

# NETGEAR®

---

## ProSafe 20-AP Wireless Controller WC7520 Reference Manual



350 East Plumeria Drive  
San Jose, CA 95134  
USA

February 20, 2012  
202-10686-04  
1.1

©2010–2011 NETGEAR, Inc. All rights reserved

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

## Technical Support

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

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

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

## Trademarks

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

## Statement of Conditions

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

## Revision History

| Publication Part Number | Version | Publish Date  | Comments   |
|-------------------------|---------|---------------|--|
| 202-10686-04            | v1.1    | February 2012 | Added hexadecimal address information to <a href="#">Guidelines for the Autodiscovery Process Across Layer 3 Networks</a> on page 52.  |
| 202-10686-04            | v1.0    | October, 2011 | <p>Added the following new information:</p> <ul style="list-style-type: none"> <li>• New features:                             <ul style="list-style-type: none"> <li>- Discovery and management of remote access points (see <a href="#">Requirements for Autodiscovery of Remote Access Points</a> on page 52) and <a href="#">Add Access Points to the Managed List after Discovery</a> on page 57</li> <li>- Support for sentry mode (see <a href="#">Edit and Remove Access Point Information</a> on page 59)</li> <li>- Rogue AP mitigation (see <a href="#">Configure Basic Rogue Detection Settings</a> on page 114)</li> <li>- Captive portal accounts (see <a href="#">Manage Users, Accounts, and Passwords</a> on page 128)</li> </ul> </li> <li>• Changes and improvements to the monitoring screens</li> <li>• Additional troubleshooting information</li> </ul> |

## ProSafe 20-AP Wireless Controller WC7520

|              |      |                |   |
|--------------|------|----------------|---|
| 202-10686-03 | v1.0 | July, 2011     | <p>Added the following new information:</p> <ul style="list-style-type: none"> <li>• Support for the WNDAP360 access point (see <a href="#">NETGEAR ProSafe Access Points</a>)</li> <li>• New features: <ul style="list-style-type: none"> <li>- N:1 redundancy (see <a href="#">Manage Redundancy</a>)</li> <li>- Monitoring stacking and redundancy (see <a href="#">View the Network Summary Screen</a>)</li> <li>- External RADIUS-based MAC authentication (see <a href="#">Guidelines for External MAC Authentication</a>)</li> <li>- External RADIUS-based captive portal authentication (see <a href="#">Configure Captive Portal Settings</a>)</li> </ul> </li> </ul>  |
| 202-10686-02 | v1.0 | March 2011     | <p>Added the following new information:</p> <ul style="list-style-type: none"> <li>• Support for the WNAP320 access point.</li> <li>• New features: <ul style="list-style-type: none"> <li>- Capability to specify use of an access point's internal or external antenna or antennas (see <a href="#">Edit and Remove Access Point Information</a>).</li> <li>- Capability to adjust the Tx power for all managed access points (see <a href="#">Configure Channels</a>).</li> <li>- Capability to adjust the channel and Tx power for individual access points (see <a href="#">Configure Wireless Settings</a>).</li> <li>- Capability to edit IP settings of individual access points (see <a href="#">Manage the Access Point List</a>).</li> <li>- Display of radio-mode capabilities on the managed AP list (see <a href="#">Manage the Access Point List</a>).</li> </ul> </li> </ul> <p>Revised existing content and reorganized the manual.<br/> Made changes to some monitoring screens (see <a href="#">Chapter 11, Monitoring the Wireless Network and Components</a>).</p> |
| 202-10686-01 | v1.4 | October 2010   | Made a minor revision to indicate the number of supported MAC addresses per SSID.   |
| 202-10686-01 | v1.3 | September 2010 | Added an index and made minor revisions to existing content.  |
| 202-10686-01 | v1.2 | September 2010 | Added new content and revised existing content in chapters 1, 2, 4, 5, 9, and 10.<br>Added chapters 11 and 12 and appendix A.   |
| 202-10686-01 | v1.1 | September 2010 | Added new content to chapters 1 through 4.  |
| 202-10686-01 | v1.0 | August 2010    | Initial publication.  |

# Table of Contents

## Chapter 1 Introduction and Overview

|  |    |
|--|----|
| Key Features and Capabilities . . . . .                        | 9  |
| Package Contents . . . . .                                     | 11 |
| Hardware Features . . . . .                                    | 12 |
| Front Panel Ports and LEDs . . . . .                           | 12 |
| Rear Panel Features . . . . .                                  | 13 |
| Bottom Panel with Product Label . . . . .                      | 14 |
| WC7520 Wireless Controller System Components . . . . .         | 14 |
| NETGEAR ProSafe Access Points . . . . .                        | 15 |
| What Can You Do with the WC7520 Wireless Controller? . . . . . | 16 |
| Licenses . . . . .   | 18 |
| Maintenance and Support . . . . .                              | 18 |
| Web Management Interface Layout . . . . .                      | 19 |
| Initial Connection and Configuration . . . . .                 | 20 |
| Basic and Advanced Settings . . . . .                          | 22 |
| Profile Groups . . . . .                                       | 23 |
| Choose a Location for the Wireless Controller . . . . .        | 25 |
| Deploy the Wireless Controller . . . . .                       | 26 |

## Chapter 2 System Planning and Deployment Scenarios

|  |    |
|--|----|
| System Planning . . . . .  | 27 |
| Preinstallation Planning . . . . .                                     | 27 |
| Before You Configure a Wireless Controller . . . . .                   | 28 |
| Single Controller Configuration with Basic Profile Group . . . . .     | 30 |
| Single Controller Configuration with Advanced Profile Groups . . . . . | 31 |
| Stacked Controller Configuration . . . . .                             | 32 |
| Management VLAN and Data VLAN Strategies . . . . .                     | 32 |
| Deployment Scenarios . . . . .   | 34 |
| Scenario Example 1: Basic Network with Single VLAN . . . . .           | 34 |
| Scenario Example 2: Advanced Network with VLANs and SSIDs . . . . .    | 35 |
| Scenario Example 3: Advanced Network with Redundancy . . . . .         | 38 |

## Chapter 3 RF Planning

|  |    |
|--|----|
| RF Planning Overview . . . . .                         | 41 |
| Planning Requirements . . . . .                        | 41 |
| Define and Edit Buildings and Floors . . . . .         | 42 |
| Specify Access Point Requirements . . . . .            | 45 |
| View and Manage Heat Maps for Deployed Plans . . . . . | 48 |

**Chapter 4 Access Point Discovery and Management**

|  |    |
|--|----|
| Access Point Discovery and Discovery Guidelines . . . . .        | 51 |
| Requirements for Autodiscovery of Local Access Points . . . . .  | 51 |
| Requirements for Autodiscovery of Remote Access Points . . . . . | 52 |
| Run the Discovery Wizard . . . . .                               | 54 |
| Discovery Results . . . . .                                      | 56 |
| Manage the Access Point List . . . . .                           | 57 |
| Add Access Points to the Managed List after Discovery . . . . .  | 57 |
| Edit and Remove Access Point Information . . . . .               | 59 |

**Chapter 5 Configuring Network Settings**

|  |    |
|--|----|
| Configure General Settings . . . . .                       | 63 |
| Time Management . . . . .                                  | 64 |
| Configure IP and VLAN Settings . . . . .                   | 65 |
| Management VLANs . . . . .                                 | 66 |
| Untagged VLANs . . . . .                                   | 67 |
| Manage the DHCP Server . . . . .                           | 67 |
| Manage Certificates . . . . .                              | 70 |
| Configure Syslog and Alarm Notification Settings . . . . . | 71 |
| Configure Syslog Settings . . . . .                        | 71 |
| Configure Alarm Notification Settings . . . . .            | 72 |
| Configure the Email Notification Server . . . . .          | 72 |

**Chapter 6 Managing Security Profiles and Profile Groups**

|   |    |
|---|----|
| Manage Wireless Security Profiles . . . . .                       | 74 |
| Small WLAN Networks . . . . .                                     | 75 |
| Larger WLAN Networks . . . . .                                    | 75 |
| Profile Naming Conventions . . . . .                              | 76 |
| Considerations Before You Configure Profiles . . . . .            | 76 |
| Configure Security Profiles for the Basic Profile Group . . . . . | 77 |
| Edit and Remove Profiles from the Basic Profile Group . . . . .   | 80 |
| Network Authentication and Data Encryption Options . . . . .      | 81 |
| Configure Security Profiles for Advanced Profile Groups . . . . . | 84 |
| Edit and Remove Profiles from an Advanced Profile Group . . . . . | 87 |
| Remove an Advanced Profile Group . . . . .                        | 87 |
| Manage Basic and Advanced Profile Groups in the WLAN . . . . .    | 87 |

**Chapter 7 Configuring Wireless and QoS Settings**

|  |    |
|--|----|
| About Basic and Advanced Wireless and QoS Configurations . . . . . | 90 |
| Configure the Radio . . . . .                                      | 91 |
| Basic Radio Configuration . . . . .                                | 91 |
| Advanced Radio Configuration for Profile Groups . . . . .          | 92 |
| Configure Wireless Settings . . . . .                              | 93 |
| Basic Wireless Configuration . . . . .                             | 93 |
| Advanced Wireless Configuration for Profile Groups . . . . .       | 96 |

- Configure Channels ..... 99
- Specify RF Management ..... 101
  - Basic RF Management..... 102
  - Advanced RF Management for Profile Groups..... 104
- Configure QoS for Profile Groups ..... 105
- Configure Load Balancing ..... 107
- Configure Rate Limiting ..... 109
  - Basic Rate Limiting..... 109
  - Advanced Rate Limiting for Profile Groups ..... 110

**Chapter 8 Configuring Network Access and Security**

- About Basic and Advanced Security Configurations ..... 112
- Manage Rogue Access Points ..... 113
  - Configure Basic Rogue Detection Settings ..... 114
  - Configure Advanced Rogue Detection Settings ..... 116
- Manage MAC Authentication and MAC Authentication Groups..... 117
  - Guidelines for External MAC Authentication ..... 118
  - Configure Basic Local MAC Authentication Settings ..... 118
  - Configure Local MAC Authentication Groups..... 120
- Manage Authentication Servers and Authentication Server Groups .... 122
  - Configure Basic Authentication Server Settings..... 123
  - Configure RADIUS Authentication Server Groups ..... 125
- Manage Guest Network Access ..... 126
  - Configure Captive Portal Settings ..... 126
- Manage Users, Accounts, and Passwords..... 128

**Chapter 9 Maintaining the Controller**

- Manage the Configuration File ..... 135
  - Back Up and Restore the Configuration File ..... 135
  - Upgrade the Configuration File..... 137
- Reboot or Reset the Wireless Controller ..... 139
- Reboot Access Points ..... 141
- Manage External Storage..... 141
- Manage Remote Access ..... 142
  - Specify Session Time-Outs ..... 144
- View Alerts and Events and Save the Logs ..... 144
  - Save the Logs..... 144
  - View Alerts and Events..... 145
- Manage Licenses ..... 149
  - View Your Licenses ..... 149
  - Configure the License Server Settings..... 150
  - Register Your Licenses ..... 151
  - Retrieve Your Licenses ..... 153

## Chapter 10 Managing Stacking and Redundancy

|   |     |
|---|-----|
| Manage Stacking . . . . .                   | 154 |
| Configure Stacking . . . . .                | 155 |
| Controller Selection List . . . . .         | 157 |
| Manage Redundancy . . . . .                 | 158 |
| Single Controller with Redundancy . . . . . | 158 |
| N:1 Redundancy . . . . .                    | 160 |
| Configure Redundancy . . . . .              | 164 |

## Chapter 11 Monitoring the Wireless Network and Components

|  |     |
|--|-----|
| Monitor the Network . . . . .  | 167 |
| View the Network Summary Screen . . . . .  | 168 |
| View Network Usage . . . . .   | 170 |
| View Wireless Controllers in the Network . . . . .                                   | 171 |
| View Managed Access Points in the Network . . . . .                                  | 172 |
| View Clients in the Network . . . . .  | 176 |
| View Security Profiles in the Network . . . . .                                      | 178 |
| Monitor the Wireless Controller . . . . .  | 179 |
| View the Wireless Controller Summary Screen . . . . .                                | 180 |
| View Wireless Controller Usage . . . . .   | 182 |
| View Access Points Managed by the Wireless Controller . . . . .                      | 182 |
| View Clients Managed by the Wireless Controller . . . . .                            | 184 |
| View Neighboring Clients Detected by the Wireless Controller . . . . .               | 184 |
| View Rogue Access Points Detected by the Wireless Controller . . . . .               | 185 |
| View Security Profiles Managed by the Wireless Controller . . . . .                  | 187 |
| View DHCP Leases Provided by the Wireless Controller . . . . .                       | 188 |
| View Captive Portal Guests and Users Managed by<br>the Wireless Controller . . . . . | 188 |
| Monitor the SSIDs . . . . .  | 190 |
| Monitor the Clients . . . . .  | 191 |
| View Local Clients . . . . .   | 191 |
| View Blacklisted Clients . . . . .   | 192 |

## Chapter 12 Troubleshooting

|  |     |
|--|-----|
| Troubleshoot Basic Functioning . . . . .                             | 194 |
| Power LED Not On . . . . .   | 194 |
| Test LED Never Turns Off . . . . .                                   | 195 |
| LAN Port LEDs Not On . . . . .                                       | 195 |
| Troubleshoot the Web Management Interface . . . . .                  | 195 |
| Ethernet Cabling . . . . .   | 195 |
| IP Address Configuration . . . . .                                   | 195 |
| Internet Browser . . . . .   | 196 |
| Troubleshoot a TCP/IP Network Using the Ping Utility . . . . .       | 197 |
| Test the LAN Path to Your Wireless Controller . . . . .              | 197 |
| Use the Factory Default Button to Restore Default Settings . . . . . | 198 |
| Problems with Date and Time . . . . .                                | 198 |

Problems with Access Points . . . . . 198  
    Discovery Problems . . . . . 198  
    Connection Problems . . . . . 199  
    Network Performance and Rogue Access Point Detection . . . . . 200  
Use the Diagnostic Tools on the Wireless Controller . . . . . 200

**Appendix A Factory Default Settings and Technical Specifications**

**Appendix B Notification of Compliance**

**Index**



# Introduction and Overview

---

# 1

This chapter includes the following sections:

- *Key Features and Capabilities*
- *Package Contents*
- *Hardware Features*
- *WC7520 Wireless Controller System Components*
- *What Can You Do with the WC7520 Wireless Controller?*
- *Licenses*
- *Maintenance and Support*
- *Web Management Interface Layout*
- *Initial Connection and Configuration*
- *Basic and Advanced Settings*
- *Choose a Location for the Wireless Controller*
- *Deploy the Wireless Controller*

---

**Note:** For more information about the topics covered in this manual, visit the support website at <http://support.netgear.com>.

---

## Key Features and Capabilities

The ProSafe 20-AP Wireless Controller WC7520 is intended for medium-sized businesses, schools, and hospitals. In a stacked configuration and with the appropriate licenses, a wireless controller can support up to 150 access points (APs) with up to 1,500 users or more. The wireless controller supports the IEEE 802.11a/b/g/n protocols. The wireless controller allows you to manage your wireless network from a central point, implement security features centrally, support Layer 2 and Layer 3 fast roaming, configure a guest access captive portal, and support Voice over Wi-Fi (VoWi-Fi).

The wireless controller provides the following key features and capabilities:

- **Scalable architecture with stacking and redundancy**
  - Support for 20 access points on a single wireless controller with no additional license.
  - Purchased licenses (WC7510L) in increments of 10 access points allow for support of up to a maximum number of 50 access points on a single wireless controller.
  - A maximum of three stacked wireless controllers allows for up to 150 access points in a single network.
  - Support of N:1 redundancy.
  - Support of 802.11a, 802.11b, 802.11g, and 802.11n modes.
- **Autodiscovery of access points**
  - Autodiscovery of access points in the same Layer 2 domain.
  - Autodiscovery of access points across a Layer 3 domain.
  - Autodiscovery of remote access points over a site-to-site VPN connection or behind a NAT router.
  - Automatic download of wireless controller-based firmware to discovered access points that are added to the managed access point list.
- **Centralized management**
  - Single point of management for the entire wireless network.
  - Visualization of live coverage and heat maps for the wireless network.
  - Automatic firmware upgrade to all managed access points.
  - DHCP server for IP address provisioning.
  - Configurable management VLAN.
- **Security**
  - Identity-based security authentication with an external RADIUS or LDAP (Active Directory) server, or with an internal authentication server.
  - Up to 8 profiles per profile group and 8 profiles per radio (therefore, dual-band access points can support up to 16 profiles in one profile group).
  - Support for up to 128 access point profiles<sup>1</sup> per wireless controller (8 profiles per group and 8 groups per radio). Each access point profile supports settings for SSID, network authentication, data encryption, client separation, VLAN, MAC ACL, and wireless QoS.
  - Support for up to 8 access point profile *groups*<sup>2</sup> per wireless controller.
  - Rogue access point detection, classification, and mitigation.
  - Guest access and captive portal access with cost and expiration accounting.
  - Scheduled wireless on/off times.

---

1. Number of profiles depends on the access point model used with the wireless controller.

2. Number of profile groups depends on the access point model used with the wireless controller.

- **Wi-Fi Multimedia Quality of Service and advanced wireless features**
  - Wi-Fi Multimedia (WMM) support for video, audio, and Voice over Wi-Fi (VoWi-Fi).
  - WMM power save option.
  - Automatic WLAN healing mechanism ensures seamless coverage for wireless users.
  - Layer 2 and Layer 3 seamless roaming support (FRS).
  - Local Layer 2 traffic switching at access point level for fast processing and roamed Layer 3 traffic processing at controller level.
- **RF planning and management**
  - RF planning tool to predict the number and placement of access points based on signal strength and the number of users per building floor, and to display the predicted coverage.
  - Automatic control of access point transmit power and channel allocation to reduce interference.
  - Automatic load balancing of clients across access points.
  - Rate limiting per profile.
- **Monitoring and reporting**
  - Access point heat maps by wireless band and signal strength for real-time status view of the WLAN.
  - Monitoring of the status of the network, wireless controllers, WLANs, and clients, and network usage statistics.
  - Specific health monitoring of access points.
  - Logging and emailing of system events, RF events, load-balancing events, rate-limiting events, and redundancy failover events.

For a list of all features and capabilities of the wireless controller, see the datasheet at [http://support.netgear.com/app/products/model/a\\_id/13060](http://support.netgear.com/app/products/model/a_id/13060).

## Package Contents

The ProSafe 20-AP Wireless Controller WC7520 product package contains the following items:

- ProSafe 20-AP Wireless Controller WC7520 appliance
- One AC power cable
- Rubber feet (4) with adhesive backing
- One rack-mount kit
- Straight-through Category 5 Ethernet cable
- *WC7520 ProSafe Wireless Controller Installation Guide*
- *Resource CD*

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

## Hardware Features

The front panel ports and LEDs, rear panel components, and bottom label of the wireless controller are described in this section.

### Front Panel Ports and LEDs

The following figure shows the front panel ports and status LEDs of the wireless controller.

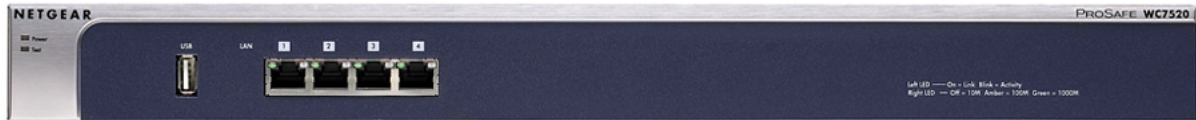


Figure 1.

From left to right, the wireless controller's front panel shows the following ports and LEDs:

- Power LED
- Test LED
- USB port for external storage, for example for more floor heat maps and extended statistics history
- Four 10/100/1000 Mbps LAN Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs. All Ethernet ports provide switched N-way, automatic speed negotiating, auto MDI/MDIX technology.

---

**Note:** The four ports of the wireless controller function as a single switch.

---

The function of each LED is described in the following table:

Table 1. LED functions

| LED       | Status | Description  |
|-----------|--------|--|
| Power LED | On     | The green Power LED should be lit when the wireless controller is on.  |
|           | Off    | If the power LED is not lit when the wireless controller is on, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off (see <a href="#">Power LED Not On</a> on page 194). |

Table 1. LED functions (continued)

| LED                                    | Status           | Description  |
|--|------------------|--|
| Test LED                               | On               | The wireless controller is initializing. After approximately 2 minutes, when the wireless controller has completed its initialization, the Test LED turns off. If the Test LED remains on, the initialization has failed (see <a href="#">Test LED Never Turns Off</a> on page 195). |
|  | Off              | The wireless controller has completed its initialization successfully. The Test LED should be off during normal operation.   |
|  | Blinking         | Firmware is being upgraded.  |
| Left LAN port LED (one for each port)  | Off              | The port has no physical link, that is, no Ethernet cable is plugged into the wireless controller (see also <a href="#">LAN Port LEDs Not On</a> on page 195).   |
|  | On (green)       | The port has detected a link with a connected Ethernet device.   |
|  | Blinking (green) | Data is being transmitted or received by the port.   |
| Right LAN port LED (one for each port) | Off              | The port is operating at 10 Mbps.  |
|  | On (amber)       | The port is operating at 100 Mbps.   |
|  | On (green)       | The port is operating at 1000 Mbps.  |

## Rear Panel Features

The following figure shows the rear panel components of the wireless controller.

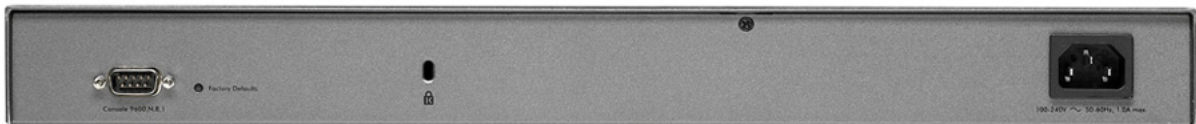


Figure 2.

From left to right, the wireless controller's rear panel components are:

- **Console port.** RS232 port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The configuration is 8 bits, no parity, and 1 stop bit.

---

**Note:** The console port is for debugging under guidance of NETGEAR technical support only.

---

- **Factory Defaults button.** Using a sharp object, press and hold this button for about 10 seconds until the front panel LED flashes and the wireless controller returns to factory default settings.

---

**Note:** If you reset the wireless controller, all configuration settings are lost and the default password is restored.

---

- **Kensington lock.** Attach an optional Kensington lock to prevent unauthorized removal of the wireless controller.
- **AC power socket.** Attach the power cord to this socket. (There is no separate on/off power switch.)

## Bottom Panel with Product Label

The product label on the bottom of the wireless controller's enclosure displays the default IP address, default user name, and default password, as well as regulatory compliance, input power, and other information.



Figure 3.

## WC7520 Wireless Controller System Components

A WC7520 wireless controller *system* consists of one or more wireless controllers and a collection of access points that are organized into groups based on location or network access.

The wireless controller system can include a single wireless controller, a single wireless controller with a backup wireless controller for N:1 redundancy, or a group of up to three stacked wireless controllers, with or without a redundant wireless controller.

The WC7520 wireless controller system supports the following access point models:

- NETGEAR WNAP210 ProSafe wireless-N access point
- NETGEAR WNAP320 ProSafe wireless-N access point
- NETGEAR WNDAP350 ProSafe dual-band wireless-N access point
- NETGEAR WNDAP360 ProSafe dual-band wireless-N access point

Future releases will support additional access point models.

## NETGEAR ProSafe Access Points

You can connect access points to the wireless controller either directly with an Ethernet cable through a router or switch, or remotely through an IP network. After you have used the automatic discovery process and added access points to the managed access point list on the wireless controller, the wireless controller converts the standard access points to dependent access points by pushing firmware to the access points. From then on, you can centrally manage and monitor the access points.

A WC7520 wireless controller system can support the following access points:

- **WNAP210 ProSafe Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W
  - Requires minimum firmware version WNAP210\_2.0.8 or a newer version.

For product documentation and firmware, see  
[http://support.netgear.com/app/products/model/a\\_id/8101](http://support.netgear.com/app/products/model/a_id/8101).

- **WNAP320 ProSafe Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W
  - Accepts optional antennas
  - Requires minimum firmware version WNAP320\_2.0.7 or a newer version.

For product documentation and firmware, see  
[http://support.netgear.com/app/products/model/a\\_id/18601](http://support.netgear.com/app/products/model/a_id/18601).

- **WNDAP350 ProSafe Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices
  - Supports PoE with a power consumption of up to 10.75W
  - Concurrent operation in 2.4 GHz and 5 GHz radio band while in 802.11n mode
  - Accepts optional antennas
  - Requires minimum firmware version WNDAP350\_V2.0 or a newer version.

For product documentation and firmware, see  
[http://support.netgear.com/app/products/model/a\\_id/12823](http://support.netgear.com/app/products/model/a_id/12823).

- **WNDAP360 ProSafe Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices
  - Supports PoE with a power consumption of up to 10.51W
  - Concurrent operation in 2.4 GHz and 5 GHz radio band while in 802.11n mode
  - Accepts optional antennas
  - Requires minimum firmware version WNDAP360\_2.0.3 or a newer version.

For product documentation and firmware, see [http://support.netgear.com/app/products/model/a\\_id/19189](http://support.netgear.com/app/products/model/a_id/19189).

## What Can You Do with the WC7520 Wireless Controller?

These are some of the tasks that you can perform with a WC7520 wireless controller:

### *Plan a Wireless Network*

- **Design a WLAN.** Design an efficient WLAN with building and floor dimensions for your specific environment.
- **Estimate the number of required access points and their approximate locations.** Estimate how many access points you need for your wireless coverage and determine their optimum location for best coverage and performance.

For more information, see [Chapter 3, RF Planning](#).

### *Discover Access Points in the Network and Provision IP Addresses and Firmware*

- **Discover access points in the network.** The access points can be in factory default state or functioning in standalone mode, but after discovery by the wireless controller and addition to the managed access point list, the access points become dependent (managed) access points.
- **Provision IP addresses to the access points.** Use the internal DHCP server to provision IP addresses to all or selected managed access points in the network.
- **Upgrade access point firmware.** Update and synchronize new firmware versions to all managed access points in the network.

For more information, see [Chapter 4, Access Point Discovery and Management](#).

### *Organize the Network*

- **Create access point profiles.** Organize access points in profiles to differentiate between SSIDs, client authentication, authentication settings, and wireless QoS settings.
- **Create access point profile groups.** Organize access point profiles in access point profile groups to differentiate between buildings, floors, businesses or business divisions,



and so on. Easily assign access points to profile groups or make changes to assignments.

For more information, see [Chapter 6, Managing Security Profiles and Profile Groups](#).

### *Centrally Manage the Wireless Settings for the Network*

- **Schedule the radios.** Schedule the entire network to go offline, or schedule access point profile groups to go offline.
- **Manage wireless settings and channel allocation.** Manage the wireless settings such as wireless mode, data rate, channel width, and so on, for the entire network or for access point profile groups, and manage channel allocation for the entire network.
- **Manage QoS settings.** Manage QoS queue settings for data, background, video, and voice traffic for access point profile groups.
- **Configure RF management settings.** Configure WLAN healing and wireless coverage hole detection for the entire network or for access point profile groups.

For more information, see [Chapter 7, Configuring Wireless and QoS Settings](#).

### *Centrally Manage Security in the Network*

- **Manage secure access to the network and secure data transmission.** Manage client authentication, encryption, wireless client security separation, and MAC authentication in access point profiles.
- **Manage authentication servers for the network.** Manage all internal and external authentication servers for the entire network or for access point profile groups.
- **Manage MAC authentication.** Specify trusted and untrusted MAC addresses for the entire network.
- **Manage rogue access points.** Manage rogue access points and their associated clients in the network.
- **Manage guest access.** Manage guest access and captive portal access to the network.

For more information, see [Chapter 8, Configuring Network Access and Security](#).

### *Manage Other Wireless Controllers in the Network*

- **Manage stacking.** Specify the primary and secondary wireless controllers in a stack and synchronize information between the wireless controller.
- **Manage redundancy groups.** Specify the primary and secondary wireless controllers in redundancy group and enable failover protection.

For more information, see [Chapter 10, Managing Stacking and Redundancy](#).

### *Monitor the Network and Its Components*

- **View heat maps.** View the real-time heat maps for a deployed WLAN. See the RF signal propagation per floor, and identify coverage holes and weak signal spots.
- **Monitor the status of all wireless devices.** View the status the wireless controllers, access points, clients, access point profiles, and the entire network, and view network usage statistics.
- **Monitor network health.** See which access points are healthy and which ones are down or compromised.

For more information, see [Chapter 11, Monitoring the Wireless Network and Components](#).

## Licenses

The wireless controller includes an built-in license to support up to 20 access points in 802.11a/b/g/n mode. You can purchase licenses in 10–access point increments (WC7510L) for support of up to 50 access points for a single wireless controller. To support 50 access points, you would need to purchase 3 WC7510L licenses; if you have three wireless controllers in a stack and want to support the maximum number of 150 access points, you would need to purchase 9 WC7510L licenses.

Adding a redundant wireless controller also requires you to purchase licenses to support the required number of access points on the redundant wireless controller.

Licenses are tied to the serial number of the wireless controller.

For more information, see the License Configuration section in the datasheet at [http://support.netgear.com/app/products/model/a\\_id/13060](http://support.netgear.com/app/products/model/a_id/13060).

For information about how to manage your licenses, see [Manage Licenses](#) on page 149.

## Maintenance and Support

NETGEAR offers technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR ProSupport website at [http://kb.netgear.com/app/answers/detail/a\\_id/212](http://kb.netgear.com/app/answers/detail/a_id/212).

## Web Management Interface Layout

The following figure shows the menu at the top and the left of the wireless controller's web management interface (the screen's content has been removed for more clarity).

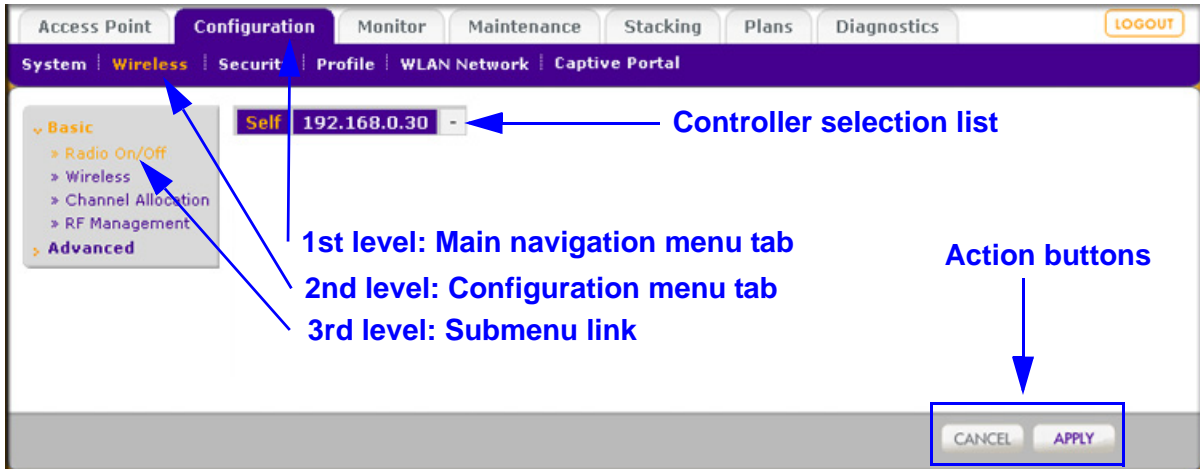


Figure 4.

A web management interface screen can include the following components:

- **1st level: Main navigation menu tab.** The main navigation menu tabs in the light gray bar across the top of the web management interface provide access to all configuration menu tabs of the wireless controller and remain constant. When you select a main navigation menu tab, the letters are displayed in white against a blue background.
- **2nd level: Configuration menu tab.** The configuration menu tabs in the blue bar (immediately below the main navigation menu bar) change according to the main navigation menu tab that you select. When you select a configuration menu tab, the letters are displayed in orange against a blue background.
- **3rd level: Submenu link.** Each configuration menu tab has one or more submenu links that are listed on the left side of the screen in a gray box. When you select a submenu link, the text is displayed in orange against a gray background. On many screens, the submenus are divided into a basic submenu and an advanced submenu.
- **Action buttons.** Action buttons change the configuration or allow you to make changes to the configuration. These are the most common action buttons:
  - **Apply.** Saves all configuration changes made on the current screen. Saved settings are retained when the wireless controller is powered off or rebooted, while unsaved configuration changes are lost.
  - **Cancel.** Resets options on the current screen to the last-applied or -saved settings.
  - **Add.** Adds a new item to the current screen. Typically, a pop-up window opens that enables you to enter information in additional fields.
  - **Edit.** Allows you to edit the configuration of the selected item.
  - **Remove or Delete.** Removes the selected item from the table or screen configuration.

- **Back.** Return to the previous screen.
- **Next.** Advance to the next screen.
- **Controller selection list.** In a stacked configuration, the controller selection list lets you select the wireless controller to configure.

## Initial Connection and Configuration

Follow the steps in this section to set up the wireless controller. For additional information, see the *WC7520 ProSafe Wireless Controller Installation Guide* that you can access from [http://kb.netgear.com/app/products/model/a\\_id/13060](http://kb.netgear.com/app/products/model/a_id/13060).

### ➤ To set up, configure, and deploy the wireless controller:

1. Connect the wireless controller to your computer:
  - a. Configure a computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
  - b. Connect the wireless controller to the computer through the network or directly to one of the wireless controller's ports.
  - c. Connect the power cord from the wireless controller to an AC power outlet.
  - d. Check the lights on the front of the wireless controller:
    - **Power.** The green Power LED should be lit. If the Power LED is not lit, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off.
    - **Test.** The Test LED is on briefly when the controller is first turned on.
    - **LAN** The Ethernet (LAN) LED should be lit (amber for 10/100 Mbps and green for 1000 Mbps) indicating that a connection has been made. If it is not, make sure that the Ethernet cable is securely attached at both ends.
2. Log in to the wireless controller:
  - a. Open your browser and type **http://192.168.0.250** in the browser's address field.

---

**Note:** You need to use a web browser such as Microsoft Internet Explorer 5.1 or later or Mozilla Firefox 1.x or later with JavaScript, cookies, and SSL enabled.

---

The wireless controller’s login window displays:

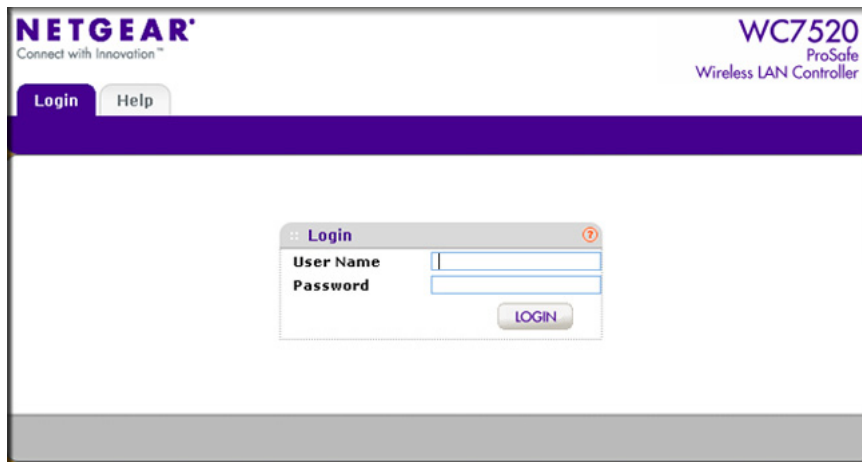


Figure 5.

- b. When prompted, enter **admin** for the user name and **password** for the password, both in lowercase letters.
- c. Click **Login**. The wireless controller’s web management interface displays, with the default status screen (the path is Monitor > Controller > Summary), which shows the network status and related information:

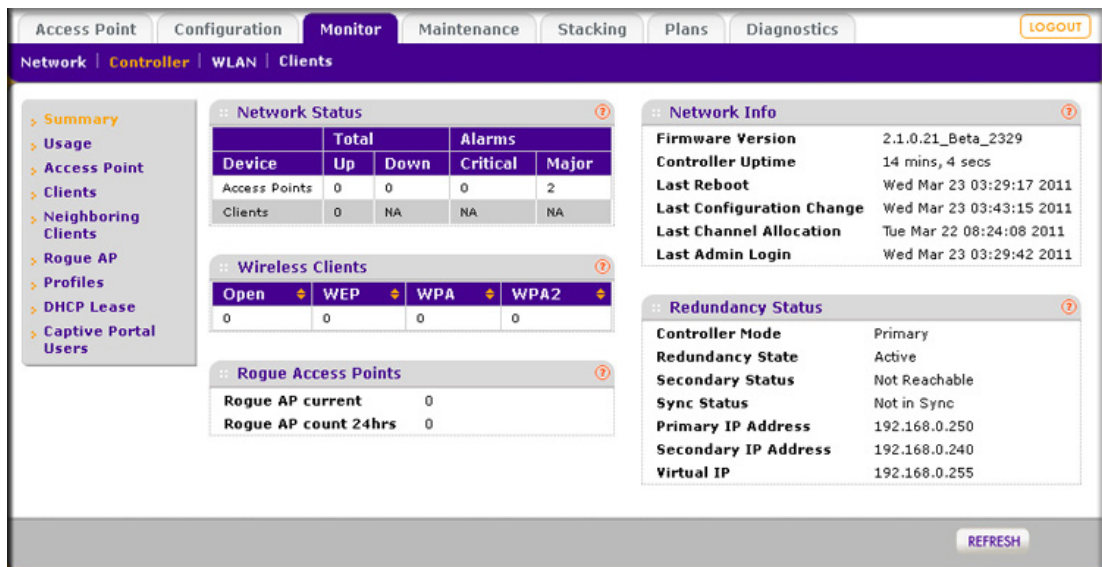


Figure 6.

**Note:** The Network navigation menu tab displays under the Monitor main navigation tab only when you have configured stacking.

For information about the layout and general characteristics of the web management interface, see [Web Management Interface Layout](#) on page 19.

For information about the network status and related information, see [View the Wireless Controller Summary Screen](#) on page 180.

3. Configure the wireless controller and your network:
  - a. **RF planning.** Follow instructions in [Chapter 3, RF Planning](#), to plan the number and location of the access points.
  - b. **Configure your network.** Follow the instructions in [Chapter 4](#) through [Chapter 10](#) to configure your network, including the SSIDs, security, MAC ACLs, captive portal, QoS, rate limiting, and so on.
  - c. **Set up the wireless controller.** Follow the instructions in [System Planning](#) on page 27 to select the type of deployment for your network.
  - d. **Add the access points.** Follow the steps in [Access Point Discovery and Discovery Guidelines](#) on page 51 to discover your access points and add them to wireless controller's managed access point list.

## Basic and Advanced Settings

You can deploy the wireless controller in a small wireless network with 10 or 20 access points or in a large wireless network with up to 150 access points. Small networks require a basic configuration, but large networks can become very complex and require you to configure the advanced features of the wireless controller.

Depending on your network configuration, use basic settings or advanced settings to manage your access points:

- **Basic settings for a typical network.** The basic settings work with most common network configurations. For example, all access points on the WLAN are for the same organization or business and therefore adhere to the same policies and use a small number of service set identifiers (SSIDs, or network names).
- **Advanced settings for access point profile groups.** If you have a large wireless network, or if completely separate networks share a single WLAN, use the advanced settings to set up multiple access point profile groups with multiple security profiles (SSIDs with associated security settings). For example, a shopping mall might need several access point profile groups if several businesses share a WLAN but each business has its own network. Larger networks could require multiple access point profile groups to allow different policies per building or department. The access points could have different security profiles per building and department, for example, one for guests, one for management, one for sales, and so on.

---

**Note:** Access point profile groups are also referred to as just profile groups.

Profiles, security profiles, and SSIDs (that is, SSIDs with associated security settings) are terms that are interchangeable.

---

To accommodate all types of networks, almost all configuration menus of the web management interface are divided into basic and advanced submenus. The following figure shows an example of the Security > Wireless > Basic submenu on the left and the Security > Wireless > Advanced submenu on the right:

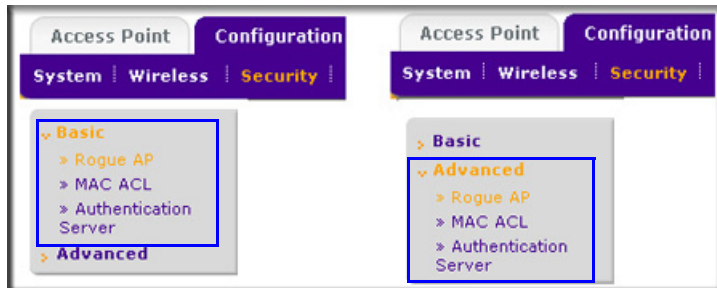


Figure 7.

Before you start the configuration of your wireless controller, decide whether you can use a basic configuration (that is, follow the basic submenus) or need to use an advanced configuration (that is, follow the advanced submenus). Once you have made your choice, configuring the wireless controller should be fairly easy if you consistently follow either the basic submenus or the advanced submenus.

## Profile Groups

Each access point can support up to 8 security profiles (16 for dual-band access points), each with its own SSID, security settings, MAC ACL, rate-limiting settings, WMM, and so on.

The wireless controller follows the same architecture. A profile group on the wireless controller includes all the features that you can configure for an individual access point: up to 8 profiles (16 for dual-band access points), each of which has its own SSID, security, MAC ACL, rate-limiting settings, WMM settings, and so on.

### Basic Profile

The basic profile includes all the settings that are required to configure a fully functional access point with up to 8 security profiles (16 for dual-band access points).

After you have used the automatic discovery process and added access points to the managed AP list on the wireless controller, the access points are assigned by default to the basic profile group.

If your network requires the wireless controller to manage multiple access points with different configurations, use the advanced profile.

### Advanced Profile

The advanced profile lets you configure up to 8 access point profile groups. Each group includes all the settings that are required to configure a fully functional access point with up to 8 security profiles (16 for dual-band access points).

For example, if there are four buildings, each with a completely different wireless network, you simply create four profile groups. You then assign all access points in one building to one profile group, all access points in another building to a second profile group, and so on.

For each profile group, you can create an individual radio-on/off schedule, RF management settings, MAC ACL authentication, and an authentication server. For each radio in a profile group (2.4-GHz radio and 5-GHz radio), you can create individual wireless settings, WMM, and rate-limit settings.

The following figure shows the advanced profile group architecture. The structure that is shown under Group-1 is implemented in all profile groups (that is, Group-2 through Group-8):

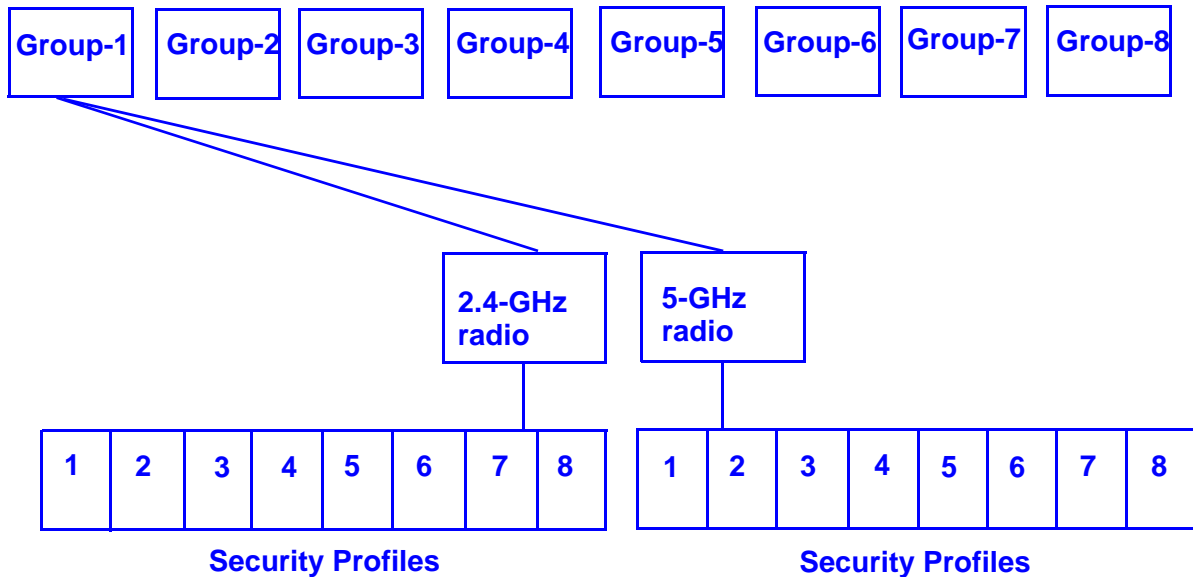


Figure 8.

The following figure shows an example of three access point profile groups, in which the first profile group (Group-1) has three security profiles. For each profile in this profile group, the profile name, radio mode, and authentication setting are shown. (Group-1 is the default group in the advanced profile group configuration; you need to create the other profiles groups.)



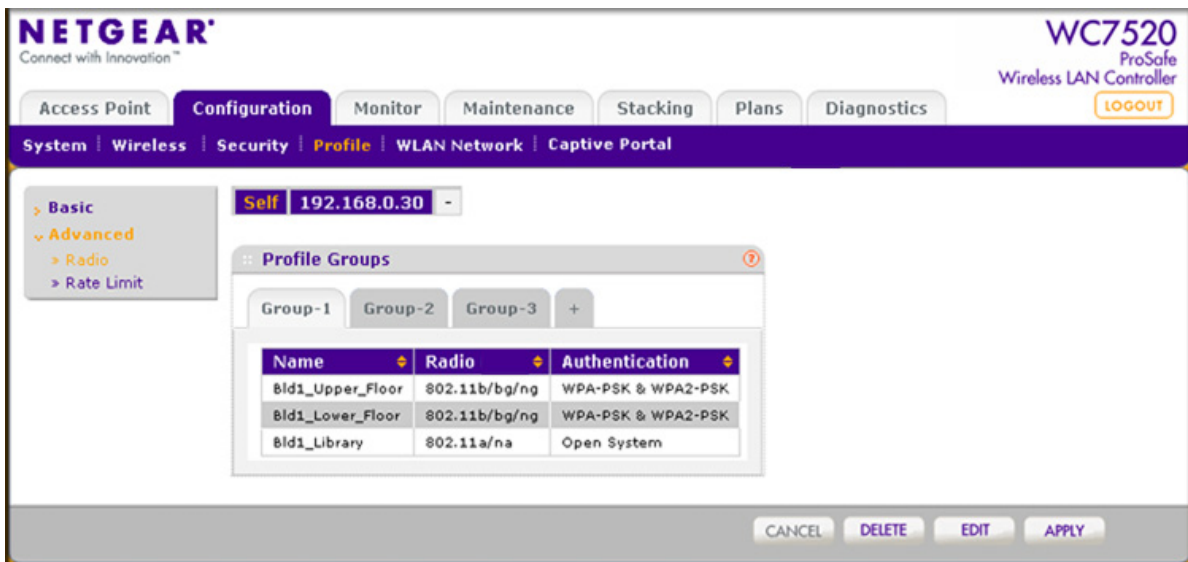


Figure 9.

## Choose a Location for the Wireless Controller

The wireless controller is suitable for use in an office environment where it can be freestanding on its runner feet or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the wireless controller in a wiring closet or equipment room. A mounting kit, containing two mounting brackets and screws, is provided in the wireless controller package.

Consider the following when deciding where to position the wireless controller:

- The unit is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the wireless controller, see [Appendix A, Factory Default Settings and Technical Specifications](#).

## Deploy the Wireless Controller

➤ **To deploy the wireless controller:**

1. Disconnect the wireless controller from the computer and place it where you will deploy it. If necessary, you can now reconfigure the computer that you used in the configuration process back to its original TCP/IP settings.
2. Connect an Ethernet cable from your wireless controller to a LAN port on your network.
3. Connect the power cord to the wireless controller and plug the power cord into a power outlet. The Power, Test, and Ethernet LEDs should light up. If any of these do not light up, see [Troubleshoot Basic Functioning](#) on page 194.

# System Planning and Deployment Scenarios

---

# 2

This chapter includes the following sections:

- *System Planning*
- *Management VLAN and Data VLAN Strategies*
- *Deployment Scenarios*

## System Planning

This section includes the following subsections:

- *Preinstallation Planning*
- *Before You Configure a Wireless Controller*
- *Single Controller Configuration with Basic Profile Group*
- *Single Controller Configuration with Advanced Profile Groups*
- *Stacked Controller Configuration*

### Preinstallation Planning

Before you install any wireless controllers, determine the following:

- Number of access points required to provide seamless coverage
- Number of wireless controllers required
- 802.11 frequency band and the channels that are optimal for Wi-Fi usage

NETGEAR recommends that you perform a site survey:

- Run a spectrum analysis of channels of the site to determine the current RF behavior and detect both 802.11 and non-802.11 noise.
- Run an access point-to-client connectivity test to determine the maximum throughput achievable on the client.
- Identify potential RF obstructions and interference sources.
- Determine areas where denser coverage might be required because of heavier usage.

After the survey is complete, use the collected data to set up an RF plan. For more information, see [RF Planning Overview](#) on page 41.

## Before You Configure a Wireless Controller

These sections assume that you have deployed at least one wireless controller in your network and are ready to configure the wireless controller. For information about how to deploy the wireless controller in your network, see the *WC7520 ProSafe Wireless Controller Installation Guide* that you can access from [http://kb.netgear.com/app/products/model/a\\_id/13060](http://kb.netgear.com/app/products/model/a_id/13060).

For many configurations, you can use the default wireless settings. The IP address, VLAN, DHCP server, client authentication, and data encryption settings are specific to your environment. Following are short sections that discuss these settings (with the exception of IP address settings, which are self-explanatory). For information about how to configure these settings, see the relevant sections.

### VLANs

The management VLAN is the dedicated VLAN for access to the wireless controller. All traffic that is directed to the wireless controller, including HTTP, HTTPS, SNMP, and SSH traffic, is carried over the management VLAN.

If the management VLAN is also configured as a tagged VLAN (the most common configuration), the packets to and from the wireless controller carry the 802.1Q VLAN header with the assigned VLAN number. If the management VLAN is marked as untagged, the packets that are sent from the wireless controller do not carry the 802.1Q header, and all untagged packets that are sent to the wireless controller are treated as management VLAN traffic.

---

**Note:** Use a tagged VLAN or change the tagged VLAN ID only if the hubs and switches on your LAN support 802.1Q. If they do not, and you have not specifically configured a tagged VLAN with the same VLAN ID on the hubs and switches in your network, IP connectivity might be lost.

---

The wireless controller needs to have IP connectivity with the access points through the management VLAN. If the wireless controller and the access points are on different management VLANs, external VLAN routing needs to allow IP connectivity between the wireless controller and the access points.

For information about how to configure management VLANs, see [Configure IP and VLAN Settings](#) on page 65.

## Client VLANs

Each authenticated wireless user is placed into a VLAN that determines the user's DHCP server, IP address, and Layer 2 connection. Although you could place all authenticated wireless users into the single VLAN that is specified in the basic security profile, the wireless controller allows you to group wireless users into separate VLANs based on the wireless SSID to differentiate access to network resources. For example, you might place authorized employee users into one VLAN, and itinerant users, such as contractors or guests, into a separate VLAN. To use different VLANs, you need to create different security profiles.

For information about how to configure regular VLANs, see [Manage Rogue Access Points](#) on page 113.

## DHCP Server

The wireless controller can function as a DHCP server and assign IP addresses to both wireless and wired devices that are connected to it. You can add up to 64 DHCP server pools, each assigned to a different VLAN.

## Client Authentication and Data Encryption

A user needs to authenticate to the WLAN to be able to access WLAN resources. The wireless controller supports several types of security methods, including those that require an external RADIUS or LDAP authentication server.

The encryption option that you can select depends upon the authentication method that you have selected. The following table lists the authentication methods available, with their corresponding encryption options:

**Table 2. Authentication and encryption options**

| Authentication method | Encryption option               | Authentication server   |
|-----------------------|---------------------------------|---|
| Open system           | 64-bit, 128-bit, or 152-bit WEP | None  |
| Shared Key            | 64-bit, 128-bit, or 152-bit WEP | None  |
| WPA-PSK               | TKIP or TKIP+AES                | None  |
| WPA2-PSK              | AES or TKIP+AES                 | None  |
| WPA-PSK and WPA2-PSK  | TKIP+AES                        | None  |
| WPA                   | TKIP or TKIP+AES                | One of the following authentication servers: <ul style="list-style-type: none"> <li>External RADIUS server</li> <li>Internal authentication server</li> <li>External LDAP server</li> </ul> |

**Table 2. Authentication and encryption options (continued)**

| Authentication method | Encryption option | Authentication server   |
|-----------------------|-------------------|---|
| WPA2                  | AES or TKIP+AES   | One of the following authentication servers: <ul style="list-style-type: none"> <li>• External RADIUS server</li> <li>• Internal authentication server</li> <li>• External LDAP server</li> </ul> |
| WPA and WPA2          | TKIP+AES          | One of the following authentication servers: <ul style="list-style-type: none"> <li>• External RADIUS server</li> <li>• Internal authentication server</li> <li>• External LDAP server</li> </ul> |

For information about how to configure client authentication and data encryption, see [Manage Rogue Access Points](#) on page 113.

For information about how to configure authentication servers, see [Manage Authentication Servers and Authentication Server Groups](#) on page 122.

## Single Controller Configuration with Basic Profile Group

A basic configuration consists of a single wireless controller that controls a collection of access points that are organized into the basic default group.

### ➤ To set up a single wireless controller system with a basic profile group:

| Step | Configuration  | Web management interface path  |
|------|--|--|
| 1.   | Optional: Create an RF plan.   | <b>Plans &gt; Layout</b>   |
| 2.   | If you have not yet done so, configure the system settings of the wireless controller:                       |  |
|      | 1. Configure the country code of operation.  | <b>Configuration &gt; System &gt; General</b>                            |
|      | 2. Configure the IP address of wireless controller.  | <b>Configuration &gt; System &gt; IP/VLAN</b>                            |
|      | 3. Verify that VLAN 1 is set as the management VLAN and is marked as untagged, which is the default setting. |  |
| 3.   | Configure up to 8 profiles, and for each profile, do at least the following:                                 |  |
|      | 1. Configure an SSID for wireless access.  | <b>Configuration &gt; Profile &gt; Basic</b>                             |
|      | 2. Configure the network authentication and data encryption.   |  |
|      | 3. Assign the VLAN.  |  |
|      | If required, configure the authentication server.  | <b>Configuration &gt; Security &gt; Basic &gt; Authentication Server</b> |
| 4.   | Run the Discovery Wizard and add the access points to the managed access point list.                         | <b>Access Point &gt; Discovery Wizard</b>                                |

## Single Controller Configuration with Advanced Profile Groups

A more complex configuration consists of a single wireless controller that controls a collection of access points that are organized in access point profile groups and might use several profiles in each access point profile group.

➤ **To set up a single wireless controller system with advanced profile groups:**

| Step   | Configuration   | Web management interface path                   |
|--|---|---|
| 1.   | Optional: Create an RF plan.  | <b>Plans &gt; Layout</b>                        |
| 2.   | If you have not yet done so, configure the system settings of the wireless controller:  |   |
|  | 1. Configure the country code of operation.   | <b>Configuration &gt; System &gt; General</b>   |
|  | 2. Configure the IP address of wireless controller.   | <b>Configuration &gt; System &gt; IP/VLAN</b>   |
|  | 3. Verify that VLAN 1 is set as the management VLAN and is marked as untagged, which is the default setting.                    |   |
| 3.   | Configure up to 8 access point profile <i>groups</i> , and for each access point profile in a group, do at least the following: |   |
|  | 1. Configure an SSID for wireless access.   | <b>Configuration &gt; Profile &gt; Advanced</b> |
|  | 2. Configure the network authentication and data encryption.  |   |
|  | 3. Assign the VLAN.   |   |
| 4. If required, configure the authentication server. | <b>Configuration &gt; Security &gt; Advanced &gt; Authentication Server</b>   |   |
| 5.   | Run the Discovery Wizard and add the access points to the managed access point list.  | <b>Access Point &gt; Discovery Wizard</b>       |
| 6.   | Assign the access points to the access point profile <i>groups</i> (also referred to as WLAN groups).                           | <b>Configuration &gt; WLAN Network</b>          |

## Stacked Controller Configuration

A stacked controller configuration can consist of up to three wireless controllers and up to 150 access points.

➤ **To set up a stacked controller configuration:**

| Step | Configuration   | Web management interface path  |
|------|---|--|
| 1.   | On each individual wireless controller that you intend to make a stack member, follow the configuration steps as explained in one of the previous sections.<br><br><b>Note:</b> If the stack members will be on different floors or in different buildings, you can configure a separate access point profile group for each building or floor. | See <a href="#">Single Controller Configuration with Basic Profile Group</a> on page 30 or <a href="#">Single Controller Configuration with Advanced Profile Groups</a> on page 31 |
| 2.   | Configure the primary wireless controller and deploy it in the network.   |  |
| 3.   | Configure the secondary wireless controllers and deploy them in the network.  |  |
| 4.   | Interconnect the wireless controllers that you intend to make members of the stack. The connection needs to be a wired connection but does not need to be a direct connection, that is, a switch or router can be located in between the wireless controllers that are part of a stack.   |  |
| 5.   | Configure the stacking group on the wireless controller that you intend as the primary controller.  | <b>Stacking &gt; Stacking</b>  |
| 6.   | Synchronize all wireless controllers that are members of the stack.   |  |

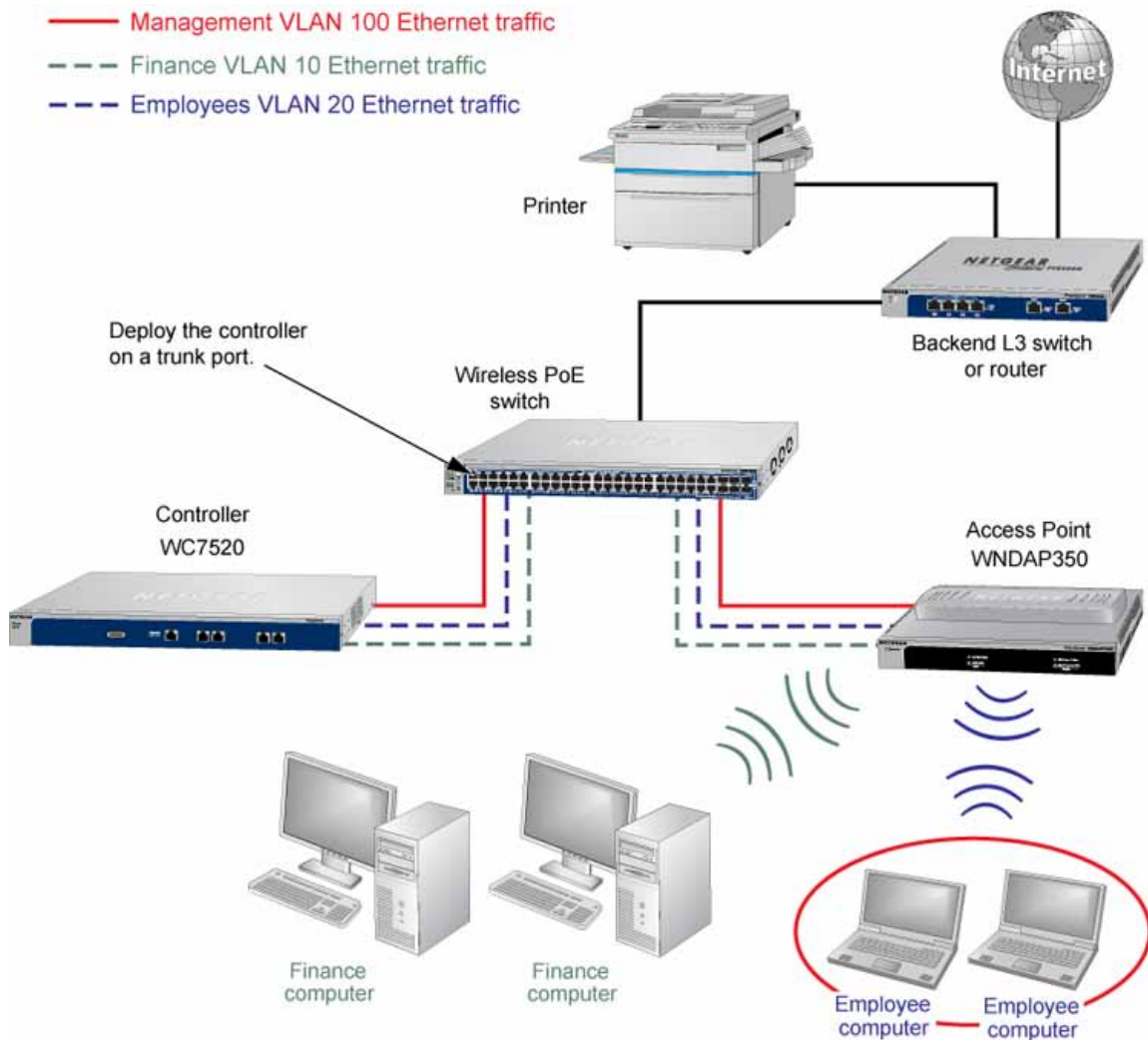
## Management VLAN and Data VLAN Strategies

If your network includes 10 or more access points, NETGEAR recommends that you set up at least two VLAN groups: a management VLAN group and a data VLAN group. If your network is large, you should create a number of data VLAN groups. Setting up data VLANs for clients allows you to:

- Segregate traffic by user category
- Create different policies such as access policies that are based on user category

The following illustration shows a simplified view of how you can use VLANs to segregate traffic by user category:





**Figure 10.**

The wireless controller uses the management VLAN to continually exchange packets with the access points. For large networks, if all traffic uses a single VLAN, the client traffic could potentially flood the network. If this happens, and the wireless controller is not able to exchange packets with the access points, it can cause network performance to slow down, and the access points can lose their connectivity with the wireless controller.

You should deploy the wireless controller on a trunk port on your switch. The trunk port should have access to all VLANs. Use a high-speed port on your switch as the trunk port to accommodate the traffic load of the trunk.

## Deployment Scenarios

This section provides three deployment scenarios to illustrate how the wireless controller can function in a variety of network configurations:

- *Scenario Example 1: Basic Network with Single VLAN*
- *Scenario Example 2: Advanced Network with VLANs and SSIDs*
- *Scenario Example 3: Advanced Network with Redundancy*

### Scenario Example 1: Basic Network with Single VLAN

The following sample scenario consists of a simple network with a wireless controller, PoE switch, Layer 3 switch or router, and access points:

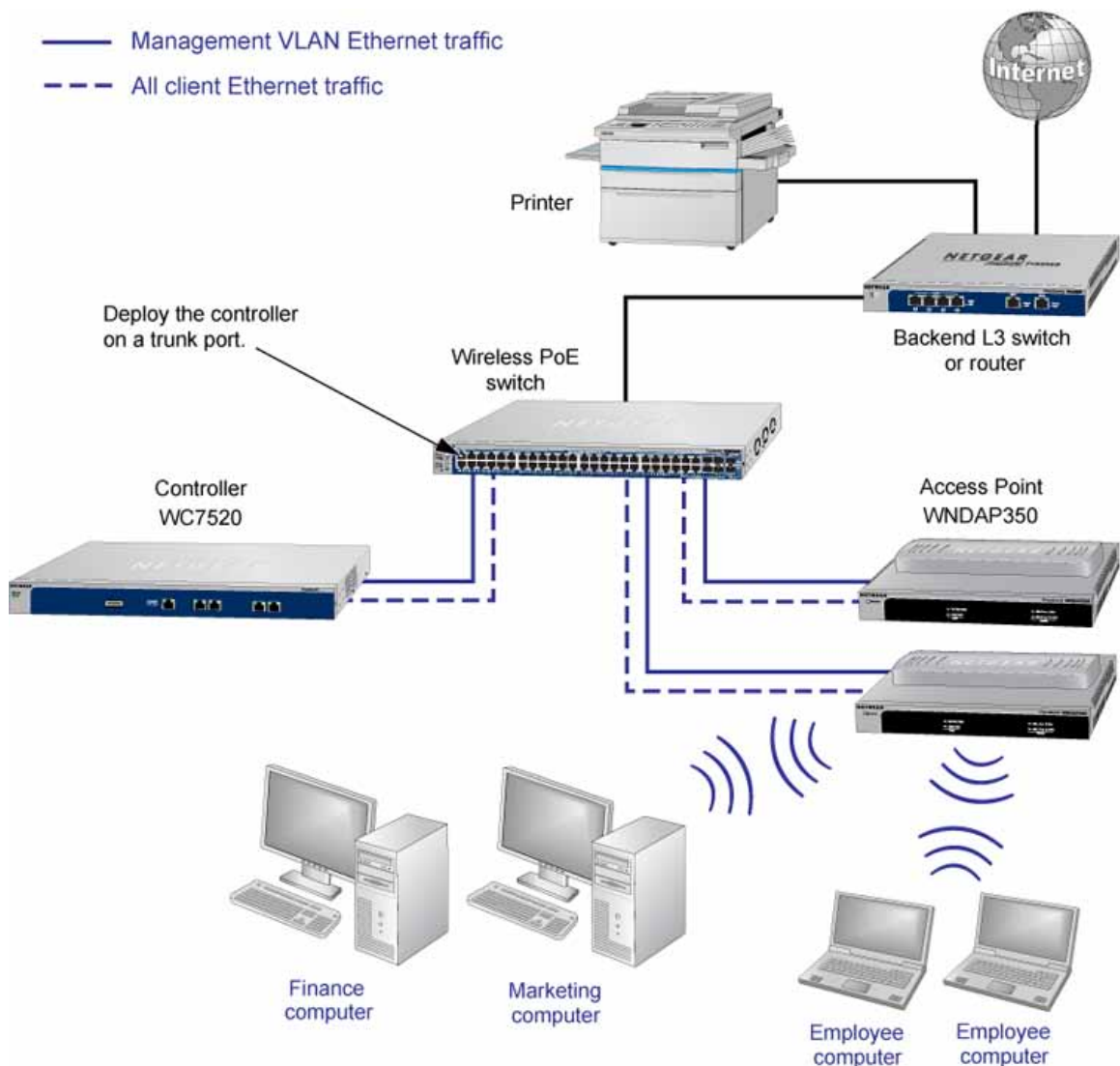


Figure 11.

The access points and wireless controller are connected in the same subnet and use the same IP address range that is assigned for that subnet. There are no routers between the access points and the wireless controller. The access points are connected to a PoE switch, which, in turn, is connected to the wireless controller. The uplink of PoE switch connects to a Layer 3 switch or router that provides Internet access.

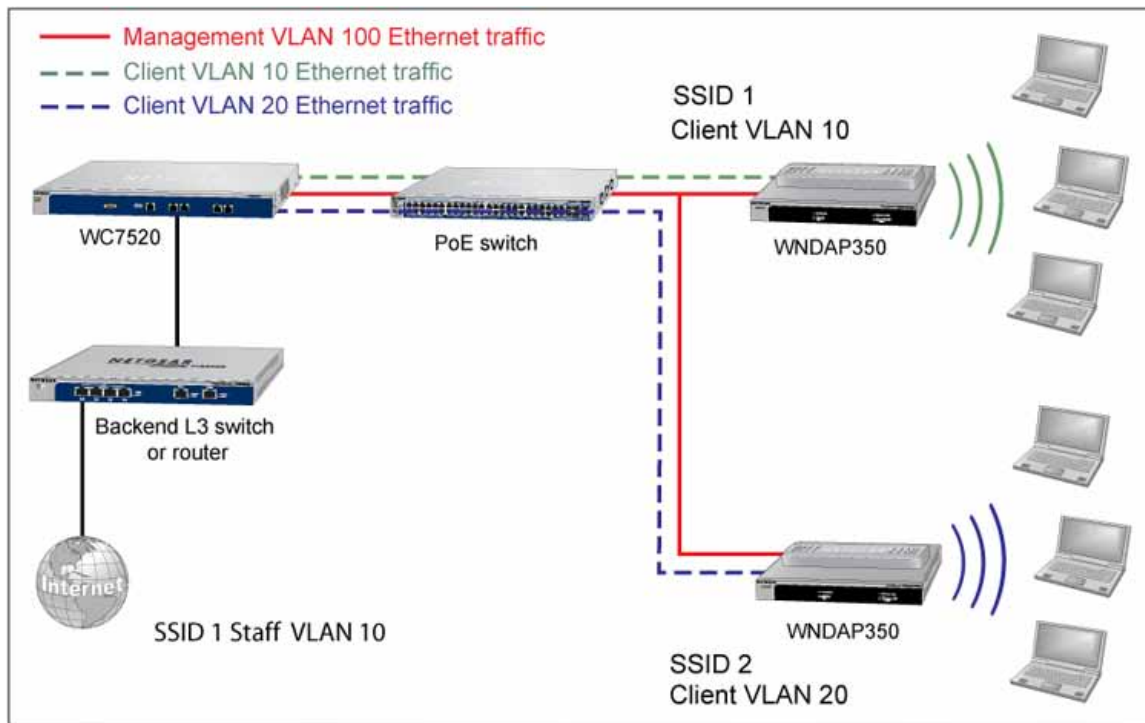
### Provisioning the Wireless Controller

| Step | Configuration   | Web management interface path    |
|------|---|----------------------------------|
| 1.   | Configure the basic system settings:  |                                  |
|      | 1. Configure the country code of operation.   | Configuration > System > General |
|      | 2. Configure the IP address of wireless controller.   | Configuration > System > IP/VLAN |
|      | 3. Verify that VLAN 1 is set as the management VLAN and is marked as untagged, which is the default setting.  |                                  |
| 2.   | Configure the basic wireless settings and security:   |                                  |
|      | 1. Configure an SSID for wireless access.   | Configuration > Profile > Basic  |
|      | 2. Configure the network authentication and data encryption.  |                                  |
|      | 3. Configure the encryption.  |                                  |
| 3.   | Use any port of the wireless controller to connect the wireless PoE switch.   |                                  |
| 4.   | Deploy the access points and connect them to the same wireless PoE switch.  |                                  |
| 5.   | Run the Discovery Wizard, select the network layout, and select the access points that you want to be managed by the wireless controller.<br><br><b>Note:</b> By default, all access points are added to the basic group and all settings from the basic group (profile definition, client authentication, authentication settings, and wireless QoS) are applied to the access points. | Access Point > Discovery Wizard  |

### Scenario Example 2: Advanced Network with VLANs and SSIDs

The following sample scenario consists of an advanced network with a wireless controller, PoE switch, Layer 3 switch or router, access points, and several VLANs and SSIDs. These are the VLANs in the wireless controller system:

- VLAN 1, the default untagged VLAN to access the wireless controller
- VLAN 10, a tagged client VLAN
- VLAN 20, another tagged client VLAN
- VLAN 100, a tagged management VLAN



**Figure 12.**

The access points and wireless controller are connected in the same subnet and same VLAN and use the same IP address range that is assigned for that subnet. There are no routers between the access points and the wireless controller. The access points are connected to a PoE switch, which, in turn, is connected to the wireless controller. The uplink of the PoE switch connects to a Layer 3 switch or router that provides Internet access.

### **Prerequisites**

This network configuration has the following prerequisites:

- VLANs 10, 20, and 100 are tagged VLANs and are configured on both the wireless controller and the PoE switch.
- The wireless controller is connected to the PoE switch through default VLAN 1. You manage the wireless controller from a computer over VLAN 1 through the PoE switch.
- The DHCP server on the wireless controller is configured in management VLAN 100 to enable the access points to receive an IP address through VLAN 100.
- The PoE switch port to which the wireless controller is connected is configured as a tagged port to allow tagged traffic from VLAN 100.

## Provisioning the Wireless Controller

| Step | Configuration   | Web management interface path                     |
|------|---|---|
| 1.   | For initial discovery and configuration of the access points, temporarily configure management VLAN 100 as an untagged management VLAN on both the wireless controller and the PoE switch.  | <b>Configuration &gt; System &gt; IP/VLAN</b>     |
| 2.   | Configure the basic system settings:  |   |
|      | 1. Configure the country code of operation.   | <b>Configuration &gt; System &gt; General</b>     |
|      | 2. Configure the IP address of wireless controller.   | <b>Configuration &gt; System &gt; IP/VLAN</b>     |
|      | 3. Configure the management VLAN as VLAN 100.   |   |
| 3.   | 4. Clear the <b>Untagged Vlan</b> check box. This changes VLAN 1 to a tagged VLAN.  |   |
|      | Add a DHCP server that uses VLAN 100:   |   |
|      | 1. Configure the IP address range for VLAN 100.   | <b>Configuration &gt; System &gt; DHCP Server</b> |
|      | 2. Configure the other DHCP server fields, including the gateway and DNS servers.   |   |
| 4.   | Configure the following profiles, and configure network authentication and data encryption for these profiles:  |   |
|      | 1. A profile with SSID 1 and VLAN 10.   | <b>Configuration &gt; Profile &gt; Basic</b>      |
|      | 2. A profile with SSID 2 and VLAN 20.   |   |
| 5.   | Connect the wireless controller to the PoE switch.  |   |
| 6.   | Before you connect the access points to the PoE switch, verify that the switch ports to which you intend to connect the access points are configured as access ports in management VLAN 100.  |   |
| 7.   | Deploy the access points and connect them to the designated PoE switch ports.   |   |
| 8.   | Wait until the access points are up and running, run the Discovery Wizard, specify the network layout by selecting the <b>Same L2 network</b> radio button, and select the access points that you want to be managed by the wireless controller.<br><br><b>Note:</b> By adding the access points to managed list, you enable them to receive an IP address from the DHCP server over management VLAN 100. | <b>Access Point &gt; Discovery Wizard</b>         |

| Step | Configuration  | Web management interface path |
|------|--|-------------------------------|
| 9.   | For each access point on the managed list, clear the <b>Untagged Vlan</b> check box and configure VLAN 100 as the management VLAN. Doing so causes the access points to lose connectivity with the wireless controller.  |                               |
| 10.  | Restore connectivity between the access points and the wireless controller by changing the PoE switch ports to which the access points are connected to tagged ports. (During the discovery process, these switch ports were access ports in management VLAN 100.) |                               |

### Scenario Example 3: Advanced Network with Redundancy

The following sample scenario consists of an advanced network with one wireless controller, one redundant wireless controller, one core switch, two PoE switches in different buildings, access points, and several VLANs and SSIDs. These are the components in the wireless controller system:

- One wireless controller
- 50 access points (managed by the wireless controller through management VLAN 1)
- One redundant wireless controller
- Four VLANs: VLAN 10, VLAN 20, VLAN 30, and VLAN 40
- Three SSIDs: SSID 1, SSID 2, and SSID 3

In this scenario, the VLANs and SSIDs are used to accommodate traffic for different user groups in a school that is spread out over two buildings.

- Building 1:
  - SSID 1 in VLAN 10 for staff traffic
  - SSID 2 in VLAN 20 for middle school students
  - SSID 3 in VLAN 30 for guests
- Building 2:
  - SSID 1 in VLAN 10 for staff traffic
  - SSID 2 in VLAN 40 for high school students
  - SSID 3 in VLAN 30 for guests

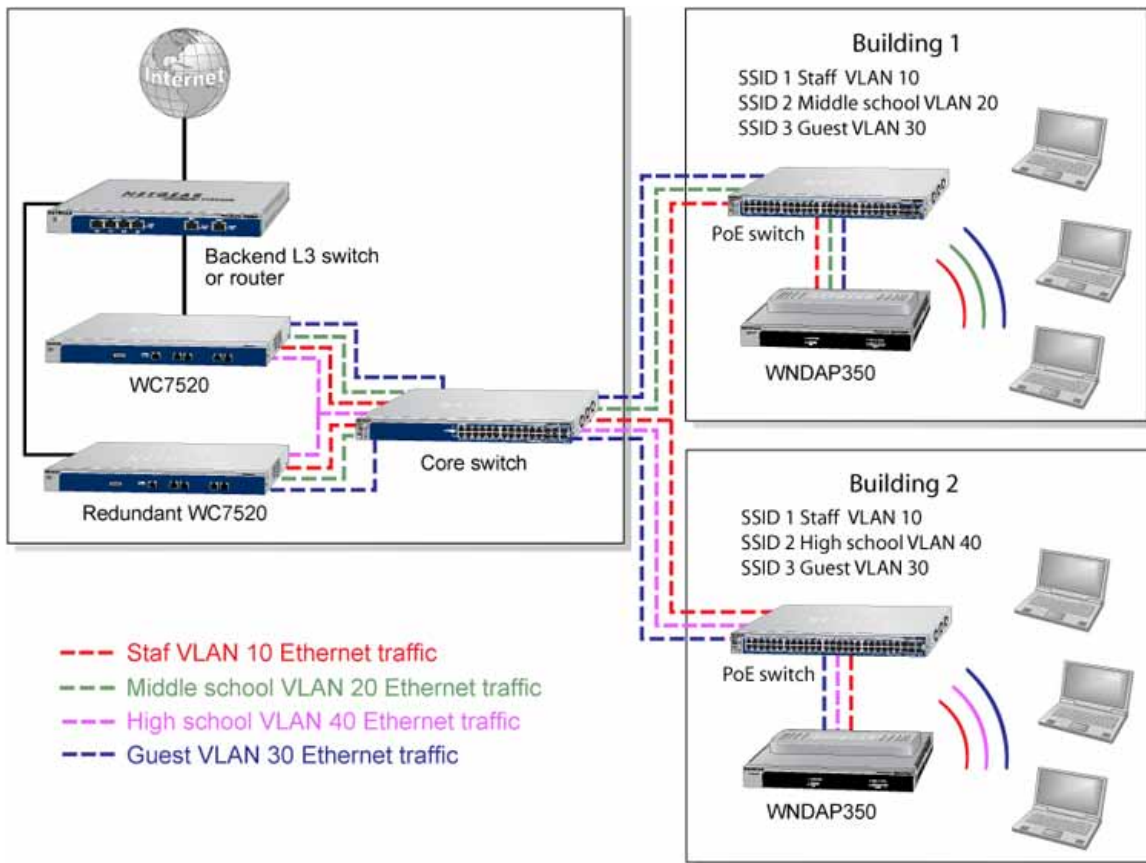


Figure 13.

The access points and wireless controllers are connected in the same subnet and same VLAN and use the same IP address range that is assigned for that subnet. The core switch is located between the wireless controllers and the PoE switches, to which the access points are connected. The core switch provides Internet access.

### Prerequisites

This network configuration has the following prerequisites:

- VLAN 1 is configured on the wireless controllers, core switch, and PoE switches. This VLAN is untagged.
- VLANs 10, 20, and 30 are configured on the wireless controllers, core switch, and the PoE switch in Building 1. These VLANs are tagged.
- VLANs 1, 10, 20, 30, and 40 are configured on the wireless controllers, core switch, and PoE switches. Except for VLAN 1, these VLANs are tagged.

## Provisioning the Wireless Controller

| Step | Configuration   | Web management interface path                   |
|------|---|---|
| 1.   | Configure the basic system settings:  |   |
|      | 1. Configure the country code of operation.   | <b>Configuration &gt; System &gt; General</b>   |
|      | 2. Configure the IP address of wireless controller.   | <b>Configuration &gt; System &gt; IP/VLAN</b>   |
|      | 3. Verify that VLAN 1 is set as the management VLAN and is marked as untagged, which is the default setting.  |   |
| 2.   | Configure the following profiles, and configure network authentication and data encryption for these profiles:  |   |
|      | 1. A profile with SSID 1 and VLAN 10.   | <b>Configuration &gt; Profile &gt; Basic</b>    |
|      | 2. A profile with SSID 2 and VLAN 20.   |   |
|      | 3. A profile with SSID 2 and VLAN 30.   |   |
|      | 4. A profile with SSID 3 and VLAN 40.   |   |
| 3.   | Configure the following profile groups:   |   |
|      | 1. A profile group with the name Building 1, to which you add the following profiles: <ul style="list-style-type: none"> <li>- The profile with SSID 1 and VLAN 10</li> <li>- The profile with SSID 2 and VLAN 20</li> <li>- The profile with SSID 2 and VLAN 30</li> </ul> | <b>Configuration &gt; Profile &gt; Advanced</b> |
|      | 2. A profile group with the name Building 2, to which you add the following profiles: <ul style="list-style-type: none"> <li>- The profile with SSID 1 and VLAN 10</li> <li>- The profile with SSID 2 and VLAN 30</li> <li>- The profile with SSID 3 and VLAN 40</li> </ul> |   |
| 4.   | Deploy the access points and connect them to PoE switches.  |   |
| 5.   | Wait until the access points are up and running, run the Discovery Wizard, specify the network layout by selecting the <b>Same L2 network</b> radio button, and select the access points that you want to be managed by the wireless controller.                            | <b>Access Point &gt; Discovery Wizard</b>       |
| 7.   | Assign the access points to the access point profile <i>groups</i> (also referred to as WLAN groups).   | <b>Configuration &gt; WLAN Network</b>          |



This chapter includes the following sections:

- *RF Planning Overview*
- *Define and Edit Buildings and Floors*
- *Specify Access Point Requirements*
- *View and Manage Heat Maps for Deployed Plans*

## RF Planning Overview

You can do the following with RF planning:

- Define WLAN coverage.
- Estimate the number of access points required based on signal quality and number of clients per access point.
- Optimize the placement of access points for the best coverage.
- Monitor WLAN coverage, rogue access points, and blacklisted clients for a plan that is in deployment.
- Identify weak signal spots and dead spots from the coverage hole and add additional access points to mitigate the situation.

RF planning provides a view of each floor, allowing you to specify how Wi-Fi coverage should be provided. It then provides coverage maps and access point placement locations. Real-time calibration lets you visualize the indoor propagation of RF signals to identify areas with weak signal or dead spots and add additional access points in the right location to mitigate the weak signal or dead spots.

## Planning Requirements

Collect the following information before using RF planning to expedite your planning efforts.

- Building dimensions.
- Number of floors.
- Distance between floors.

- Total number of users and number of users per access point.
- Radio type or types.
- Desired data rates for access points.
- Identify areas where you do not necessarily want coverage.
- Identify areas where you cannot deploy an access point.

Use a worksheet similar to the following to collect your information.

**Table 3. Building planning worksheet**

| Building dimensions              |  |
|----------------------------------|--|
| Height                           |  |
| Width                            |  |
| Number of floors                 |  |
| User information                 |  |
| Number of users                  |  |
| Users per access point           |  |
| Radio types                      |  |
| Access point desired signal rate |  |
| 802.11b/bg/ng                    |  |
| 802.11a/na                       |  |
| Don't care/don't deploy areas    |  |
|                                  |  |
|                                  |  |
|                                  |  |

## Define and Edit Buildings and Floors

This section explains how you can define your buildings and floors, and make modifications after you have defined them. You can add a maximum of three local buildings and three remote buildings, a total of six buildings.

### ➤ To define a building:

1. Select **Plans > Layout**. The Layout Buildings screen displays with the Local Building tab and associated screen in view. To define a remote building, click the **Remote Building** tab.

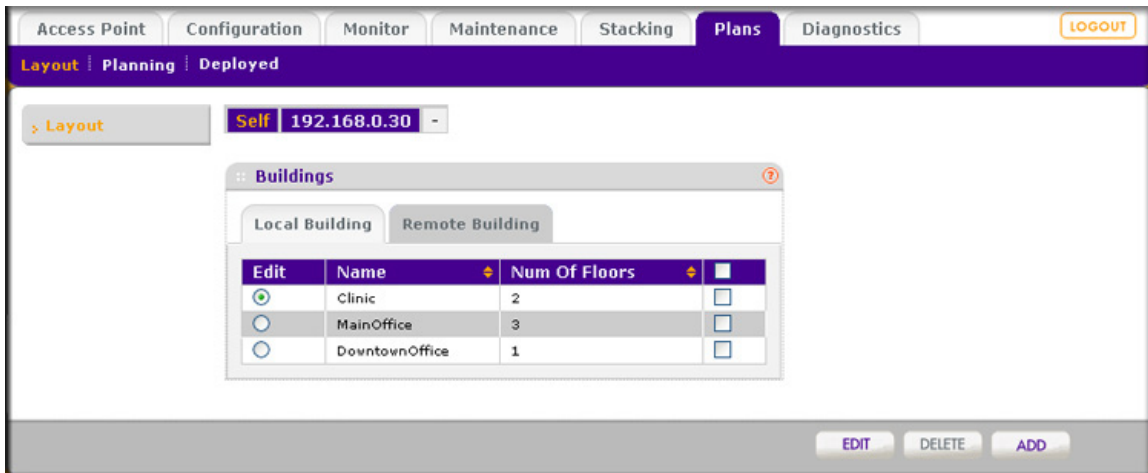


Figure 14.

2. The Buildings table shows the names of the previously defined buildings and their number of floors.
3. To add a building, click **Add**. The Add Building pop-up window displays.
4. Enter a name for your building in the Building Name field, and then click **Add**. The new building is added to the Buildings table. The name is an alphanumeric string up to 64 characters in length.
5. To define the floors of the building, select the radio button that corresponds to the building, and then click **Edit**. The Layout Floors screen displays:

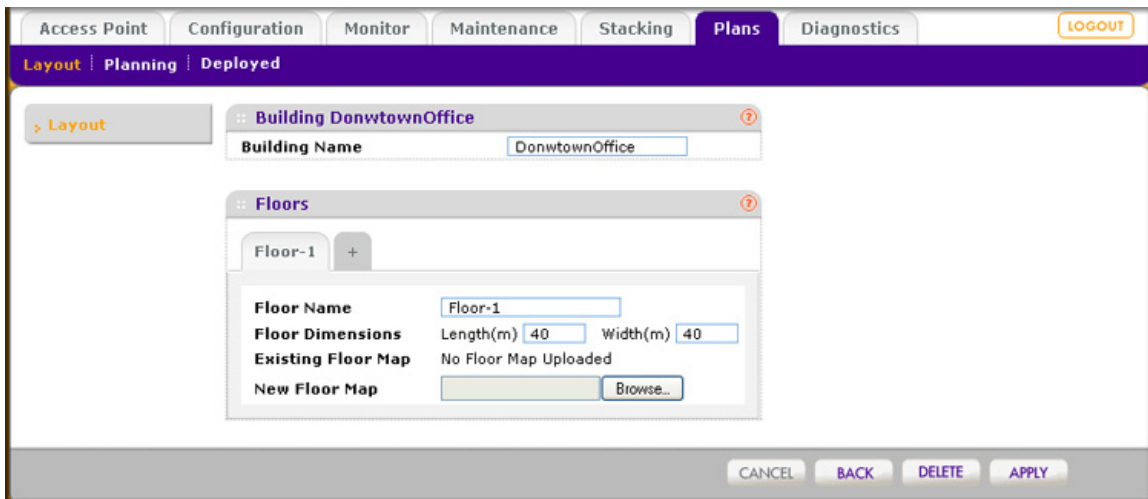


Figure 15.

6. Define the floors as explained in the following table:

**Table 4. Building name and floors**

| Setting            | Description   |
|--------------------|---|
| <b>Building</b>    |   |
| Building Name      | You can modify the previously defined building name, which is an alphanumeric string up to 64 characters in length.   |
| <b>Floors</b>      |   |
| Floor Names        | The floor name is an alphanumeric string up to 64 characters in length.   |
| Floor Dimensions   | Enter the floor length in meters in the Length field; enter the floor width in meters in Width field. The default measurements for both are 40 meters.  |
| Existing Floor Map | If you have imported a floor map, a very small image of the floor map is shown. Click <b>Preview</b> to enlarge the map. (If you did not import a floor map, the Preview button is not displayed.)  |
| New Floor Map      | <p>If you have an existing floor map, import the map into the RF planning tool by clicking <b>Browse</b> and navigating to the location where you have stored the map. Follow the directions of your browser to import the map.</p> <p><b>Note:</b> Background images need to be in JPEG format and cannot exceed 2048 x 2048 pixels in size. If you attempt to import a file with a larger pixel footprint, the image will not scale to fit the image area in the floor display area.</p> <p><b>Note:</b> Images are scaled (stretched) to fit the display area. The display area aspect ratio is determined by the floor dimensions.</p> <p><b>Note:</b> The internal flash memory of the wireless controller supports up to three floor maps. If you want to define additional floors, use external USB storage (see <a href="#">Manage External Storage</a> on page 141).</p> <p><b>Note:</b> Because background images for your floors are embedded in the XML file that defines your building, minimize the file size of the JPEGs that you use for your backgrounds. You can minimize the file size by selecting maximum compression (lowest quality) in most graphics programs.</p> |

7. To add another floor, click the **+** tab next to the Floor-1 name, or whatever name you have given the first floor, and define the floors as explained in [Table 4](#) on page 44. You can add up to six floors in one building but will need external USB storage if you add more than three floor maps.
8. Click **Apply** to save your settings.
9. Click **Back** to return to the Layout Buildings screen.

➤ **To edit a building:**

1. Select the radio button in the Edit column that corresponds to the building that you want to edit.
2. Click **Edit**.

➤ **To delete a building:**

1. Select the check box that corresponds to the building that you want to delete, or select the check box at the top row of the table to delete all buildings.
2. Click **Delete**.

## Specify Access Point Requirements

After you have defined the buildings and floors, you need to specify the following RF requirements for each floor and each supported access point model (WNAP210, WNAP320, WNDAP350, and WNDAP360):

- **Frequency band.** The radio frequency to be used (802.11b/bg/ng or 802.11a/na).
- **Signal quality.** The signal strength that you expect for the WLAN. This setting determines the automatic channel allocation and automatic transmission power of the access points (see the explanation in the table later in this section).
- **Number of client per access point.** The total number of clients that you expect to be supported on each access point.
- **Total number of clients per floor.** The total number of clients that you expect to be supported on each floor.

Along with the floor dimensions, these settings determine the estimated number of access points. A screen lets you visually optimize the access point locations for best coverage.

➤ **To specify the WLAN requirements for a floor, estimate the number of access points required, and view their suggested locations:**

1. Select **Plans > Planning**. The Planning Buildings screen displays with the Local Building tab and associated screen in view. To specify the information for a remote building, click the **Remote Building** tab.

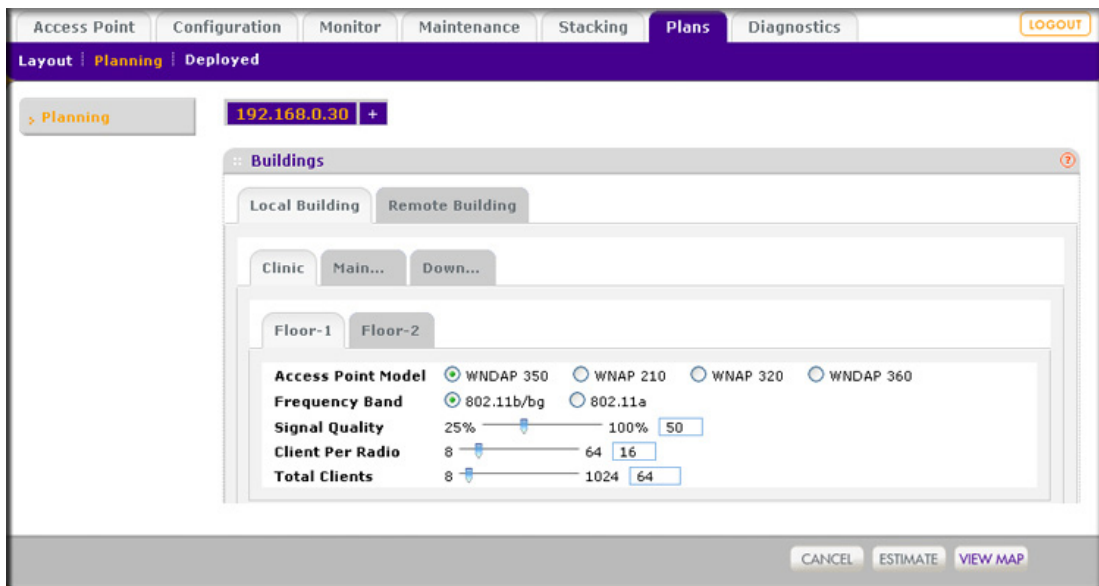


Figure 16.

The Planning Buildings screen shows a tab for each building that you previously defined. For each building, the screen shows the floors that you previously defined.

2. Select the building and floor that you want to configure by clicking the corresponding tabs.
3. Specify the WLAN requirements for the floor as explained in the following table:

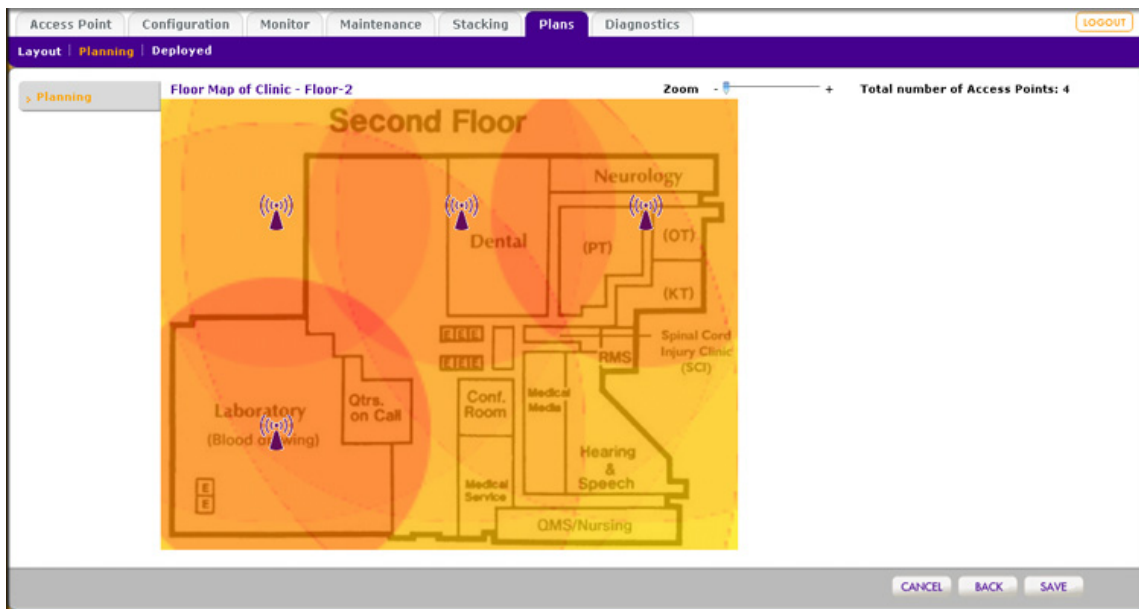
**Table 5. Floor WLAN requirements**

| Setting            | Description  |
|--------------------|--|
| Access Point Model | Specify the access point model that you will use on the floor by selecting the <b>WNDAP 350</b> , <b>WNAP 210</b> , <b>WNAP 320</b> , or <b>WNDAP 360</b> radio button.  |
| Frequency Band     | Select one of the following radio buttons to specify the frequency band that the access points will function in: <ul style="list-style-type: none"> <li>• <b>802.11b/bg/ng</b></li> <li>• <b>802.11a/na</b></li> </ul>             |
| Signal Quality     | Specify the required signal quality by moving the slider or by entering a percentage in the field to the right of the slider. The minimum signal quality is 25 percent; the maximum is 100 percent.                                |
| Client Per Radio   | Specify the expected maximum number of clients per access point by moving the slider or by entering a number in the field to the right of the slider. The maximum number of clients that you can configure per access point is 64. |
| Total Clients      | Specify the expected total number of clients on the floor by moving the slider or by entering a number in the field to the right of the slider. The maximum number of total clients that you can configure on the floor is 1024.   |

4. Click **Estimate** to view the number of access points required for the settings that you entered. The number of access points displays in a pop-up window. Access points that you want to deploy in sentry mode are not included in this number. (For information about sentry mode, see [Edit and Remove Access Point Information](#) on page 59.)

After you have closed the pop-up window, the Estimated Access Points row is added to the Planning Buildings screen.

5. Click **View Map** to view and optimize the suggested approximate access point locations for the settings that you entered:



**Figure 17.**

Note that the planning tool provides only default placement and shows the coverage area for each access point.

6. Move the access points to optimize coverage in desired areas and avoid coverage in unwanted areas based on the floor plan.

Colored circles around the access point symbols indicate the expected approximate coverage of the individual access point. The color of the circle represents the expected quality of the signal strength: a darker color indicates signal overlap with nearby access points.

**Note:** A red color indicates the strongest coverage area: better than  $-50$  dBm RSSI; an orange color better than  $-60$  dBm; a yellow color better than  $-70$  dBm; and so on.

Moderate overlap is required for seamless roaming. No overlap will lead to disconnections and dead spots.

You can click an access point icon and drag it to manually reposition it to see how the new location would affect the coverage. Click **Cancel** to undo any access point repositioning changes.

Use the Zoom slider to increase or decrease the size of the map.

7. Click **Save** to save the location map, or click **Back** to return to the Planning Buildings screen without saving changes to the location map.

---

**Note:** For each floor, you can save one location map only. When you modify and save the location map, the previously saved location map is overwritten.

---

## View and Manage Heat Maps for Deployed Plans

A heat map lets you view in real time, by wireless frequency band, the signal strength and wireless coverage for a building floor. The heat map shows the actual signal strengths that each access point is detecting from neighbor access points.

---

**Note:** For the heat maps to work correctly, the access point placement on the floor plan needs to closely match the actual physical location of the access points.

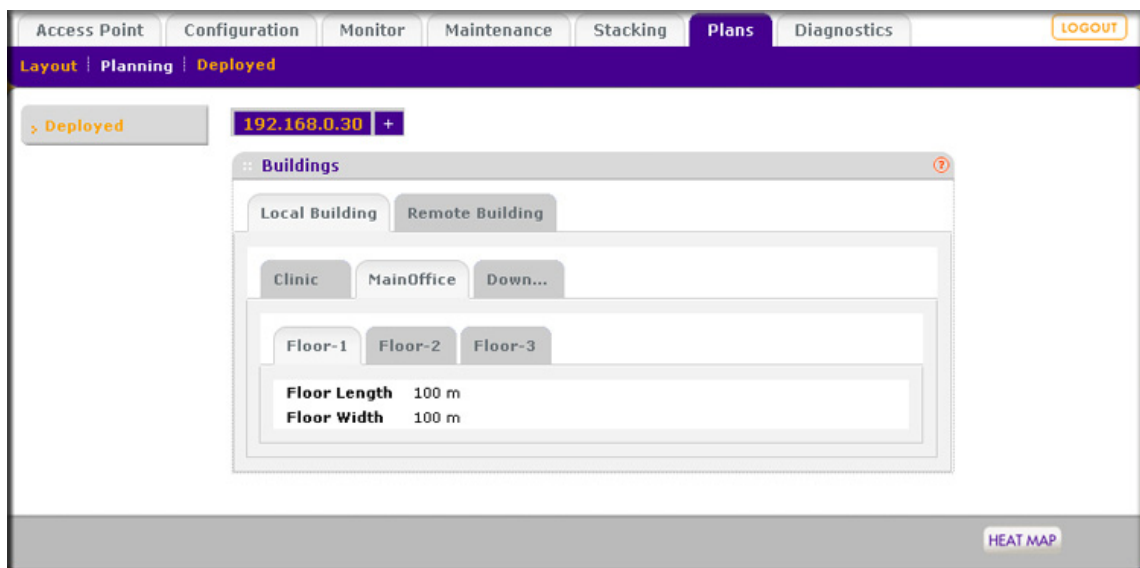
---

The heat map shows the following information:

- Signal strength and wireless coverage, including coverage holes
- Known access points that are managed by the wireless controller
- Location of rogue access points
- Location of clients associated with the access points
- Location of blacklisted clients

➤ **To view the heat map for a building floor and to adjust access points:**

1. Select **Plans > Deployed**. The Deployed Buildings screen displays with the Local Building tab and associated screen in view. To view the information for a remote building, click the **Remote Building** tab.



**Figure 18.**

The Deployed Buildings screen shows a tab for each building that you previously defined. For each building, the screens shows the floors that you previously defined.



2. Select the building and floor for which you want to view the heat map by clicking the corresponding tabs.
3. Click **Heat Map**. The heat map for the selected floor displays:

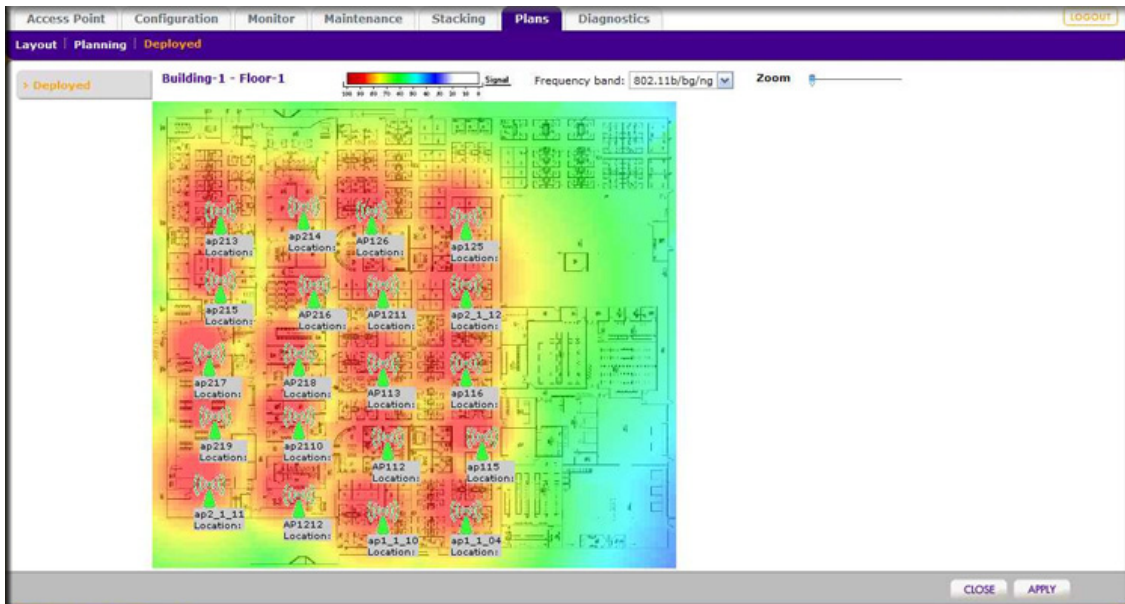


Figure 19.

4. The first time you view the heat map, the access points need to be manually placed on the heat map to closely match their actual physical locations.
5. Click **Apply** to save the locations. Doing so regenerates the complete heat map of the floor.

The spectrum bar at the top of the screen indicates how the colors correspond to the signal strength and wireless coverage.

To view information about an access point or client on the heat map, place your pointer over the icon. The following information becomes available:

- IP address
- MAC address
- Name
- Model
- Status
- Power per channel
- Configured and operating channel bandwidth

To select another wireless frequency band, make a selection from the Frequency band drop-down list above the heat map.

Use the Zoom slider to increase or decrease the size of the map.

6. Make adjustments to the wireless signal strength and coverage in real time by dragging the access point icons to new locations.

The colors disappear from the heat map until you click **Apply** again. When you apply the new position, the heat map is refreshed based on the new location and the RF data collected from the access points.

7. Click **Apply** to view how your changes affect the heat map. Depending on the size of your WLAN, it might take several minutes before the heat map is updated. If you do not want to apply the changes, click **Close** to return to the Deployed Buildings screen.

# Access Point Discovery and Management

---

# 4

This chapter includes the following sections:

- *Access Point Discovery and Discovery Guidelines*
- *Run the Discovery Wizard*
- *Discovery Results*
- *Manage the Access Point List*

## Access Point Discovery and Discovery Guidelines

You need to run the Discovery Wizard for the wireless controller to discover supported NETGEAR access points on the LAN or WAN. The wireless controller can discover access points that are still in their factory default state and access points that are deployed and running. After the access points are discovered, you can add them to the Managed AP List. The wireless controller can configure, manage, and monitor the managed access points.

### Requirements for Autodiscovery of Local Access Points

If the access points still have their factory default settings, the autodiscovery process should work fine. If you changed the access point configuration, make sure that the configuration meets the following general guidelines:

#### *General Guidelines*

- All standalone access points need to have SNMP and SSH enabled.
- UDP port number 7890 needs to be unblocked in the firewall.
- Each access point needs to have an IP address. All access points that are the same model ship with the same default IP address. With the exception of access points in factory default state that are in the same Layer 2 network, if more than one access point has the same IP address, then only one of them is discovered at a time. You have to add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with that IP address.

- An access point needs to run at least its initial firmware release or a newer version. There are no other firmware requirements for the access point to function with the wireless controller.

### ***Guidelines for the Autodiscovery Process Across Layer 3 Networks***

In addition to the previous general guidelines, for the autodiscovery process to work across Layer 3 networks, enable either one of the following options:

- Multicast routing for IP address 254.0.100.250 between the wireless controller and the access points.
- DHCP option 43 (vendor-specific information) on the DHCP server. Specify the wireless controller's IP address in hexadecimal format to allow the access points to receive the wireless controller's IP address and to allow the DHCP server to assign IP addresses to the access points. The hexadecimal address needs to be preceded by the vendor-specific octets 02:04:.

To compose the address, start with 02:04: and then add each of the four address octets in hexadecimal format, separated by colons. For example:

192.168.33.27 in decimal format equals c0:a8:21:1b in hexadecimal format. After you have added the vendor-specific octets, the complete address is 02:04:c0:a8:21:1b.

The DHCP server on the wireless controller automatically enables DHCP option 43 with its own IP address.

## **Requirements for Autodiscovery of Remote Access Points**

The wireless controller can autodiscover remote access point over a site-to-site VPN connection or behind a remote NAT router without a VPN connection. Make sure that the configuration meets the following general guidelines.

### ***Guidelines for the Autodiscovery Process of Remote Access Points***

- All standalone access points need to have SNMP and SSH enabled.
- The following ports need to be unblocked in the firewall at the site where the wireless controller is located in order for the remote access points to communicate with the wireless controller:
  - TCP port 22. Used by Secure Shell (SSH) and Secure Copy (SCP) for the transfer of software images and large configuration files and for the transfer over a tunnel.
  - UDP port 69. Used by TFTP for software image upgrades of standalone access points.
  - UDP port 123. Used by Network Time Protocol (NTP).
  - UDP port 138. Used by NetBIOS to resolve names.
  - UDP port 161. Used by the SNMP discovery process.

- UDP port 6650. Used by the control channel between the wireless controller and the remote access point.
- UDP port 7890. Used by the multicast discovery process. This port does not need to be unblocked in a configuration in which remote access points are located behind a NAT router.
- Enable DHCP option 43 (vendor-specific information) on the DHCP server. Specify the wireless controller's IP address to allow the access points to receive the wireless controller's IP address and the DHCP server to assign IP addresses to the access points.

The DHCP server on the wireless controller automatically enables DHCP option 43 with its own IP address.

- Access points behind a NAT router first need to be converted to managed access points and then be installed behind the NAT router.
- Each access point needs to have an IP address. All access points that are the same model ship with the same default IP address. With the exception of access points in factory default state that are in the same Layer 2 network at the remote site, if more than one access point has the same IP address, then only one of them is discovered at a time. You have to add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with that IP address.
- An access point needs to run at least its initial firmware release or a newer version. There are no other firmware requirements for the access point to function with the wireless controller.

**Tip:** For management and monitoring purposes, make sure that you give the remote access points at one site the same location name and that you create and assign meaningful building and floor names. For information about creating building and floor names, see [Define and Edit Buildings and Floors](#) on page 42; for information about assigning location, building, and floor names, see [Edit and Remove Access Point Information](#) on page 59.

### **Limitations after Discovery**

The following limitations apply after remote access points have been discovered:

- Seamless Layer 2 roaming is supported for the clients of a remote access points, but seamless Layer 3 roaming is not supported for the clients across remote access points. When clients move from one IP subnet to another at the remote site, they are disconnected from their access point and need to reconnect to another access point.
- If a remote access point is disconnected from the wireless controller, for example, because the VPN connection goes down, the following occurs:
  - The remote access point uses its last known configuration and functions as a standalone access point while continuously attempting to reconnect to the wireless controller.
  - If the access point uses WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK authentication, it can continue to accept new clients. If the access point uses RADIUS

authentication with the local RADIUS server of the wireless controller instead of an external RADIUS server, the access point can no longer accept new clients.

- If the access point is rebooted, it loses its configuration.

After the connection with the wireless controller is reestablished, the remote access point functions once again as a managed access point.

## Run the Discovery Wizard

The Discovery Wizard finds access points that are not yet on the managed access point list.

### ➤ To run the Discovery Wizard:

1. Select **Access Point > Discovery Wizard**. The Discovery Wizard screen displays:

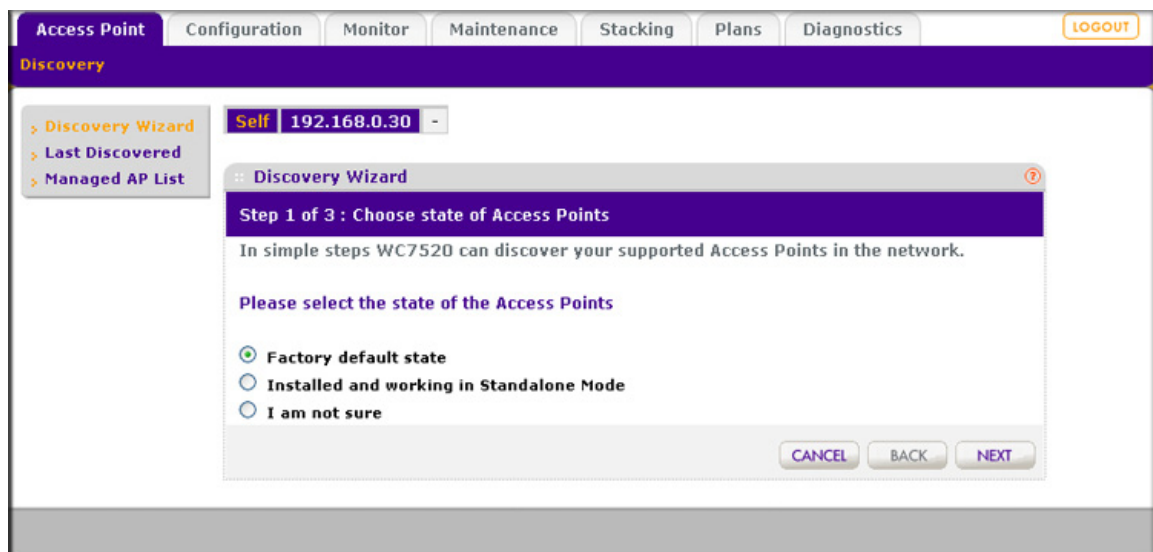


Figure 20.

2. Select the radio button to specify the state of the access points that you want to discover:
  - **Factory default state.** The access points have not been configured.
  - **Installed and working in Standalone Mode.** The access points have been configured or deployed, but they are not yet on the Managed AP List.
  - **I am not sure.** Select this radio button to display documentation.
3. Click **Next**. The next Discovery Wizard screen displays:

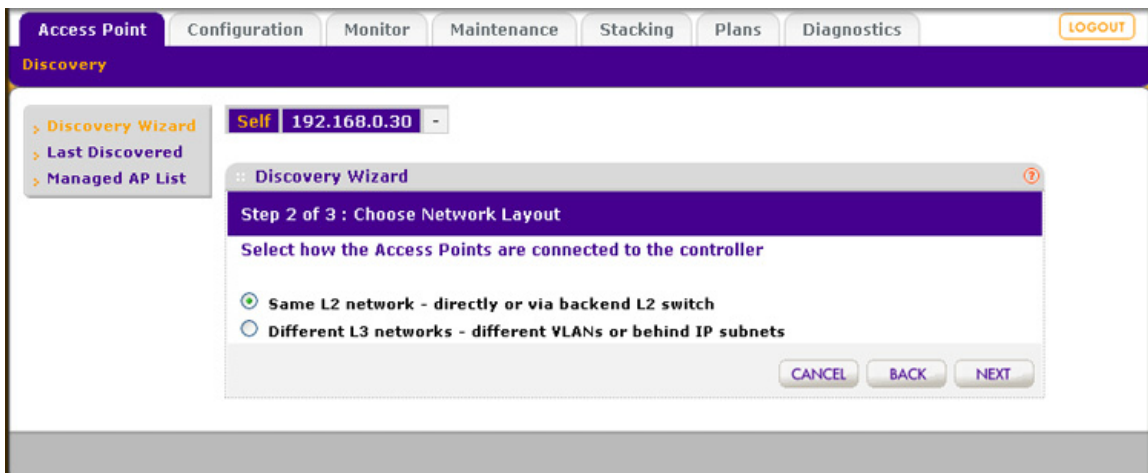


Figure 21.

4. Select the radio button that specifies the network layout of the access points, and click **Next**.
  - **Same L2 network - directly or via backend L2 switch.** Discover all access points on the LAN that are in the same IP subnet and are connected to the wireless controller either directly or through a back-end Layer 2 switch.
  - **Different L3 networks - different VLANs or behind IP subnets.** Discover access points that are in different IP subnets and that are connected to the wireless controller through a router.
5. If prompted, fill in the Start IP and End IP fields to specify a range of IP addresses in which the wireless controller should discover access points:

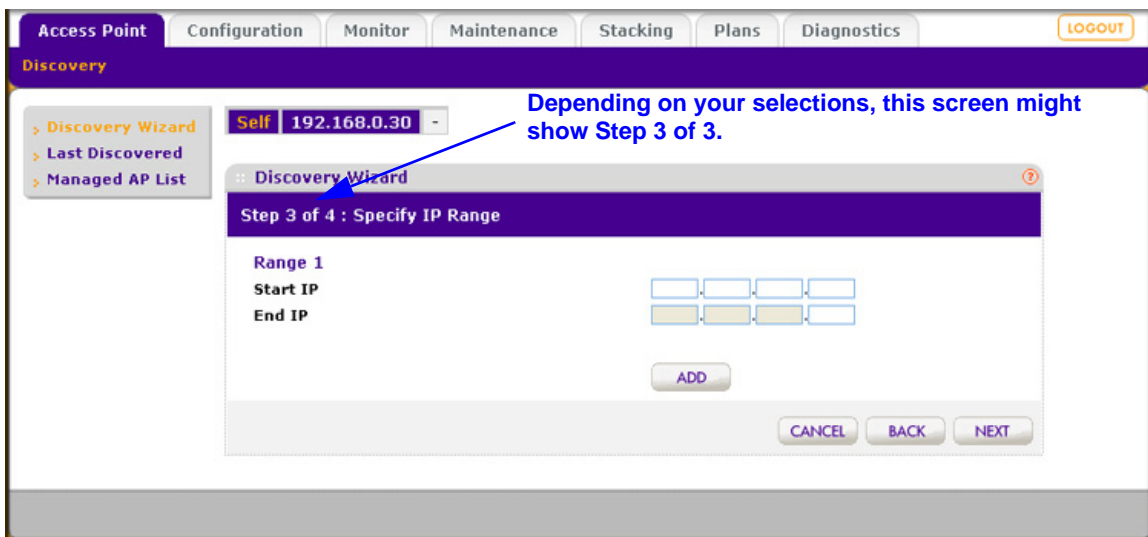


Figure 22.

6. Optional step: Click **Add** to add an additional IP address range for the wireless controller to search in. You can add a maximum of three IP ranges. You can search a maximum of 255 IP addresses at a time. (Do several searches if you have access points in several networks.)

7. Click **Next** to continue. The following occurs:
  - The wireless controller searches for NETGEAR products on the LAN based on MAC address, and then identifies which products are supported access point models.
  - When discovery is finished, the table shows the access points that were located: for each access point, the table includes the model number, IP address, MAC address, and name.

The next Discovery Wizard Select Access Points to Manage screen displays. The following figure shows the screen after the access points have been discovered:

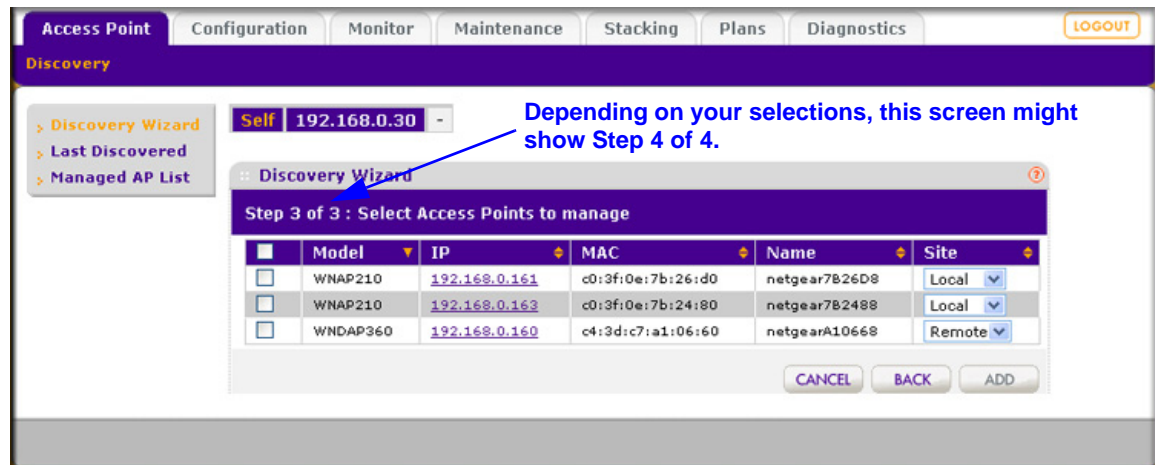


Figure 23.

8. Check the discovery results to make sure that all the access points are listed. See the following section, [Discovery Results](#).
9. Select the site designation and add the access points as described in [Add Access Points to the Managed List after Discovery](#) on page 57.

## Discovery Results

The effectiveness of autodiscovery depends in part on how the access points on your LAN are set up. If each access point is configured with a unique IP address and is running current firmware, then discovery is usually simple.

If the discovery results are not what you expect, check the following:

- Access points already managed by the wireless controller are not in the discovery list. To view the Managed AP List, select **Access Point > Managed AP List**.
- The access points might be in a different IP subnet. Verify that you can ping the access point's IP address from the wireless controller's ping utility (see [Use the Diagnostic Tools on the Wireless Controller](#) on page 200).
- If the access points are in factory default mode and across a router, they are not detected.
- With the exception of access points in factory default state that are in the same layer network, if more than one access point has the same IP address, then only one of them is



discovered at a time. You have to add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with that IP address.

- Make sure that a DHCP server is available in the network or on the wireless controller.

---

**Note:** For troubleshooting information, see *Problems with Access Points* on page 198.

---

## Manage the Access Point List

### Add Access Points to the Managed List after Discovery

After the wireless controller autodiscovers the access points, as explained in *Access Point Discovery and Discovery Guidelines* on page 51, select the site designation and then add the access points to the managed list so that the wireless controller can manage them.

#### ➤ To select the site designation and add discovered access points to the managed list:

1. On the last Discovery Wizard screen (Step 3 of X: Select Access Points to manage; see *Figure 23* on page 56) that displays the discovered access points, select an access point that you want to designate as a remote access point.
2. From the Site drop-down list, select **Remote**. The default is Local. (All access points for which you do not change the site designation to Remote are designated as Local.)
3. Repeat *step 1* and *step 2* for each access point that you want to designate as a remote access point.
4. Select the check boxes for individual access points, or select the check box on the upper left to select all access points.
5. Click **Add**. Depending on the type of access points that have been discovered, a screen that lets you enter or ignore a login name and password might display.

The access points are added to the Managed AP List, and the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller.

- If you want to wait until later to add the discovered access points, you can select **Access Point > Last Discovered** to view the most recently discovered access points. From this screen, you can add the access points to the Managed AP List.
  - After you have added the access points to the Managed AP List, they are removed from the discovery results and the Last Discovered screen.
6. Select **Access Point > Managed AP List**. The Managed AP List screen displays. Because this is a wide screen, it is shown in the following two figures:

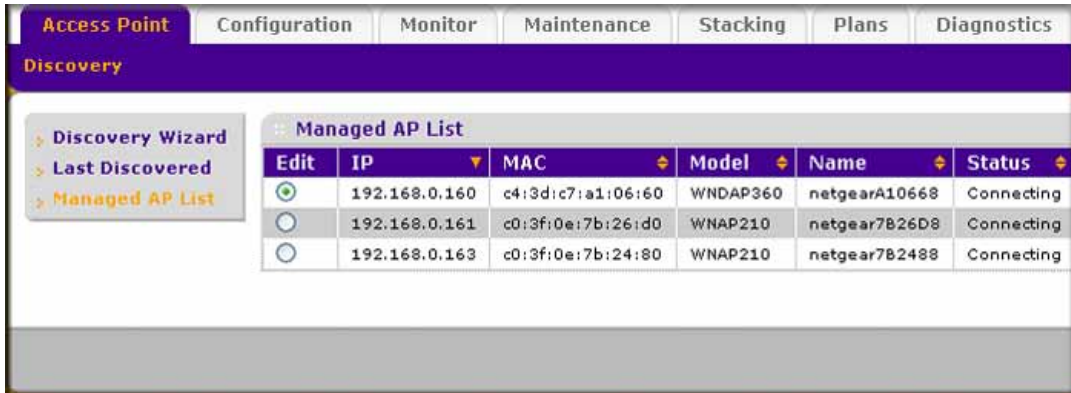


Figure 24. Left side of the Managed AP List screen

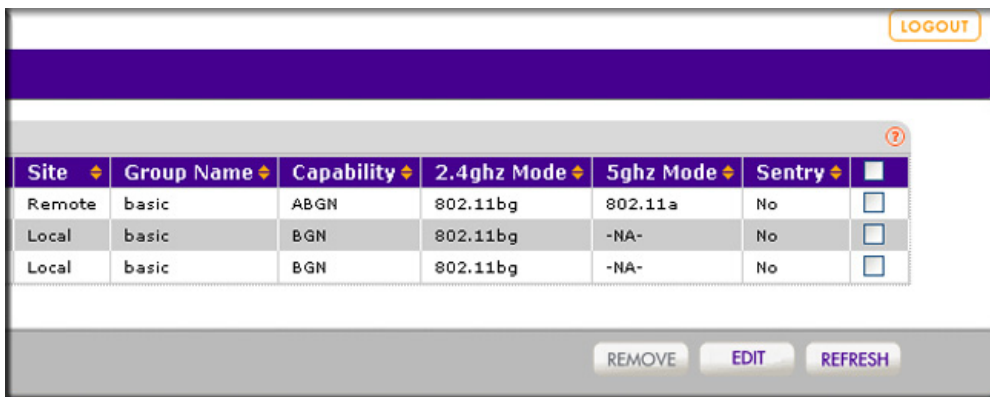


Figure 25. Right side of the Managed AP List screen

The Managed AP List shows the following entries for each access point that you added to the list:

Table 6. Managed AP list information

| Item  | Description                          |
|-------|--------------------------------------|
| IP    | The IP address of the access point.  |
| MAC   | The MAC address of the access point. |
| Model | The model of the access point.       |
| Name  | The name of the access point.        |

Table 6. Managed AP list information (continued)

| Item        | Description  |
|-------------|--|
| Status      | <p>Shows one of the following status options:</p> <ul style="list-style-type: none"> <li>• <b>Authentication in progress.</b> (This status can last several minutes)</li> <li>• <b>Applying configurations.</b></li> <li>• <b>Firmware upgrade.</b></li> <li>• <b>AP is rebooting.</b></li> <li>• <b>Connecting.</b></li> <li>• <b>Connected.</b> This status indicates normal operation.</li> <li>• <b>Not Connected.</b> The wireless controller cannot communicate with the access point at the configured IP address. The wireless controller tries to log in to managed access points each minute. If the error is temporary, the status automatically changes to connected. If the error is prolonged, verify the access point's IP address and network connectivity.</li> </ul> <p><b>Note:</b> Make sure that there is a DHCP server enabled in the network; otherwise, the managed access points remain in the Connecting state and do not enter the Connected state.</p> |
| Site        | <p>Shows whether the access point is a local or remote one:</p> <ul style="list-style-type: none"> <li>• <b>Local.</b> The AP is deployed at the local site.</li> <li>• <b>Remote.</b> The AP is deployed at a remote site.</li> </ul>   |
| Group Name  | The default group is basic.  |
| Capability  | <p>The wireless modes that are supported by the access point.</p> <p><b>Note:</b> Capability information lets you determine which access points are 802.11n mode capable but function in 802.11g mode.</p>   |
| 2.4ghz Mode | The access point's wireless modes that function in the 2.4-GHz band.   |
| 5ghz Mode   | The access point's wireless modes that function in the 5-GHz band.   |
| Sentry      | <p>Shows whether or not sentry mode is enabled:</p> <ul style="list-style-type: none"> <li>• <b>No.</b> Sentry mode is disabled.</li> <li>• <b>Yes.</b> Sentry mode is enabled.</li> </ul>   |

## Edit and Remove Access Point Information

### ➤ To edit an access point in the Managed AP List:

1. Select **Access Point > Managed AP List** to view the Managed AP List (see [Figure 24](#) on page 58 and [Figure 25](#) on page 58).
2. Select the access point that you want to edit by selecting its radio button in the Edit column of the Managed AP List.
3. Click **Edit**. The Edit Access Point screen displays:

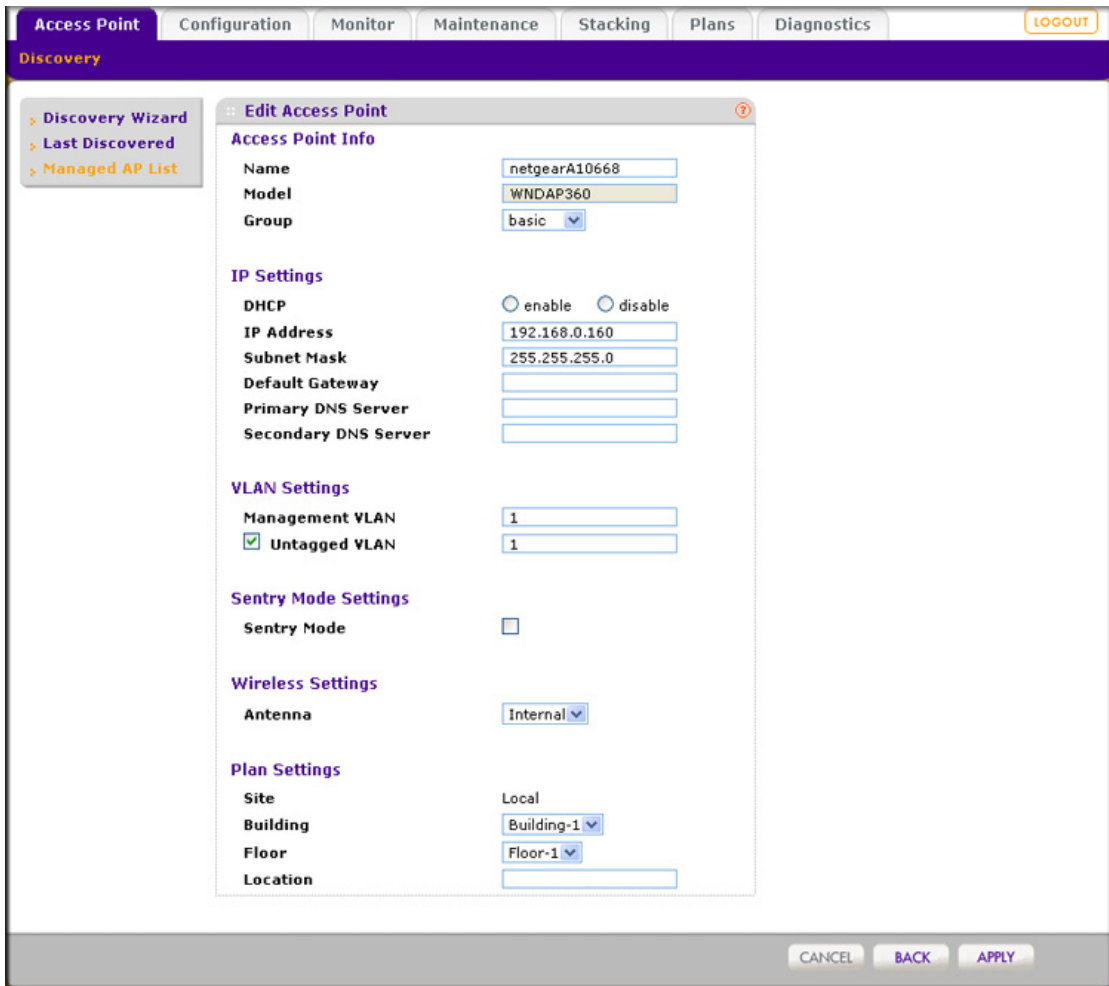


Figure 26.

4. Configure the settings as explained in the following table. Some fields are masked out and cannot be edited; other fields are masked out but *can* be edited.

Table 7. Access point settings

| Setting                          | Description  |
|----------------------------------|--|
| <b>Access Point Info section</b> |  |
| Name                             | Enter a unique value that indicates the access point name. By default, the name is netgearxxxxxx, where xxxxxx represents the last six hexadecimal digits of the access point's MAC address. You can change the name to one that is meaningful to you. |
| Model                            | The model of the access point. This field is populated during the access point discovery process and cannot be edited.   |

Table 7. Access point settings (continued)

| Setting   | Description  |
|---|--|
| Group   | The group to which the access point is assigned. After the access point discovery process, the access point is automatically assigned to the basic group. If you have set up profile groups, you can assign the access point to another profile group by selecting one from the drop-down list. You can also change the group assignment at a later time on the WLAN Group Assignment screen. For more information, see <a href="#">Manage Basic and Advanced Profile Groups in the WLAN</a> on page 87. |
| <b>IP Settings</b>  |  |
| These fields show the IP address and other IP settings of the access point. By default, these fields are populated during the access point discovery process. These are the functions of the radio buttons:   |  |
| <ul style="list-style-type: none"> <li>• <b>Enable.</b> By default, the <b>Enable</b> radio button is selected, allowing the access point to function as a DHCP client. The IP settings fields are masked out, preventing you from making changes.</li> <li>• <b>Disable.</b> Select the <b>Disable</b> radio button to disable the access point's DHCP client. The IP settings fields become available, allowing you to make changes, including changes to the access point's IP address.</li> </ul> |  |
| IP Address  | The IP address of the access point.  |
| Subnet Mask   | The subnet mask of the access point.   |
| Default Gateway   | The default gateway of the access point.   |
| Primary DNS Server  | The primary DNS server of the access point.  |
| Secondary DNS Server  | The secondary DNS server of the access point.  |
| <b>VLAN Settings section</b>  |  |
| Untagged VLAN   | Enter a VLAN ID or leave the default ID. By default, the untagged VLAN is 1 and the Untagged VLAN check box is selected. When the wireless controller sends frames associated with the untagged VLAN to the LAN (Ethernet) interface, those frames are untagged. When the wireless controller receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.   |
| Managed VLAN  | Enter a VLAN ID or leave the default ID. By default, the management VLAN is 1. For more information about management VLANs, see <a href="#">VLANs</a> on page 28 and <a href="#">Management VLANs</a> on page 66.  |
| <b>Sentry Mode Settings section</b>   |  |
| Sentry Mode   | Select this check box to configure the access point to function in sentry mode. In sentry mode, the access point monitors the wireless network for faster detection and mitigation of rogue access points but cannot serve wireless clients.<br><br><b>Note:</b> The WNAP210 access point does not support sentry mode.  |
| <b>Wireless Settings section</b>  |  |
| Antenna   | You can specify which antenna the access point uses by making a selection from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Internal.</b> The access point uses its internal antenna.</li> <li>• <b>External.</b> The access point uses its external antenna or antennas. External antennas are optional antennas that do not come standard with an access point.</li> </ul>  |

Table 7. Access point settings (continued)

| Setting                      | Description  |
|------------------------------|--|
| <b>Plan Settings section</b> |  |
| Site                         | The site designation that you have selected (see <a href="#">Add Access Points to the Managed List after Discovery</a> on page 57).  |
| Building                     | After you have configured buildings (see <a href="#">Define and Edit Buildings and Floors</a> on page 42), select the building in which the access point is located from the drop-down list. |
| Floor                        | After you have configured floors (see <a href="#">Define and Edit Buildings and Floors</a> on page 42), select the floor on which the access point is located from the drop-down list.       |
| Location                     | Enter a name that is meaningful to you.  |

5. Click **Apply** to save your settings.
6. Click **Back** to return to the Managed AP List.

➤ **To remove an access point from the Managed AP List:**

1. On the Managed AP List, select the check box to the right of the access point that you want to remove.
2. Click **Remove**.

---

**Note:** To restore a managed access point to its original firmware and use it once again as a standalone access point, remove the access point from the Managed AP List. Log in to the access point's web management interface, upgrade the firmware to the standalone AP firmware version, and then reboot the access point.

---

# Configuring Network Settings

# 5

This chapter includes the following sections:

- [Configure General Settings](#)
- [Time Management](#)
- [Configure IP and VLAN Settings](#)
- [Manage the DHCP Server](#)
- [Manage Certificates](#)
- [Configure Syslog and Alarm Notification Settings](#)

## Configure General Settings

**Note:** You need to select the correct country or region of operation. It might not be legal to operate the access points in a country or region not shown here. If your location is not listed, check with your local government agency or check the NETGEAR website for more information about which channels to use.

The General Settings screen lets you configure the basic settings of your wireless controller.

➤ **To configure general settings:**

1. Select **Configuration > System > General**. The General Settings screen displays:

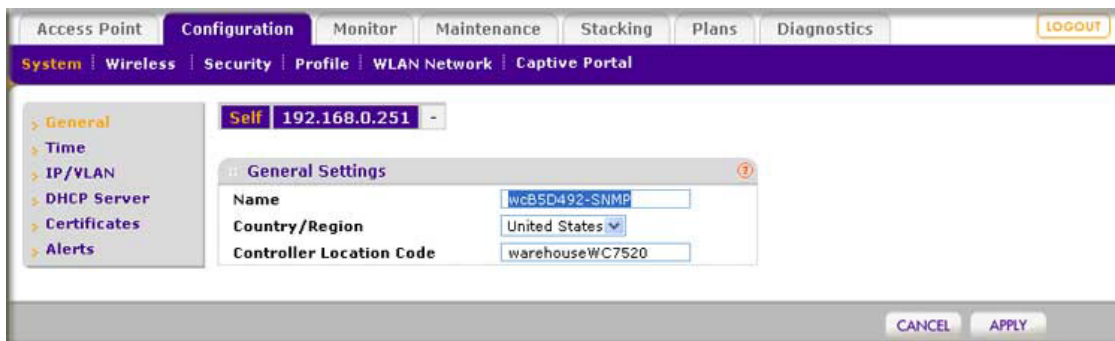


Figure 27.

- Configure the settings as explained in the following table:

**Table 8. General settings**

| Setting                  | Description  |
|--------------------------|--|
| Name                     | Enter a unique value as the wireless controller name. NETGEAR recommends changing the name as soon as possible after setting up. The name needs to contain only alphabetical characters, numbers, and hyphens, and needs to be 31 characters or less.  |
| Country/Region           | From the drop-down list, select the region of operation for the wireless controller and the access points managed by the wireless controller. This setting is crucial for optimal performance of the wireless controller. The wireless controller uses the country code to determine the best wireless settings for your access points. In the United States, the country is preset and cannot be changed on the access points. If the country or region is not set up correctly, the wireless controller might not be able to access the access points. |
| Controller Location Code | Optionally, enter a code to identify the physical location of the wireless controller. This is especially useful if you use more than one wireless controller.   |

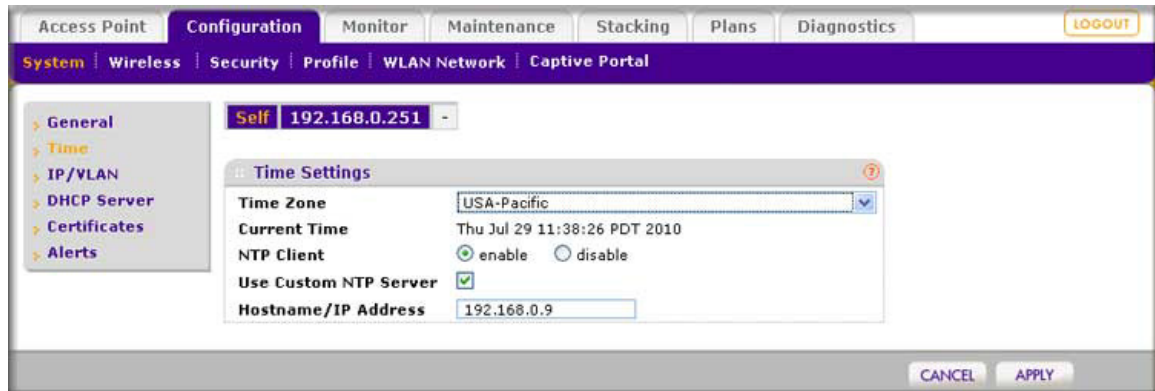
- Click **Apply** to save your settings.

## Time Management

This screen lets you configure the time-related settings of your wireless controller and managed access points.

- **To configure time settings:**

- Select **Configuration > System > Time**. The Time Settings screen displays:



**Figure 28.**



- Configure the settings as explained in the following table:

**Table 9. Time settings**

| Setting               | Description  |
|-----------------------|--|
| Time Zone             | From the drop-down list, select the local time zone for your country or region.  |
| Current Time          | This is a nonconfigurable field that displays the current time at your location.   |
| NTP Client            | Select the <b>Enable</b> radio button to use a Network Time Protocol (NTP) server to synchronize the clock of the wireless controller and managed access points. Select the <b>Disable</b> radio button if you do not want to use an NTP server. |
| Use Custom NTP Server | Select this check box if you want to use an alternate NTP server. By default, the NETGEAR NTP server is used.  |
| Hostname/IP Address   | Enter the host name or IP address of the NTP server, if you are using a custom NTP server.   |

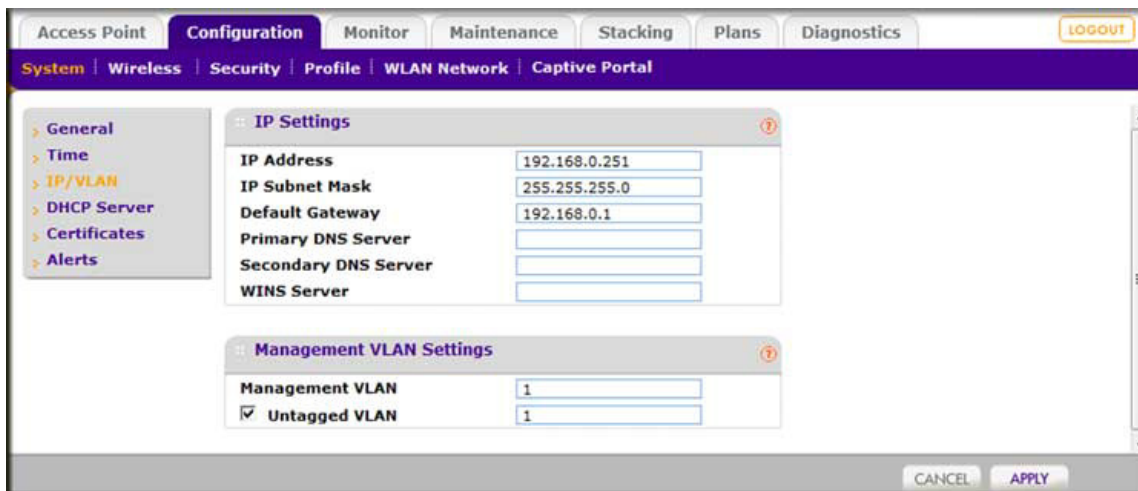
- Click **Apply** to save your settings.

## Configure IP and VLAN Settings

The IP Settings screen lets you configure the management IP address settings of the wireless controller.

- **To configure IP/VLAN settings:**

- Select **Configuration > System > IP/VLAN**. The IP Settings screen displays:



**Figure 29.**

2. Configure the settings as explained in the following table:

**Table 10. IP and management VLAN settings**

| Setting                                 | Description  |
|---|--|
| <b>IP Settings section</b>              |  |
| IP Address                              | Enter the IP address of the wireless controller. The default IP address is 192.168.0.250. To change it, enter an available IP address from the address range used on your LAN. |
| IP Subnet Mask                          | Enter the subnet mask value used on your LAN. The default value is 255.255.255.0.  |
| Default Gateway                         | Enter the IP address of the gateway for your LAN.  |
| Primary DNS Server                      | Enter the IP address of the primary Domain Name Server (DNS) that you want to use.   |
| Secondary DNS Server                    | Enter the IP address of the secondary DNS that you want to use.  |
| WINS Server                             | Enter the IP address of the Windows Internet Name Service (WINS) that you want to use.   |
| <b>Management VLAN Settings section</b> |  |
| Management VLAN                         | Enter the management VLAN. For information, see <a href="#">Management VLANs</a> following this table.   |
| Untagged VLAN                           | Select this check box if the configured VLAN is untagged. For information, see <a href="#">Untagged VLANs</a> on this page.  |

3. Click **Apply** to save your settings.

## Management VLANs

Management VLANs are used for all SNMP and HTTP traffic to and from the wireless controller and managed access points.

For large deployments, NETGEAR recommends that the wireless controller and access points are in separate VLANs to ensure uninterrupted connectivity between the wireless controller and the access points.

The wireless controller and access points share heartbeat messages to keep synchronized and share configurations and client key data to facilitate seamless roaming.

## Untagged VLANs

When the Untagged VLAN check box is selected, one VLAN can be configured as an untagged VLAN:

- When the wireless controller sends frames associated with the untagged VLAN to the LAN (Ethernet) interface, those frames do not carry an 802.1Q VLAN header.
- When the wireless controller receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.

If the Untagged VLAN check box is cleared, the wireless controller tags all outgoing LAN (Ethernet) frames, and accepts only incoming frames that are tagged with known VLAN IDs.

---

**Note:** Clear the Untagged VLAN check box only if the hubs and switches on your LAN support the VLAN (802.1Q) standard. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the VLAN (802.1Q) standard.

---

Changing either of these values will result in a loss of IP connectivity if the hubs and switches on your network have not yet been configured with the corresponding VLANs.

## Manage the DHCP Server

---

**Note:** Make sure that a DHCP server is available; otherwise, the Discovery Wizard does not function correctly. If you already have a DHCP server on your network, do not enable the DHCP server on the wireless controller.

---

The wireless controller can function as a DHCP server. Multiple DHCP server pools can be added for different VLANs. This screen lets you enable and configure the DHCP server. You can also add DHCP servers.

➤ **To add a DHCP server and configure its settings:**

1. Select **Configuration > System > DHCP**. The DHCP Settings screen displays. The following figure shows part of the DHCP Settings screen:

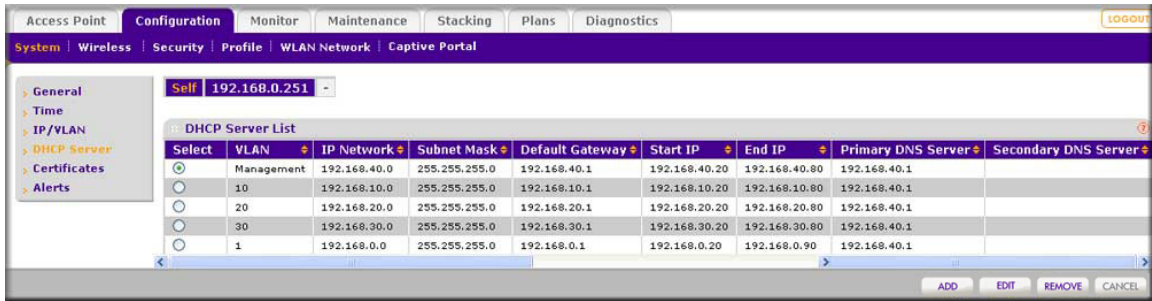


Figure 30.

The DHCP Server List shows the DHCP servers that are already configured on the wireless controller.

2. Click **Add**. The Add DHCP Server pop-up window displays:

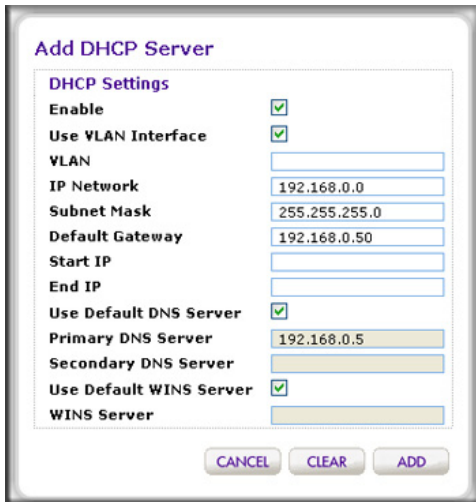


Figure 31.

3. Configure the settings as explained in the following table:

Table 11. DHCP settings

| Setting            | Description   |
|--------------------|---|
| Enabled            | Select this check box to enable the DHCP server. When the check box is cleared, the DHCP server is disabled.  |
| Use VLAN Interface | Select this check box to allow the DHCP server to function with multiple VLANs.   |
| VLAN               | Enter the DHCP server VLAN ID. The range is between 1 and 4094. The DHCP server will service this VLAN.   |
| IP Network         | Enter the IP address for the wireless controller in the VLAN that you have specified in the VLAN field. If you have not selected the Use VLAN Interface check box, the IP address of the wireless controller's management VLAN is used. |

Table 11. DHCP settings (continued)

| Setting                 | Description   |
|-------------------------|---|
| Subnet Mask             | Enter the subnet mask that is assigned to the wireless clients by the DHCP server.  |
| Default Gateway         | Enter the IP address of the default network gateway for all traffic beyond the local network.   |
| Start IP                | Enter the starting IP address of the range that can be assigned by the DHCP server.   |
| End IP                  | Enter the ending IP address of the range that can be assigned by the DHCP server.   |
| Use Default DNS Server  | Select this check box to allow the DHCP server to use the wireless controller's default DNS servers. The Primary DNS Server and Secondary DNS Server fields are masked out. |
| Primary DNS Server      | Enter the IP address of the primary DNS server for the network.   |
| Secondary DNS Server    | Enter the IP address of the secondary DNS server for the network.   |
| Use Default WINS Server | Select this check box to allow the DHCP server to use the wireless controller's default WINS server. The WINS Server field is masked out.                                   |
| WINS Server             | Enter the IP address of the WINS Server for the network.  |

4. Click **Add** to save your settings and add the new DHCP server to the DHCP Server List.

➤ **To edit a DHCP server:**

1. On the DHCP Server List, select the radio button in the Edit/Remove column that corresponds to the DHCP server that you want to edit.
2. Click **Edit**. The Edit DHCP Server pop-up window displays. This window is identical to the Add DHCP Server window (see the previous figure).
3. Make your changes (see the previous table).
4. Click **Apply** to save your changes.

➤ **To delete a DHCP server:**

1. On the DHCP Server List, select the radio button in the Edit/Remove column that corresponds to the DHCP server that you want to remove.
2. Click **Remove**.

## Manage Certificates

The internal authentication server for certificate-based authentication requires you to install a certificate on the wireless controller. There is a default self-signed server certificate installed on the wireless controller. However, NETGEAR strongly recommends that you replace this default certificate with a custom certificate issued for your site or domain by a trusted Certificate Authority (CA).

To obtain a security certificate for the wireless controller, generate and submit a certificate signing request (CSR) to the CA of your choice. Upon receiving the CA-signed server certificate, install the certificate from your PC as described in this section. Certificates need to be in X.509 PEM format.

### ➤ To add certificates:

1. Select **Configuration > System > Certificates**. The Add Certificates screen displays:

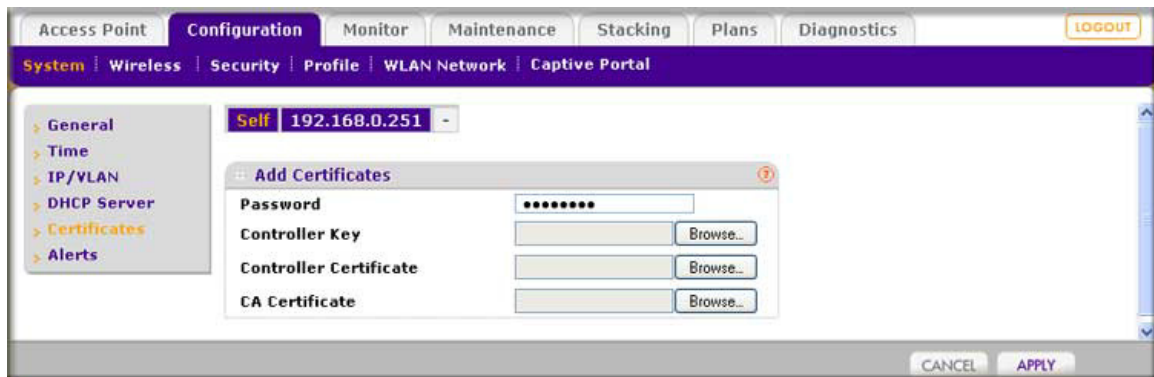


Figure 32.

2. Configure the settings as explained in the following table:

Table 12. Certificates settings

| Setting                | Description  |
|------------------------|--|
| Password               | The password for wireless controller certificates.           |
| Controller Key         | Click <b>Browse</b> , and select the controller key.         |
| Controller Certificate | Click <b>Browse</b> , and select the controller certificate. |
| CA Certificate         | Click <b>Browse</b> , and select the CA certificate.         |

3. Click **Apply** to save your settings.

## Configure Syslog and Alarm Notification Settings

From the Alerts menu you can configure the syslog and the alarms, and specify the email address from which alerts originate.

### Configure Syslog Settings

This screen lets you configure the settings to connect to a syslog server, if you have one configured in your network.

➤ **To configure Syslog settings:**

1. Select **Configuration > System > Alerts > Syslog**. The Syslog Settings screen displays:

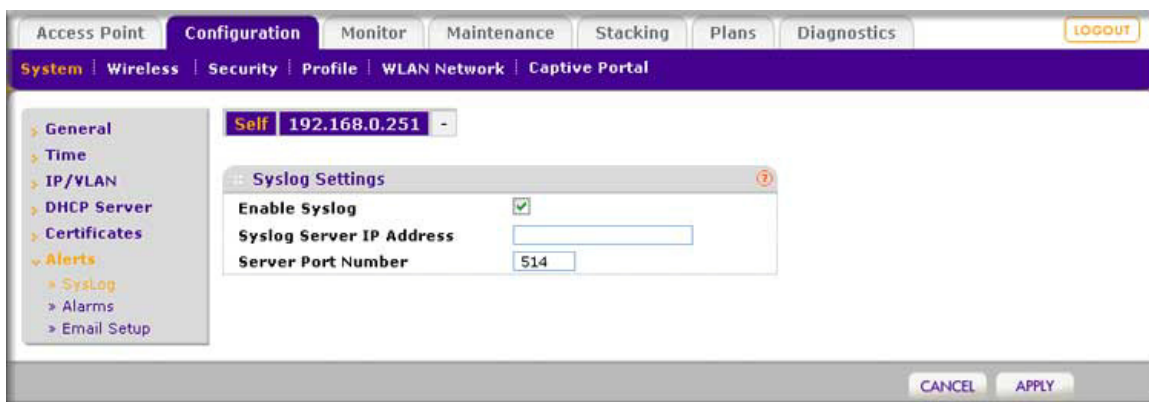


Figure 33.

2. Configure the settings as explained in the following table:

Table 13. Syslog settings

| Setting                  | Description   |
|--------------------------|---|
| Enable Syslog            | Enable the syslog settings, if you have a syslog server on your network.  |
| Syslog Server IP Address | Enter the IP address to which the wireless controller and managed access points will send all syslogs, if the Syslog check box is selected. |
| Server Port Number       | Enter the number of the port at which your syslog server is configured to listen to requests.   |

3. Click **Apply** to save your settings.

## Configure Alarm Notification Settings

You can classify certain events as critical, major, normal, or minor. Some events you can classify only as critical or major. For example, on the RF Management screen, you can specify whether a coverage hole should be classified as critical or major (see [Basic RF Management](#) on page 102).

➤ **To configure alarm actions:**

1. Select **Configuration > System > Alerts > Alarms**. The Alarm Actions screen displays:

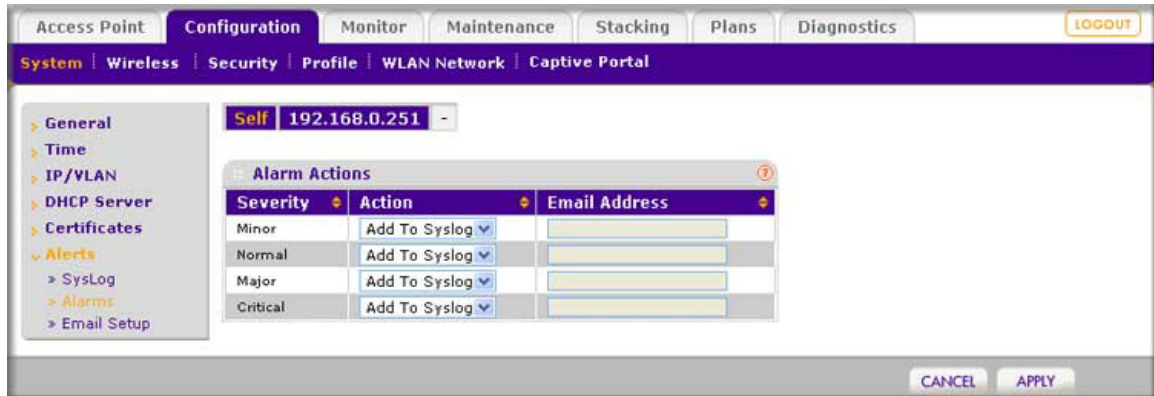


Figure 34.

2. For each alarm severity (Minor, Normal, Major, and Critical), select the desired action from its corresponding Action drop-down list.
  - **No Action.** When the alarm occurs, no action is taken.
  - **Add To Syslog.** When the alarm occurs, the wireless controller adds an entry to the syslog.
  - **Send Email.** When the alarm occurs, the wireless controller sends an email.
3. For each alarm severity for which you have selected the Send Email option in the previous step, enter an email address.
4. Click **Apply** to save your settings.

## Configure the Email Notification Server

The email notification server is the location from which the email alerts originate.

➤ **To configure email settings:**

1. Select **Configuration > System > Alerts > Email**. The Email Configuration screen displays:



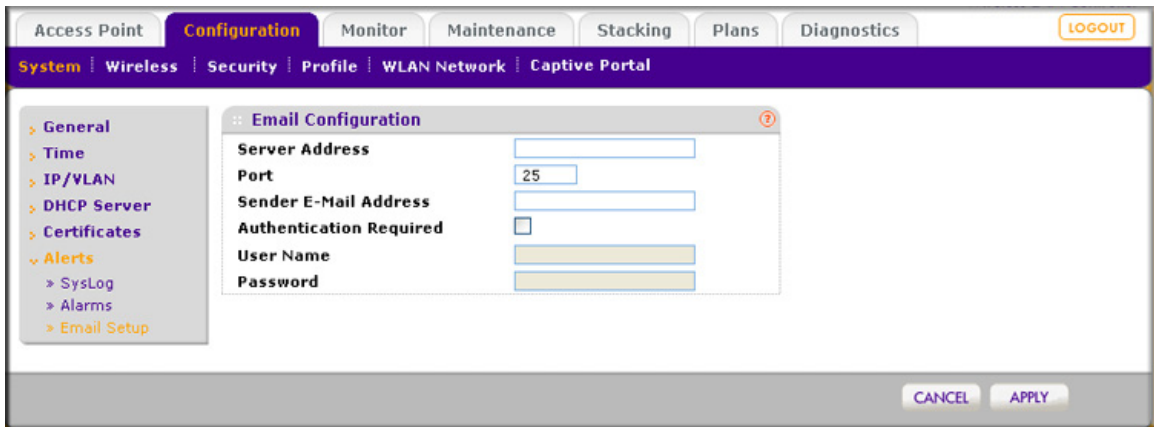


Figure 35.

2. Configure the settings as explained in the following table:

Table 14. Email configuration settings

| Setting                 | Description  |   |
|-------------------------|--|---|
| Server Address          | Enter the IP address of the server from which email notifications are sent.  |   |
| Port                    | Enter the port number of the server from which email notifications are sent. The default is port number 25.        |   |
| Sender Email Address    | Enter the email address from which email notifications are sent.   |   |
| Authentication Required | Select this check box if the email server requires authentication, and complete the User Name and Password fields. |   |
|                         | User Name  | Enter the user name that is associated with the email server. |
|                         | Password   | Enter the password that is associated with the email server.  |

3. Click **Apply** to save your settings.

# Managing Security Profiles and Profile Groups

---

# 6

This chapter includes the following sections:

- *Manage Wireless Security Profiles*
- *Configure Security Profiles for the Basic Profile Group*
- *Configure Security Profiles for Advanced Profile Groups*
- *Manage Basic and Advanced Profile Groups in the WLAN*

---

**Note:** In this chapter and in the following chapters, access point profile groups are referred to as just profile groups. Profiles, security profiles, and SSIDs (that is, SSIDs with associated security settings) are terms that are interchangeable.

---

## Manage Wireless Security Profiles

Profiles are sets of configurations that you can apply to an access point. The configuration includes radio parameters, load-balancing parameters, and rate-limit parameters. Each wireless radio on an access point is capable of supporting 8 profiles. This means that the dual-band WNDAP350 access point can support a total of 16 profiles. Therefore, in one profile group on the wireless controller, you can configure up to 8 profiles for each radio, that is, up to 8 profiles for the 2.4-GHz radio *and* up to 8 profiles for the 5-GHz radio.

Setting up profiles allows you to configure the WLAN network offline. Then, when the WLAN network is up and running, you can push the configuration onto managed access points. You can configure profiles and profile groups without taking the state of the access points into consideration. When the access points connect to the controller, the profile configurations are pushed onto the access points.

---

**Note:** Note that if an access point is removed from its building (someone takes it home or it is stolen) the access point does not retain the configuration that it received from the wireless controller. The configuration is not stored in memory on the access point.

---

Depending on your network needs, you can either use the basic profile group (that is, the basic configuration) or the advanced profile groups (that is, the advanced configuration). The basic profile group works well for small-scale WLAN networks; advanced profile groups are useful for larger deployments.

---

**Note:** For more information about basic and advanced profile groups, see *Basic and Advanced Settings* on page 22.

---

## Small WLAN Networks

For small WLAN networks, you can use the basic configuration with the basic profile group. All access points belong to the same group and use the same wireless, security, and QoS configurations.

The basic profile group can contain up to 16 profiles for a dual-band access point, or 8 profiles for a single-band access point. Each profile has its own SSID and can have its own VLAN to allow the profile to establish its own tunnel. Profiles can also share the same VLAN.

For example, in an enterprise network in which all access points managed by the wireless controller serve the same wireless networks and have the same settings, you can use the basic configuration.

## Larger WLAN Networks

For larger network deployments that consist of different sets of WLAN networks, consider using the advanced configuration to create multiple profile groups. The access points that belong to the same profile group use the same wireless, security, and QoS configurations.

The wireless controller supports up to 8 profile groups. Each profile group can have its own wireless, security, and QoS configurations. Each profile group can contain up to 16 profiles for a dual-band access point, or 8 profiles for a single-band access point. Using dual-band access points, the wireless controller could support a total of 128 profiles. Each profile has its own SSID and can have its own VLAN to allow the profile to establish its own tunnel. Profiles can also share the same VLAN.

In larger network deployments also, you would assign guests to a separate VLAN because guests typically access only the Internet, not the business network, and do not have peer-to-peer access.

## Profile Naming Conventions

You can use profile naming conventions that are based on user groups such as Marketing, or based on VLANs such as VLAN40, or you can use other naming conventions such as CompanyName15.

---

**Note:** In the advanced configuration, you cannot change the names of profile groups. However, you can change the group names of MAC ACLs and external RADIUS servers.

---

## Considerations Before You Configure Profiles

Before you create and configure profiles for the basic profile group or an advanced profile group, consider the following:

- **Authentication servers.** If you want to use external LDAP or RADIUS authentication, or both, first create the authentication server settings:
  - Configure basic server settings on the basic Authentication Server screen (see [Configure Basic Authentication Server Settings](#) on page 123).
  - For more complex networks, configure additional RADIUS servers on the advanced Authentication Server screen (see [Configure RADIUS Authentication Server Groups](#) on page 125).

After you have configured authentication server settings, you can then assign any authentication server to a security profile in a basic profile group or advanced profile group.

---

**Note:** You can configure profiles to function with different authentication servers. For example, you could set up a guest profile with no authentication, an engineering profile that uses external RADIUS authentication, and a marketing profile that uses external LDAP authentication. You can also use additional external RADIUS servers in other profiles.

---

- **MAC authentication.** If you want to use a MAC access control list (ACL) to control access of wireless clients, first create one or more MAC ACLs:
  - Configure the basic MAC ACL on the basic MAC Authentication screen (see [Configure Basic Local MAC Authentication Settings](#) on page 118).
  - For more complex networks, configure additional MAC ACLs on the advanced MAC Authentication screen (see [Configure Local MAC Authentication Groups](#) on page 120).

After you have configured one or more MAC ACLs, you can then assign any MAC ACL to a security profile in a basic profile group or advanced profile group.

- **Cloning profiles.** For faster setup you can clone a profile and rename it. Cloning copies all settings except for the name and SSID.

## Configure Security Profiles for the Basic Profile Group

The Edit Profile (Basic) screen lets you create and configure up to 8 security profiles per wireless radio (8 profiles for a single-band access point; 16 profiles for a dual-band access point). Separate profiles are applied to 802.11b/bg/ng-mode and 802.11a/na-mode radios.

### ➤ To add a security profile to the basic profile group:

1. Select **Configuration > Profile > Basic > Radio**. The Edit Profile (Basic) screen displays:

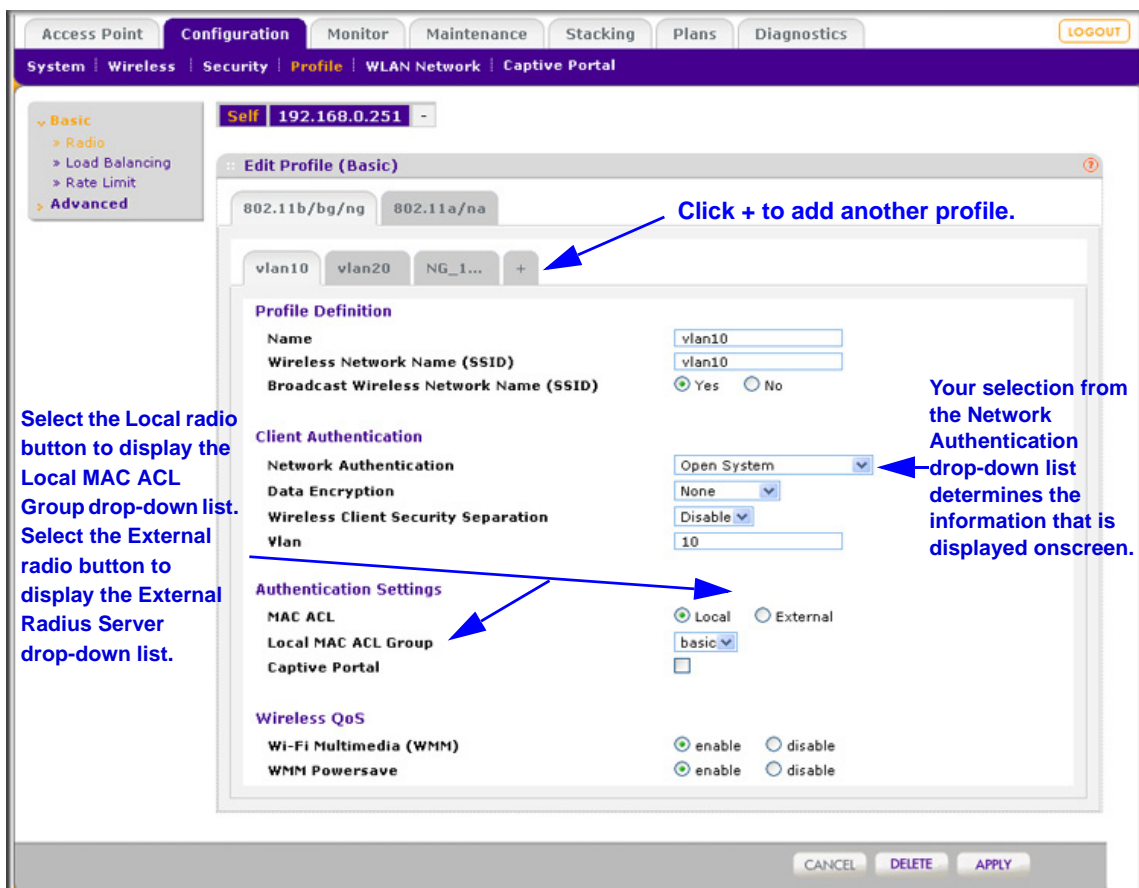


Figure 36.

By default, an NG\_11g profile and an NG\_11a profile are present in the basic profile group.

2. Click a tab to select a radio.

- Click the + button to add a profile to the basic profile group. The Add Profiles pop-up window displays:

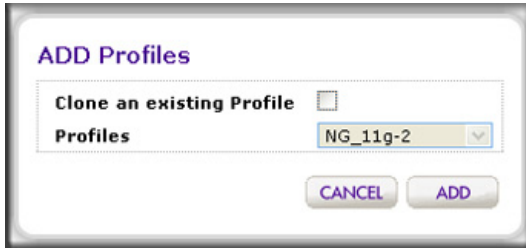


Figure 37.

- Either click **Add**, or, if you want to clone an existing profile, select the **Clone an existing Profile** check box, select a profile from the Profiles drop-down list, and then click **Add**. The newly created profile displays onscreen, and the tab for the new profile is automatically selected to let you configure the new profile.

---

**Note:** The selections that are available in the Network Authentication field are affected by the authentication server settings that you specify on the Authentication Server screen. See [Manage Authentication Servers and Authentication Server Groups](#) on page 122. If the selection in the Network Authentication field requires authentication, an additional field, the corresponding Authentication Server field, displays.

---

- Configure the settings as described in the following table:

Table 15. Basic security profile definition settings

| Setting                           | Description   |
|-----------------------------------|---|
| <b>Profile Definition section</b> |   |
| Name                              | Enter a unique name to identify the profile. This value can be up to 32 alphanumeric characters. Use meaningful profile names instead of the default names. The default profile names are Profile1, Profile2, and so on, through Profile8.                  |
| Wireless Network Name (SSID)      | Enter a unique name for the wireless network associated with this profile.  |
| Broadcast Wireless Network Name   | Select the <b>Yes</b> radio button to enable broadcast of the SSID. This is the default setting. Select the <b>No</b> radio button to disable broadcast of the SSID, in which case only devices that have the correct SSID can connect to the access point. |

Table 15. Basic security profile definition settings (continued)

| Setting  | Description   |   |
|--|---|---|
| <b>Client Authentication section</b>   |   |   |
| <b>Note:</b> The options that display onscreen depend on the selection from Network Authentication drop-down list. |   |   |
| Network Authentication   | From the drop-down list, select the authentication type to be used: see <a href="#">Table 16</a> on page 81.  |   |
| Data Encryption  | From the drop-down list, select the data encryption type to be used. The options available for data encryption as well as other requirements such as entering a key or passphrase depend on the network authentication settings: see <a href="#">Table 16</a> on page 81. |   |
| Wireless Client Security Separation  | From the drop-down list, select <b>Disable</b> to prevent associated wireless clients from communicating with each other or <b>Enable</b> to allow such communication. Wireless client separation is intended for hotspots and other public access situations.            |   |
| VLAN   | Enter the VLAN ID to be associated with this security profile. This VLAN ID needs to match the VLAN ID that is used by other network devices.   |   |
| <b>Authentication Settings section</b>   |   |   |
| <b>Note:</b> The options that display onscreen depend on the selection from Network Authentication drop-down list. |   |   |
| Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK   | MAC ACL   | <p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> <li>• <b>Local.</b> Use local MAC authentication. The Local MAC ACL Group drop-down list displays so you can select a group. For more information, see <a href="#">Manage MAC Authentication and MAC Authentication Groups</a> on page 117.</li> <li>• <b>External.</b> Use external MAC authentication. The External Radius Server drop-down list displays so you can select a server. You can use either the basic-Auth RADIUS server or a RADIUS server of an advanced authentication group. You cannot use the external LDAP server. For information about setting up and enabling internal and external authentication servers, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.</li> </ul> <p><b>Note:</b> The MAC ACL radio buttons do not display onscreen if the network authentication uses an external RADIUS server. The reason for this is that you can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA &amp; WPA2 (or you use Legacy 802.1X) , you cannot use external MAC authentication, and the MAC ACL radio buttons do not display on screen. You still can use internal MAC authentication.</p> |

Table 15. Basic security profile definition settings (continued)

| Setting  | Description  |  |
|--|--|--|
| Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK (continued) | Captive Portal   | Select this check box if you want to enable the captive portal. For more information, see <a href="#">Configure Captive Portal Settings</a> on page 126.<br><br><b>Note:</b> You cannot configure captive portal authentication if the network authentication uses an external RADIUS server. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), the Captive Portal check box is not shown onscreen.   |
| WPA with Radius, WPA2 with RADIUS, and WPA & WPA2 with Radius                  | Authentication Server  | Select one of the following radio buttons:<br><ul style="list-style-type: none"> <li>• <b>Local.</b> Use the local authentication server.</li> <li>• <b>External.</b> Use an external authentication server. Select an external authentication server from the Authentication Server drop-down list.</li> </ul> <b>Note:</b> For information about setting up and enabling internal and external authentication servers, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122. |
| <b>Wireless QoS section</b>  |  |  |
| Wi-Fi Multimedia (WMM)   | To enable Wi-Fi Multimedia (WMM), select the <b>Enable</b> radio button, which is the default setting. Select the <b>Disable</b> button to disable the feature. For more information, see <a href="#">Configure QoS for Profile Groups</a> on page 105.                                      |  |
| WMM Powersave  | The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. To enable this feature, select the <b>Enable</b> radio button, which is the default setting. Select the <b>Disable</b> button to disable the feature. |  |

6. Click **Apply** to save your settings.

## Edit and Remove Profiles from the Basic Profile Group

### ➤ To edit an existing profile:

1. On the Basic Profile screen, click a tab to select a profile.
2. Click a tab to select a radio.
3. Change the settings as explained in the previous table and the following table.
4. Click **Apply** to save your settings.

### ➤ To remove an existing profile:

- On the Basic Profile screen, click a tab to select a profile.
  - Click a tab to select a radio.
5. Click **Delete**, and then confirm that you want to delete the profile.



## Network Authentication and Data Encryption Options

The following table shows the data encryption options based on network authentication, and the required configuration steps to implement a selected network authentication.

---

**Note:** On the Edit Profile (Basic) or Edit Profile (Group-X) screen, for any selection from the Network Authentication drop-down list that requires a RADIUS server, note that authentication is actually not restricted to a RADIUS server; you can also use an internal authentication server or an external LDAP server.

---



---

**Note:** For information about requirements for WEP keys and WPA passphrases, see [Table 54](#) on page 203.

---



---

**Note:** You can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure external MAC authentication, you cannot use an external RADIUS server with WPA, WPA2, or WPA & WPA2.

---

**Table 16. Network authentication and data encryption settings**

| Network authentication selection | Data encryption options | Configuration steps  |
|----------------------------------|-------------------------|--|
| Open                             | None<br>WEP             | <p>You can use an open system without any encryption or with WEP encryption:</p> <ul style="list-style-type: none"> <li>• <b>No encryption.</b> An open system without encryption is the default setting. No further authentication and encryption configuration is required.</li> <li>• <b>WEP encryption.</b> To configure an open system with WEP encryption, see the Shared Key and WEP information further down in this table.</li> </ul> |

Table 16. Network authentication and data encryption settings (continued)

| Network authentication selection | Data encryption options                  | Configuration steps   |
|----------------------------------|--|---|
| Shared Key                       | 64-bit WEP<br>128-bit WEP<br>152-bit WEP | <p>To configure Shared Key authentication with WEP:</p> <ol style="list-style-type: none"> <li>From the Data Encryption drop-down list, select a level of WEP encryption: <ul style="list-style-type: none"> <li>- <b>64-bit WEP</b>. Uses 40/64-bit encryption.</li> <li>- <b>128-bit WEP</b>. Uses 104/128-bit encryption.</li> <li>- <b>152-bit WEP</b>. A proprietary mode that works only with other wireless devices that support this mode.</li> </ul> </li> <li>Select a key radio button (<b>Key1</b>, <b>Key2</b>, <b>Key3</b>, or <b>Key4</b>).</li> <li>Enter a key in the corresponding field: <ul style="list-style-type: none"> <li>- 64-bit WEP requires a key with 10 characters.</li> <li>- 128-bit WEP requires a key with 26 characters.</li> <li>- 152-bit WEP requires a key with 32 characters.</li> </ul> </li> </ol> |
| Legacy 802.1x                    | None                                     | <p>To configure legacy 802.1x authentication:</p> <ol style="list-style-type: none"> <li>Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.</li> <li>Select the <b>Local</b> or <b>External</b> radio button.</li> <li>If you select the External radio button, select the authentication server that you wish to use from the drop-down list.</li> </ol>   |
| WPA with Radius                  | TKIP<br>TKIP + AES                       | <p>To configure WPA authentication with a RADIUS server:</p> <ol style="list-style-type: none"> <li>Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.</li> <li>From the Data Encryption drop-down list, select the type of encryption: <ul style="list-style-type: none"> <li>- <b>TKIP</b>. Supports Temporal Key Integrity Protocol (TKIP) only.</li> <li>- <b>TKIP + AES</b>. Supports both TKIP and Advanced Encryption Standard (AES).</li> </ul> </li> <li>Select the <b>Local</b> or <b>External</b> radio button.</li> <li>If you select the External radio button, select the authentication server that you wish to use from the drop-down list.</li> </ol>                        |

Table 16. Network authentication and data encryption settings (continued)

| Network authentication selection  | Data encryption options | Configuration steps   |
|---|-------------------------|---|
| WPA2 with Radius  | AES<br>TKIP + AES       | To configure WPA2 authentication with a RADIUS server: <ol style="list-style-type: none"> <li>1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.</li> <li>2. From the Data Encryption drop-down list, select the type of encryption:               <ul style="list-style-type: none"> <li>- <b>AES</b>. Supports AES only.</li> <li>- <b>TKIP + AES</b>. Supports both TKIP and AES.</li> </ul> </li> <li>3. Select the <b>Local</b> or <b>External</b> radio button.</li> <li>4. If you select the External radio button, select the authentication server that you wish to use from the drop-down list.</li> </ol> |
| WPA & WPA2 with Radius<br><br><b>Note:</b> Use this option if there are both WPA and WPA2 clients in the network. | TKIP + AES              | To configure WPA & WPA2 authentication with a RADIUS server: <ol style="list-style-type: none"> <li>1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.</li> <li>2. Select the <b>Local</b> or <b>External</b> radio button.</li> <li>3. If you select the External radio button, select the authentication server that you wish to use from the drop-down list.</li> </ol> <p><b>Note:</b> The Data Encryption drop-down list displays TKIP + AES, which is the only available option. Both TKIP and AES are supported.</p>  |
| WPA-PSK   | TKIP<br>TKIP + AES      | To configure WPA-PSK authentication: <ol style="list-style-type: none"> <li>1. From the Data Encryption drop-down list, select the type of encryption:               <ul style="list-style-type: none"> <li>- <b>TKIP</b>. Supports TKIP only.</li> <li>- <b>TKIP + AES</b>. Supports both TKIP and AES.</li> </ul> </li> <li>2. Type a passphrase of at least 8 characters in the WPA Passphrase (Network Key) field.</li> </ol>   |
| WPA2-PSK  | AES<br>TKIP + AES       | To configure WPA2-PSK authentication: <ol style="list-style-type: none"> <li>1. From the Data Encryption drop-down list, select the type of encryption:               <ul style="list-style-type: none"> <li>- <b>AES</b>. Supports AES only.</li> <li>- <b>TKIP + AES</b>. Supports both TKIP and AES.</li> </ul> </li> <li>2. Type a passphrase of at least 8 characters in the WPA Passphrase (Network Key) field.</li> </ol>  |

Table 16. Network authentication and data encryption settings (continued)

| Network authentication selection  | Data encryption options | Configuration steps  |
|---|-------------------------|--|
| WPA-PSK & WPA2-PSK<br><br><b>Note:</b> Use this option if there are both WPA-PSK and WPA2-PSK clients in the network. | AES<br>TKIP + AES       | To configure WPA-PSK & WPA2-PSK authentication, type a passphrase of at least 8 characters in the WPA Passphrase (Network Key) field.<br><br><b>Note:</b> The Data Encryption drop-down list displays TKIP + AES, which is the only available option. Both TKIP and AES are supported. |

## Configure Security Profiles for Advanced Profile Groups

The advanced Profile Group screen lets you create up to 8 profile groups. For each profile group you can create and configure up to 8 security profiles per wireless radio (8 profiles for a single-band access point; 16 profiles for a dual-band access point). Separate profiles are applied to 802.11b/bg/ng-mode and 802.11a/na-mode radios.

By default, all access points are assigned to the basic profile group. After you have created advanced profile groups, you can use the WLAN Network screen to reassign access points to any of these advanced profile groups (see [Manage Basic and Advanced Profile Groups in the WLAN](#) on page 87).

- **To add a profile group, configure a new profile, and then add another profile:**
  1. Select **Configuration > Profile > Advanced > Radio**. The Profile Groups screen displays:

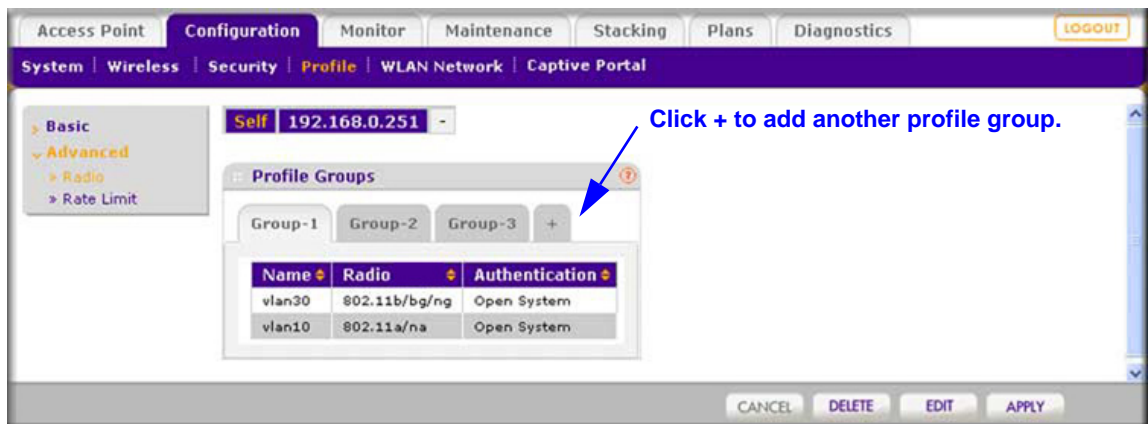


Figure 38.

The following table describes the fields that are shown for each profile in a profile group.

**Table 17. Profile group settings**

| Setting        | Description  |
|----------------|--|
| Name           | The unique profile name.   |
| Radio          | The wireless radio mode in which the profile is operating.       |
| Authentication | The authentication setting under which the profile is operating. |

- Click the **+** button to create an additional profile group. The new profile group displays on the advanced Profile Groups screen. By default, an NG\_11g-0 profile and an NG\_11a-0 profile are present in a profile group.

---

**Note:** By default, profile groups are named Group-1, Group-2, Group-3, and so on. You *cannot* change these profile group names.

---

- Click **Edit**. The advanced Edit Profile screen displays.

---

**Note:** The selections that are available in the Network Authentication field are affected by the authentication server settings that you specify on the Authentication Server screen. See [Manage Authentication Servers and Authentication Server Groups](#) on page 122. If the selection in the Network Authentication field requires authentication, an additional field, the corresponding Authentication Server field, displays.

---

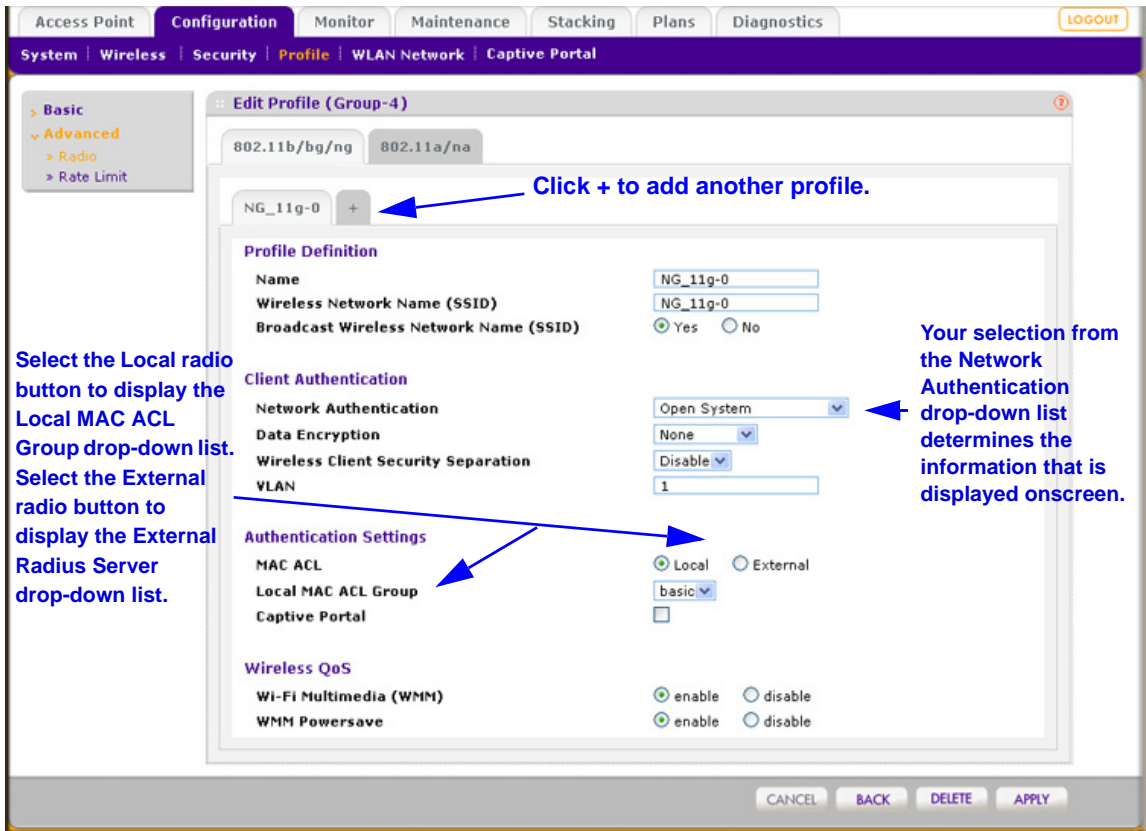


Figure 39.

4. Click a tab to select a radio.
5. Specify the settings as described in [Table 15](#) on page 78 and [Table 16](#) on page 81.
6. Click **Apply** to save your settings.
7. To add another profile to the new profile group:
  - a. Click a tab to select a radio.
  - b. Click the **+** button. The Add Profiles pop-up window displays:



Figure 40.

- c. Either click **Add**, or, if you want to clone an existing profile, select the **Clone an existing Profile** check box, select a profile from the Profiles drop-down list, and then click **Add**. The newly created profile displays onscreen, and the tab for the new profile is automatically selected to let you configure the new profile.
8. Specify the settings as described in [Table 15](#) on page 78 and [Table 16](#) on page 81.

9. Click **Apply** to save your settings.

## Edit and Remove Profiles from an Advanced Profile Group

- **To edit an existing profile to an advanced profile group:**
  1. On the Profile Groups screen, click a tab to select a profile group.
  2. Click **Edit**. The Edit Profile screen displays.
  3. Click a tab to select a radio.
  4. Click a tab to select a profile.
  5. Change the settings as explained in the [Table 15](#) on page 78 and [Table 16](#) on page 81.
  6. Click **Apply** to save your settings.
- **To remove an existing profile from an advanced profile group:**
  1. On the Profile Groups screen, click a tab to select a profile group.
  2. Click **Edit**. The Edit Profile screen displays.
  3. Click a tab to select a radio.
  4. Click a tab to select a profile.
  5. Click **Delete**, and then confirm that you want to delete the profile.

## Remove an Advanced Profile Group

- **To remove an advanced profile group:**
  1. On the Profile Groups screen, click a tab to select a profile group.
  2. Click **Delete**.

---

**Note:** You edit profile groups by adding, removing, or changing profiles.

---

## Manage Basic and Advanced Profile Groups in the WLAN

By default, all access points are automatically assigned to the basic profile group. You can use this screen to assign access points to other profile groups.

- **To assign access points to a profile group:**
  1. Select **Configuration > WLAN Network**. The WLAN Group Assignment screen displays:

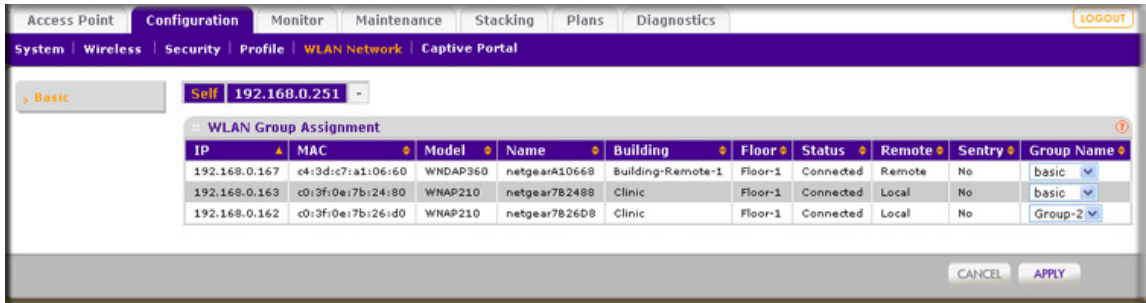


Figure 41.

The displayed settings are explained in the following table:

Table 18. WLAN group assignments

| Setting  | Description   |
|----------|---|
| IP       | The IP address of the access point.   |
| MAC      | The MAC address of the access point.  |
| Model    | The model of the access point.  |
| Name     | The name that you specified for the access point.   |
| Building | The building in which the access point is located. For more information, see <a href="#">Define and Edit Buildings and Floors</a> on page 42 and <a href="#">Edit and Remove Access Point Information</a> on page 59.   |
| Floor    | The floor on which the access point is located. For more information, see <a href="#">Define and Edit Buildings and Floors</a> on page 42 and <a href="#">Edit and Remove Access Point Information</a> on page 59.  |
| Status   | <p>The access point connectivity status.</p> <ul style="list-style-type: none"> <li>• <b>Authentication in progress.</b> (This status can last several minutes)</li> <li>• <b>Applying configurations.</b></li> <li>• <b>Firmware upgrade.</b></li> <li>• <b>AP is rebooting.</b></li> <li>• <b>Connecting.</b></li> <li>• <b>Connected.</b> This status indicates normal operation.</li> <li>• <b>Not Connected.</b> The wireless controller cannot communicate with the access point at the configured IP address. The wireless controller tries to log in to managed access points each minute. If the error is temporary, the status automatically changes to connected. If the error is prolonged, verify the access point's IP address and network connectivity.</li> </ul> <p><b>Note:</b> Make sure that there is a DHCP server enabled in the network; otherwise, the managed access points remain in the Connecting state and do not enter the Connected state.</p> |



Table 18. WLAN group assignments (continued)

| Setting   | Description  |
|-----------|--|
| Remote AP | Shows whether the access point is a local or remote one: <ul style="list-style-type: none"><li>• <b>Local.</b> The AP is deployed at the local site.</li><li>• <b>Remote.</b> The AP is deployed at a remote site.</li></ul> |
| Sentry    | Shows whether or not sentry mode is enabled: <ul style="list-style-type: none"><li>• <b>No.</b> Sentry mode is disabled.</li><li>• <b>Yes.</b> Sentry mode is enabled.</li></ul>   |

2. To assign an access point to a profile group, select the profile group name from the Group Name drop-down list. For information about adding and specifying groups, see the previous section.
3. Click **Apply** to save your settings.

# Configuring Wireless and QoS Settings

---

# 7

This chapter includes the following sections:

- [About Basic and Advanced Wireless and QoS Configurations](#)
- [Configure the Radio](#)
- [Configure Wireless Settings](#)
- [Configure Channels](#)
- [Specify RF Management](#)
- [Configure QoS for Profile Groups](#)
- [Configure Load Balancing](#)
- [Configure Rate Limiting](#)

During initial setup, enter your country and region in the General Settings screen ([Configure General Settings](#) on page 63). Based on your location and environment, the wireless controller determines the recommended wireless settings for your access points, and establishes these settings the defaults that will be sent to your managed access points. When you are ready to configure your access points, NETGEAR recommends using the default settings as they are unless you have specific reasons to change them.

## About Basic and Advanced Wireless and QoS Configurations

It is important to know how to configure your network and decide which configuration model better fits your needs, basic or advanced. Once you follow one, it is easy to use the same configuration model for the wireless and Quality of Service (QoS) settings. Before you configure the wireless settings, read [Basic and Advanced Settings](#) on page 22.

- **Basic wireless settings.** If you use the basic configuration model, the following wireless and QoS settings apply to all profiles in the basic profile group:
  - Basic radio on/off schedule
  - Basic wireless settings for each radio in the basic profile
  - Basic RF management
  - Basic rate limiting for each radio in the basic profile

- **Advanced wireless settings.** If you use the advanced configuration model, you can configure the following wireless and QoS settings separately for each profile group that you have created:
  - Advanced radio on/off schedules for up to 8 profile groups
  - Advanced wireless settings for each radio in up to 8 profile groups
  - Advanced QoS settings for each radio in up to 8 profile groups
  - Advanced RF management for up to 8 profile groups
  - Advanced rate limiting for each radio in up to 8 profile groups
- **Global wireless settings.** The following wireless and QoS settings apply to all profiles, whether in the basic profile group or in any of the advanced profile groups:
  - Basic channel allocation
  - Basic load balancing for each type of access point model

## Configure the Radio

Radio On/Off is a green feature that can be used during scheduled vacations or plant shutdowns, on evenings, or on weekends.

### Basic Radio Configuration

#### ➤ To schedule the radio:

1. Select **Configuration > Wireless > Basic > Radio On/Off**. The basic Schedule screen displays:

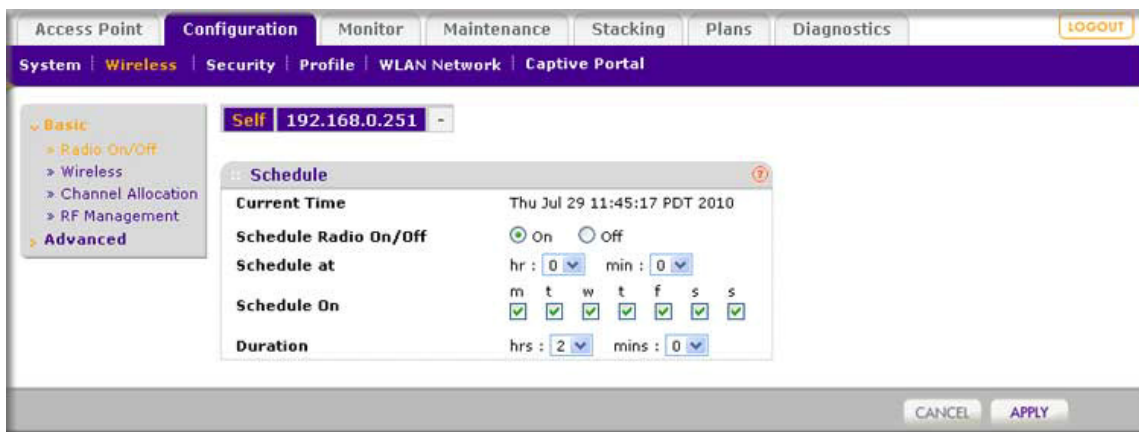


Figure 42.

- Configure the settings as explained in the following table:

**Table 19. Schedule radio on/off settings**

| Setting               | Description   |
|-----------------------|---|
| Current Time          | This is a nonconfigurable field that displays the current time for the wireless controller.   |
| Schedule Radio On/Off | You can specify either when the radio is on by selecting the <b>On</b> radio button or when it is off by selecting the <b>Off</b> radio button. |
| Schedule at           | From the drop-down lists, specify the time (hours and minutes) when you want to turn the radio either on or off.                                |
| Schedule On           | Select the check boxes for each day of the week that you want to schedule the radio to be either on or off.                                     |
| Duration              | From the drop-down lists, specify the duration (in hours and minutes) that the radio should be either on or off.                                |

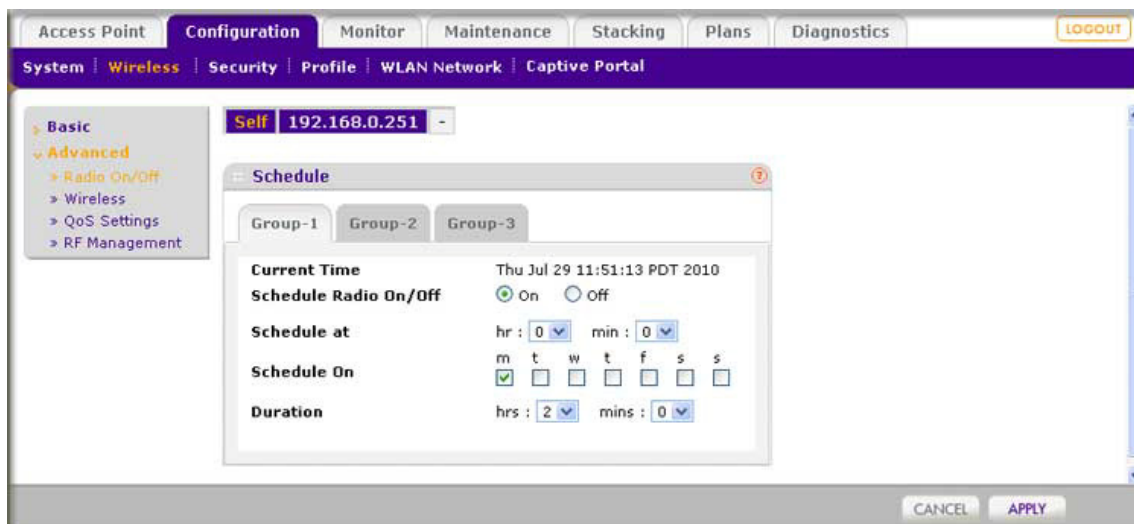
- Click **Apply** to save your settings.

## Advanced Radio Configuration for Profile Groups

You can schedule the radio for specific groups to match their network usage. For example, during registration, a school could leave the radios on for the main office or administration building, and turn off radios in buildings that contain only classrooms that are not in use.

➤ **To schedule the radio for profile groups:**

- Select **Configuration > Wireless > Advanced > Radio On/Off**. The advanced Schedule screen displays:



**Figure 43.**

- Click a tab to select a profile group.

3. Configure the settings as explained in the previous table.
4. Click **Apply** to save your settings.

## Configure Wireless Settings

Typically, the default wireless settings do not need adjustment. Override the wireless settings only if there is a specific need, such as a phone vendor that specifies a setting different from the default. You can configure wireless settings for the basic profile group and for advanced profile groups (see [Advanced Wireless Configuration for Profile Groups](#) on page 96).

### Basic Wireless Configuration

➤ **To configure basic wireless settings:**

1. Select **Configuration > Wireless > Basic > Wireless**. The Basic Wireless Settings screen displays:

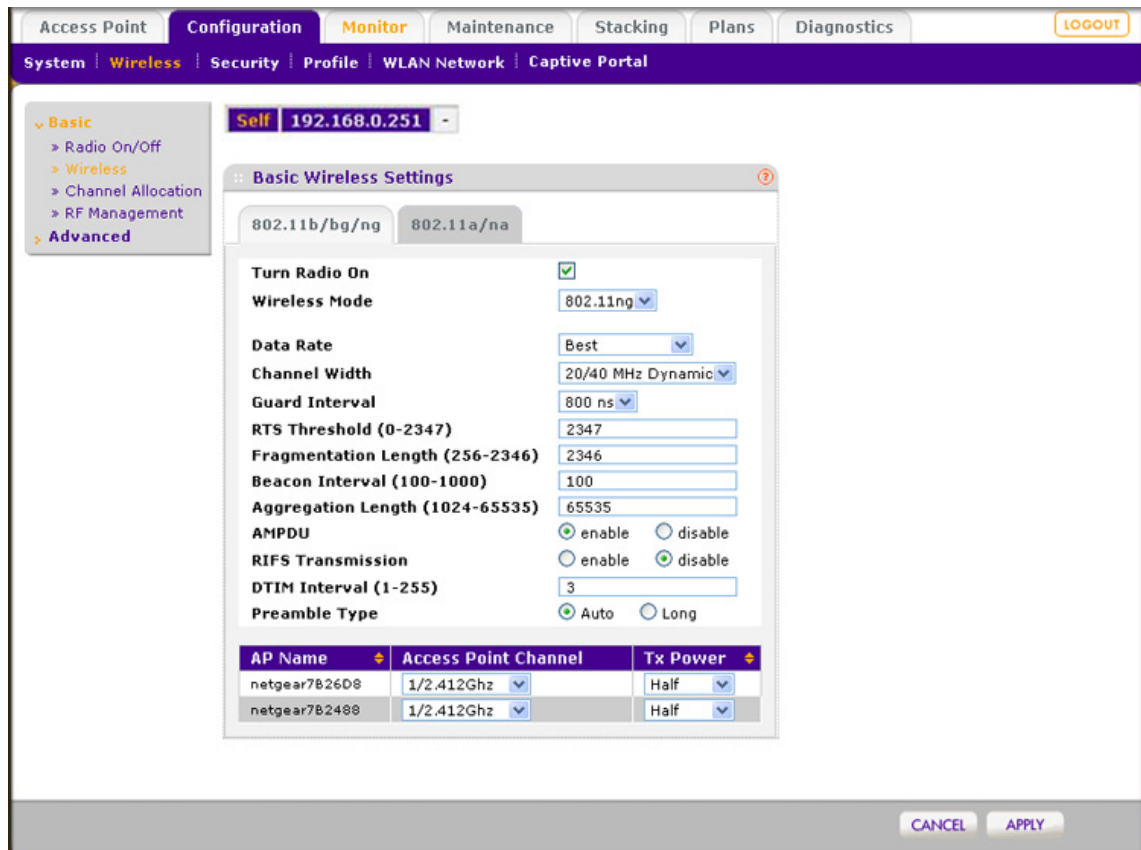


Figure 44.

2. Click a tab to select a radio.
3. Select the **Turn Radio On** check box to enable configuration of the wireless settings.

---

**Note:** If automatic channel allocation is enabled on the Channel Allocation screen (see *Configure Channels* on page 99), you cannot configure the wireless settings on the Basic Wireless Settings screen. You need to disable automatic channel allocation to be able to configure the wireless settings.

---



---

**Note:** You cannot configure the wireless settings if there are no access points assigned to a radio in a profile group.

---

4. Configure the settings as explained in the following table:

**Table 20. Wireless settings**

| Setting                       | Description   |
|-------------------------------|---|
| Wireless Mode                 | <p>The selections that are available depend on the selected radio mode. From the drop-down list select the wireless mode:</p> <ul style="list-style-type: none"> <li>• 802.11b/bg/ng mode:                             <ul style="list-style-type: none"> <li>- <b>11ng</b>. This is the default setting.</li> <li>- <b>11bg</b>.</li> <li>- <b>11b</b>.</li> </ul> </li> <li>• 802.11a/na mode:                             <ul style="list-style-type: none"> <li>- <b>11na</b>. This is the default setting.</li> <li>- <b>11a</b>.</li> </ul> </li> </ul> <p><b>Note:</b> If you select 802.11bg or 802.11b mode, both 802.11n- and 802.11g-compliant devices can connect to the access points. However, if you select 802.11ng mode, 802.11b-compliant devices cannot connect.</p> |
| Data Rate                     | From the drop-down list, select the available transmit data rates of the wireless network.  |
| Channel Width (802.11n only)  | From the drop-down list, select the available channel width. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.   |
| Guard Interval (802.11n only) | From the drop-down list, select a value that protects transmissions from interference. A shorter guard interval improves performance, but some legacy devices can operate only with a long guard interval.  |

Table 20. Wireless settings (continued)

| Setting   | Description   |
|---|---|
| RTS Threshold (0-2347)                            | Enter the size of the Request to Send (RTS) threshold packet.<br>The RTS threshold is related to the transmission mechanism (CSMA/CA or CSMA/CD) for the packets. If the packet size is equal to or less than this threshold, the data frame is transmitted immediately; if the packet size is larger than the specified value, the transmitting station needs to send an RTS threshold packet to the receiving station, and then should wait for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data. |
| Fragmentation Length (256-2346)                   | Enter the size that specifies the maximum fragmentation length for data packets. Packets larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length needs to be an even number.   |
| Beacon Interval (100-1000)                        | Enter the time interval for each beacon transmission that allows the access point to synchronize the wireless network.  |
| Aggregation Length (1024-65535)<br>(802.11n only) | Enter the maximum length of Aggregated MAC Protocol Data Unit (AMPDU) packets. Larger aggregation lengths can lead to better network performance. Aggregation is a mechanism used to achieve higher throughput.   |
| AMPDU<br>(802.11n only)                           | Select the <b>On</b> radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU can lead to better network performance. Select the <b>Off</b> radio button to disable this option.  |
| RIFS Transmission<br>(802.11n only)               | Select the <b>On</b> radio button to enable the Reduced Interframe Space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS can lead to better network performance. Select the <b>Off</b> radio button to disable this option.  |
| DTIM Interval (1-255)                             | Enter the Delivery Traffic Indication Message (DTIM) or the data beacon rate that you want to use. This sets the message period of the beacon delivery traffic indication in multiples of beacon intervals.   |
| Preamble Type<br>(802.11b/bg only)                | Select one of the following radio buttons to specify the preamble type: <ul style="list-style-type: none"> <li>• <b>Auto.</b> Automatically handles both long and short preambles. A short transmit preamble provides better performance. Auto is the default setting.</li> <li>• <b>Long.</b> Enables a long transmit preamble to provide a more reliable connection or a slightly longer range.</li> </ul>  |

- Optionally, you can override the channel and transmission power for individual access points.

---

**Note:** If automatic Tx power control is enabled on the basic RF Management screen (see [Basic RF Management](#) on page 102), you cannot configure the transmission power on the Basic Wireless Settings screen. You need to disable automatic Tx power control to enable the Tx Power drop-down list on the Basic Wireless Settings screen.

---

The table on the Basic Wireless Settings screen shows the access points that are managed in the profiles of the basic profile group and to which the channel allocation and basic RF management settings apply. Use the drop-down lists to change channel or transmission power settings.

**Table 21. Basic profile group: channel and transmission power settings**

| Setting              | Description   |
|----------------------|---|
| AP Name              | The name of the access point.   |
| Access Point Channel | <p>Override these settings only if there is a specific need. From the drop-down list, select a channel and frequency for the access point to operate in.</p> <p><b>Note:</b> Changing a channel might temporarily affect the traffic on the access point.</p> <p><b>Note:</b> By default, the access point's channel and frequency are set to the ones that are enabled for the radio and profile group. If the channel and frequency are not available on the access point, then the channel and frequency are set to the ones providing the highest performance. For more information, see <a href="#">Configure Channels</a> on page 99.</p> |
| Tx Power             | <p>From the drop-down list, select the transmission power of the access point.</p> <p><b>Note:</b> By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management screen. For more information, see <a href="#">Basic RF Management</a> on page 102.</p>   |

6. Click **Apply** to save your settings.

## Advanced Wireless Configuration for Profile Groups

NETGEAR recommends using the default wireless settings unless you have specific reasons to change them. You can configure wireless settings for the basic profile group (see the previous section) or for advanced profile groups.

➤ **To configure wireless settings for profile groups:**

1. Select **Configuration > Wireless > Advanced > Wireless**. The Advanced Wireless Settings screen displays:



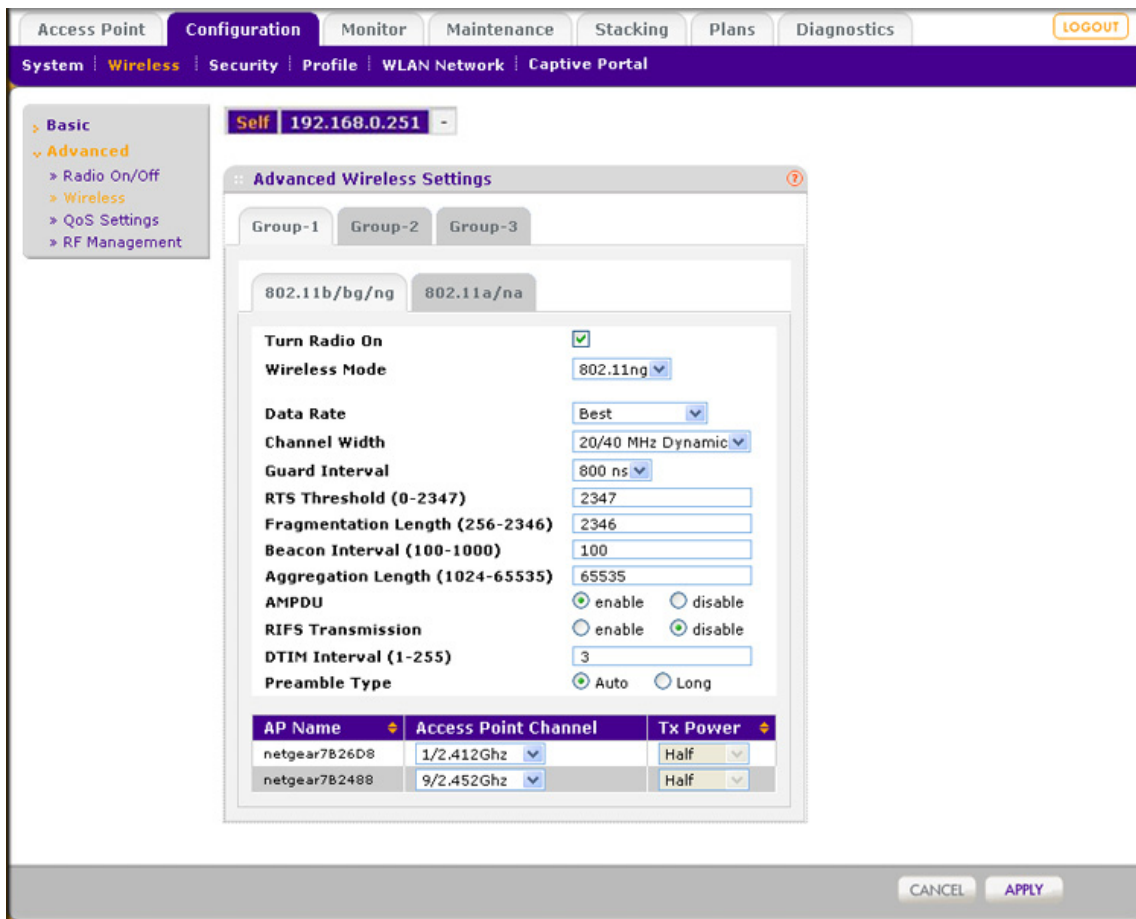


Figure 45.

2. Click a tab to select a profile group.
3. Click a tab to select a radio.
4. Select the **Turn Radio On** check box to enable configuration of the wireless settings.

---

**Note:** If automatic channel allocation is enabled on the Channel Allocation screen (see [Configure Channels](#) on page 99), you cannot configure the wireless settings on the Advanced Wireless Settings screen. You need to disable automatic channel allocation to be able to configure the wireless settings.

---



---

**Note:** You cannot configure the wireless settings if there are no access points assigned to a radio in a profile group.

---

5. Configure the settings as explained in [Table 20](#) on page 94.

6. Optionally, you can override the channel and transmission power for individual access points.

---

**Note:** If automatic Tx power control is enabled on the advanced RF Management screen (see [Advanced RF Management for Profile Groups](#) on page 104), you cannot configure the transmission power on the Advanced Wireless Settings screen. You need to disable automatic Tx power control to enable the Tx Power drop-down list on the Advanced Wireless Settings screen.

---

The table on the Advanced Wireless Settings screen shows the access points that are managed in the profiles of the selected profile group and to which the channel allocation and advanced RF management settings apply. Use the drop-down lists to change channel or transmission power settings.

**Table 22. Advanced profile groups: channel and transmission power settings**

| Setting              | Description   |
|----------------------|---|
| AP Name              | The name of the access point.   |
| Access Point Channel | <p>Override these settings only if there is a specific need. From the drop-down list, select a channel and frequency for the access point to operate in.</p> <p><b>Note:</b> Changing a channel might temporarily affect the traffic on the access point.</p> <p><b>Note:</b> By default, the access point's channel and frequency are set to the ones that are enabled for the radio and profile group. If the channel and frequency are not available on the access point, then the channel and frequency are set to the ones providing the highest performance. For more information, see <a href="#">Configure Channels</a> on page 99.</p> |
| Tx Power             | <p>From the drop-down list, select the transmission power of the access point.</p> <p><b>Note:</b> By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management screen. For more information, see <a href="#">Advanced RF Management for Profile Groups</a> on page 104.</p>   |

7. Click **Apply** to save your settings.

## Configure Channels

**CAUTION:**

Do not disable channel allocation unless you are debugging or there is an extreme situation that affects the channels.

Automatic channel allocation distributes channels across the managed access points to reduce interference. Each wireless controller allocates channels for its managed access points, regardless of their configured security profiles. The wireless controller detects interference, traffic load on the access point, and neighborhood maps to determine the best channel for an access point. This information, collected over the previous 24 hours, is used by the controller to determine the best possible channel for the access point.

You can configure channel allocation to allow allocation of only the specified channels when channel allocation is scheduled to run. This ensures that the access points use only the channels allowed according to administration policies.

---

**Note:** Click the **Run Now** button to immediately allocate channels when circumstances warrant, such as when you add a new access point or change your network. Running channel allocation might temporarily affect traffic on the managed access points in the network.

---

To adhere to best practices when adjusting channel allocation, NETGEAR recommends the following:

- Select channels that do not overlap. For example, for 2.4 GHz, use channels 1, 6, and 11.
- Schedule channel allocation once a day at times when the fewest clients are expected to be connected. This allows better management of available bandwidth during the day.

---

**Note:** The allocated channels apply to all access points, irrespective of whether they are managed in profiles of the basic profile group or profiles of an advanced profile group.

---

---

**Note:** You *can* override the general channel allocation settings for individual access points on the Basic Wireless Settings screen and on the Advanced Wireless Settings screen. For more information, see [Configure Wireless Settings](#) on page 93.

---

➤ To change the channel allocation:

1. Select **Configuration > Wireless > Basic > Channel Allocation**. The Channel Allocation screen displays:

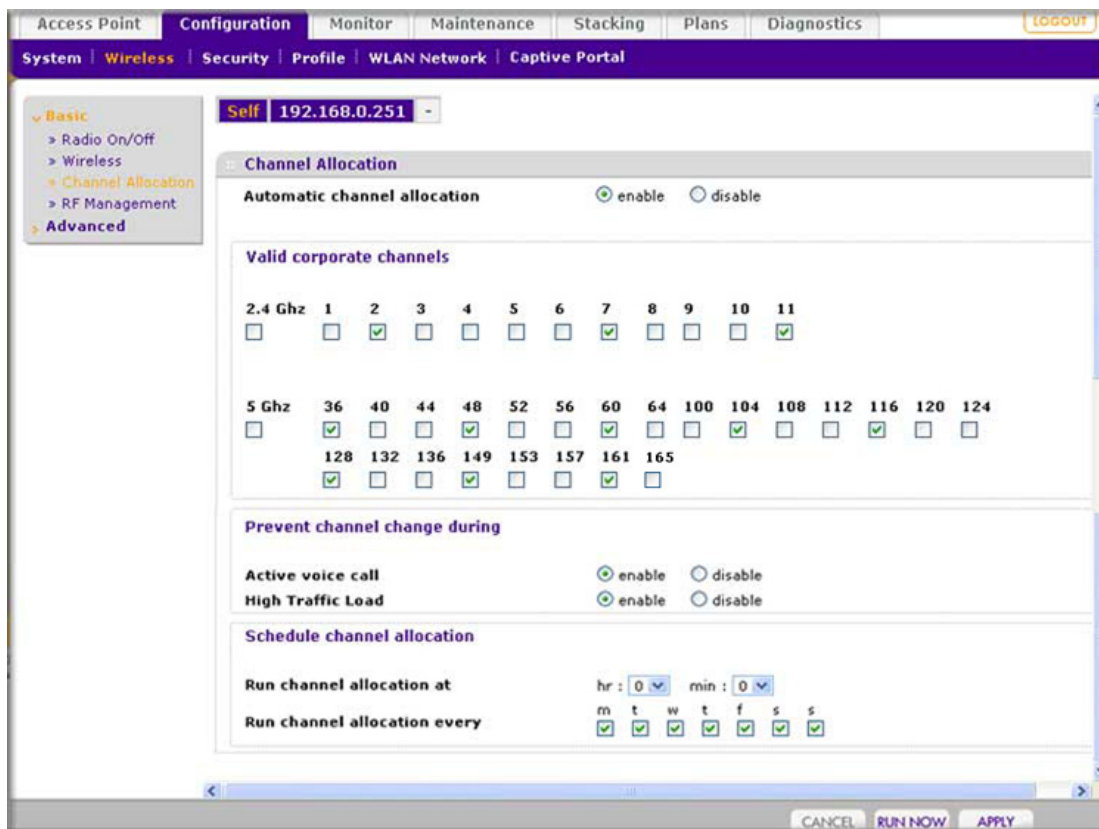


Figure 46.

2. Configure the settings as explained in the following table:

Table 23. Channel allocation settings

| Setting                      | Description   |
|------------------------------|---|
| Automatic channel allocation | Ensure that the <b>Enable</b> radio button is selected during normal operation. Automatic channel allocation distributes channels across the managed access points to reduce interference. To disable automatic channel allocation, select the <b>Disable</b> radio button.   |
| Valid corporate channels     | Specify the wireless band by selecting the <b>2.4 GHz</b> or <b>5 GHz</b> check box. For each wireless band, the following applies: <ul style="list-style-type: none"> <li>• You can remove one or more channels from the list of available channels by clearing its check box. This is a good way to avoid interference with competing equipment such as in a medical setting where medical devices use a specific channel.</li> <li>• You cannot add channels. The wireless controller determines available channels based on the country or region that you specified on the General Settings screen (see <a href="#">Configure General Settings</a> on page 63).</li> </ul> |

Table 23. Channel allocation settings (continued)

| Setting  | Description                  |  |
|--|------------------------------|--|
| Prevent channel change during<br><br><b>Note:</b> If the wireless controller is prevented from reallocating a channel because it is in use, the wireless controller checks again at the next scheduled channel allocation. | Active voice call            | Select the <b>Enable</b> radio button to prevent channel changes during voice calls. Select the <b>Disable</b> radio button to allow channel changes during voice calls.                 |
|  | High Traffic Load            | Select the <b>Enable</b> radio button to prevent channel changes during a high traffic load. Select the <b>Disable</b> radio button to allow channel changes during a high traffic load. |
| Schedule channel allocation<br><br><b>Note:</b> NETGEAR recommends that you schedule channel allocation once a day at times when the fewest clients are expected to be connected.  | Run channel allocation at    | From the drop-down lists, select the hour and minutes when the channel allocation should run.  |
|  | Run channel allocation every | Select the check boxes to specify the day or days when the channel allocation should run.  |

- Optionally, click the **Run Now** button to run the channel allocation immediately and apply the selected channels to connected managed access points.

**IMPORTANT:**

**Changing channels might temporarily affect traffic on the managed access points in the network.**

- Click **Apply** to save your settings.

## Specify RF Management

You can configure centralized RF management for the basic profile group on the basic RF Management screen. If you use advanced profile groups, you can use the advanced RF Management screen to customize settings for each profile group. RF management optimizes the channel allocation for access points based on clients, user data traffic, and the nearby RF environment of access points.

The wireless controller periodically checks the radio neighborhood maps and detects changes in the radio neighborhood maps or loss of connectivity to the controller by an access point. When WLAN healing is used, if an access point goes down or loses connectivity, other access points share its load to avoid a coverage hole. To do this, the other access points increase their transmit power. WLAN healing is configured per security profile group and runs between the access points sharing a common security configuration.

The wireless controller has the capacity for automatic WLAN healing through the following features:

- **Automatic channel allocation.** Allows an access point channel to be distributed automatically by the wireless controller across the access points on a floor to reduce interference. Auto channel allocation takes into consideration the floor plan, interference, traffic load on the access point, and neighborhood floor maps, as well as the wireless mode and bandwidth (also referred to as channel width) to provide the best channel for the access point. For information about how to configure auto channel allocation, including the option to skip auto channel allocation if there is a heavy traffic load or voice activity, see [Configure Channels](#) on page 99.
- **Automatic transmission power.** Automatically determines the optimum transmit power of an access point based on the coverage requirement. The access point scans its neighborhood to determine the RF environment to minimize neighboring access point interference, leakage across floors, and coverage holes.

When you configure WLAN healing, NETGEAR recommends the following:

- Configure the WLAN self-healing wait time to a value greater than the access point reboot time, which is usually 1 minute. This allows for fluctuations in the power of nearby access points when access points are rebooted.
- The number of neighbors to participate in WLAN self-healing should not be very large (three to four usually suffices in most deployments). This avoids too many access points increasing power for a single failed access point.

---

**Note:** You can override the default transmission power settings for individual access points on the Basic Wireless Settings screen and on the Advanced Wireless Settings screen. For more information, see [Configure Wireless Settings](#) on page 93.

---

## Basic RF Management

➤ **To configure basic RF management:**

1. Select **Configuration > Wireless > Basic > RF Management**. The basic RF Management screen displays:

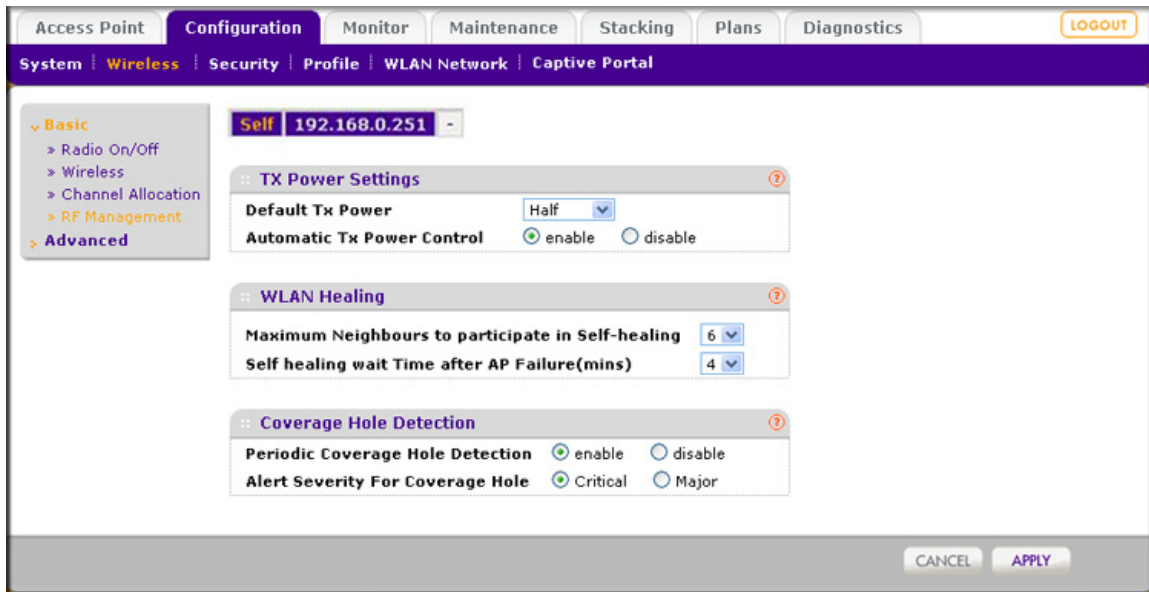


Figure 47.

2. Configure the settings as explained in the following table:

Table 24. RF management settings

| Setting  | Description  |
|--|--|
| <b>TX Power Settings section</b>                 |  |
| Default Tx Power                                 | Make a selection from the drop-down list to specify how the transmission (Tx) power is configured on the access points: <b>Full, Half, Quarter, Eighth, or Minimum</b> .<br>When automatic Tx power control is enabled, the selection from the drop-down list is used as the initial power level for the access points.  |
| Automatic Tx Power Control                       | Select the <b>Enable</b> radio button to enable automatic Tx power control: <ul style="list-style-type: none"> <li>• When a client attempts to connect to an access point at low power, the access point's Tx power is automatically increased above the default level.</li> <li>• When there are overlapping coverage areas, the access point's Tx power is automatically decreased below default level.</li> </ul> Select the <b>Disable</b> radio button to disable automatic Tx power control. |
| <b>WLAN Healing section</b>                      |  |
| Maximum Neighbors to Participate in Self-healing | From the drop-down list, select the maximum number of neighboring access points that increase or decrease power to cover for a failing access point. Selecting 0 (zero) disables this feature. Use close neighbors, not a distant access point, and do not use all access points.  |
| Self healing wait Time after AP Failure          | From the drop-down list, select the number of minutes to validate ( that is, wait) before confirming a failed access point and increasing transmit power to cover the area. Enter a value greater than the access point reboot time, which is usually 1 minute. This allows for fluctuations in the power of nearby access points when access points are rebooted.   |

Table 24. RF management settings (continued)

| Setting                                | Description  |
|--|--|
| <b>Coverage Hole Detection section</b> |  |
| Periodic Coverage Hole Detection       | Select the <b>Enable</b> radio button to allow coverage hole detection to run in the background periodically. Select the <b>Disable</b> radio button to disable this option.   |
| Alert Severity for Coverage Hole       | Select a radio button to specify the type of alarm severity to be associated with a coverage-hole detection event on the Logs & Alerts screen: <ul style="list-style-type: none"> <li>• <b>Critical</b></li> <li>• <b>Major</b></li> </ul> For more information, see <a href="#">Configure Alarm Notification Settings</a> on page 72. |

3. Click **Apply** to save your settings.

## Advanced RF Management for Profile Groups

You can configure centralized RF management for profile groups on the advanced RF Management screen.

- **To configure advanced RF management:**

1. Select **Configuration > Wireless > Advanced > RF Management**. The advanced RF Management screen displays:

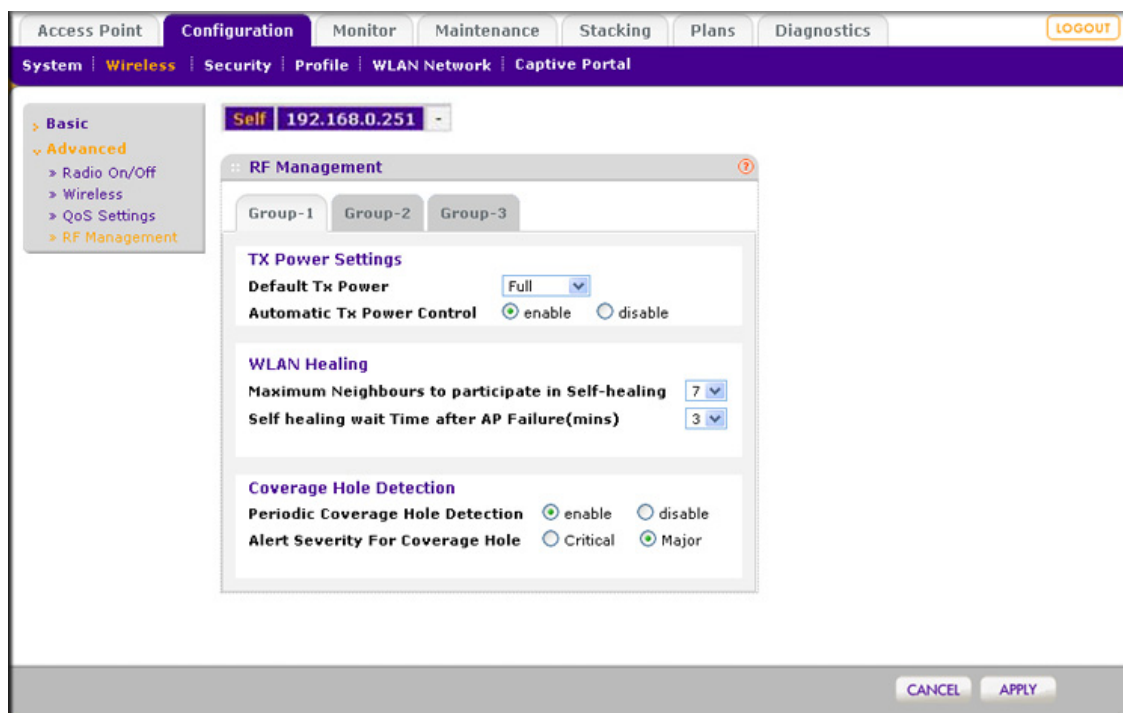


Figure 48.



2. Click a tab to select a profile group.
3. Configure the settings as explained in the previous table.
4. Click **Apply** to save your settings.

## Configure QoS for Profile Groups

Quality of Service (QoS) works by default. Change QoS only if there is a reason, such as device vendor specifications that require you to use different settings.

Using QoS Wi-Fi MultiMedia (WMM) ensures that the applications that require better throughput and performance are provided special queues with higher priority. For example, video and audio applications are given higher priority over applications such as FTP. WMM defines the following four queues in decreasing order of priority:

- **Voice.** The highest priority queue with minimum delay, which makes it ideal for applications such as voice over IP (VoIP) and streaming media.
- **Video.** The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort.** The medium priority queue with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background.** Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

QoS prioritization and coordination of wireless medium access is on. QoS settings on the access point control downstream traffic, flowing from the access point to the client station (*AP* Enhanced Distributed Channel Access [EDCA] parameters) and the upstream traffic flowing from the client station to the access point (*Station* EDCA parameters).

### ➤ To configure the QoS settings for profile groups:

1. Select **Configuration > Wireless > Advanced > QoS**. The Advanced QoS Settings screen displays:

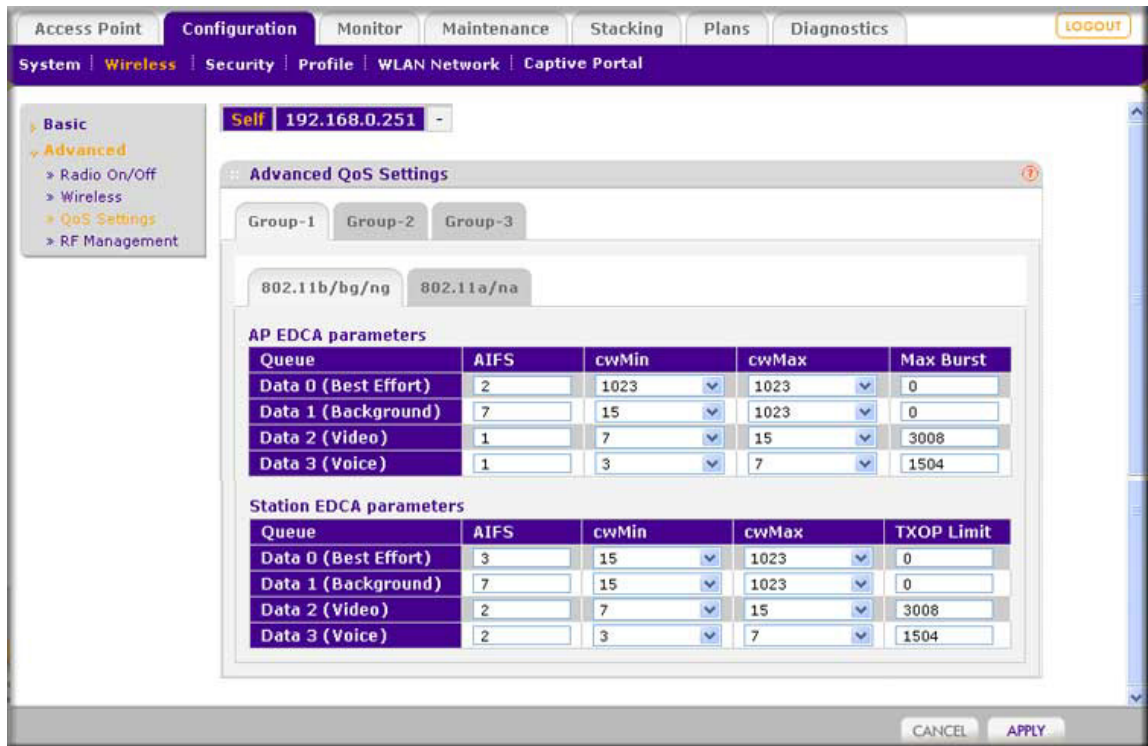


Figure 49.

2. Click a tab to select a profile group.
3. Click a tab to select a radio.

This screen lets you modify the QoS settings per profile group and per radio for upstream traffic flowing from the station (that is, the wireless client) to managed access points and the downstream traffic flowing from managed access points to the station. These settings are applied only to managed access points that are capable of supporting these settings.

Disabling WMM deactivates QoS control of station EDCA parameters for upstream traffic flowing from the client station to the access point. (You can change the settings for the station EDCA parameters, but these settings do not take effect until you enable WMM.) However, when WMM is disabled, you can still set some parameters for downstream traffic flowing from the access point to the client station (AP EDCA parameters), and these settings do take effect even when WMM is disabled.

4. Configure the settings as explained in the following table:

Table 25. QoS settings

| Setting    | Description   |
|------------|---|
| AIFS       | Specify a wait time (in milliseconds) for data frames. Valid values for Arbitration Inter-Frame Space (AIFS) are 1 through 255.   |
| CwMin      | Specify an upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for this field are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for the Minimum Contention Window (CwMin) needs to be lower than the value for the Maximum Contention Window (CwMax). |
| CwMax      | Specify an upper limit (in milliseconds) for the doubling of the random backoff value. Valid values for this field are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for the Maximum Contention Window (CwMax) needs to be higher than the value for Minimum Contention Window (CwMin).                                |
| Max Burst  | Specify (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9. The maximum burst length applies only to AP EDCA parameters.       |
| TXOP Limit | Specify the Transmission Opportunity (TXOP) limit. The TXOP limit applies only to station AP EDCA parameters and specifies the maximum period during which the client station client can initiate transmissions.  |

5. Click **Apply** to save your settings.

## Configure Load Balancing

Load balancing allows the wireless controller to distribute access point clients equally among access points. You configure load balancing per type of access point model and per radio. There are two criteria, the maximum number of clients and the signal strength.

- **Maximum number of clients.** If more than the maximum number of clients per access points try to associate, they are pushed to another access point.
- **Signal strength.** Signal strength determines speed. If many clients are close, and one client is far, there is too much air time for the distant client. That client would have to wait while sending and receiving. You can give a threshold for signal strength, which is specified as a percentage, such as 50 percent.

---

**Note:** The load-balancing settings apply to all profiles, whether they are in the basic profile group or in advanced profile groups.

---

The controller supports balancing of load on the access points it manages. This is based on the number of clients connected to access points as well as signal quality of clients. When a client discovers access points (using probe requests) or sends association frames, the

access point determines whether or not to accept a client based on the number of clients already connected or the signal strength of the clients.

- **Number of clients.** When there are several access points and you want a good distribution of clients between the access points, set the maximum number of clients to a low value (compared to the total number of clients in an office or on a floor).
- **RSSI.** When you want only clients near access points to associate to the access point in situations where the throughput expectation is high, set the received signal strength indication (RSSI) to a high percentage. In situations in which the clients can be expected to be far away or there are fewer access points, set the RSSI to a lower value.

➤ **To configure load balancing:**

1. Select **Configuration > Profile > Basic > Load Balancing**. The Load Balancing screen displays:

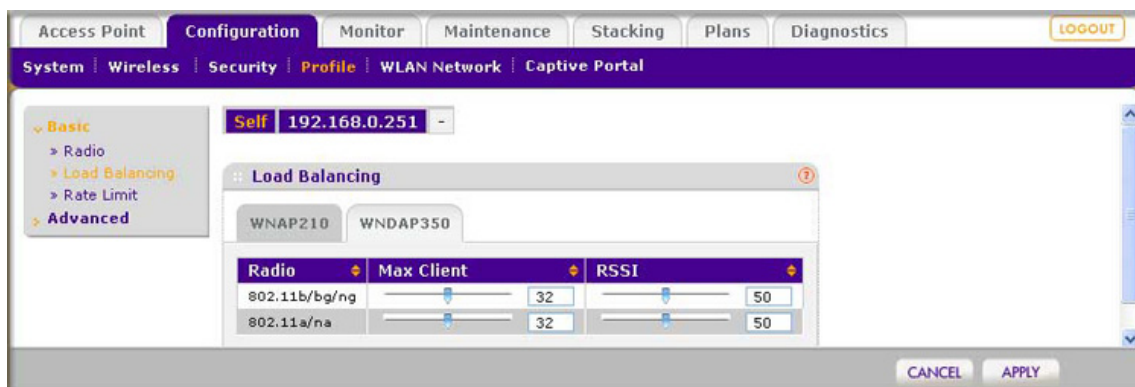


Figure 50.

2. If there are different access point models managed by the wireless controller, select a tab that represents a model.
3. Configure the settings as explained in the following table:

Table 26. Load-balancing settings

| Setting    | Description  |
|------------|--|
| Max Client | Use the slider to specify or enter the maximum number of wireless clients that can connect to each radio of an access point at one time. You can select a value of 64 to allow the maximum number that is supported by an access point.            |
| RSSI       | Use the slider to specify or enter the minimum signal quality in percentage (0 to 100 percent) expected from the wireless clients that connect to the access points. A value of 0 means this check is not enforced and load balancing is disabled. |

4. Click **Apply** to save your settings.

## Configure Rate Limiting

The available bandwidth is determined by the number of errors during transmission and the time that a packet spends in the transmission queues.

Within a profile group (including the basic profile group), you configure rate limiting separately for each wireless radio (2.4 GHz and 5 GHz). Within a profile group, for each wireless radio, rate limiting needs to add up to a maximum of 100 percent. (It can be less than 100 percent.)

For example, within one profile group, if there are four profiles that use the 802.11b/bg/ng mode and two profiles that use the 802.11a/na mode, you create one rate-limiting configuration for the four profiles that use the 802.11b/bg/ng mode and another rate-limiting configuration for the two profiles that use the 802.11a/na mode. The combined percentages of the four profiles that use the 802.11b/bg/ng mode cannot exceed 100 percent; similarly, the combined percentages of the two profiles that use the 802.11a/na mode cannot exceed 100 percent.

On each managed access point (or on each radio in a managed *dual-band* access point), the available bandwidth is distributed in the specified percentages among the profiles in a profile group. The percentage that is configured for a single profile is shared among all the clients connected to it.

If you do not want to configure rate limiting for a profile, configure rate limiting as 0 (zero) percent. This effectively disables rate limiting for that profile. A setting of 0 (zero) percent can work well profiles that are used for management, administration, or testing.

### Basic Rate Limiting

In the basic profile group, for each radio mode (802.11b/bg/ng mode and 802.11a/na mode), rate limiting per profile adds up to a maximum of 100 percent. (It can be less than 100 percent.) There is a tab for each wireless radio mode.

➤ **To configure basic rate limiting:**

1. Select **Configuration > Profile > Basic > Rate Limit**. The basic Rate Limit screen displays:

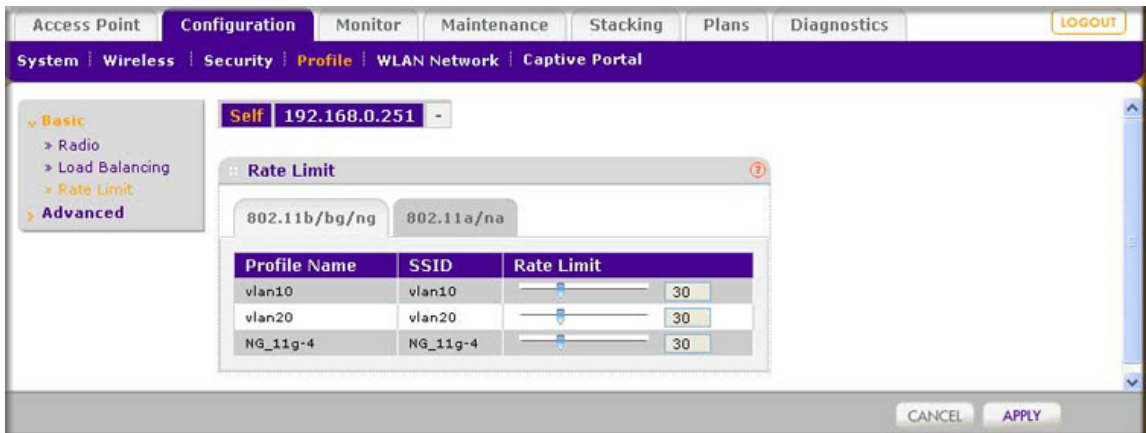


Figure 51.

2. Click a tab to select a radio.
3. For each profile on a wireless radio, specify the rate limit as a percentage. You can use the slider bars to adjust the values in the rate limit fields to the right of the slider bars. Make sure that the total percentages of all profiles on one wireless radio do not exceed 100 percent.
4. Click **Apply** to save your settings.

## Advanced Rate Limiting for Profile Groups

For each profile group, and for each radio mode (802.11b/bg/ng mode and 802.11a/na mode), rate limiting per profile adds up to a maximum of 100 percent. (It can be less than 100 percent.) There is a tab for each group and for each wireless radio mode.

### ➤ To configure advanced rate limiting:

1. Select **Configuration > Profile > Advanced > Rate Limit**. The advanced Rate Limit screen displays:

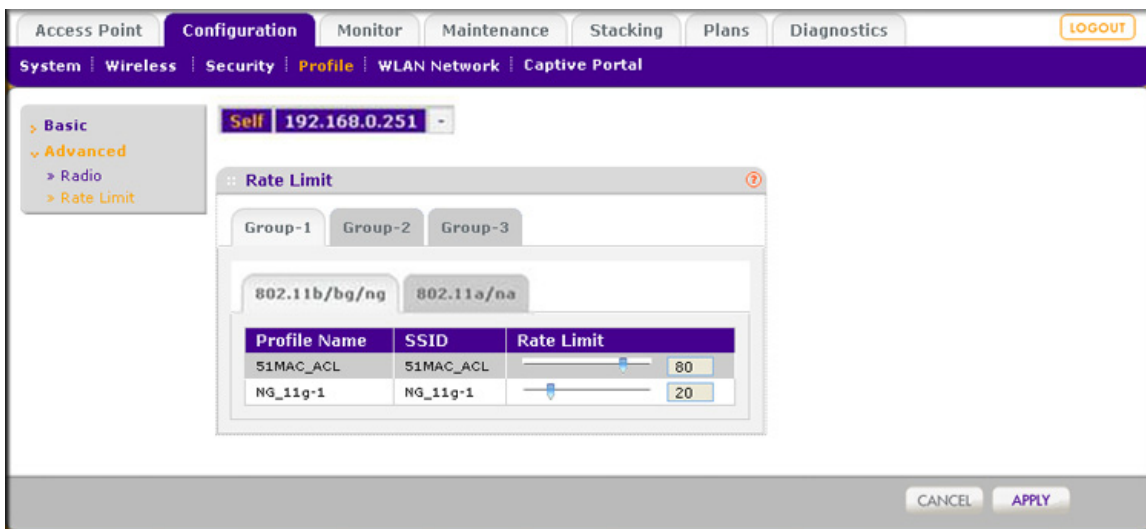


Figure 52.

2. Click a tab to select a profile group.
3. Click a tab to select a radio.
4. For each profile on a wireless radio in the selected profile group, specify the rate limit as a percentage. You can use the slider bars to adjust the values in the rate limit fields to the right of the slider bars. Make sure that the total percentages of all profiles on one wireless radio in the selected profile group do not exceed 100 percent.
5. Click **Apply** to save your settings.

# Configuring Network Access and Security

---

# 8

This chapter includes the following sections:

- [About Basic and Advanced Security Configurations](#)
- [Manage Rogue Access Points](#)
- [Manage MAC Authentication and MAC Authentication Groups](#)
- [Manage Authentication Servers and Authentication Server Groups](#)
- [Manage Guest Network Access](#)
- [Manage Users, Accounts, and Passwords](#)



## **IMPORTANT:**

**Before you use the wireless controller to push the configurations to your access points, first determine which profiles and security you need, configure authentication servers and MAC authentication as described in this chapter, and then complete configuration of the profiles that you intend to use (see [Chapter 6, Managing Security Profiles and Profile Groups](#)).**



## **CAUTION:**

If security is not set up, or is set up incorrectly, when the wireless controller pushes the configurations to the access points, you could accidentally wipe out all security, leaving your entire network open to access.

## About Basic and Advanced Security Configurations

The basic security configuration model (Configuration > Security > Basic) does not apply strictly to the basic profile group, nor does the advanced security configuration model (Configuration > Security > Advanced) apply strictly to advanced profile groups. The reason is that you apply an authentication server and a MAC ACL to an individual profile and not to a profile group.



- **Basic security settings.** You can apply the following security settings to *any* profile, whether in the basic profile group or in an advanced profile group:
  - Basic MAC authentication (the MAC ACL group that is called basic)
  - Basic authentication server (the RADIUS server that is called basic-Auth or the LDAP server that is called basic-LDAP)
- **Advanced security settings.** You can apply the following security settings to *any* profile, whether in the basic profile group or in an advanced profile group:
  - Advanced MAC authentication (the MAC ACLs that are, by default, called, Acl-1, Acl-2, Acl-3, and so on; you can change these default names)
  - Advanced authentication server (the RADIUS servers that are, by default, called Auth-1, Auth-2, Auth-3, and so on; you can change these default names)
- **Global security settings.** The following security settings apply to all profiles, whether in the basic profile group or in any of the advanced profile groups:
  - Basic rogue AP detection
  - Advanced rogue AP detection

## Manage Rogue Access Points

Rogue access point detection is disabled by default on the wireless controller. If you want to detect rogue access points, you need to enable rogue access point detection and specify how aggressively access points should scan for rogue access points. Scanning affects the service availability of the access point. If rogue access point detection is set up as aggressive, the access point scans often, at which time it is unavailable for clients to associate to it.

An access point is defined as rogue if:

- The access point's radio basic service set identifier (BSSID) is observed by any of the managed access points.
- The access point is seen transmitting on the Ethernet side on the same Layer 2 as the managed access points.
- At least one client is connected to the access point.

Any unmanaged access point not meeting all these conditions is classified as a neighbor.

The access points transmit broadcast frames on the Ethernet during the time access point radios are off-channel (and scanning).

---

**Note:** For the triangulation of the rogue access points to work, ensure that the access points are positioned correctly in the floor plan. See [View and Manage Heat Maps for Deployed Plans](#) on page 48.

---

## Configure Basic Rogue Detection Settings

In a basic setup you can set up one detection server. In an advanced setup you can create multiple detection servers (for more information, see [Configure Advanced Rogue Detection Settings](#) on page 116).

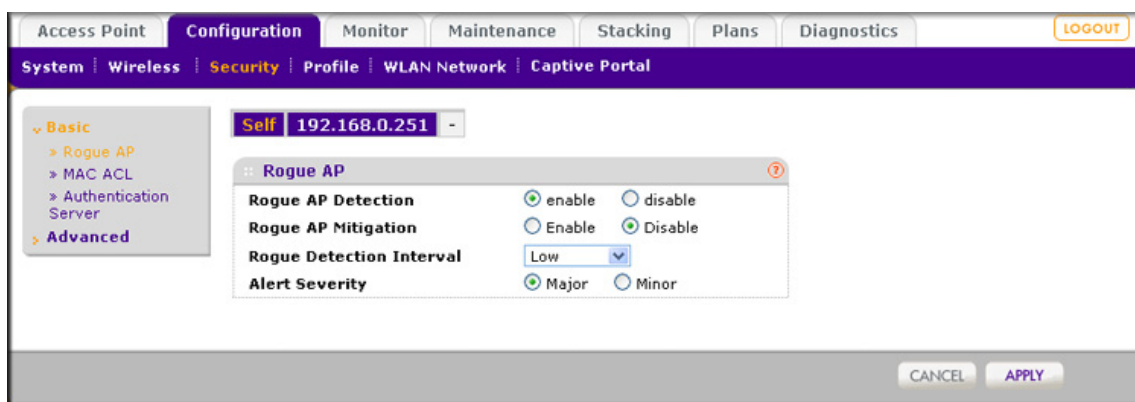
---

**Note:** If there are long delays in the network or clients are unexpectedly disconnected from access points, disable rogue access point detection and mitigation.

---

➤ **To set up a server to detect rogue access points:**

1. Select **Configuration > Security > Basic > Rogue AP**. The basic Rogue AP screen displays:



**Figure 53.**

The wireless controller can support a total of up to 512 access points from the known and unknown lists combined.

2. Configure the settings as explained in the following table:

**Table 27. Basic rogue AP detection settings**

| Setting            | Description   |
|--------------------|---|
| Rogue AP Detection | Select the <b>Enable</b> radio button to enable rogue AP detection, and to allow all neighbor as well as rogue access points to be displayed. A maximum of 512 access points (both neighbor and rogue) can be detected and maintained on the controller. The controller also maintains current count of the rogue access points as well rogue access points detected in the last 24 hours. When external storage is present, rogue access point information is saved for 72 hours. To disable rogue AP detection, select the <b>Disable</b> radio button. |

Table 27. Basic rogue AP detection settings (continued)

| Setting                  | Description   |
|--------------------------|---|
| Rogue AP Mitigation      | <p>Select the <b>Enable</b> radio button to enable rogue AP mitigation. Rogue mitigation does the following:</p> <ul style="list-style-type: none"> <li>• Prevents wireless clients from associating with rogue access points in the network.</li> <li>• Attempts to disconnect clients from rogue access points in the network.</li> <li>• Performs denial of service (DoS) attacks against rogue access points in the network.</li> </ul> <p>To disable rogue AP mitigation, select the <b>Disable</b> radio button.</p> <p><b>Note:</b> You can configure one or more access points to function in sentry mode to monitor the wireless network for faster detection and mitigation of rogue access points. For information about sentry mode, see <a href="#">Edit and Remove Access Point Information</a> on page 59.</p> |
| Rogue Detection Interval | <p>If rogue AP detection is enabled, select the detection interval from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Low.</b> With the Low setting, the access point goes off-channel less frequently than with the Medium, High, or Aggressive setting. NETGEAR recommends the Low setting, which should work well in most network configurations.</li> <li>• <b>Medium.</b></li> <li>• <b>High.</b></li> <li>• <b>Aggressive.</b> If you have security concerns, select the Aggressive setting to allow frequent scanning.</li> </ul>  |
| Alert Severity           | <p>If rogue AP detection is enabled, specify the severity of the alarm when a rogue access point is detected. Either select the <b>Major</b> or the <b>Minor</b> radio button.</p>  |

3. Click **Apply** to save your settings.

Because the neighbor and rogue access points are detected during off-channel scans, it typically takes about 10 minutes after the rogue AP detection is enabled for the neighbor and rogue access points to be detected and the known list (that is, the database with known access points) and unknown list (that is, the database with unknown access points) on the wireless controller to be populated.

---

**Note:** When rogue access point detection is enabled, access points intermittently go off channel for short periods, which can affect network performance. If security concerns are more important than network performance, you can temporarily select a high or aggressive rogue access point detection interval. If network performance is more important than security concerns, select a low or medium rogue access point detection interval, in which case security is addressed but network performance is not compromised. Under normal circumstances, NETGEAR recommends a low rogue access point detection interval.

---

## Configure Advanced Rogue Detection Settings

The advanced Rogue AP screen allows you to identify what could be an access point from a neighboring business that is known. As you identify them, mark them as known or unknown so that the wireless controller does not keep finding them and flagging them. This will help you to identify your own equipment that should be managed and the rogue access points that should be detected. A rogue access point has both a wireless and LAN connection. A neighbor is an access point with only a wireless connection, not a LAN connection.

➤ **To configure advanced rogue access point detection:**

1. Select **Configuration > Security > Advanced > Rogue AP**. The advanced Rogue AP screen displays:

The screenshot shows the 'Rogue AP' configuration page. At the top, there are navigation tabs: Access Point, Configuration (selected), Monitor, Maintenance, Stacking, Plans, and Diagnostics. Below these are system-level tabs: System, Wireless, Security (selected), Profile, WLAN Network, and Captive Portal. A left sidebar contains a tree view with 'Basic' expanded, and 'Advanced' containing 'Rogue AP' (selected), 'MAC ACL', and 'Authentication Server'. The main area is titled 'Rogue AP' and includes an 'Import Known List' field with a 'Browse...' button and radio buttons for 'Merge' and 'Replace'. Below this is a 'Rogue List' table with columns: MAC Address, SSID, Channel, Privacy, Last Beacon, Type, Rogue Type, and Name. The table contains 11 rows of data. At the bottom of the table are 'PREVIOUS' and 'NEXT' links. Below the table are 'Move to:' buttons for 'KNOWN' and 'UNKNOWN'. At the very bottom are 'APPLY', 'IMPORT', and 'CANCEL' buttons.

| <input type="checkbox"/> | MAC Address       | SSID         | Channel | Privacy   | Last Beacon              | Type     | Rogue Type | Name |
|--------------------------|-------------------|--------------|---------|-----------|--------------------------|----------|------------|------|
| <input type="checkbox"/> | e0:91:f5:0a:fc:50 | NG_11a       | 36      | Unsecured | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | e0:91:f5:a6:24:f0 | 1MSTR_g_wpa2 | 11      | Secured   | Mon Mar 14 13:54:47 2011 | Neighbor | Known      |      |
| <input type="checkbox"/> | e0:91:f5:0a:f0:f0 | wc-2-g0-g0   | 6       | Secured   | Mon Mar 14 13:49:46 2011 | Neighbor | Known      |      |
| <input type="checkbox"/> | 00:22:3f:85:33:9c | NETGEAR-3G   | 3       | Unsecured | Mon Mar 14 13:54:46 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | c0:3f:0e:b4:66:da | Bell66DA     | 11      | Secured   | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | e0:91:f5:0a:ef:10 | NG_11a       | 36      | Unsecured | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | e0:91:f5:0a:fb:54 | wc-1-g0-a4   | 40      | Unsecured | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:18:f3:ef:db:84 | Customer ID  | 11      | Secured   | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | e0:91:f5:0a:fb:50 | wc-3-g0-a0   | 40      | Secured   | Mon Mar 14 13:54:47 2011 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:18:4d:c3:fa:c4 | NETGEAR      | 3       | Unsecured | Mon Mar 14 13:54:46 2011 | Neighbor | Unknown    |      |

Figure 54.

The screen displays the Rogue List, which shows all detected rogue access points with essential information, including information about their last beacon. To scroll through the Rogue List, click **Next** or **Previous**.

As an option, you can import a list of access points from a file. For more information, see the next section.

2. Classify the access points in the Rogue List:
  - a. Select one or more check boxes that correspond to the access points, or select all access point in the Rogue List by selecting the check box at the top of the table.
  - b. Click one of the following two buttons, both of which are located below the Rogue List:
    - **Known.** Moves the selected access points to the known list. As an option, for each access point, you can enter a name in the Name column, so the access point is more easily identified.
    - **Unknown.** Moves the selected access points to the unknown list.

3. Click **Apply** to save your settings.

### *Importing a List of Known Access Points from a File*

You can import a list of known access points from a saved file. To do this, create a text file that includes the MAC address of each access point. This file needs to be a simple text file with one MAC address per line. The wireless controller can support a total of up to 512 access points from the known and unknown lists combined.

➤ **To import a list of known access points from a file:**

1. Create a text file that includes a list of MAC addresses for the access points. Each MAC address should be on a separate line with hard returns between lines as shown in the following example:

```
00:00:11:11:22:29
00:00:11:11:22:28
00:00:11:11:22:27
00:00:11:11:22:26
00:00:11:11:22:25
```

2. Select **Configuration > Security > Advanced > Rogue AP** to access the Rogue AP screen.
3. Click **Browse**, navigate to the file containing the list of known access points, and select it.
4. Next to Import Known List, select one of the following radio buttons:
  - **Merge**. Merges the list of access points that you intend to import with those that are already present in the Rogue List.
  - **Replace**. Replaces the access points that are present in the Rogue List with those in the file that you intend to import.
5. Click **Import**.
6. Click **Apply** to save your settings.

## Manage MAC Authentication and MAC Authentication Groups

MAC authentication lets you set up an external or a local access control list (ACL) with MAC addresses of clients to either allow or deny the network access privilege of the specified clients with the wireless controller–managed access point. The settings are applied only to managed access points.

---

**Note:** The wireless controller can support an aggregate number of 4096 MAC addresses for all its local ACLs.

---

## Guidelines for External MAC Authentication

### ➤ To use an external ACL:

1. Configure an ACL on an external RADIUS server.
2. On an Edit Profile screen (see [Chapter 6, Managing Security Profiles and Profile Groups](#)), next to MAC ACL, select the **External** radio button.
3. From the External Radius Server drop-down list, select an external authentication server.

The wireless controller consults the MAC ACL at initial client authentication. While a client roams, the wireless controller uses cached authentication information. After a client has disassociated from the access point and then attempts to reassociate again, the wireless controller once again consults the MAC ACL.

Note the following external RADIUS server guidelines:

- For each MAC authentication client, you need to configure a policy on the RADIUS server.
- During MAC authentication, the wireless controller sends the following information to the RADIUS server:
  - MAC address in the format xx:xx:xx:xx:xx:xx
  - user name
  - calling station ID
- The wireless controller uses CHAP as the authentication protocol with the RADIUS server.
- You can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server (see [Network Authentication and Data Encryption Options](#) on page 81), but not both. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2, you cannot use external MAC authentication but are limited to internal MAC authentication.

## Configure Basic Local MAC Authentication Settings

You would typically use the basic MAC authentication group in the profiles of a basic profile group of a small-scale network. However, you can assign the basic MAC authentication group to *any* profile, whether in the basic profile group or in an advanced profile group.

### ➤ To set up basic MAC authentication:

1. Select **Configuration > Security > Basic > MAC ACL**. The basic MAC Authentication screen displays:

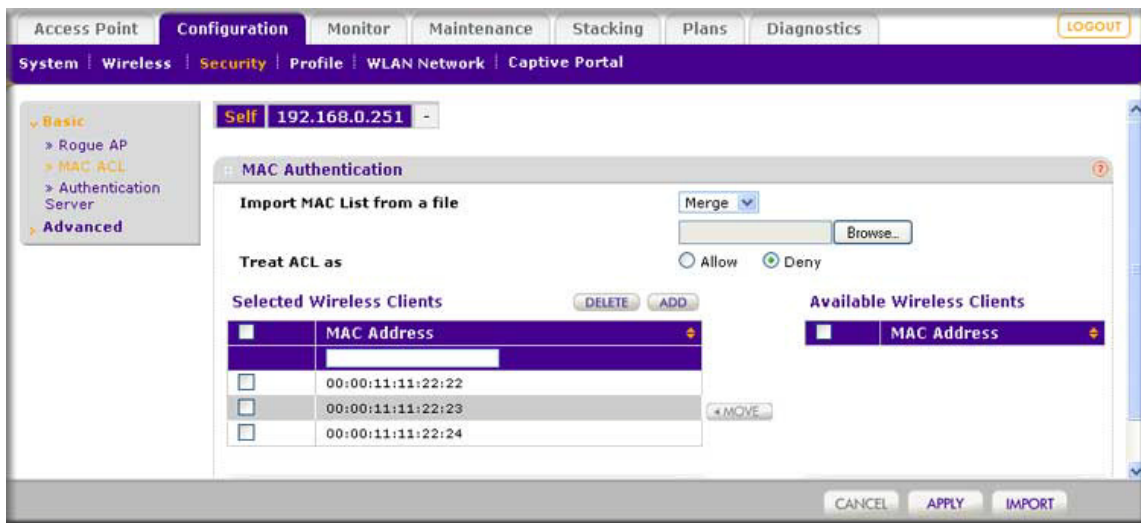


Figure 55.

As an option, you can import a list of MAC addresses from a file. For more information, see the next section.

2. Next to Trust ACL as, select one of the following radio buttons:
  - **Allow.** Network access is granted to the clients for which the MAC addresses are listed in the Selected Wireless Clients list.
  - **Deny.** Network access is denied to the clients for which the MAC addresses are listed in the Selected Wireless Clients list.
3. Add a wireless client to the Selected Wireless Clients list through one of the following methods:
  - Enter a MAC address in the MAC Address field, and then click **Add**.
  - Select a MAC address from the Available Wireless Clients list, and then click **Move**. The Available Wireless Clients list contains wireless stations that are present in the vicinity of the access point.

To delete a MAC address from the Selected Wireless Clients list, select the corresponding check box, and then click **Delete**.

**Note:** The wireless controller supports a maximum of 256 MAC addresses per SSID.

4. Click **Apply** to save your settings.

## Importing a MAC List from a File

You can import a precompiled list of MAC address from a saved file. This file needs to be a simple text file with one MAC address per line.

### ➤ To import a MAC list from a file:

1. Create a text file that includes a list of MAC addresses. Each MAC address should be on a separate line with hard returns between lines as shown in the following example:

```
00:00:11:11:22:29
00:00:11:11:22:28
00:00:11:11:22:27
00:00:11:11:22:26
00:00:11:11:22:25
```

2. Select **Configuration > Security > Basic > MAC ACL** to access the MAC Authentication screen.
3. Click **Browse**, navigate to the file containing the list of MAC addresses, and select it.
4. Make one of the following selections from the Import MAC List from a file drop-down list:
  - **Merge**. Merges the list of MAC addresses that you intend to import with those that are already present in the Selected Wireless Clients list.
  - **Replace**. Replaces the MAC addresses that are present in the Selected Wireless Clients list with those in the file that you intend to import.
5. Click **Import**.
6. Click **Apply** to save your settings.

## Configure Local MAC Authentication Groups

For greater security flexibility, you can create up to 8 MAC authentication groups (MAC ACLs) to block or allow network access privilege of different clients. You can assign any MAC authentication group, including the basic MAC authentication group, to *any* profile, whether in the basic profile group or in an advanced profile group.

### ➤ To set up a MAC authentication group:

1. Select **Configuration > Security > Advanced > MAC Authentication**. The advanced MAC Authentication screen displays:



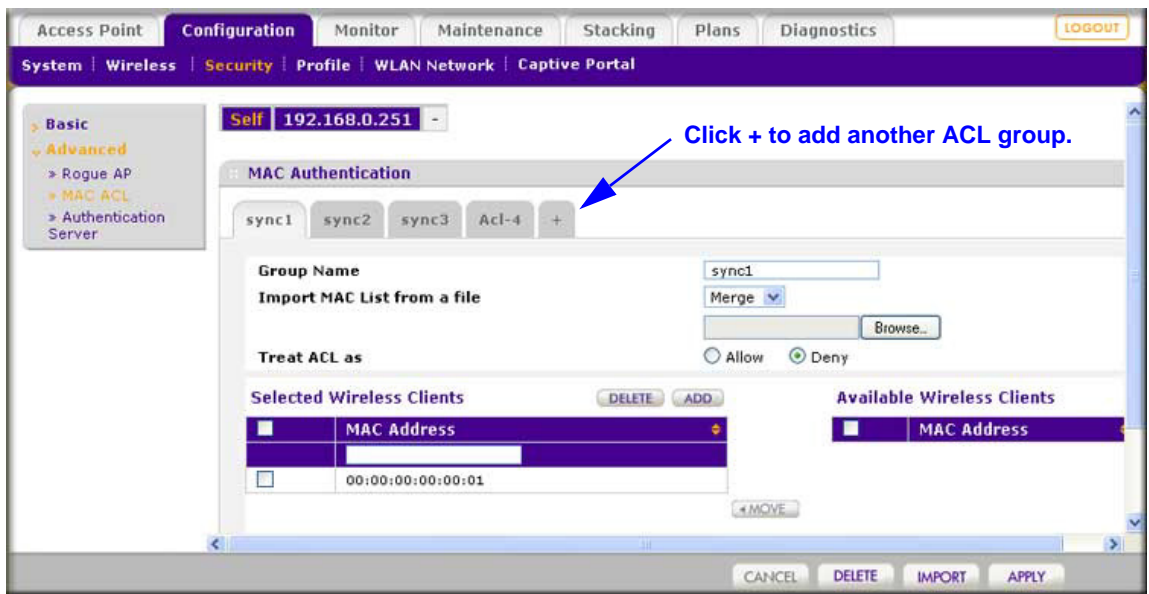


Figure 56.

- Click the + button to create an additional ACL group. The new ACL group displays on the advanced MAC Authentication screen, and the tab for the new ACL is automatically selected to let you configure the new group.

---

**Note:** By default, profile groups are named Acl-1, Acl-2, Acl-3, and so on. You can change these ACL group names.

---

- In the Group Name field, enter a unique name for the ACL group.
- Compile the Selected Wireless Clients list as explained in the previous section, [Configure Basic Local MAC Authentication Settings](#).

**Note:** The wireless controller supports a maximum of 256 MAC addresses per SSID.

- Click **Apply** to save your settings.

To delete an ACL group, select its tab, and then click **Delete**.

## Manage Authentication Servers and Authentication Server Groups

You can specify three types of authentication servers: internal, external RADIUS, and external LDAP:

- **Internal authentication server.** The wireless controller handles authentication. If you use this setting, set up Wi-Fi clients on the User Management screen (see [Manage Users, Accounts, and Passwords](#) on page 128.)
- **External RADIUS server.** You can define a basic external RADIUS server that you would typically use in the profiles of a basic profile group of a small-scale network. You need to specify its configuration on the basic Authentication Server screen (see the next section) so that you can select this authentication option during the configuration of a profile. As part of the advanced authentication server settings, you can define multiple external RADIUS servers that you would typically use in a more complex network with many profiles. You can then assign different RADIUS servers to different profiles.

By default, the external RADIUS server for the basic authentication group is called basic-Auth. You cannot change this name. By default, the external RADIUS authentication servers for the advanced authentication groups are called Auth1 through Auth8, and you *can* change these names. You can assign the basic-Auth server to an advanced profile group, and you can assign a RADIUS server of an advanced authentication group to the basic profile group.

See the following configuration guidelines for external RADIUS servers:

- For configuration guidelines for external MAC authentication, see [Guidelines for External MAC Authentication](#) on page 118.
- For configuration guidelines for external authentication of captive portal users, see [Configure Captive Portal Settings](#) on page 126.
- **External LDAP server.** You can define one external LDAP server (commonly referred to as an Active Directory [AD] server). You need to specify its configuration on the basic Authentication Server screen (see the next section) so that you can select this authentication option during the configuration of a profile.

By default, the external LDAP server for the basic authentication group is called basic-LDAP. You cannot change this name, and you cannot configure any LDAP servers for the advanced authentication groups. You can assign the basic-LDAP server to both the basic profile group and to advanced profile groups.

All three servers can be active so that the profiles that you set up can be configured to work with different authentication servers. For example, you could set up a guest profile with no authentication, an engineering profile that uses external RADIUS authentication, and a marketing profile that uses external LDAP authentication. The settings that you specify on the Authentication Server screen affect the selections available in the Network Authentication drop-down list and the corresponding Authentication Server field on the Edit Profile screens (see [Figure 36](#) on page 77 and [Figure 39](#) on page 86.)

## Configure Basic Authentication Server Settings

Use the basic Authentication Server screen to set up the internal authentication server, the basic external RADIUS server (which is called Auth-basic), and the external LDAP server (which is called Auth-LDAP). After you have set up these authentication servers, you can assign any of them to *any* profile, whether in the basic profile group or in an advanced profile group.

➤ **To configure a basic authentication server:**

1. Select **Configuration > Security > Basic > Authentication Server**. The basic Authentication Server screen displays:

The screenshot shows the configuration interface for the Authentication Server. The top navigation bar includes tabs for Access Point, Configuration, Monitor, Maintenance, Stacking, Plans, and Diagnostics, with a LOGOUT button on the right. Below the navigation bar, the breadcrumb trail is System | Wireless | Security | Profile | WLAN Network | Captive Portal. The left sidebar shows a tree view with Basic, Advanced, and Authentication Server options. The main content area displays the following settings:

- Self: 192.168.0.251
- Choose Authentication Server Type:
  - External RADIUS Server
  - Internal Authentication Server
  - External LDAP Server
- External LDAP Server:
  - Server IP: 1.1.1.1
  - Server Port: 389
  - User Base DN: OU=ldapusers,CN=var
  - Workgroup Name: varsalesdomain
  - Admin Domain: VARSALESDOMAIN.LOC
  - Domain Admin User: admin
  - Domain Admin Password: \*\*\*\*\*

At the bottom right, there are CANCEL and APPLY buttons.

Figure 57.

2. Select the radio button that corresponds to the authentication server that you want to set up:
  - External RADIUS Server
  - Internal Authentication Server
  - External LDAP Server

3. Configure the settings that correspond to the selected authentication server as described in the following table:

**Table 28. Authentication server settings**

| Setting                        | Description                       |  |   |
|--------------------------------|-----------------------------------|--|---|
| External RADIUS Server         | Primary Authentication Server     | Specify the IP address, port (default 1812), and shared secret.  | For information about shared secret requirements, see <a href="#">Table 54</a> on page 203. |
|                                | Secondary Authentication Server   | Specify the IP address, port (default 1812), and shared secret.  |   |
|                                | Primary Accounting Server         | Specify the IP address, port (default 1813), and shared secret.  |   |
|                                | Secondary Accounting Server       | Specify the IP address, port (default 1813), and shared secret.  |   |
|                                | Reauthentication time (Seconds)   | Specify the time after which reauthentication occurs for all wireless clients.   |   |
|                                | Update Global Key Every (Seconds) | Select the check box to enable update of the global key, and specify the interval (in seconds) after which the global key is updated for all wireless clients. |   |
| Internal Authentication Server | Reauthentication Time (seconds)   | Specify the reauthentication time (in seconds) after which reauthentication occurs for all wireless clients.   |   |
|                                | Update Global Key Every (seconds) | Select the check box to enable update of the global key, and specify the interval (in seconds) after which the global key is updated for all wireless clients. |   |
| External LDAP Server           | Server IP                         | Specify the IP address of the external active directory (AD) authentication server.  |   |
|                                | Server Port                       | Specify the port of the external AD server. The default is port 389.   |   |
|                                | User Base DN                      | Specify the user base distinguished name (DN) on the AD server.  |   |
|                                | Workgroup Name                    | Specify the workgroup name on the AD server.   |   |
|                                | Admin Domain                      | Specify the administrative domain on the AD server.  |   |
|                                | Domain Admin User                 | Specify the user name for the administrative domain.   |   |
|                                | Domain Admin Password             | Specify the password for the administrative domain.<br><br><b>Note:</b> For information about password requirements, see <a href="#">Table 54</a> on page 203. |   |

4. Click **Apply** to save your settings.

## Configure RADIUS Authentication Server Groups

For greater security flexibility, you can create up to 8 external RADIUS servers to authenticate different groups of users. After you have set up these authentication servers, you can assign any of them, including the basic RADIUS server, to *any* profile, whether in the basic profile group or in an advanced profile group.

➤ **To set up a RADIUS authentication group:**

1. Select **Configuration > Security > Advanced > Authentication Server**. The advanced Authentication Server screen displays:

The screenshot shows the 'Authentication Server' configuration page. At the top, there are tabs for 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Stacking', 'Plans', 'Diagnostics', and 'LOGOUT'. Below these are sub-tabs for 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. The 'Security' sub-tab is active, and the 'Advanced' section is expanded. The main configuration area is for 'Auth-3'. It includes a 'Group Name' field with 'Auth-3' entered. Below this is the 'External RADIUS Server' section, which contains a table with four rows: 'Primary Authentication Server', 'Secondary Authentication Server', 'Primary Accounting Server', and 'Secondary Accounting Server'. Each row has fields for 'IP Address', 'Port', and 'Shared Secret'. The 'Port' field is set to 1812 for authentication servers and 1813 for accounting servers. Below the table are fields for 'Reauthentication Time (Seconds)' and 'Update Global Key Every (Seconds)', both set to 0. At the bottom right, there are 'CANCEL', 'DELETE', and 'APPLY' buttons.

|                                 | IP Address | Port | Shared Secret |
|---------------------------------|------------|------|---------------|
| Primary Authentication Server   |            | 1812 | .....         |
| Secondary Authentication Server |            | 1812 | .....         |
| Primary Accounting Server       |            | 1813 | .....         |
| Secondary Accounting Server     |            | 1813 | .....         |

Figure 58.

2. Click the **+** button to create an additional authentication group. The new authentication group displays on the advanced Authentication Server screen, and the tab for the new authentication is automatically selected to let you configure the new group.

---

**Note:** By default, authentication groups are named Auth-1, Auth-2, Auth-3, and so on. You can change these authentication group names.

---

3. In the Group Name field, enter a unique name for the authentication group.
4. Specify the settings as described in the External RADIUS Server section in the previous table.
5. Click **Apply** to save your settings.

To delete an authentication group, select its tab, and then click **Delete**.

## Manage Guest Network Access

Users with management (admin) credentials—for example, receptionists or hotel clerks—can provision guests. Guests need to provide their email address, or both their email address and a password. These latter guests are referred to as captive portal users, for which you need to set up a captive portal and captive portal user credentials.

### Configure Captive Portal Settings

Captive portal authentication is typically used for hotspot users and paying guests such as hotel guests who purchase access time for an Internet connection. You can configure a single captive portal only per wireless controller.

When you configure a captive portal, you can use either the wireless controller as a local authentication server for the captive portal clients, or you can configure an external RADIUS server for authentication. There are two types of portal settings:

- **Guest portal.** Use this portal if all wireless users are allowed to access the network by supplying only their email address. You do *not* need to define user names and passwords for these users.
- **Captive portal.** Use this portal type if wireless users need to supply their login name and password before being allowed access to the network. You need to define user names and passwords for these users (see [Manage Users, Accounts, and Passwords](#) on page 128).

---

**Note:** You cannot configure captive portal authentication if the network authentication uses an external RADIUS server. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), you cannot configure captive portal authentication; the network authentication needs to be Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK (see [Network Authentication and Data Encryption Options](#) on page 81).

---

Note these guidelines for captive portal user authentication and accounting through an external RADIUS server:

- You can use either the basic-Auth RADIUS server or a RADIUS server of an advanced authentication group. You cannot use the external LDAP server.
- The wireless controller uses CHAP or MS-CHAP as the authentication protocol with the authentication server.
- The following RADIUS authentication variables are supported on the wireless controller:
  - User-Name
  - User-Password

- WISPr-Session-Terminate-Time
- Session-Timeout

If you change the values for any of these variables before the wireless client disassociates from the access point, the new values are not updated on the wireless controller.

- A managed access point can send accounting information to the external RADIUS server because the wireless controller functions as a proxy RADIUS client for the managed access point. The following RADIUS accounting variables are supported on the wireless controller:

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Gigawords
- Acct-Output-Gigawords

➤ **To configure a captive portal:**

1. Select **Configuration > Captive Portal**. The Portal Settings screen displays:

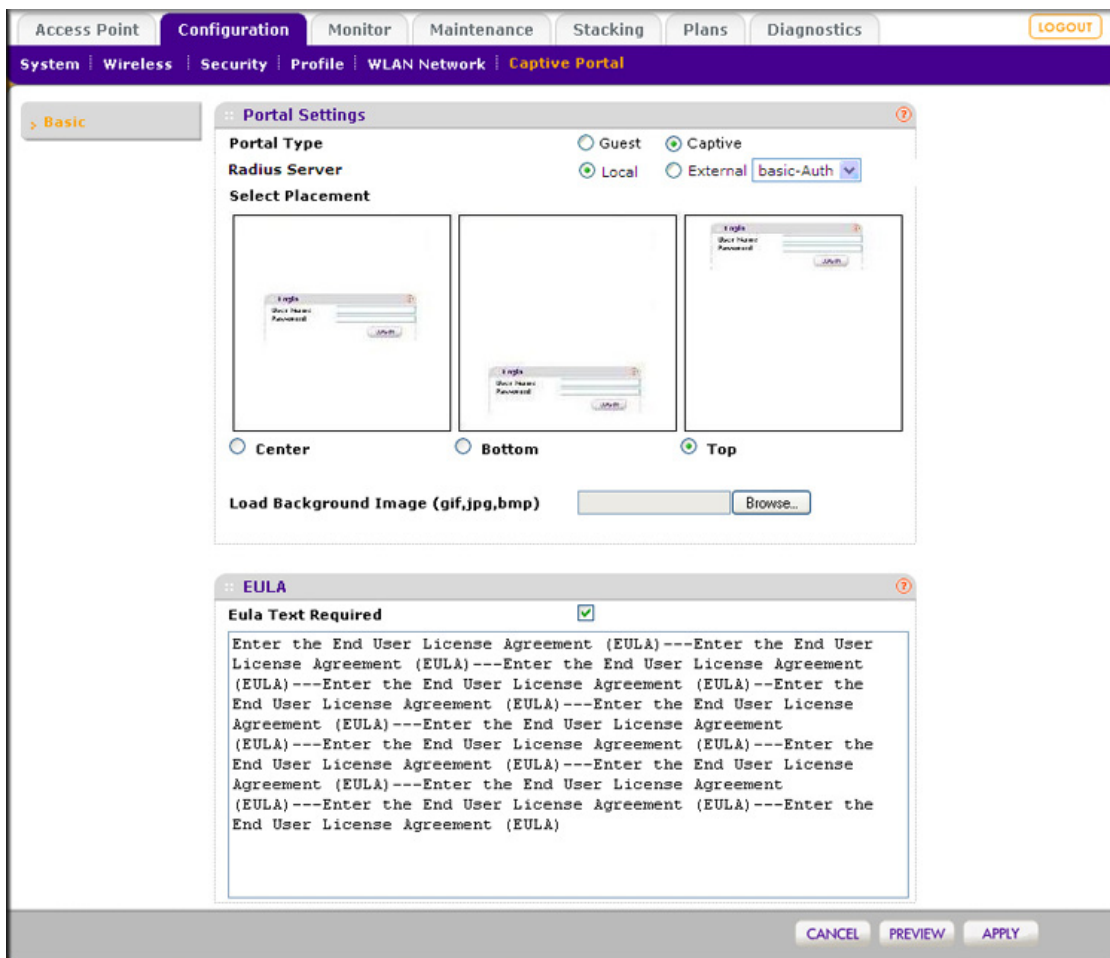


Figure 59.

- Configure the settings as described in the following table.

Table 29. Portal settings

| Setting  | Description  |
|--|--|
| <b>Portal Settings section</b>   |  |
| Portal Type  | Select one of the following radio buttons: <ul style="list-style-type: none"> <li>• <b>Guest.</b> A guest portal with a field for entering an email address. Guests do not need to provide a password and can have unlimited access to the network. You do not need to configure guest accounts.</li> <li>• <b>Captive.</b> A captive portal with a field for entering a login user name and a field for entering a password. If you select this option, the Radius Server radio buttons and drop-down list display. For information about how to configure captive portal users and accounts, see <a href="#">Manage Users, Accounts, and Passwords</a> on page 128.</li> </ul> |
| Radius Server<br><b>Note:</b> This setting is for a captive portal only. | Select one of the following radio buttons: <ul style="list-style-type: none"> <li>• <b>Local.</b> Use the local authentication server.</li> <li>• <b>External.</b> Select an external authentication server from the drop-down list.</li> </ul> <b>Note:</b> For information about setting up and enabling internal and external authentication servers, see <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122.   |
| Select Placement   | Select <b>Center</b> , <b>Bottom</b> , or <b>Top</b> to specify the location of the login prompt on the login screen.  |
| Load Background Image  | As an option, click <b>Browse</b> to navigate to and select an image file to be used for the background of the login screen. You can use a .gif, .jpg, or .bmp image.  |
| <b>EULA section</b>  |  |
| EULA Text Required   | Select this check box if you want to present the end user license agreement (EULA) on the guest login screen or captive portal login screen so users can view the EULA before they log in. Enter the EULA text in the text field.  |

- Click **Apply** to save your settings.
- Click **Preview** to display the portal settings that you have configured. The default URL for the captive portal is [http://192.168.0.250/guest\\_access/index.php](http://192.168.0.250/guest_access/index.php).

## Manage Users, Accounts, and Passwords

The wireless controller supports three types of users: management users, captive portal users, and Wi-Fi clients. *All* of these users need to provide their login name and password to be authenticated by the wireless controller's internal authentication server and to access the wireless controller's web management interface or wireless network.

- **Management users.** These users have access to the wireless controller's web management interface. There are four groups:
  - **Administrators.** Administrative users (admins) with read and write capabilities. These users can change the configuration of the wireless controller.



- **Read-only.** These users have access to the wireless controller's web management interface but can access only the Monitor main navigation tab and the Help main navigation tab. These users cannot change the configuration of the wireless controller.
- **Guest provisioning.** These users can configure only captive portal users, that is, they can access only the User Management configuration menu tab under the Maintenance main navigation tab.
- **License management only.** These users can configure only licenses, that is, they can access only the License configuration menu tab under the Maintenance main navigation tab (for more information, see [Manage Licenses](#) on page 149).
- **Captive portal users.** Users with credentials to access the captive portal and who are granted temporary access or access without expiration.
- **Wi-Fi clients.** Users with credentials to access the wireless network. These users do not need to use the captive portal or the guest portal to access the wireless network, nor is their access subject to expiration.

In addition to the users, you can also configure captive portal accounts that you use in combination with captive portal users. Accounts specify the period during which wireless access is available and the amount that is charged for it.

➤ **To add a user or an account:**

1. Select **Maintenance > User Management**. The User Management screen displays with the Management tab and associated screen in view.
2. Select one of the following tabs to display the associated screen:
  - **Management.** The Management screen displays. (This is the default screen that displays when you select **Maintenance > User Management**.)

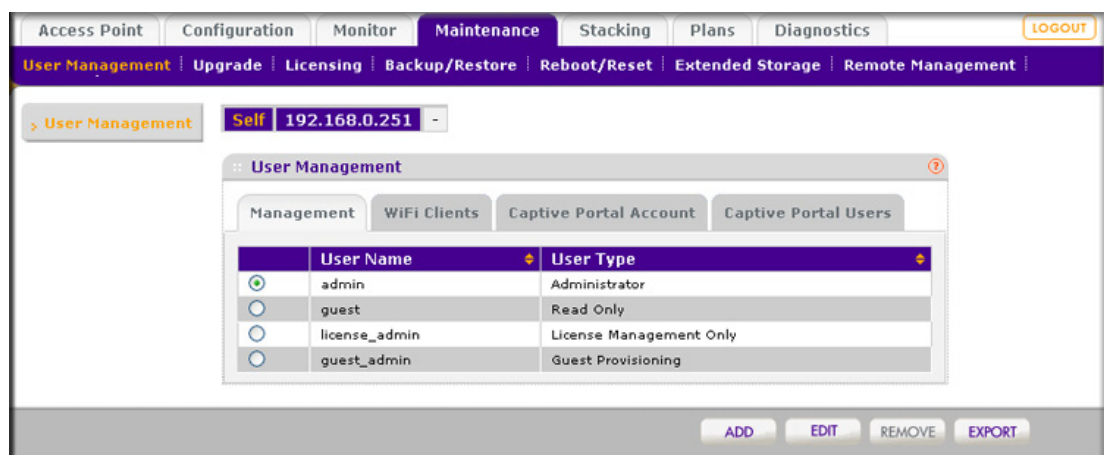


Figure 60.

- **WiFi Clients.** The WiFi Client screen displays:

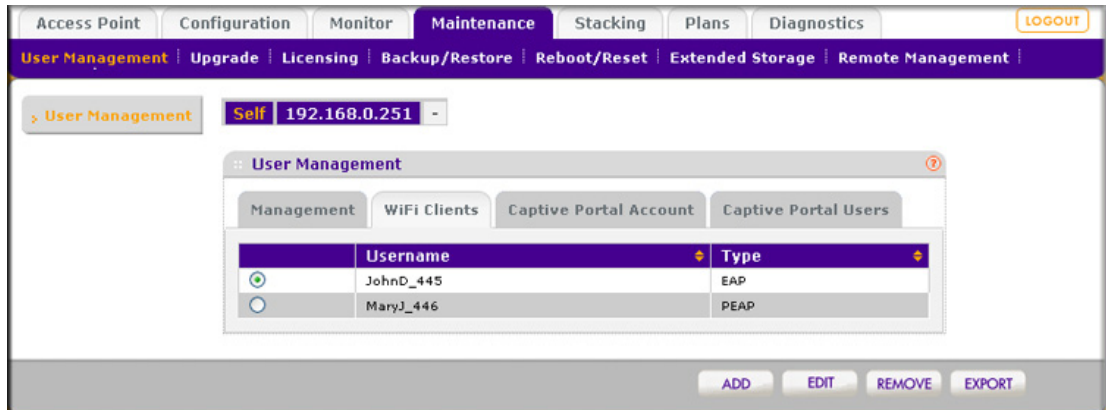


Figure 61.

- **Captive Portal Account.** The Captive Portal Account screen displays:

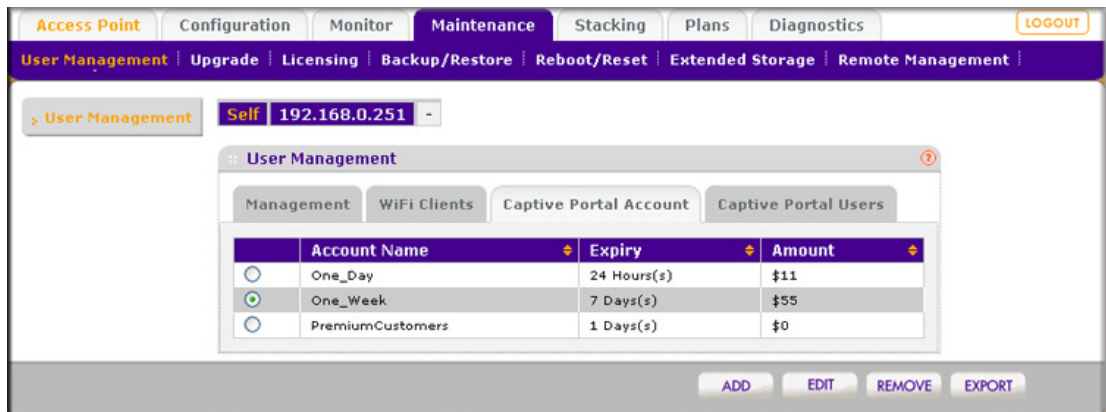


Figure 62.

- **Captive Portal Users.** The Captive Portal Users screen displays:

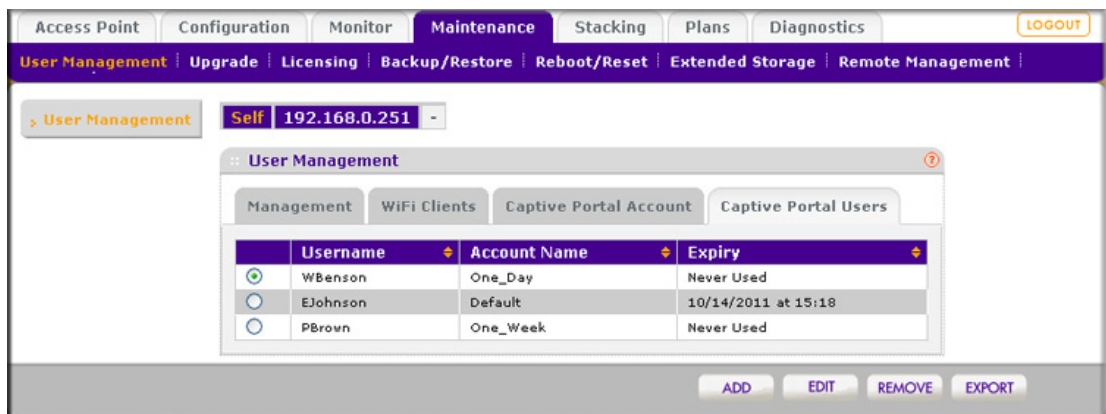
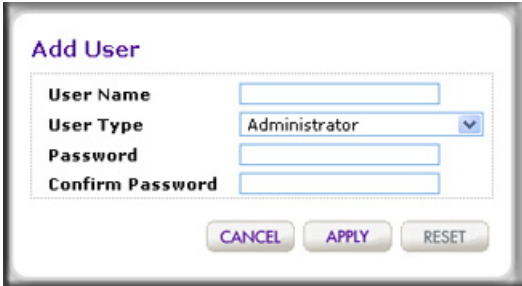


Figure 63.

3. Click **Add** to add a new user or account. A pop-up window displays. The pop-up windows are shown in the following table.
4. Configure the users or account settings as described in the following table.

**Table 30. User and account settings**

| Setting    | Description  |  |
|------------|--|--|
| Management |  |  |
|            | User Name  | Enter a unique user name. Only alphanumeric characters and underscore characters (_) are supported.  |
|            | User Type  | From the drop-down list, select the type of user, which determines their access to the wireless controller's web management interface. <ul style="list-style-type: none"> <li>• <b>Administrator.</b> Full access with read and write capabilities.</li> <li>• <b>Read Only.</b> Read-only access that is restricted to the Monitor and Help main navigation tabs.</li> <li>• <b>Guest Provisioning.</b> Access that is restricted to the User Management configuration menu tab under the Maintenance main navigation tab.</li> <li>• <b>License Management Only.</b> Access that is restricted to the License configuration menu tab under the Maintenance main navigation tab.</li> </ul> |
|            | Password   | Enter a password in the Password field, and confirm the password in the Confirm Password field.  |

**Table 30. User and account settings (continued)**

| Setting   | Description   |              |   |          |   |                     |  |        |  |               |  |
|---|---|--------------|---|----------|---|---------------------|--|--------|--|---------------|--|
| WiFi Clients  | <div data-bbox="527 344 1045 642" style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">User Name</td> <td style="padding: 5px;">Enter a unique user name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported.</td> </tr> <tr> <td style="padding: 5px;">Password</td> <td style="padding: 5px;">Enter a password in the Password field, and confirm the password in the Confirm Password field.</td> </tr> <tr> <td style="padding: 5px;">Authentication Type</td> <td style="padding: 5px;">From the drop-down list, select one of the following protocols:                             <ul style="list-style-type: none"> <li>• <b>EAP</b>. Extensible Authentication Protocol.</li> <li>• <b>PEAP</b>. Protected EAP.</li> </ul> </td> </tr> </table>   | User Name    | Enter a unique user name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported.    | Password | Enter a password in the Password field, and confirm the password in the Confirm Password field. | Authentication Type | From the drop-down list, select one of the following protocols: <ul style="list-style-type: none"> <li>• <b>EAP</b>. Extensible Authentication Protocol.</li> <li>• <b>PEAP</b>. Protected EAP.</li> </ul> |        |  |               |  |
| User Name   | Enter a unique user name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported.  |              |   |          |   |                     |  |        |  |               |  |
| Password  | Enter a password in the Password field, and confirm the password in the Confirm Password field.   |              |   |          |   |                     |  |        |  |               |  |
| Authentication Type   | From the drop-down list, select one of the following protocols: <ul style="list-style-type: none"> <li>• <b>EAP</b>. Extensible Authentication Protocol.</li> <li>• <b>PEAP</b>. Protected EAP.</li> </ul>  |              |   |          |   |                     |  |        |  |               |  |
| Captive Portal Accounts<br><br><b>Note:</b> This selection is disabled if the portal setting is a guest portal instead of a captive portal. | <div data-bbox="527 959 1045 1341" style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Account Name</td> <td style="padding: 5px;">Enter a unique account name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported.</td> </tr> <tr> <td style="padding: 5px;">Amount</td> <td style="padding: 5px;">Enter the total amount that is charged for the period during which access is available.</td> </tr> <tr> <td style="padding: 5px;">Currency Sign</td> <td style="padding: 5px;">Enter the currency that is associated with the amount.</td> </tr> <tr> <td style="padding: 5px;">Expiry</td> <td style="padding: 5px;">From the drop-down list, select one of the following periods, and then enter a valid number in the field to the left of the drop-down list:                             <ul style="list-style-type: none"> <li>• <b>Hour(s)</b>. The expiration period is measured in one or more hours.</li> <li>• <b>Day(s)</b>. The expiration period is measured in one or more days.</li> <li>• <b>Week(s)</b>. The expiration period is measured in one or more weeks.</li> <li>• <b>Month(s)</b>. The expiration period is measured in one or more months.</li> </ul> </td> </tr> <tr> <td style="padding: 5px;">Print Message</td> <td style="padding: 5px;">As an option, enter a message for the captive portal user.</td> </tr> </table> | Account Name | Enter a unique account name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported. | Amount   | Enter the total amount that is charged for the period during which access is available.         | Currency Sign       | Enter the currency that is associated with the amount.   | Expiry | From the drop-down list, select one of the following periods, and then enter a valid number in the field to the left of the drop-down list: <ul style="list-style-type: none"> <li>• <b>Hour(s)</b>. The expiration period is measured in one or more hours.</li> <li>• <b>Day(s)</b>. The expiration period is measured in one or more days.</li> <li>• <b>Week(s)</b>. The expiration period is measured in one or more weeks.</li> <li>• <b>Month(s)</b>. The expiration period is measured in one or more months.</li> </ul> | Print Message | As an option, enter a message for the captive portal user. |
| Account Name  | Enter a unique account name. Only alphanumerical characters and underscore characters ( <code>_</code> ) are supported.   |              |   |          |   |                     |  |        |  |               |  |
| Amount  | Enter the total amount that is charged for the period during which access is available.   |              |   |          |   |                     |  |        |  |               |  |
| Currency Sign   | Enter the currency that is associated with the amount.  |              |   |          |   |                     |  |        |  |               |  |
| Expiry  | From the drop-down list, select one of the following periods, and then enter a valid number in the field to the left of the drop-down list: <ul style="list-style-type: none"> <li>• <b>Hour(s)</b>. The expiration period is measured in one or more hours.</li> <li>• <b>Day(s)</b>. The expiration period is measured in one or more days.</li> <li>• <b>Week(s)</b>. The expiration period is measured in one or more weeks.</li> <li>• <b>Month(s)</b>. The expiration period is measured in one or more months.</li> </ul>  |              |   |          |   |                     |  |        |  |               |  |
| Print Message   | As an option, enter a message for the captive portal user.  |              |   |          |   |                     |  |        |  |               |  |

**Table 30. User and account settings (continued)**

| Setting   | Description  |           |   |          |  |        |  |
|---|--|-----------|---|----------|--|--------|--|
| <p>Captive Portal Users</p> <p><b>Note:</b> This selection is disabled if the portal setting is a guest portal instead of a captive portal.</p> | <div data-bbox="529 331 1166 848" style="border: 1px solid gray; padding: 10px; margin-bottom: 10px;"> <p><b>Add User</b></p> <p>User Name <input type="text"/></p> <p>Password <input type="password"/></p> <p style="text-align: center;"><input type="button" value="GENERATE"/></p> <p>Confirm Password <input type="password"/></p> <p><b>Expiry</b></p> <p><input type="radio"/> Account <input type="text" value="One_Day"/></p> <p><input type="radio"/> No Expiry</p> <p><input type="radio"/> Expires in <input type="text" value="1"/> mins</p> <p><input checked="" type="radio"/> Expires at hr: <input type="text" value="19"/> mins: <input type="text" value="5"/></p> <p>Month: <input type="text" value="10"/> Date: <input type="text" value="26"/> Year: <input type="text" value="2011"/></p> <p style="text-align: center;"> <input type="button" value="CANCEL"/> <input type="button" value="APPLY"/> <input type="button" value="PRINT"/> <input type="button" value="RESET"/> </p> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">User Name</td> <td style="padding: 5px;">Enter a unique user name. Only alphanumeric characters and underscore characters (_) are supported.</td> </tr> <tr> <td style="padding: 5px;">Password</td> <td style="padding: 5px;">Enter a password in the Password field, and confirm the password in the Confirm Password field.<br/>As an alternate method to entering a password in both the Password and Confirm Password fields, click <b>Generate</b>.</td> </tr> <tr> <td style="padding: 5px;">Expiry</td> <td style="padding: 5px;">                     Select one of the following radio buttons to specify the expiration of the wireless access:                     <ul style="list-style-type: none"> <li>• <b>Account.</b> Select an account from the drop-down list. Wireless access expires according to the expiration item that is specified in the selected account.</li> <li>• <b>No Expiry.</b> Wireless access does not expire.</li> <li>• <b>Expires in.</b> Wireless access expires within 1 hour. From the mins drop-down list, select in how many minutes access expires.</li> <li>• <b>Expires at.</b> Wireless access expires at a date and time that you specify by making selections from the following drop-down lists: hr, mins, Month, Date, and Year.</li> </ul> </td> </tr> </table> | User Name | Enter a unique user name. Only alphanumeric characters and underscore characters (_) are supported. | Password | Enter a password in the Password field, and confirm the password in the Confirm Password field.<br>As an alternate method to entering a password in both the Password and Confirm Password fields, click <b>Generate</b> . | Expiry | Select one of the following radio buttons to specify the expiration of the wireless access: <ul style="list-style-type: none"> <li>• <b>Account.</b> Select an account from the drop-down list. Wireless access expires according to the expiration item that is specified in the selected account.</li> <li>• <b>No Expiry.</b> Wireless access does not expire.</li> <li>• <b>Expires in.</b> Wireless access expires within 1 hour. From the mins drop-down list, select in how many minutes access expires.</li> <li>• <b>Expires at.</b> Wireless access expires at a date and time that you specify by making selections from the following drop-down lists: hr, mins, Month, Date, and Year.</li> </ul> |
| User Name   | Enter a unique user name. Only alphanumeric characters and underscore characters (_) are supported.  |           |   |          |  |        |  |
| Password  | Enter a password in the Password field, and confirm the password in the Confirm Password field.<br>As an alternate method to entering a password in both the Password and Confirm Password fields, click <b>Generate</b> .   |           |   |          |  |        |  |
| Expiry  | Select one of the following radio buttons to specify the expiration of the wireless access: <ul style="list-style-type: none"> <li>• <b>Account.</b> Select an account from the drop-down list. Wireless access expires according to the expiration item that is specified in the selected account.</li> <li>• <b>No Expiry.</b> Wireless access does not expire.</li> <li>• <b>Expires in.</b> Wireless access expires within 1 hour. From the mins drop-down list, select in how many minutes access expires.</li> <li>• <b>Expires at.</b> Wireless access expires at a date and time that you specify by making selections from the following drop-down lists: hr, mins, Month, Date, and Year.</li> </ul>   |           |   |          |  |        |  |

5. Click **Apply** to save your changes.
6. Click **Close** to close the pop-up window.

---

**Note:** For information about password requirements, see [Table 54](#) on page 203.

---

➤ **To edit or remove a user or an account:**

1. Click a tab (**Management**, **WiFi Clients**, **Captive Portal Account**, or **Captive Portal Users**).
2. Select a radio button that corresponds to a user or an account.
3. Click one of the following buttons:
  - **Edit**. Opens a pop-up window that lets you change the user settings as described in the previous table. You cannot change the user name and user type or the account name.
  - **Remove**. Removes the user from the user table.

➤ **To export a list of users or accounts:**

1. Click a tab (**Management**, **WiFi Clients**, **Captive Portal Account**, or **Captive Portal Users**).
2. Click **Export**. The selected list is saved or opened as a zipped comma-separated values (CSV) file to a location that you specify.
3. Follow the directions of your browser to complete the procedure.

# Maintaining the Controller

---

# 9

This chapter includes the following sections:

- *Manage the Configuration File*
- *Reboot or Reset the Wireless Controller*
- *Reboot Access Points*
- *Manage External Storage*
- *Manage Remote Access*
- *View Alerts and Events and Save the Logs*
- *Manage Licenses*

## Manage the Configuration File

This section includes the following subsections:

- *Back Up and Restore the Configuration File*
- *Upgrade the Configuration File*

The configuration settings of the wireless controller are stored in a configuration file on the wireless controller. This file can be saved (backed up) to a computer, retrieved (restored) from the computer, or cleared to factory default settings.

Once the wireless controller is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the wireless controller settings from this file.

### Back Up and Restore the Configuration File

To display the Backup/Restore screen, select **Maintenance > Backup/Restore**:

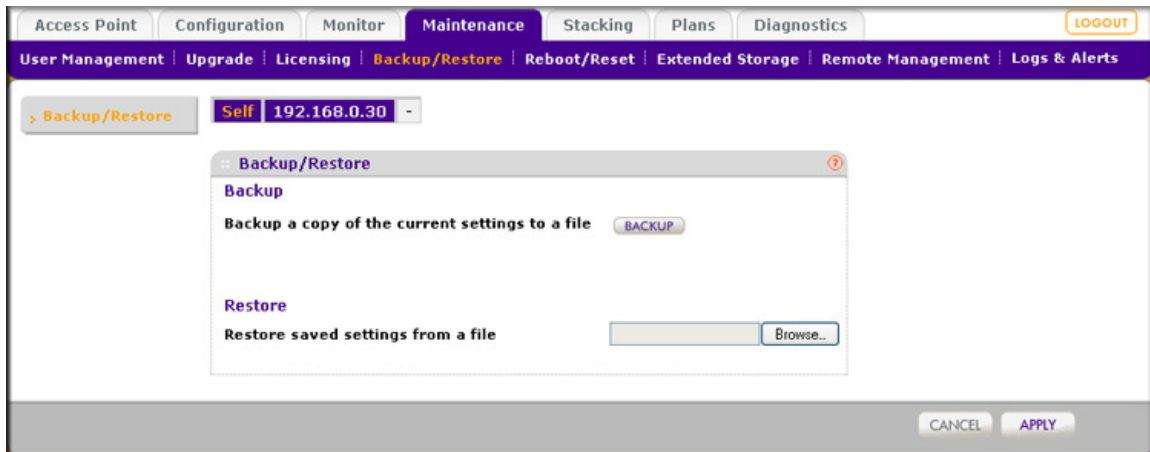


Figure 64.

The Backup/Restore screen lets you:

- Back up and save a copy of the current settings
- Restore saved settings from the backed-up file

➤ **To back up the configuration file:**

1. On the Backup/Restore Settings screen (see the previous figure), click the **Backup** button to save a copy of your current settings. A dialog box displays, showing the file name of the backup file. The backup file has the following format: backup.tar.gz.
2. Follow the instructions of your browser to save the configuration file.

➤ **To restore the configuration file:**

1. On the Backup/Restore Settings screen (see the previous figure), click the **Browse** button.
2. Navigate to the saved configuration file.
3. Click **Apply** to load the configuration file. The wireless controller reboots.



**WARNING!**

**When you restore the configuration file, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting! When the LED light turns off, wait a few more seconds before you do anything.**

---

**Note:** Restore only settings that were backed up from the same software version.

---



## Upgrade the Configuration File

The wireless controller provides two methods for upgrading its firmware:

- Scheduled, automatic update
- Manual update

There are two boot partitions to allow you to switch the wireless controller from one firmware version to another.

### ➤ To upgrade the firmware:

1. Go to the NETGEAR support page for the WC7520 wireless controller at [http://kb.netgear.com/app/products/model/a\\_id/13060](http://kb.netgear.com/app/products/model/a_id/13060) or to a TFTP or FTP server.
2. If you intend use a local file for the upgrade, download the firmware from the NETGEAR support page for the WC7520 wireless controller and save it to your computer.
3. Select **Maintenance > Upgrade**. The Firmware Upgrade screen displays:

The screenshot shows the 'Firmware Upgrade' configuration page. At the top, there are navigation tabs: Access Point, Configuration, Monitor, Maintenance (selected), Stacking, Plans, and Diagnostics. Below these are sub-tabs: User Management, Upgrade (selected), Licensing, Backup/Restore, Reboot/Reset, Extended Storage, Remote Management, and Logs & Alerts. The main content area is titled 'Firmware Upgrade' and includes a 'Self' dropdown menu showing '192.168.0.30'. The upgrade method is set to 'FTP'. The 'Server Parameters' section has input fields for 'Server IP', 'File Name', 'User Name', and 'Password'. The 'Boot Information' section shows 'Active Partition' as 'Partition 1 (Firmware version: 2.1.0\_1747)', with 'Boot Partition to Upgrade' and 'After upgrade boot from' both set to 'Partition 1'. The 'Schedule' section has 'Scheduled Upgrade Status' set to 'None' and 'When to Upgrade?' set to 'Now'. At the bottom right, there are 'CANCEL' and 'APPLY' buttons.

Figure 65.

4. Configure the settings as explained in the following table:

**Table 31. Firmware upgrade settings**

| Setting  | Description   |
|--|---|
| TFTP, FTP, or Local File                             | Select one of the following radio buttons to specify from which location the upgrade should occur. The screen adjusts to display the fields that are required for each upgrade location. <ul style="list-style-type: none"> <li>• <b>TFTP.</b> Upgrade from a TFTP server. The Server IP and File Name server parameters fields display.</li> <li>• <b>FTP.</b> Upgrade from an FTP server. All of the server parameters fields display.</li> <li>• <b>Local File.</b> Upgrade from a local file that you have downloaded. The server parameter fields do not display, but the Browse field becomes available. Follow the directions of your browser to select the firmware upgrade file from your computer.</li> </ul> |
| <b>Server Parameters section (TFTP and FTP only)</b> |   |
| Server IP  | Enter the IP address of the TFTP or FTP server.   |
| File Name  | Enter the file name of the firmware.  |
| User Name (FTP only)                                 | Enter the user name to access the FTP server.   |
| Password (FTP only)                                  | Enter the password to access the FTP server.  |
| <b>Boot Information section</b>                      |   |
| Active Partition                                     | This is an informational field that displays the active partition and the current firmware version.   |
| Boot Partition to Upgrade                            | Select the radio button for the partition to which the new firmware should be saved.  |
| After upgrade boot from                              | Select the radio button for the partition from which the wireless controller should reboot after the firmware has been upgraded.  |
| <b>Schedule section</b>                              |   |
| Schedule Update Status                               | This is an informational field that displays when the firmware upgrade will occur. If no update is scheduled, the field displays None.  |
| When to Upgrade?                                     | Select when the firmware upgrade should occur: <ul style="list-style-type: none"> <li>• <b>Later.</b> Make selections from the drop-down lists to specify the date and time when the upgrade should occur.</li> <li>• <b>Now.</b> The upgrade occurs immediately after you click Apply.</li> </ul>  |

5. Click **Apply** to save your settings. If you selected the Now radio button to upgrade the firmware immediately, the wireless controller reboots.

**WARNING!**

During a firmware upgrade, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting! When the LED light turns off, wait a few more seconds before you do anything.

6. To verify that the wireless controller is running the latest firmware, select **Monitor > Network > Controller** to display the Controllers screen, and look at the firmware version in the Version column.

---

**Note:** After you have upgraded the firmware, if the browser does not display the latest features of the web management interface, clear the browser's cache, and refresh the screen.

---

---

**Note:** In some cases, such as a major firmware upgrade, you might need to erase the configuration and manually reconfigure the wireless controller after the firmware upgrade. Refer to the Release Notes for the firmware version to find out if you need to reconfigure the wireless controller.

---

## Reboot or Reset the Wireless Controller

The Reboot/Reset Controllers screen lets you reboot or reset the wireless controller. There are two types of reset:

- **Hard reset.** The settings of the wireless controller are restored to factory default settings. This reset has the same function as the Factory Defaults button on the rear panel.
- **Soft reset.** Saves the IP addresses, floor plans, and managed access point list but clears all other settings such as profiles, profile groups, authentication servers, and so on.

To display the Reboot/Reset Controllers screen, select **Maintenance > Reboot/Reset > Controllers**:

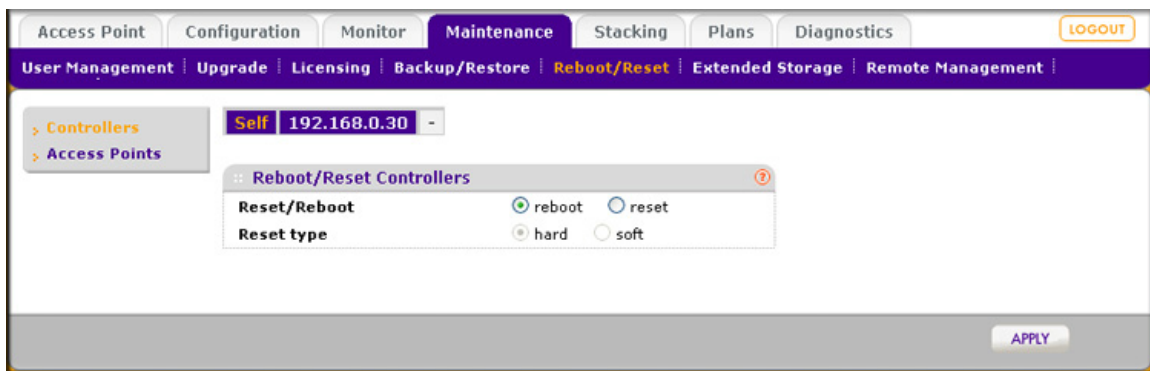


Figure 66.

➤ **To reboot the wireless controller:**

1. Select the **Reboot** radio button.
2. Click **Apply** to save your settings. The wireless controller reboots. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

➤ **To reset the wireless controller:**

1. Select the **Reset** radio button.
2. Select one of the following radio buttons to specify a hard reset or soft reset:
  - **Hard.** Restore the factory default settings (which are listed in [Appendix A, Factory Default Settings and Technical Specifications](#)) to the wireless controller.
  - **Soft.** Clear all settings except for the IP addresses, floor plans, and managed access point list.
3. Click **Apply** to save your settings. If you selected a hard reset, the wireless controller reboots.

---

**Note:** Restoring the factory default settings of the wireless controller does *not* restore the settings of the access points that are managed by the wireless controller.

---



**WARNING!**

If you perform a hard reset, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting! When the LED light turns off, wait a few more seconds before you do anything.

## Reboot Access Points

Under normal circumstances, there is no reason to reboot an access point. If there is a problem with an access point, you can reboot it to see if this resolves the problem.

### ➤ To reboot an access point:

1. Select **Maintenance > Reboot/Reset > Access Points**. The Reboot Access Points screen displays:

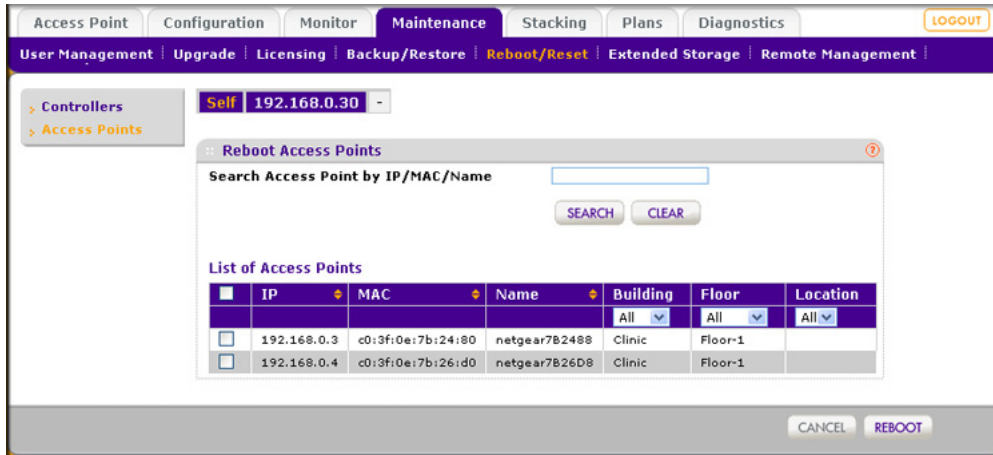


Figure 67.

2. As an optional step, enter the IP address, MAC address, or name of an access point in the Search Access Point by IP/MAC/Name field, and click **Search**.
3. From the List of Access Points, which you can sort by building, floor, or location, specify the access points that you want to reboot by selecting the check boxes corresponding to the access points, or specify that you want to reboot all access points by selecting the check box in the heading of the list.
4. Click **Reboot**.

## Manage External Storage

The Extended Storage screen displays information about an optionally attached external storage device such as a USB memory stick or external hard drive, and lets you mount and dismount the storage device. You can use an external storage device to store more floor heat maps and extended statistics history.

### ➤ To mount an external storage device and view information about the device:

1. Select **Maintenance > Extended Storage**. The Extended Storage screen displays. As an example, the screen shows information about an attached USB memory stick.

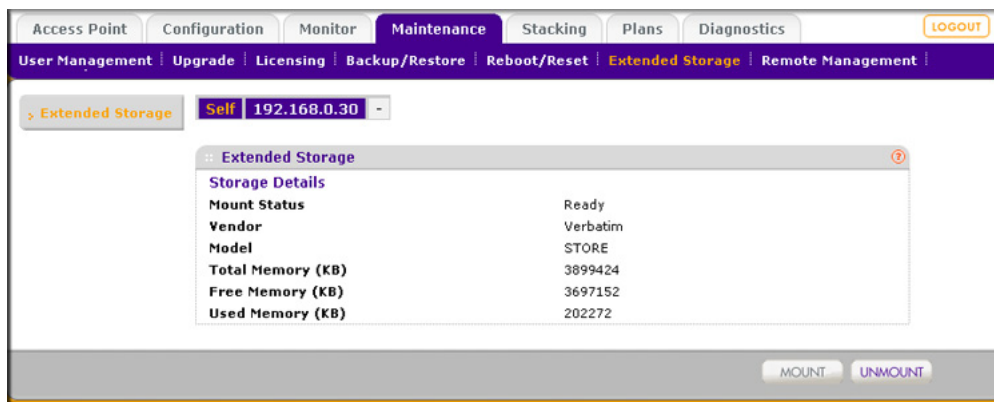


Figure 68.

2. Attach the external storage device to the USB port on the front panel of the wireless controller.
3. Click **Mount**. The storage details become visible on the Extended Storage screen. Before you remove the external storage device from the USB port, click **Unmount**.

## Manage Remote Access

Enable SNMP to allow SNMP network management software, such as HP OpenView, to monitor the wireless controller by using SNMPv1 or SNMPv2c protocol.

With the exception of the following features, you can configure the wireless controller through SNMP:

- Heat maps
- Guest access management
- RF management
- Stacking management

### ➤ To enable and configure SNMP:

1. Select **Maintenance > Remote Management > SNMP**. The SNMP screen displays:

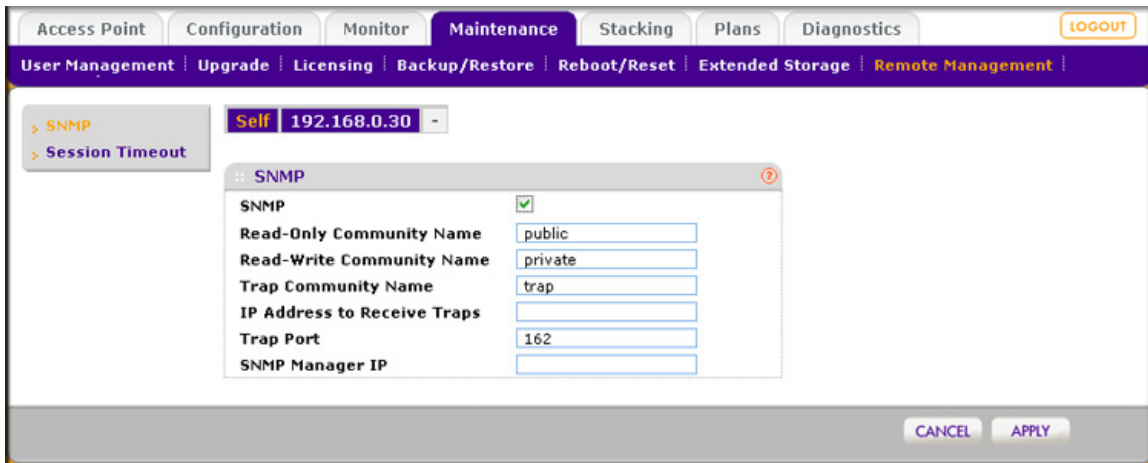


Figure 69.

2. Enable SNMP and configure the settings as explained in the following table:

Table 32. SNMP settings

| Setting                     | Description   |
|-----------------------------|---|
| SNMP                        | Select this check box to enable SNMP for the wireless controller.   |
| Read-Only Community Name    | Enter the community string that allows the SNMP manager to read the wireless controller’s MIB objects. The default setting is public.             |
| Read-Write Community Name   | Enter the community string that allows the SNMP manager to read and write the wireless controller’s MIB objects. The default setting is private.  |
| Trap Community Name         | Enter the community name that is associated with the IP address to receive traps. The default setting is trap.                                    |
| IP Address to Receive Traps | Enter the IP address at which the SNMP manager receives traps sent from the wireless controller.  |
| Trap Port                   | Enter the port on which the SNMP manager receives traps sent from the wireless controller. The default setting is port 162.                       |
| SNMP Manager IP             | Enter the IP address of the SNMP manager.<br><br><b>Note:</b> To allow any SNMP manager to access the wireless controller, keep this field blank. |

3. Click **Apply** to save your settings.

---

**Note:** The wireless controller supports Telnet and SSH through the console port. However, the console port is for debugging under guidance of NETGEAR technical support only.

---

## Specify Session Time-Outs

If an HTTP session times out, the user is redirected to the login window for password verification.

- **To specify the length of the HTTP session time-out for the wireless controller:**
  1. Select **Maintenance > Remote Management > Session Timeout**. The Session Timeout screen displays:

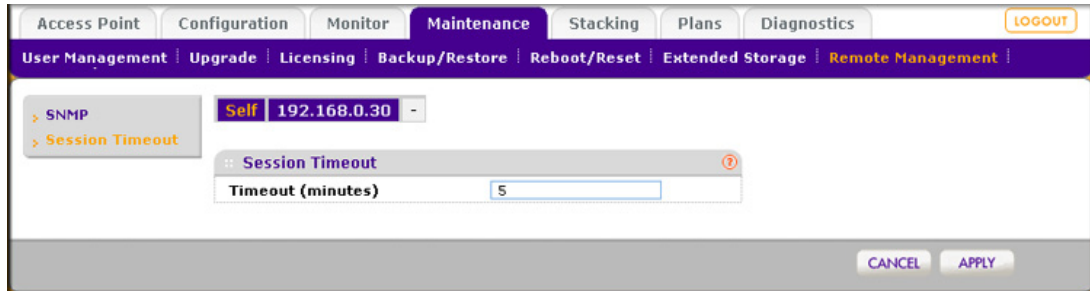


Figure 70.

2. In the Timeout (minutes) field, specify number of minutes before an active HTTP login session expires.
3. Click **Apply** to save your settings.

## View Alerts and Events and Save the Logs

You can view system alerts and save system logs that are collected on the wireless controller. You can also save logs of individual access points. In the event of a problem or failure, these logs along with backed-up configuration settings could help determine the cause.

### Save the Logs

- **To save access point logs:**
  1. Select **Maintenance > Logs & Alerts > Save Logs > AP Logs**. The Access Points screen displays:



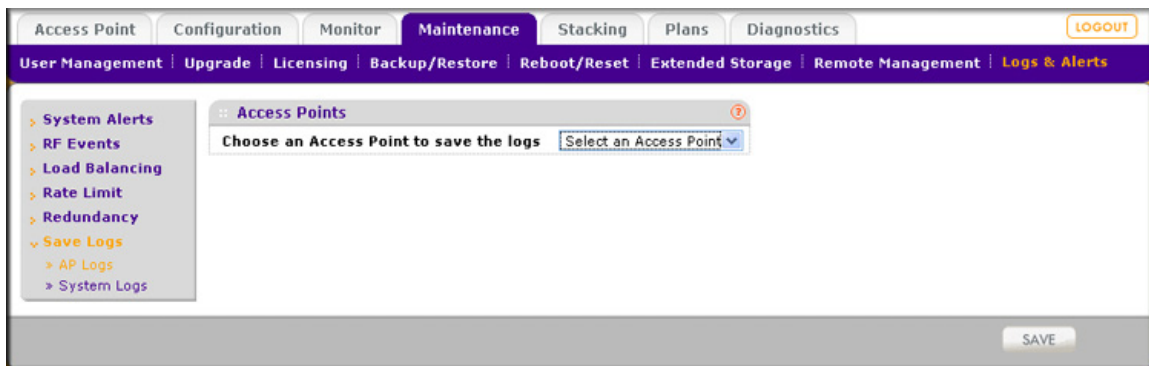


Figure 71.

2. Select an access point from the drop-down list.
3. Click **Save**, and follow the directions of your browser to save the logs to the selected access point. The name of the zipped log file is ap\_logs.tgz.

➤ **To save system logs:**

1. Select **Maintenance > Logs & Alerts > Save Logs > System Logs**. The System Logs screen displays:

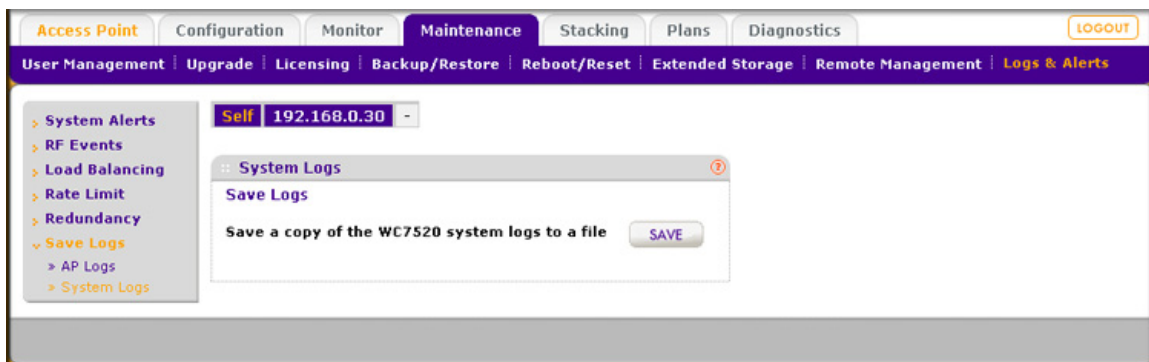


Figure 72.

2. Click **Save**, and follow the directions of your browser to save the logs to your computer. The name of the zipped log file is wnc\_logs.tgz.

## View Alerts and Events

The wireless controller lets you view the following alerts and events:

- **System Alerts.** System alerts such as an access point coming up or being shut down, the wireless controller coming up or being shut down, a firmware upgrade, and so on.
- **RF Events.** Radio frequency events such as the detection of a coverage hole, a change of channel, or a managed access point going down.
- **Load Balancing.** Load-balancing events such as a bad RSSI for a client, or the violation of a load-balancing threshold.

- **Rate Limit.** Rate-limit events such as the violation of a rate-limit threshold.
- **Redundancy.** Redundancy events such as the redundant wireless controller coming up or going down, or a failover to another wireless controller.
- **Stacking.** Stacking events such as a secondary wireless controller (slave) coming up or going down, or the synchronization between two wireless controllers.

Each screen that displays alerts or events contains a table with three columns:

- **Severity.** The alarm severity level: All, Minor, Normal, Major, or Critical. You can sort each table on severity level by using the Severity drop-down list.
- **Description.** The description of the alert or event, which is self-explanatory.
- **Raised Time.** The date and time that the alert or event was raised. You can sort each table on the time that the alert or event was raised by using the Raised Time drop-down list.

To view additional alerts or events, click **Next**; to return to the previous alerts or events, click **Previous**.

To display the latest information onscreen, click the **Refresh** button. To clear all information from the screen and from memory, click the **Clear All** button.

➤ **To view system alerts:**

Select **Maintenance > Logs & Alerts > System Alerts**. The System Alerts screen displays:

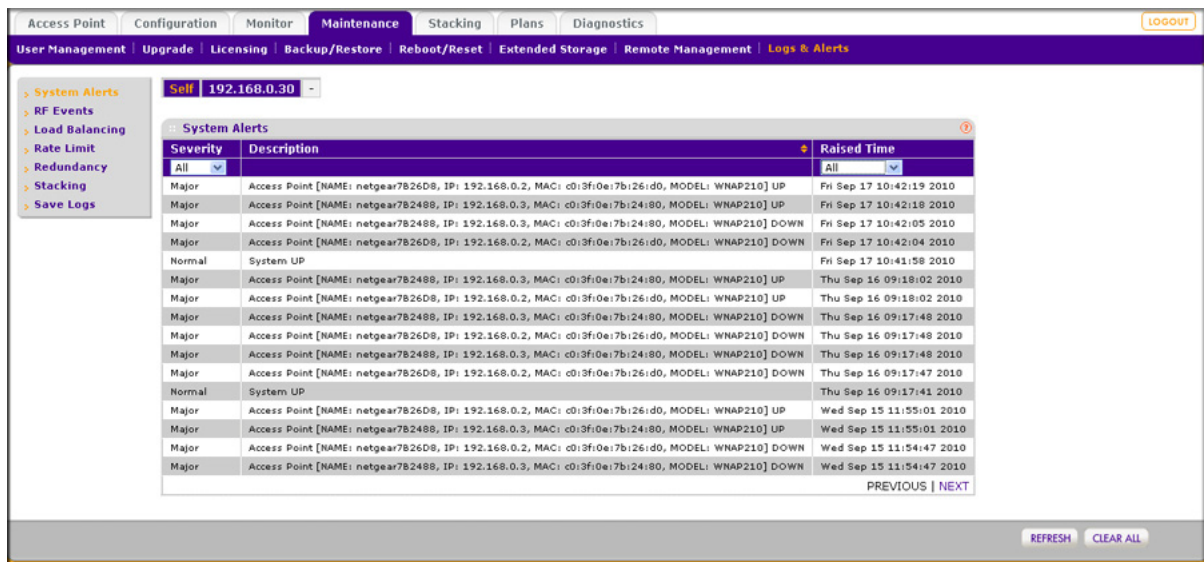


Figure 73.

To clear the existing Alerts log, click **Clear All**. Consider saving the contents before you clear the system alerts (see [Save the Logs](#) on page 144).

➤ **To view RF events:**

Select **Maintenance > Logs & Alerts > RF Events**. The RF Events screen displays:

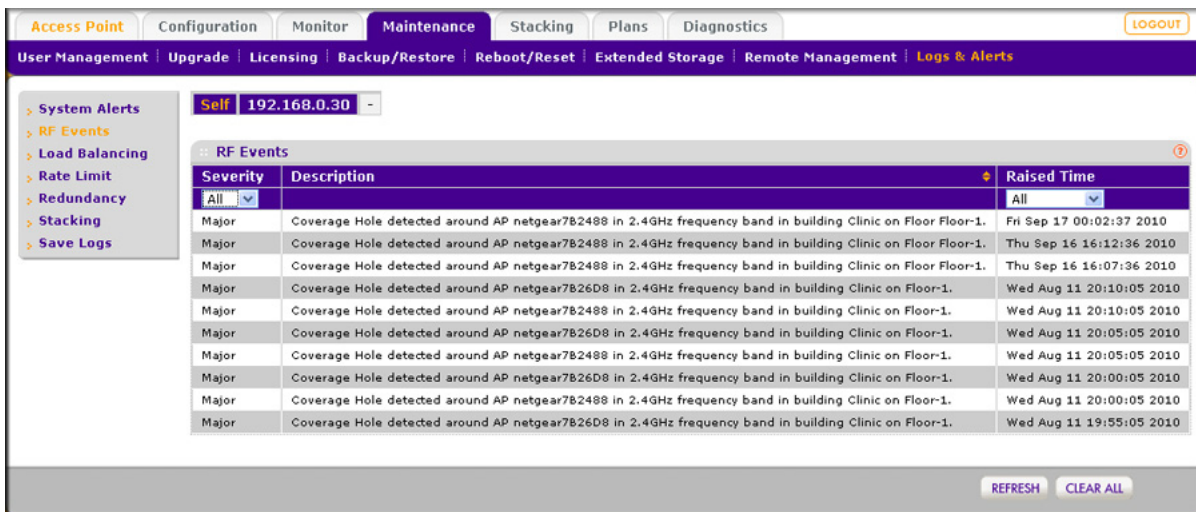


Figure 74.

➤ To view load-balancing events:

Select **Maintenance > Logs & Alerts > Load Balancing**. The Load Balancing screen displays:

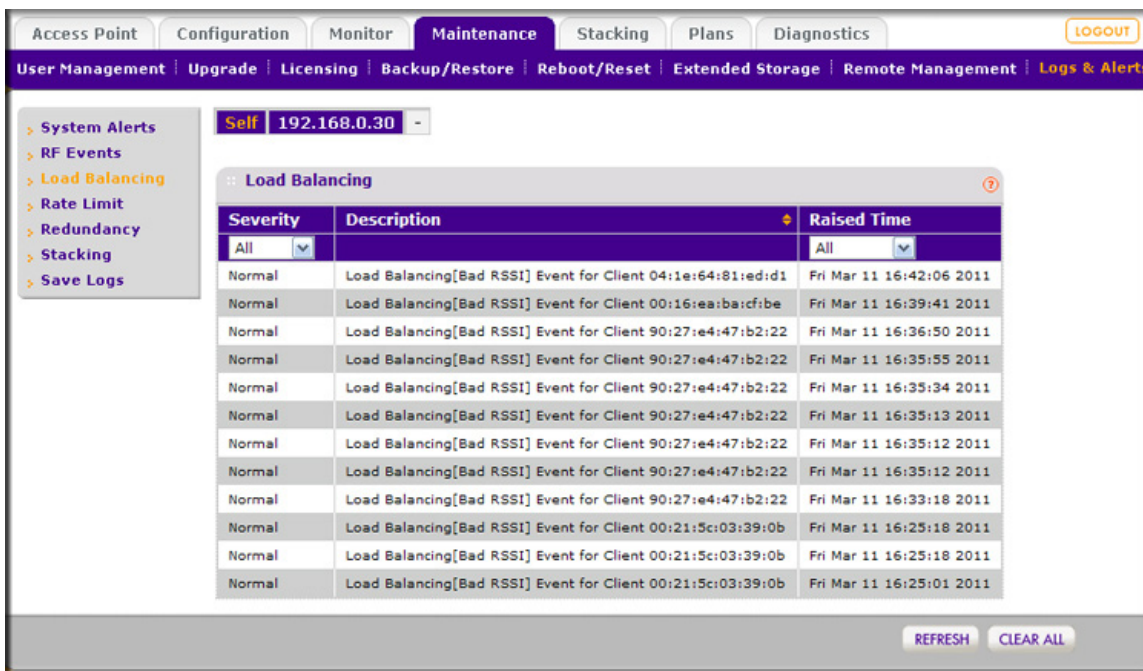


Figure 75.

➤ To view rate-limit events:

Select **Maintenance > Logs & Alerts > Rate Limit**. The Rate Limit screen displays:

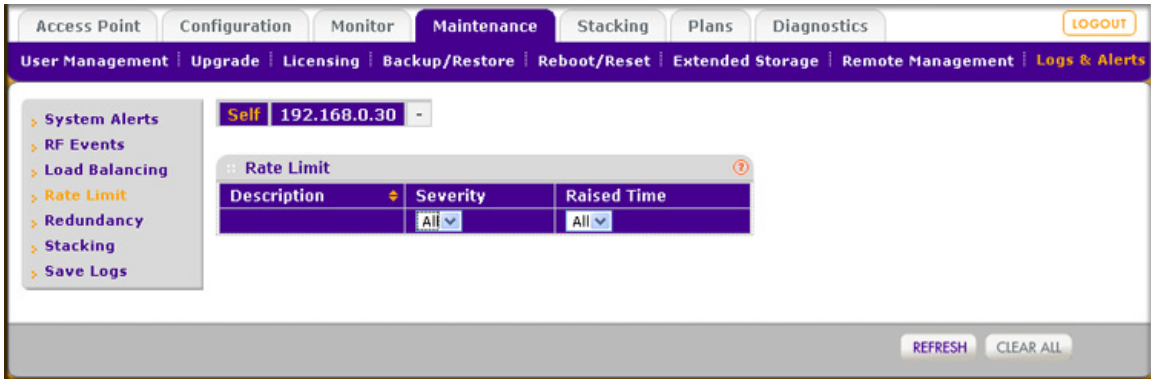


Figure 76.

➤ To view redundancy events:

Select **Maintenance > Logs & Alerts > Redundancy**. The Redundancy screen displays:

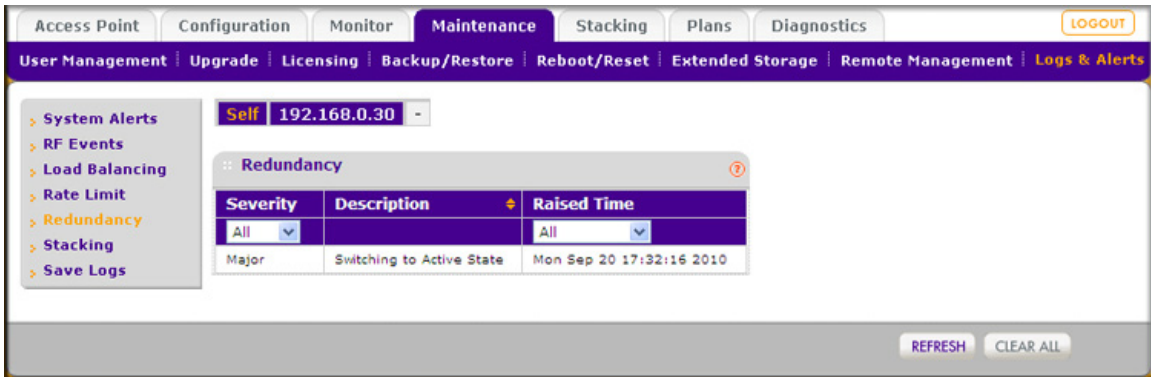


Figure 77.

➤ To view stacking events:

Select **Maintenance > Logs & Alerts > Stacking**. The Stacking screen displays:

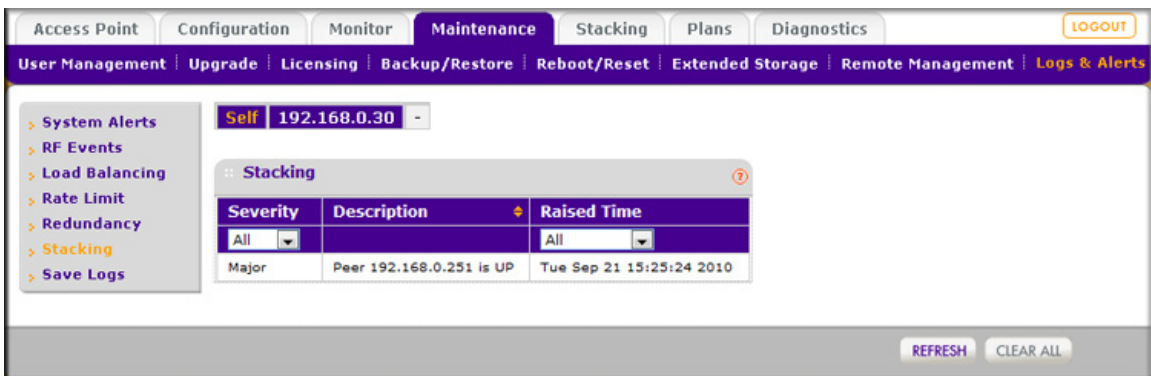


Figure 78.

## Manage Licenses

The License screen allows you to import, register, and view the licenses that you require for your network. For more information about licenses, see [Licenses](#) on page 18.

The License screen consists of four separate screens:

- **Inventory screen.** Provides an overview of your licenses.
- **Server Settings screen.** Allows you to configure the server settings to import your licenses.
- **Registration screen.** Allows to register your licenses.
- **Advanced screen.** Lets you retrieve your licenses. This screen displays relevant information only if you have received a replacement unit from NETGEAR.

## View Your Licenses

### ➤ To view your licenses:

Select **Maintenance > License**, and then click the **Inventory** tab. The Inventory screen displays:

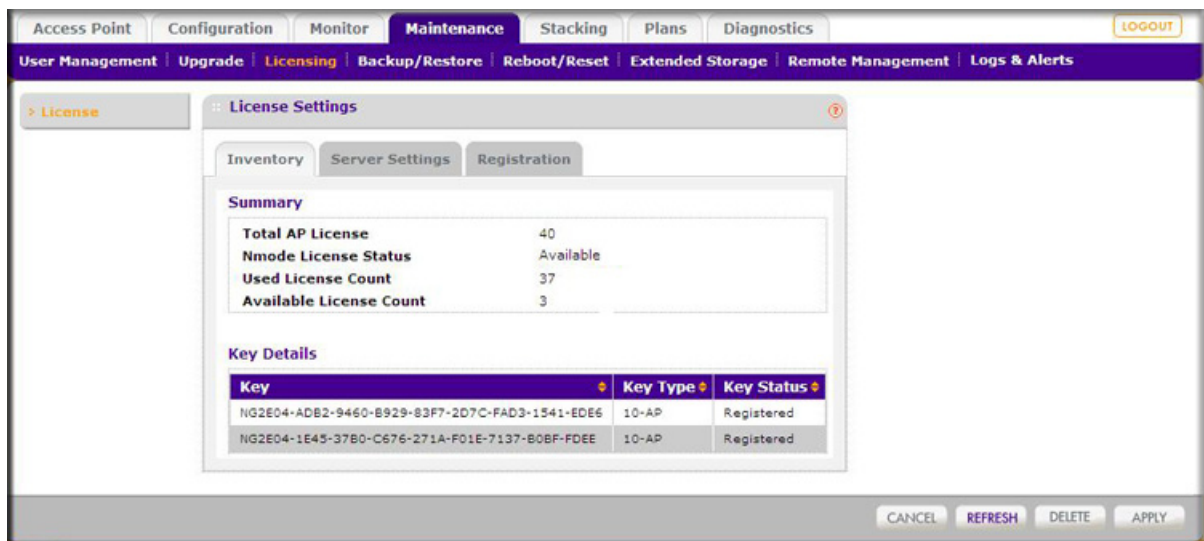


Figure 79.

The following table explains the fields of the screen:

Table 33. License inventory settings

| Setting                | Description   |
|------------------------|---|
| <b>Summary section</b> |   |
| Total AP License       | The number of access points that your licenses support. |

Table 33. License inventory settings (continued)

| Setting                    | Description   |
|----------------------------|---|
| Nmode License Status       | Availability of the 802.11n mode license. (This license is available by default, indicated by either Pre-installed or Available.) |
| Used License Count         | Number of access points used from the total number that is supported by your licenses.  |
| Available License Count    | Number of access points still available from the total number that is supported by your licenses.                                 |
| <b>Key Details section</b> |   |
| Key                        | The value of the key that unlocks the license.  |
| Key Type                   | The type of the key that determines the number of access points that are supported and the mode that is supported.                |
| Key Status                 | The status of the key (Registering key with server or Registered).  |

To refresh your license information, click **Refresh**.

## Configure the License Server Settings

### ➤ To configure the license server settings:

1. Select **Maintenance > License**, and then click the **Server Settings** tab. The Server Settings screen displays:

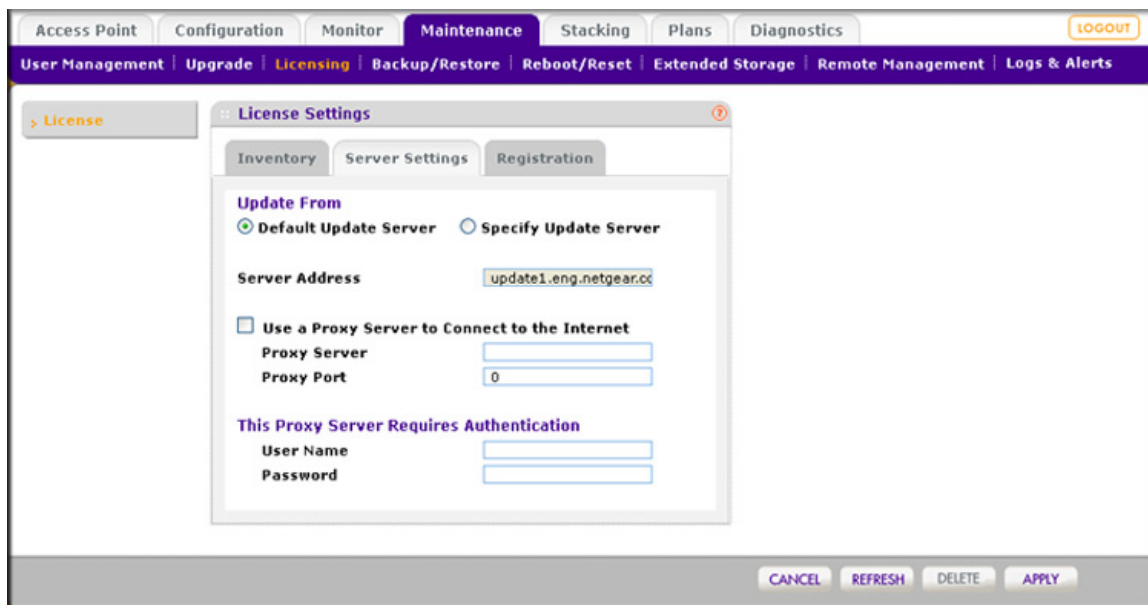


Figure 80.

- Configure the settings as explained in the following table:

**Table 34. License server settings**

| Setting                                       | Description  |   |
|---|--|---|
| Update From                                   | Select one of the following radio buttons to specify the license update server:  |   |
|   | <ul style="list-style-type: none"> <li>• <b>Default Update Server.</b> The default license update server is used.</li> <li>• <b>Specify Update Server.</b> You need to specify the license update server. Fill in the Server Address field.</li> </ul> |   |
| Use a Proxy Server to Connect to the Internet | Server Address   | Enter the IP address or FQDN of the server from which you import your licenses. |
|   | Select this check box if you use a proxy server to connect to the Internet.  |   |
|   | Proxy Server   | Enter the IP address or FQDN of the proxy server.                               |
| This Proxy Server Requires Authentication     | Proxy Port   | Enter the port that the proxy server uses.                                      |
|   | Select this check box if the proxy server requires authentication.   |   |
|   | User Name  | Enter the user name to access the proxy server.                                 |
|   | Password   | Enter the password to access the proxy server.                                  |

- Click **Apply** to save your settings.

## Register Your Licenses

### ➤ To register your licenses:

- Make sure that the wireless controller is connected to the Internet.
- Select **Maintenance > License**, and then click the **Registration** tab. The Registration screen displays:

Access Point Configuration Monitor Maintenance Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management Logs & Alerts

> License

License Settings

Inventory Server Settings Registration

Registration Key

ADD

| Key  | Key Type | Key Status |
|--|----------|------------|
| <input type="radio"/> NG2E04-ADB2-9460-B929-B3F7-2D7C-FAD3-1541-EDE6 | 10-AP    | Registered |
| <input type="radio"/> NG2E04-1E45-37B0-C676-271A-F01E-7137-B0BF-FDEE | 10-AP    | Registered |

Customer Information

Company Name

First Name

Last name

Email Address

Fax Number

Phone Number

Address

Zip

City

State

Country

VAR Information

Company Name

First Name

Last name

Email Address

Fax Number

Phone Number

Address

Zip

City

State

Country

CANCEL REFRESH DELETE APPLY

Figure 81.

- Complete the Customer Information fields with the customer information that is associated with the key that you want to add and register. These fields are self-explanatory.
- Complete the VAR Information fields with the value-added reseller (VAR) information that is associated with the key that you want to add and register. These fields are self-explanatory.
- In the Registration Key field, enter the registration key for the license that you want to add and register.
- Click **Add** to add your license to the table. The key details have the same meaning as those shown on the Inventory screen (see the Key Details section in [Table 33](#) on page 149).
- Click **Apply** to register your license.

To delete a license from the table, select its radio button, and then click **Delete**.



## Retrieve Your Licenses

If NETGEAR exchanged your wireless controller for another one, your licenses no longer display on the Inventory and Registration screens. You need to retrieve your licenses from the license update server.

- **To retrieve licenses after you have received a replacement unit from NETGEAR:**
  1. Make sure that the wireless controller is connected to the Internet.
  2. Select **Maintenance > License**, and then click the **Advanced** tab. The Advanced screen displays.
  3. Click **Replace**. The wireless controller connects to the license update server and retrieves your licenses.

# Managing Stacking and Redundancy

# 10

This chapter includes the following sections:

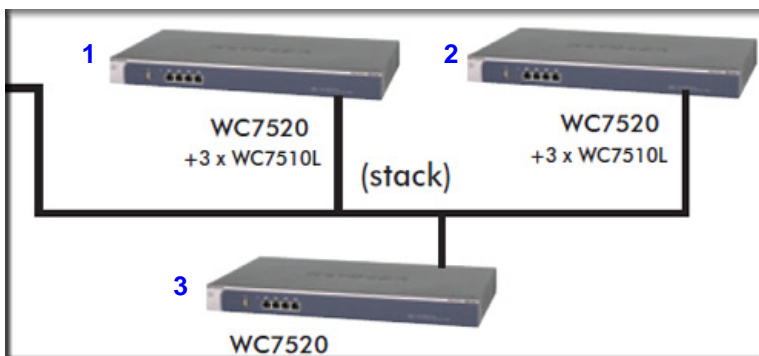
- *Manage Stacking*
- *Manage Redundancy*

## Manage Stacking

The wireless controller supports stacking of up to three units for management of up to 150 access points through purchased licensing (see [Licenses](#) on page 18). One wireless controller functions as the primary controller (also known as the master), and the other two wireless controllers function as secondary controllers (also known as slaves).

The following figure shows a stacked configuration that is licensed to manage up to 120 access points:

- Two controllers (**1** and **2**) each support up to 50 access points.
- One controller (**3**) supports up to 20 access points.



**Figure 82.**

The wireless controllers that you intend to make members of the stack need to be connected over a wired connection. A switch or router can be located between the wireless controllers that are part of a stack.

You configure the primary and secondary controllers individually, enable stacking on all controllers, and then synchronize their access point configurations with the primary

controller. When stacking is enabled, the primary controller synchronizes the administrative user name and password and the firmware image with the secondary controllers.

The master controller can push all configuration changes to the individual access points through the secondary controllers. For ease of management, you can configure location-based profiles on the master controller and assign a location to each secondary controller.

The stacking feature allows wireless clients to roam from an access point that is managed by one of the controllers in the stacking group to any access point managed by the other controllers in the same stacking group.

These are the capacities of the primary and secondary controllers in a stack:

- **Primary controller.** You can perform the following tasks:
  - Manage the secondary controllers
  - Perform RF planning for the secondary controllers
  - Configure the entire network, including access point discovery and license reinforcement
  - Monitor the entire network
  - Push new a firmware image to the secondary controllers
- **Secondary controller.** You can perform the following tasks:
  - Access the primary controller's web management interface (all controllers share the same administrative user name and password)
  - Configure the subnetwork
  - Monitor the subnetwork
  - Upgrade the firmware image on the secondary controller only
  - Perform access point discovery for the subnetwork
  - Reinforce licenses for the subnetwork

## Configure Stacking

➤ **To configure stacking:**

1. Select **Stacking > Stacking/Redundancy**. The Stacking/Redundancy screen displays:

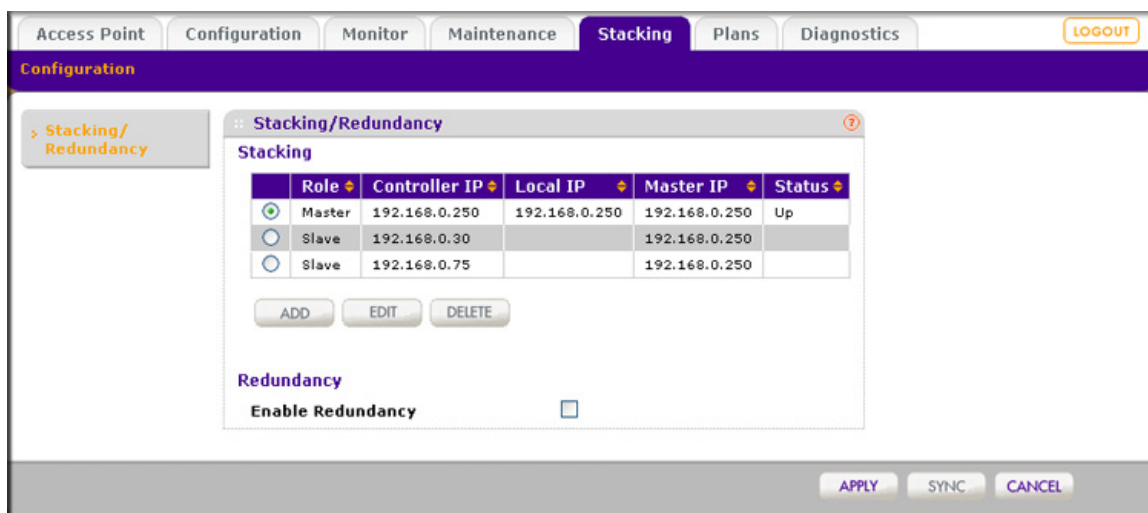


Figure 83.

The Stacking table shows all wireless controllers in the stack, with their IP address and role (Master or Slave).

2. Click **Add** to add a wireless controller to the stack. The Add Settings pop-up window displays:

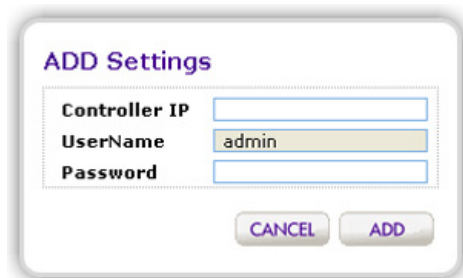


Figure 84.

3. Configure the settings as explained in the following table:

Table 35. Stacking settings

| Setting       | Description   |
|---------------|---|
| Controller IP | Enter the IP address of the controller.   |
| UserName      | The user name is a nonconfigurable field that displays the user name with which you logged in to the web management interface of the wireless controller. |
| Password      | Enter the password to access the controller.  |

4. Click **Add**. The wireless controller is added to the Stacking table, which shows the following fields:

Table 36. Stacking table fields

| Setting    | Description  |
|------------|--|
| Role       | The role or function that the wireless controller has in the stack: either Master or Slave.  |
| Controller | The IP address of the wireless controller.   |
| Local IP   | The local IP address of the wireless controller in a redundancy group. If you have not configured redundancy, the local IP address for the master controller is identical to its controller IP address, and there is no local IP address for any slave controller. |
| Master IP  | The IP address of the master in the stack.   |
| Status     | The status of the wireless controller: either Up or Down.  |

- As an option, click **Sync** on the master controller in the stack to synchronize the profiles, captive portals, and user management settings to the slave controller in the stack. After synchronization, the slave controller reboots.

---

**Note:** On the slave controller in the stack, if you add the master controller as a stack member, the slave controller becomes the new master controller, and the original master controller becomes the new slave controller.

---

## Controller Selection List

After you have added one or more wireless controllers to the stack, most screens in the web management interface display a controller selection list that lets you select the wireless controller that you want to configure:

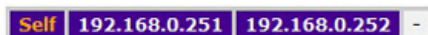


Figure 85.

Click **Self** to configure the wireless controller that you have accessed through the web management interface (in the previous figure, the controller with IP address 192.168.0.251); click another IP address (in the previous figure, IP address 192.168.0.252) to configure that controller in the stack. The following figure provides an example of a screen that shows the controller selection list.

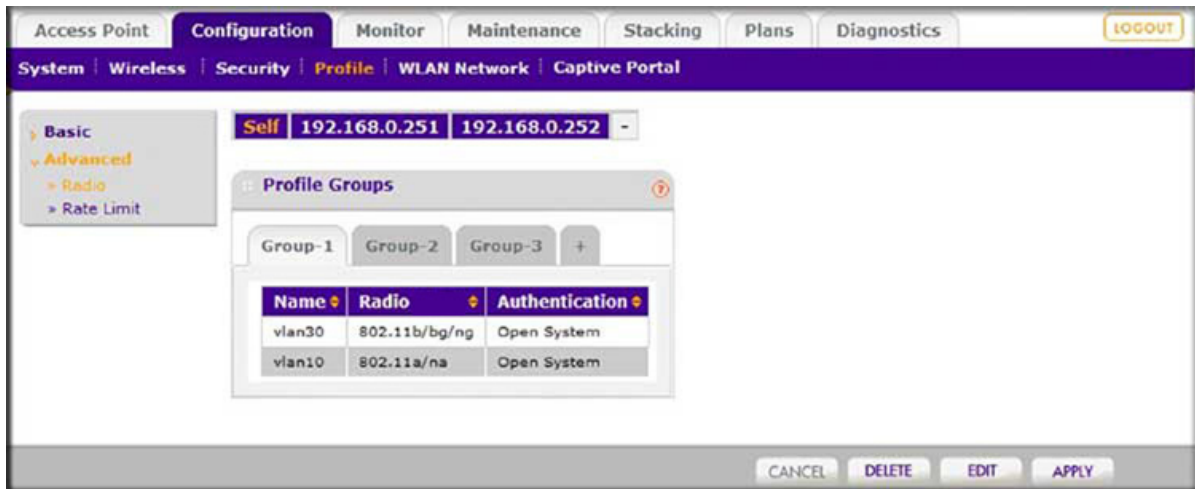


Figure 86.

## Manage Redundancy

The wireless controller supports N:1 redundancy with failover. Redundancy is implemented through the use of the Virtual Router Redundancy Protocol (VRRP).

### Single Controller with Redundancy

You can configure two controllers to form a redundancy group. You then designate one controller in the redundancy group as the primary controller and the other wireless controller as the redundant controller. If the primary controller fails or is disconnected from the network, an automatic failover to the redundant controller occurs. The redundant controller then takes over all functions of the primary controller.

If you want to add a redundant controller to a stack of two or three controllers, see [N:1 Redundancy](#) on page 160.

---

**Note:** When a redundancy failover occurs, wireless clients might experience a service interruption of a few seconds.

---

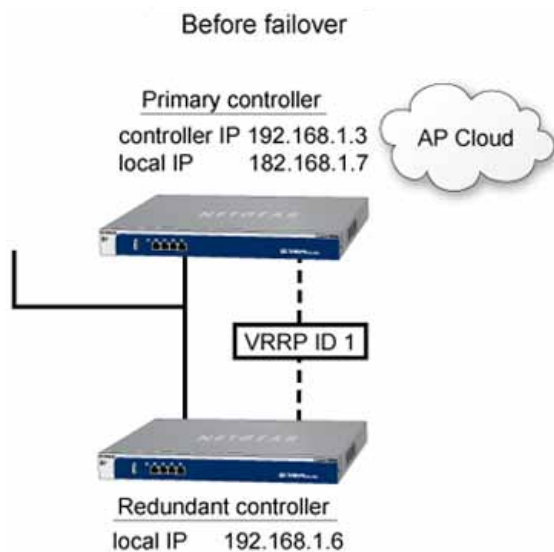
### Requirements and Restrictions for a Single Controller with Redundancy

These are the requirements and restrictions for a single controller with redundancy to function correctly:

- The primary controller and redundant controller need to be in the same management VLAN and IP subnet.
- The VRRP ID for the relationship between the primary controller and redundant controller needs to be unique, also in relation to any other VRRP IDs that might be used for other purposes in the network.
- The primary controller and redundant controller need to run the same firmware version. If the firmware versions do not match, redundancy does not work.
- The licenses on the redundant controller need to match those on the primary controller. If the licenses do not match, redundancy does not work.
- The primary controller and redundant controller need to have the same controller IP address at which they provide the service, but each controller has its own unique local IP address.

### Example of a Configuration with a Single Controller with Redundancy

The following figure shows a configuration with a primary controller and a redundant controller before a failover has occurred.



**Figure 87.**

The following figure shows the settings on the Stacking/Redundancy screen before a failover has occurred.



Figure 88.

The following figure shows a configuration with a primary controller and a redundant controller *after* a failover has occurred:

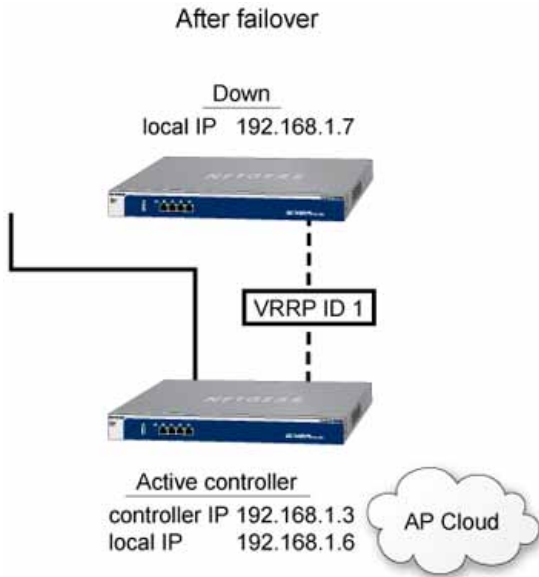


Figure 89.

## N:1 Redundancy

With N:1 redundancy, you can add one redundant controller for up to three controllers, that is, a redundancy group can consist of four controllers, one of which is a redundant controller.

In an N:1 redundancy group with three primary controllers and one redundant controller, you could consider the redundant controller to consist of three virtual controllers, each of which



has a redundancy relationship with a primary controller. You need a unique VRRP ID for each relationship.

Each controller in the redundancy group has a unique controller IP address and a unique local IP address. Local addresses remain constant so a controller can always be identified before and after a failover. If the primary controller fails or is disconnected from the network, an automatic failover to the redundant controller occurs. The redundant controller then takes ownership of the controller IP address of the primary controller and takes over all functions of the primary controller.

After a failover has occurred, there is no longer any redundancy available for the other primary controllers in the redundancy group.

When the primary controller that went down and for which the redundant controller took over comes back up *and* is stable, a switchback occurs automatically, in which case ownership of the controller IP address is returned to the primary controller that came back up. The redundant controller reassumes its passive position, and redundancy is once again available for all primary controllers in the redundancy group.

---

**Note:** When a redundancy failover occurs, wireless clients might experience a service interruption of a few seconds.

---

### ***Requirements and Restrictions for N:1 Redundancy***

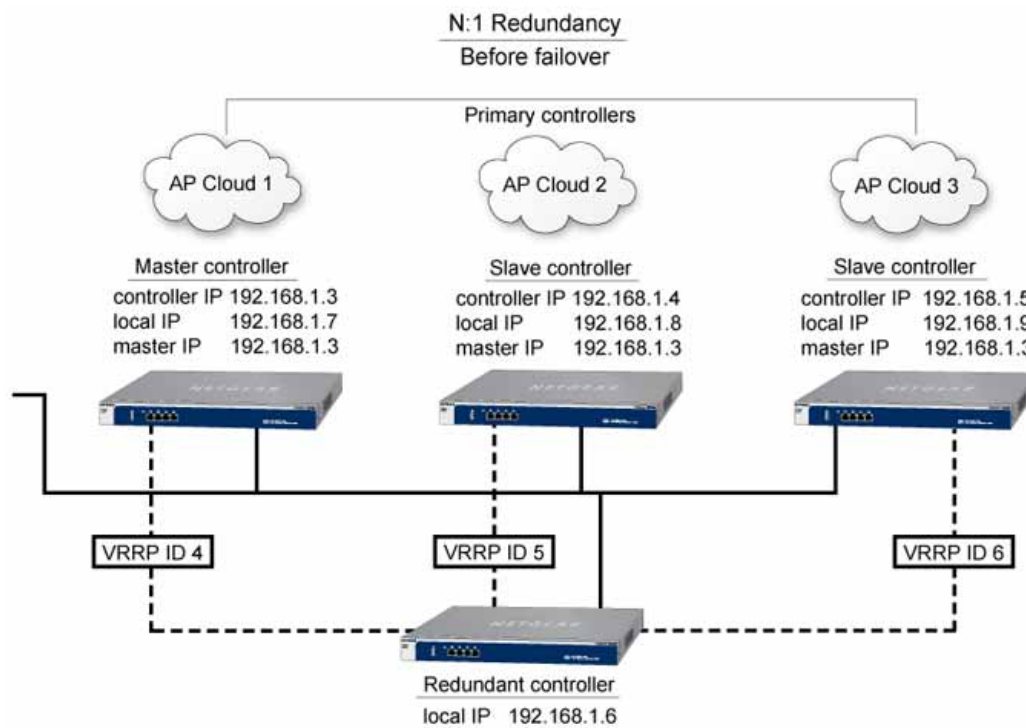
These are the requirements and restrictions for N:1 redundancy to function correctly:

- All controllers in a redundancy group need to be in the same management VLAN and IP subnet.
- The primary controllers need to be stacked.
- If three or four controllers are in the same redundancy group, you need to configure one controller as the redundant controller and all other controllers as primary controllers.
- All controllers in the redundancy group need to run the same firmware version. If the firmware versions do not match, redundancy does not work.
- The licenses on the redundant controller need to match those on the primary controller that has the largest number of licenses. For example, in a redundancy group with two primary controllers, if one primary controller has a license for 20 access points and the other primary controller has a license for 50 access point, the redundant controller needs to have a license for 50 access point. If the licenses do not match, redundancy does not work.
- For the relationship of each primary controller with the redundant controller, you need to configure a unique VRRP ID, also in relation to any other VRRP IDs that might be used for other purposes in the network. You also need to configure a unique local controller IP address for each controller in the redundancy group.

- When a failover occurs and the redundant controller takes over for a primary controller, redundancy is no longer available for the other primary controllers in the redundancy group.
- When you upgrade from a firmware release before release 2.2 to release 2.2, you need to reconfigure redundancy.

### Example of an N:1 Redundancy Configuration

The following figure shows an N:1 configuration with three stacked controllers and one redundant controller before a failover has occurred.



**Figure 90.**

The following figure shows the N:1 settings on the Stacking/Redundancy screen before a failover has occurred.

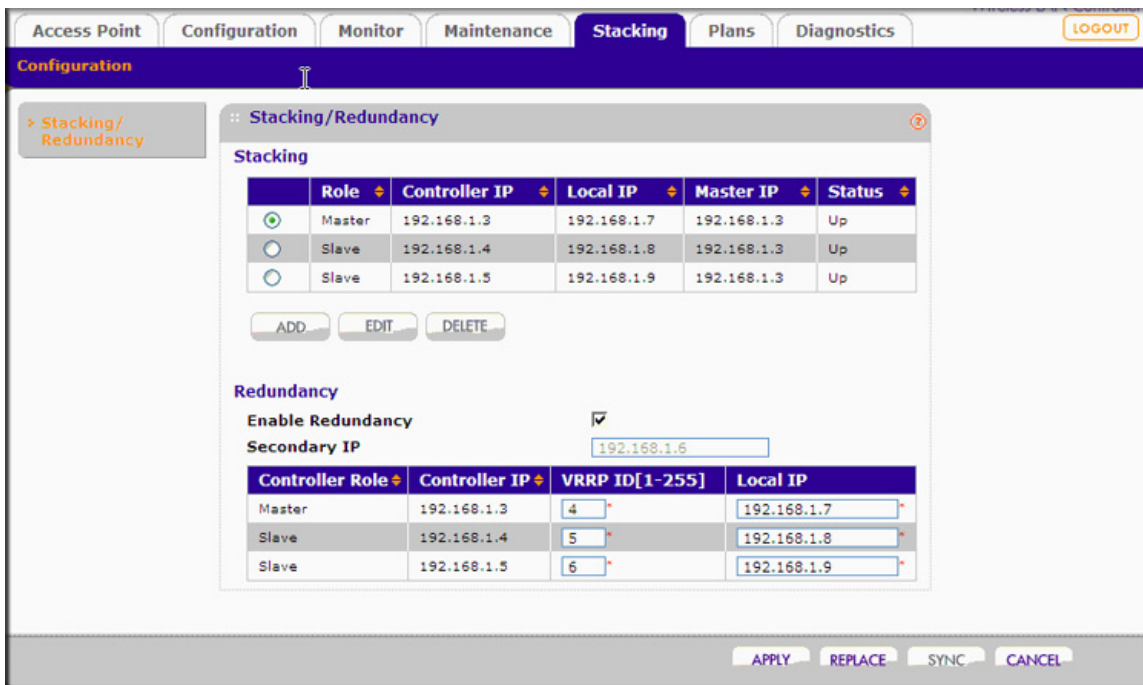


Figure 91.

The following figure shows an N:1 configuration with three primary controllers and one redundant controller *after* a failover has occurred:

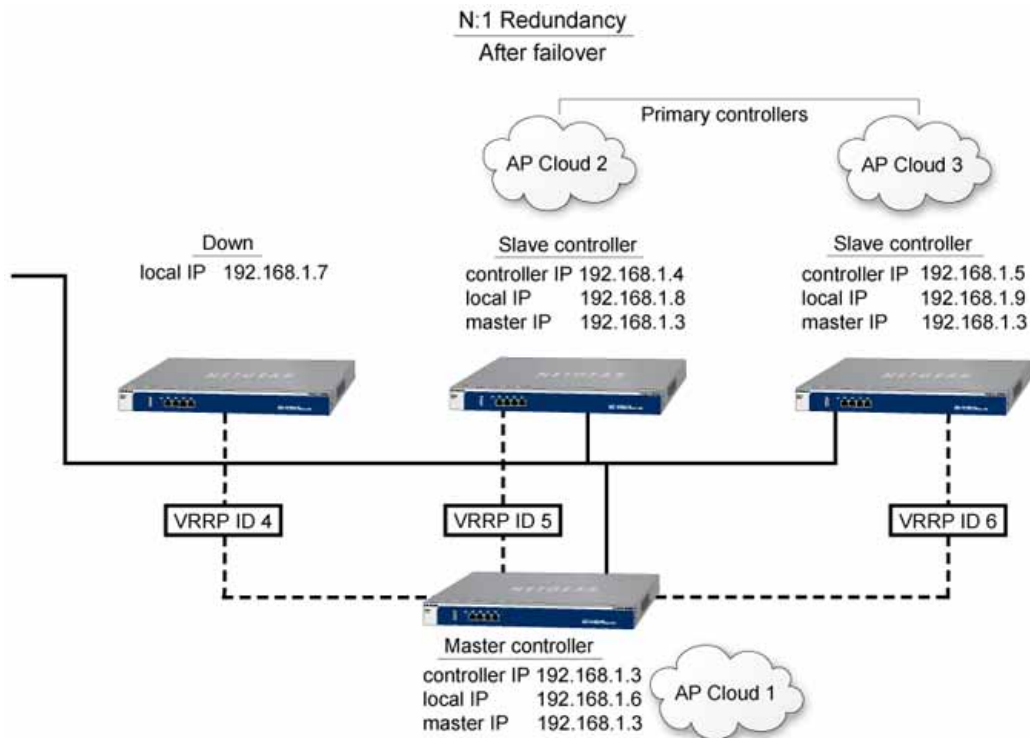


Figure 92.

## Configure Redundancy

To enable redundancy, configure the redundancy settings on both the primary and redundant controllers. If you configure redundancy with two controllers, there is a single primary controller; if you configure N:1 redundancy, there are two or three primary controllers.

➤ **To configure redundancy:**

1. Select **Stacking > Stacking/Redundancy**. The Stacking/Redundancy screen displays (see [Figure 83](#) on page 156).
2. Select the **Enable Redundancy** check box. The Stacking/Redundancy screen expands to display the Redundancy table, and the Secondary Controller Information pop-up window displays.

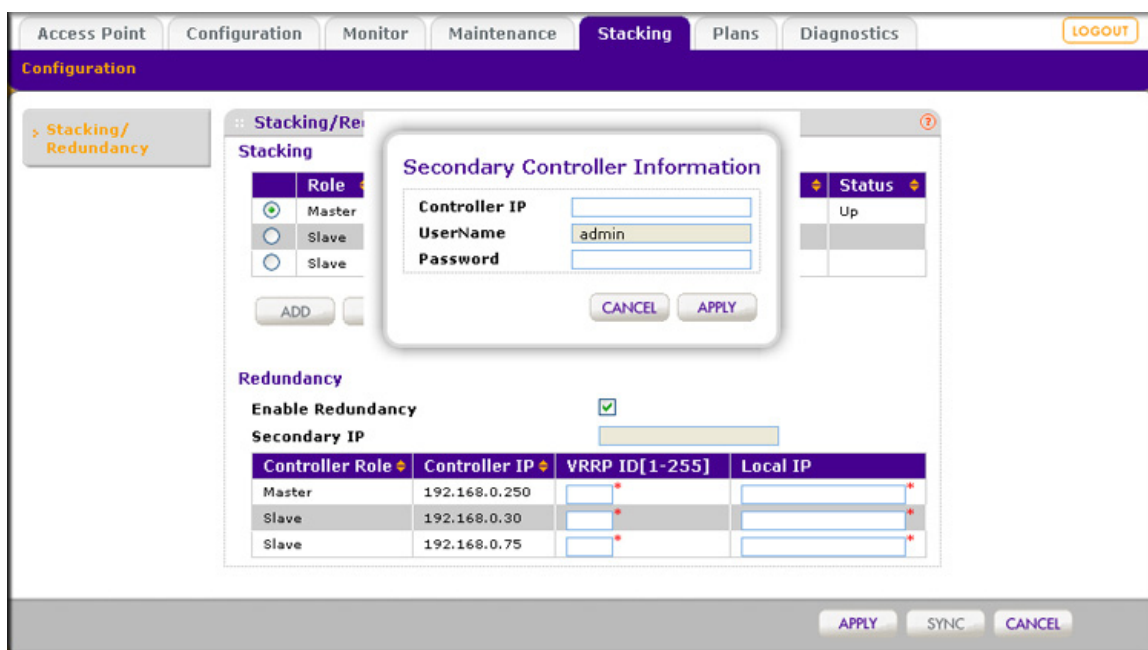


Figure 93.

3. Configure the settings as explained in the following table:

**Table 37. Redundant (or secondary) controller settings**

| Setting       | Description  |
|---------------|--|
| Controller IP | Enter the local IP address of the redundant controller. This IP address remains assigned to the redundant controller to allow it to be identified before and after a failover. |
| UserName      | The user name is a nonconfigurable field that displays the user name with which you logged in to the web management interface of the wireless controller.                      |
| Password      | Enter the password to access the redundant controller.   |

4. Click **Apply**. The local IP address of the redundant controller is displayed in the Secondary IP field above the Redundancy table.

5. Configure the VRRP IDs and local IP addresses of the controllers in the stack so they can become part of the redundancy group. The settings, including the nonconfigurable fields, are explained in the following table:

**Table 38. Redundancy settings**

| Setting         | Description   |
|-----------------|---|
| Controller Role | This is a nonconfigurable field that shows if the primary controller functions as a master or slave controller in the stack for which you are configuring redundancy.<br><br><b>Note:</b> For a single controller with redundancy, the primary controller role is always master.  |
| Controller IP   | This is a nonconfigurable field that shows the IP address of the primary controller. This IP address is transferred to the redundant controller if a failover occurs.   |
| VRRP ID [1-255] | For each primary controller in the redundancy group, enter a number from 1 through 255 as the VRRP ID. This enables each primary controller to have a unique relationship with the redundant controller.<br><br><b>Note:</b> For a single controller with redundancy, there is a single primary controller and therefore a single VRRP ID.  |
| Local IP        | For each primary controller in the redundancy group, enter a local IP address. This IP address remains assigned to the primary controller and is <i>not</i> transferred to the redundant controller if a failover occurs. This allows each primary controller to be identified before and after a failover.<br><br><b>Note:</b> For a single controller with redundancy, there is a single primary controller for which you need to enter a local IP address. |



**WARNING!**

**Enabling redundancy causes the wireless controller to reboot, which might temporarily affect traffic on the managed access points in the network.**

6. Click **Apply** to save your settings.

---

**Note:** After you have configured redundancy, click **Refresh** on the Network monitoring screens to display redundancy information (see [Monitor the Network](#) on page 167).

---

➤ **To modify the redundant controller after you have configured redundancy:**

1. Click **Replace**. The Replacing Controller Information pop-up window displays.

***Note:** The Replace button displays onscreen only after a redundancy configuration has become active. The button is shown on [Figure 91](#) on page 163.*



The image shows a dialog box titled "Replacing Controller Information". It contains three input fields: "Local IP" (empty), "UserName" (containing "admin"), and "Password" (empty). At the bottom of the dialog are two buttons: "CANCEL" and "APPLY".

2. Modify the settings as explained in [Table 37](#) on page 164.
3. Click **Apply**. The modified local IP address of the redundant controller is displayed above the Redundancy table.

➤ **To delete a redundancy group:**

Clear the **Enable Redundancy** check box. Doing so causes the redundant controllers in the redundancy group to reboot and return to the factory default state except for their IP address.

# Monitoring the Wireless Network and Components

---

# 11

This chapter includes the following sections:

- [Monitor the Network](#)
- [Monitor the Wireless Controller](#)
- [Monitor the SSIDs](#)
- [Monitor the Clients](#)

The monitoring screens display *read-only* status information of the network and its various components. Most screens have a Refresh button; clicking this button displays the most recent information.

---

**Note:** In tables with many entries, you can select how many entries are displayed onscreen by selecting a number from the Entry Per Page drop-down list in the lower left of the table.

---

---

**Note:** There is no consistency of information among the screens that are shown in this chapter.

---

## Monitor the Network

---

**Note:** The Network configuration menu tab displays under the Monitor main navigation menu tab *only* when you have configured stacking. If you have not configured stacking, go to [Monitor the Wireless Controller](#) on page 179.

---

---

**Note:** After you have configured redundancy, click **Refresh** on the Network monitoring screens to display redundancy information.

---

➤ **To monitor the network:**

1. Select **Monitor > Network**.
2. Select one of the following submenu links to display a network monitoring screen:
  - **Summary**. See [View the Network Summary Screen](#)
  - **Usage**. See [View Network Usage](#)
  - **Controller**. See [View Wireless Controllers in the Network](#)
  - **Access Points**. See [View Managed Access Points in the Network](#)
  - **Clients**. See [View Clients in the Network](#)
  - **Profiles**. See [View Security Profiles in the Network](#)

## View the Network Summary Screen

The following figure shows the Network Summary screen when both stacking and redundancy are configured.

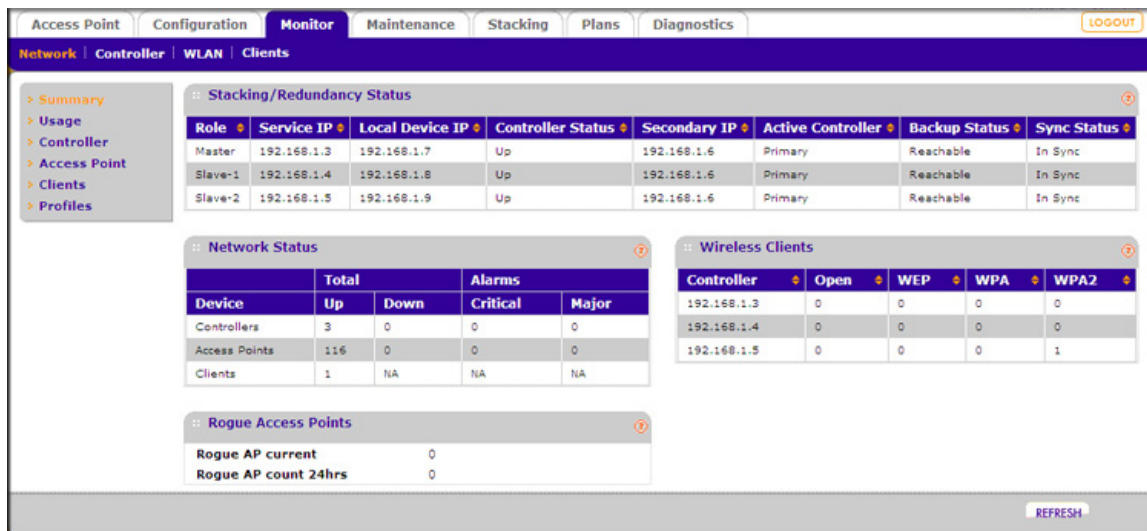


Figure 94.

The following table explains the fields of the Stacking/Redundancy Status, Network Status, Wireless Clients, and Rogue Access Points tables on the Network Summary screen:

Table 39. Network summary information

| Item                                      | Description  |
|---|--|
| <b>Stacking/Redundancy Status section</b> |  |
| Role                                      | The role of the wireless controller in a stacking configuration (Master or Slave).   |
| Service IP                                | The controller IP address. This IP address is transferred to the secondary controller after a failover has occurred in a redundancy group. |



Table 39. Network summary information (continued)

| Item  | Description  |   |
|---|--|---|
| Local Device IP   | The local IP address of a primary controller in a redundancy group. This IP address remains assigned to the primary controller and is not transferred to the secondary controller if a failover occurs. This allows the primary controller to be identified before and after a failover. |   |
| Controller Status   | The state of the wireless controller (Up or Down).   |   |
| Secondary IP  | The IP address of the secondary controller in a redundancy group.  |   |
| Active Controller   | The active controller in a redundancy group (Primary or Secondary).  |   |
| Backup Status   | The status of the secondary controller in a redundancy group (Reachable or Not reachable).   |   |
| Sync Status   | The synchronization status between the wireless controllers in a redundancy group (In Sync or Not in Sync).  |   |
| <b>Network Status section</b>   |  |   |
| For each wireless controller, access point, and client, the following information displays: |  |   |
| Total   | Up   | The total number of managed devices that are running correctly.   |
|   | Down   | The total number of managed devices that cannot be pinged.  |
| Alarms  | Critical   | The wireless controller can ping these managed devices, but either cannot log in or has detected that these device are different from the ones that were configured.  |
|   | Major  | The number of managed devices for which the configuration differs from the one that is set on the wireless controller. This situation occurs most likely because the device runs outdated firmware or the wireless controller changed the configuration while the device was down or offline. |
| <b>Wireless Clients section</b>   |  |   |
| For each wireless controller and wireless client, the following information displays:       |  |   |
| Controller  | The IP address of the wireless controller that manages the access points to which the wireless clients are connected.  |   |
| Open  | The number of wireless clients that are connected to managed access points using security profiles configured with open mode.  |   |
| WEP   | The number of wireless clients that are connected to managed access points using security profiles configured with WEP.  |   |
| WPA   | The number of wireless clients that are connected to managed access points using security profiles configured with WPA.  |   |
| WPA2  | The number of wireless clients that are connected to managed access points using security profiles configured with WPA2.   |   |

Table 39. Network summary information (continued)

| Item                               | Description  |
|------------------------------------|--|
| <b>Rogue Access Points section</b> |  |
| Rogue AP current                   | The total number of unique rogue and unmanaged neighboring access points that are detected now in the network.                     |
| Rogue AP count 24hrs               | The total number of unique rogue and unmanaged neighboring access points that were detected over the last 24 hours in the network. |

## View Network Usage

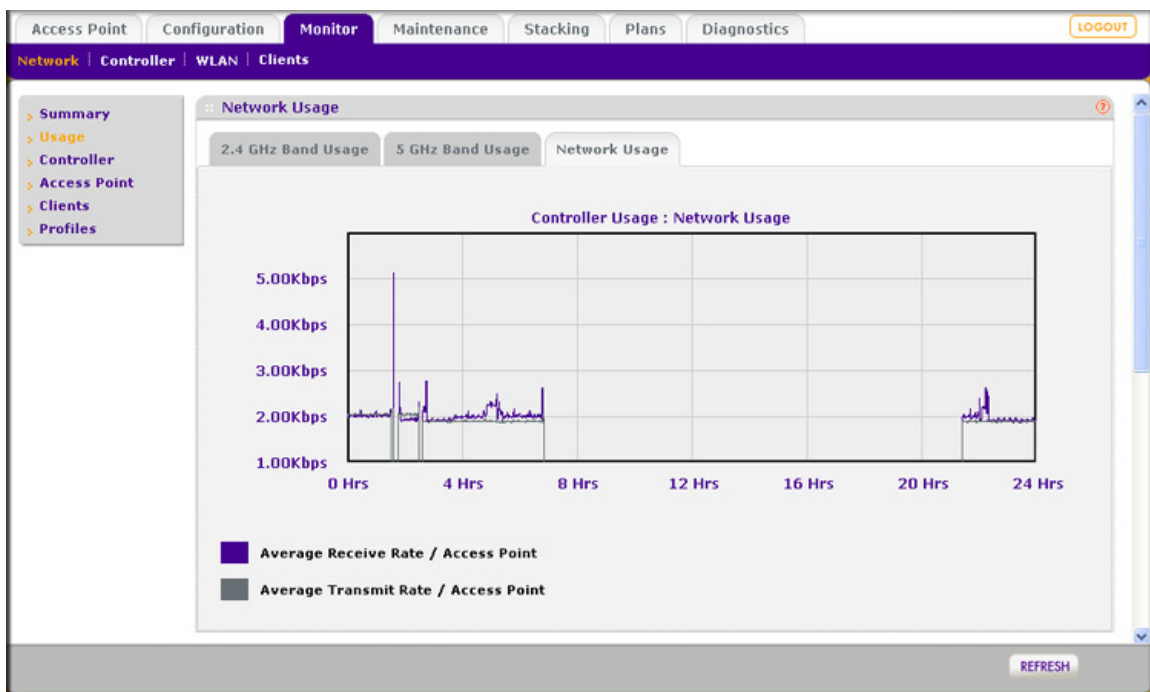
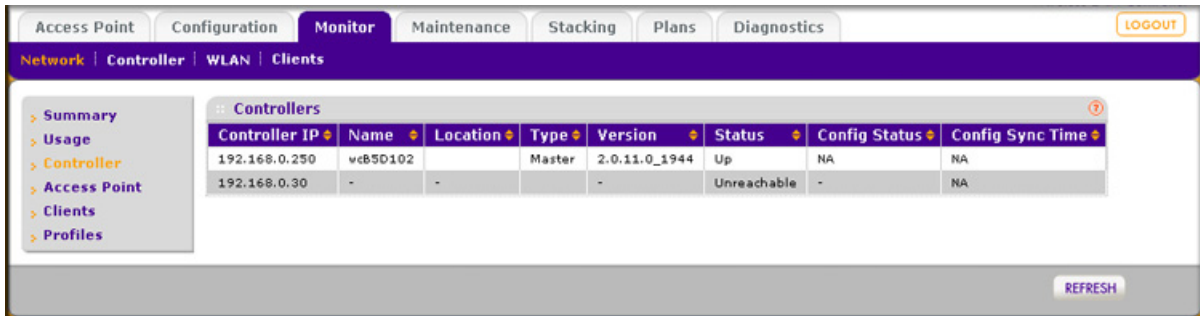


Figure 95.

The Network Usage screen displays a graphic of the average data traffic rate that was received and transmitted over the last 24 hours by all access points in the network. Select the type of usage you want to display by clicking one of the following tabs:

- **2.4 GHz Band Usage.** Displays combined 802.11b-, 802.11g-, and 802.11n-mode usage.
- **5 GHz Band Usage.** Displays combined 802.11a- and 802.11n-mode usage.
- **Network Usage.** Displays Ethernet usage (shown in the previous figure).

## View Wireless Controllers in the Network



**Figure 96.**

The Network Controllers screen lets you monitor the stacking configuration of the wireless controllers in the network.

The following table explains the fields of the Controllers table on the Network Controllers screen:

**Table 40. Network controllers information**

| Item             | Description  |
|------------------|--|
| Controller IP    | The IP address of the wireless controller.   |
| Name             | The name of the wireless controller (see <a href="#">Configure General Settings</a> on page 63).   |
| Location         | The location of the wireless controller (see <a href="#">Configure General Settings</a> on page 63).   |
| Type             | The function of the wireless controller in a stack (either Master or Slave).   |
| Version          | The firmware version that the wireless controller is running.  |
| Status           | The stacking status of the wireless controller (for example, Up or Unreachable).   |
| Config Status    | The firmware configuration status of the wireless controller (for example, Update Successful).<br><b>Note:</b> This field is applicable only to a wireless controller that functions as a slave. |
| Config Sync Time | The time that the wireless controller synchronized its firmware.<br><b>Note:</b> This field is applicable only to a wireless controller that functions as a slave.                               |

## View Managed Access Points in the Network

Because the Network Access Point screen is a wide screen, it is shown in the following two figures:

The screenshot shows the 'Monitor' tab of the Network Access Point screen. The left sidebar contains a navigation menu with the following items: Summary, Usage, Controller, Access Point (highlighted), Clients, and Profiles. The main content area displays a table titled 'Access Point' with the following data:

| Select                           | Name          | Location       | Status  | MAC               | IP            | Model    | Remote |
|----------------------------------|---------------|----------------|---------|-------------------|---------------|----------|--------|
| <input checked="" type="radio"/> | netgearA10668 | Administration | healthy | c4:3d:c7:a1:06:60 | 192.168.0.168 | WNDAP360 | Remote |
| <input type="radio"/>            | netgear7B2488 | Orthopedics    | healthy | c0:3f:0e:7b:24:80 | 192.168.0.163 | WNAP210  | Local  |
| <input type="radio"/>            | netgear7B26D8 | Surgery        | healthy | c0:3f:0e:7b:26:d0 | 192.168.0.162 | WNAP210  | Local  |

Figure 97. Left side of the Network Access Point screen

The screenshot shows the right side of the Network Access Point screen. The top right corner has a 'LOGOUT' button. The main content area displays a table with the following data:

| Sentry | Building          | Floor   | 2.4 GHz Channel | 5 GHz Channel | Uptime           | Controller IP |
|--------|-------------------|---------|-----------------|---------------|------------------|---------------|
| No     | Building-Remote-1 | Floor-1 | 1 / 2.412Ghz    | 36 / 5.180Ghz | 20 mins, 16 secs | 192.168.0.250 |
| No     | Clinic            | Floor-1 | 6 / 2.437Ghz    | NA            | 20 mins, 18 secs | 192.168.0.250 |
| No     | Clinic            | Floor-1 | 11 / 2.462Ghz   | NA            | 20 mins, 20 secs | 192.168.0.250 |

At the bottom of the table, there are three buttons: REFRESH, DETAILS, and EXPORT.

Figure 98. Right side of the Network Access Point screen

The Network Access Point screen lets you monitor all managed access points in the network. To view additional access points, click **Next**; to return to the previous access points, click **Previous**.

The following table explains the fields of the Access Point table on the Network Access Point screen:

Table 41. Network access point information

| Item     | Description   |
|----------|---|
| Select   | The radio button that lets you select the access point. When you click the <b>Details</b> button, the corresponding AP Details pop-up window displays (see <a href="#">Figure 99</a> on page 174 and <a href="#">Figure 100</a> on page 174). |
| Name     | The name of the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59).   |
| Location | The location of the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59).   |

Table 41. Network access point information (continued)

| Item            | Description  |
|-----------------|--|
| Status          | The status of the access point (Healthy or Down).  |
| MAC             | The MAC address of the access point.   |
| IP              | The IP address of the access point.  |
| Model           | The model of the access point (WNAP210, WNAP320, WNDAP350, or WNDAP360).   |
| Remote          | Shows the site designation (Local or Remote) of the access point.  |
| Sentry          | Shows whether or not (Yes or No) sentry mode is enabled.   |
| Building        | The building to which you assigned the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59).   |
| Floor           | The floor to which you assigned the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59).  |
| 2.4 GHz Channel | The configured 2.4 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation. |
| 5 GHz Channel   | The configured 5 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation.   |
| Uptime          | The period since the access point was last restarted.  |
| Controller IP   | The IP address of the wireless controller that manages the access point.   |

To export the list of access points, click **Export**.

To see details about an access point, select its corresponding radio button in the Select column of the Access Point table, and then click the **Details** button to display the AP Details pop-up window. Because of its size, an example of this window is shown in two figures.

To close the AP Details window, click **OK**.

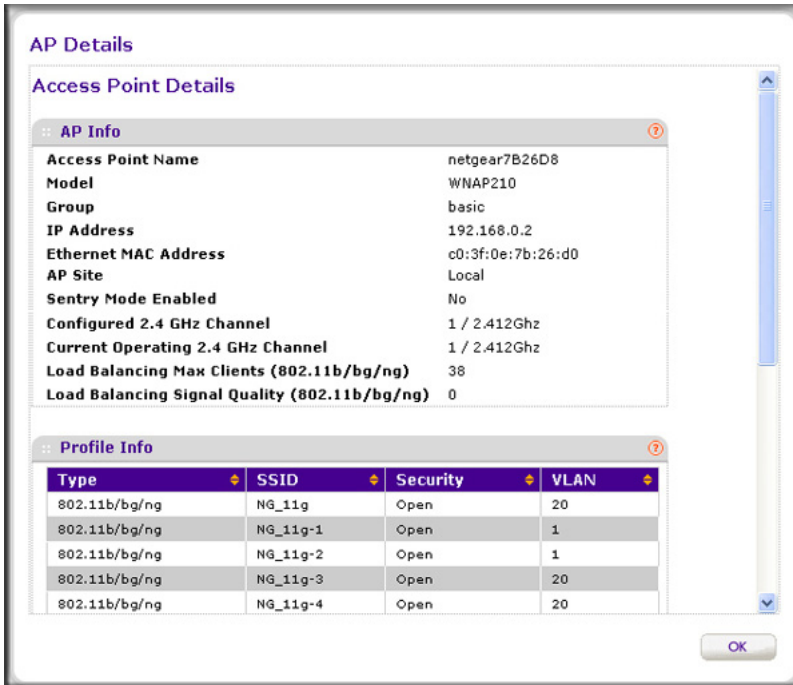


Figure 99.

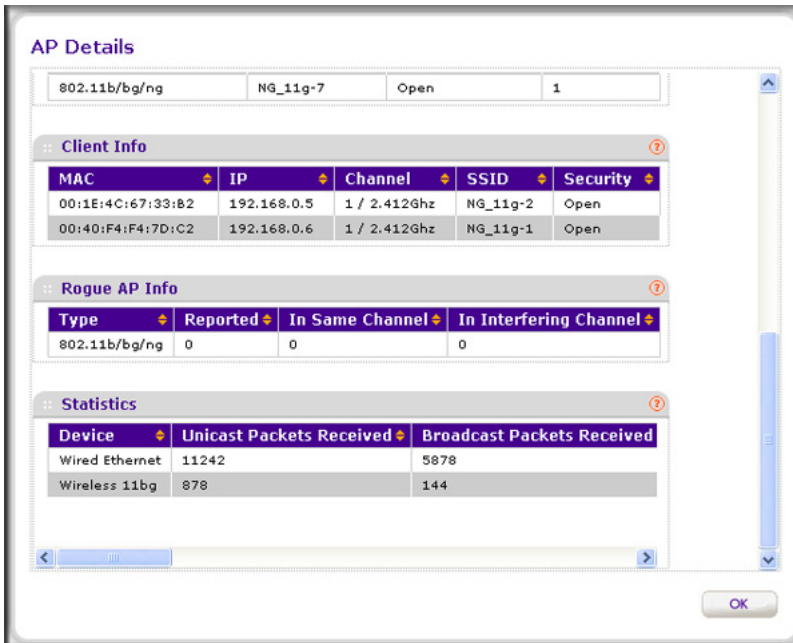


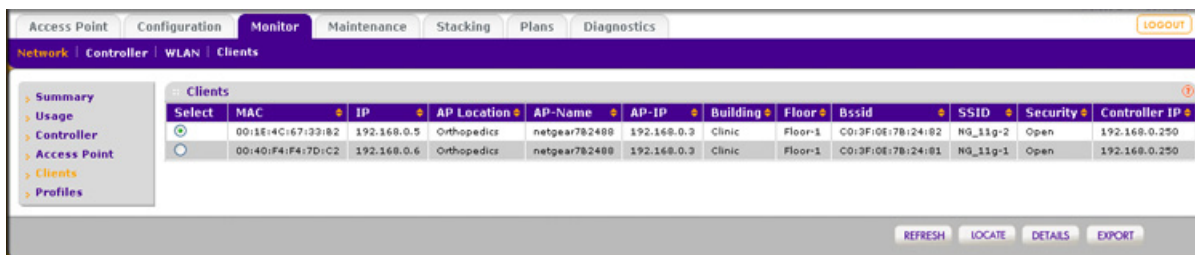
Figure 100.

The following table explains the fields of the AP Details window:

**Table 42. Network access point details information**

| Item  | Description   |
|---|---|
| <b>AP Info section</b>  |   |
| This information is self-explanatory.   |   |
| <b>Profile Info section</b>   |   |
| For each security profile that is configured on the selected access point, the following information displays:  |   |
| Type  | The type of profile (802.11b/bg/ng or 802.11a/na).  |
| SSID  | The wireless network SSID for the security profile.   |
| Security  | The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) for the security profile.   |
| VLAN  | The VLAN ID or VLAN name for the security profile.  |
| <b>Client Info section</b>  |   |
| The information that displays depends on the type and security of the connection that the client has to the access point.   |   |
| For each wireless client that is connected to the selected access point, some or all of the following information displays:   |   |
| MAC   | The MAC address of the wireless client.   |
| IP  | The IP address of the client.   |
| Channel   | The channel that the wireless client is using to connect to the access point.   |
| SSID  | The wireless network SSID that the wireless client is using to connect to the access point.                             |
| Security  | The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2). |
| <b>Rogue AP Info section</b>  |   |
| For all rogue and unmanaged neighboring access points combined that are detected by the selected managed access point, the following information displays:  |   |
| Type  | The type of profile that the rogue access point is using to connect to the access point (802.11b/bg/ng or 802.11a/na).  |
| Reported  | The total number of detected rogue access points in the wireless mode.  |
| In Same Channel   | The total number of detected rogue access points in the same channel.   |
| In Interfering Channel  | The total number of detected rogue access points in the interfering channel.  |
| <b>Statistics</b>   |   |
| For each type of usage (Ethernet, 802.11b/bg/ng or 802.11a/na), statistics about transmitted and received packets and bytes displays for the selected access point. The actual statistics are self-explanatory. |   |
| <b>Note:</b> To see all fields of the table on the AP Details window, scroll to the right.  |   |

## View Clients in the Network



**Figure 101.**

The Network Clients screen lets you monitor all clients that are connected to the network. To view additional clients, click **Next**; to return to the previous clients, click **Previous**.

The following table explains the fields of the Clients table on the Network Clients screen:

**Table 43. Network clients information**

| Item          | Description   |
|---------------|---|
| Select        | The radio button that lets you select the client. When you click the <b>Details</b> button, the corresponding Client Details pop-up window displays (see <a href="#">Figure 102</a> on page 177). You can also click the <b>Locate</b> button to see the location of the client on a floor map. |
| MAC           | The MAC address of the wireless client.   |
| IP            | The IP address of the wireless client.  |
| AP Location   | The location of the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59) to which the wireless client is connected.   |
| AP-Name       | The name of the access point (see <a href="#">Edit and Remove Access Point Information</a> on page 59) to which the wireless client is connected.   |
| AP-IP         | The IP address of the access point to which the wireless client is connected.   |
| Building      | The building in which the wireless client is connected to the access point.   |
| Floor         | The floor on which the wireless client is connected to the access point.  |
| BSSID         | The MAC address of the access point's radio to which the wireless client is connected.  |
| SSID          | The wireless network SSID that the wireless client is using to connect to the access point.   |
| Security      | The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) that the wireless client is using to connect to the access point.   |
| Controller IP | The IP address of the wireless controller that manages the access point to which the wireless client is connected.  |

To see the location of the client on a floor map, select the client's radio button (in the Select column), and then click the **Locate** button.



To export the list of clients, click **Export**.

To see details about a client, select its corresponding radio button in the Select column of the Client table, and then click the **Details** button to display the Client Details pop-up window:

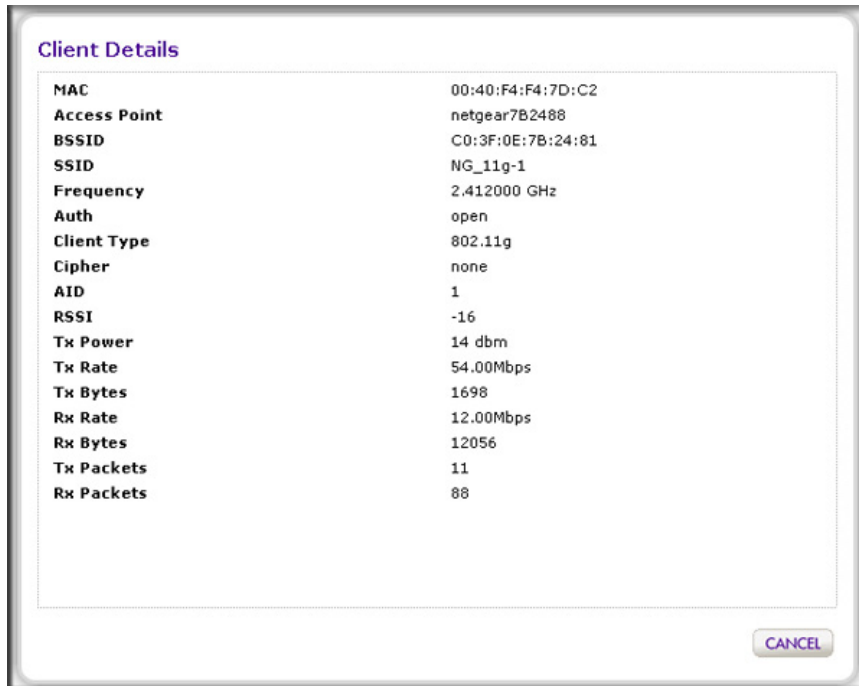


Figure 102.

To close the Client Details window, click **Cancel**.

The following table explains the fields of the Client Details window:

Table 44. Network client details information

| Item         | Description   |
|--------------|---|
| MAC          | The MAC address of the wireless client.   |
| Access Point | The name of the access point to which the wireless client is connected.   |
| BSSID        | The MAC address of the access point's radio to which the wireless client is connected.                                  |
| SSID         | The wireless network SSID that the wireless client is using to connect to the access point.                             |
| Frequency    | The channel frequency that the wireless client is using to connect to the access point.                                 |
| Auth         | The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2). |
| Client Type  | The wireless mode that the wireless client is using to connect to the access point (802.11a, b, g, or n).               |

Table 44. Network client details information (continued)

| Item       | Description   |
|------------|---|
| Cipher     | The type of encryption that the wireless client is using (WEP, AES, TKIP, or TKIP + AES). |
| AID        | The association ID of the client.   |
| RSSI       | The received signal strength indicator (RSSI) of the wireless client.                     |
| Tx Power   | The transmit power of the wireless client.  |
| Tx Rate    | The transmit rate in Mbps of the wireless client.   |
| Tx Bytes   | The number of bytes that the wireless client transmitted.                                 |
| Rx Rate    | The receive rate in Mbps of the wireless client.  |
| Rx Bytes   | The number of bytes that the wireless client received.                                    |
| Tx packets | The number of packets that the wireless client transmitted.                               |
| Rx Packets | The number of packets that the wireless client received.                                  |

## View Security Profiles in the Network

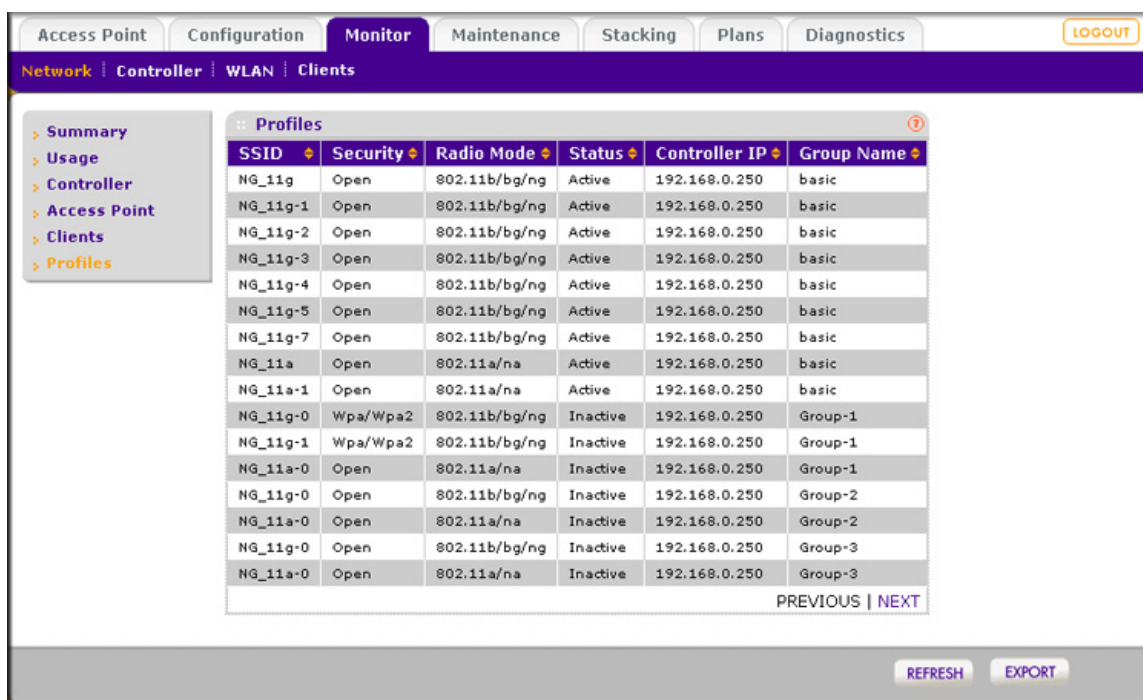


Figure 103.

The Network Profiles screen lets you monitor all security profiles in the network. To view additional profiles, click **Next**; to return to the previous profiles, click **Previous**.

The following table explains the fields of the Profiles table on the Network Profiles screen:

**Table 45. Network security profiles information**

| Item          | Description  |
|---------------|--|
| SSID          | The wireless network SSID for the security profile.                                    |
| Security      | The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) for the security profile.        |
| Radio Mode    | The wireless mode for the security profile (802.11b/bg/ng or 802.11a/na).              |
| Status        | The status of the security profile (Active or Inactive).                               |
| Controller IP | The IP address of the wireless controller on which the security profile is configured. |
| Group Name    | The name of the group of which the security profile is a member.                       |

To export the list of profiles, click **Export**.

## Monitor the Wireless Controller

To monitor a specific wireless controller, log in to its web management interface, and use the Monitor Controller screens described in this section.

---

**Note:** If you stack wireless controllers, you can view similar information about the stack by using the network monitor screens (see *Monitor the Network* on page 167).

---

➤ **To monitor the wireless controller:**

1. Select **Monitor > Controller**.
2. Select one of the following submenu links to display a wireless controller monitoring screen:
  - **Summary.** See *View the Wireless Controller Summary Screen*
  - **Usage.** See *View Wireless Controller Usage*
  - **Access Points.** See *View Access Points Managed by the Wireless Controller*
  - **Clients.** See *View Clients Managed by the Wireless Controller*
  - **Neighboring Clients.** See *View Neighboring Clients Detected by the Wireless Controller*
  - **Rogue AP.** See *View Rogue Access Points Detected by the Wireless Controller*
  - **Profiles.** See *View Security Profiles Managed by the Wireless Controller*
  - **DHCP Lease.** See *View DHCP Leases Provided by the Wireless Controller*
  - **Captive Portal Users.** See *View Captive Portal Guests and Users Managed by the Wireless Controller*

## View the Wireless Controller Summary Screen

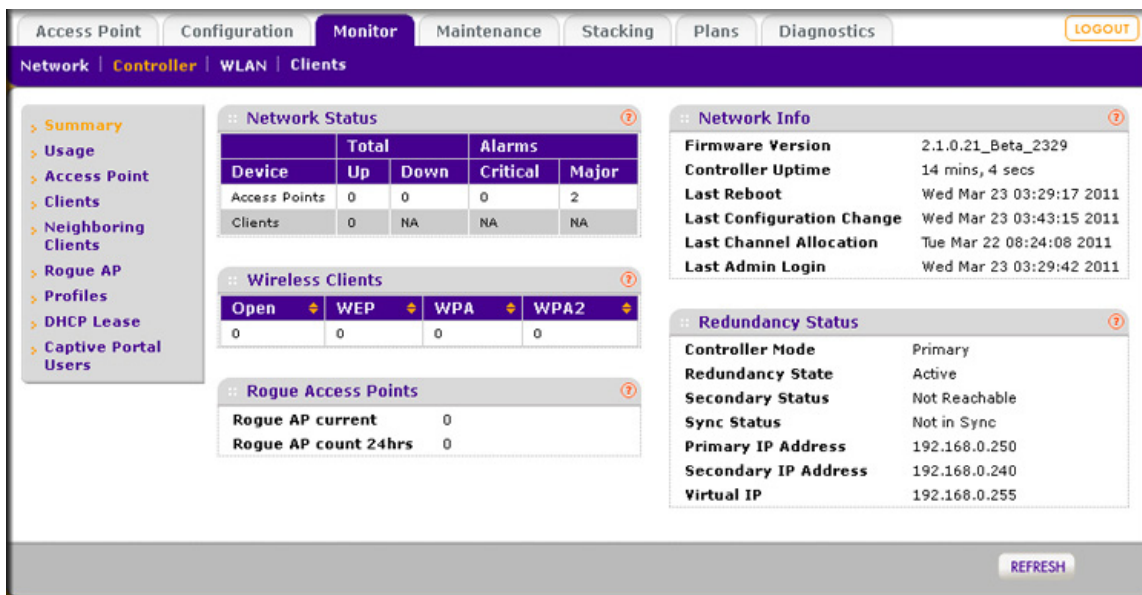


Figure 104.

The following table explains the fields of the Network Status, Wireless Clients, Rogue Access Points, Network Info, and Redundancy Status tables on the Controller Summary screen:

Table 46. Controller summary information

| Item  | Description   |   |
|---|---|---|
| <b>Network Status section</b>   |   |   |
| For each access point and client, the following information displays: |   |   |
| Total   | Up  | The total number of managed devices that are running correctly.   |
|   | Down  | The total number of managed devices that cannot be pinged.  |
| Alarms  | Critical  | The wireless controller can ping these managed devices, but either cannot log in or has detected that these device are different from the ones that were configured.  |
|   | Major   | The number of managed devices for which the configuration differs from the one that is set on the wireless controller. This situation occurs most likely because the device runs outdated firmware or the wireless controller changed the configuration while the device was down or offline. |
| <b>Wireless Clients section</b>                                       |   |   |
| For each wireless client, the following information displays:         |   |   |
| Open  | The number of wireless clients that are connected to managed access points using security profiles configured with open mode. |   |
| WEP   | The number of wireless clients that are connected to managed access points using security profiles configured with WEP.       |   |

**Table 46. Controller summary information (continued)**

| Item  | Description  |
|---|--|
| WPA   | The number of wireless clients that are connected to managed access points using security profiles configured with WPA.                                    |
| WPA2  | The number of wireless clients that are connected to managed access points using security profiles configured with WPA2.                                   |
| <b>Rogue Access Points section</b>  |  |
| Rogue AP current  | The total number of unique rogue and unmanaged neighboring access points that are detected now by the wireless controller.                                 |
| Rogue AP count 24hrs  | The total number of unique rogue and unmanaged neighboring access points that were detected over the last 24 hours by the wireless controller.             |
| <b>Network Info section</b>   |  |
| This information is self-explanatory.   |  |
| <b>Redundancy Status section</b>  |  |
| This information displays only if wireless controller redundancy is configured. |  |
| Controller Mode   | The redundancy mode in which the wireless controller functions (Primary or Secondary).   |
| Redundancy State  | The state of the redundancy group (Active, Down, Sync in progress, Firmware mismatch).   |
| Secondary Status  | The status of the secondary controller in the redundancy group (Reachable or Not reachable).   |
| Sync Status   | The synchronization status between the wireless controllers in the redundancy group (In Sync or Not in Sync).  |
| Primary IP Address  | The IP address of the primary controller in the redundancy group.  |
| Secondary IP Address  | The IP address of the secondary controller in the redundancy group.  |
| Virtual IP  | The common IP address that is used by both the primary and secondary controller in the redundancy group and that always is owned by the active controller. |

## View Wireless Controller Usage

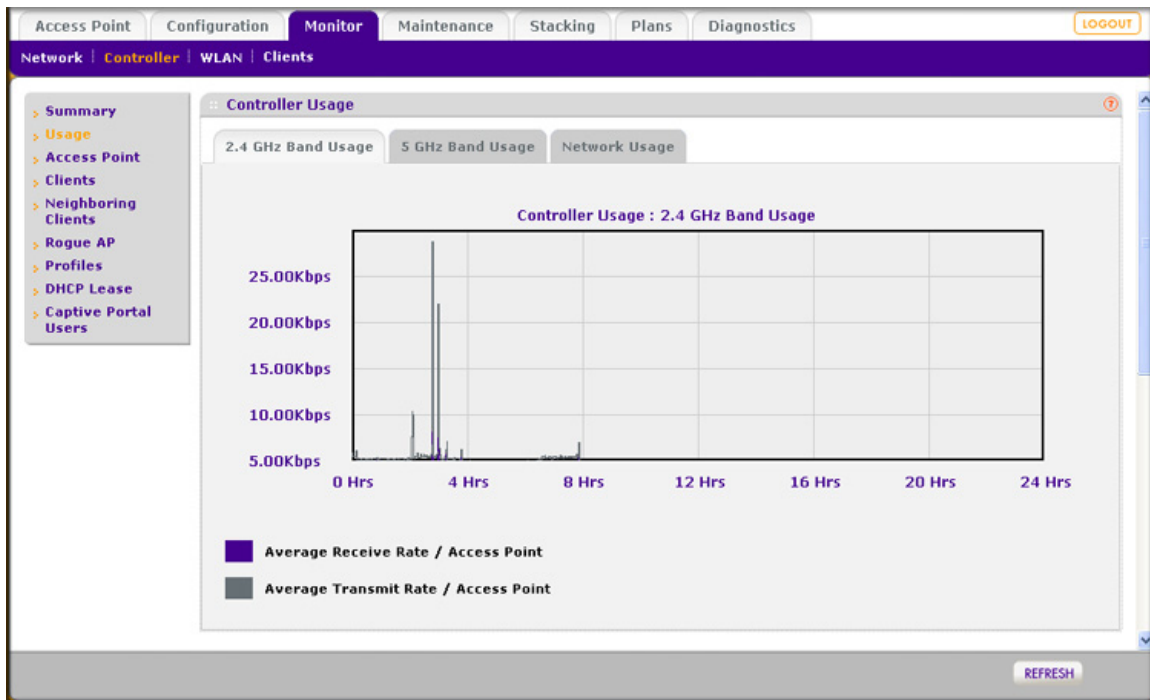


Figure 105.

The Controller Usage screen displays a graphic of the average rate of data traffic that was received and transmitted over the last 24 hours by all access points that are managed by the wireless controller and by the rogue access points that were detected by the wireless controller. Select the type of usage you want to display by clicking one of the following tabs:

- **2.4 GHz Band Usage.** Displays combined 802.11b-, 802.11g-, and 802.11n-mode usage (shown in the previous figure).
- **5 GHz Band Usage.** Displays combined 802.11a- and 802.11n-mode usage.
- **Network Usage.** Displays Ethernet usage.

## View Access Points Managed by the Wireless Controller

Because the Controller Access Point screen is a wide screen, it is shown in the following two figures:

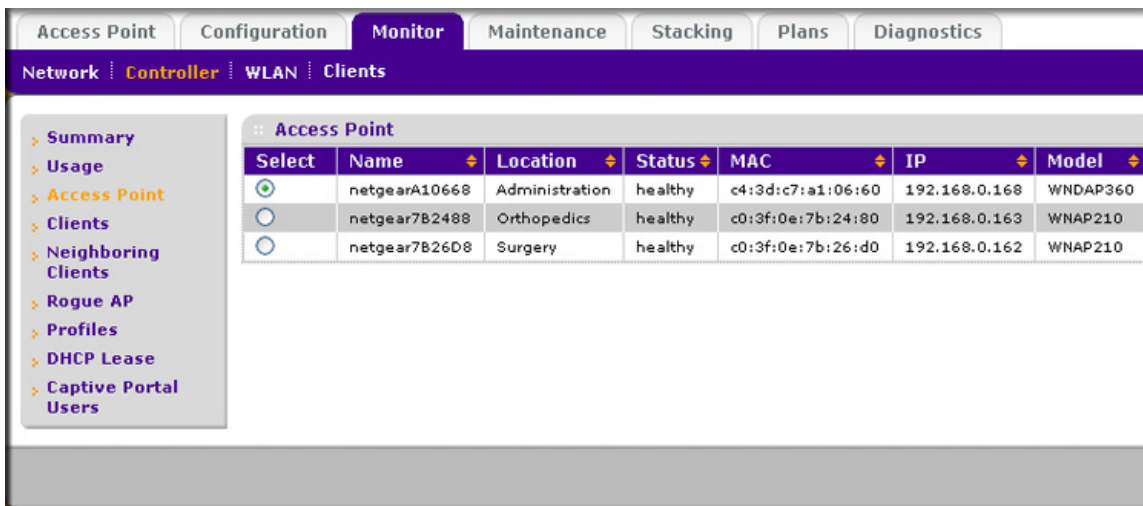


Figure 106. Left side of the Controller Access Point screen

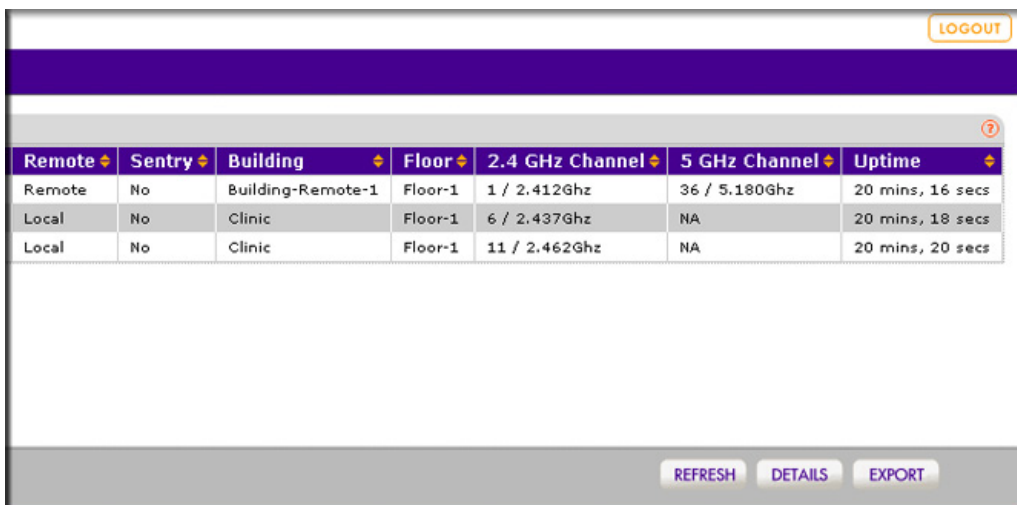


Figure 107. Right side of the Controller Access Point screen

The Controller Access Point screen lets you monitor all access points that are managed by the wireless controller. To view additional access points, click **Next**; to return to the previous access points, click **Previous**. Because this screen is almost identical to the Network Access Point screen, see [Table 41](#) on page 172 for information about the fields.

To export the list of access points, click **Export**.

To see details about an access point, select its corresponding radio button in the Select column of the Access Point table, and then click the **Details** button to display the AP Details pop-up window. Because this screen is identical to the AP Details pop-up window that you can access from the Network Access Point screen, see [Table 42](#) on page 175 for information about the fields. The AP Details pop-up window is shown in [Figure 99](#) on page 174 and [Figure 100](#) on page 174.

## View Clients Managed by the Wireless Controller

| Select                           | MAC               | IP          | Location    | AP-Name       | AP-IP       | Building | Floor   | Bssid             | SSID     | Security |
|----------------------------------|-------------------|-------------|-------------|---------------|-------------|----------|---------|-------------------|----------|----------|
| <input checked="" type="radio"/> | 00:1E:4C:67:33:B2 | 192.168.0.5 | Orthopedics | netgear7B2488 | 192.168.0.3 | Clinic   | Floor-1 | C0:3F:0E:7B:24:82 | NG_11g-2 | Open     |
| <input type="radio"/>            | 00:40:F4:F4:7D:C2 | 192.168.0.6 | Orthopedics | netgear7B2488 | 192.168.0.3 | Clinic   | Floor-1 | C0:3F:0E:7B:24:81 | NG_11g-1 | Open     |

Figure 108.

The Controller Clients screen lets you monitor all clients that are connected to access points that are managed by the wireless controller. To view additional clients, click **Next**; to return to the previous clients, click **Previous**. Because this screen is almost identical to the Network Clients screen, see [Table 43](#) on page 176 for information about the fields.

To see the location of the client on a floor map, select the client's radio button (in the Select column), and then click the **Locate** button.

To export the list of clients, click **Export**.

To see details about a client, select its corresponding radio button in the Select column of the Client table, and then click the **Details** button to display the Client Details pop-up window. Because this screen is identical to the Client Details pop-up window that you can access from the Network Clients screen, see [Table 44](#) on page 177 for information about the fields. The Client Details pop-up window is shown in [Figure 102](#) on page 177.

## View Neighboring Clients Detected by the Wireless Controller

| Locate                           | MAC               | Bssid             | RSSI | Rogue |                          |
|----------------------------------|-------------------|-------------------|------|-------|--------------------------|
| <input checked="" type="radio"/> | 00:26:c6:87:91:32 | ff:ff:ff:ff:ff:ff | 14   | No    | <input type="checkbox"/> |
| <input type="radio"/>            | 4c:44:64:f1:5d:5e | 2b:fd:0a:76:a7:0d | -109 | No    | <input type="checkbox"/> |
| <input type="radio"/>            | 00:13:e8:09:b6:13 | c0:3f:0e:85:c6:71 | -86  | No    | <input type="checkbox"/> |
| <input type="radio"/>            | 00:26:c6:87:6a:6c | ff:ff:ff:ff:ff:ff | 12   | No    | <input type="checkbox"/> |
| <input type="radio"/>            | 00:24:d7:ad:0e:28 | ff:ff:ff:ff:ff:ff | 16   | No    | <input type="checkbox"/> |
| <input type="radio"/>            | 00:26:c6:80:be:0c | c0:3f:0e:85:cc:d0 | -90  | No    | <input type="checkbox"/> |

Figure 109.



The Controller Neighboring Clients screen lets you monitor clients that are attached to known or rogue access points and that were detected by the wireless controller. To view additional neighboring clients, click **Next**; to return to the previous neighboring clients, click **Previous**.

The following table explains the fields of the Neighboring Clients table on the Controller Neighboring Clients screen:

**Table 47. Neighboring clients information**

| Item   | Description   |
|--------|---|
| Locate | The radio button that lets you select the neighboring client to locate it on a floor map.     |
| MAC    | The MAC address of the neighboring client.  |
| BSSID  | The MAC address of the access point's radio to which the neighboring client is connected.     |
| RSSI   | The received signal strength indicator (RSSI) of the neighboring client.                      |
| Rogue  | Shows whether or not (Yes or No) the neighboring client is connected to a rogue access point. |

To see the location of the neighboring client on a floor map, select the neighboring client's radio button (in the Locate column), and then click the **Locate** button.

To disconnect neighboring clients, select one or more check boxes that correspond to the neighboring clients, or select all neighboring clients in the Neighboring Clients table by selecting the check box at the top right of the table, and then click **Disconnect**.

To export the list of neighboring clients, click **Export**.

## View Rogue Access Points Detected by the Wireless Controller

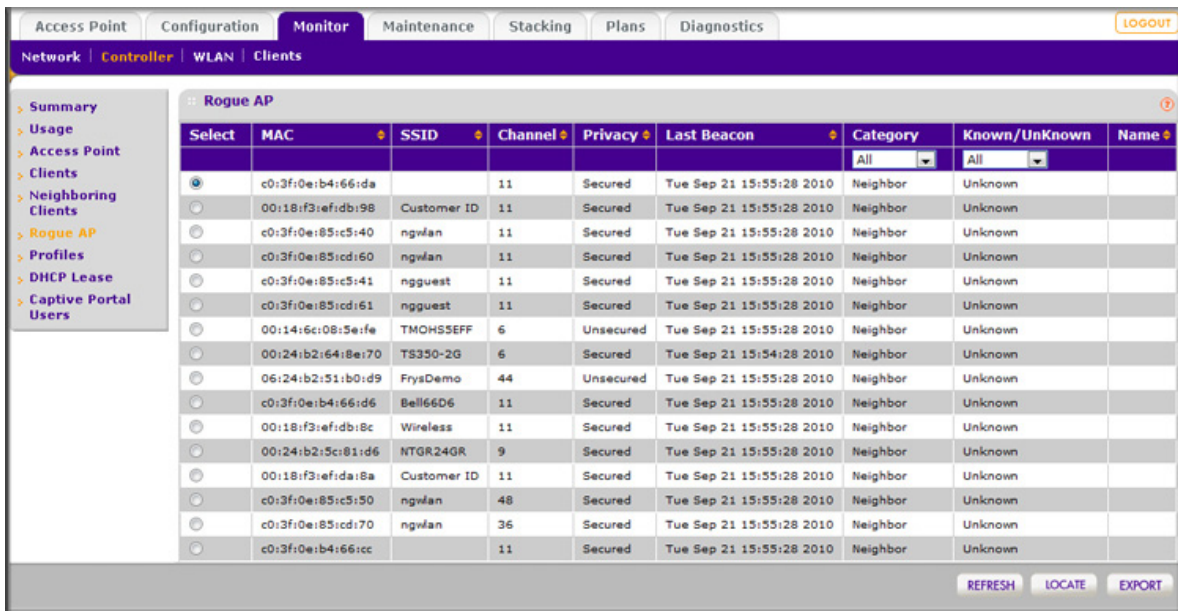


Figure 110.

The Controller Rogue AP screen lets you monitor all rogue access points that were detected by the wireless controller. To view additional rogue access points, click **Next**; to return to the previous rogue access points, click **Previous**.

The following table explains the fields of the Rogue AP table on the Controller Rogue AP screen:

**Table 48. Controller rogue AP information**

| Item          | Description   |
|---------------|---|
| Select        | The radio button that lets you select the rogue access point to locate it on a floor map.   |
| MAC           | The MAC address of the rogue access point.  |
| SSID          | The wireless network SSID that the rogue access point is using.   |
| Channel       | The channel that the rogue access point is using.   |
| Privacy       | The security of the rogue access point (Secured or Unsecured).  |
| Last Beacon   | The last beacon that the rogue access point transmitted.  |
| Category      | The category that the rogue access point belongs to. From the drop-down list, you can select to display <b>Neighbor</b> , <b>Rogue</b> , or <b>All</b> access points. |
| Known/Unknown | The status of the rogue access point. From the drop-down list, you can select to display <b>Known</b> or <b>Unknown</b> access points.                                |
| Name          | The name of the rogue access point, if you assigned a name.   |

To see the location of the rogue access point on a floor map, select the access point's radio button (in the Select column), and then click the **Locate** button.

To export the list of rogue access points, click **Export**.

## View Security Profiles Managed by the Wireless Controller

The screenshot shows the 'Monitor' tab selected in the top navigation bar. The left sidebar contains a tree view with 'Profiles' highlighted. The main content area displays a table of security profiles. The table has the following data:

| SSID     | Security | Radio Mode    | Status   | Group Name |
|----------|----------|---------------|----------|------------|
| NG_11g   | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-1 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-2 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-3 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-4 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-5 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11g-7 | Open     | 802.11b/bg/ng | Active   | basic      |
| NG_11a   | Open     | 802.11a/na    | Active   | basic      |
| NG_11a-1 | Open     | 802.11a/na    | Active   | basic      |
| NG_11g-0 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | Group-1    |
| NG_11g-1 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | Group-1    |
| NG_11a-0 | Open     | 802.11a/na    | Inactive | Group-1    |
| NG_11g-0 | Open     | 802.11b/bg/ng | Inactive | Group-2    |
| NG_11a-0 | Open     | 802.11a/na    | Inactive | Group-2    |
| NG_11g-0 | Open     | 802.11b/bg/ng | Inactive | Group-3    |
| NG_11a-0 | Open     | 802.11a/na    | Inactive | Group-3    |

At the bottom of the table, there are 'PREVIOUS' and 'NEXT' links. At the bottom of the page, there are 'REFRESH' and 'EXPORT' buttons.

Figure 111.

The Controller Profiles screen lets you monitor all security profiles on the access points that are managed by the wireless controller. To view additional profiles, click **Next**; to return to the previous profiles, click **Previous**.

Because this screen is almost identical to the Network Profiles screen, see [Table 45](#) on page 179 for information about the fields.

To export the list of profiles, click **Export**.

## View DHCP Leases Provided by the Wireless Controller

| Host Name                 | IP           | End Time | End Date   | MAC               | VLAN       |
|---------------------------|--------------|----------|------------|-------------------|------------|
| Unknown                   | 192.168.0.29 | 09:55:17 | 2010/09/22 | 00:26:f2:9a:1b:a0 | Management |
| VWC-0004-MAC-000201040000 | 192.168.0.20 | 17:43:02 | 2010/09/21 | 00:02:01:04:00:00 | Management |
| VWC-0002-MAC-000201020000 | 192.168.0.21 | 17:43:02 | 2010/09/21 | 00:02:01:02:00:00 | Management |
| Unknown                   | 192.168.0.30 | 11:37:02 | 2010/09/22 | 00:26:f2:8b:2d:80 | Management |
| VWC-0001-MAC-000201010000 | 192.168.0.22 | 17:43:02 | 2010/09/21 | 00:02:01:01:00:00 | Management |
| VWC-0003-MAC-000201030000 | 192.168.0.23 | 17:43:02 | 2010/09/21 | 00:02:01:03:00:00 | Management |
| VWC-0005-MAC-000201050000 | 192.168.0.24 | 17:42:52 | 2010/09/21 | 00:02:01:05:00:00 | Management |
| VWC-0001-MAC-000101060000 | 192.168.0.25 | 17:43:02 | 2010/09/21 | 00:01:01:06:00:00 | Management |
| VWC-0001-MAC-001f33e98044 | 192.168.0.26 | 14:25:26 | 2010/09/22 | 00:1f:33:e9:80:44 | Management |
| VWC-0002-MAC-001f33e9804b | 192.168.0.27 | 14:25:26 | 2010/09/22 | 00:1f:33:e9:80:4b | Management |
| VWC-0001-MAC-000101010000 | 192.168.0.28 | 14:25:27 | 2010/09/22 | 00:01:01:01:00:00 | Management |

Figure 112.

The DHCP Leases screen displays the current DHCP clients that have been allocated IP addresses by the DHCP server on the wireless controller. To view additional DHCP leases, click **Next**; to return to the previous DHCP leases, click **Previous**.

The following table explains the fields of the DHCP Leases table on the Controller DHCP Leases screen:

Table 49. Controller DHCP lease information

| Item      | Description   |
|-----------|---|
| Host Name | The host name of the DHCP client.                                   |
| IP        | The IP address that is allocated to the DHCP client.                |
| End Time  | The DHCP lease end time for the DHCP client.                        |
| End Date  | The DHCP lease end date for the DHCP client.                        |
| MAC       | The MAC address of the DHCP client.                                 |
| VLAN      | The VLAN that the DHCP server and DHCP client are using to connect. |

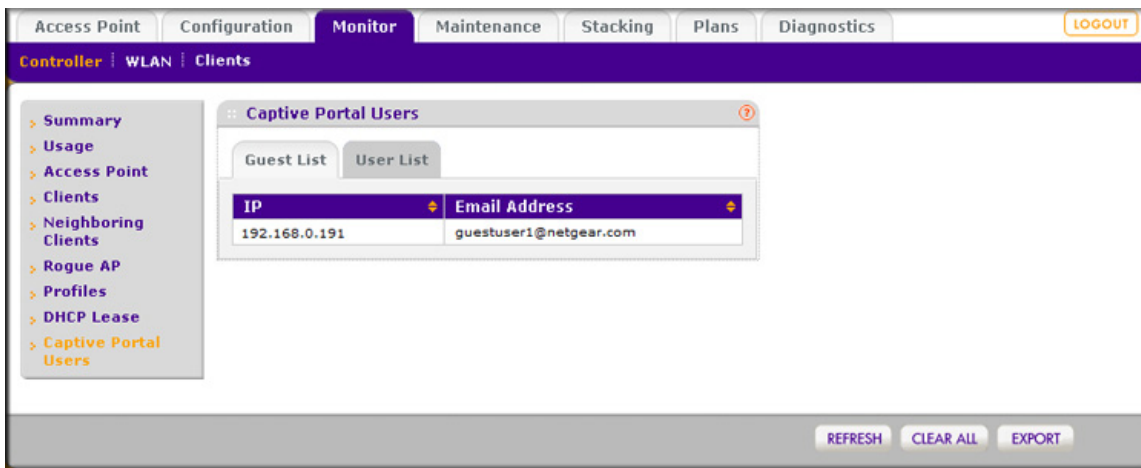
To export the list of DHCP leases, click **Export**.

## View Captive Portal Guests and Users Managed by the Wireless Controller

The Controller Captive Portal Users screen displays the current guests and users that are logged in to a captive portal on the access points that are managed by the wireless controller.

➤ **To view the guest list:**

Click the **Guest List** tab. The associated Guest List screen displays:



**Figure 113.**

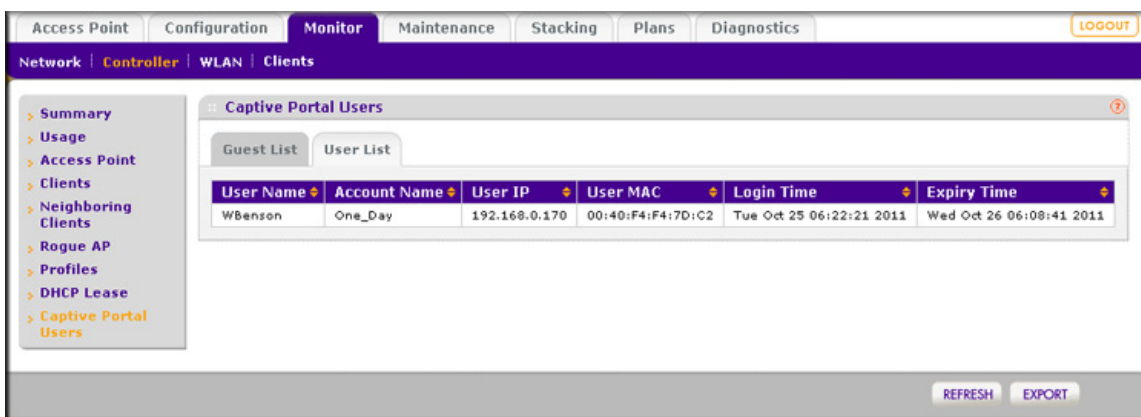
The Guest List table shows the IP addresses and email addresses of the logged-in guests. To view additional guests, click **Next**; to return to the previous guests, click **Previous**.

To clear all user information from the screen, click **Clear All**.

To export the list of captive portal guests, click **Export**.

➤ **To view the captive portal user list:**

Click the **User List** tab. The associated User List screen displays:



**Figure 114.**

The Guest List table shows information about logged-in captive portal users that are required to log in with a user name and password. To view additional users, click **Next**; to return to the previous users, click **Previous**.

The following table explains the fields of the User List table:

**Table 50. Captive portal user information**

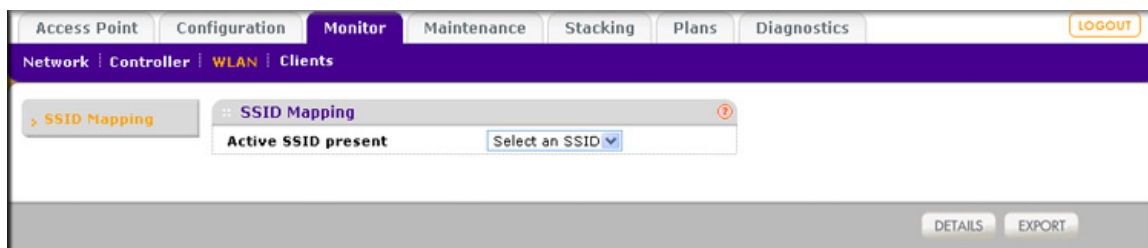
| Item         | Description   |
|--------------|---|
| User Name    | The login name of the user.                                     |
| Account Name | The account name, if any, that is associated with the user.     |
| User IP      | The IP address of the user.                                     |
| User MAC     | The MAC address of the device with which the user is logged in. |
| Login Time   | The time that the user has logged in.                           |
| Expiry Time  | The time when the login access will expire.                     |

To export the list of captive portal users, click **Export**.

## Monitor the SSIDs

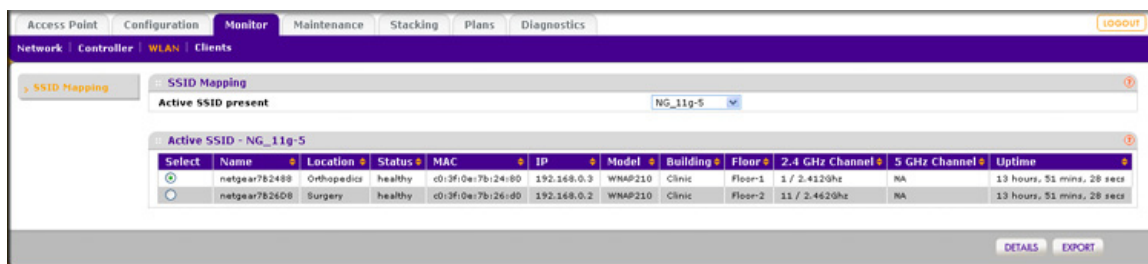
➤ To monitor the active SSIDs in the network:

1. Select **Monitor > WLAN**. The SSID Mapping screen displays.



**Figure 115.**

2. From the Active SSID present drop-down list, select an SSID. The Active SSID table for the selected SSID displays.



**Figure 116.**

The Active SSID table on the WLAN SSID Mapping screen lets you monitor all access points that function in an SSID. To view additional access points, click **Next**; to return to the previous access points, click **Previous**.

Because this table is almost identical to the Access Point table on the Network Access Point screen, see [Table 41](#) on page 172 for information about the fields.

To export the list of access points, click **Export**.

To see details about an access point, select its corresponding radio button in the Select column of the Access Point table, and then click the **Details** button to display the AP Details pop-up window. Because this screen is identical to the AP Details pop-up window that you can access from the Network Access Point screen, see [Table 42](#) on page 175 for information about the fields. The AP Details pop-up window is shown in [Figure 99](#) on page 174 and [Figure 100](#) on page 174.

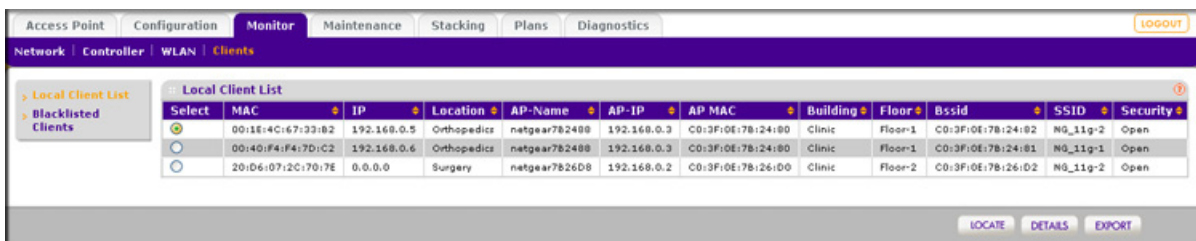
## Monitor the Clients

### ➤ To monitor the clients in the network:

1. Select **Monitor > Clients**.
2. Select one of the following submenu links to display a network monitoring screen:
  - **Local Clients List**
  - **Blacklisted Clients**

These screens are explained in the following sections.

## View Local Clients



| Select                | MAC               | IP          | Location    | AP-Name       | AP-IP       | AP MAC            | Building | Floor   | Bssid             | SSID     | Security |
|-----------------------|-------------------|-------------|-------------|---------------|-------------|-------------------|----------|---------|-------------------|----------|----------|
| <input type="radio"/> | 00:1E:4C:67:33:B2 | 192.168.0.5 | Orthopedics | netgear782488 | 192.168.0.3 | C0:3F:0E:78:24:80 | Clinic   | Floor-1 | C0:3F:0E:78:24:82 | NG_11g-2 | Open     |
| <input type="radio"/> | 00:40:F4:F4:7D:C2 | 192.168.0.6 | Orthopedics | netgear782488 | 192.168.0.3 | C0:3F:0E:78:24:80 | Clinic   | Floor-1 | C0:3F:0E:78:24:81 | NG_11g-1 | Open     |
| <input type="radio"/> | 20:D6:07:2C:70:7E | 0.0.0.0     | Surgery     | netgear7826D8 | 192.168.0.2 | C0:3F:0E:78:26:D0 | Clinic   | Floor-2 | C0:3F:0E:78:26:D2 | NG_11g-2 | Open     |

**Figure 117.**

The Local Client List screen lets you monitor all clients that were locally authenticated and that are connected to access points managed by the wireless controller. To view additional clients, click **Next**; to return to the previous clients, click **Previous**. Because this screen is almost identical to the Network Clients screen, see [Table 43](#) on page 176 for information about the fields.

---

**Note:** The Local Client List screen shows *all* clients in the network (that is, all clients managed by all wireless controllers in the network), whereas the Controller Clients screen (see [Figure 108](#) on page 184) shows only the clients that are managed by a single wireless controller.

---

To see the location of the client on a floor map, select the client's radio button (in the Select column), and then click the **Locate** button.

To export the list of clients, click **Export**.

To see details about a client, select its corresponding radio button in the Select column of the Client table, and then click the **Details** button to display the Client Details pop-up window. Because this screen is identical to the Client Details pop-up window that you can access from the Network Clients screen, see [Table 44](#) on page 177 for information about the fields. The Client Details pop-up window is shown in [Figure 102](#) on page 177.

## View Blacklisted Clients

| Select                | MAC               | TYPE                  | AP-Name    | AP-IP        | SSID       | RSSI | Count | Last Seen                |
|-----------------------|-------------------|-----------------------|------------|--------------|------------|------|-------|--------------------------|
| <input type="radio"/> | 00:02:01:02:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49   | 2     | Mon Sep 20 17:55:25 2010 |
| <input type="radio"/> | 00:02:01:04:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49   | 3     | Mon Sep 20 18:02:25 2010 |
| <input type="radio"/> | 00:02:01:01:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49   | 2     | Mon Sep 20 18:02:10 2010 |

**Figure 118.**

The Blacklisted Clients screen lets you monitor all clients that attempted to connect but were denied access because they provided incorrect authentication credentials or their MAC address is blocked in a MAC ACL. To view additional clients, click **Next**; to return to the previous clients, click **Previous**.

The following table explains the fields of the Blacklisted Clients table on the Blacklisted Clients screen:

**Table 51. Blacklisted clients information**

| Item      | Description  |
|-----------|--|
| Select    | The radio button that lets you select the blacklisted client to locate it on a floor map.  |
| MAC       | The MAC address of the blacklisted client.   |
| Type      | The type of offense such as failed authentication (Authentication Failed) or denied access because of a blocked MAC address (Denied Client). |
| AP-Name   | The name of the access point to which the blacklisted client attempted to connect.   |
| AP-IP     | The IP address of the access point to which the blacklisted client attempted to connect.   |
| RSSI      | The received signal strength indicator (RSSI) of the blacklisted client.   |
| SSID      | The wireless network SSID that the blacklisted client used to attempt to connect to the access point.  |
| Count     | The number of times the client's authentication failed.  |
| Last Seen | The last time that the blacklisted client attempted to log in.   |



To see the location of the blacklisted client on a floor map, select the client's radio button (in the Select column), and then click the **Locate** button.

To export the list of blacklisted clients, click **Export**.

This chapter includes the following sections:

- *Troubleshoot Basic Functioning*
- *Troubleshoot the Web Management Interface*
- *Troubleshoot a TCP/IP Network Using the Ping Utility*
- *Use the Factory Default Button to Restore Default Settings*
- *Problems with Date and Time*
- *Problems with Access Points*
- *Use the Diagnostic Tools on the Wireless Controller*

## Troubleshoot Basic Functioning

After you turn on power to the wireless controller, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
  - a. The Test LED is no longer lit.
  - b. The left LAN port LEDs are lit for any local ports that are connected.

If a port's left LED is lit, a link has been established to the connected device. If a port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is amber. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see to the appropriate following section.

### Power LED Not On

If the Power and other LEDs are off when your wireless controller is turned on, make sure that the power cord is correctly connected to your wireless controller and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR technical support.

## Test LED Never Turns Off

When the wireless controller is powered on, the Test LED turns on for approximately 2 minutes and then turns off when the wireless controller has completed its initialization. If the Test LED remains on, there is a fault within the wireless controller.

If the Test LED is still on more than several minutes after power-up:

- Turn the power off, and then turn it on again to see if the wireless controller recovers.
- Reset the wireless controller's configuration to factory default settings. Doing so sets the wireless controller's IP address to **192.168.0.250**. This procedure is explained in [Reboot or Reset the Wireless Controller](#) on page 139.

If the error persists, you might have a hardware problem and should contact NETGEAR technical support.

## LAN Port LEDs Not On

If the LAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the wireless controller and at the hub, switch, or router.
- Make sure that power is turned on to the connected hub, switch, or router.
- Be sure that you are using the correct cables:

## Troubleshoot the Web Management Interface

If you are unable to access the wireless controller's web management interface from a PC on your local network, try to isolate the problem. It is most likely one of the following:

### Ethernet Cabling

Check the Ethernet connection between the PC and the wireless controller as described in the previous section (see [LAN Port LEDs Not On](#)).

### IP Address Configuration

- Make sure your PC's IP address is on the same subnet as the wireless controller. If you are using the recommended addressing scheme, make sure your PC has a static IP address of 192.168.0.210 and a subnet of 255.255.255.0.

---

**Note:** If your PC's IP address is shown as 169.254.x.x: Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the wireless controller and reboot your PC.

---

- If the wireless controller's IP address has been changed and you do not know the current IP address, reset the wireless controller's configuration to factory default settings. This sets the wireless controller's IP address to 192.168.0.250. This procedure is explained in [Reboot or Reset the Wireless Controller](#) on page 139.

---

**Note:** If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the wireless controller and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the wireless controller's LAN interface address.

---

## Internet Browser

- Make sure that you are using the http://address login rather than the https://address login.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

If the wireless controller does not save changes you have made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another tab or screen, or your changes are lost.
- Click the **Refresh** or **Reload** button in your web browser. The changes might have occurred, but the web browser might be caching the old configuration.

After you have upgraded the firmware, if the browser does not display the latest features of the web management interface, clear the browser's cache, and refresh the screen.

## Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshooting a TCP/IP network by using the ping utility in your computer.

### Test the LAN Path to Your Wireless Controller

You can ping the wireless controller from your PC to verify that the LAN path to your wireless controller is set up correctly.

➤ **To ping the wireless controller from a PC running Windows 95 or later:**

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type `ping` followed by the IP address of the wireless controller, as in this example:

```
ping 192.168.0.250
```

3. Click **OK**.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure that the LAN LED is on. If the LED is off, follow the instructions in [LAN Port LEDs Not On](#) on page 195.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your computer and wireless controller.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  - Verify that the IP address for your wireless controller and your computer are correct and that the addresses are on the same subnet.

## Use the Factory Default Button to Restore Default Settings

If you can access the wireless controller, you can use the Reboot/Reset Controllers screen (select **Maintenance > Backup/Restore**) to perform a soft or hard reset (see [Reboot or Reset the Wireless Controller](#) on page 139).

If you can no longer access the wireless controller, press the **Factory Default** button on the rear panel (see [Rear Panel Features](#) on page 13) to restore the factory default settings.

➤ **To clear all data and restore the factory default values:**

1. Press and hold the **Factory Default** button for about 8 seconds until the Test LED turns on and begins to blink.
2. Release the **Factory Default** button. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

---

**Note:** After restoring the factory default configuration, the wireless controller's default LAN IP address is 192.168.0.250, the default login user name is admin, and the default login password is password.

---

## Problems with Date and Time

The Time Settings screen displays the current date and time of day (see [Time Management](#) on page 64). The wireless controller uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

When the date shown is January 1, 2000, the wireless controller has not yet successfully reached a network time server. Verify that the wireless controller can reach the Internet. If you have just completed configuring the wireless controller, wait at least 5 minutes and check the date and time again.

## Problems with Access Points

### Discovery Problems

If the wireless controller does not discover any or all access points, check the following:

**For all access points (local and remote):**

- Make sure that the wireless controller is connected to the LAN (see [LAN Port LEDs Not On](#) on page 195).

- Make sure that you have entered the correct IP range if the access points function in different VLANs, are behind an IP subnet, or are already installed and working in standalone mode (see [Access Point Discovery and Discovery Guidelines](#) on page 51).
- Verify that access points that are already installed and working in standalone mode have SSH and SNMP enabled (which is the default setting).
- Make sure that UDP port number 7890 is unblocked in the firewall.
- With the exception of access points in factory default state that are in the same Layer 2 network, if more than one access point has the same IP address, then only one of them is discovered at a time. You have to add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with that IP address.
- Make sure that the access points run at least their initial firmware release or a newer version. For firmware requirements, see [NETGEAR ProSafe Access Points](#) on page 15.

#### For local access points that are installed across a Layer 3 network:

Make sure that either one of the following options is enabled:

- Multicast routing for IP address 254.0.100.250 between the wireless controller and the access point.
- DHCP option 43 (vendor-specific information) on the DHCP server. (Specifying a DHCP server on the wireless controller automatically enables DHCP option 43 with its own IP address.)

#### For remote access points:

- Make sure that DHCP option 43 (vendor-specific information) is enabled on the DHCP server. (Specifying a DHCP server on the wireless controller automatically enables DHCP option 43 with its own IP address.)
- Make sure that the following ports are unblocked in the firewall:
  - TCP port 22.
  - UDP ports 69, 123, 138, 161, and 6650. (These ports are in addition to port 7890).
- Make sure that access points behind a NAT router have been converted to managed access points before they are installed behind the NAT router.

## Connection Problems

When an access point is converted from standalone-AP mode to managed-AP mode, its static IP address is changed to an IP address that is issued by the DHCP server, either one in the network or one that is configured on the wireless controller. This occurs to ensure that each managed access point has a unique IP address.

If there is no DHCP server or if the access point cannot reach the DHCP server, the access point remains in the Connecting state, attempting to obtain an IP address. If there is no DHCP server in the network, configure one on the wireless controller (see [Manage the DHCP](#)

[Server](#) on page 67). When a DHCP server becomes available, the access point can transition from the Connecting state to the Connected state.

## Network Performance and Rogue Access Point Detection

When rogue access point detection is enabled, access points intermittently go off channel for short periods, which can affect network performance. If security concerns are more important than network performance, you can temporarily select a high or aggressive rogue access point detection interval. If network performance is more important than security concerns, select a low or medium rogue access point detection interval, in which case security is addressed but network performance is not compromised. Under normal circumstances, NETGEAR recommends a low rogue access point detection interval.

## Use the Diagnostic Tools on the Wireless Controller

As part of the diagnostics functions on the wireless controller, you can ping a managed access point from the wireless controller or trace its route from the wireless controller.

### ➤ To ping an access point:

1. Select **Diagnostics > Ping**. The Ping screen displays.

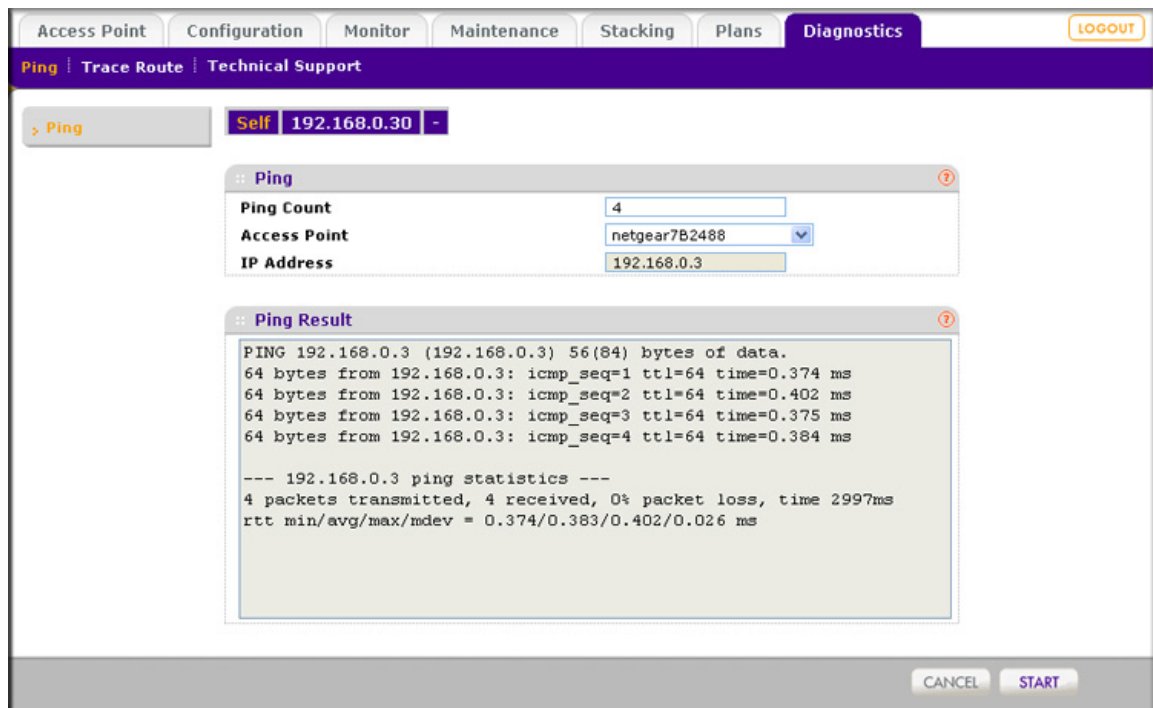


Figure 119.

2. In the Ping Count field, enter the number of ping packets to be sent. (The default number is 10.)



3. From the Access Point drop-down list, select the access point to be pinged. After you have made your selection, the IP address of the access point displays in the IP Address field.
4. Click **Start**. The results are shown in the Ping Result field.

➤ **To trace a route to an access point:**

1. Select **Diagnostics > Trace Route**. The Trace Route screen displays (see the following figure).
2. From the Access Point drop-down list, select the access point for which you want to trace the route. After you have made your selection, the IP address of the access point displays in the IP Address field.
3. Click **Start**. The results are shown in the TraceRoute Result field.

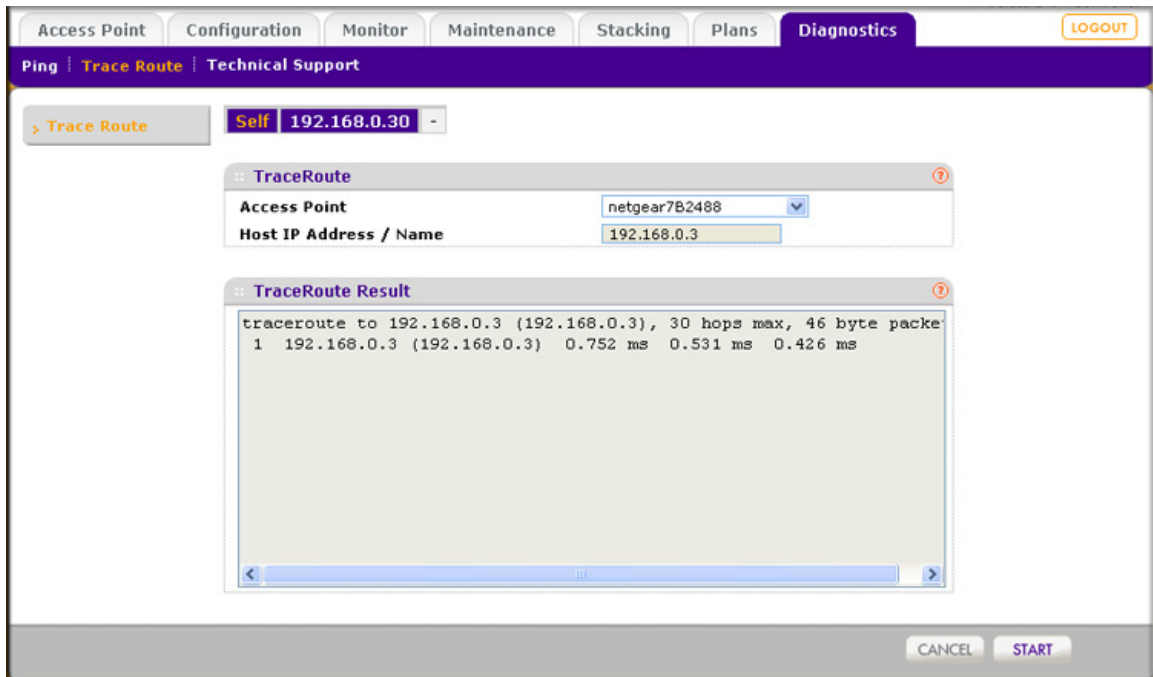


Figure 120.

# Factory Default Settings and Technical Specifications



You can restore the wireless controller to its factory default settings on the Reboot/Reset Controllers screen (see [Reboot or Reset the Wireless Controller](#) on page 139) or by using the Factory Defaults button on the rear panel (see [Use the Factory Default Button to Restore Default Settings](#) on page 198). The wireless controller will return to the factory configuration settings shown in the following table:

**Table 52. Factory default settings**

| Feature |  | Default Setting                                |
|---------|--|--|
| Login   | User login URL                               | http:192.168.0.250                             |
|         | User name (case-sensitive)                   | admin  |
|         | Login password (case-sensitive)              | password                                       |
| LAN     | LAN IP                                       | 192.168.0.250                                  |
|         | Subnet mask                                  | 255.255.255.0                                  |
|         | Default gateway                              | 192.168.0.1                                    |
|         | Time zone                                    | PST for North America, GMT for other locations |
|         | Time zone adjusted for daylight savings time | Enabled  |
|         | SNMP   | Disabled.                                      |

The following table lists the technical and physical specifications.

**Table 53. Technical and physical specifications**

| Feature                   | Default Setting  |
|---------------------------|--|
| Electrical specifications | 100-240V, AC/50-60 Hz, universal input<br>DC 5V/8A (internal power supply) |
| Dimensions (W x H x D)    | cm: 26.1 x 4.3 x 44<br>in.: 10.3 x 1.7 x 17.3                              |
| Weight                    | kg: 2.912<br>lb: 6.4   |

**Table 53. Technical and physical specifications (continued)**

| Feature                             | Default Setting   |
|-------------------------------------|---|
| Operating temperatures and humidity | 0° to 45° C (32° to 113° F)<br>90% maximum relative humidity  |
| Storage temperatures and humidity   | -20° to 70° C (-4° to 58° F)<br>95% maximum relative humidity |
| Major regulatory compliance         | FCC Class A, CE, WEEE, RoHS                                   |

---

**Note:** For more information, see the *ProSafe 20-AP Wireless Controller WC7520* data sheet at [http://support.netgear.com/app/products/model/a\\_id/13060](http://support.netgear.com/app/products/model/a_id/13060).

---

The following table lists the password requirements.

**Table 54. Password requirements**

| Web management interface path  | User type or data encryption  | Restrictions                         |  | Section in this manual   |   |
|--|---|--------------------------------------|--|--|---|
|  |   | Allowed characters                   | Length   |  |   |
| Maintenance > User Management > Management tab   | <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Read Only</li> <li>• Guest Provisioning</li> <li>• License Management Only</li> </ul> | Alphanumerics and special characters | Up to 31   | See <a href="#">Manage Users, Accounts, and Passwords</a> on page 128. |   |
| Maintenance > User Management > Captive Portal tab   | Captive portal user   | Alphanumerics and special characters | Up to 31   |  |   |
| Maintenance > User Management > WiFi Clients tab   | Wi-Fi user  | Alphanumerics only                   | Up to 31   |  |   |
| Basic Profile:<br>1. Configuration > Profile > Basic > Radio.<br>2. Select a profile.<br>3. Make a selection from the Network Authentication drop-down list. | Shared Key  | 64-bit WEP                           | Hexadecimal  | 10 fixed   | See <a href="#">Configure Security Profiles for the Basic Profile Group</a> on page 77. |
|  |   | 128-bit WEP                          | Hexadecimal  | 26 fixed   |   |
|  |   | 152-bit WEP                          | Hexadecimal  | 32 fixed   |   |
|  | WPA-PSK   | TKIP                                 | Alphanumerics and special characters, excluding quotes | Up to 63   |   |
|  |   | TKIP + AES                           |  |  |   |
|  | WPA2-PSK  | AES                                  |  |  |   |
|  |   | TKIP + AES                           |  |  |   |
| WPA-PSK & WPA2-PSK   | TKIP + AES  |                                      |  |  |   |

**Table 54. Password requirements (continued)**

| Web management interface path  | User type or data encryption | Restrictions       |  | Section in this manual |   |
|--|------------------------------|--------------------|--|------------------------|---|
|  |                              | Allowed characters | Length   |                        |   |
| Advanced Profile:<br>1. Configuration > Profile > Advanced > Radio.<br>2. Select a group.<br>3. Click Edit.<br>4. Select a profile.<br>5. Make a selection from the Network Authentication drop-down list. | Shared Key                   | 64-bit WEP         | Hexadecimal  | 10 fixed               | See <a href="#">Configure Security Profiles for Advanced Profile Groups</a> on page 84.         |
|  |                              | 128-bit WEP        | Hexadecimal  | 26 fixed               |   |
|  |                              | 152-bit WEP        | Hexadecimal  | 32 fixed               |   |
|  | WPA-PSK                      | TKIP               | Alphanumerics and special characters, excluding quotes | Up to 63               |   |
|  |                              | TKIP + AES         |  |                        |   |
|  | WPA2-PSK                     | AES                |  |                        |   |
|  |                              | TKIP + AES         |  |                        |   |
| WPA-PSK & WPA2-PSK   | TKIP + AES                   |                    |  |                        |   |
| Configuration > Security > Authentication Server   | External RADIUS Server       | Shared Secret      | Alphanumerics and special characters                   | Up to 127              | See <a href="#">Manage Authentication Servers and Authentication Server Groups</a> on page 122. |
|  | External LDAP Server         | Domain Admin User  | Alphanumerics and special characters                   | Up to 32               |   |

# Notification of Compliance

---



## NETGEAR Wired Products

### **Regulatory Compliance Information**

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

### **FCC Requirements for Operation in the United States**

#### **FCC Information to User**

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

#### **FCC Guidelines for Human Exposure**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

#### **FCC Declaration Of Conformity**

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSafe 20-AP Wireless Controller WC7520 complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

### **FCC Radio Frequency Interference Warnings & Instructions**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

### **Canadian Department of Communications Radio Interference Regulations**

This digital apparatus, ProSafe 20-AP Wireless Controller WC7520, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

### **European Union**

The ProSafe 20-AP Wireless Controller WC7520 complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

### **GPL License Agreement**

GPL may be included in this product; to view the GPL license agreement go to <ftp://downloads.netgear.com/files/GPLnotice.pdf>.

For GNU General Public License (GPL) related information, please visit [http://support.netgear.com/app/answers/detail/a\\_id/2649](http://support.netgear.com/app/answers/detail/a_id/2649).

# Index

## Numerics

- 2.4 GHz and 5 GHz channels **100**
- 802.11 wireless modes **94**
- 802.1Q VLAN header **28, 67**

## A

- AC power socket **14**
- access point groups
  - assignment **87**
  - basic (or default) **23**
  - description **23**
  - MAC authentication **120**
  - QoS **105**
  - radio, turning on and off **92**
  - rate limiting **110**
  - RF management **104**
  - security profiles **75**
  - wireless settings **96**
- access points
  - adding **57**
  - antennas, configuring **61**
  - channel allocation
    - automatic **99–101**
    - manual **96, 98**
  - DHCP client, disabling **61**
  - discovery **51**
  - discovery results **56**
  - dual-band **15, 16, 23, 74, 109**
  - editing settings **60**
  - factory default state **54**
  - firmware, minimum version **15**
  - floor and building settings **62**
  - IP addresses **61**
  - IP subnet **55, 56**
  - known and unknown **116**
  - local **51, 57–59**
  - managed status **59**
  - models, supported **15**
  - pinging **200**
  - rebooting **141**
  - remote **52, 57–59**
  - rogue
    - detecting, managing, and mitigating **113**
    - viewing in the network **170**
    - viewing on the managed access point **175**
    - viewing on the wireless controller **186**
  - sentry mode **61**
  - standalone mode **54, 62**
  - supported models **15**
  - tracing a route **201**
  - troubleshooting **198**
  - TX power, controlling
    - automatically **103**
    - manually **96, 98**
  - viewing
    - in the network **172**
    - on the wireless controller **183**
    - security profiles **175**
    - statistics **175**
  - VLAN settings **61**
- access, remote **142**
- accounts, captive portal **128**
- active SSIDs, viewing **191**
- active voice calls, preventing channel allocation **101**
- Advanced Encryption Standard (AES) **82**
- advanced settings, description **22, 74**
- AES (Advanced Encryption Standard) **82**
- Aggregated Mac Protocol Data Unit (AMPDU) **95**
- aggregation length **95**
- AIFS (Arbitration Inter-Frame Space) **107**
- alarms
  - settings **72**
  - viewing in the network **169**
  - viewing on the wireless controller **180**
- alerts, viewing **146**
- AMPDU (Aggregated Mac Protocol Data Unit) **95**
- antenna **61**
- Arbitration Inter-Frame Space (AIFS) **107**
- authentication
  - certificates **70**
  - external
    - MAC authentication **79, 118**
    - RADIUS and LDAP servers **82, 122–124, 128**
  - internal **124**
  - methods supported **29**
  - servers **122**
- automatic channel allocation **102**
- automatic transmission power **102**



## B

- background QoS queue [105](#)
- backing up the configuration [135](#)
- basic access point group [23](#)
- basic service set identifier (BSSID) [113](#)
- basic settings, description [22](#), [74](#)
- beacon interval [95](#)
- best effort QoS queue [105](#)
- blacklisted clients, viewing [192](#)
- bottom label [14](#)
- broadcasting SSID [78](#)
- BSSID (basic service set identifier) [113](#)
- buildings, planning [44](#)

## C

- cabling, troubleshooting [195](#)
- captive portal accounts and users, viewing [188](#)
- captive portal, configuring [126](#)
- certificates, authentication [70](#)
- channel allocation
  - automatic [99–101](#)
  - manual [96](#), [98](#)
- channel width [94](#)
- client separation [79](#)
- client VLANs [29](#), [32](#)
- clients, DHCP [61](#)
- clients, viewing
  - blacklisted in the network [192](#)
  - in the network [169](#), [176](#), [191](#)
  - neighboring in the network [185](#)
  - on the access point [175](#)
  - on the wireless controller [180](#), [184](#)
- clients, wireless, maximum number [108](#)
- community names, SNMP [143](#)
- compliance [205](#)
- configuration
  - backing up and restoring [135](#)
  - upgrading [137](#)
- connection problems, troubleshooting [199](#)
- connectivity test [27](#)
- console port [13](#)
- contents, package [11](#)
- controller selection, stacking [157](#)
- country and region of operation [64](#)
- coverage area [47](#)
- coverage hole detection [104](#)
- customer information, licenses [152](#)
- CwMin and CwMax (Minimum or Maximum Contention Window) [107](#)

## D

- data encryption
  - configuring [79](#)
  - supported methods [29](#)
- data rate [94](#)
- data sheet [203](#)
- date, troubleshooting [198](#)
- default access point group [23](#)
- default settings [13](#), [198](#), [202](#)
- Delivery Traffic Indication Message (DTIM) interval [95](#)
- detecting rogue access points [114](#)
- DHCP client, access points [61](#)
- DHCP leases, viewing [188](#)
- DHCP option 43 [52](#)
- DHCP server
  - description [29](#)
  - settings [68](#)
- diagnostic tools [200](#)
- discovering access points [51](#)
- discovery problems, troubleshooting [198](#)
- DNS servers [66](#)
- DTIM (Delivery Traffic Indication Message) interval [95](#)
- dual-band access points [15](#), [16](#), [23](#), [74](#), [109](#)

## E

- EAP (Extensible Authentication Protocol) [132](#)
- electrical specifications [202](#)
- email notification server [72](#)
- encryption, methods supported [29](#)
- end user license agreement (EULA) [128](#)
- Extensible Authentication Protocol (EAP) [132](#)
- external antenna [61](#)
- external authentication
  - MAC authentication [79](#), [118](#)
  - RADIUS and LDAP servers [82](#), [122–124](#), [128](#)
- external storage [141](#)

## F

- factory default settings, wireless controller [13](#), [198](#), [202](#)
- factory default state, access points [54](#)
- failover, redundancy [158](#), [161](#)
- features, overview [9](#), [16](#)
- firmware
  - minimum version for access points [15](#)
  - scheduling updates [138](#)
  - upgrading [137](#)
  - version [171](#)
- floors, planning [44](#)

fragmentation length **95**

frequency band **46**

FTP server, firmware upgrade **138**

## G

guard interval **94**

guest access, captive portal **126**

GUI, troubleshooting **195**

## H

hard reset **139, 198**

heat map **48**

high traffic load, preventing channel allocation **101**

hotspot users **126**

## I

interference sources **27**

internal antenna **61**

internal authentication server **124**

internal RADIUS server **122**

interval, rogue access point detection **115**

inventory, licenses **149**

IP addresses

access points **61**

DHCP server assignment **69**

license server **151**

redundancy settings **164, 165**

SNMP manager **143**

stacking settings **156**

syslog server **71**

TFTP and FTP servers **138**

wireless controller **66**

IP settings

access points **61**

wireless controller **66**

IP subnets

access points **55, 56**

LAN **66**

troubleshooting **199**

## K

Kensington lock **14**

keys, licenses **150, 152**

## L

label, bottom **14**

LAN path, troubleshooting **197**

LAN port LEDs **13, 195**

LAN ports **12**

Layer 2 and 3 networks, autodiscovery **55**

LDAP server **82, 122–124, 128**

LEDs

front panel **12**

troubleshooting **194**

licenses

number and types required **18**

redundancy group **159, 161**

registering and managing **149–152**

viewing **149**

load balancing **107**

load balancing logs, viewing **147**

local access points **51, 57–59**

local buildings **42**

location, placement **25**

lock, Kensington **14**

logs

downloading **144**

saving **144**

## M

MAC authentication **117**

managed AP list **57**

managed status, access points **59**

management VLANs **28, 32, 66**

master controller, stacking **156**

maximum burst length **107**

maximum number, wireless clients **108**

memory partition **138**

Minimum and Maximum Contention Window (CwMin or CwMax) **107**

mitigating rogue access points **115**

models, access points supported **15**

multicast routing **52**

## N

neighboring clients, viewing **185**

network authentication **79**

network performance, troubleshooting **200**

network status, viewing summary **169**

network usage, viewing **170**

notification server, emails **72**

N-to-1 redundancy **160**

NTP (Network Time Protocol), client and server **65**

number of clients, per radio **46**

**P**

package contents **11**  
 partition, memory **138**  
 password requirements **203**  
 passwords  
   restoring default **198**  
   users **128**  
 physical specifications **202**  
 pinging, access points **200**  
 PoE (Power over Ethernet), access points **15**  
 ports **12–13**  
 Power LED **12, 194**  
 power socket, AC **14**  
 preamble type **95**  
 preventing channel allocation **101**  
 primary controller, stacking **155**  
 product label **14**  
 profile groups. See access point groups.  
 profiles. See security profiles.

**Q**

QoS (quality of service) **105**

**R**

rack-mounting **25**  
 radio, turning on and off **91**  
 RADIUS servers **82, 122–124, 128**  
 rate limit logs, viewing **147**  
 rate limiting **109**  
 rebooting  
   access points **141**  
   wireless controller **139, 198**  
 received signal strength indication (RSSI) **47, 108**  
 reduced interframe space (RIFS) transmission **95**  
 redundancy logs, viewing **148**  
 redundancy status, viewing **168**  
 redundancy, managing **158**  
 redundant controller **164**  
 registrant keys, licenses **150, 152**  
 remote access **142**  
 remote access points **52, 57–59**  
 remote buildings **42**  
 requirements  
   autodiscovery **51**  
   redundancy **159**  
   RF planning  
     access points **45**  
     overview **41**

resetting  
   Factory Default button **13**  
   passwords **198**  
   wireless controller **139**  
 restoring the configuration **135**  
 RF  
   logs, viewing **146**  
   management **101**  
   obstructions **27**  
 RIFS (reduced interframe space) transmission **95**  
 rogue access points  
   detecting, managing, and mitigating **113**  
   viewing  
     in the network **170**  
     on the managed access point **175**  
     on the wireless controller **181, 186**  
 RSSI (received signal strength indication) **47, 108**  
 RTS threshold **95**

**S**

scheduling  
   channel allocation **101**  
   firmware updates **138**  
 secondary controller, stacking **155**  
 security profiles  
   configuring **77, 84**  
   managing **74**  
   viewing in the network **179**  
   viewing on the access point **175**  
   viewing on the wireless controller **187**  
 self, controller selection **157**  
 self-healing **103**  
 sentry mode **61**  
 server, licenses **150**  
 service set ID (SSID) **78**  
 session time-out **144**  
 shared key requirements (RADIUS) **203**  
 signal quality **46**  
 signal strength **107**  
 slave controller, stacking **156**  
 sniffer **196**  
 SNMP **142**  
 soft reset **139**  
 spectrum analysis **27**  
 SSID (service set ID or wireless network name) **78**  
 stacking logs, viewing **148**  
 stacking status, viewing **168**  
 stacking, managing **154**  
 standalone mode, access points **54, 62**  
 storage, external **141**

subnet masks  
     access point **61**  
     DHCP server **69**  
     wireless controller **66**  
 support, NETGEAR **18**  
 syslog server **71**  
 system alerts, viewing **146**  
 system logs, saving **144**

## T

tagged VLANs **67**  
 TCP/IP network, troubleshooting **197**  
 technical specifications **202**  
 technical support **2**  
 temperatures and humidity **203**  
 Temporal Key Integrity Protocol (TKIP) **82**  
 Test LED **13, 195**  
 TFTP server, firmware upgrade **138**  
 time and time zone  
     configuring **65**  
     troubleshooting **198**  
 TKIP (Temporal Key Integrity Protocol) **82**  
 tracing a route **201**  
 trademarks **2**  
 transmission opportunity (TXOP) limit **107**  
 transmission power, controlling  
     automatically **103**  
     manually **96, 98**  
 trap port, SNMP **143**  
 troubleshooting  
     access points **198**  
     basic functioning **194**  
     configuration settings, using sniffer **196**  
     connection problems **199**  
     date **198**  
     diagnostic tools **200**  
     discovery problems **198**  
     GUI **195**  
     LAN path **197**  
     LEDs **194**  
     network performance **200**  
     pinging access points **200**  
     restoring factory default settings **198**  
     TCP/IP network **197**  
     time and time zone **198**  
     tracing an access point route **201**  
     web management interface **195**  
 Tx power, controlling  
     automatically **103**  
     manually **96, 98**  
 TXOP (transmission opportunity) limit **107**

## U

untagged VLANs **67**  
 upgrading firmware **137**  
 USB port **12**  
 users, managing **128**

## V

VAR information, licenses **152**  
 video QoS queue **105**  
 Virtual Router Redundancy Protocol (VRRP) **158, 165**  
 VLANs **66**  
     client **29, 32**  
     DHCP server **68**  
     management **28, 32**  
     security profiles **79**  
     settings, access points **61**  
     untagged **67**  
 voice QoS queue **105**  
 VRRP (Virtual Router Redundancy Protocol) **158, 165**

## W

WC7510L licenses **18, 149**  
 web management interface, troubleshooting **195**  
 WEP encryption **82**  
 WEP key requirements **203**  
 WINS servers **66**  
 wired connection, stacking **154**  
 wireless band usage, viewing  
     in the network **170**  
     on the wireless controller **182**  
 wireless client separation **79**  
 wireless clients, maximum number **108**  
 wireless clients, viewing  
     blacklisted in the network **192**  
     in the network **169, 176, 191**  
     neighboring in the network **185**  
     on the access point **175**  
     on the wireless controller **180, 184**  
 wireless controller, viewing  
     active SSIDs **191**  
     captive portal accounts and users **188**  
     DHCP leases **188**  
     in the network **171**  
     redundancy status **181**  
     summary **180**  
     usage **182**  
 wireless modes **94**  
 wireless network name (SSID) **78**  
 wireless settings **93**  
 wizard, access point discovery **51**

WMM (Wi-Fi multimedia) **105**

WNAP210, WNAP320, WNDAP350, and WNDAP360  
**15**

WPA and WPA2 authentication **82–84**

WPA passphrase requirements **203**