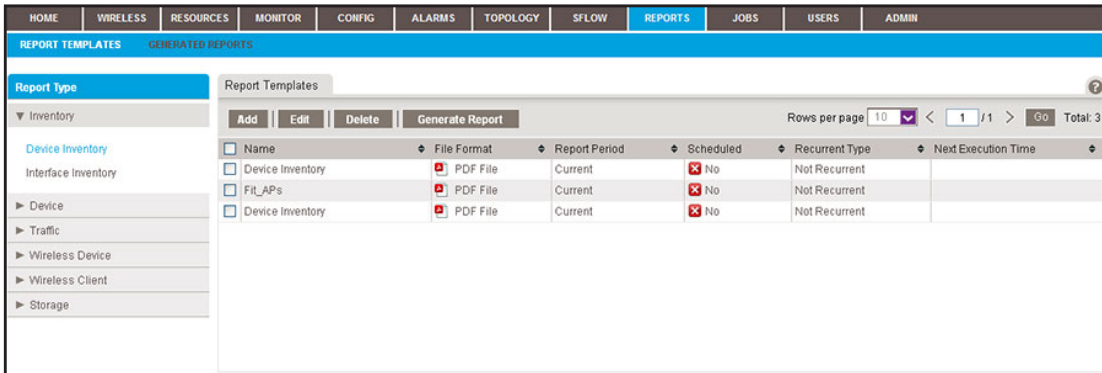
2. Enter your user name and password.

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 **REPORTS > REPORT TEMPLATES**.

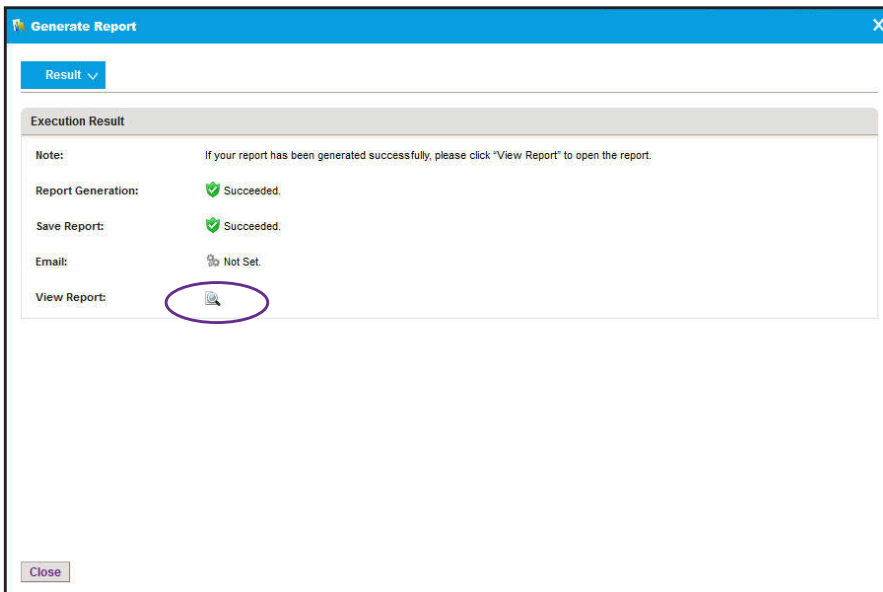


5. To add columns to or remove them from the Report Templates table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

You can choose from the following columns: Name, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

6. From the **Report Type** menu, select the report type.
7. Select the report template.
8. Click the **Generate Report** button.

The Generate Report screen displays the results.



9. Click the **View Report** button.

The report displays.

10. Click the **Close** button.

The screen closes.

Schedule a Report

You can schedule a report from an existing template for generation at a future time, or you can schedule the report for generation on a recurring basis.

➤ **To generate a report according to a schedule:**

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 18.

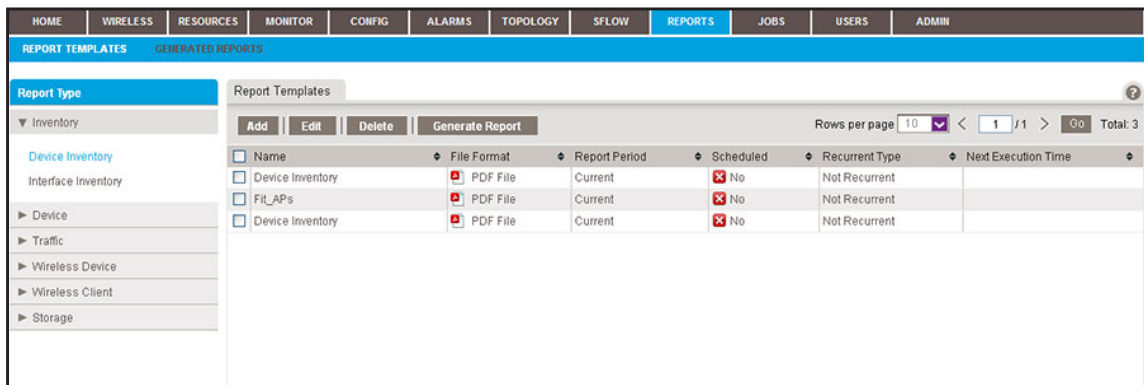
2. Enter your user name and password.

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 **REPORTS > REPORT TEMPLATES**.



5. To add columns to or remove them from the Report Templates 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, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

6. From the **Report Type** menu, select the report type.
7. Select the report template.

- Click the **Edit** button.

Depending on your type of report selection, a different Edit Report Template screen might display.

- Click the **Add Schedule** button.

- From the **Enable** menu, select **Yes**.
- Specify whether the application generates the report once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering the corresponding information:
 - One time scheduled.** This is the default selection.
In the **Starting On** field, enter a date and time.

- **Recurrent.** The screen adjusts to display more fields.

Enter the following information:

- In the **Starting On** field, enter a date and time.
 - From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.
 - Select the **End Time** radio button and enter the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.
12. Click the **Submit** button.

The Schedule screen closes. The report generation schedule becomes part of the report template.

13. On the Edit Report Template screen, click the **Save** button.

The report is generated according to the schedule that you set.

View and Remove Saved Reports

You can view the saved reports in the application. However, reports are saved for the data retention period. For more information, see [Set the Data Retention Period](#) on page 247. You can also remove reports that you no longer need.

View a Saved Report

You can view a saved report.

➤ **To view a saved report:**

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 18.

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 **REPORTS > GENERATED REPORTS**.

<input type="checkbox"/>	Report Name	Report Category	Report Type	Report Period	File Format
<input type="checkbox"/>	Device Inventory	Inventory	Device Inventory	Current	PDF File
<input type="checkbox"/>	Client Count per Radio	Wireless Client	Client Count per Radio	Last 24 hours	PDF File
<input type="checkbox"/>	Client Count per Radio	Wireless Client	Client Count per Radio	Last 24 hours	PDF File
<input type="checkbox"/>	Client Count per Radio	Wireless Client	Client Count per Radio	Today	PDF File
<input type="checkbox"/>	Client Count per Radio	Wireless Client	Client Count per Radio	Customized period(by date)	PDF File
<input type="checkbox"/>	Client Count per AP	Wireless Client	Client Count per AP	Today	PDF File
<input type="checkbox"/>	WLAN Utilization	Wireless Device	WLAN Utilization	Today	PDF File
<input type="checkbox"/>	Traffic per SSID	Wireless Device	Traffic per SSID	Today	PDF File
<input type="checkbox"/>	Traffic per Radio	Wireless Device	Traffic per Radio	Today	PDF File
<input type="checkbox"/>	Client Count per SSID	Wireless Client	Client Count per SSID	Today	PDF File

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

You can choose from the following columns: Report Name, Report Category, Report Type, Report Period, File Format, Execution Type, Created Time, Created By, and Description.

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

You can filter the current jobs by criteria such as time range, category, and report type. The previous figure shows the Generated Reports table after a time range filter for the past 30 days was applied.

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

7. Select the report.
8. Double-click the report.

Your report opens.

Remove a Saved Report

You can remove a saved report that you no longer need.

➤ To remove a saved report:

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 18.

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 **REPORTS > GENERATED REPORTS**.

Report Name	Report Category	Report Type	Report Period	File Format
Device Inventory	Inventory	Device Inventory	Current	PDF File
Client Count per Radio	Wireless Client	Client Count per Radio	Last 24 hours	PDF File
Client Count per Radio	Wireless Client	Client Count per Radio	Last 24 hours	PDF File
Client Count per Radio	Wireless Client	Client Count per Radio	Today	PDF File
Client Count per Radio	Wireless Client	Client Count per Radio	Customized period(by date)	PDF File
Client Count per AP	Wireless Client	Client Count per AP	Today	PDF File
WLAN Utilization	Wireless Device	WLAN Utilization	Today	PDF File
Traffic per SSID	Wireless Device	Traffic per SSID	Today	PDF File
Traffic per Radio	Wireless Device	Traffic per Radio	Today	PDF File
Client Count per SSID	Wireless Client	Client Count per SSID	Today	PDF File

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

You can choose from the following columns: Report Name, Report Category, Report Type, Report Period, File Format, Execution Type, Created Time, Created By, and Description.

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

You can filter the current jobs by criteria such as time range, category, and report type. The previous figure shows the Generated Reports table after a time range filter for the past 30 days was applied.

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

7. Select the report.

8. Click the **Delete** button.

A pop-up confirmation screen displays.

9. Click the **Yes** button.

The report is removed from the Generated Reports table and deleted.

10. Manage Jobs

10

Manage the system jobs

You can view job detail and status information.

This chapter covers the following topics:

- *Schedule Jobs*
- *View and Manage Jobs*

Schedule Jobs

The application supports regular and time-consuming jobs that are used for configuration and management tasks. You can schedule these jobs for future execution on a one-time basis or on a recurrent basis for batch operations.

The application supports the following jobs, which are scheduled when you complete the corresponding procedures (see the section references in the following list):

- **Configuration file backup.** Both one-time and recurrent jobs are supported. For more information, see [Schedule a Backup Job](#) on page 117.
- **Configuration file restore.** One-time jobs are supported. For more information, see [Restore the Configuration of a Single Device](#) on page 123 and [Restore the Configuration of Several Identical Devices](#) on page 134.
- **Firmware upgrade.** One-time jobs are supported. For more information, see [Execute or Schedule a Firmware Upgrade](#) on page 150.
- **Report generation.** Both one-time and recurrent jobs are supported. For more information, see [Schedule a Report](#) on page 228.
- **Resource discovery.** Both one-time and recurrent jobs are supported. For more information, see [Schedule or Reschedule an Existing Discovery Job](#) on page 42.

Output files from completed jobs are saved for the data retention period. For more information, see [Set the Data Retention Period](#) on page 247.

View and Manage Jobs

You can view job detail and status information. You can also enable, disable, and delete jobs. For information about modifying or rescheduling jobs, see the section references in the previous section, [Schedule Jobs](#).

When you delete any of the following items from the Jobs table, the application deletes its corresponding profile or template from its database:

- **Discovery job.** You can create a discovery profile. For more information, see [Add or Modify a Discovery Profile](#) on page 37.
- **Backup job.** You can create a new backup profile. For more information, see [Add or Modify a Backup Profile](#) on page 112.
- **Report generation job.** You can create a report template. For more information, see [Manage Report Templates](#) on page 221.

When you delete any of the following items from the Jobs table, the application does *not* delete the related file from its database:

- **Restore configuration job.** To remove the configuration file from the application, you must delete the configuration file manually. For more information, see [Restore Your Device Configurations](#) on page 122.
- **Firmware upgrade job.** To remove the firmware file from the application, you must delete the firmware file manually. For more information, see [Upgrade Firmware for One or More Devices](#) on page 148.

➤ **To view and manage jobs:**

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 18.

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 **JOBS > JOB MANAGEMENT**.

Enable	Job Name	Job Type	Recurrent Type	Status	Last Execution Time	Next Execution Time
<input type="checkbox"/>	No 3.1.0.13	Image Upgrade	Not Recurrent	Failed	09/11/2013 03:18:22	
<input checked="" type="checkbox"/>	Yes Inventory Polling	Inventory	Daily	Wait to run	09/11/2013 01:00:00	09/12/2013 01:00:00
<input type="checkbox"/>	No 3.1.0.13	Image Upgrade	Not Recurrent	Failed	09/10/2013 23:29:44	
<input type="checkbox"/>	No 3.1.0.13	Image Upgrade	Not Recurrent	Failed	09/10/2013 23:29:16	
<input type="checkbox"/>	No 9500-3.1.0.14	Image Upgrade	Not Recurrent	Failed	09/10/2013 23:24:55	
<input type="checkbox"/>	No Quick Discover	Discovery	Not Recurrent	Succeeded	09/10/2013 23:22:50	

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

You can choose from the following columns: Enable, Job Name, Job Type, Recurrent Type, Status, Last Execution Time, Next Execution Time, Last Execution Status, Job End Time, Created By, and Create Time.

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

You can filter the current jobs by criteria such as job type, status, and last execution time.

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

7. Select a job.

8. Take one of the following actions:
 - Enable the job. Click the **Enable** button.
 - Disable the job. Click the **Disable** button.
 - Display job details. Click the **Detail** button.

Depending on your selection, a different Job Detail screen might display.

To close the Job Detail screen, click the **Close** button.

- Delete the job:
 - a. Click the **Delete** button.
 - A pop-up confirmation screen displays.
 - b. Click the **Yes** button.
 - The job is removed from the Jobs table and deleted.

11 Manage Users and Security Profiles

11

Manage the system users

You can manage security profiles, the user base, and online users.

This chapter covers the following topics:

- *Security Profile Concepts*
- *Add a Security Profile*
- *Modify or Remove a Security Profile*
- *Add a User Profile to the User Base*
- *Modify or Remove a User Profile*
- *View and Log Off Online Users*

Note: Only admin users (that is, users with a security profile that is set to Admin) can perform user management tasks.

Security Profile Concepts

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.

Add a Security Profile

If one of the default security profiles does not satisfy your needs, you can add a security profile and specify the tasks that are associated with the security profile. For most functions, you can specify whether the security profile includes viewing only, modifying only, or both viewing and modifying. You can specify the following tasks in a security profile:

- Monitoring
- Configuring
- Managing alarms
- Managing topologies
- Discovering
- Reporting
- Managing jobs
- Managing users and security profiles
- Performing administrative tasks

➤ To view the existing security profiles and add a security 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 18.

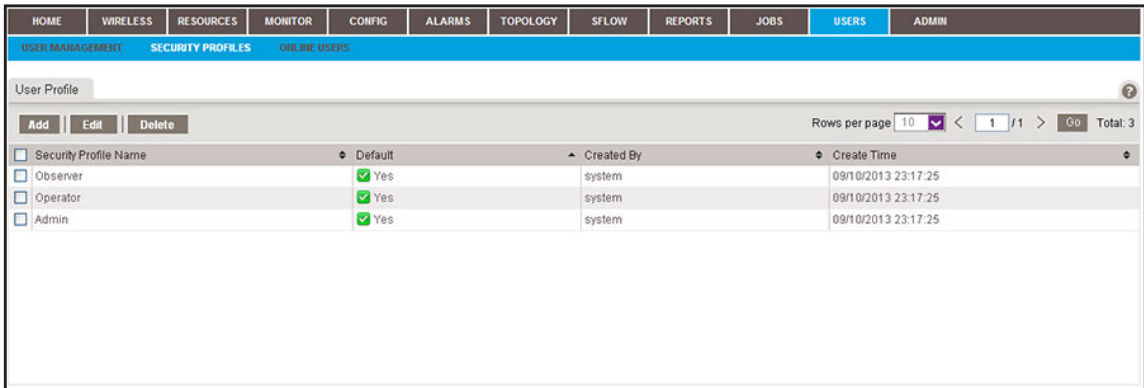
2. Enter your user name and password.

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

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

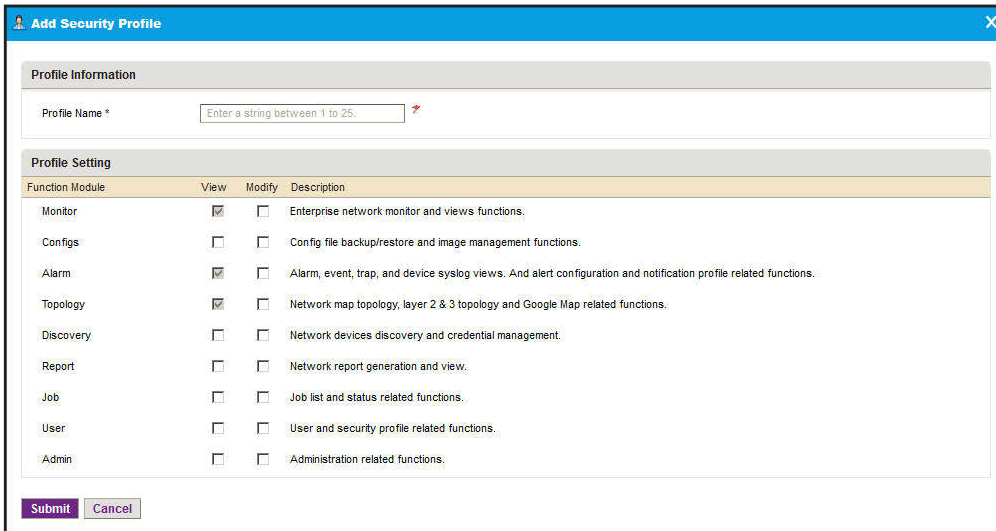
The Network Summary screen displays.

4. Select **USERS > SECURITY PROFILES**.



5. Click the **Add** button.

The Add Security profile screen displays.



6. In the **Profile Name** field, enter a name.

7. In the Profile settings section of the screen, select the check boxes for the functions that you want to include in the security profile.

8. Click the **Submit** button.

The security profile is saved and added to the User Profile table.

Modify or Remove a Security Profile

You can modify or remove a security profile. For a default security profile, you can change only the profile name. For a custom security profile, you can change the profile name and the tasks. You cannot remove a default security profile.

➤ **To modify or remove a security 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 18.

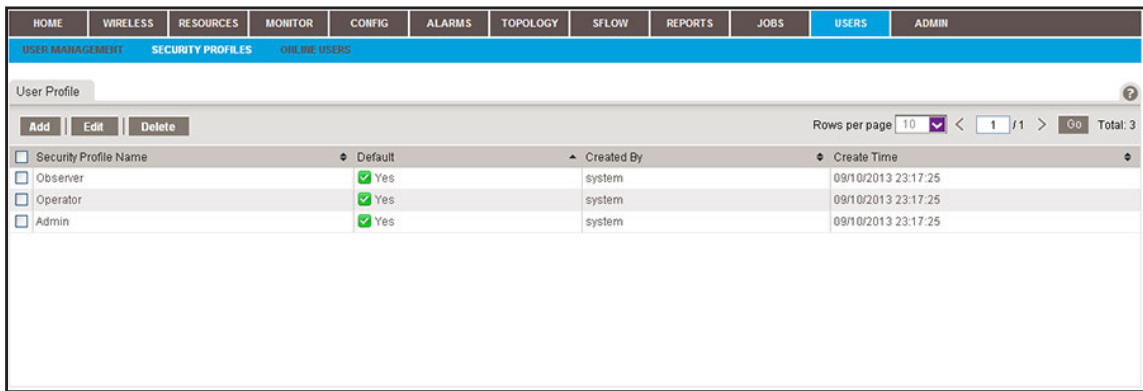
2. Enter your user name and password.

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.

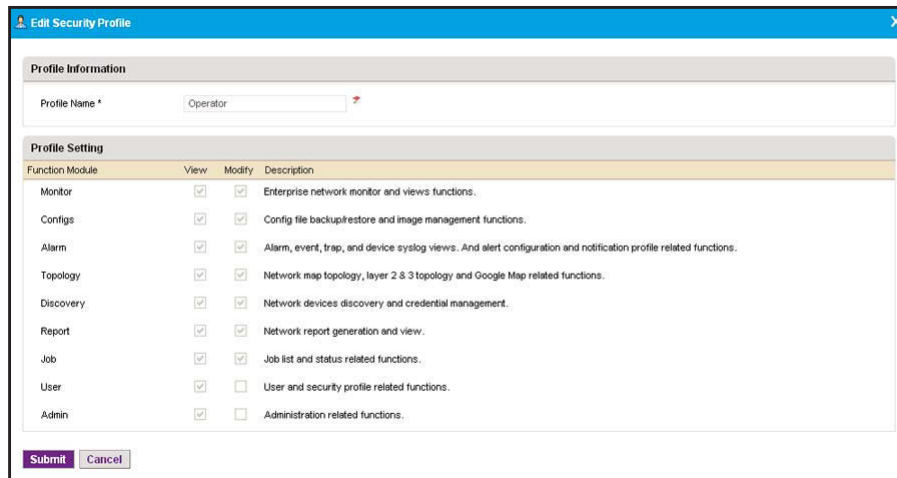
4. Select **USERS > SECURITY PROFILES**.



5. Select the security profile.
6. Take one of the following actions:
 - Modify the security profile:

- a. Click the **Edit** button.

The Edit Security Profile screen displays.



- b. (Optional) In the **Profile Name** field, modify the name.

- c. (Optional) In the Profile settings section of the screen, select the check boxes for the functions that you want to include in the security profile.

For a default security profile, you can change only the profile name.

- d. Click the **Submit** button.

The modified security profile is saved and added to the User Profile table.

- Remove the security profile:

- a. Click the **Delete** button.

You cannot remove a default security profile.

A pop-up confirmation screen displays.

- b. Click the **Yes** button.

The security profile is removed from the User Profile table and deleted.

Add a User Profile to the User Base

The application includes one default user profile, which is a user with the name admin to which an Admin security profile is assigned. You can add multiple user profiles to the user base.

➤ To view the existing user profiles and 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 18.

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 screenshot shows the 'User Management' section of the NMS300 application. At the top, there is a navigation bar with tabs for HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, **USERS**, and ADMIN. Below this, there are sub-tabs for USER MANAGEMENT, SECURITY PROFILES, and ONLINE USERS. The main content area is titled 'User Management' and contains a table with columns for Status, User Name, Security Profile, E-mail, Last Name, First Name, and Telephone. The table lists four users: 'admin' (Admin profile), 'JustLooking' (Observer profile), 'JustOperating' (Operator profile), and 'roland' (Admin profile). All users are marked as 'Active'.

Status	User Name	Security Profile	E-mail	Last Name	First Name	Telephone
<input type="checkbox"/> Active	admin	Admin	admin@email.com			
<input type="checkbox"/> Active	JustLooking	Observer	justlooking@email.com			
<input type="checkbox"/> Active	JustOperating	Operator	justoperating@email.com			
<input type="checkbox"/> Active	roland	Admin	roland@email.com			

The Status column displays whether the user is active and 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.

For more information about security profiles, see [Security Profile Concepts](#) on page 238.

7. Click the **Submit** button.

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

Modify or Remove a User Profile

You can modify or remove a user profile.

➤ To modify or remove 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 18.

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**.

Status	User Name	Security Profile	E-mail	Last Name	First Name	Telephone
Active	admin	Admin	admin@email.com			
Active	JustLooking	Observer	justlooking@email.com			
Active	JustOperating	Operator	justoperating@email.com			
Active	roland	Admin	roland@email.com			

5. Select the user profile.
6. Take one of the following actions:
 - Modify the user profile:
 - a. Click the **Edit** button.

The Edit User screen displays.

- a. (Optional) In the User Basic Information section, modify the user name, password, or email address for the user. The first and last name and telephone number are optional.
- b. In the User Status section, select whether the user profile is active and select the security profile that applies to the user.

For more information about security profiles, see [Security Profile Concepts](#) on page 238.

- c. Click the **Submit** button.

The modified user profile is saved and added to the User Management table.

- Remove the user profile:
 - a. Click the **Delete** button.

A pop-up confirmation screen displays.

 - b. Click the **Yes** button.

The user profile is removed from the User Management table and deleted.

View and Log Off Online Users

You can view the users who are currently logged in and log them off:

➤ **To view and log off (abort) users who are online:**

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 18.

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 > ONLINE USERS**.

Status	User Name	Security Profile	E-mail	Telephone	Login Time	Login IP
<input checked="" type="checkbox"/> Active	roland	Admin	roland@email.com		09/11/2013 09:49:57	192.168.10.4
<input checked="" type="checkbox"/> Active	JustLooking	Observer	justlooking@ema...		09/11/2013 09:51:07	127.0.0.1

5. To add columns to or remove them from the Online User 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, User Name, Security Profile, E-mail, Telephone, Login Time, Login IP, First Name, and Last Name.

6. Select one or more users.

To select all users, select the check box at the left in the table heading.

7. Click the **Abort** button.

A pop-up confirmation screen displays.

8. Click the **Yes** button.

The users are logged off.

12. Customize Global Settings

12

Customize select global system settings

You can change global settings from the administration dashboard. Except for the procedures that are described in this chapter, all procedures that you can perform from the System and Website Setting screen of the administration dashboard are described in the subject-specific chapters.

This chapter covers the following topics:

- *Set Up an External File Server*
- *Set the Data Retention Period*
- *Set the Inventory Polling*
- *Set the Idle Time-Out*
- *Set the Real-time Chart*
- *Change the Auto Refresh Setting*

Note: Only admin users (that is, users with a security profile that is set to Admin) can customize the global settings that are described in this chapter.

Set Up an External File Server

By default, the application uses an internal file server to save and retrieve configuration files. If you set up an external file server, you can import and export configuration files (see *Import and Export Configuration Files to an External File Server* on page 145).

Even if you set up an external files server, all file transfers are still handled by the NMS300 server, that is, the external file server is for file storage only.

➤ To set up an external file 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 18.

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**.

The screenshot shows the 'ADMIN > SETTINGS' page. The top navigation bar includes: HOME, WIRELESS, RESOURCES, MONITOR, CONFIG, ALARMS, TOPOLOGY, SFLOW, REPORTS, JOBS, USERS, and ADMIN. Below the navigation bar, there are sub-sections: SETTINGS, AUDIT LOG, and LICENSE MANAGEMENT. The main content area is titled 'System and Website Settings' and contains several cards:

- Getting Started with NMS**: Discover your network and add the devices you want to manage. Links: Discover Devices, SMTP Email Settings, SMS Server Settings, Device Groups.
- System Settings**: Set global settings for the system and website. Links: Data Retention Period, Inventory Polling, Idle Time Out, Real-time Chart.
- Customize**: Customize the navigation and look of your web portal. Links: Customize Network Summary View, Customize Wireless Summary, Customize Alarm Color, Auto Refresh Setting, Customize Network Dashboard.
- Account Information**: View or modify users, or create new users. Links: User Management, Edit Account, Change Password.
- Manage Monitor and Alarm**: Network monitor, alarm and threshold related configurations. Links: Alarm Configuration, Monitor Configuration.
- my.NETGEAR.com Account Profile**: Configure and validate my.NETGEAR.com account profile through my.NETGEAR.com Web API. Link: my.NETGEAR.com Account Profile.
- sFlow**: Set sFlow related configurations. Links: sFlow Settings, Manage sFlow Source.
- Manage External File Server**: External File Server configurations and File Processing with External File Server. Link: **External File Server Settings** (circled in red), Import or Export Config Files.
- License And Version Information**: View NMS300 license, supported device and version information. Links: License Management, NMS300 Version.

5. Under Manage External File Server, click the **External File Server Setting** link.

The External File Server Setting screen displays.

- From the **File Server Type** menu, select **External File Server**.

The screen adjusts.

- Specify the server settings:

- **External Server IP.** Enter the IP address of the external file server.
- **Directory Path.** Enter the directory path where the configuration files are stored.

You must enter the directory path for the external file server in the xxx/xxx format, in which the delimiting character is a slash (for example, backup/NMS300).

- **User Name.** Enter the user name to access the external file server.
- **Password.** Enter the password to access the external file server.

- Click the **Test** button.

Access to the external file server is verified.

- Click the **Submit** button.

Your changes are saved.

Set the Data Retention Period

You can change how long the application retains your network data. The longer information is retained, the more disk space is required on the NMS300 server. You can monitor the NMS300 server information (see [View the NMS300 Server Information](#) on page 107).

➤ To modify the data retention period:

- 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 18.

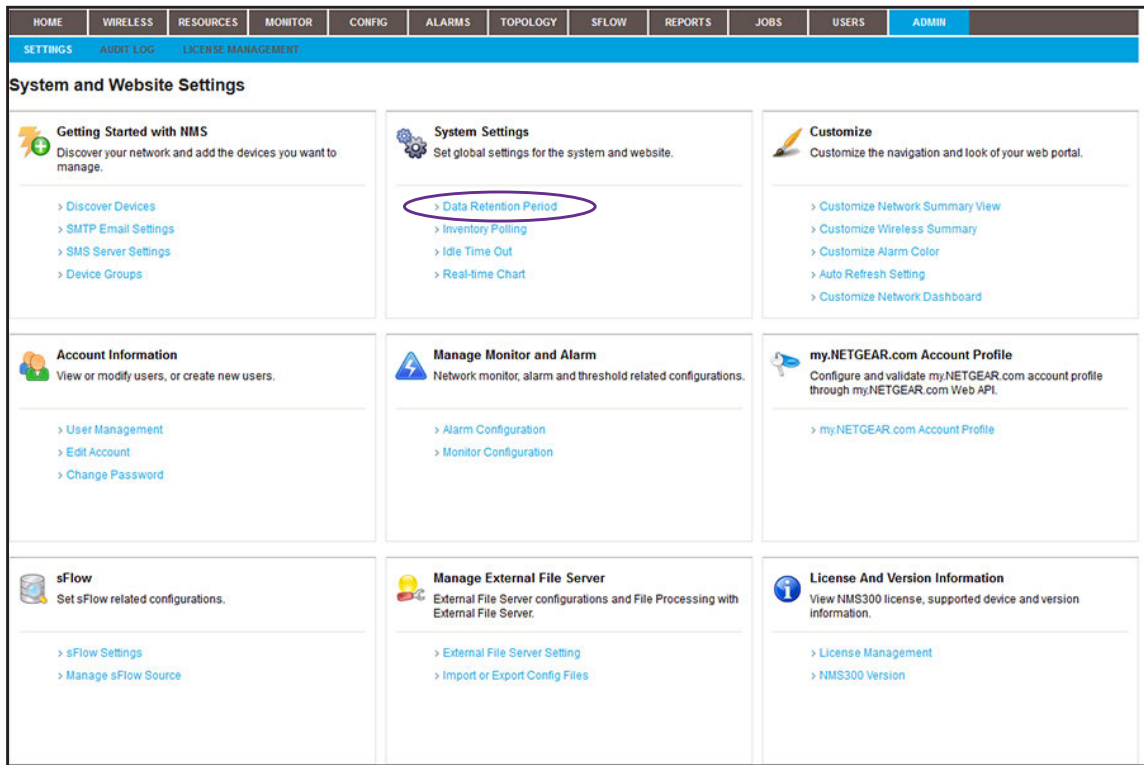
- Enter your user name and password.

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

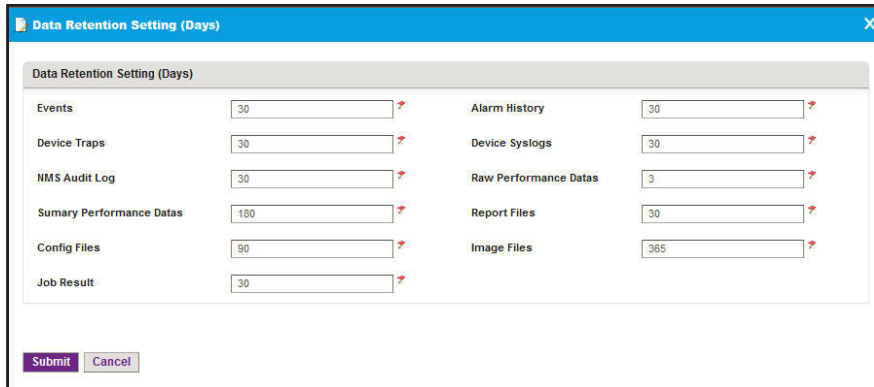
- Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under System Settings, click the **Data Retention Period** link.



6. For the data retention periods that you want to change, enter the updated information:

- **Events.** This setting determines how long events are retained. The default period is 30 days. For more information, see *View and Manage Network Event Notifications* on page 176.
- **Device Traps.** This setting determines how long trap data is retained. The default period is 30 days. For more information, see *View and Manage Device Traps* on page 177.

- **NMS Audit Log.** This setting determines how long audit logs are retained. The default period is 30 days. For more information, see [View and Export Audit Logs](#) on page 105.
 - **Summary Performance Data.** This setting determines how long summary performance data is retained. The default period is 180 days. For more information, see [Customize the Optional Network Dashboard](#) on page 97.
 - **Configuration Files.** This setting determines how long backed-up configuration files are retained. The default period is 90 days. For more information, see [Back Up Your Device Configurations](#) on page 112.
 - **Job Result.** This setting determines how long job execution reports are retained. For more information, see [View and Manage Jobs](#) on page 234.
 - **Alarm History.** This setting determines how long alarms are retained. The default period is 30 days. For more information, see [View and Manage the Alarm History](#) on page 161.
 - **Device Syslogs.** This setting determines how long syslogs are retained. The default period is 30 days. For more information, see [View and Manage Device System Logs](#) on page 179.
 - **Raw Performance Data.** This setting determines how long raw performance data is retained. The default period is 3 days. For more information, see [Manage the Configuration Monitors](#) on page 92.
 - **Report Files.** This setting determines how long job reports are retained. The default period is 30 days. For more information, see [View and Remove Saved Reports](#) on page 230.
 - **Image Files.** This setting determines how long device firmware files are retained. The default period is 365 days. For more information, see [Upgrade Firmware for One or More Devices](#) on page 148.
7. Click the **Submit** button.
- Your changes are saved.

Set the Inventory Polling

You can change how often the application polls the network for your device inventory.

➤ To modify the inventory polling:

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 18.

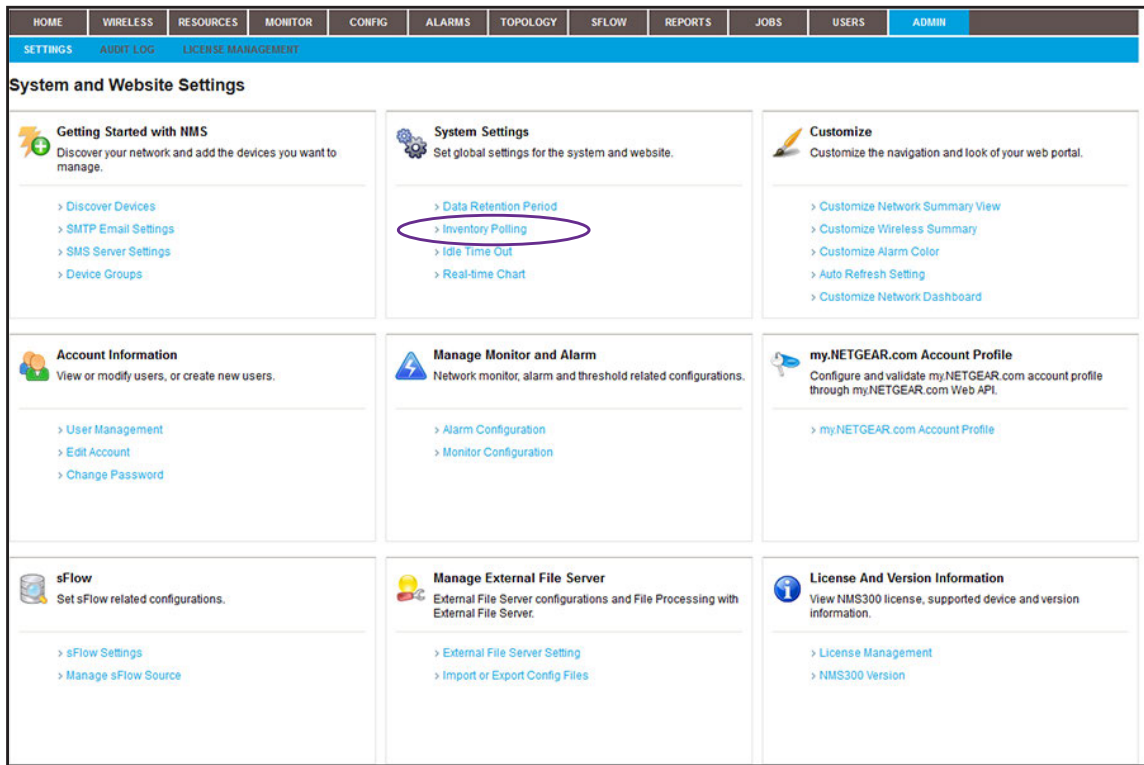
2. Enter your user name and password.

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

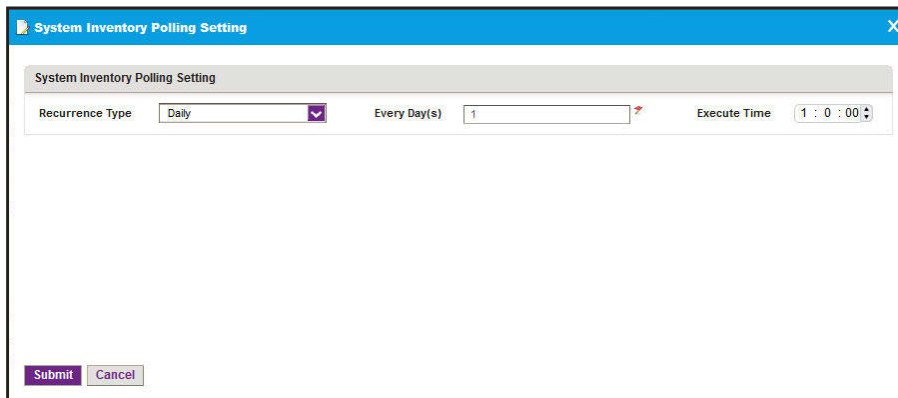
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under System Settings, click the **Inventory Polling** link.



6. Specify the recurrence type and execution time.

If you select **Hourly** from the **Recurrence Type** menu, the screen adjusts.

7. Click the **Submit** button.

Your changes are saved.

Set the Idle Time-Out

You can change how long the application waits before it logs you out for inactivity. The default period is 30 minutes.

➤ **To modify the idle time-out:**

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 18.

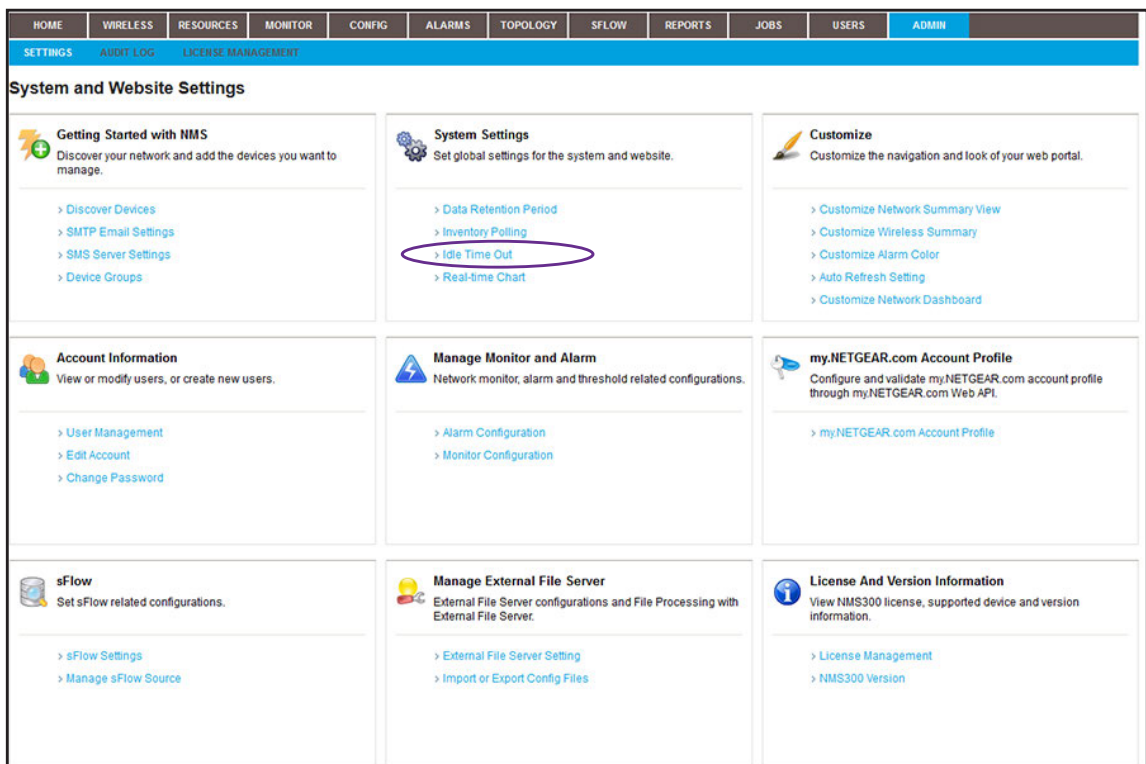
2. Enter your user name and password.

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

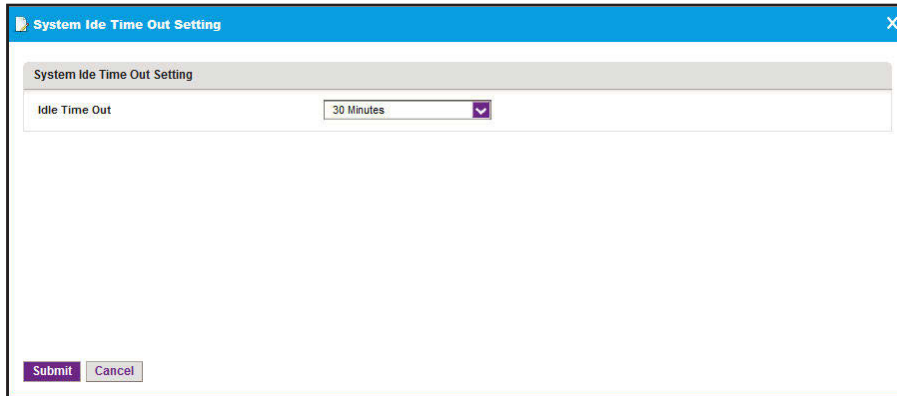
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under System Settings, click the **Idle Time Out** link.



The screenshot shows a dialog box titled "System Idle Time Out Setting". Inside the dialog, there is a label "System Idle Time Out Setting" and a form field "Idle Time Out" with a dropdown menu showing "30 Minutes". At the bottom of the dialog, there are "Submit" and "Cancel" buttons.

6. Specify the new idle time-out period.
7. Click the **Submit** button.

Your changes are saved.

Set the Real-time Chart

You can change how often the application refreshes your chart data and the maximum time range that is displayed on your charts. By default, the data refresh interval is 10 seconds and the maximum time range is 5 minutes.

➤ To modify the chart settings:

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 18.

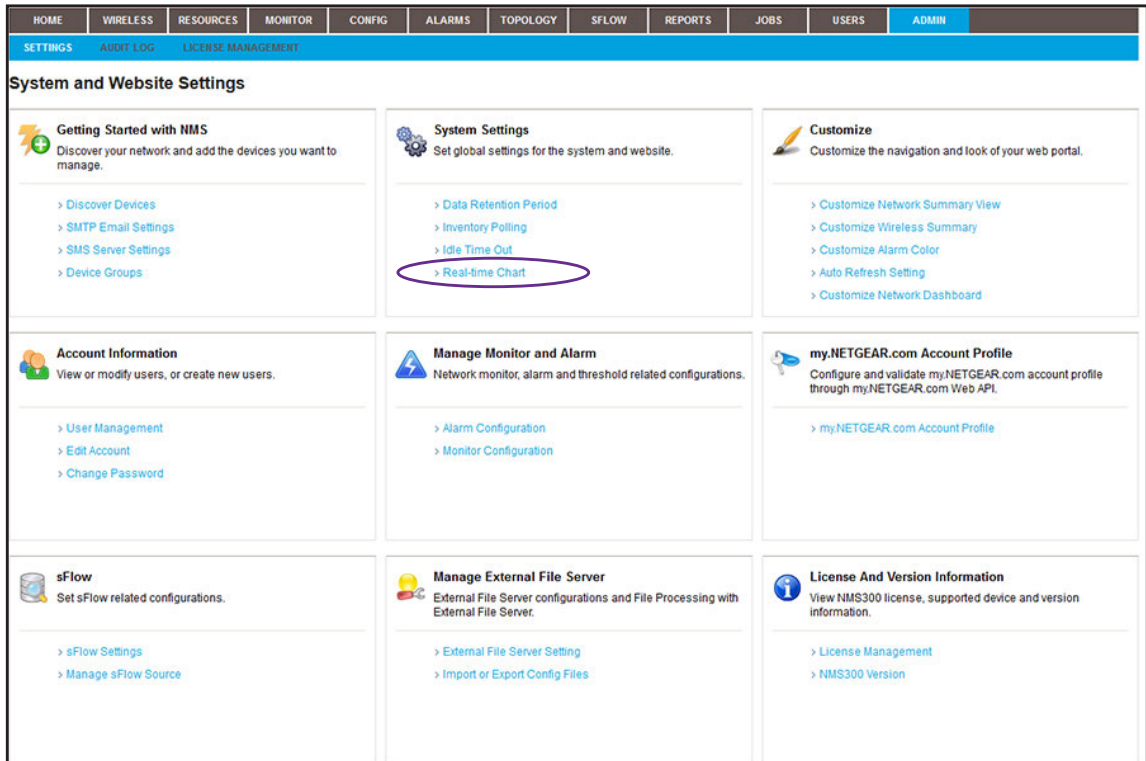
2. Enter your user name and password.

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

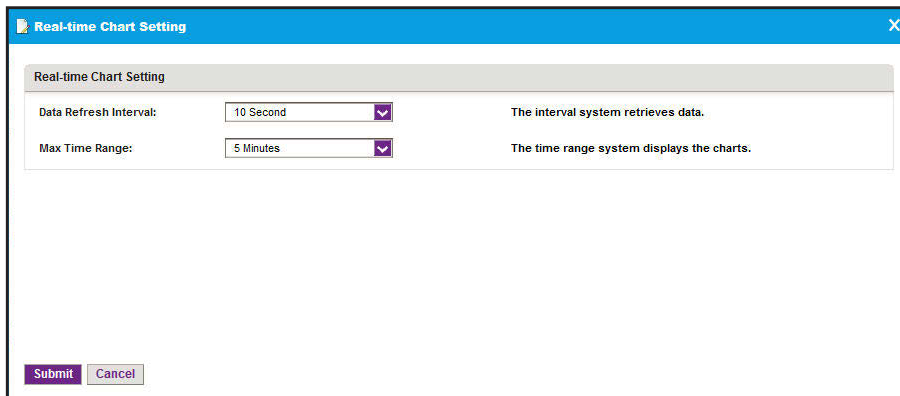
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under System Settings, click the **Real-time Chart** link.



6. Specify the data refresh interval and maximum time range.

7. Click the **Submit** button.

Your changes are saved.

Change the Auto Refresh Setting

You can change how often the application refreshes the browser screen for the web management interface. By default, the screen refresh interval is one minute.

➤ **To modify the auto refresh setting:**

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 18.

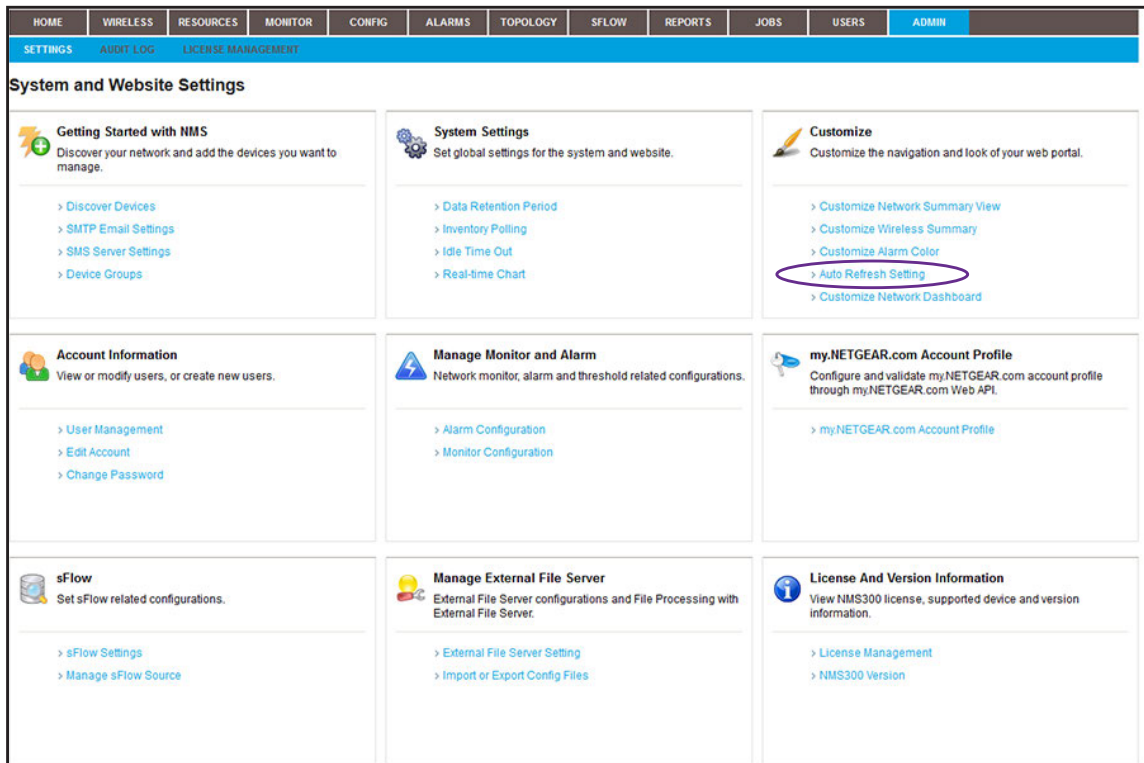
2. Enter your user name and password.

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

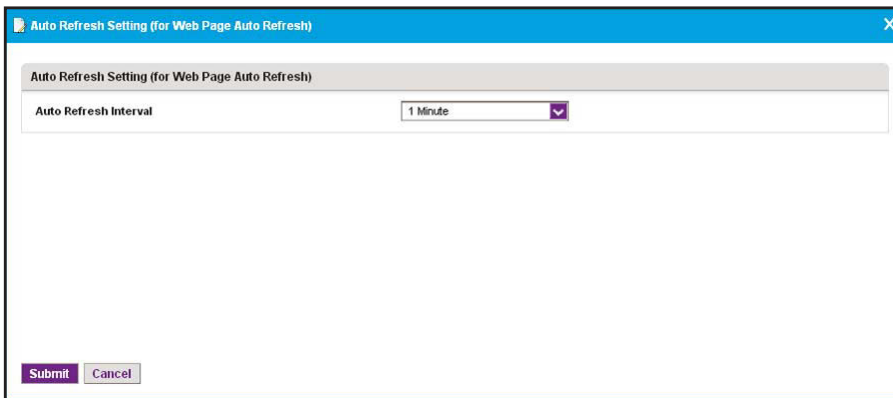
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under Customize, click the **Auto Refresh Setting** link.



The screenshot shows a dialog box titled "Auto Refresh Setting (for Web Page Auto Refresh)". The dialog contains a single configuration item: "Auto Refresh Interval" with a dropdown menu set to "1 Minute". At the bottom left of the dialog, there are two buttons: "Submit" and "Cancel".

6. Specify the new auto refresh interval.
 7. Click the **Submit** button.
- Your changes are saved.

13. Manage Licenses

13

Manage the system licenses

You can view license information, add a license, and deregister a license.

This chapter covers the following topics:

- *View License Information*
- *Register a License*
- *Deregister a License*

Note: Only admin users (that is, users with a security profile that is set to Admin) can perform license management tasks.

View License Information

The default license that comes with the application supports up to 200 devices. Each device that the application discovers and adds to its device inventory is subtracted from the balance of 200 devices. However, controller-managed APs are not subtracted from the balance.

For information about managing more than 200 devices, contact your NETGEAR sales contact.

➤ To view license 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 18.

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 > LICENSE MANAGEMENT**.

License Name	Device Count	Expiration Time	Key	Registered
NMS300 Default License	200	Never	DEFAULT	Yes

The Device Count section of the screen displays the maximum number of allowed devices with the current license or licenses and the number of devices that the application manages.

5. To add columns to or remove them from the License 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: License Name, Device Count, Expiration Time, Key, Registered, Created By, and Created Time.

Register a License

To register a license, you need a license key, and the NMS300 server must be connected to the Internet to connect to a NETGEAR license server.

➤ **To register a license:**

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 18.

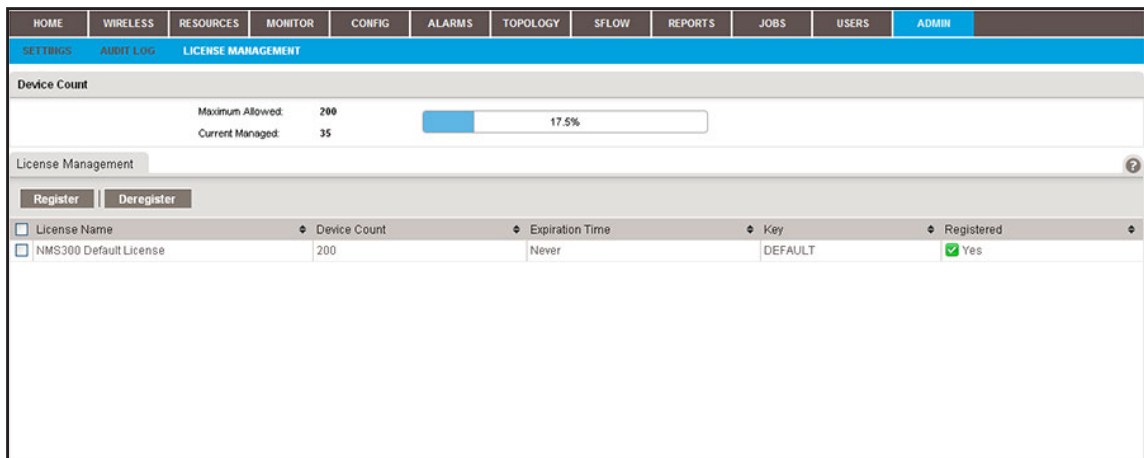
2. Enter your user name and password.

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

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

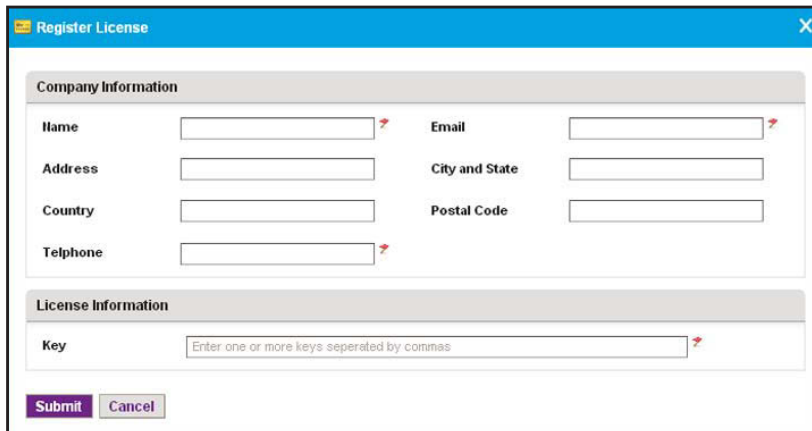
The Network Summary screen displays.

4. Select **ADMIN > LICENSE MANAGEMENT**.



5. Select the license.

6. Click the **Register** button.



7. In the Company Information section, enter your information.

You must enter information in the **Name**, **Email**, and **Telephone** fields.

8. In the License Information section, enter the license key in the **Key** field.

You must enter a single license key.

9. Click the **Submit** button.

The license is registered with a NETGEAR license server. After successful registration, the license is added to the License Registration table. The license is tied to the MAC address of the NMS300 server.

Deregister a License

You can deregister a license on one NMS300 server, transfer it to another NMS300 server, and reregister the license on the new NMS300 server. You cannot deregister the default license.

After you deregister a license, if the number of allowed devices falls below the number of managed devices, the application displays a wizard. To bring the number of managed devices within the limit of the number of allowed devices, the wizard lets you select devices from the currently managed list that you can delete from the application.

To deregister a license, the NMS300 server must be connected to the Internet to connect to a NETGEAR license server.

➤ To deregister a license:

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 18.

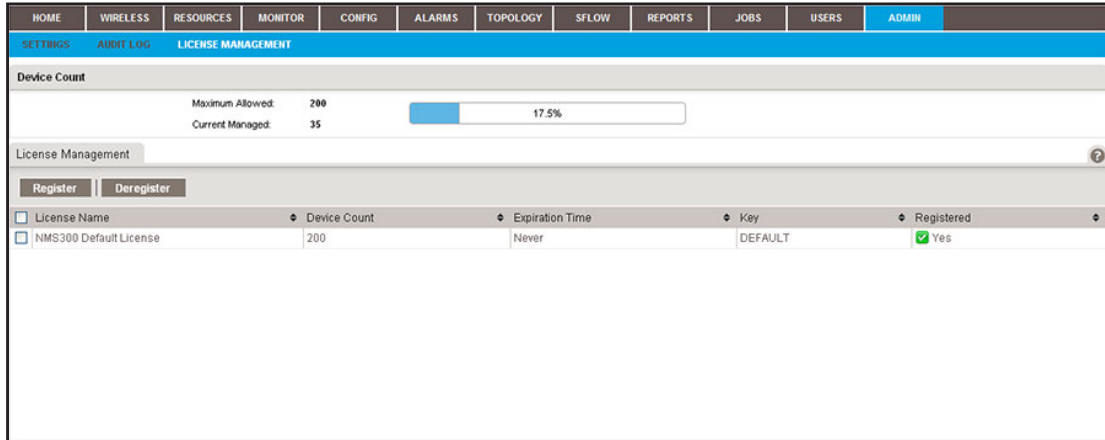
2. Enter your user name and password.

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.

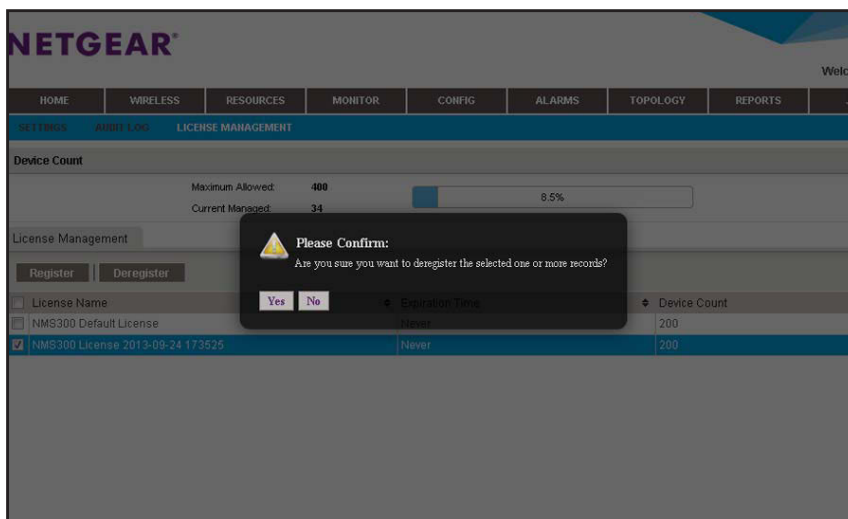
4. Select **ADMIN > LICENSE MANAGEMENT**.



5. Select the license.

6. Click the **Deregister** button.

A pop-up confirmation screen displays.



7. Click the **Yes** button.

The license is removed from the License Management table and deregistered.

14. Register Devices

14

Manage the registration of devices

You can view registration information, register one or more devices, and resynchronize your device registration status.

This chapter covers the following topics:

- *Registration Concepts*
- *Set Up and Validate Your Account Profile in the Application*
- *Register One or More Devices*
- *Register All Devices*
- *Resynchronize Previously Registered Devices*

Note: Only admin users (that is, users with a security profile that is set to Admin) and operators (that is, users with a security profile that is set to Operator) can perform registration tasks.

Registration Concepts

Before you can use the registration tool that the application provides, you must create a customer account at the NETGEAR product registration website. After you create a customer account, you must set up the account profile in the application. For more information, see *Set Up and Validate Your Account Profile in the Application* on page 262.

The registration tool lets you register one, several, or all devices that the application manages. Registration occurs with the NETGEAR registration server. For more information, see *Register One or More Devices* on page 265 and *Register All Devices* on page 268.

If you already registered your devices, either through the NETGEAR registration website or through the application, and you install or reinstall the application, you can resynchronize the previously registered devices. For more information, see *Resynchronize Previously Registered Devices* on page 270.

Set Up and Validate Your Account Profile in the Application

If you do not yet own a customer account to register devices, create a customer account at the NETGEAR product registration website. For more information, visit <https://my.netgear.com/registration/login.aspx>.

Set Up Your Account Profile for Device Registration

If you own a customer account, enter your account email address and password in the application to create an account profile. This account profile enables you to register and resynchronize devices through the application.

➤ **To set up your account profile for device registration:**

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 18.

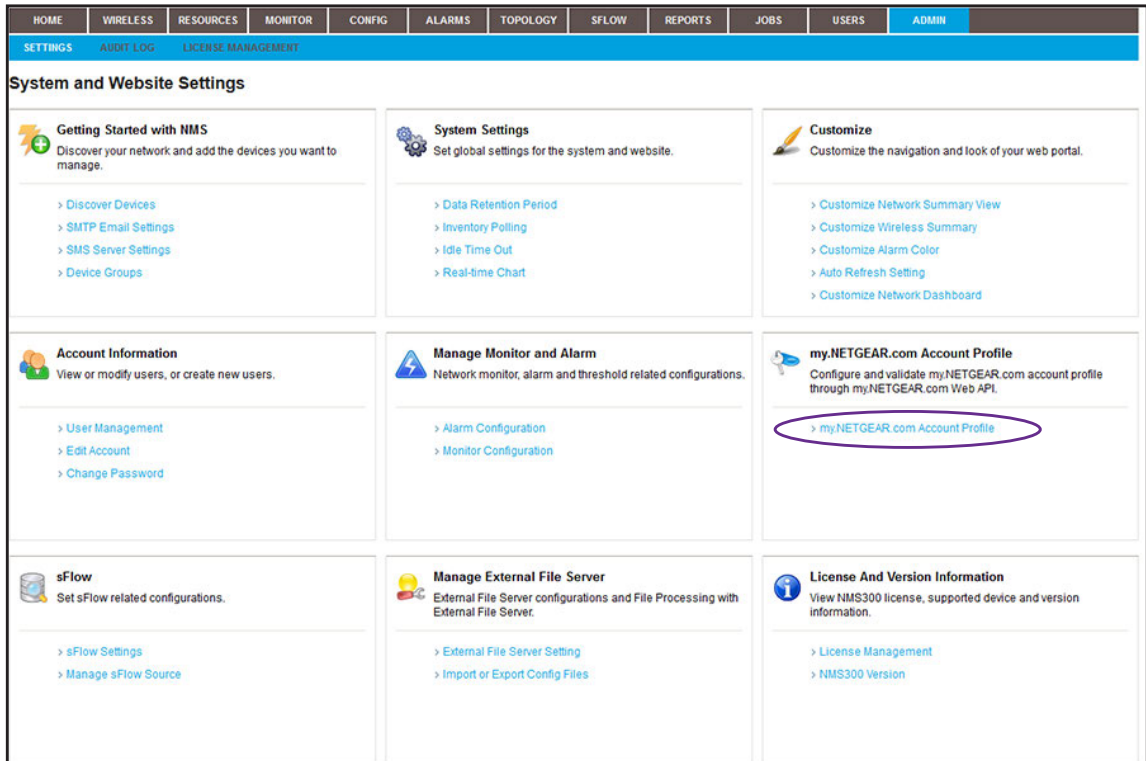
2. Enter your user name and password.

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

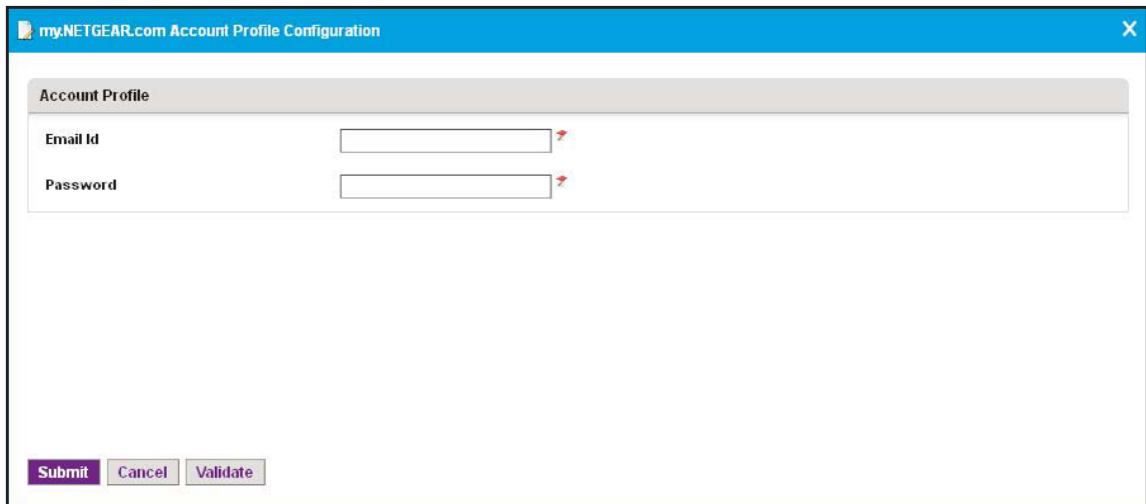
3. Click the **Sign In** button.

The Network Summary screen displays.

4. Select **ADMIN > SETTINGS**.



5. Under my.NETGEAR.com Account Profile, click the **my.NETGEAR.com Account Profile** link.



6. Configure the account profile:
- In the **Email Id** field, enter the email address that corresponds to your NETGEAR customer account.
 - In the **Password** field, enter the password that corresponds to your NETGEAR customer account.

7. Click the **Submit** button.

The application connects to the NETGEAR registration server to verify the validity of the email address and password. A pop-up screen informs you whether the operation was successful.

Validate and Retrieve Your Customer Account Information

If you own a customer account, you can retrieve your account information in the application.

➤ **To validate and retrieve your customer 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 18.

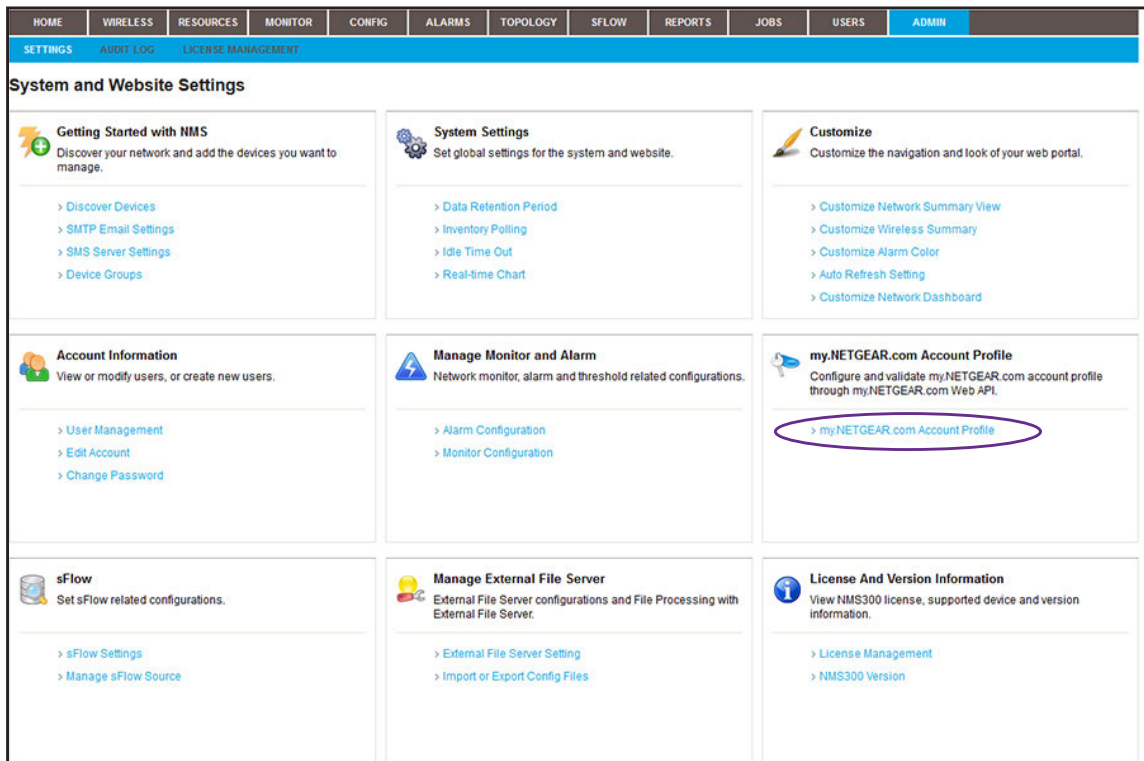
2. Enter your user name and password.

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**.

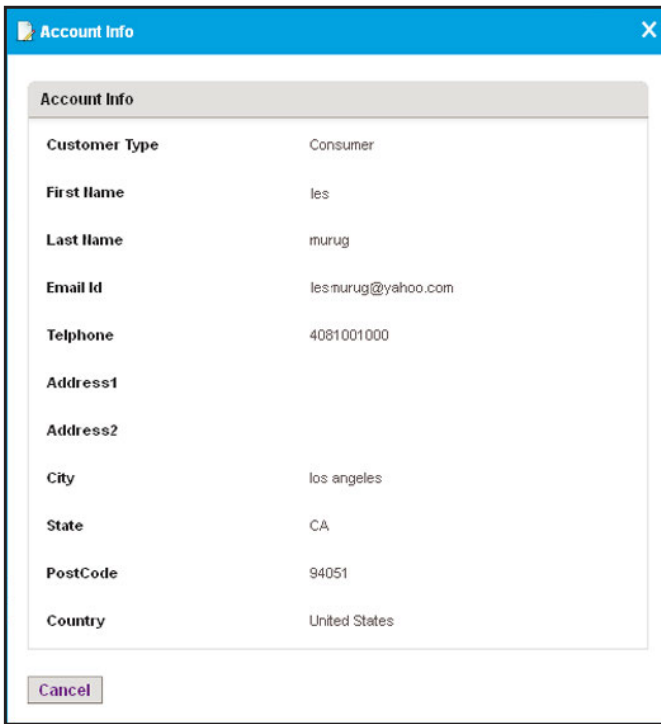


5. Under my.NETGEAR.com Account Profile, click the **my.NETGEAR.com Account Profile** link.

The my.NETGEAR.com Account Profile screen displays.

- Click the **Validate** button.

The application connects to the NETGEAR registration server to retrieve the customer account information.



The screenshot shows a dialog box titled "Account Info" with a close button (X) in the top right corner. Inside the dialog, there is a table with the following information:

Account Info	
Customer Type	Consumer
First Name	les
Last Name	murug
Email Id	les.murug@yahoo.com
Telephone	4081001000
Address1	
Address2	
City	los angeles
State	CA
PostCode	94051
Country	United States

At the bottom left of the dialog box, there is a "Cancel" button.

- Click the **Cancel** button.

The Account Info screen closes.

- Click the **Cancel** button.

The my.NETGEAR.com Account Profile screen closes.

- To change any account information, visit <https://my.netgear.com/registration/login.aspx>.

Register One or More Devices

You can register a single device or a selection of devices. However, the application cannot register NETGEAR devices that do not report their serial number to the application. If the Devices table does not list a serial number in the Serial Number column for a device, the device does not report its serial number to the application.

➤ To register one or more devices:

- 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 18.

- Enter your user name and password.

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

- Click the **Sign In** button.

The Network Summary screen displays.

- Select **RESOURCES > DEVICES**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74:44:01:90:f4:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c8:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

The screen displays the devices that the application discovered.

- 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.

- 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.

- Select one or more devices.

- From the **More** menu, select **Register Device**.

Device Registration

Purchase Info > Result

Select one or more devices in the table below. Populate the appropriate value for Date of Purchase and Country of Purchase for the selected devices by entering in the fields below and clicking on Apply. Once these are populated for all selected devices, then click on Execute.

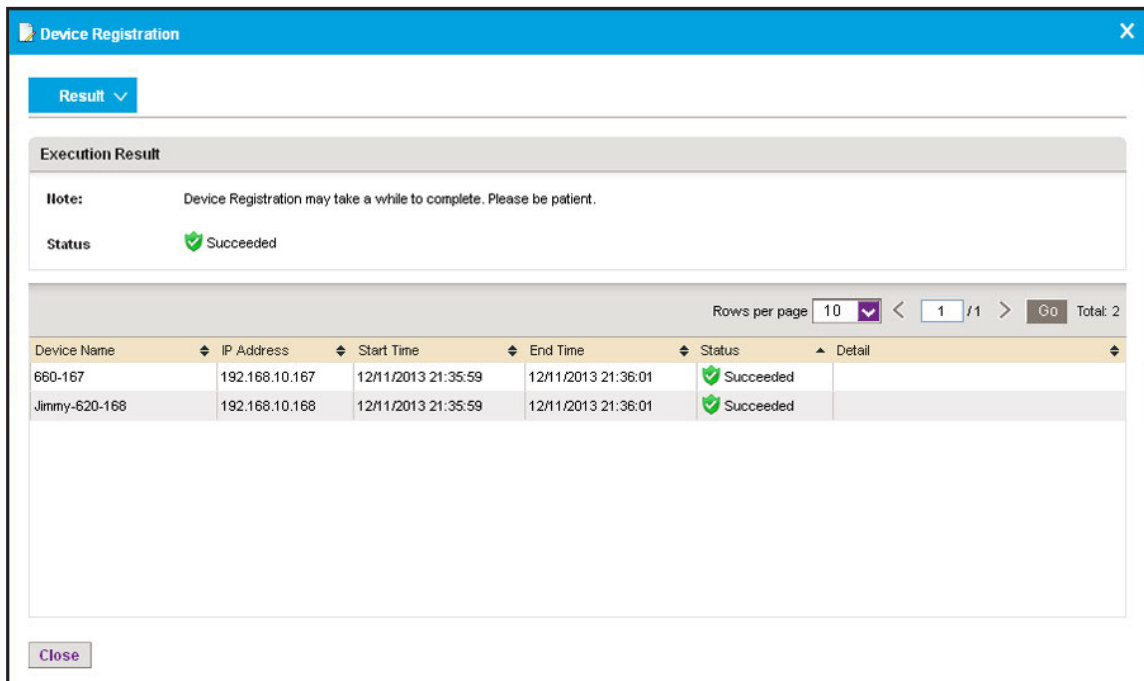
Date of Purchase: 12/13/2013

Country of Purchase: Argentina

<input checked="" type="checkbox"/>	Device Name	Device Type	IP Address	Serial Number	Date of Purchase	Country of Purchase
<input checked="" type="checkbox"/>	660-167	Standalone AP	192.168.10.167	2XX129NA00067		United States
<input checked="" type="checkbox"/>	Jimmy-620-168	Standalone AP	192.168.10.168	2XP128NA00037		United States

- In the **Date of Purchase** field, enter the date of purchase, and click the **Apply** button.
 - In the **Country of Purchase** field, enter the country of purchase, and click the **Apply** button.
The date of purchase is applied to all selected devices.
- By default, the application lists the country that you entered when you created your customer account at the NETGEAR product registration website. You can change the country of purchase, which is applied to all selected devices.
- Click the **Execute** button.

The application contacts the NETGEAR registration server. The Result screen displays whether the registration is successful.



Note: A serial number must be unique for a device registration to be successful.

12. Click the **Close** button.

The screen closes.

Register All Devices

You can register all devices simultaneously. You can also clear selected devices so they are not registered. The application cannot register NETGEAR devices that do not report their serial number to the application. If the Devices table does not list a serial number in the Serial Number column for a device, the device does not report its serial number to the application.

➤ To register all devices simultaneously:

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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mine	192.168.10.230	74.44.01.90fd.72		IP Address	shanghai CN	Switch	OSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f9e:95:37		IP Address		Switch	OSM7328Sv2
Up	192.168.10.114	192.168.10.114	20:4e:7f91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-28G3
Up	192.168.10.125	192.168.10.125	c0:3f0e:7fcb:c5		IP Address	beijing	Switch	OSM7249v2
Up	192.168.10.201	192.168.10.201	10:0d:7fb3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	OS724TV3
Up	192.168.10.217	192.168.10.217	20:4e:7f7b:d7:9a		IP Address	Jun6-location-217	Switch	OSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:d4:0e		IP Address		Switch	OS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	OSM7252PS

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.

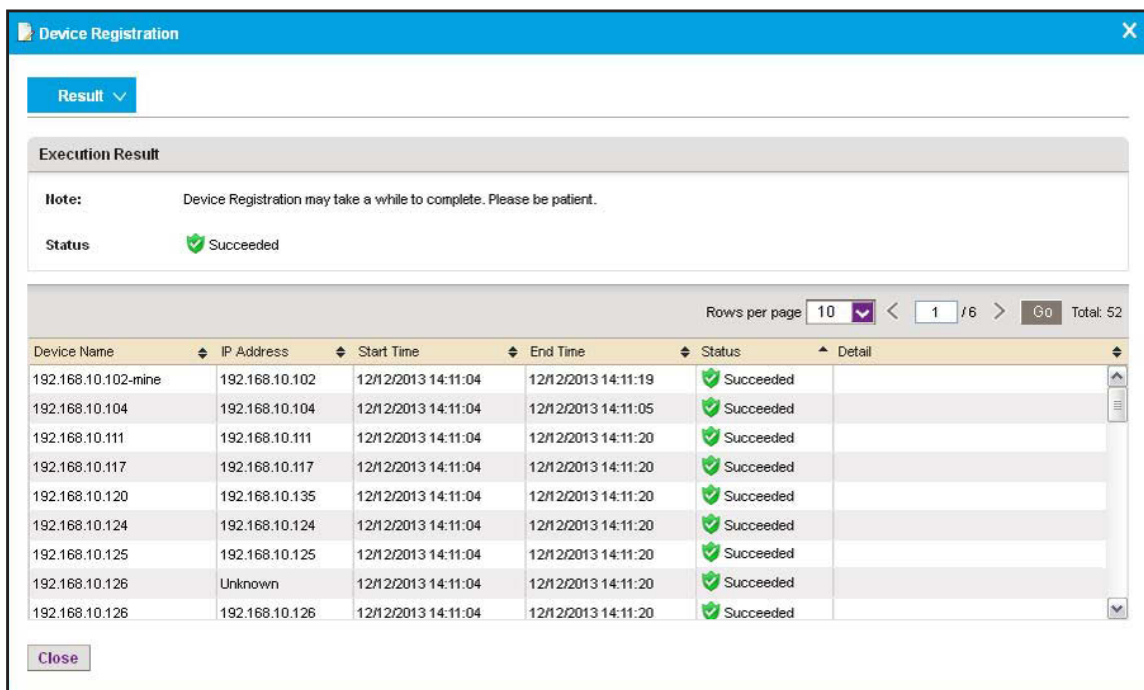
To hide the filter, click the **Hide Filter** button.

7. From the **More** menu, select **Register All Devices**.

Device Name	Device Type	IP Address	Serial Number	Date of Purchase	Country of Purchase
res-d5-09-da	Storage	192.168.10.128	3JUI350D00A67		United States
vms-41	VMS	192.168.10.41			United States
July17-660-163	Standalone AP	192.168.10.163	2XX12ANJ0018E		United States
netgearA623F8	Standalone AP	192.168.10.150			United States
Jimmy-620-168	Standalone AP	192.168.10.168	2XP128NA00037		United States
netgearD2D228	Standalone AP	192.168.10.133	2GY2245W002B7		United States
660-167	Standalone AP	192.168.10.167	2XX129NA00067		United States
350-157	Standalone AP	192.168.10.157	2921075E00104		United States
192.168.10.104	Switch	192.168.10.104			United States
192.168.10.70	Switch	192.168.10.70	2XN12459F0029		United States
192.168.10.62	Switch	192.168.10.62	2JE11B52F002D		United States

8. If you want to exclude some devices, clear the associated check boxes.
9. In the **Date of Purchase** field, enter the date of purchase, and click the **Apply** button.
The date of purchase is applied to all selected devices.
10. In the **Country of Purchase** field, enter the country of purchase, and click the **Apply** button.
By default, the application lists the country that you entered when you created your customer account at the NETGEAR product registration website. You can change the country of purchase, which is applied to all selected devices.
11. Click the **Execute** button.

The application contacts the NETGEAR registration server. The Result screen displays whether the registration is successful.



Note: A serial number must be unique for a device registration to be successful.

12. Click the **Close** button.
The screen closes.

Resynchronize Previously Registered Devices

The application lets you resynchronize previously registered devices. This capability is useful in the following situations:

- You already registered your devices directly at the NETGEAR product registration website and you install the application for the first time or upgrade the application to a version that supports device registration.

After you resynchronized the previously registered devices with the NETGEAR registration server, the application displays which devices are already registered and which devices still require registration.

- You already registered your devices through the application and you remove and reinstall the application. In such a situation, the registration information is deleted from the local database of the application.

After you resynchronized the previously registered devices with the NETGEAR registration server, the registration information in the local database of the application is restored.

➤ **To resynchronize previously registered devices:**

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 18.

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**.

Status	Device Name	IP Address	MAC Address	Hostname	Managed By	Location	Device Type	Device Model
Up	192.168.10.102-mime	192.168.10.230	74:44:01:90:fd:72		IP Address	shanghai CN	Switch	GSM7224v2
Up	192.168.10.104	192.168.10.104	00:22:3f:9e:95:37		IP Address		Switch	GSM7328SV2
Up	192.168.10.114	192.168.10.114	20:4e:7f:91:5b:c6		IP Address	san jose	Switch	GS728TPS
Up	192.168.10.120	192.168.10.120	4c:60:de:db:77:68		IP Address	san jose	Switch	M5300-2803
Up	192.168.10.125	192.168.10.125	c0:3f:0e:7f:cb:c5		IP Address	beijing	Switch	GSM7248v2
Up	192.168.10.201	192.168.10.201	10:0d:7f:b3:06:08		IP Address		Switch	GS748TPS
Up	192.168.10.216	192.168.10.216	28:c6:8e:01:9b:2b		IP Address		Switch	GS724Tv3
Up	192.168.10.217	192.168.10.217	20:4e:7f:7b:d7:9a		IP Address	Jun6-location-217	Switch	GSM7212F
Up	192.168.10.226	192.168.10.226	00:8e:f2:5a:da:0e		IP Address		Switch	GS752TXS
Up	192.168.10.237	192.168.10.237	30:46:9a:1b:b2:b7		IP Address		Switch	GSM7252PS

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. From the **More** menu, select **Resync Registration**.

A pop-up screen informs you whether the operation was successful.

Technical Specifications



Hardware and software requirements

Table 4. Hardware and software requirements

Item	Specification
System architecture	<ul style="list-style-type: none">• B/S-based multitiered system
Browser support (HTTP and HTTPS)	<ul style="list-style-type: none">• Internet Explorer 9 or 10• Firefox 20.0.1• Chrome 26.0.1410.64 m
OS support	<ul style="list-style-type: none">• 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
VM support	<ul style="list-style-type: none">• Support hypervisors include VMWare and other major ones such as Hyper-V and XenServer
Standard server requirement (for 200 devices)	<ul style="list-style-type: none">• 2.8 GHz dual-core CPU• 4 G RAM (32-bit OS) or 8 G RAM (64-bit OS)• 20 G HD (free space)• Static IP
Standard client requirement	<ul style="list-style-type: none">• 2 GHz CPU• 2 G RAM• 3 G HD (free space)
Installation	<ul style="list-style-type: none">• Server is installed through an automated GUI-based installer• Single server deployment• Client is web-based and no installation is required
Language support	<ul style="list-style-type: none">• English• Chinese

Table 4. Hardware and software requirements (continued)

Item	Specification
Management interface support	<ul style="list-style-type: none">• SNMP (v1, v2c, v3)• TFTP• Telnet/HTTP/HTTPS• Web management interface
Supported devices	See <i>Compatible Devices</i> on page 12
DB	MySQL (v5.5)










B Device Details

B

Device details that you can display

You can view many details for a device and its interfaces. For information about how to view details, see [View Device Details and Interface Details](#).

The detailed information that the application can provide depends on the type of device. The Devices table can list the following devices in the Device Type column:

-  **Switch.** For information about the available details, see [Switch Details](#) on page 275 and [Interface Details](#) on page 283.
-  **Firewall.** For information about the available details, see [Firewall Details](#) on page 276.
-  **Standalone AP.** For information about the available details, see [Standalone AP Details](#) on page 277.
-  **Controller-Managed AP.** For information about the available details, see [Controller-Managed AP Details](#) on page 278.
-  **Wireless Controller.** For information about the available details, see [Wireless Controller Details](#) on page 279 and [Interface Details](#) on page 283.
-  **WMS.** For information about the available details for a wireless management system, see [Wireless Managements System Details](#) on page 280.
-  **Storage.** For information about the available details for a storage system, see [Storage System Details](#) on page 281.
-  **Router.** For information about the available details, see [Router Details](#) on page 282 and [Interface Details](#) on page 283.
-  **Unknown.** For information about the available details for an unknown device, see [Unknown Device Details](#) on page 283.

Switch Details

The following table lists the dashboard options and widgets or tables that are available for a switch.

Table 5. Detailed information available for a switch

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Average CPU and Memory Utilization (Today)
	Inventory Information
	Min/Max/Average Response Time
	Latest 10 Alarms
	CPU
	Top 10 Interface by Traffic (Today)
	Memory
	Latest 10 Config Backups
Interface List	Slot List Note: Supported for M6100 managed switches only.
Slot List	Interface List Note: For more information, see Table 14 on page 283.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Bandwidth Monitor	Received Bytes Real-time Chart
	Transmitted Bytes Real-time Chart
	Selected interfaces
Config Files	Config File Backup List
Credential	Authentication Association

Firewall Details

The following table lists the dashboard options and widgets or tables that are available for a firewall.

Table 6. Detailed information available for a firewall

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Latest 10 Alarms
	Top 10 Interface by Traffic (Today)
	Latest 10 Config Backups
Interface List	Interface List Note: For more information, see Table 14 on page 283.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Bandwidth Monitor	Received Bytes Real-time Chart
	Transmitted Bytes Real-time Chart
	Selected interfaces
Config Files	Config File Backup List
Credential	Authentication Association

Standalone AP Details

The following table lists the dashboard options and widgets or tables that are available for a standalone AP.

Table 7. Detailed information available for a standalone AP

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Device Details	General Information	
	Average Response Time and Packet Loss (Today)	
	Average CPU and Memory Utilization (Today)	
	Inventory Information	
	Min/Max/Average Response Time	
	Wireless Info (Current)	
	CPU	
	Latest 10 Alarms	
	Memory	
	Latest 10 Config Backups	
Radios and Network	2.4 GHz	Radio and networks
		SSID and authentication information
	5 GHz	Radio and networks
		SSID and authentication information
Client List	Active Client List Note: For more information, see Monitor Wireless Clients and View Client Details on page 89.	
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 SSID by Client Count (Current)	
	Top 10 SSID by Traffic (Today)	

Table 7. Detailed information available for a standalone AP (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Wireless Monitor	WLAN Utilization	
	Monitor per SSID	Wireless Client Count By SSID
		Wireless Traffic (Received and Transmitted) By SSID
		Wireless Frames (Received and Transmitted) By SSID
	Monitor per Radio	Wireless Traffic (Received and Transmitted) By Radio
		Wireless Client Count By Radio
		Wireless Packets (Received and Transmitted) By Radio
Wired Monitor	Total Traffic	Wired Received/Transmitted Bytes
		Wired Received/Transmitted Packets
	Traffic by Protocol	IP Traffic Monitor
		ICMP Traffic Monitor
		TCP Traffic Monitor
		UDP Traffic Monitor
		SNMP Traffic Monitor
Config Files	Config File Backup List	
Credential	Authentication Association	

Controller-Managed AP Details

The following table lists the dashboard options and widgets or tables that are available for a controller-managed AP.

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

Table 8. Detailed information available for a controller-managed AP

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Controller Managed AP Details	General Information
	Latest 10 Alarms

Table 8. Detailed information available for a controller-managed AP (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Radios and Network	2.4 GHz	Radio and Networks
		SSID and authentication information
	5 GHz	Radio and Networks
		SSID and authentication information
Client List	Active Client List Note: For more information, see <i>Monitor Wireless Clients and View Client Details</i> on page 89.	
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 SSID by Client Count (Current)	
AP Monitor	Monitor per SSID	Wireless Client Count By SSID
	Monitor per Radio	Wireless Client Count By Radio

Wireless Controller Details

The following table lists the dashboard options and widgets or tables that are available for a wireless controller.

Table 9. Detailed information available for a wireless controller

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Controller Details	General Information	
	Average Response Time and Packet Loss (Today)	
	Min/Max/Average Response Time	
	Inventory Information	
	Latest 10 Alarms	
	Latest 10 Config Backups	
Profiles	802.11b/bg/ng	Profiles
	802.11a/na	Profiles
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 Controller Managed AP by Client Count (Current)	
	Top 10 SSID by Client Count (Current)	
AP List	Access Points	

Table 9. Detailed information available for a wireless controller (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Client List	Active Client List Note: For more information, see <i>Monitor Wireless Clients and View Client Details</i> on page 89.
Interface List	Interface List Note: For more information, see <i>Table 14</i> on page 283.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Bandwidth Monitor	Received Bytes Real-time Chart
	Transmitted Bytes Real-time Chart
	Selected interfaces
Config File	Config File Backup List
Credential	Authentication Association

Wireless Managements System Details

The following table lists the dashboard options and widgets or tables that are available for a wireless management system (WMS).

Table 10. Detailed information available for a WMS

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Inventory Information
	Latest 10 Alarms
	Latest 10 Config Backups
Interface List	Interface List Note: For more information, see <i>Table 14</i> on page 283.

Table 10. Detailed information available for a WMS (continued)

Dashboard Menu Option	Widget or Table
Config Files	Config File Backup List
Credential	Authentication Association

Storage System Details

The following table lists the dashboard options and widgets or tables that are available for a storage system.

Table 11. Detailed information available for a storage system

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Inventory Information
	Volume Information
	Latest 10 Alarms
	Disk Information
	Latest 10 Config Backups
Interface List	Interface List Note: For more information, see Table 14 on page 283.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Bandwidth Monitor	Received Bytes Real-time Chart
	Transmitted Bytes Real-time Chart
	Selected interfaces
Temperature Monitor	Storage Temperature (°C)
	Disk Temperature (°C)

Table 11. Detailed information available for a storage system (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Disk and Fan Monitor	Disk Utilization (%)
	Fan Speed (RPM)
	Disk Capacity
Config File	Config File Backup List
Credential	Authentication Association

Router Details

The following table lists the dashboard options and widgets or tables that are available for a router.

Table 12. Detailed information available for a router

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Inventory Information
	Top 10 Interface by Traffic (Today)
	Latest 10 Alarms
Interface List	Interface List Note: For more information, see Table 14 on page 283.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Credential	Authentication Association

Unknown Device Details

The following table lists the dashboard option and widgets that are available for an unknown device.

Table 13. Detailed information available for an unknown device

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Latest 10 Alarms

Interface Details

The interface details can display for switches, wireless controllers, wireless management systems, and routers. The following table lists the dashboard options and widgets or tables that are available for an interface.

Table 14. Detailed information available for an interface

Dashboard Menu Option	Widget or Table
Interface Details	General Information
	Traffic Information
	Latest 10 Alarms
Monitor Data	Interface Received/Transmitted Bytes
	Interface Received/Transmitted Packets
	Interface Utilization (%)
	Interface Traffic Rate (bps)
	Interface Inbound/Outbound Error Packets
	Interface Inbound/Outbound Discards
Network Details	VLAN Membership
	Forwarding Database
	Common STP Port Status

Index

A

- access points, supported **14**
- account information, changing **22**
- administrator user name, default **19**
- administrator user security profile **238**
- alarms, managing **159–175**
- application notifications **109**
- audit logs **105**
- autorefreshing browser **254**

B

- backing up device configurations **112–122**
- basic spring view, network topology **198**
- browser, autorefreshing **254**
- browsers, supported **272**

C

- chart data, refreshing **252**
- charts, performance **99**
- childmaps **188**
- Chinese, language menu **18**
- colors, alarms **174**
- configurations, customizing, promoting, and restoring **122–145**
- controlled devices. See devices.
- controller-managed AP, described **30**
- controllers, supported **15**
- CPU alarms **163**
- credentials, devices
 - adding and modifying **34**
 - described **15**
- critical alarms **159, 163**
- current alarms, viewing and managing **159**
- customizing screens
 - DashBoard View **98**
 - Network Dashboard **103**
 - Network Summary **70**
 - Top 10, all devices **77**
 - Top 10, wireless devices **83**
 - Wireless Summary **83**

D

- dashboard (network), customizing **97–104**
- data retention period **247**
- data, refreshing **252**
- defaults
 - administrator user name **19**
 - auto refresh settings **254**
 - data retention periods **248**
 - device credentials **32**
 - idle time-out **251**
 - license **257**
 - Network Summary screen **69**
 - real-time chart settings **252**
 - report templates **221**
 - Top 10 screen, all devices **74**
 - Top 10 screen, wireless devices **81**
 - user security profiles **238**
 - Wireless Summary screen **81**
 - world map **183**
- deregistering licenses **259**
- details viewing, devices **274–283**
- device metrics, monitoring **92–97**
- devices
 - adding to a map **191**
 - configurations
 - backing up **112–122**
 - restoring **122–145**
 - upgrading **148–157**
 - credentials
 - adding and modifying **34**
 - described **15**
 - details, viewing **85, 274–283**
 - discovering **30–46**
 - firmware, managing **111–157**
 - groups
 - described **11**
 - managing **63**
 - IP addresses, discovery **32, 39**
 - managing **47–67**
 - rebooting **57**
 - registering **261–271**
 - reports **221**
 - supported **12**

- tables of **47–51**
- third-party **30**
- discovering devices **30–46**
- dynamic device groups **65**

E

- email server **23**
- English, language menu **18**
- event notifications, network **176**
- exporting
 - alarm configurations **163**
 - alarm history **161**
 - alarms **159**
 - configuration files **140**
 - device traps **177**
 - firmware files **155**
 - inventory and interface list tables **62**
 - network events **176**
 - system logs **179**
- exporting, external file server **146**
- external file server **145**

F

- file server, external **145**
- firewalls, supported **14**
- firmware versions, viewing **106**
- firmware, managing **111–157**

G

- global system settings, customizing **245–255**
- Gmail account, email server **25**
- groups, devices
 - described **11**
 - managing **63**

H

- header size, sFlow **216**
- hierarchical maps **186**
- history retention period, sFlow **216**
- history, alarms **161**
- HTTP, device credentials
 - adding and modifying **34**
 - described **16**
- HTTPS, device credentials **34**
- Hyper-V **272**

I

- idle time-out **251**
- importing
 - child maps **188**
 - configuration files **138**
 - firmware files **148**
 - from external file server **146**
- informational alarms **159**
- interface details, viewing **85**
- inventory and interface list tables, exporting **62**
- inventory polling **249**
- inventory reports **221**
- IP addresses, device discovery **32, 39**

J

- jobs, managing **233–236**

L

- language, selecting **18**
- levels of alarms **159**
- licenses, managing **256–260**
- link tree view, network topology **198**
- links, adding
 - on a map **193**
 - on a topology view **206**
- LLDP, device discovery **39**
- logging in
 - devices **56**
 - NMS300 **18**
- logging off users **244**
- logs
 - audit **105**
 - network events **176**
 - system (syslog) **179**

M

- major alarms **159**
- managed switches, supported **12**
- management systems, supported **15**
- managing
 - alarms **159–175**
 - device registrations **261–271**
 - devices **47–67**
 - firmware **111–157**
 - groups **63**
 - jobs **233–236**
 - licenses **256–260**
 - maps **183–198**

- monitors [92–97](#)
 - network topologies [198–213](#)
 - reports [220–232](#)
 - security profiles (users) [238–241](#)
 - sFlow [214](#)
 - SNMP traps [177](#)
 - topologies [198–213](#)
 - traps [177](#)
 - users [241–243](#)
 - maps, managing [183–198](#)
 - memory alarms [163](#)
 - MIB browser [59](#)
 - minor alarms [159](#)
 - monitoring devices and network [68–92](#)
 - monitors, managing [92–97](#)
- N**
- network dashboard, customizing [97–104](#)
 - network event notifications [176](#)
 - network summary, viewing and customizing [69–74](#)
 - network topologies, managing [198–213](#)
 - NMS300 server
 - described [10](#)
 - monitoring [107](#)
 - requirements [272](#)
 - notification profiles, alarms [169](#)
 - notifications
 - alarms [174](#)
 - application [109](#)
 - file backup results [113](#)
 - network events [176](#)
- O**
- observer and operator, security profiles [238](#)
 - operating systems, supported [272](#)
- P**
- password, changing [20](#)
 - performance, real-time [99](#)
 - pinging devices [57](#)
 - polling intervals, configuring [96, 249](#)
 - port, sFlow server [216](#)
 - profiles
 - alarm notification [169](#)
 - backup [112](#)
 - customer account for registration [262](#)
 - discovery [33](#)
 - user security [238](#)
 - promoting configurations [127–134](#)
 - protocols, device credentials [35](#)
- Q**
- quick discovery [31](#)
- R**
- radial view, network topology [198](#)
 - ReadyDATA and ReadyNAS systems, supported [15](#)
 - real-time chart, refreshing [252](#)
 - real-time performance [99](#)
 - rebooting devices [57](#)
 - registering
 - devices [261–271](#)
 - licenses [258](#)
 - reports, managing [220–232](#)
 - resources. See devices.
 - restoring device configurations [122–145](#)
 - results, sFlow monitoring [218](#)
 - resynchronizing registered devices [270](#)
 - retention period [247](#)
 - roles, users [238](#)
- S**
- sampling rate, sFlow [216](#)
 - scheduling
 - backup jobs [117](#)
 - discovery jobs [42](#)
 - firmware upgrades [150](#)
 - jobs [234](#)
 - reports [228](#)
 - restoring of configurations [123, 134](#)
 - security profiles (users), managing [238–241](#)
 - servers
 - email [23](#)
 - NMS300
 - described [10](#)
 - monitoring [107](#)
 - requirements [272](#)
 - sFlow [216](#)
 - SMS [26](#)
 - SMTP [24, 28](#)
 - sFlow, managing sources and viewing result [214](#)
 - smart switches, supported [13](#)
 - SMS server [26](#)
 - SMTP server [24, 28](#)
 - SNMP MIB browser [59](#)
 - SNMP traps, managing [177](#)

- SNMP, device credentials
 - adding and modifying **34**
 - described **16**
- software versions, viewing **106**
- software, managing **111–157**
- sources, sFlow **216**
- standalone AP, described **30**
- static device groups **63**
- storage systems
 - reports **221**
 - supported **15**
- summary, sFlow **218**
- supported devices **12**
- switches, supported **12–14**
- synchronizing devices **54**
- syslogs **179**
- system settings (global), customizing **245–255**

T

- technical support **2**
- Telnet, device credentials
 - adding and modifying **34**
 - described **16**
- templates, reports **221**
- third-party devices **30**
- time-out, idle **251**
- Top 10 widgets
 - all devices **74–80**
 - wireless devices **80–85**
- topologies, managing **198–213**
- tracing a route to a device **57**
- trademarks **2**
- traffic reports **221**
- traps, managing **177**
- types of users **11**

U

- upgrading device configurations **148–157**
- user name, default **19**
- user security profiles, managing **238–241**
- users
 - managing **241–243**
 - types of **11**

V

- VMWare **272**

W

- wireless access points, supported **14**
- wireless clients, monitoring **89**
- wireless controllers and management systems, supported **15**
- wireless device and client reports **221**
- wireless summary, viewing and customizing **80–85**

X

- XenServer **272**