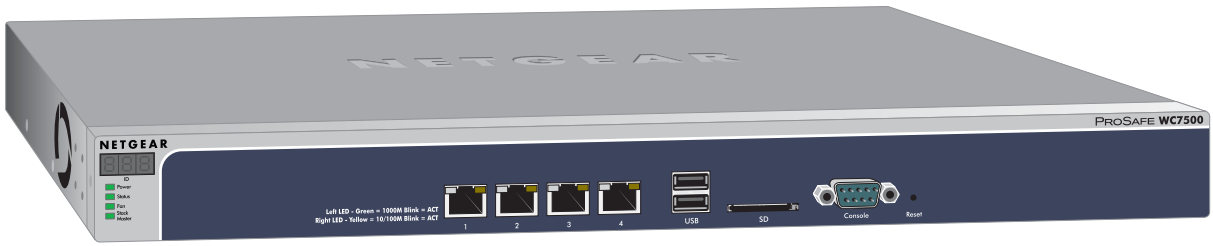
NETGEAR®

ProSAFE Wireless Controller Models WC7500, WC7600, WC7600v2, and WC9500

User Manual



April 2016
202-11659-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit *www.netgear.com/support* to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Conformity

For the current EU Declaration of Conformity, visit *http://kb.netgear.com/app/answers/detail/a_id/11621*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-11659-01	April 2016	• First publication of the combined manual for all models. • Introduction of model WC7500 and model WC7600v2.

Contents

Chapter 1 Introduction

Models, Key Features, and Capabilities 11
Model WC7500 11
Model WC7600 11
Model WC7600v2 11
Model WC9500 12
Model Scalability and Feature Differences 12
Model Common Features and Capabilities 13
What Can You Do With a Wireless Controller? 14
Licenses 16
Maintenance and Support 16

Chapter 2 Hardware Descriptions

Package Contents 18
Hardware Models WC7500 and WC7600v2 18
WC7500 and WC7600v2 Front Panel Ports and Slots 18
WC7500 and WC7600v2 Back Panel Components 20
WC7500 and WC7600v2 Product Labels 20
Hardware Models WC7600 and WC9500 21
WC7600 and WC9500 Front Panel Ports and Slots 21
WC7600 and WC9500 Back Panel Components 22
WC7600 and WC9500 Product Labels 23
LED Functions (All Models) 24
Wireless Controller System Components 25
Supported NETGEAR Access Points 26
Supported NETGEAR Antennas 30

Chapter 3 System Planning and Deployment Scenarios

Basic and Advanced Setting Concepts 32
Profile Group Concepts 33
Basic Profile 33
Advanced Profile 33
System Planning Concepts 35
Preinstallation Planning 35
Before You Configure a Wireless Controller 35
High-Level Configuration Examples 38
Single Controller Configuration With Basic Profile Group 38
Single Controller Configuration With Advanced Profile Groups 39
Stacked Controller Configuration 40

Management VLAN and Data VLAN Strategies 41
High-Level Deployment Scenarios 43
Scenario Example 1: Network With Single VLAN 43
Scenario Example 2: Advanced Network With VLANs and SSIDs 45
Scenario Example 3: Advanced Network With Redundancy 47

Chapter 4 RF Planning and Deployment

Application, Browser, and Port Requirements for RF Planning 52
RF Planning Overview 52
Planning Requirements 53
Recommended RF Planning Procedure for a Building 55
Manage a Building and Floors for an RF Plan 55
Add a Building and Floors 56
Add a Single Floor to a Building 58
Scale a Floor 59
Add a WiFi Coverage or WiFi Noncoverage Zone to a Floor 60
Remove a WiFi Coverage or Noncoverage Zone From a Floor 61
Add a WiFi Building Obstacle to a Floor 61
Remove a Building Obstacle From a Floor 63
Add a WiFi Obstruction Area 64
Remove a WiFi Obstruction Area 65
Change the Name, Map, or Dimensions of a Floor 65
Change the Name of a Building 66
Duplicate an Entire Building With All Floors 67
Duplicate a Single Floor 67
Remove a Single Floor 68
Remove an Entire Building With All Its Floors 69
Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor 69
Manually Add and Manage Access Points on a Floor Map for an RF Plan 75
Manually Add and Manage Antennas on a Floor Map for an RF Plan 78
Display and Recalculate the WiFi Coverage for a Heat Map 82
Display or Change the WiFi Inventory for an RF Plan 83
Download a Report for an RF Plan 86
View the Heat Map for a Deployed Floor Plan 87

Chapter 5 Installation and Configuration Overview

Connect Your Computer to the Wireless Controller 91
Log In to the Wireless Controller 91
Roadmap for Initial Configuration 93
Roadmap for Configuring Management of Your WiFi Network 95
Choose a Location for the Wireless Controller 97
Deploy the Wireless Controller 97

Chapter 6 Configure the System and Network Settings and Register the Licenses

Configure the General Settings 99

Manage the Time Settings 100
Manage the IP, VLAN, and Link Aggregation Settings 101
Management VLAN Concepts 101
Untagged VLAN Concepts 102
Link Aggregation Concepts 102
Configure the IP, VLAN, and Link Aggregation Settings 103
Manage the DHCP Server 105
Add a DHCP Server 105
Change the Settings for a DHCP Server 107
Remove a DHCP Server 108
Register Your Licenses 109
Configure the License Server Settings 109
Register Your Licenses With the License Server 110
Manage Certificates 112
Configure Log, Syslog, Alarm Notification, and Email Settings 113
Configure the Event Tracing Log Settings 113
Configure the Syslog Settings 115
Configure Alarm Notification Settings 116
Configure the Email Notification Server 117

Chapter 7 Manage Security Profiles and Profile Groups

WiFi Security Profile Concepts 120
Small WLAN Networks 120
Large WLAN Networks 121
Profile Naming Conventions 121
Considerations Before You Configure Profiles 121
Basic and Advanced Security Configuration Concepts 122
Manage Security Profiles for the Basic Profile Group 123
Configure a Profile in the Basic Profile Group 123
Change the Settings for a Profile in the Basic Profile Group 127
Remove a Profile From the Basic Profile Group 128
Manage Security Profiles for Advanced Profile Groups 128
Add an Advanced Profile Group 128
Remove an Advanced Profile Group 130
Configure a Profile in an Advanced Profile Group 130
Change the Settings for a Profile in an Advanced Profile Group 134
Remove a Profile From an Advanced Profile Group 135
Network Authentication and Data Encryption Options 136
Manage Authentication Servers and Authentication Server Groups 139
Authentication Server Concepts 139
Configure Basic Authentication Server Settings 141
Configure a RADIUS Authentication Server Group 143
Remove a RADIUS Authentication Server Group 144
Manage MAC Authentication and MAC Authentication Groups 145
Guidelines for External MAC Authentication 145
Configure Basic Local MAC Authentication Settings 145
Remove a MAC Address From a Wireless Client List 147
Import a MAC List From a File 147

Configure a Local MAC Authentication Group 148
Remove a Local MAC Authentication Group 150
Select an ACL for a Profile in the Basic Profile Group 150
Select an ACL for a Profile in an Advanced Profile Group. 151

Chapter 8 Discover and Manage Access Points

Access Point Discovery Guidelines 154
General Discovery Guidelines 154
Layer 3 Discovery Guidelines 154
Remote Access Point Discovery Guidelines 156
Discover Access Points With the Discovery Wizard. 158
Discover Access Points in Factory Default State and Access Points in a Layer 2 Subnet. 158
Discover Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks 162
Manage the Managed AP List 166
View the Managed AP List. 166
Change Access Point Information on the Managed AP List 168
Remove Access Points From the Managed AP List 171
Assign Access Points to Buildings, Floors, and Advanced Profile Groups 172

Chapter 9 Configure WiFi and QoS Settings

Basic and Advanced WiFi and QoS Configuration Concepts 176
Configure the Radio 176
Configure the Radio for the Basic Profile Group 176
Configure the Radio for an Advanced Profile Group 177
Configure WiFi Settings 179
Configure WiFi Settings for the Basic Profile Group 179
Override Channel and Transmission Power in the Basic Profile Group 183
Configure WiFi Settings for an Advanced Profile Group. 185
Override Channel and Transmission Power in an Advanced Profile Group 189
Configure Channels. 191
Specify Radio Frequency Management 194
Radio Frequency Concepts 194
WLAN Healing Concepts 195
Configure Radio Frequency Management for the Basic Profile Group. . . . 195
Configure Radio Frequency Management for an Advanced Profile Group 197
Manage the Preferred Bands. 199
Configure the Preferred Band for WNDAP620 Access Points in the Basic Profile Group. 200
Configure the Preferred Band for WNDAP620 Access Points in an Advanced Profile Group 201
Manage Quality of Service for an Advanced Profile Group 202
Quality of Service Concepts 202
Configure Quality of Service for a Profile Group. 203

Manage Load Balancing 205
Load Balancing Concepts 205
Configure Load Balancing 206
Manage Rate Limiting 207
Rate Limiting Concepts 207
Configure Rate Limiting for the Basic Profile Group 208
Configure Rate Limiting for an Advanced Profile Group 209
Manage the LED Behavior 210
Manage the LED Behavior for the Basic Profile Group 210
Manage the Behavior for an Advanced Profile Group 211

Chapter 10 Manage Rogue Access Points, Guest Network Access, and Users

Manage Rogue Access Points 214
Rogue Access Point Concepts 214
Configure Basic Rogue Detection Settings 214
Classify Rogue Access Points 215
Import a List of Known Access Points From a File 217
Manage Guest Network Access Through Guest Portals and Captive Portals . 218
Portal Concepts 218
Configure a Basic Guest Portal or Captive Portal 219
Configure an Advanced Guest Portal or Captive Portal 224
Remove a Portal 230
Manage Users, Accounts, and Passwords 230
User and Account Concepts 230
Add a Management User 231
Add a WiFi User 233
Add a Captive Portal Account 234
Add a Logo and Message on Captive Portal User Information 236
Add a Captive Portal User 238
Add Multiple Captive Portal Users Simultaneously 240
Change the Settings for a User or Account 242
Remove Users or Accounts 243
Export a List of Users or Accounts 244

Chapter 11 Maintain the Wireless Controller and Access Points

Manage the Configuration File or Upgrade the Firmware 246
Back Up the Configuration File 246
Restore the Configuration File 247
Upgrade the Firmware 248
Reboot the Wireless Controller 251
Reset the Wireless Controller 251
Manage External Storage 252
Manage Remote Access 254
Specify Session Time-Outs 255
Save the Logs 256
Save the System Logs 256

Save and Clear the Logs for an Access Point 257
View Alerts and Events 259
View System Alerts 259
View Radio Frequency Events 260
View Load-Balancing Events 261
View Rate-Limit Events 263
View Redundancy Events 264
View Stacking Events 265
Manage Licenses 266
View Your Licenses 266
Retrieve Your Licenses 268
Reboot Access Points 269
Configure Multicast Firmware Upgrade for Access Points 270
Change the Multicast Firmware Upgrade Settings 270
Disable Multicast Firmware Upgrade 271

Chapter 12 Manage Stacking and Redundancy

Stacking Concepts 273
Configure a Stack of Wireless Controllers 275
Remove a Wireless Controller From a Stack 279
Select Which Wireless Controller in a Stack to Configure 280
Manage Redundancy for a Single Controller 283
VRRP Redundancy Concepts 283
Configure a Single Controller With Redundancy 285
Manage a Redundancy Group With N:1 Redundancy 289
VRRP N:1 Redundancy Concepts 289
Configure a Redundancy Group With N:1 Redundancy 292
Replace a Redundant Controller 297
Remove a Redundancy Group 298

Chapter 13 Monitor the WiFi Network and Its Components

Monitor the Network 301
View the Network Summary Page 301
View the Wireless Controllers in the Network 303
View the Access Points in the Network 305
View the Clients in the Network 310
View the Profiles in the Network 314
Monitor the Wireless Controller 316
View the Wireless Controller Summary Page 316
View Wireless Controller Usage 319
View Access Points That the Wireless Controller Manages 320
View Clients on Access Points That the Wireless Controller Manages 325
View Neighboring Clients That the Wireless Controller Detects 329
View Neighboring Access Points That the Wireless Controller Does Not Manage 331
View Security Profiles That the Wireless Controller Manages 332
View DHCP Leases That Are Provided by the Wireless Controller 334

View Captive Portal Users on Access Points That the Wireless Controller Manages. . . . 335
View the Guest Email Address Database for Access Points That the Wireless Controller Manages . . . 337
Monitor the SSIDs on the Wireless Controller. . . . 338
Monitor Local Clients in the Network. . . . 343
Monitor Accepted Clients . . . 343
Monitor Blacklisted Clients . . . 347

Chapter 14 Troubleshooting and Diagnostics

Troubleshoot Basic Functioning. . . . 351
Power LED Is Not Lit. . . . 351
Status LED Never Turns Off . . . 351
Ethernet Port LEDs Are Not Lit. . . . 351
Troubleshoot the Web Management Interface . . . 352
Check the Ethernet Cabling. . . . 352
Check the IP Address Configuration . . . 352
Check the Internet Browser . . . 353
Troubleshoot a TCP/IP Network Using the Ping Utility . . . 353
Use the Reset Button to Restore Default Settings . . . 354
Resolve Problems With Date and Time. . . . 354
Resolve Network Problems . . . 355
Resolve Problems With Access Points . . . 355
Resolve Discovery Problems . . . 355
Resolve Connection Problems. . . . 356
Network Performance and Rogue Access Point Detection. . . . 356
Use the Diagnostic Tools on the Wireless Controller . . . 356
Ping an Access Point. . . . 356
Trace a Route to an Access Point . . . 357

Appendix A Factory Default Settings, Technical Specifications, and Passwords Requirements

Factory Default Settings . . . 360
Technical Specifications Models WC7500 and WC7600v2. . . . 360
Technical Specifications Models WC7600 and WC9500 . . . 361
Password Requirements . . . 362

Index

Introduction

1

This chapter includes the following sections:

- *Models, Key Features, and Capabilities*
- *What Can You Do With a Wireless Controller?*
- *Licenses*
- *Maintenance and Support*

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

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

Note: In this manual, the terms *wireless* and *WiFi* are interchangeable.

Models, Key Features, and Capabilities

The NETGEAR ProSAFE Wireless Controller is a high-capacity, secured wireless controller intended for medium- to large-sized businesses, higher education institutions, hospitals, and hotels.

The wireless controller supports the IEEE 802.11a/b/g/n/ac protocols. With the wireless controller, you can 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).

This user manual supports models WC7500, WC7600, WC7600v2, and WC9500. For a comparison between the models, see *Table 1* on page 12.

Note: For information about the manuals for the legacy model WC7520, visit *downloadcenter.netgear.com/en/product/WC7520*.

Model WC7500

One WC7500 wireless controller with the appropriate licenses can support up to 15 access points (APs) with up to 400 users. Model WC7500 is an entry-level model: You cannot stack the WC7500, nor is controller redundancy supported.

Model WC7500 provides four RJ-45 Gigabit Ethernet ports. These ports are available to access the wireless controller for management and for data and control communications between the wireless controller and the access points.

Model WC7600

One WC7600 wireless controller with the appropriate licenses can support up to 50 access points (APs) with up to 2,000 users. In a stacked configuration, a stack of three wireless controllers can support up to 150 access points with up to 6,000 users.

Model WC7600 provides one RJ-45 Gigabit Ethernet port and two 10 Gigabit Ethernet (10GbE) slots with standard SFP+ form factor for optional 10GBASE or 1000BASE GBICs. These ports are available to access the wireless controller for management and for data and control communications between the wireless controller and the access points.

Model WC7600v2

One WC7600v2 wireless controller with the appropriate licenses can support up to 50 access points (APs) with up to 2,000 users. In a stacked configuration, a stack of three wireless controllers can support up to 150 access points with up to 6,000 users.

Model WC7600v2 provides four RJ-45 Gigabit Ethernet ports. These ports are available to access the wireless controller for management and for data and control communications between the wireless controller and the access points.

Model WC9500

One WC9500 standalone wireless controller with the appropriate licenses can support up to 300 access points with up to 9,000 clients. In a stacked configuration, one wireless controller with the appropriate licenses can support up to 200 access points with up to 6,000 clients. A stack can support three wireless controllers with up to 18,000 clients.

Model WC9500 provides one RJ-45 Gigabit Ethernet port and two 10 Gigabit Ethernet (10GbE) slots with standard SFP+ form factor for optional 10GBASE or 1000BASE GBICs. These ports are available to access the wireless controller for management and for data and control communications between the wireless controller and the access points.

Model Scalability and Feature Differences

The following table show the differences in scalability and features between the wireless controller models.

Table 1. Model differences and scalable architecture

Feature	WC7500	WC7600	WC7600v2	WC9500
License in AP increments	5	10, 50	10, 50	10, 50, 100, 200
Single controller Max. number of APs Max. number of users	 15 400	 50 2,000	 50 2,000	 300 9.000
Stack of three controllers Max. number of APs Max. number of users	 Stacking is not supported	 150 6,000	 150 6,000	 600 18,000
Controller redundancy	Not supported	Supported	Supported	Supported
Link aggregation	Not supported	Supported	Not supported	Supported
WNDAP620 access point	Not supported	Supported	Not supported	Supported
Monitor blacklisted clients	Not supported	Supported	Not supported	Supported
1G ports	4	1	4	1
SFP slots	None	2	None	2
USB ports	2	1	2	1
SD card slot	1[1]	None	1[1]	None
Optional extra power supply	Not supported	Supported	Not supported	Supported

1. An SD card will be supported in a future release.

Model Common Features and Capabilities

The wireless controller provides the following common key features and capabilities:

- **WiFi modes**
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
  - 802.11ac
- **Autodiscovery of access points**
  - Autodiscovery of access points in the same Layer 2 domain.
  - Autodiscovery of access points across a Layer 3 domain.
  - 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 WiFi 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.
  - Support for nine access point profile groups (one basic and eight advanced) on one wireless controller.
  - Support for up to 8 profiles per access point profile group and 8 profiles per radio (therefore, dual-band access points can support up to 16 profiles in one access point profile group).
  - Support for up to 144 profiles on one wireless controller (8 profiles per access point group and eight groups per radio). Each profile supports settings for SSID, network authentication, data encryption, client separation, VLAN, MAC ACL, and WiFi QoS.
  - Rogue access point detection and classification.
  - Guest access and captive portal access with cost and expiration accounting.
  - Scheduled WiFi on/off times.
- **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 WiFi users.
  - Layer 2 and Layer 3 seamless roaming support.
  - Local Layer 2 traffic switching and Layer 3 traffic processing at access point level for fast processing.

- **Wireless and Radio Frequency (RF) management**
  - 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.
  - Multicast and broadcast rate limiting
  - ARP suppression
- **Monitoring and reporting**
  - 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, and rate-limiting events.

For a list of all features and capabilities of the wireless controller, see the datasheets:

- For the WC7500, visit *support.netgear.com/product/WC7500*
- For the WC7600, visit *support.netgear.com/product/WC7600*.
- For the WC7600v2, visit *support.netgear.com/product/WC7600*.
- For the WC9500, visit *support.netgear.com/product/WC9500*.

What Can You Do With a Wireless Controller?

You can perform the following tasks with a wireless controller:

- **Organize the Network**
  - **Create access point profiles**. Organize access points in profiles to differentiate between SSIDs, client authentication, authentication settings, and WiFi QoS settings.
  - **Create access point profile *groups***. Organize access point profiles in access point profile groups to differentiate between buildings, floors, businesses, business divisions, and so on. Easily assign access points to profile groups or change assignments.

  For more information, see *Chapter 7, Manage Security Profiles and Profile Groups*.
- **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 8, Discover and Manage Access Points*.

- **Centrally Manage Security in the Network**
  - **Manage secure access to the network and secure data transmission**. Manage client authentication, encryption, WiFi 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 10, Manage Rogue Access Points, Guest Network Access, and Users*.
- **Centrally Manage the WiFi Settings for the Network**
  - **Schedule the radios**. Schedule the entire network to go offline, or schedule access point profile groups to go offline.
  - **Manage WiFi settings and channel allocation**. Manage the WiFi settings such as wireless mode, data rate, and channel width 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 for access point profile groups.

  For more information, see *Chapter 9, Configure WiFi and QoS Settings*.
- **Manage Other Wireless Controllers in the Network**
  - **Manage stacking**. Specify the master and slave wireless controllers in a stack and synchronize information between the wireless controller.[1]

  For more information, see *Chapter 12, Manage Stacking and Redundancy*.
- **Monitor the Network and Its Components**
  - **Monitor the status of all WiFi devices**. View the status of 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 13, Monitor the WiFi Network and Its Components*.

1. Model WC7500 does not support stacking.

Licenses

By default, the wireless controller comes with a trial license for two access points. You must purchase and register licenses for the access points in your network. Licenses are tied to the serial number of the wireless controller.

Depending on the model, you can purchase licenses in 5–, 10–, 50–, 100–, or 200–access point increments for support of multiple access points on a single wireless controller.

Table 2. Purchasable license increments

License increments	WC7500	WC7600	WC7600v2	WC9500
5 APs	WC5APL-10000S		—	—
10 APs	—	WC10APL-10000S	WC10APL-10000S	WC10APL-10000S
50 APs	—	WC50APL-10000S	WC50APL-10000S	WC50APL-10000S
100 APs	—	—	—	WC100APL-10000S
200 APs	—	—	—	WC200APL-10000S

For example, if you installed three WC9500 wireless controllers in a stack and want to support the maximum number of 600 access points in a stacked configuration, you must purchase three WC200APL licenses (or a combination of other licenses that add up to a total of 600 access points).

For information about how to register and manage your licenses, see *Register Your Licenses* on page 109 and *Manage Licenses* on page 266.

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*.

2 Hardware Descriptions

This chapter includes the following sections:

- *Package Contents*
- *Hardware Models WC7500 and WC7600v2*
- *Hardware Models WC7600 and WC9500*
- *LED Functions (All Models)*
- *Wireless Controller System Components*
- *Supported NETGEAR Access Points*
- *Supported NETGEAR Antennas*

Package Contents

The product package contains the following items:

- One ProSAFE wireless controller appliance
- One AC power cable
- Rubber feet (four) with adhesive backing
- One rack-mount kit
- Straight-through Category 5 Ethernet cable
- *ProSAFE Wireless Controller Installation Guide*

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. We recommend that you keep the carton, including the original packing materials, in case you must return the product for repair.

Hardware Models WC7500 and WC7600v2

The front panel ports, slots, and LEDs, back panel components, and product label of models WC7500 and WC7600v2 are described in the following sections.

WC7500 and WC7600v2 Front Panel Ports and Slots

The following figure shows the front panel of models WC7500 and WC7600v2. (The label on the right states PROSAFE WC7500 but the front panel for the WC7600v2 is identical.)

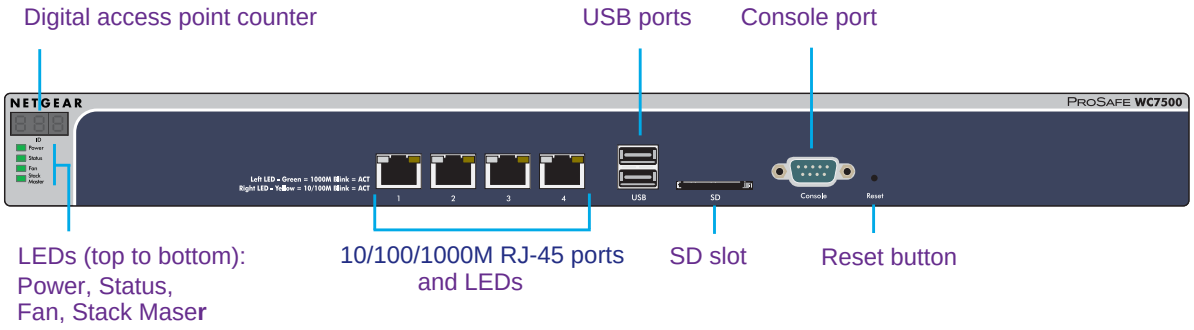


Figure 1. Front panel models WC7500 and WC7600v2

The following figure shows a close-up of the left side of the front panel.

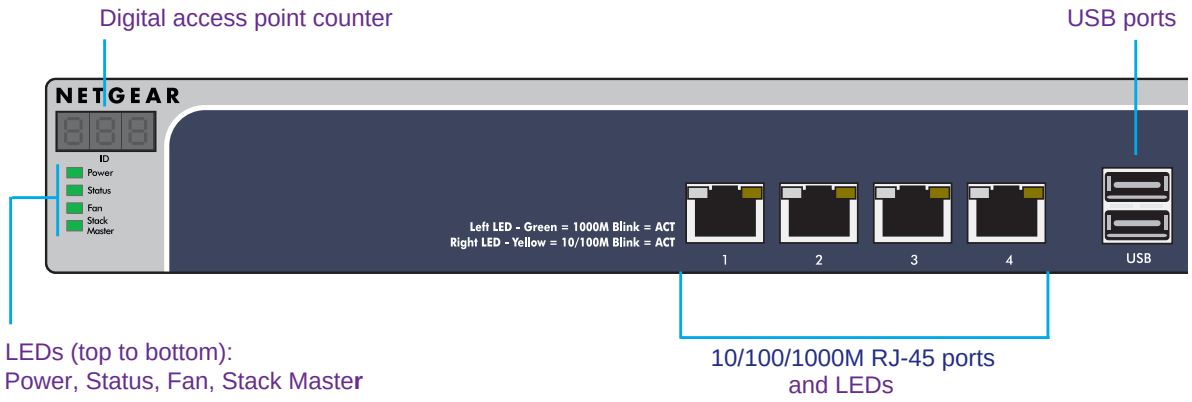


Figure 2. Front panel close-up models WC7500 and WC7600v2

From left to right, the front panel of models WC7500 and WC7600v2 show the components that are described in the following table.

Table 3. Front panel components models WC7500 and WC7600v2

Component	Description
Digital counter	Displays the number of connected access points that are in a healthy state.
System LEDs	From top to bottom: Power LED, Status LED, Fan LED, and Stack Master LED. These LEDs are described in *Table 5* on page 24.
Ethernet ports and LEDs	Four 10/100/1000 Mbps LAN Ethernet port with an RJ-45 connector, left LED, and right LED. The Ethernet port provides switched N-way, automatic speed negotiating, auto MDI/MDIX technology.
USB ports	Two USB 2.0 ports for external storage of floor heat maps, saving of the syslogs, and backing up the configuration. The USB ports support FAT32 file systems.
SD card slot	An SD card for saving of the system logs will be supported in a future release.
Console port	RS232 port for connecting to an optional console terminal. The port provides a DB9 male connector. The default baud rate is 115200 bits/second. **Note:** The console port is for debugging under guidance of NETGEAR technical support only.
Reset button	Using a sharp object, press and hold this button for about 10 seconds until the Status LED blinks and the wireless controller returns to factory default settings. If you reset the wireless controller, all configuration settings are lost and the default password is restored.

WC7500 and WC7600v2 Back Panel Components

The wireless controller comes with a single internal power supply and internal fans. The back panel provides a Kensington™ lock slot and the AC power supply connector for the 100–240V, 3A, 50–60 Hz power supply.

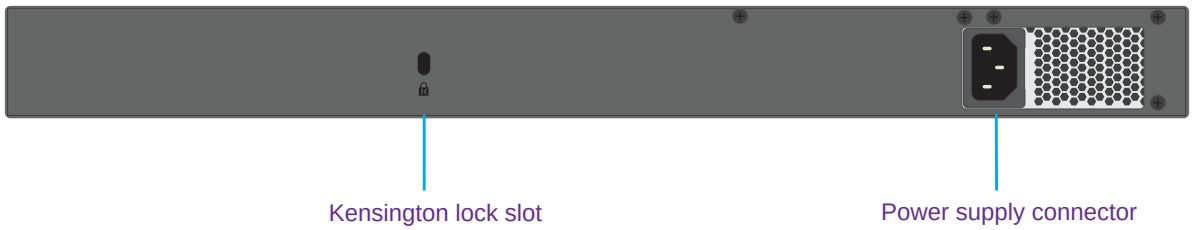


Figure 3. Back panel models WC7500 and WC7600v2

Attach the power cord to the power supply connector. (The wireless controller does not provide an on/off power switch.)

WC7500 and WC7600v2 Product Labels

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.

Model WC7500 and model WC7600v2 share the same product label. The actual model number (WC16A for both the WC7500 and the WC7600v2) is stated in the **MODEL** field.

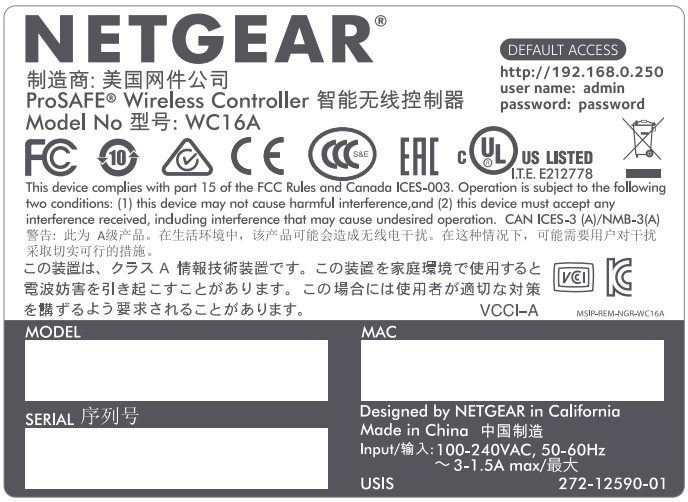


Figure 4. Product label model WC7500 and model WC7600v2

Hardware Models WC7600 and WC9500

The front panel ports, slots, and LEDs, back panel components, and product label of models WC7600 and WC9500 are described in the following sections.

WC7600 and WC9500 Front Panel Ports and Slots

The following figure shows the front panel of models WC7600 and WC9500. (The label on the right states PROSAFE WC9500 but the front panel for the WC7600 is identical.)

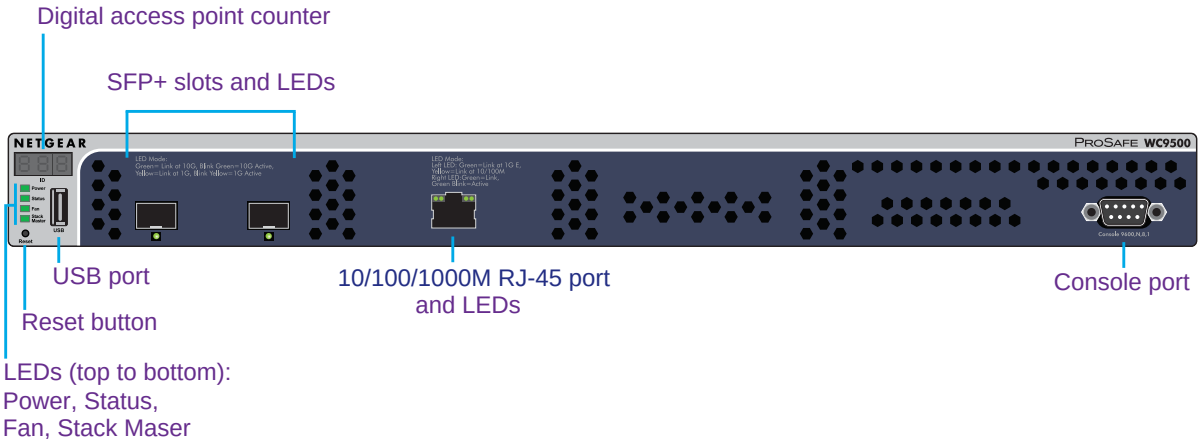


Figure 5. Front panel models WC7600 and WC9500

The following figure shows a close-up of the left side of the front panel.

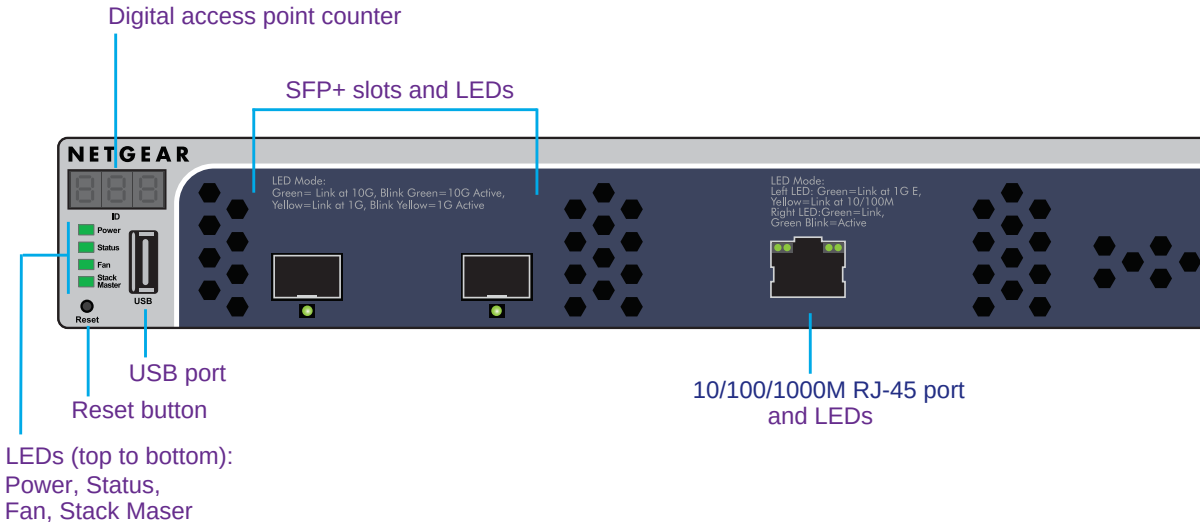


Figure 6. Front panel close-up models WC7600 and WC9500

From left to right, the front panel of models WC7600 and WC9500 show the components that are described in the following table.

Table 4. Front panel components models WC7600 and WC9500

Component	Description
Digital counter	Displays the number of connected access points that are in a healthy state.
System LEDs	From top to bottom: Power LED, Status LED, Fan LED, and Stack Master LED. These LEDs are described in *Table 5* on page 24.
Reset button	Using a sharp object, press and hold this button for about 10 seconds until the Status LED blinks and the wireless controller returns to factory default settings. If you reset the wireless controller, all configuration settings are lost and the default password is restored.
USB port	One USB 2.0 port for external storage of floor heat maps, saving of the syslogs, and backing up the configuration. The USB port supports FAT32 file systems.
SFP+ slots and LEDs	Two SFP+ slots for optional 10GE SFP+ or 1G SFP gigabit interface converters (GBICs), each slot with an LED.
Ethernet port and LEDs	One 10/100/1000 Mbps LAN Ethernet port with an RJ-45 connector, left LED, and right LED. The Ethernet port provides switched N-way, automatic speed negotiating, auto MDI/MDIX technology.
Console port	RS232 port for connecting to an optional console terminal. The port provides a DB9 male connector. The default baud rate is 9600 bits/second. **Note:** The console port is for debugging under guidance of NETGEAR technical support only.

WC7600 and WC9500 Back Panel Components

The wireless controller comes with a single internal power supply but supports an optional second power supply for power redundancy. The power supplies are hot-swappable.

The following figure shows the back panel of the wireless controller with a single internal power supply, the power supply connector, and two double fans.

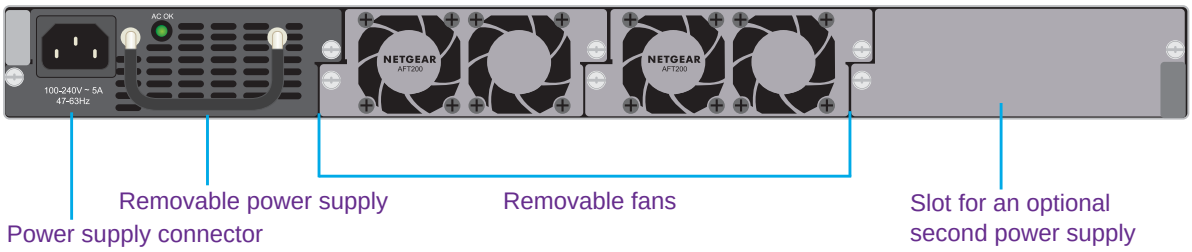


Figure 7. Back panel models WC7600 and WC9500

From left to right, the back panel of models WC7600 and WC9500 provide the following components:

- **Power supply**. 100–240V, 5A, 47–63 Hz power supply, which includes the following external components:
  - **AC power socket**. Attach the power cord to this socket. (The wireless controller does not provide an on/off power switch.)
  - **Power supply with handle**. The handle allows for easy removal and insertion of the power supply.
  - **LED**. The power supply LED is lit green when the power supply functions correctly. If the LED is off, power is not supplied to the power supply, or a problem occurred.
- **Fans**. Two double fans, each of which can be easily exchanged.
- **Slot for optional second power supply**. The cover plate can be removed so you can insert a second removable power supply for power redundancy.

WC7600 and WC9500 Product Labels

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 8. Product label model WC7600

Figure 9. Product label WC9500

LED Functions (All Models)

The function of each LED is described in the following table. These LEDS apply to all models except where noted otherwise.

Table 5. LED functions for all models

LED	Status	Description
Power LED	Solid green	The wireless controller is on.
	Off	The wireless controller is 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 *Power LED Is Not Lit* on page 351).
Status LED	Solid yellow	The wireless controller is initializing. After approximately two minutes, when the wireless controller completes its initialization, the Status LED turns solid green. If the Status LED remains solid yellow, the initialization failed (see *Status LED Never Turns Off* on page 351).
	Solid green	The wireless controller completed its initialization successfully. The Status LED is solid green during normal operation.
	Off	The wireless controller is not receiving power.
	Blinking yellow	Firmware is being upgraded.
Fan LED	Solid green	The fans are functioning correctly.
	Solid yellow	One or more fans are not functioning correctly.

Table 5. LED functions for all models (continued)

LED	Status		Description
Stack Master LED **Note:** Does not apply to WC7500	Solid green		The wireless controller is functioning as the master controller in a stack.
	Solid yellow		The wireless controller is functioning as a slave controller in a stack.
SFP slot LEDs **Note:** Does not apply to WC7500 and WC7600v2	Solid green		The slot is operating at 10G.
	Blinking green		Data is being transmitted or received at 10G.
	Solid yellow		The slot is operating at 1G.
	Blinking yellow		Data is being transmitted or received at 1G.
Left Ethernet port LED	Off		The port is not connected to a powered-on Ethernet device (see *Ethernet Port LEDs Are Not Lit* on page 351).
	WC7500 and WC7600v2	Solid green	The port is operating at 1000 Mbps.
		Blinking green	Data is being transmitted or received at 1000 Mbps.
	WC7600 and WC9500	Solid green	The port is operating at 1000 Mbps.
		Solid yellow	The port is operating at 100 Mbps or 10 Mbps.
Right Ethernet port LED	Off		The port is not connected to a powered-on Ethernet device (see *Ethernet Port LEDs Are Not Lit* on page 351).
	WC7500 and WC7600v2	Solid yellow	The port is operating at 100 Mbps or 10 Mbps.
		Blinking yellow	Data is being transmitted or received at 100 Mbps or 10 Mbps.
	WC7600 and WC9500	Solid green	The port is connected to a powered-on Ethernet device.
		Blinking green	Data is being transmitted or received.

Wireless Controller System Components

A 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 or a group of up to three stacked wireless controllers that can function in a redundant configuration[1].

The wireless controller system supports the following NETGEAR ProSAFE access point models:

- WAC730 ProSAFE 3x3 Dual-Band Wireless AC Access Point
- WAC720 ProSAFE 2x2 Dual-Band Wireless AC Access Point
- WN370 ProSAFE Wall Mount Wireless N Access Point

1. Model WC7500 does not support stacking and redundancy.

- WND930 Outdoor Dual Band Wireless-N
- WNDAP660 ProSAFE Premium 3x3 Dual Band Concurrent Wireless-N Access Point
- WNDAP620 ProSAFE Premium 3x3 Dual Band Wireless-N Access Point[1]
- WNDAP380R ProSAFE Dual Band Wireless-N Access Point with RFID support
- WNDAP360 ProSAFE Dual Band Wireless-N Access Point
- WNDAP350 ProSAFE Dual Band Wireless-N Access Point
- WNAP320 ProSAFE Wireless-N Access Point
- WNAP210v2 ProSAFE Wireless-N Access Point

Supported NETGEAR 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 a VPN network. After you use the automatic discovery process and add 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.

The following table lists the minimum firmware versions that must run on the standalone access points before you convert them to managed access points. If your access point runs a firmware version that is earlier than the minimum firmware version, first upgrade the access point to the minimum firmware version or a later version.

Table 6. Minimum firmware versions

Access Point Model	Minimum Firmware Version on Standalone Access Point
WAC730	All firmware versions are supported.
WAC720	All firmware versions are supported.
WN370	All firmware versions are supported.
WND930	2.0.4 or a newer version is supported.
WNDAP660	2.0.2 or a newer version is supported.
WNDAP620	2.0.4 or a newer version is supported. **Note:** This access point is not supported on models WC7500 and WC7600v2.
WNDAP380R	All firmware versions are supported.
WNDAP360	2.1.6 or a newer version is supported.
WNDAP350	2.1.7 or a newer version is supported.
WNAP320	2.1.1 or a newer version is supported.
WNAP210v2	All firmware versions are supported.

1. The WNDAP620 is not supported on models WC7500 and WC7600v2.

A wireless controller system supports the following access points:

- **WAC730 ProSAFE 3x3 Dual-Band Wireless AC Access Point**
  - Supports concurrently 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports 3x3 multiple input, multiple output (MIMO).
  - Supports speeds of up to 1300 Mbps for 802.11ac network devices.
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3af standard.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WAC730*.
- **WAC720 ProSAFE 2x2 Dual-Band Wireless AC Access Point**
  - Supports concurrently 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports 2x2 multiple input, multiple output (MIMO).
  - Supports speeds of up to 867 Mbps for 802.11ac network devices
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3af standard.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WAC720*.
- **WN370 ProSAFE Wall Mounted Wireless-N Access Point**
  - Supports concurrently 802.11b, 802.11g, and 802.11n network devices.
  - Operates in the 2.4 GHz radio band.
  - Supports speeds of up to 300 Mbps for 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3af standard.

  For product documentation and firmware, visit *http://support.netgear.com/product/WN370*.
- **WND930 Outdoor Dual Band Wireless-N**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports speeds of up to 300 Mbps for 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3af or 802.3at standards.

  For product documentation and firmware, visit *http://support.netgear.com/product/WND930*.

- **WNDAP660 ProSAFE Premium 3x3 Dual Band Concurrent Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports 3x3 multiple input, multiple output (MIMO).
  - Supports speeds of up to 450 Mbps for 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3at standard.

    Note: If your network does not include a PoE device that can provide the WNDAP660 access point with PoE power according to the 802.3at standard, you can instead use two ports of a PoE device that complies with the 802.3af standard. (The WNDAP660 access point provides two Ethernet ports that accept PoE.)

  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNDAP660*.
- **WNDAP620 ProSAFE Premium 3x3 Dual Band Wireless-N Access Point**[1]
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates in either the 2.4 GHz radio band or the 5 GHz radio band (nonconcurrent operation).
  - Supports 3x3 multiple input, multiple output (MIMO).
  - Supports speeds of up to 450 Mbps for 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption that complies with the 802.3af standard.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNDAP620*.
- **WNDAP380R ProSAFE Dual Band Wireless-N Access Point with RFID support**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 10.51W.
  - Accepts an RFID module for support of RFID devices and tags.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNDAP380R*.

1. The WNDAP620 is not supported on models WC7500 and WC7600v2.

- **WNDAP360 ProSAFE Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 10.51W.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNDAP360*.
- **WNDAP350 ProSAFE Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Operates concurrently in the 2.4 GHz and 5 GHz radio bands.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 10.75W.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNDAP350*.
- **WNAP320 ProSAFE Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices.
  - Operates in the 2.4 GHz radio band.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W.
  - Accepts optional antennas.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNAP320*.
- **WNAP210v2 ProSAFE Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices.
  - Operates in the 2.4 GHz radio band.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W.
  - Operates in the 2.4 GHz radio band.

  For product documentation and firmware, visit *http://support.netgear.com/product/WNAP210*.

  Note: The WNAP210v1 cannot function in a wireless controller system, but the WNAP210v2 can.

Supported NETGEAR Antennas

A wireless controller system supports the following antennas:

- **ANT2409 ProSAFE Indoor/Outdoor 9 dBi Omni-directional Antenna**
  - 9 dBi omni-directional antenna for indoor or outdoor use
  - WiFi signal 802.11g
  - Frequency range 2400–2485 MHz
  - Maximum range 11.5 km (7.2 miles)
  - Polarization vertical

  For product documentation and firmware, visit *http://support.netgear.com/product/ANT2409v2*.
- **ANT224D10 ProSAFE 10 dBi 2x2 Indoor/Outdoor Directional Antenna**
  - 10 dBi directional antenna for indoor or outdoor use
  - WiFi signal 802.11n
  - Frequency range 2400–2500 MHz
  - Maximum range 8.5 km (5.28 miles)
  - Polarization linear; vertical

  For product documentation and firmware, visit *http://support.netgear.com/product/ANT224*.

System Planning and Deployment Scenarios

3

This chapter includes the following sections:

- *Basic and Advanced Setting Concepts*
- *Profile Group Concepts*
- *System Planning Concepts*
- *High-Level Configuration Examples*
- *Management VLAN and Data VLAN Strategies*
- *High-Level Deployment Scenarios*

Basic and Advanced Setting Concepts

You can deploy the wireless controller in a small WiFi network with 10 or 20 access points or in a large WiFi network with up to 600 access points. Small networks require a basic configuration, but large networks can become 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 few service set identifiers (SSIDs, or network names).
- **Advanced settings for access point profile groups**. In a large WiFi network, or if 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 maintains its own network. Larger networks could require multiple access point profile groups to allow different policies per building or department. The access points could support different security profiles per building and department, for example, one for guests, one for management, and one for sales.

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 Configuration > Security > Basic submenu on the left and the Configuration > Security > Advanced submenu on the right:

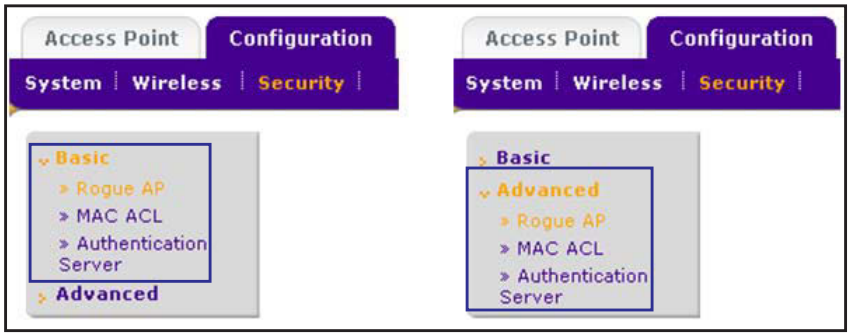


Figure 10. Basic and advanced submenus

Before you start the configuration of your wireless controller, decide whether you can use a basic configuration (that is, follow the Basic submenus) or must use an advanced configuration (that is, follow the Advanced submenus). Once you make your choice, configuring the wireless controller can be fairly easy if you consistently follow either the Basic submenus or the Advanced submenus.

Profile Group Concepts

Each access point can support up to eight 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 supports 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 eight security profiles (16 for dual-band access points).

After you use the automatic discovery process and add 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 eight access point profile groups. Each group includes all the settings that are required to configure a fully functional access point with up to eight security profiles (16 for dual-band access points).

For example, if your company site includes four buildings, each with a different WiFi 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 WiFi 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):

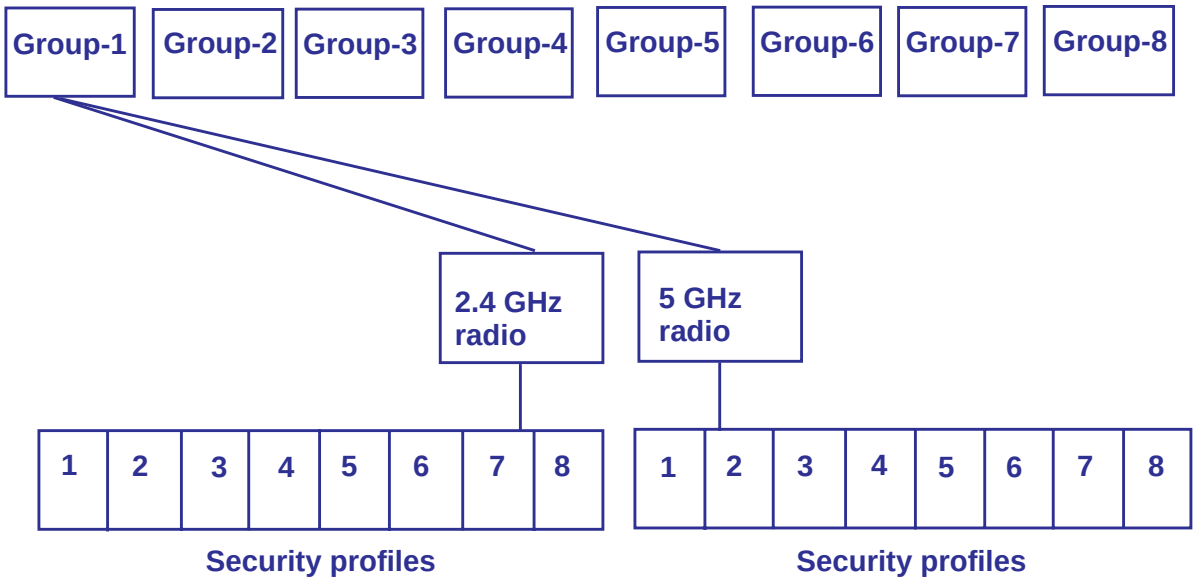


Figure 11. Advanced profile group architecture

The following figure shows an example of three access point profile groups, in which the first profile group (Group-1) supports five 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 must create the other profiles groups.)

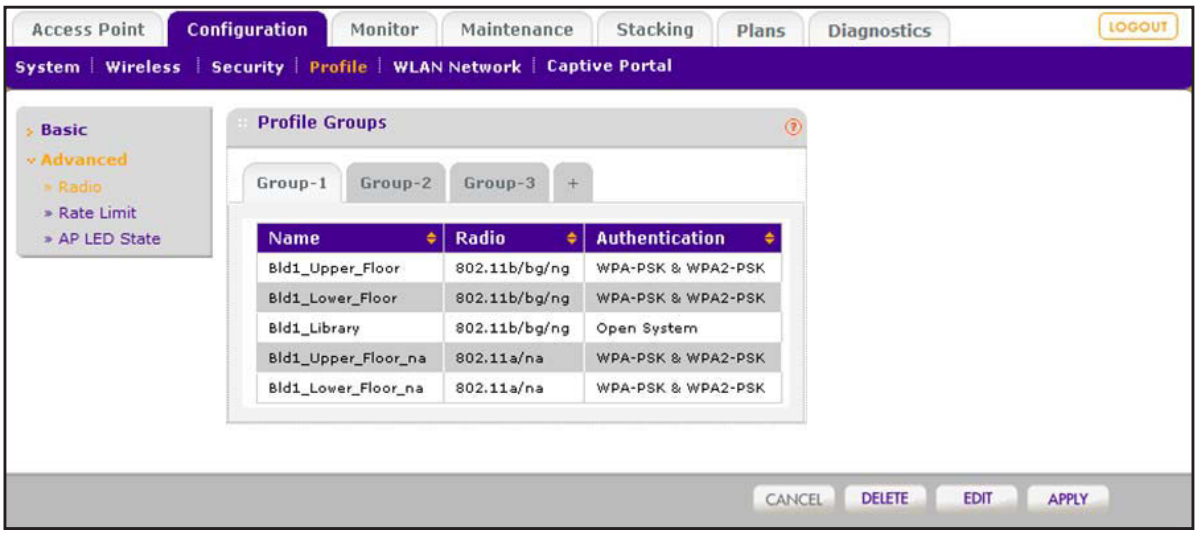


Figure 12. Example of profile groups with security profiles

System Planning Concepts

This section includes the following subsections:

- *Preinstallation Planning*
- *Before You Configure a Wireless Controller*

Preinstallation Planning

Before you install any wireless controllers, determine the following:

- Number of access points required to provide seamless coverage
- Number of licenses required to cover all access points that must be managed
- Number of wireless controllers required
- 802.11 frequency band and the channels that are optimal for WiFi usage

We recommend that you perform a site survey:

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

Before You Configure a Wireless Controller

These sections assume that you 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 *ProSAFE Wireless Controller Installation Guide* that you can download from *http://support.netgear.com/product/WC9500*.

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

Management VLAN

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 did not configure a tagged VLAN with the same VLAN ID on the hubs and switches in your network, IP connectivity might be lost.

The management VLAN must provide IP connectivity between the wireless controller and the access points. If the wireless controller and the access points are on different management VLANs, external VLAN routing must allow IP connectivity between the wireless controller and the access points.

For information about how to configure management VLANs, see *Manage the IP, VLAN, and Link Aggregation Settings* on page 101.

Client VLANs

Each authenticated WiFi 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 WiFi users into the single VLAN that is specified in the basic security profile, the wireless controller allows you to group WiFi users into separate VLANs based on the WiFi 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 must create different security profiles.

For information about how to configure regular VLANs, see *Manage the IP, VLAN, and Link Aggregation Settings* on page 101.

DHCP Server

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

Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 (vendor-specific information) with the IP address of the wireless controller. Whether you must enable option 43 on an *external* DHCP server in a Layer 2 network depends on the firmware version that the wireless controller is running:

- **Firmware version 4.x and earlier versions**. Option 43 must be enabled on an *external* DHCP server in a Layer 2 network.
- **Firmware version 5.x and later versions**. Option 43 is not required on an *external* DHCP server in a Layer 2 network.

For discovery across Layer 3 networks, you always must enable option 43 on an *external* DHCP server.

Client Authentication and Data Encryption

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

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

Table 7. 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: • External RADIUS server • Internal authentication server • External LDAP server
WPA2	AES or TKIP+AES	One of the following authentication servers: • External RADIUS server • Internal authentication server • External LDAP server
WPA and WPA2	TKIP+AES	One of the following authentication servers: • External RADIUS server • Internal authentication server • External LDAP server

For information about how to configure client authentication, data encryption, and authentication servers, see *Chapter 7, Manage Security Profiles and Profile Groups*.

High-Level Configuration Examples

This section includes the following subsections:

- *Single Controller Configuration With Basic Profile Group*
- *Single Controller Configuration With Advanced Profile Groups*
- *Stacked Controller Configuration*

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.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight profiles, and for each profile, do at least the following:	
	1. Configure an SSID for WiFi access.	**Configuration > Profile > Basic**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Basic > Authentication Server**
3.	Run the Discovery Wizard and add the access points to the managed access point list.	**Access Point > Discovery Wizard**

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.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight access point profile *groups*, and for each access point profile in a group, do at least the following:	
	1. Configure an SSID for WiFi access.	**Configuration > Profile > Advanced**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Advanced > Authentication Server**
3.	Run the Discovery Wizard and add the access points to the managed access point list.	**Access Point > Discovery Wizard**
4.	Assign the access points to the access point profile *groups* (also referred to as WLAN groups).	**Configuration > WLAN Network**

Stacked Controller Configuration

A stacked controller configuration can consist of up to three wireless controllers and up to 600 access points.

Note: If the stack members are on different floors or in different buildings, you could configure a separate access point profile group for each building or floor.

➢ **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, configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure the master wireless controller and deploy it in the network. Configure up to eight access point profile *groups*, and for each access point profile in a group, do at least the following:	
	1. Configure an SSID for WiFi access.	**Configuration > Profile > Advanced**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Advanced > Authentication Server**

Step	Configuration	Web Management Interface Path
3.	Configure the slave wireless controllers and deploy them in the network. For each slave wireless controller, configure up to eight access point profile *groups*, and for each access point profile in a group, do at least the following:	
	1. Configure an SSID for WiFi access.	**Configuration > Profile > Advanced**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Advanced > Authentication Server**
4.	Interconnect the wireless controllers that you intend to make members of the stack. The connection must 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 master controller.	**Stacking > Stacking**
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, we recommend that you set up at least two VLAN groups: a management VLAN group and a data VLAN group. If your network is large, we recommend that you create a number of data VLAN groups. Setting up data VLANs for clients allows you to do the following:

- 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.

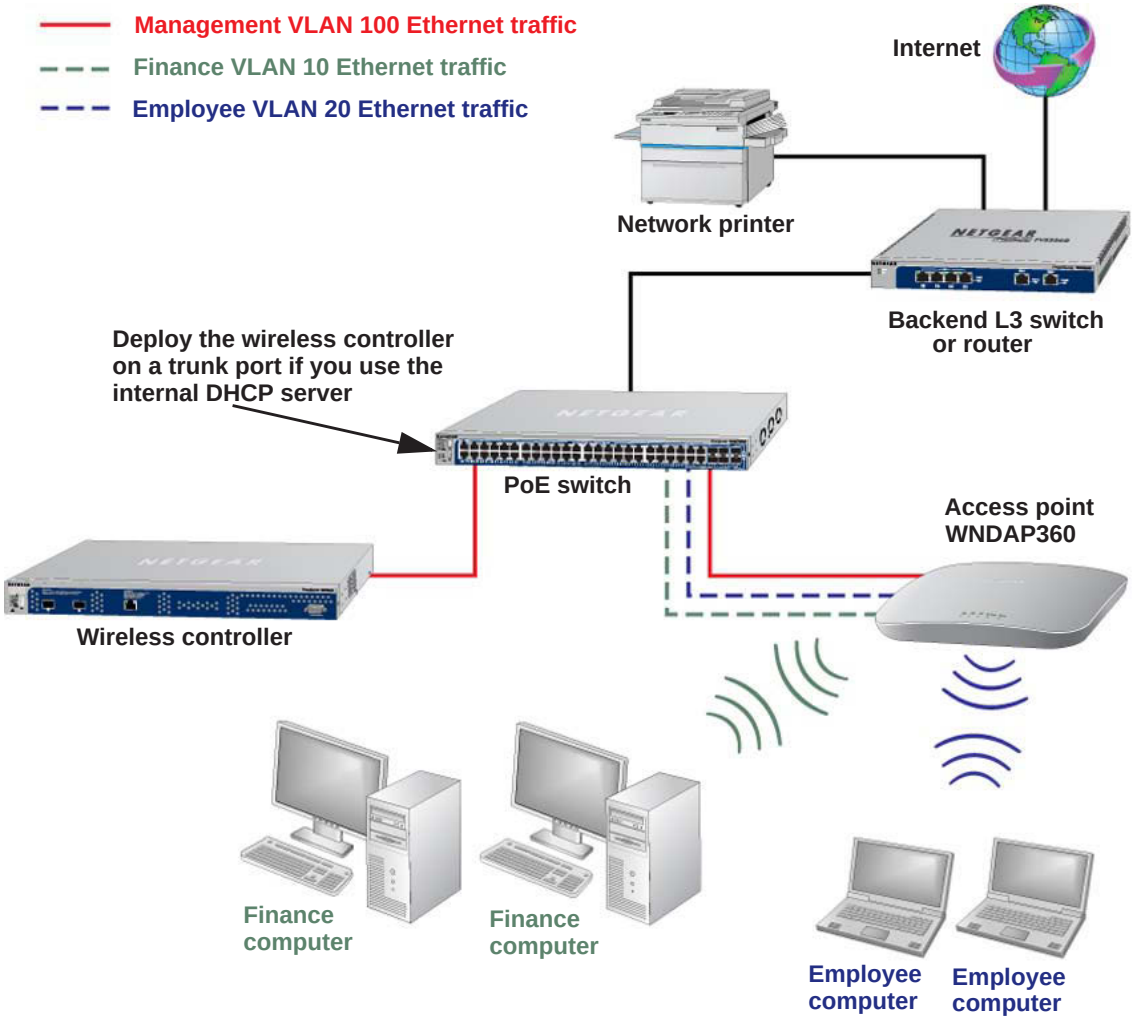


Figure 13. Example: Use VLANs to segregate traffic by user categories

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 flooding occurs and the wireless controller is not able to exchange packets with the access points, the network performance can slow down, and the access points can lose their connectivity with the wireless controller.

If you use the internal DHCP server of the wireless controller, deploy the wireless controller on a trunk port on your switch. The trunk port must provide access to all VLANs.
To accommodate the traffic load of the trunk, use a high-speed port on your switch as the trunk port. If you use an external DHCP server, you do not need to deploy the wireless controller on a trunk port on your switch.

High-Level Deployment Scenarios

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

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

Scenario Example 1: 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.

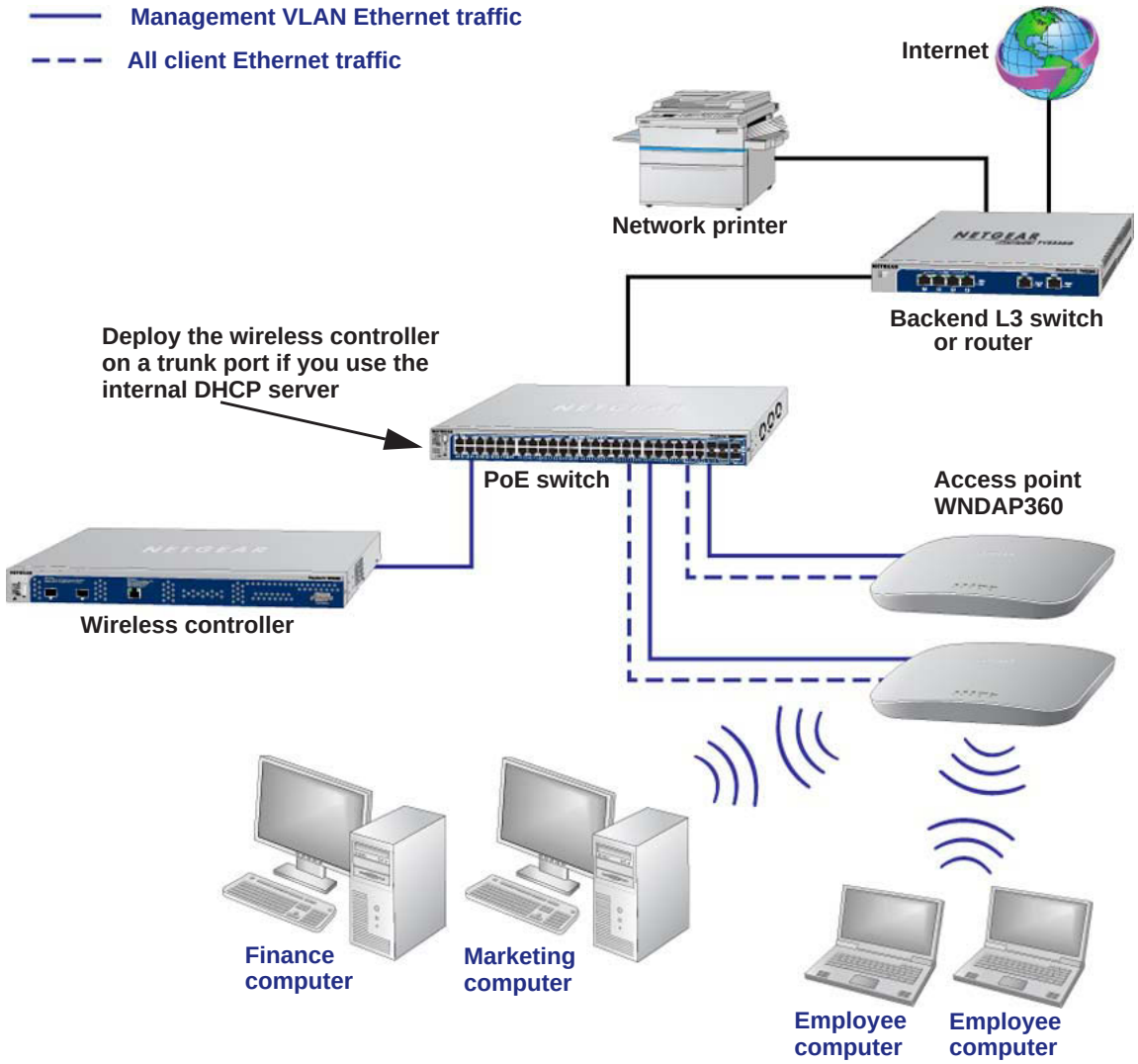


Figure 14. Example: Basic network with a single VLAN

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. The configuration does not include any 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.

➢ **To provision the wireless controller:**

Step	Configuration	Web Management Interface Path
1.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight profiles, and for each profile, do at least the following:	
	1. Configure an SSID for WiFi access.	**Configuration > Profile > Basic**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Basic > Authentication Server**
3.	Use any port of the wireless controller to connect the WiFi PoE switch.	
4.	Deploy the access points and connect them to the same WiFi PoE switch.	

Step	Configuration	Web Management Interface Path
5.	When the access points are operating, open the Discovery Wizard to do the following:	Access Point > Discovery Wizard
	1. Specify the state of the access points. The state can be either factory default in a Layer 2 network or already installed and functioning in standalone mode.	
	2. Run the Discovery Wizard.	
	3. Select the access points that you want the wireless controller to manage and add them to the managed list. **Note:** 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 WiFi QoS) are applied to the access points.	

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. The wireless controller system includes the following VLANs:

- 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

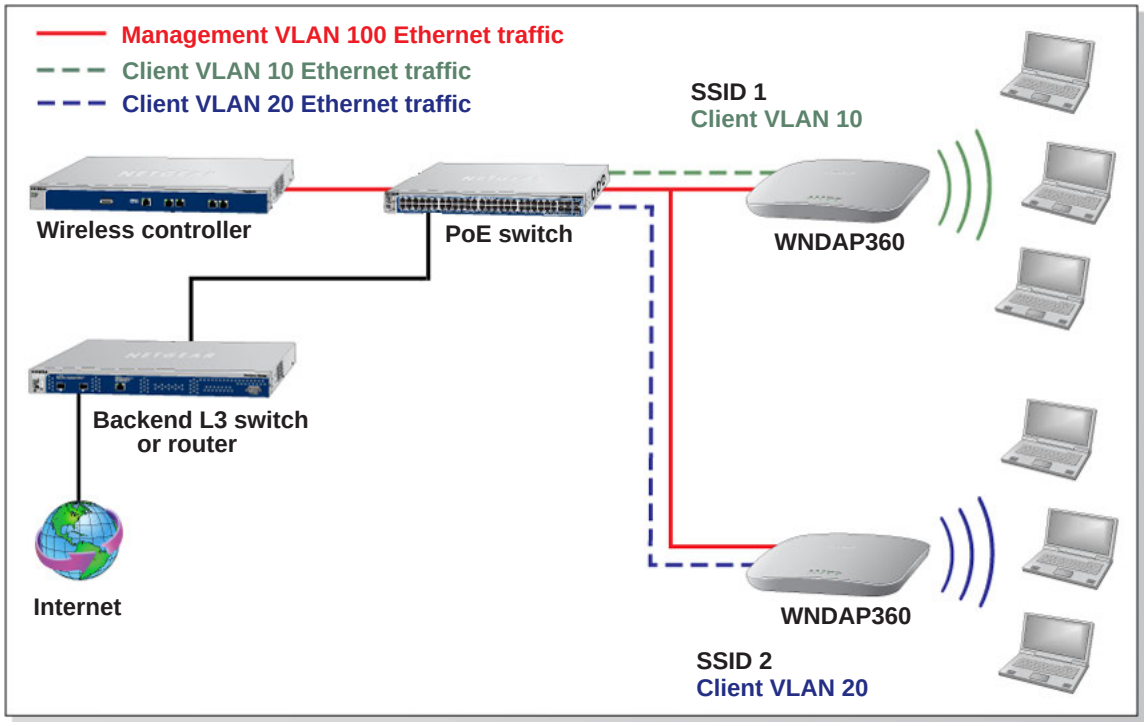


Figure 15. Example: Advanced network with VLANs and SSIDs

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. The configuration does not include any 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 Layer 3 switch or router that provides Internet access.

This network configuration requires the following conditions:

- VLANs 10, 20, and 100 are tagged VLANs and are configured on 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.

➢ **To provision 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 time settings.	**Configuration > System > Time**
	3. Configure the IP address of wireless controller.	**Configuration > System > IP/VLAN**
	4. For initial discovery and configuration of the access points, temporarily configure management VLAN 100 as an untagged management VLAN on the wireless controller.	
	5. Change default VLAN 1 to a tagged VLAN.	
2.	For initial discovery and configuration of the access points, temporarily configure management VLAN 100 as an untagged management on the PoE switch.	
3.	Configure either the network's DHCP server or the wireless controller's DHCP server to use VLAN 100. If you use the wireless controller's DHCP server:	
	1. Configure the IP address range for VLAN 100.	**Configuration > System > DHCP Server**
	2. Configure the other DHCP server fields, including the gateway and DNS servers.	

Step	Configuration	Web Management Interface Path
4.	Configure the following profiles, and configure network authentication and data encryption for these profiles:	
	1. A profile with SSID 1 and VLAN 10.	**Configuration > Profile > Basic**
	2. A profile with SSID 2 and VLAN 20.	
	3. If necessary for the selected network authentication options, configure one or more authentication servers.	**Configuration > Security > Basic > Authentication Server**
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.	When the access points are operating, open the Discovery Wizard to do the following:	**Access Point > Discovery Wizard**
	1. Specify the state of the access points, which is factory default in a Layer 2 network.	
	2. Run the Discovery Wizard.	
	3. Select the access points that you want the wireless controller to manage and add them to the managed list. **Note:** By adding the access points to managed list, you enable them to receive an IP address from the DHCP server over management VLAN 100.	
9.	For each access point on the managed list, disable the untagged VLAN 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[1], 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
- Fifty access points (managed by the wireless controller through management VLAN 1)

1. Model WC7500 does not support controller redundancy.

- 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

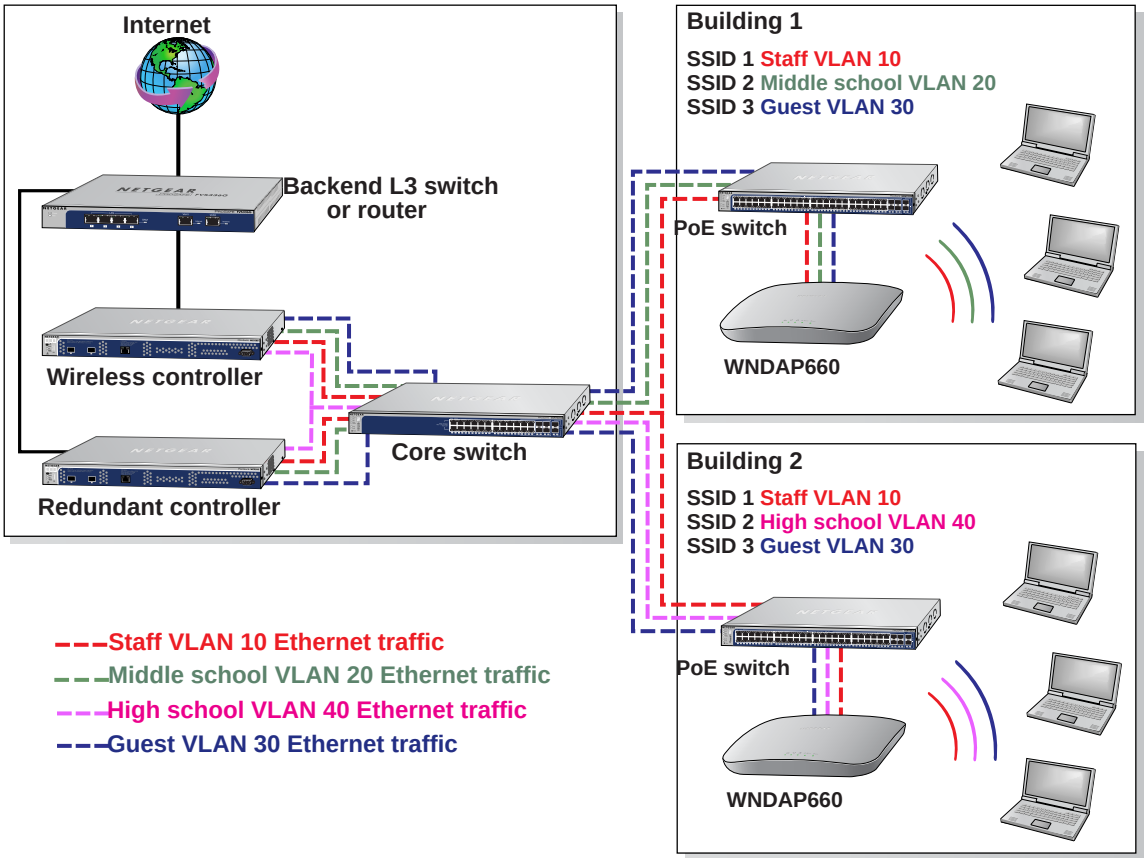


Figure 16. Example: Advanced network with redundancy

The access points and wireless controllers are connected in the same subnet and the 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.

This network configuration requires the following conditions:

- 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.

➢ **To provision 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 time settings.	**Configuration > System > Time**
	3. Configure the IP address of wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure the following profiles, and configure network authentication and data encryption for these profiles:	
	1. A profile with SSID 1 and VLAN 10.	**Configuration > Profile > Basic**
	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.	
	5. If necessary for the selected network authentication options, configure one or more authentication servers.	**Configuration > Security > Basic > Authentication Server**
3.	Configure the following profile groups:	
	1. A profile group with the name Building 1, to which you add the following profiles: - The profile with SSID 1 and VLAN 10 - The profile with SSID 2 and VLAN 20 - The profile with SSID 2 and VLAN 30	**Configuration > Profile > Advanced**
	2. A profile group with the name Building 2, to which you add the following profiles: - The profile with SSID 1 and VLAN 10 - The profile with SSID 2 and VLAN 30 - The profile with SSID 3 and VLAN 40	
4.	Deploy the access points and connect them to PoE switches.	

Step	Configuration	Web Management Interface Path
5.	When the access points are operating, open the Discovery Wizard to do the following: 1. Specify the state of the access points, which is the factory default state in a Layer 2 network. 2. Run the Discovery Wizard. 3. Select and add the access points that you want to be managed by the wireless controller to the managed list. **Note:** By default, all access points are added to the basic group.	**Access Point > Discovery Wizard**
6.	Assign the access points to the access point profile *groups* (also referred to as WLAN groups) Building 1 and Building 2.	**Configuration > WLAN Network**

RF Planning and Deployment

4

This chapter includes the following sections:

- *Application, Browser, and Port Requirements for RF Planning*
- *RF Planning Overview*
- *Manage a Building and Floors for an RF Plan*
- *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor*
- *Manually Add and Manage Access Points on a Floor Map for an RF Plan*
- *Manually Add and Manage Antennas on a Floor Map for an RF Plan*
- *Display and Recalculate the WiFi Coverage for a Heat Map*
- *Display or Change the WiFi Inventory for an RF Plan*
- *Download a Report for an RF Plan*
- *View the Heat Map for a Deployed Floor Plan*

Application, Browser, and Port Requirements for RF Planning

For you to be able to access the RF planning pages in the web management interface, make sure that your computer can run Adobe Flash Player and that Java is enabled in your browser. If you get a Java security warning, add an exception.

To display the RF planning pages, you might need to refresh your browser's cache. For most browsers, to refresh the cache, press the **F5** key.

For remote access (that is, access over a WAN interface) to the RF planning pages, specific ports must be open your computer's firewall:

- For remote HTTPS access, make sure that ports 4430 and 8443 are open.
- For remote HTTP access, make sure that ports 80 and 8080 are open.

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 a coverage hole and add additional access points to mitigate the situation.

RF planning provides a view of each floor in a building, allowing you to specify how WiFi coverage must be provided. RF planning then provides coverage maps and access point placement locations.

For deployed RF plans, real-time calibration lets you visualize the indoor propagation of RF signals to identify areas with a weak signal or dead spots and add additional access points in the right location to mitigate the weak signal or dead spots.

Note: In a stacking configuration, RF planning is accessible only from the master controller. The access points that are controlled by the slave controllers are displayed in the web management interface of the master controller. These access point are displayed in the default building (Building-1) on the default floor (Floor-1) of the master controller.

Note: In a redundancy group, after a failover occurs to a redundant controller, RF planning is no longer accessible. Only after a switchback to the primary controller occurs, RF planning becomes available again.

Planning Requirements

To expedite your planning efforts, collect the information that is listed in *Table 8* and *Table 9* before you use RF planning.

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

Table 8. Building planning table

Item	Your Information
Building length	
Building width	
Building height	
Number of floors	
Distance in height between floors	

Use a worksheet similar to the following table to collect your information for each floor in the building.

Table 9. Floor planning table

Item	Your Information
Floor dimensions if different from building dimensions	
Length	
Width	
Height	
Define WiFi coverage and noncoverage areas	
WiFi coverage areas	
WiFi noncoverage areas	
WiFi building obstacles	
Dry walls	
Wood walls	
Plastic walls	
Glass walls	

Table 9. Floor planning table (continued)

Item	Your Information
Brick walls	
Concrete walls	
Light doors	
Metal doors	
Heavy doors	
Thin windows	
Thick windows	
Other obstacles	
WiFi building obstruction areas	
Cubicle office areas	
Closed office areas	
Elevator shafts	
Warehouses with low-density stock	
Warehouses with medium-density stock	
Warehouses with high-density stock	
WiFi client information	
Total number of expected clients on floor	
Expected number of clients per access point	
WiFi radio band or bands	
Access point protocol for each WiFi radio band	
2.4 GHz (802.11b/bg/ng)	
5 GHz (802.11a/na/ac)	
Access point transmission power (from full to minimum) for each WiFi radio band	
2.4 GHz	
5 GHz	
WiFi coverage and signal strength	
WiFi coverage percentage	
Minimum required signal strength in dBm	

Recommended RF Planning Procedure for a Building

We recommend that you first set up your building and floors to scale and define the floor plans. For more information, see *Manage a Building and Floors for an RF Plan* on page 55.

Then, for each floor, perform the following tasks:

- Use the WiFi Auto Planning Advisor

  See *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69.
- (Optional) Manually add and fine-tune access points on each floor.

  See *Manually Add and Manage Access Points on a Floor Map for an RF Plan* on page 75.
- (Optional) Manually add and fine-tune antennas.

  See *Manually Add and Manage Antennas on a Floor Map for an RF Plan* on page 78.
- (Optional) Display the WiFi coverage.

  See *Display and Recalculate the WiFi Coverage for a Heat Map* on page 82.
- (Optional) Display and fine-tune the WiFi inventory.

  See *Display or Change the WiFi Inventory for an RF Plan* on page 83.
- (Optional) Download the report.

  See *Download a Report for an RF Plan* on page 86.

After you install or move the physical access points and antennas according to the RF plan for a floor, deploy the floor plan by placing the virtual access points at the virtual locations on the floor map to match the actual physical locations of the physical access points on the floor as closely as possible. Doing so enables you to generate a realistic heat map for the deployed floor plan.

For more information, see *View the Heat Map for a Deployed Floor Plan* on page 87.

Manage a Building and Floors for an RF Plan

This section describes how you can define a building and floors and make modifications after you define them.

Defining a floor includes the following main tasks:

- Uploading a custom floor map and setting dimensions (see *Add a Building and Floors* on page 56)
- If you do not set dimensions, scaling the floor (see *Scale a Floor* on page 59)
- Adding WiFi coverage zones and WiFi noncoverage zones (see *Add a WiFi Coverage or WiFi Noncoverage Zone to a Floor* on page 60)
- Adding WiFi building obstacles (see *Add a WiFi Building Obstacle to a Floor* on page 61)
- Adding WiFi obstruction areas (see *Add a WiFi Obstruction Area* on page 64)

Add a Building and Floors

The wireless controller includes a default building and default floor with a default floor map. You cannot remove the default building or default floor but you can replace the default floor map with a custom floor map.

You can add up to 30 buildings, each of which can include up to 20 floors. However, the total number of floors that the wireless controller can support is 128.

➢ **To add and define a building and floors:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

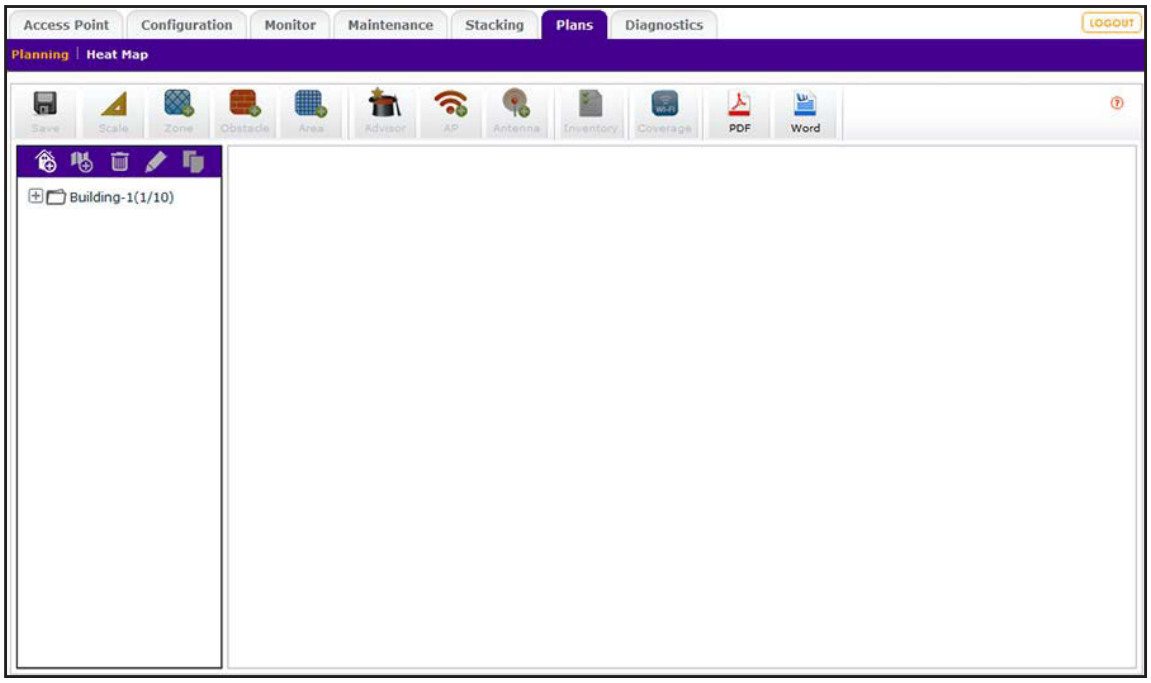
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.



5. To add a building, in the building tree on the left, click the **Add Building** icon.

   The Add Building pop-up window displays.

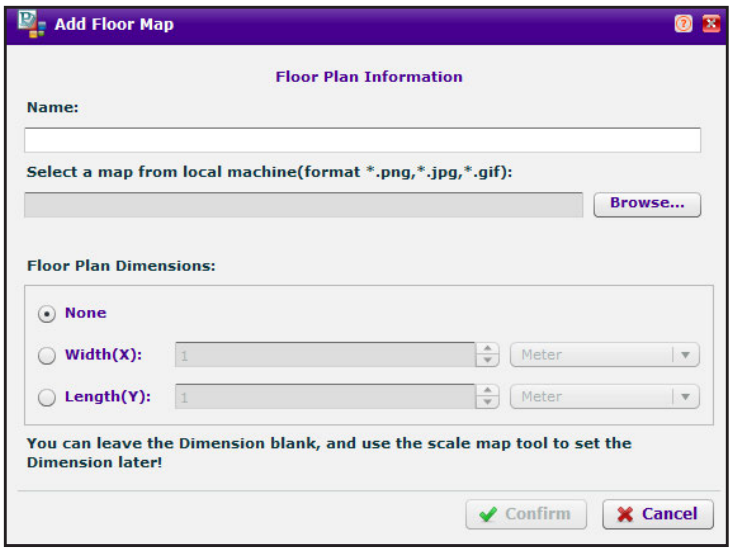
6. Enter a name for the building and click the **Confirm** button.
7. In the building tree, click the **+** icon of the building that you added.

The Floor-1 name displays. This default floor name was added automatically when you added the building.

8. Click **Floor-1**.

   The default floor map displays. This default floor map was added automatically when you added the building.

9. To add a custom floor map, click the **Add Floor** icon.



10. Define the floor:
    a. Enter a name for the floor.
    b. Upload a custom floor map by clicking the **Browse** button, following the directions of your browser to navigate to a floor map, and selecting the floor map.

       You can upload a plan in `.png`, `.jpg`, or `.gif` format.

    c. To either specify the floor width or the floor length, do the following:
       - To specify the floor width, click the **Width(X)** button, select **Meter** or **Feet** from the menu, and enter the floor width.
       - To specify the floor length, click the **Length(Y)** button, select **Meter** or **Feet** from the menu, and enter the floor length.

       Note: If you do not want to enter the length or width or the information is not available, you can scale the floor later (see *Scale a Floor* on page 59).

    d. Click the **Confirm** button.

       The floor map is uploaded and displays onscreen.

11. Click the **Save** icon.

    Your settings are saved.

12. To add another floor and floor map, repeat *Step 9* through *Step 11*.

Add a Single Floor to a Building

You can add a single floor to an existing building.

➢ **To add a single floor to a building:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

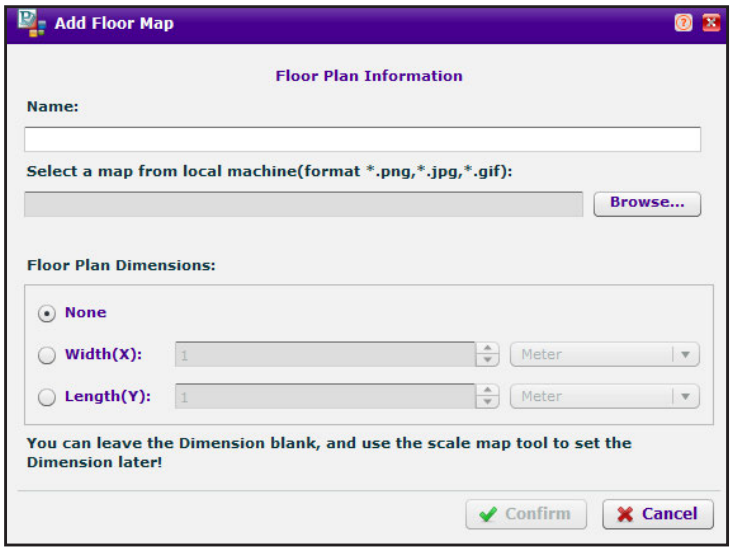
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the name of the building to which you are adding a floor.
6. Click the **Add Floor** icon.



7. Define the floor:
   a. Enter a name for the floor.
   b. Upload a custom floor map by clicking the **Browse** button, following the directions of your browser to navigate to a floor map, and selecting the floor map.

      You can upload a plan in `.png`, `.jpg`, or `.gif` format.

   c. To either specify the floor width or the floor length, do the following:
      - To specify the floor width, click the **Width(X)** button, select **Meter** or **Feet** from the menu, and enter the floor width.

- To specify the floor length, click the **Length(Y)** button, select **Meter** or **Feet** from the menu, and enter the floor length.

Note: If you do not want to enter the length or width or the information is not available, you can scale the floor later (see *Scale a Floor* on page 59).

d. Click the **Confirm** button.

The floor map is uploaded and displays onscreen.

8. Click the **Save** icon.

Your settings are saved.

Scale a Floor

If you did not specify the floor width or floor length while adding a new floor (see *Add a Building and Floors* on page 56 or *Add a Single Floor to a Building* on page 58), you can do so by scaling the floor. You must know the distance in meters or feet between two known points on the floor.

➢ **To scale a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Scale** icon.
8. Select a line between two points on the map by anchoring the line at one point and releasing the line at the other point.

   The points do not need to cover the entire length or width of the floor.

   The Scale Map pop-up window opens.

9. Select **Meter** or **Feet** from the menu and enter the distance between the two points.

10. Click the **Confirm** button.

    The floor map is scaled.

11. Click the **Save** icon.

    Your settings are saved.

Add a WiFi Coverage or WiFi Noncoverage Zone to a Floor

A WiFi coverage zone on a floor is an area in which access points must provide WiFi coverage. A WiFi noncoverage zone on a floor is an area in which access points do not need to provide WiFi coverage, for example, a storage area.

Note: Before you add a WiFi coverage or WiFi noncoverage zone, first define the floor dimensions (see *Add a Single Floor to a Building* on page 58) or scale the floor (see *Scale a Floor* on page 59).

➢ **To add a WiFi coverage or WiFi noncoverage zone to a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Zone** icon.
8. Click either the **Coverage Zone** icon or the **Non-AP Zone** icon.
9. Anchor a rectangle at one point on the floor map and define the WiFi coverage zone or the zone in which you do not need WiFi coverage.
10. To remove the zone, click the **Undo** link, and repeat *Step 7* though *Step 9*.
11. Click the **Save** icon.

    Your settings are saved.

12. To add another zone, repeat *Step 7* though *Step 11*.

Remove a WiFi Coverage or Noncoverage Zone From a Floor

After you add and save a WiFi coverage or noncoverage zone on a floor, you can remove it from the floor.

➢ **To remove a WiFi coverage area or WiFi noncoverage zone from a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Zone** icon.
8. Click the zone on the map.
9. Click the **Delete** link.
10. Click the **Save** icon.

    Your settings are saved.
11. To remove another zone, repeat *Step 7* though *Step 10*.

Add a WiFi Building Obstacle to a Floor

WiFi building obstacles can be any of the following predefined obstacles with their predefined attenuation factor (WiFi signal loss) in dB or a custom defined building obstacle:

- Dry wall (4 dB)
- Wood wall (4 dB)
- Plastic wall (4 dB)
- Glass wall (8 dB)
- Brick wall (8 dB)
- Concrete wall (12 dB)
- Light door (4 dB)

- Metal door (11 dB)
- Heavy door (15 dB)
- Thin window (2 dB)
- Thick window 4 dB)

These obstacles contribute to the WLAN signal degradation based on their construction materials and interferences.

Note: Before you add a building obstacle, first define the floor dimensions (see *Add a Single Floor to a Building* on page 58) or scale the floor (see *Scale a Floor* on page 59).

➢ **To add a WiFi building obstacle to a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Obstacle** icon.
8. Take one of the following actions:
   - Select the icon for one of the predefined obstacles.
   - Define a custom obstacle:
     a. Click the **Add Obstacle Type** link.

        The Add New Obstacle Type pop-up window opens.

     b. Enter a name.
     c. Enter the attenuation factor in dB.
     d. Select a color.
     e. Click the **Confirm** button.

f. Click the **Obstacle** icon.

g. Select the icon for the custom obstacle that you just added.

9. Select a line between two points on the map by anchoring the line at one point and releasing the line at the other point.
10. To remove the obstacle, click the **Undo** link, and repeat *Step 7* though *Step 9*.
11. Click the **Save** icon.

    Your settings are saved.
12. To add another obstacle repeat *Step 7* though *Step 11*.

Remove a Building Obstacle From a Floor

After you add and save a WiFi building obstacle on a floor, you can remove it from the floor.

➢ **To remove a WiFi building obstacle from a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Obstacle** icon.
8. Click the obstacle on the map.
9. Click the **Delete** link.
10. Click the **Save** icon.

    Your settings are saved.
11. To remove another obstacle, repeat *Step 7* though *Step 10*.

Add a WiFi Obstruction Area

WiFi obstructions areas can be any of the following predefined areas:

- Cubicle office area
- Closed office area
- Elevator shaft
- Warehouse stock with low density
- Warehouse stock with medium density
- Warehouse stock with high density

These areas contribute to the WLAN signal degradation based on openness (or lack thereof) and interferences.

Note: Before you add a WiFi obstruction area, first define the floor dimensions (see *Add a Single Floor to a Building* on page 58) or scale the floor (see *Scale a Floor* on page 59).

➢ **To add a WiFi obstruction area to a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Area** icon.
8. Anchor a rectangle at one point on the floor map and define the WiFi obstruction area.
9. To remove the area, click the **Undo** link, and repeat *Step 7* and *Step 8*.
10. Click the **Save** icon.

    Your settings are saved.
11. To add another area, repeat *Step 7* though *Step 10*.

Remove a WiFi Obstruction Area

After you add and save a WiFi obstruction area on a floor, you can remove it from the floor.

➢ **To remove a WiFi obstruction area from a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Area** icon.
8. Click the area on the map.
9. Click the **Delete** link.
10. Click the **Save** icon.

    Your settings are saved.
11. To remove another area, repeat *Step 7* though *Step 10*.

Change the Name, Map, or Dimensions of a Floor

You can change the basic properties of a floor, including those for the default floor.

➢ **To change the name, map, or dimensions of a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Edit** icon.

   A pop-up window opens and displays information about the floor plan.

8. Change the name or dimensions of the floor, upload another floor map, or perform a combination of these actions.

   For more information about the floor settings, see *Add a Single Floor to a Building* on page 58.

9. Click the **Confirm** button.

   Your settings are saved.

Change the Name of a Building

You can change only the name of a building, including the name of the default building. All other building properties are defined through the floors and the floor plans.

➢ **To change the name of a building:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the building name.
6. Click the **Edit** icon.

   A pop-up window opens.

7. Change the name.
8. Click the **Confirm** button.

   Your settings are saved.

Duplicate an Entire Building With All Floors

You can duplicate an entire building with all floors and floor plans, including all floor definitions. For information about duplicating a single floor in a building, see *Duplicate a Single Floor* on page 67.

➢ **To duplicate an entire building with all floors:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Layout**.

   The page displays the Planning icons.
5. In the building tree on the left, click the building name.
6. Click the **Duplicate** icon.

   A pop-up window opens.
7. Enter a name for the new building.
8. Click the **Confirm** button.

   The new building and floor or floors are added in the building tree.

Duplicate a Single Floor

You can duplicate a single floor and floor plan, including the floor definition. For information about duplicating an entire building with all floors, see *Duplicate an Entire Building With All Floors* on page 67.

➢ **To duplicate a single floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Layout**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click the **Duplicate** icon.

   A pop-up window opens.
8. Specify a name for the floor and select a building:
   a. Enter a name for the new floor.
   b. From the Workspace tree, select the building to which you want to add the new floor.
   c. Click the **Confirm** button.

      The new floor is added to the building.

Remove a Single Floor

You can remove a single floor from a building. However, you cannot remove the default floor of the default building.

➢ **To remove a single floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Layout**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Trashcan** icon.
8. Confirm the removal.

   The floor is removed.

Remove an Entire Building With All Its Floors

You can remove an entire building with all its floors. However, you cannot remove the default building.

➢ **To remove an entire building:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Layout**.

   The page displays the Planning icons.

5. In the building tree on the left, click the building name.
6. Click the **Trashcan** icon.
7. Confirm the removal.

   The building with all its floors is removed.

Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor

After you define a building and floors (see *Manage a Building and Floors for an RF Plan* on page 55), you can run the WiFi auto planning advisor for a floor. This tool calculates the number of access points and, optionally, antennas that you might need to provide WiFi coverage for your environment and suggests the best locations on the floor for these access points and antennas.

The WiFi auto planning advisor bases its calculations on the building and floor definitions and lets you enter the following parameters to determine the WiFi coverage for your environment:

- NETGEAR access point (see *Supported NETGEAR Access Points* on page 26)
- NETGEAR antenna (see *Supported NETGEAR Antennas* on page 30)
- For each WiFi band of a selected access point, the following parameters:
  - 802.11 protocol (depending on the access point, 802.11b/g/n, 802.11a/n/ac, or both)
  - Transmit power (from minimum power to full power)

  Note: The antenna gain and maximum number of supported clients for a selected access point are set automatically.

- Percentage of expected WiFi coverage (from 10 percent to 100 percent)
- The minimum required signal strength (from –95 dBm to –30 dBm)

  The signal strength determines the automatic channel allocation and automatic transmission power of the access points.
- The WiFi band (2.4 GHz or 5 GHz)
- The maximum number of clients that must be supported on the floor

For you to determine the expected financial investment, the WiFi auto planning advisor also lets you enter a price for the selected access point and a price for the selected antenna. Whether or not you enter a price, the WiFi auto planning advisor generates an inventory list. For more information, see *Display or Change the WiFi Inventory for an RF Plan* on page 83.

The WiFi auto planning advisor creates a heat map for the 2.4 GHz band, the 5 GHz band, or for both bands. To optimize the WLAN network coverage and throughput for your RF plan, you can manually fine-tune the placement of access points and antennas on the floor map.

For more information about adding and managing access points and antennas on a floor map, see the following sections:

- *Manually Add and Manage Access Points on a Floor Map for an RF Plan* on page 75
- *Manually Add and Manage Antennas on a Floor Map for an RF Plan* on page 78

WARNING:

For each floor, you can save one floor map only. When you run the WiFi auto planning advisor for a floor, the advisor removes all previously placed access points and antennas from the floor map.

➢ **To run the WiFi auto planning advisor and generate an RF plan and heat map for a floor:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

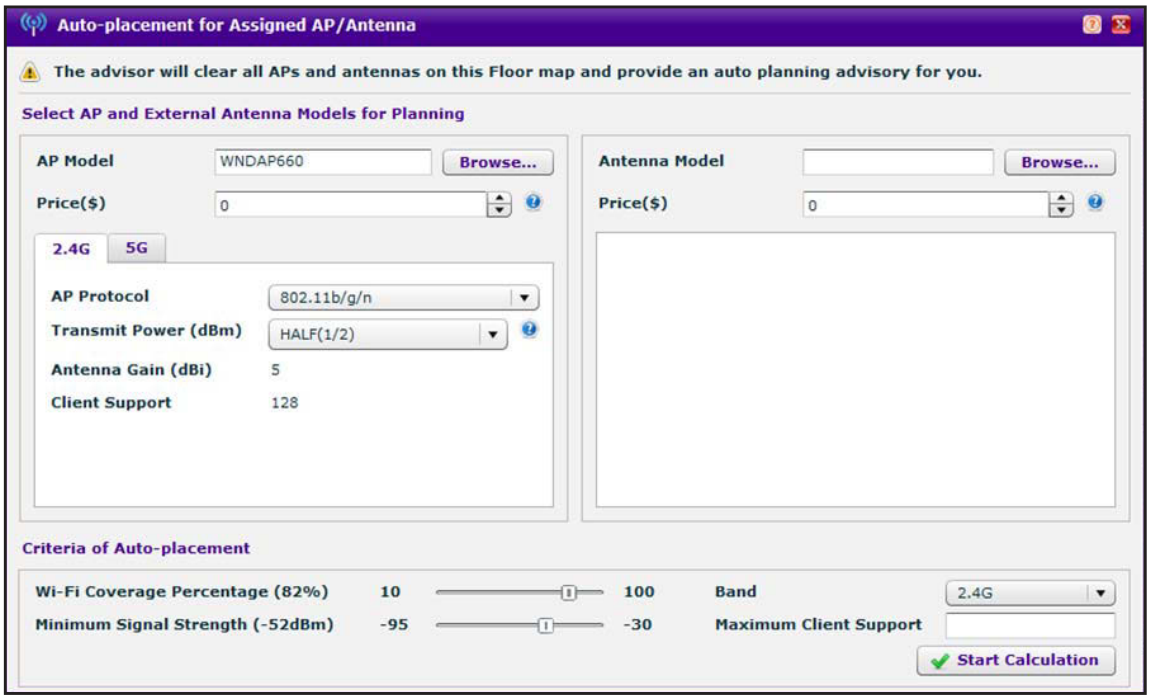
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Advisor** icon.



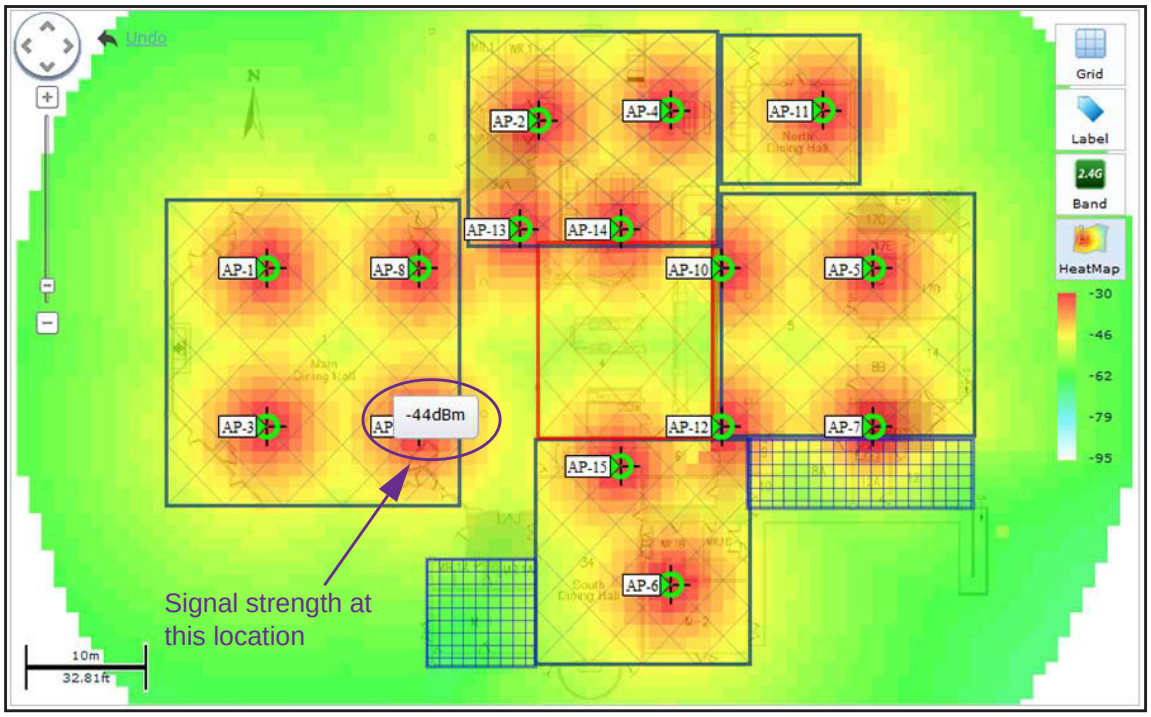
8. Specify the WLAN requirements for the floor as described in the following table.

Setting	Description
Select AP and External Antenna for Planning	
AP Model	Specify the access point that you intend to use for the floor: 1. Click the **Browse** button. The access points that the wireless controller supports display in a pop-up window. 2. Click the access point. All calculations are performed with the selected access point. 3. Click the **Confirm** button. The changes are saved and the pop-up window closes.
Price($)	As an option, enter the price of the access point.
2.4G	For the 2.4 GHz band, specify the transmission power in dBm for the access point. From the **Transmit Power (dBm)** menu, select **FULL**, **HALF(1/2)**, **QUARTER(1/4)**, **EIGHT(1/8)**, or **MINIMUM(1/16)**. The default setting is **HALF(1/2)**. **Note:** When you select an access point, the **AP Protocol**, **Antenna Gain (dBi)**, and **Client Support** fields are populated automatically.
5G	If the selected access point supports the 5 GHz band, specify the transmission power in dBm for the access point. From the **Transmit Power (dBm)** menu, select **FULL**, **HALF(1/2)**, **QUARTER(1/4)**, **EIGHT(1/8)**, or **MINIMUM(1/16)**. The default setting is **HALF(1/2)**. **Note:** When you select an access point, the **AP Protocol**, **Antenna Gain (dBi)**, and **Client Support** fields are populated automatically.
Antenna Model	Specify the antenna that you intend to use for the floor: 1. Click the **Browse** button. The antennas that the wireless controller supports for the selected access point display in a pop-up window. 2. Click the antenna. All calculations are performed with the selected antenna. 3. Click the **Confirm** button. The changes are saved and the pop-up window closes.
Price($)	As an option, enter the price of the antenna.

Setting	Description
Criteria of Auto-placement	
Wi-Fi Coverage Percentage	Move the slider to the required WiFi coverage. The minimum coverage is 10 percent; The maximum coverage is 100 percent. Base the WiFi coverage on the following components: • The required bandwidth for each connection in the covered area • The required aggregated throughput for the covered area • The required aggregated bandwidth for the covered area A small area allows you better coverage control than a large area. You might need to set the WiFi coverage percentage for the 2.4 GHz and 5 GHz bands separately. **Note:** To prevent packet loss and allow for seamless roaming between covered areas, configure moderate overlap of the covered areas and make sure that access points in overlapping areas do not use the same channels.
Minimum Signal Strength	Move the slider to the minimum required signal strength. The maximum signal quality is –30 percent; The minimum signal quality is –95 percent. The required signal strength for good coverage depends on the type of WiFi devices and applications in the network. The edge of a coverage area for an access point is based on the signal strength and signal-to-noise ratio (SNR), measured as a WiFi device moves away from the access point. **Note:** For voice applications, We recommend a minimum WiFi signal strength of -67 dBm and a minimum SNR of 25 dB.
Band	From the **Band** menu, select **2.4G** or **5G**. If the selected access point does not support the 5 GHz band, the menu selection is automatically set to **2.4G**.
Maximum Clients Supported	Enter the total number of clients that must be supported simultaneously on the floor.

9. Click the **Start Calculation** button.

   The WiFi auto planning advisor starts its calculations, displays the progress in a pop-up window, and generates a heat map.



The WiFi auto planning advisor generates a heat map that suggests the required number of access points (15 in the figure) and the locations on the floor map to achieve the optimum WiFi coverage that is based on the WLAN requirements that you specified (see *Step 8*).

10. To see the signal strength at a location on the floor map, point to the location (-44dBm at the location in the figure).
11. To switch the heat map to the 2.4 GHz or 5 GHz band, on the right, click the **Band** icon.

    The **Band** icon displays **2.4G** if the heat map for the 2.4 GHz band is shown. The **Band** icon displays **5G** if the heat map for the 5 GHz band is shown.
12. To move an access point to another location on the floor map, drag the access point to a location on the floor map.

    Note: Moving an access point turns off the heat map.
13. To move an antenna to another location on the floor map, drag the antenna to a location on the floor map.

    Note: Moving an antenna turns off the heat map.
14. To regenerate the heat map, on the right, click the **HeatMap** icon.

    The heat map is generated and displays. Use the color information on the right as guidance for WiFi coverage.
15. To show the map with or without grid, on the right side, click the **Grid** icon.

16. To show the access points by model or without a label, on the right side, click the **Label** icon and select your preference.

    By default, the access point name is shown. Because this section describes an RF plan that is not yet deployed, the IP address and channel cannot be displayed on the map.

17. To save the floor map with its new configuration, click the **Save** icon.

    The settings are saved.

Manually Add and Manage Access Points on a Floor Map for an RF Plan

You can add individual access points to a floor map for an RF plan. These access points do not need to be of the same model. After adding access points, you can change their properties, move them to another location on the floor map, or remove them from the floor map.

Note: Before you add any access points to a floor plan, first define the floor dimensions (see *Add a Single Floor to a Building* on page 58) or scale the floor (see *Scale a Floor* on page 59) and define the WiFi coverage zone (see *Add a WiFi Coverage or WiFi Noncoverage Zone to a Floor* on page 60).

➢ **To manually add and manage individual access points on a floor map for an RF plan:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

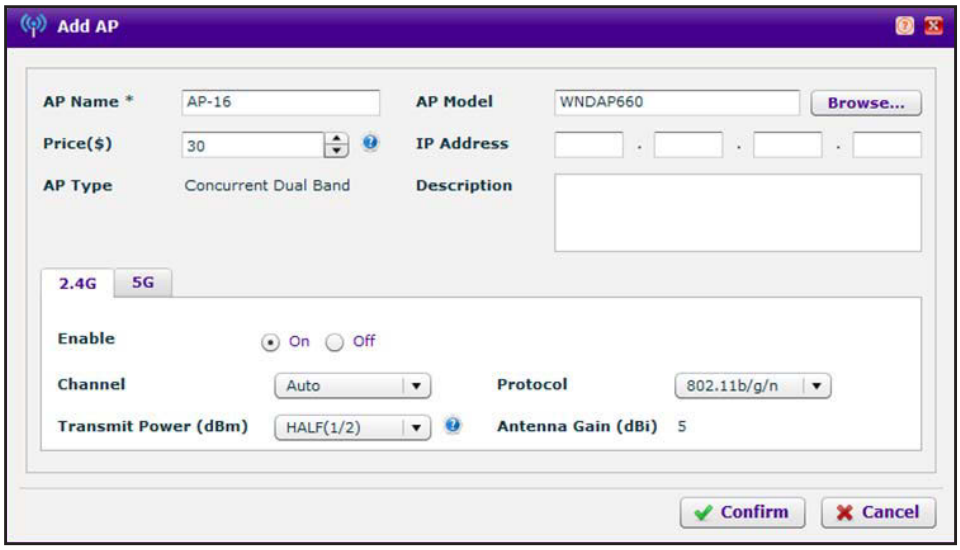
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **AP** icon.



8. Specify the access point settings as described in the following table.

Setting	Description
AP name	Enter a name for the access point. By default, the access points are numbered, for example, AP-16.
AP Model	Specify the access point that you intend to use for the floor: 1. Click the **Browse** button. The access points that the wireless controller supports display in a pop-up window. 2. Click the access point. All calculations are performed with the selected access point. 3. Click the **Confirm** button. The changes are saved and the pop-up window closes.
Price($)	As an option, enter the price of the access point.
IP Address	As an option, enter the IP address of the access point. **Note:** If your network uses a DHCP server and a deployed access point receives an IP address automatically, you can enter any IP address. If you intend to assign a static IP address to a deployed access point, enter the IP address that you want to set aside for the access point.
AP Type	When you select an access point, this field is populated automatically.
Description	As an option, enter a description for the access point.

Setting	Description
2.4G	Specify the settings for the 2.4 GHz band: • **Enable**. By default, the **On** radio button is selected and the 2.4 GHz band is enabled. To disable the 2.4 GHz band, select the **Off** radio button. • **Channel**. Leave the default selection **Auto** to enable the access point to select a channel automatically, or select a specific channel from the menu. • **Protocol**. When you select an access point, this field is populated automatically. • **Transmission Power (dBm)**. From the menu, select **FULL**, **HALF(1/2)**, **QUARTER(1/4)**, **EIGHT(1/8)**, or **MINIMUM(1/16)**. The default setting is **HALF(1/2)**. • **Antenna Gain (dBi)**. When you select an access point, this field is populated automatically.
5G	If the selected access point supports the 5 GHz band, specify the settings for the 5 GHz band: • **Enable**. By default, the **On** radio button is selected and the 5 GHz band is enabled. To disable the 5 GHz band, select the **Off** radio button. • **Channel**. Leave the default selection **Auto** to enable the access point to select a channel automatically, or select a specific channel from the menu. • **Protocol**. When you select an access point, this field is populated automatically. • **Transmission Power (dBm)**. From the menu, select **FULL**, **HALF(1/2)**, **QUARTER(1/4)**, **EIGHT(1/8)**, or **MINIMUM(1/16)**. The default setting is **HALF(1/2)**. • **Antenna Gain (dBi)**. When you select an access point, this field is populated automatically.

9. Click the **Confirm** button.

   The changes are saved and the pop-up window closes.

   The new access point is placed at the top of the floor map.

10. Move the access point to the desired location on the floor map by dragging the access point to a location on the floor map.
11. To change the properties for an access point, do the following:
    a. Double-click the access point.

       A pop-up menu displays.

    b. From the pop-menu, select **Edit Properties**.

       The Edit AP pop-up window opens. This window is identical to the Add AP pop-up window.

    c. Change the properties.

       For information about the properties, see the previous table.

    d. Click the **Confirm** button.

       The changes are saved and the pop-up window closes.
12. To remove an existing access point from the floor map, do the following:
    a. Click the access point to select it.
    b. Click the **Delete** link.

13. To add another access point to the floor map, change the properties for another access point, move another access point on the floor map, remove another access point from the floor map, or perform a combination of these tasks, repeat *Step 7* through *Step 12*.
14. To turn the heat map on or off, on the right, click the **HeatMap** icon.

    If you turn on the heat map, the heat map is generated and displays. Use the color information on the right as guidance for WiFi coverage.

    Note: Adding or removing access points changes the heat map.
15. To switch the heat map to the 2.4 GHz or 5 GHz band, on the right, click the **Band** icon.

    The **Band** icon displays 2.4G if the heat map for the 2.4 GHz band is shown. The **Band** icon displays 5G if the heat map for the 5 GHz band is shown.
16. To show the map with or without grid, on the right side, click the **Grid** icon.
17. To show the access points by model or without a label, on the right side, click the **Label** icon and select your preference.

    By default, the access point name is shown. Because this section describes an RF plan that is not yet deployed, the IP address and channel cannot be displayed on the map.
18. To save the floor map with its new configuration, click the **Save** icon.

    The settings are saved.

Manually Add and Manage Antennas on a Floor Map for an RF Plan

You can add individual antennas to a floor map for an RF plan. These antennas do not need to be of the same model. After adding antennas, you can change their properties, move them to another location on the floor map, or remove them from the floor map.

Note: Antennas are associated with access points. Therefore, before you add antennas to a floor plan, first add access points to the floor plan. For more information about adding access points to a floor plan, see *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69 and *Manually Add and Manage Access Points on a Floor Map for an RF Plan* on page 75.

➢ **To manually add and manage individual antennas on a floor map for an RF plan:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

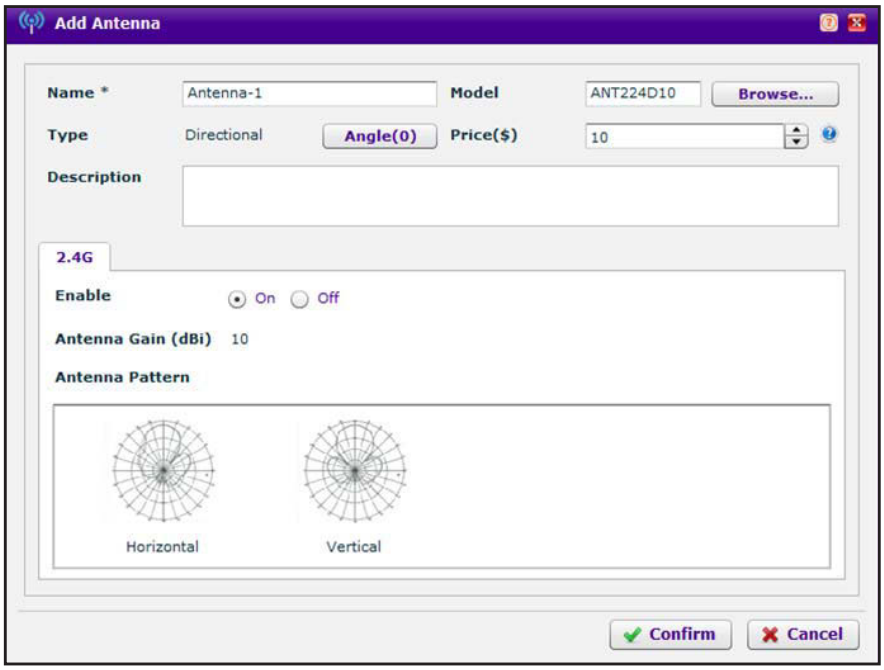
   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

   The floor map displays.
7. Click an access point to select it.
8. Click the **Antenna** icon.

   Note: The **Antenna** icon is masked if you do not select an access point.



9. Specify the antenna settings as described in the following table.

Setting	Description
Name	Enter a name for the antenna. By default, the access points are numbered, for example, Antenna-1.
Model	Specify the antenna that you intend to use for the floor: 1. Click the **Browse** button. The antennas that the wireless controller supports display in a pop-up window. 2. Click the antenna. All calculations are performed with the selected antenna. 3. Click the **Confirm** button. The changes are saved and the pop-up window closes.
AP Type	When you select an antenna, this field is populated automatically.
Angle	When you add a directional antenna, by default, the antenna points to the north. You can set the antenna direction to a desired angle. Specify the antenna angle: 1. Click the **Browse** button. A degree clock displays in a pop-up window. 2. Click the degree at which you want to direct the antenna. The yellow needle moves to the selected degree. 3. Click the **Confirm** button. The changes are saved and the pop-up window closes.
Price($)	As an option, enter the price of the antenna.
Description	As an option, enter a description for the access point.
2.4G	Specify the settings for the 2.4 GHz band: • **Enable**. By default, the **On** radio button is selected and the 2.4 GHz band is enabled for the antenna. To disable the 2.4 GHz band for the antenna, select the **Off** radio button. • **Antenna Gain (dBi)**. When you select an antenna, this field is populated automatically. • **Antenna Pattern**. When you select an antenna, this field is populated automatically.

10. Click the **Confirm** button.

    The changes are saved and the pop-up window closes.

    The new antenna is placed at the edge of the floor map and shows a connection with the access point.

11. To move an antenna to another location on the floor map, drag the antenna to a location on the floor map.

    Note: Moving an antenna turns off the heat map.

12. To change the properties for an antenna, do the following:
    a. Double-click the antenna.

       A pop-up menu displays.

    b. From the pop-menu, select **Edit Properties**.

       The Edit Antenna pop-up window opens. This window is identical to the Add Antenna pop-up window.

    c. Change the properties.

       For information about the properties, see the previous table.

    d. Click the **Confirm** button.

       The changes are saved and the pop-up window closes.

13. To remove an existing antenna from the floor map, do the following:
    a. Click the antenna to select it.
    b. Click the **Delete** link.
14. To add another antenna to the floor map, change the properties for another antenna, move another antenna on the floor map, remove another antenna from the floor map, or perform a combinations of these tasks, repeat *Step 7* through *Step 13*.
15. To turn the heat map on or off, on the right, click the **HeatMap** icon.

    If you turn on the heat map, the heat map is generated and displays. Use the color information on the right as guidance for WiFi coverage.

    Note: Adding or removing antennas changes the heat map.
16. To switch the heat map to the 2.4 GHz or 5 GHz band (for antennas that support dual bands), on the right, click the **Band** icon.

    The **Band** icon displays 2.4G if the heat map for the 2.4 GHz band is shown. The **Band** icon displays 5G if the heat map for the 5 GHz band is shown.
17. To show the map with or without grid, on the right side, click the **Grid** icon.
18. To show the antennas by model or without a label, on the right side, click the **Label** icon and select your preference.

    By default, the antenna name is shown. The IP address and channel do not apply to an antenna.
19. To save the floor map with its new configuration, click the **Save** icon.

    The settings are saved.

Display and Recalculate the WiFi Coverage for a Heat Map

After you set up an RF plan and generate a heat map for a floor, you can display the WiFi coverage and view how the WiFi coverage changes if you change the minimum signal strength with the same number of access points and antennas.

The default minimum signal strength is –62 dBm. The WiFi coverage percentage is calculated based on this value. You can change this value and recalculate the coverage percentage. However, to change the minimum signal strength for an RF plan, you must run the WiFi auto planning advisor again (see *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69).

Note: The WiFi coverage tool is for display and information only. However, heat maps can function in realtime.

➢ **To display and recalculate the WiFi coverage for an existing heat map:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Plans > Planning**.

   The page displays the Planning icons.
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.
6. Click the floor name.

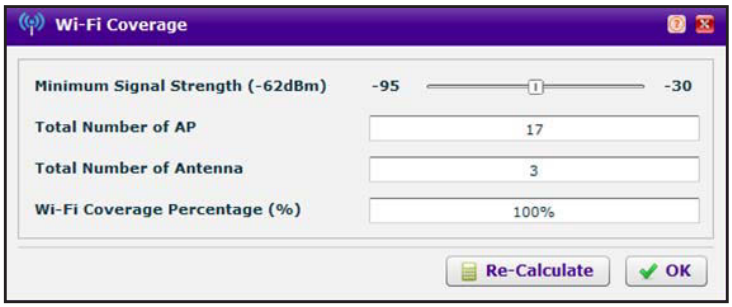
   The floor map displays.
7. On the right, click the **HeatMap** icon.

   The heat map for the 2.4 GHz band is generated and displays. Use the color information on the right as guidance for WiFi coverage.
8. To generate the heat map for the 5 GHz band, on the right, click the **Band** icon.

   The heat map for the 5 GHz band is generated and displays. Use the color information on the right as guidance for WiFi coverage.

9. Click the **Coverage** icon.

   Note: The **Coverage** icon is masked if you did not generate a heat map.



   The **Total Number of AP** and **Total Number of Antenna** fields are based on the RF plan and fixed. The **Wi-Fi Coverage Percentage (%)** field displays the WiFi coverage based on the position of the **Minimum Signal Strength** slider at –62dBm.

10. Move the position of the **Minimum Signal Strength** slider to another dBm value.
11. Click the **Re-Calculate** button.

    The **Wi-Fi Coverage Percentage (%)** field displays the WiFi coverage based on the new dBm value.

12. Click the **OK** button.

    The pop-up window closes.

    If you want to change the actual minimum signal strength for an RF plan, run the WiFi auto planning advisor again (see *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69).

Display or Change the WiFi Inventory for an RF Plan

The inventory for an RF plan of a floor displays all access points and antennas that you added by running the WiFi auto planning advisor, the access points and antennas that you added manually, or a combination of both.

➢ **To display or change the access point and antenna inventory for an RF plan:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

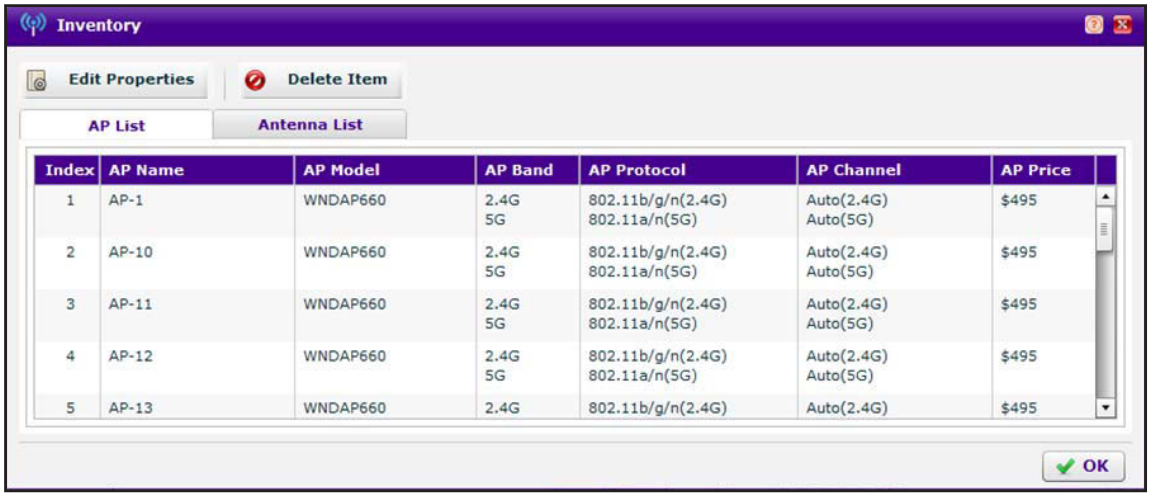
5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **Inventory** icon.



   By default, the **AP List** tab is selected and the access point inventory displays. The inventory is based on the access points that you added by running the WiFi auto planning advisor (see *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69), the access points that you added manually (see *Manually Add and Manage Access Points on a Floor Map for an RF Plan* on page 75), or a combination of both.

8. To change the properties for an access point in the inventory, do the following:

   a. Select the access point in the inventory table.

   b. Click the **Edit Properties** button.

      The Edit AP pop-up window opens.

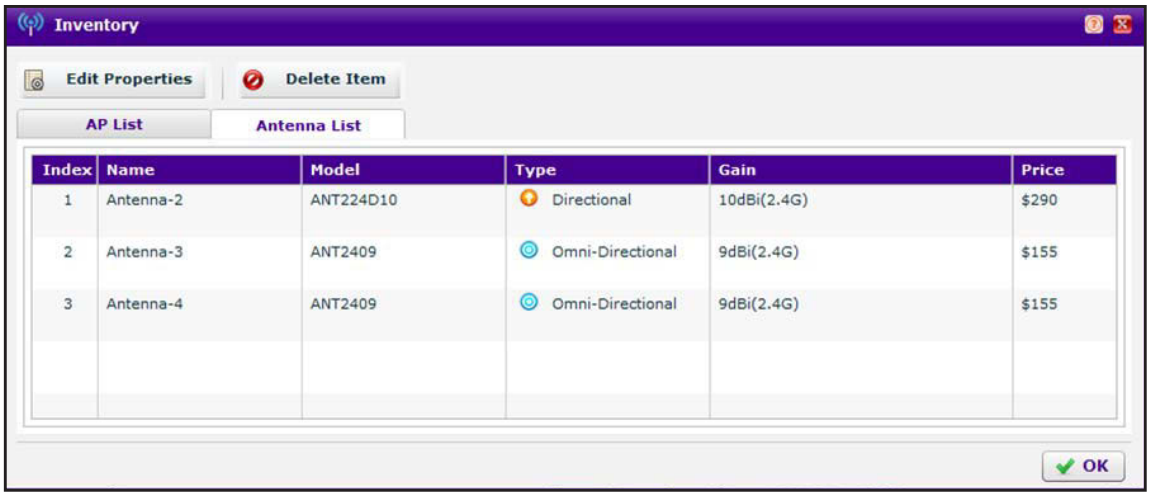
   c. Change the properties.

      For more information about changing the properties, or for information about removing an access point from the inventory, see *Manually Add and Manage Access Points on a Floor Map for an RF Plan* on page 75.

   d. Click the **Confirm** button.

      The changes are saved and the pop-up window closes.

9. On the Inventory pop-up window, click the **Antenna List** tab.



The inventory is based on the antennas that you added by running the WiFi auto planning advisor (see *Use the WiFi Auto Planning Advisor to Generate an RF Plan for a Floor* on page 69), the antennas that you added manually (see *Manually Add and Manage Antennas on a Floor Map for an RF Plan* on page 78), or a combination of both.

10. To change the properties for an antenna in the inventory, do the following:
    a. Select the antenna in the inventory table.
    b. Click the **Edit Properties** button.

       The Edit Antenna pop-up window opens.

    c. Change the properties.

       For more information about changing the properties, or for information about removing an access point from the inventory, see *Manually Add and Manage Antennas on a Floor Map for an RF Plan* on page 78.

    d. Click the **Confirm** button.

       The changes are saved and the pop-up window closes.
11. On the Inventory pop-up window, click the **OK** button.

    The Inventory pop-up window closes.
12. To save the inventory changes, click the **Save** icon.

    The settings are saved.

Download a Report for an RF Plan

The report for an RF plan includes the following components:

- Floor summary
- Inventory summary that could serve as a purchase list
- Detailed list of access points
- Detailed list of antennas (if you added any manually)
- Floor map with suggested locations of the access points and antennas
- Heat map for the 2.4 GHz band
- Heat map for the 5 GHz band

You can download the report as a PDF or a Microsoft Word file.

➢ **To generate and download a report for an RF plan:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Plans > Planning**.

   The page displays the Planning icons.

5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.

   The floor map displays.

7. Click the **PDF** icon or the **Word** icon.

   The report downloads.

8. Follow the directions of your browser to save the report.

View the Heat Map for a Deployed Floor Plan

For an RF plan, you can assign access points and antennas to a building and floor. However, these access points and antennas are used only for the purpose of planning and are not actual access points and antennas.

Access points display on the floor map of a deployed floor plan only if you assign them to the building and floor. For information about assigning access point to a building and floor, see *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172.

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

IMPORTANT:

For the heat map to provide realistic information, do the following:

1. **Scale the floor plan accurately.**
2. **Place the different types of obstacles accurately on the floor map.**
3. **Move each virtual access point to the virtual location on the floor map that matches the actual physical location of the physical access point on the floor as closely as possible.**

The heat map displays the following information:

- Signal strength and WiFi coverage, including weak coverage areas and coverage holes, indicated by color
- Access points that are managed by the wireless controller
- For each access point, the following real-time information:
  - Status in relation to the wireless controller (for example, Connected)
  - IP address
  - MAC address
  - For each WiFi band, the number of connected clients
  - For each WiFi band, the active channel
  - For each WiFi band, the transmission (output) power
- Information for each antenna

➢ **To move the access points and antennas to the correct locations on the floor map and generate a realistic heat map for a deployed floor plan:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.

3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

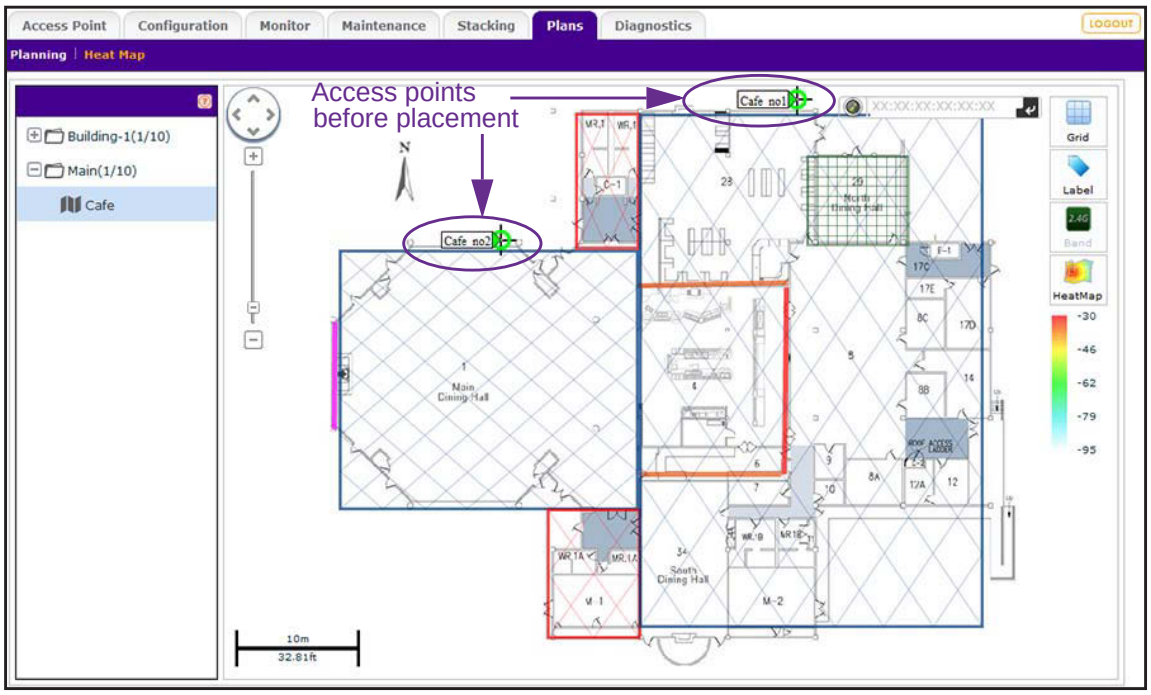
4. Select **Plans > Heat Map**.

   The page displays the Planning icons.

5. In the building tree on the left, click the **+** icon of the building that contains the floor.

   The floor names display.

6. Click the floor name.



7. The first time that you view the heat map, move the access points manually on the floor map to closely match their actual physical locations on the floor by dragging each access point to the correct location on the floor map.

8. On the right, click the **HeatMap** icon.

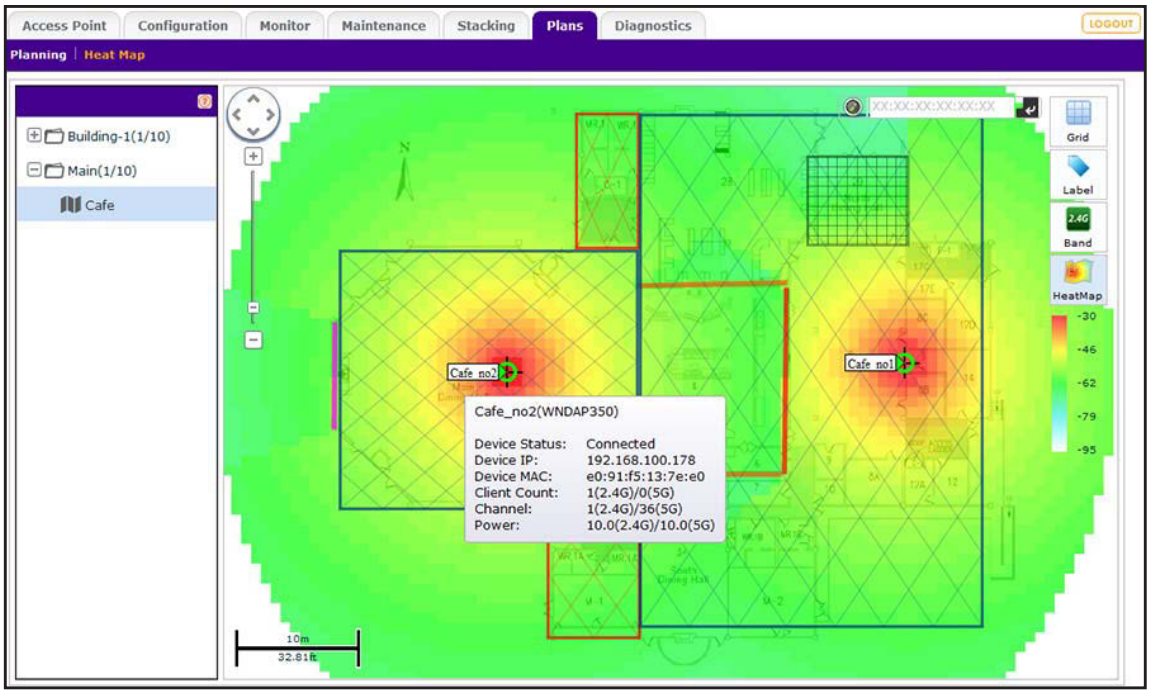
   The heat map for the 2.4 GHz band is generated and displays. Use the color information on the right as guidance for WiFi coverage.

9. To generate the heat map for the 5 GHz band, on the right, click the **Band** icon.

   The heat map for the 5 GHz band is generated and displays. Use the color information on the right as guidance for WiFi coverage.

10. To see the information about an individual access point or antenna, point to the location.

    A pop-up field displays the information.



11. To make adjustments to the WiFi coverage, drag the access points to new locations on the floor map.
12. To regenerate the heat map, on the right, click the **HeatMap** icon.

    The heat map is generated and displays. Use the color information on the right of the heat map as guidance for WiFi coverage.
13. If you made changes to the WiFi coverage on the floor map in *Step 11*, move each physical access point to the actual physical location on the floor that matches the virtual location of the virtual access point on the floor map as closely as possible.

    In other words, reverse the process that you accomplished in *Step 7* and now make sure that the actual placement on the floor matches the virtual placement on the floor map.

Installation and Configuration Overview

5

This chapter includes the following sections:

- *Connect Your Computer to the Wireless Controller*
- *Log In to the Wireless Controller*
- *Roadmap for Initial Configuration*
- *Roadmap for Configuring Management of Your WiFi Network*
- *Choose a Location for the Wireless Controller*
- *Deploy the Wireless Controller*

Connect Your Computer to the Wireless Controller

To connect to the wireless controller for initial configuration, follow the steps in this section. You can also access the *ProSAFE Wireless Controller Installation Guide* that you can download from *http://support.netgear.com/product/WC9500*.

➢ **To connect your computer to the wireless controller:**

1. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
2. Connect the wireless controller to the computer through the network or directly to the wireless controller's Ethernet port.
3. Connect the power cord from the wireless controller to an AC power outlet.
4. Verify that the following LEDs on the front panel are lit:

LED	Description
Power	The green Power LED is 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.
Status	The Status LED is lit yellow while the wireless controller is initializing. After approximately two minutes, when the wireless controller completes its initialization, the Status LED turns green.
Fan	The green Fan LED is lit, indicating that the fans are functioning correctly.
Ethernet	The right Ethernet port LED is lit green for a 1000 Mbps connection or yellow for a 100 Mbps or 10 Mbps connection. If it is not, make sure that the Ethernet cable is securely attached at both ends.

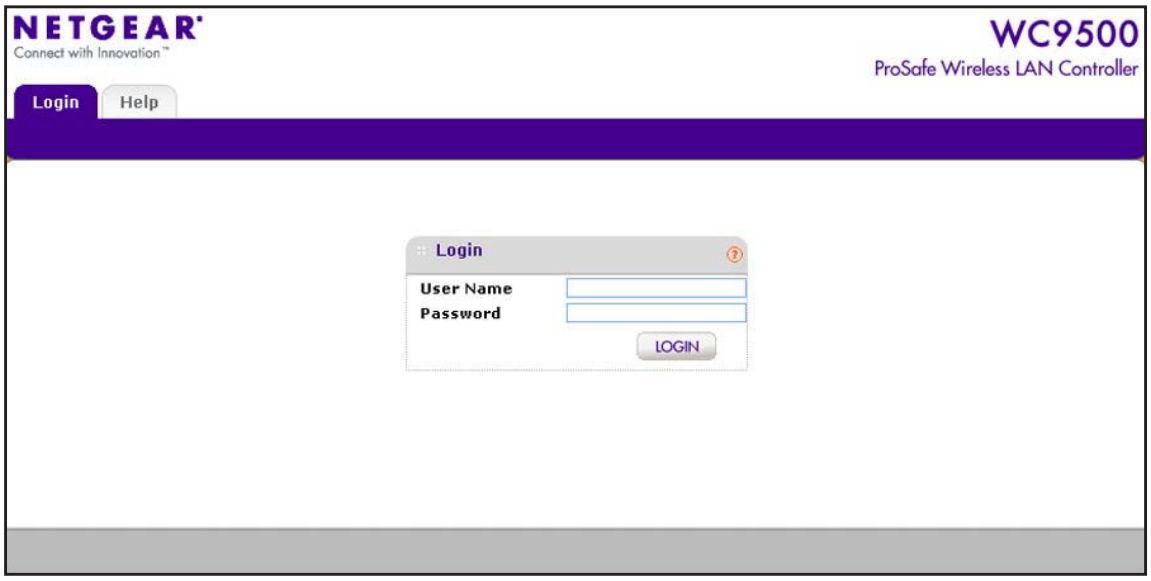
Log In to the Wireless Controller

Before you log in to the wireless controller, make sure that you follow the steps in *Connect Your Computer to the Wireless Controller* on page 91.

To log in to the wireless controller, you must use a web browser such as Microsoft Internet Explorer 9 or 10, or the latest Mozilla Firefox version, or Google Chrome 24 or later with JavaScript, cookies, and SSL enabled.

➢ **To log in to the wireless controller:**

1. Open your browser and type **http://192.168.0.250** in the browser's address field.



2. When prompted, enter **admin** for the user name and **password** for the password, both in lowercase letters.
3. Click the **Login** button.

   The first time that you log in, the Change Password Notification pop-up window opens. On model WC7600 and model WC9500, you must change the default password. However, on model WC7500 and model WC7600v2, changing the password is optional.

WC7600 and WC9500

WC7500 and WC7600v2

4. On model WC7600 and model WC9500, click the **OK** button.

   On model WC7500 and model WC7600v2, you can click either the **NOW** button to change the password immediately or the **LATER** button to change the password later. If you click the **LATER** button, the following figure, *Step 5*, and *Step 6* do not apply.

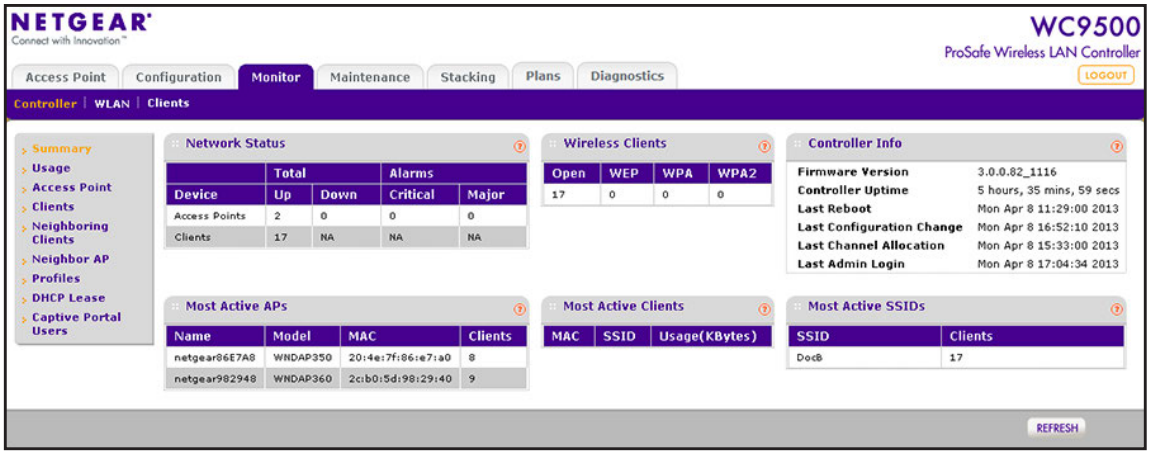
In the **Old Password** field, the old password is automatically entered.

5. In the **New Password** field, enter your new password and repeat it in the **Confirm New Password** field.

   Note: You cannot change the default user name (admin), but you can create a new administrative account with a customized user name. For more information, see *Add a Management User* on page 231.

6. Click the **OK** button.

   The wireless controller's web management interface opens and displays the Summary page (the path is **Monitor > Controller > Summary**), which shows the network status and related information:



   For information about the network status and related information, see *View the Wireless Controller Summary Page* on page 316.

Roadmap for Initial Configuration

After you connect and log in to the wireless controller, perform the initial configuration. If you are not sure how you are going to deploy the wireless controller in your network, We recommend that you read *Chapter 3, System Planning and Deployment Scenarios*.

This section is a roadmap for basic configuration only: It provides *high-level* configuration steps with references to the sections or chapters that provide detailed configuration steps.

➢ **To perform the initial configuration of the wireless controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.

3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > General**.

   The General Settings page displays.

5. Enter a name for the wireless controller and select the country in which the wireless controller is used.

6. Click the **Apply** button.

   The changes are saved.

7. Select **Configuration > System > Time**.

   The Time Setting page displays.

8. Select the time zone in which the wireless controller is used. Optionally, configure the NTP settings.

   For more information, see *Manage the Time Settings* on page 100.

9. Click the **Apply** button.

   The changes are saved.

10. Select **Configuration > System > IP/VLAN**.

    The IP Settings page displays.

11. Enter the IP settings for your network and the VLANs that you want to assign to the wireless controller.

    Note: A management VLAN is used for all SNMP and HTTP traffic to and from the wireless controller and managed access points.

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

    For more information, see *Manage the IP, VLAN, and Link Aggregation Settings* on page 101.

12. Click the **Apply** button.

    The changes are saved.

13. If your network does not include a DHCP server, configure the wireless controller's DHCP server.

    For more information, see *Manage the DHCP Server* on page 105.

14. Click the **Apply** button.

    The changes are saved.

The connection to the wireless controller is terminated because you changed its IP address.

15. Reconfigure your computer with an IP address and subnet mask that is in the same IP subnet as the new IP address of the wireless controller.
16. Log back in to the wireless controller using its new IP address.

    Continue with the following section, *Roadmap for Configuring Management of Your WiFi Network*.

Roadmap for Configuring Management of Your WiFi Network

After you perform the initial configuration and change the IP address to an address that is specific to your network (see *Roadmap for Initial Configuration* on page 93), you are ready to configure the wireless controller for management of your WiFi network.

This section is a roadmap only: It provides *high-level* configuration steps with references to the sections or chapters that provide detailed configuration steps.

➢ **To configure the wireless controller for management of your WiFi network:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Register the licenses.

   For more information, see *Register Your Licenses* on page 109.
5. (Optional but recommended) Replace the default certificate with a custom certificate for certificate-based authentication of the internal authentication server.

   For more information, see *Manage Certificates* on page 112.
6. (Optional but recommended) Configure logs, alerts, and alarms.

   For more information, see *Configure Log, Syslog, Alarm Notification, and Email Settings* on page 113.
7. Configure security profiles:
   a. Configure the security profiles for the basic profile group or for advanced profile groups.

For detailed configuration steps, see:

- *Manage Security Profiles for the Basic Profile Group* on page 123.
- *Manage Security Profiles for Advanced Profile Groups* on page 128.

b. (Optional) Configure authentication servers.

For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 139.

c. (Optional) Configure MAC authentication.

For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 145.

d. (Optional) Assign the authentication servers and MAC ACLs to the security profiles.

For more information, see:

- *Manage Security Profiles for the Basic Profile Group* on page 123.
- *Manage Security Profiles for Advanced Profile Groups* on page 128.

8. Configure the managed access point list:

a. Run the Discovery Wizard and add access points to the managed list.

For more information, see *Discover Access Points With the Discovery Wizard* on page 158.

b. (Optional) Configure access points that are on the managed list.

For more information, see *Manage the Managed AP List* on page 166.

c. (Optional) Assign access points to advanced profile groups.

For more information, see *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172.

9. (Optional) Configure rogue access point detection.

For more information, see *Manage Rogue Access Points* on page 214.

10. (Optional) Configure a guest portal or captive portal.

For more information, see *Manage Guest Network Access Through Guest Portals and Captive Portals* on page 218.

11. (Optional) Configure user accounts and portal accounts.

For more information, see *Manage Users, Accounts, and Passwords* on page 230.

12. (Optional) Configure WiFi and QoS settings.

For more information, see *Chapter 9, Configure WiFi and QoS Settings*.

13. (Optional but recommended) Back up the configuration.

For more information, see *Back Up the Configuration File* on page 246.

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 of 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, Technical Specifications, and Passwords Requirements*.

Deploy the Wireless Controller

After you follow the steps in *Roadmap for Initial Configuration* on page 93 and *Roadmap for Configuring Management of Your WiFi Network* on page 95, you are ready to deploy the wireless controller in your network.

➢ **To deploy the wireless controller:**

1. Disconnect the wireless controller from the computer that you used for configuration.
2. (Optional) Reconfigure the computer back to its original TCP/IP settings.
3. Place the wireless controller where you intend to deploy it.
4. Connect an Ethernet cable from the wireless controller to a switch or router on your wired network.
5. Connect the power cord to the wireless controller and plug the power cord into a power outlet.

   The Power, Status, and Ethernet LEDs light. If any of these do not light, see *Troubleshoot Basic Functioning* on page 351.

Configure the System and Network Settings and Register the Licenses

6

This chapter includes the following sections:

- *Configure the General Settings*
- *Manage the Time Settings*
- *Manage the IP, VLAN, and Link Aggregation Settings*
- *Manage the DHCP Server*
- *Register Your Licenses*
- *Manage Certificates*
- *Configure Log, Syslog, Alarm Notification, and Email Settings*

Configure the General Settings

Note: You must 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 page lets you configure the basic settings of your wireless controller.

➢ **To configure general settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

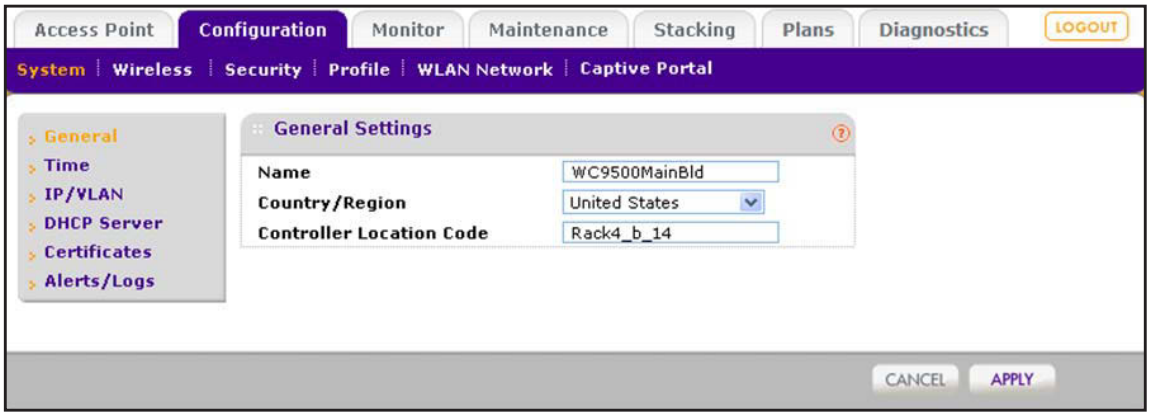
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > General**.



5. Configure the settings as described in the following table.

Setting	Description
Name	Enter a unique value as the wireless controller name. We recommend changing the name as soon as possible after setting up. The name must contain only alphabetical characters, numbers, and hyphens, and must be 31 characters or less.
Country/Region	From the menu, select the region of operation for the wireless controller and the access points that the wireless controller manages. This setting is crucial for optimal performance of the wireless controller. The wireless controller uses the country code to determine the best WiFi settings for the 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. **Note:** To enable the wireless controller to transmit at a higher power level than the level that might be specified for your country or region, select **Rest of World** from the **Country/Region** menu.
Controller Location Code	Enter a code to identify the physical location of the wireless controller. If you use more than one wireless controller, a code is especially useful.

WARNING:

If you change the selection from the Country/Region menu and you click the Apply button, the wireless controller reboots.

6. Click the **Apply** button.

   The changes are saved.

Manage the Time Settings

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

➢ **To configure time settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

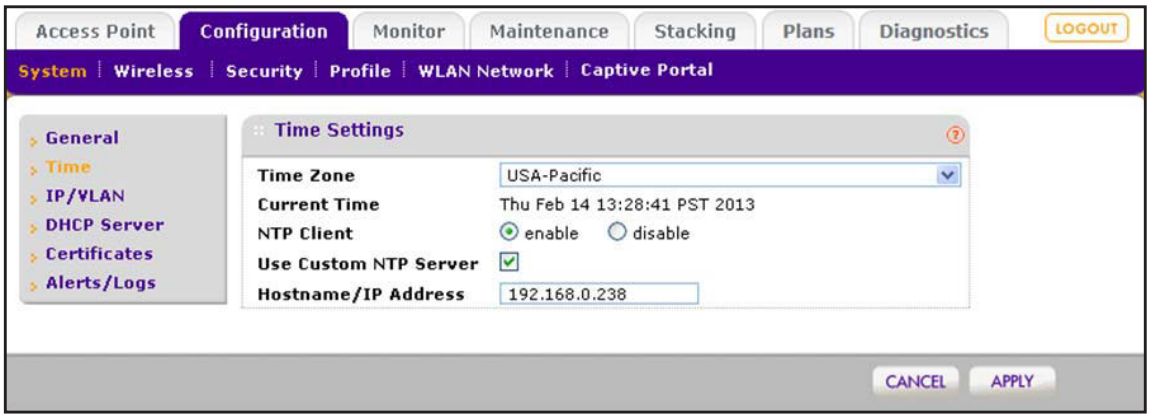
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > Time**.



5. Configure the settings as described in the following table.

Setting	Description
Time Zone	From the menu, select the local time zone for your country or region.
Current Time	This field is a nonconfigurable field that displays the current time at your location.
NTP Client	Select the **Enable** radio button to use a Network Time Protocol (NTP) server to synchronize the clock of the wireless controller and managed access points. Select the **Disable** radio button if you do not want to use an NTP server.
Use Custom NTP Server	Select the **Use Custom NTP Server** 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.

6. Click the **Apply** button.

   The changes are saved.

Manage the IP, VLAN, and Link Aggregation Settings

You can manage the IP address, VLAN settings, and link aggregation (LAG) settings of the wireless controller.

Management VLAN Concepts

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

For large deployments, we recommend 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 VLAN Concepts

When the **Untagged VLAN** check box is selected on the IP Settings page, 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 you clear the **Untagged VLAN** check box, 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 results in a loss of IP connectivity if the hubs and switches on your network are not configured with the corresponding VLANs.

Link Aggregation Concepts

Note: Link aggregation is not supported on model WC7500 and model WC7600v2.

If you connect the two 10GE connections of the wireless controller to a switch or router, the wireless controller supports dynamic link aggregation (802.3ad), which you can use either to increase bandwidth or to support link redundancy.

You can enable the wireless controller to automatically create a single link aggregation group (LAG) in which the two links share the same speed and duplex settings. The link selection for egress traffic is based on the transmit hash policy.

You can also configure a standby link in which only one link in the LAG is active. The standby link becomes active only if the active link fails. In such a situation, a failover occurs from the failed active link to the standby link, which becomes the new active link.

Configure the IP, VLAN, and Link Aggregation Settings

Note: Link aggregation is not supported on model WC7500 and model WC7600v2.

You can configure the management IP address, VLAN settings, and link aggregation (LAG) settings of the wireless controller.

➢ **To configure IP, VLAN, and LAG settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

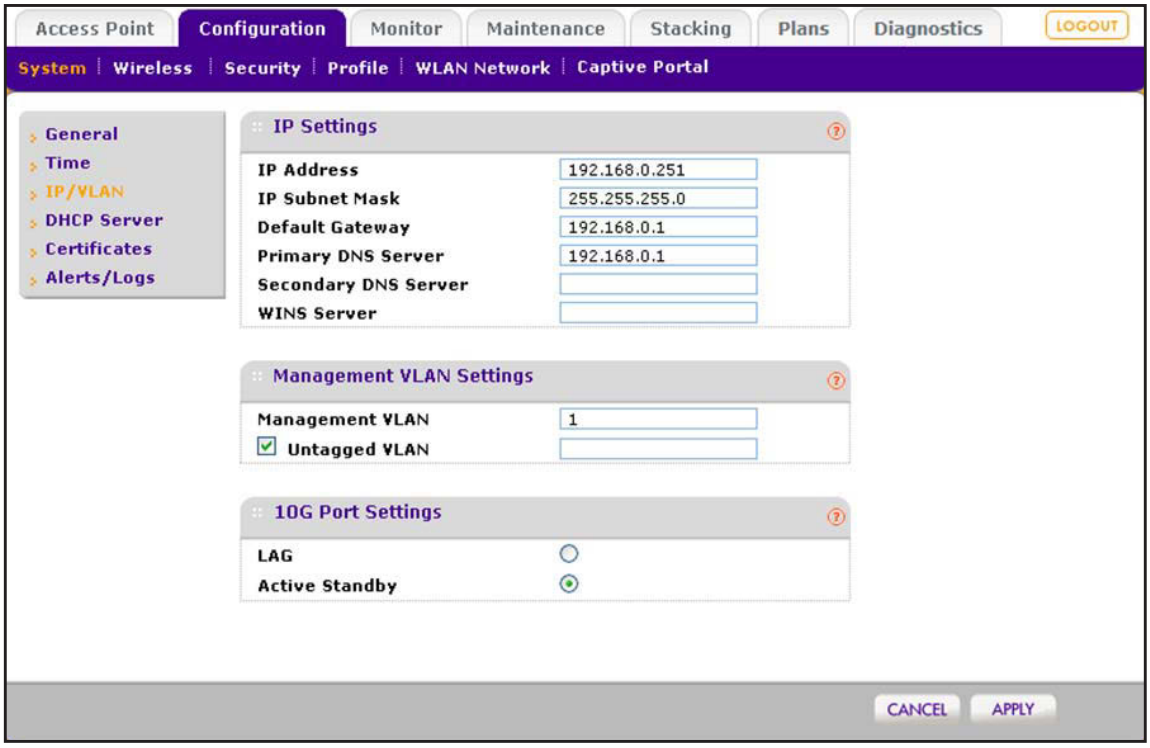
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > IP/VLAN**.



5. Configure the settings as described in the following table.

Setting	Description
IP Settings section	
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. **Note:** If you assign a static IP address to the wireless controller and then use the web management interface of a discovered access point to configure a static IP address for the access point and enter the wireless controller's static IP address, the access point attempts to reach the wireless controller only at the provided static IP address. If the IP address of the wireless controller changes, the access point can no longer reach the wireless controller. In such a situation, reset the access point to factory default settings. Doing so removes the static IP address of the wireless controller from the access point configuration.
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.
Management VLAN Settings section	
Management VLAN	Enter the management VLAN. For more information, see *Management VLAN Concepts* on page 101.
Untagged VLAN	Select the **Untagged VLAN** check box if the configured VLAN is untagged. For more information, see *Untagged VLAN Concepts* on page 102.
10G Port Settings section[1]	
LAG	Select the **LAG** radio button to enable the wireless controller to automatically create a LAG in which both links are active. The **LAG** radio button and **Active Standby** radio button are mutually exclusive. For more information, see *Link Aggregation Concepts* on page 102.
Active Standby	Select the **Active Standby** radio button to enable the wireless controller to automatically create a LAG in which only one link is active and the other link functions as a standby link. The **Active Standby** radio button and **LAG** radio button are mutually exclusive. For more information, see *Link Aggregation Concepts* on page 102.

1. Link aggregation is not supported on model WC7500 and model WC7600v2.

6. Click the **Apply** button.

   The changes are saved.

Manage the DHCP Server

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

The wireless controller can function as a DHCP server. You can add multiple DHCP server pools for different VLANs. By default, no DHCP server pool is configured on the wireless controller but you can add one or more DHCP server pools.

Add a DHCP Server

The DHCP Server List page lets you add a DHCP server pool.

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

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

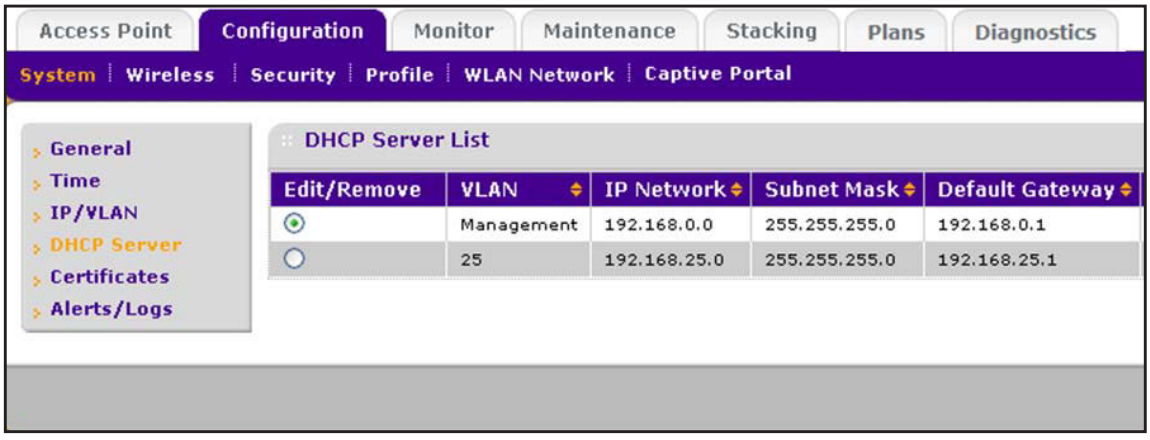
   The wireless controller's login window opens.

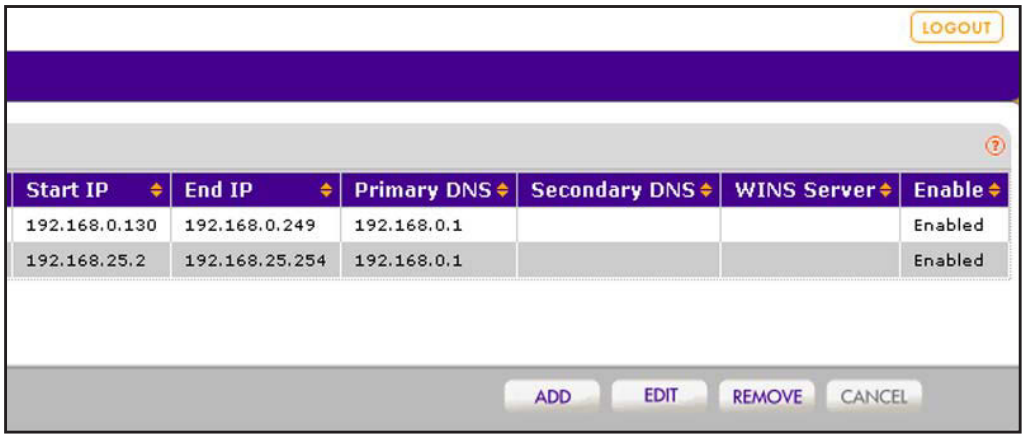
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > DHCP Server**.

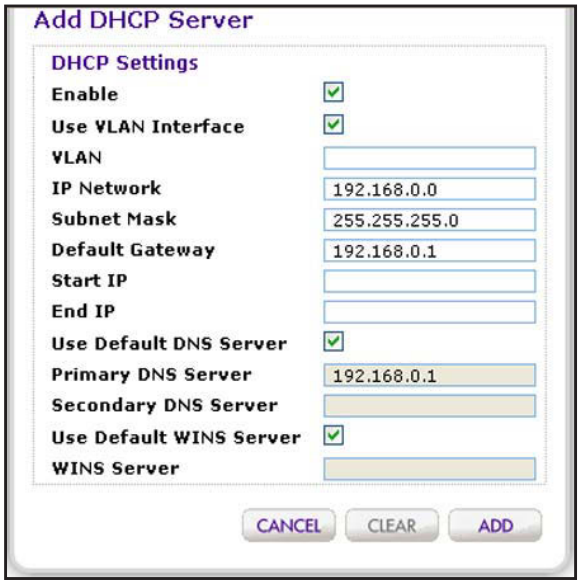
   The DHCP Server List page displays. Because this page is wide, it is shown in the following two figures.





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

5. Click the **Add** button.



6. Configure the settings as described in the following table.

Setting	Description
Enabled	Select the **Enabled** check box to enable the DHCP server. When the check box is cleared, the DHCP server is disabled.
Use VLAN Interface	Select the **Use VLAN Interface** 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 services this VLAN.

Setting	Description
IP Network	Enter the IP address for the wireless controller in the VLAN that you specified in the **VLAN** field. **Note:** If you do not select the **Use VLAN Interface** check box, the IP address of the wireless controller's management VLAN is used.
Subnet Mask	Enter the subnet mask that is assigned to the WiFi 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 start IP address of the range that the DHCP server can assign.
End IP	Enter the end IP address of the range that the DHCP server can assign.
Use Default DNS Server	Select the **Use Default DNS Server** 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 the **Use Default WINS Server** 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.

7. Click the **Add** button.

   The new DHCP server is added to the DHCP Server List.

Change the Settings for a DHCP Server

You can change the settings for a DHCP server.

➢ **To change the settings for a DHCP server:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

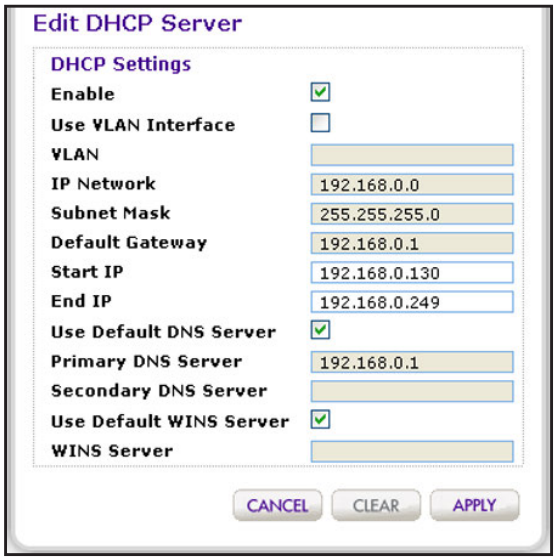
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > DHCP Server**.

   The DHCP Server List page displays.

5. Select the radio button in the Edit/Remove column that corresponds to the DHCP server for which you want to change the settings.
6. Click the **Edit** button.



7. Change the settings.
8. Click the **Apply** button.

   The changes are saved.

Remove a DHCP Server

You can remove a DHCP server.

➢ **To remove a DHCP server:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > System > DHCP Server**.

   The DHCP Server List page displays.
5. Select the radio button in the Edit/Remove column that corresponds to the DHCP server that you want to remove.
6. Click the **Remove** button.

Register Your Licenses

Make sure that your licenses cover the number of access points in your network. Before you can register your licenses, you must configure the license server settings.

Note: When you install your licenses, they replace the default trial license.

For more information about licenses, see *Licenses* on page 16 and *Manage Licenses* on page 266.

Configure the License Server Settings

Although you generally do not need to change the default license update server, you must make sure that the wireless controller can reach the license update server.

➢ **To configure the license server settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

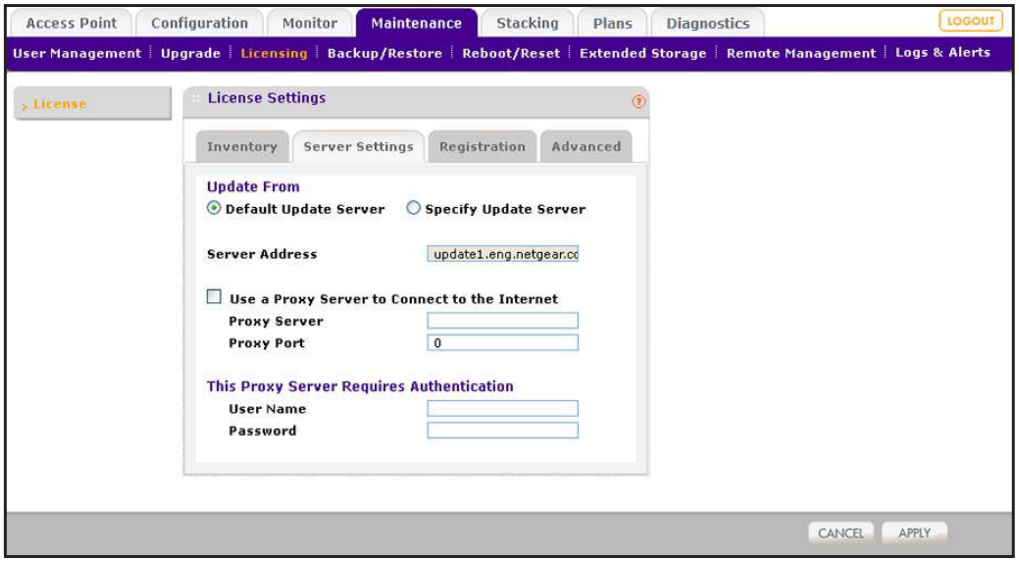
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Licensing**.
5. Click the **Server Settings** tab.



6. Configure the settings as described in the following table.

Setting	Description	
Update From	Select one of the following radio buttons to specify the license update server: • **Default Update Server**. The default license update server is used. • **Specify Update Server**. You must specify the license update server. Fill in the **Server Address** field.	
	Server Address	Enter the IP address or FQDN of the server from which you import your licenses. By default, the FQDN of the NETGEAR license server is **update1.eng.netgear.com**.
Use a Proxy Server to Connect to the Internet	Select the **Use a Proxy Server to Connect to the Internet** 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.
	Proxy Port	Enter the port that the proxy server uses.
This Proxy Server Requires Authentication	If the proxy server requires authentication, specify the user name and password.	
	User Name	Enter the user name to access the proxy server.
	Password	Enter the password to access the proxy server.

7. Click the **Apply** button.

   The changes are saved.

Register Your Licenses With the License Server

You must purchase licenses before you can register them. For more information, see *Licenses* on page 16)

➢ **To register your licenses:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

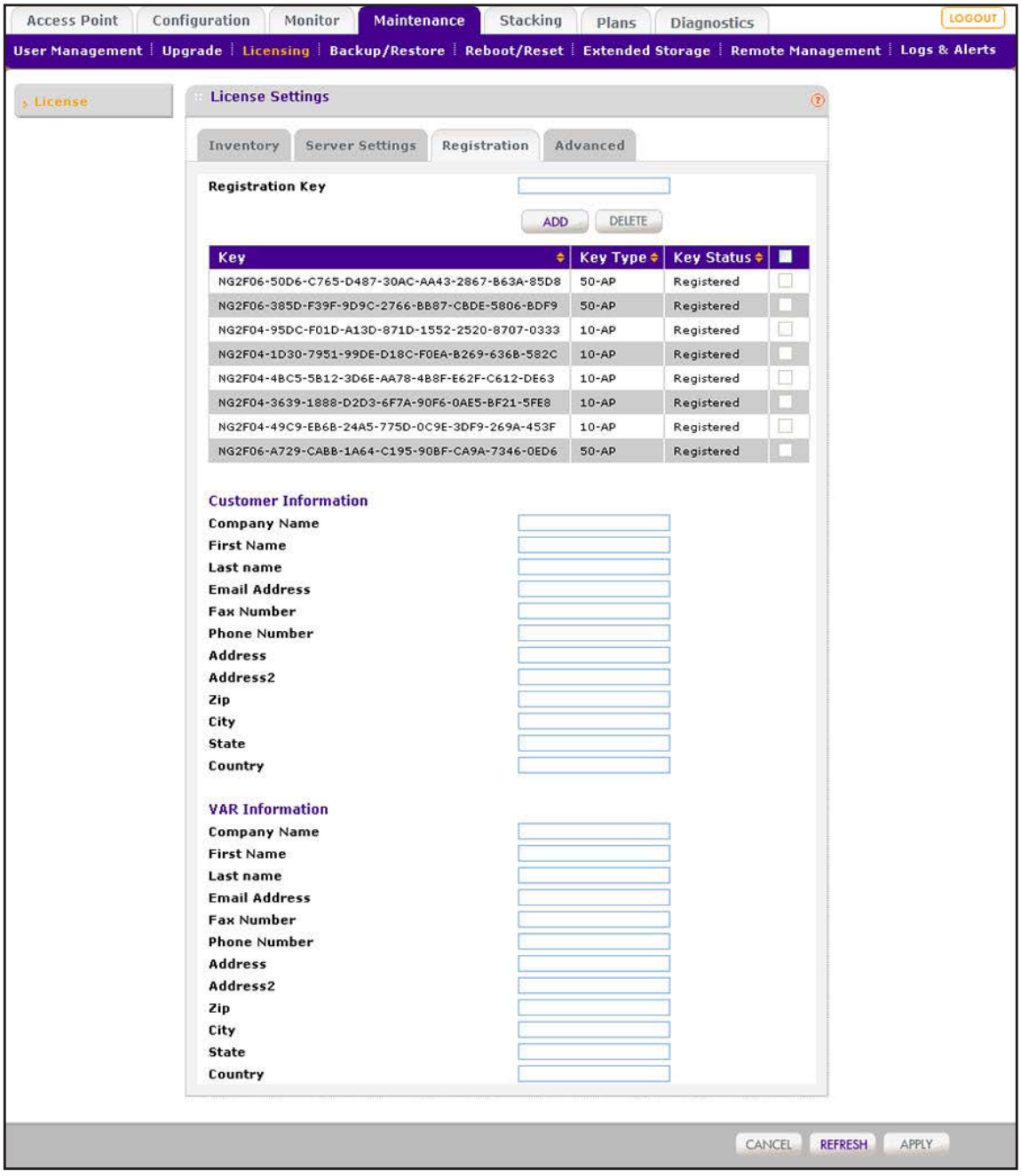
   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Make sure that the wireless controller is connected to the Internet.
5. Select **Maintenance > Licensing**.
6. Click the **Registration** tab.

The following figure shows some licenses already registered and installed. If you register licenses for the first time, the page does not yet show any licenses.



7. Complete the fields in the Customer Information section with the customer information that is associated with the key that you want to add and register.

   These fields are self-explanatory.

8. Complete the fields in the VAR Information section 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.

9. In the **Registration Key** field at the top of the page, enter the registration key for the license that you want to add and register.
10. Click the **Add** button.

    The license is added to the table. The key details in the table mean the same as the key details that are shown on the Inventory page (see the Key Details section in the table in *View Your Licenses* on page 266).

11. Click the **Apply** button.

    Your license is registered.

12. To register another license, repeat these steps.

Manage Certificates

The internal authentication server for certificate-based authentication requires you to install a certificate on the wireless controller. A default self-signed server certificate is installed on the wireless controller. However, we strongly recommend 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 computer as described in this section. Certificates must be in X.509 PEM format.

➢ **To add certificates:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

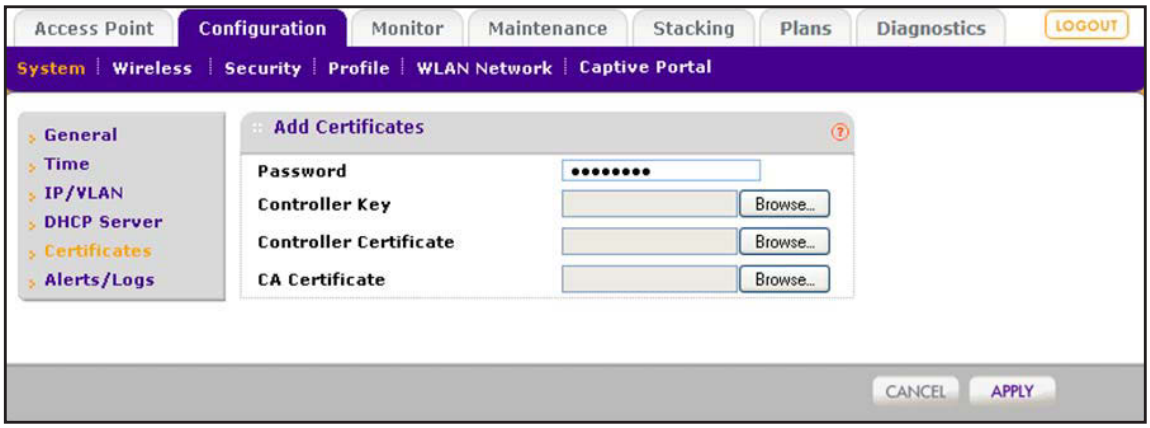
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > Certificates**.



5. Configure the settings as described in the following table.

Setting	Description
Password	Enter the password for wireless controller certificates.
Controller Key	Click the **Browse** button, and select the controller key.
Controller Certificate	Click the **Browse** button, and select the controller certificate.
CA Certificate	Click the **Browse** button, and select the CA certificate.

6. Click the **Apply** button.

   The changes are saved.

Configure Log, Syslog, Alarm Notification, and Email Settings

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

Configure the Event Tracing Log Settings

Note: Event tracing is not supported on model WC7500 and model WC7600v2.

For the logs, you can either configure event tracing or select a log level. These selections are mutually exclusive.

Event tracing can help you to debug the WiFi network. Event tracing generates logs from the wireless controller and from all controlled access points, and saves these logs in a file on the wireless controller. The file can become large quickly.

➢ **To configure the event tracing log settings and view the logs:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

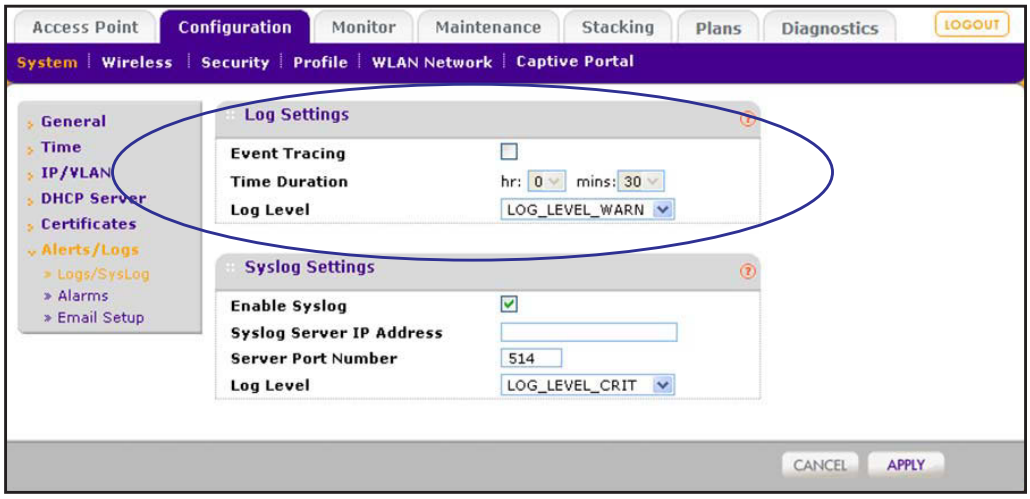
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > Alerts/Logs > Logs/Syslog**.



5. In the Log Settings section of the page, configure either event tracing or a log level (these selections are mutually exclusive):
   - **Event tracing**. To configure event tracing:
     a. Select the **Event Tracing** check box.
     b. Next to Time Duration, use the menus to specify the period during which event tracing must occur.
   - **Log level**. From the **Log Level** menu, select one of the following levels:
     - **LOG_LEVEL_CRIT**. Critical errors only are logged.
     - **LOG_LEVEL_ERR**. Noncritical errors and critical errors are logged.
     - **LOG_LEVEL_WARN**. Warnings, noncritical errors, and critical errors are logged.
     - **LOG_LEVEL_NOTICE**. Notifications, warnings, noncritical errors, and critical errors are logged.
     - **LOG_LEVEL_INFO**. Informational messages, notifications, warnings, noncritical errors, and critical errors are logged.
6. Click the **Apply** button.

   The changes are saved.

For information about saving the logs, see *Save the Logs* on page 256.

Configure the Syslog Settings

You can configure the settings to connect to a syslog server, if your network includes one.

Note: Before you configure the IP address of the syslog server on the wireless controller, make sure that you set up a syslog server (such as a computer running a syslog service) and that the syslog server is available on the network.

➢ **To configure the syslog settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

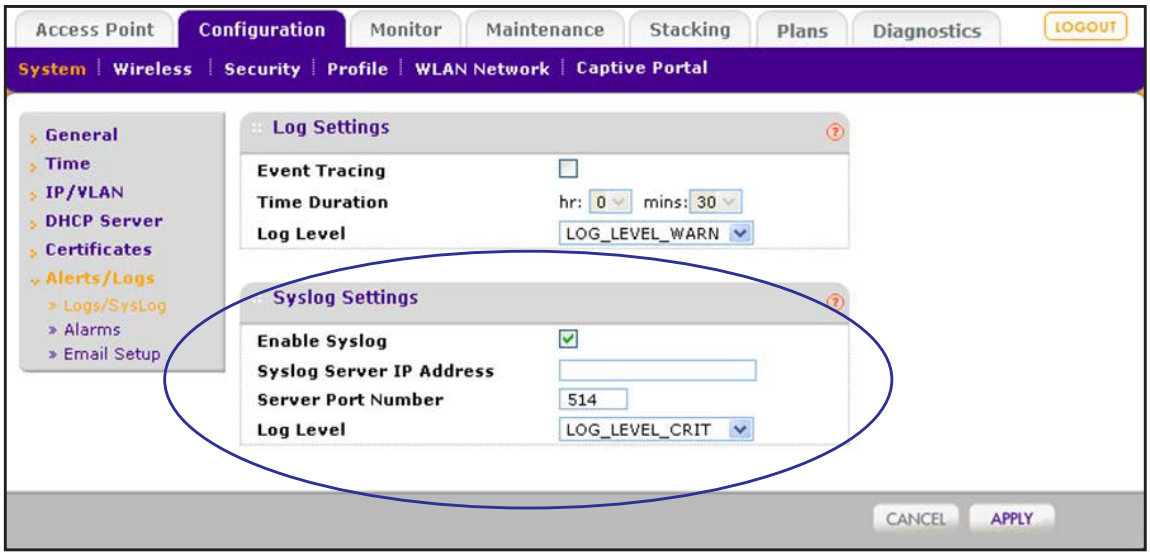
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > Alerts/Logs > Logs/Syslog**.



5. In the Syslog Settings section of the page, configure the settings as described in the following table.

Setting	Description
Enable Syslog	Enable the syslog settings, if your network includes a syslog sever.
Syslog Server IP Address	Enter the IP address to which the wireless controller and managed access points send all syslogs, if the **Enable Syslog** check box is selected. **Note:** Before you configure the IP address of the syslog server on the wireless controller, make sure that you set up a syslog server (such as a computer running a syslog service) and that the syslog server is available on the network.
Server Port Number	Enter the number of the port at which your syslog server is configured to listen to requests.
Log Level	From the **Log Level** menu, select one of the following levels: • **LOG_LEVEL_CRIT**. Critical errors only are logged. • **LOG_LEVEL_ERR**. Noncritical errors and critical errors are logged. • **LOG_LEVEL_WARN**. Warnings, noncritical errors, and critical errors are logged. • **LOG_LEVEL_NOTICE**. Notifications, warnings, noncritical errors, and critical errors are logged. • **LOG_LEVEL_INFO**. Informational messages, notifications, warnings, noncritical errors, and critical errors are logged.

6. Click the **Apply** button.

   The changes are saved.

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.

➢ **To configure alarm actions:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

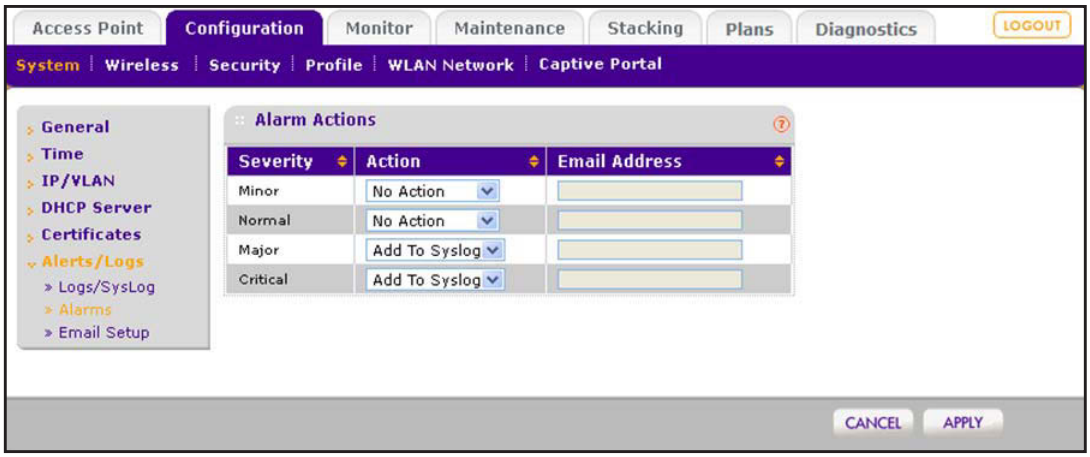
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > System > Alerts/Logs > Alarms**.



5. For each alarm severity (Minor, Normal, Major, and Critical), select the desired action from its corresponding Action menu.
   - **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.
6. For each alarm severity for which you selected the **Send Email** option in the previous step, enter an email address.
7. Click the **Apply** button.

   The changes are saved.

Configure the Email Notification Server

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

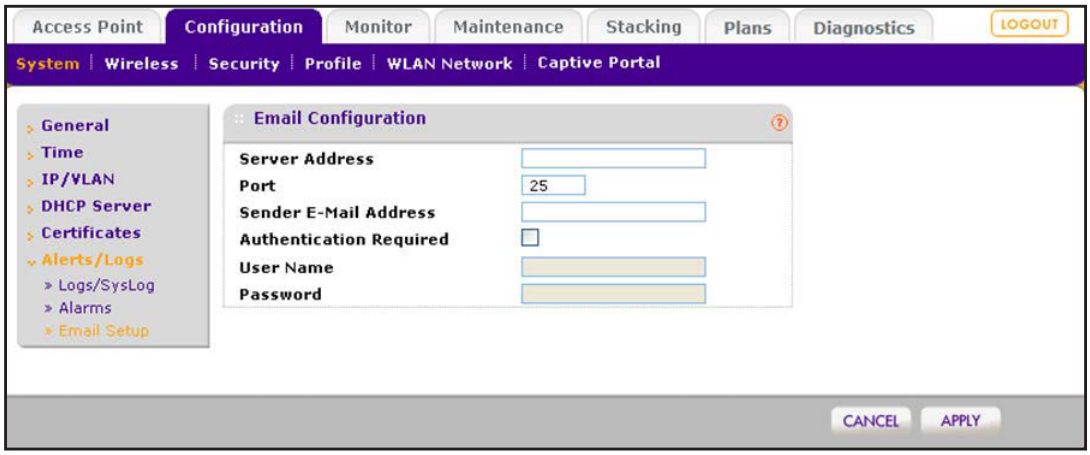
➢ **To configure email settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > System > Alerts/Logs > Email Setup**.



5. Configure the settings as described in the following table.

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 port is **25**.	
Sender Email Address	Enter the email address from which email notifications are sent.	
Authentication Required	Select the **Authentication Required** 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.

6. Click the **Apply** button.

   The changes are saved.

Manage Security Profiles and Profile Groups

7

This chapter includes the following sections:

- *WiFi Security Profile Concepts*
- *Manage Security Profiles for the Basic Profile Group*
- *Manage Security Profiles for Advanced Profile Groups*
- *Network Authentication and Data Encryption Options*
- *Manage Authentication Servers and Authentication Server Groups*
- *Manage MAC Authentication and MAC Authentication Groups*

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.

WiFi Security Profile Concepts

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 WiFi radio on an access point can support 8 profiles. For example, the dual-band WNDAP660 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 operating, 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 wireless controller, the profile configurations are pushed onto the access points.

An access point can be a member of one profile group only. If you move an access point from one profile group to another, the access point stops serving the SSIDs in the old profile group and starts serving the SSIDs in the new profile group.

Note: 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 Setting Concepts* on page 32.

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 WiFi, 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 provides its own SSID and can provide 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 that are managed by the wireless controller serve the same WiFi networks and support the same settings, you can use the basic configuration.

Large WLAN Networks

For large 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 WiFi, security, and QoS configurations.

The wireless controller supports up to eight profile groups. Each profile group can provide its own WiFi, 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 provides its own SSID and can provide its own VLAN to allow the profile to establish its own tunnel. Profiles can also share the same VLAN.

Also, in larger network deployments, you would assign guests to a separate VLAN because guests typically access only the Internet, not the business network, and are not allowed 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 configure the authentication server settings:
  - Configure basic server settings on the basic Authentication Server page (see *Configure Basic Authentication Server Settings* on page 141).
  - For more complex networks, configure additional RADIUS servers on the advanced Authentication Server page (see *Configure a RADIUS Authentication Server Group* on page 143).

  After you configure 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.

- **Captive portals and guest portals**. If you want to use captive portals, guest portals, or both, first configure the portals:
  - Configure the basic portal on the basic Portal Settings page (see *Configure a Basic Guest Portal or Captive Portal* on page 219).
  - For more complex networks, configure additional portals on the advanced Captive Portal Settings page (see *Configure an Advanced Guest Portal or Captive Portal* on page 224).

  After you configure portals, you can then assign any portal to a security profile in a basic profile group or advanced profile group.
- **MAC authentication**. If you want to use a MAC access control list (ACL) to control access of WiFi clients, first create one or more MAC ACLs:
  - Configure the basic MAC ACL on the basic MAC Authentication page (see *Configure Basic Local MAC Authentication Settings* on page 145).
  - For more complex networks, configure additional MAC ACLs on the advanced MAC Authentication page (see *Configure a Local MAC Authentication Group* on page 148).

  After you configure 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.

Basic and Advanced Security Configuration Concepts

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)

Manage Security Profiles for the Basic Profile Group

The basic profile group works well for small-scale WLAN networks. We recommend that you read the information in the previous section, *WiFi Security Profile Concepts*, before you configure any profiles.

Configure a Profile in the Basic Profile Group

The Edit Profile (Basic) page lets you create and configure up to eight security profiles per WiFi 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/ac-mode radios.

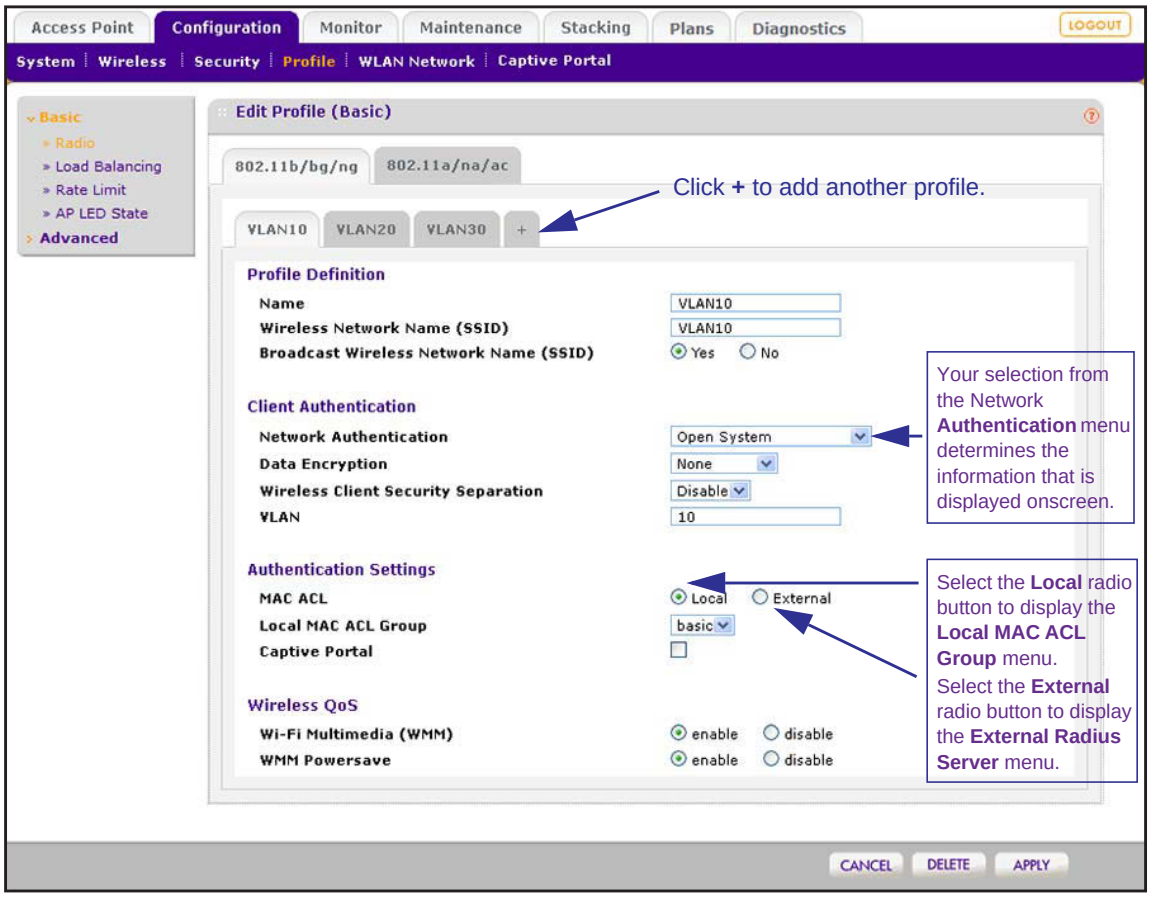
➢ **To add a security profile to the basic profile group and configure the security profile:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

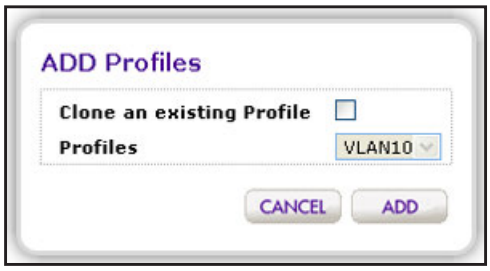
   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Profile > Basic > Radio**.



By default, an **NG_11g-01** profile and an **NG_11a-01** profile are present in the basic profile group.

5. Click the tab for the radio for which you want to add a profile.
6. Click the **+** button to add the profile to the basic profile group.



7. To clone an existing profile, do the following:
   a. Select the **Clone an existing Profile** check box.

      The previous figure shows that you can clone an existing profile with the name VLAN10.

   b. Select a profile from the **Profiles** menu.

8. Click the **Add** button.

   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 authentication server settings that you specify on the Authentication Server page affect the selections that are available from the **Network Authentication** menu. For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. If your selection from the **Network Authentication** menu requires authentication, a corresponding **Authentication Server** field displays.

9. Configure the settings as described in the following table.

Setting	Description
Profile Definition section	
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 WiFi network associated with this profile. The length of the SSID is restricted to a maximum of 31 characters. You can you use all characters except for the following: space, single quotation mark, and double quotation mark.
Broadcast Wireless Network Name	Select the **Yes** radio button to enable broadcast of the SSID. This is the default setting. Select the **No** radio button to disable broadcast of the SSID, in which case only users who know the correct SSID can connect to the access point.
Client Authentication section **Note:** The options that display onscreen depend on your selection from Network Authentication menu.	
Network Authentication	From the menu, select the authentication type to be used. *Table 10* on page 136 lists all the authentication type options.
Data Encryption	From the menu, 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. *Table 10* on page 136 lists all the data encryption options.
Wireless Client Security Separation	From the menu, select **Disable** to prevent associated WiFi clients from communicating with each other, or select **Enable** to allow such communication. WiFi 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 must match the VLAN ID that is used by other network devices.

Setting	Description	
Authentication Settings section **Note:** The options that display onscreen depend on the selection from **Network Authentication** menu.		
Note: The **MAC ACL** button displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.	MAC ACL	Select one of the following radio buttons: • **Local**. Use local MAC authentication. The **Local MAC ACL Group** menu displays so you can select a group. For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 145. • **External**. Use external MAC authentication. The **External Radius Server** menu displays so you can select a server. You can select 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 *Manage Authentication Servers and Authentication Server Groups* on page 139. **Note:** 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 & WPA2 (or you use Legacy 802.1X), you cannot use external MAC authentication, and the **MAC ACL** radio buttons do not display onscreen. You can still use internal MAC authentication.
Note: The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.	Captive Portal	Select the **Captive Portal** check box if you want to enable a guest portal or captive portal. The **Captive Portal** menu displays so you can select a portal. You can select either the **Basic** portal or a portal from the advanced portal group. For information about setting up portals, see *Manage Guest Network Access Through Guest Portals and Captive Portals* on page 218. **Note:** If the network authentication uses a RADIUS server, whether it is a local server or an external server, you cannot configure captive portal authentication. That is, if you configure a RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), the **Captive Portal** check box is not shown onscreen.

Setting	Description	
Note: The **Authentication Server** buttons and menu display only when you select **WPA with Radius**, **WPA2 with Radius**, or **WPA & WPA2 with Radius** from the **Network Authentication** menu.	Authentication Server	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Use an external authentication server. Select an external authentication server from the **Authentication Server** menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 139.
Wireless QoS section		
Wi-Fi Multimedia (WMM)	To enable Wi-Fi Multimedia (WMM), select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature. For more information, see *Manage Quality of Service for an Advanced Profile Group* on page 202.	
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 **Enable** radio button, which is the default setting. **Note:** We recommend that you do not disable the WMM Powersave feature.	

10. Click the **Apply** button.

    The changes are saved.

Change the Settings for a Profile in the Basic Profile Group

You can change the settings for a profile in the basic profile group.

➢ **To change the settings for an existing profile:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) page displays.
5. Click the tab for the radio for which you want to change a profile.
6. Click the tab for the profile that you want to change.
7. Change the settings.

For information about how to change the settings, see *Configure a Profile in the Basic Profile Group* on page 123.

8. Click the **Apply** button.

   The changes are saved.

Remove a Profile From the Basic Profile Group

You can remove a profile from the basic profile group.

➢ **To remove an existing profile:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) page displays.

5. Click the tab for the radio for which you want to remove a profile.
6. Click the tab for the profile that you want to remove.
7. Click the **Delete** button.
8. Confirm that you want to remove the profile.

Manage Security Profiles for Advanced Profile Groups

Advanced profile groups are useful for larger deployments. We recommend that you read the information in the *WiFi Security Profile Concepts* on page 120 before you configure any profile groups and profiles.

Add an Advanced Profile Group

The advanced Profile Group page lets you create up to eight profile groups. For each profile group, you can create and configure up to eight security profiles per WiFi radio (eight 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/ac-mode radios.

By default, all access points are assigned to the basic profile group. After you create advanced profile groups, you can use the WLAN Network page to reassign access points to any of these advanced profile groups (see *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).

➢ **To add an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

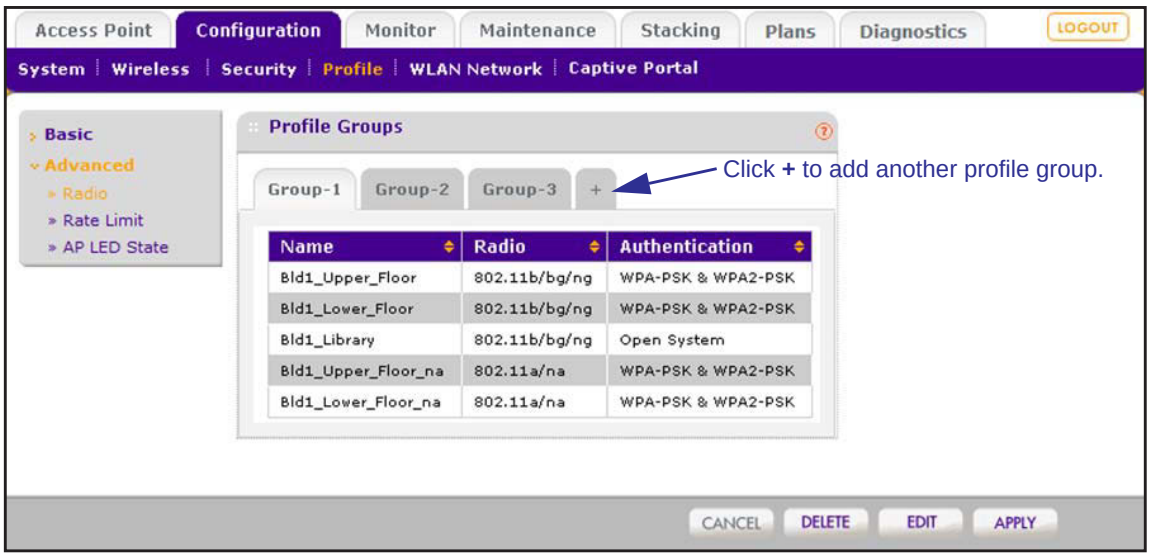
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Advanced > Radio**.



5. To add a profile group, click the **+** button.

   The new profile group displays on the Profile Groups page. By default, an **NG_11g-*x*1** profile and an **NG_11a-*x*2** profile, in which *x* is the group number, 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.

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

Setting	Description
Name	The unique profile name.
Radio	The WiFi radio in which the profile is operating.
Authentication	The authentication setting under which the profile is operating.

Remove an Advanced Profile Group

You can remove an advanced profile group

➢ **To remove an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups page displays.

5. Click the tab for the profile group that you want to remove.
6. Click the **Delete** button.

Note: A separate procedure to change profile groups does not exist. You change profile groups by adding, removing, or changing profiles in the profile group.

Configure a Profile in an Advanced Profile Group

For each profile group, the Edit Profile (Group-*X*, in which *X* is the group number) page lets you create and configure up to 8 security profiles per WiFi 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/ac-mode radios.

➢ **To add a security profile to an advanced profile group and configure the security profile:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Advanced > Radio**.

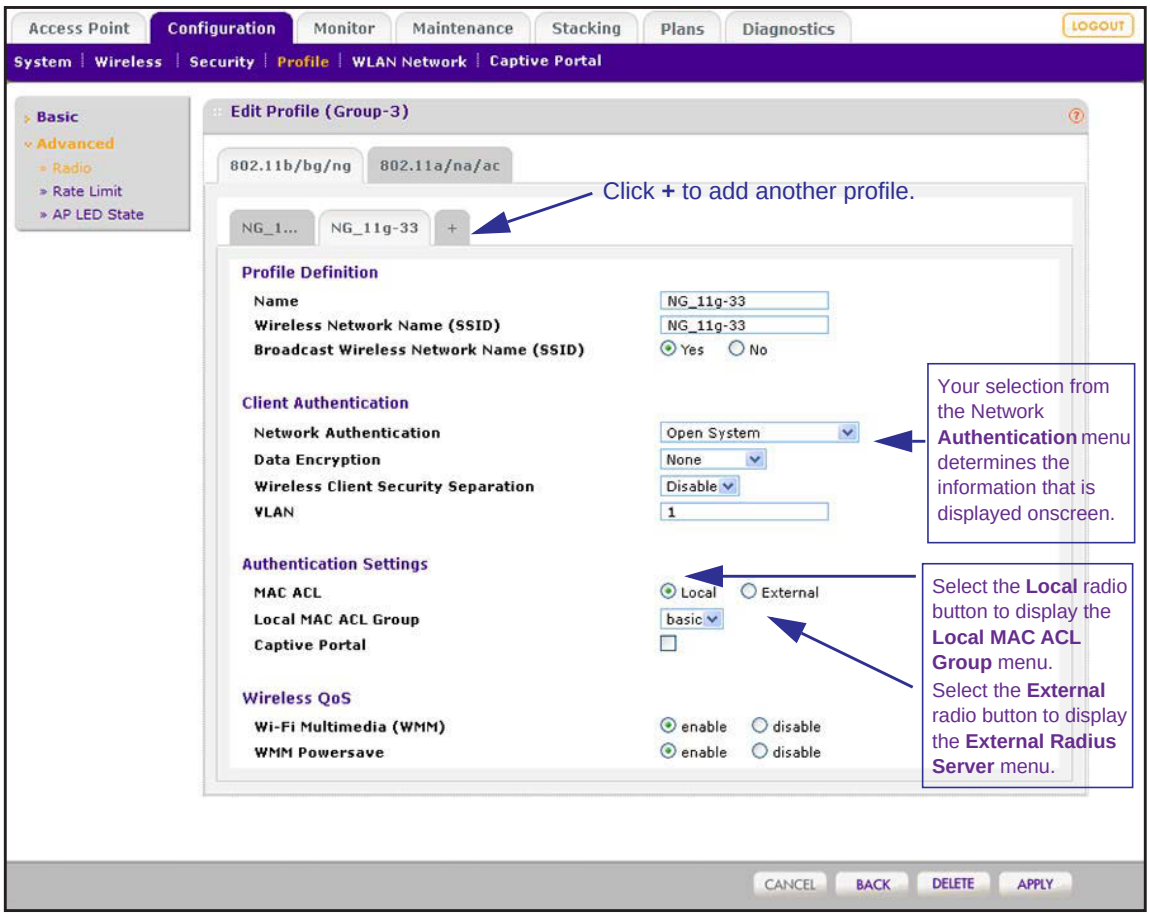
   The Profile Groups page displays.

5. Click the **Edit** button.

   The Edit Profile (Group-*X*) page displays.

6. Click the tab for the radio that for which you want to add a profile.
7. Click the **+** button to add the profile to the selected advanced profile group.

8. To clone an existing profile, do the following:
   a. Select the **Clone an existing Profile** check box.
   b. Select a profile from the Profiles menu.
9. Click the **Add** button.



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 authentication server settings that you specify on the Authentication Server page affect the selections that are available from the **Network Authentication** menu. For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. If your selection from the **Network Authentication** menu requires authentication, a corresponding **Authentication Server** field displays.

10. Configure the settings as described in the following table.

Setting	Description
Profile Definition section	
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 WiFi network associated with this profile. The length of the SSID is restricted to a maximum of 31 characters. You can you use all characters except for the following: space, single quotation mark, and double quotation mark.
Broadcast Wireless Network Name	Select the **Yes** radio button to enable broadcast of the SSID. This is the default setting. Select the **No** radio button to disable broadcast of the SSID, in which case only users who know the correct SSID can connect to the access point.
Client Authentication section **Note:** The options that display onscreen depend on your selection from **Network Authentication** menu.	
Network Authentication	From the menu, select the authentication type to be used. *Table 10* on page 136 lists all authentication types.
Data Encryption	From the menu, 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. *Table 10* on page 136 lists all data encryption options.
Wireless Client Security Separation	From the menu, select **Disable** to prevent associated WiFi clients from communicating with each other, or select **Enable** to allow such communication. WiFi 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 must match the VLAN ID that other network devices use.

Setting	Description	
Authentication Settings section **Note:** The options that display onscreen depend on the selection from **Network Authentication** menu.		
Note: The **MAC ACL** buttons displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.	MAC ACL	Select one of the following radio buttons: • **Local**. Use local MAC authentication. The **Local MAC ACL Group** menu displays so you can select a group. For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 145. • **External**. Use external MAC authentication. The **External Radius Server** menu displays so you can select a server. You can select 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 *Manage Authentication Servers and Authentication Server Groups* on page 139. **Note:** 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 & WPA2 (or you use Legacy 802.1X), you cannot use external MAC authentication, and the **MAC ACL** radio buttons do not display onscreen. You can still use internal MAC authentication.
Note: The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.	Captive Portal	Select the **Captive Portal** check box if you want to enable a guest portal or captive portal. The **Captive Portal** menu displays so you can select a portal. You can select either the **Basic** portal or a portal from the advanced portal group. For information about setting up portals, see *Manage Guest Network Access Through Guest Portals and Captive Portals* on page 218. **Note:** If the network authentication uses a RADIUS server, whether it is a local server or an external server, you cannot configure captive portal authentication. That is, if you configure a RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), the **Captive Portal** check box is not shown onscreen.

Setting	Description	
Note: The **Authentication Server** buttons and menu display only when you select **WPA with Radius**, **WPA2 with Radius**, or **WPA & WPA2 with Radius** from the **Network Authentication** menu.	Authentication Server	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Use an external authentication server. Select an external authentication server from the **Authentication Server** menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 139.
Wireless QoS section		
Wi-Fi Multimedia (WMM)	To enable Wi-Fi Multimedia (WMM), select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature. For more information, see *Manage Quality of Service for an Advanced Profile Group* on page 202.	
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 **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature.	

11. Click the **Apply** button.

    The changes are saved.

Change the Settings for a Profile in an Advanced Profile Group

You can change the settings for a profile in an advanced profile group.

➢ **To change the settings for an existing profile to an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups page displays.

5. Click the tab for the profile group for which you want to change a profile.
6. Click the **Edit** button.

   The Edit Profile page displays.

7. Click the tab for the radio for which you want to change a profile.
8. Click the tab for the profile that you want to change.
9. Change the settings.

   For information about how to change the settings, see *Configure a Profile in an Advanced Profile Group* on page 130.
10. Click the **Apply** button.

    The changes are saved.

Remove a Profile From an Advanced Profile Group

You can remove a profile from an advanced profile group.

➢ **To remove an existing profile from an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups page displays.
5. Click the tab for the profile group for which you want to remove a profile.
6. Click the **Edit** button.

   The Edit Profile (Group-*X*) page displays.
7. Click the tab for the radio for which you want to remove a profile.
8. Click the tab for the profile that you want to remove.
9. Click the **Delete** button.
10. Confirm that you want to remove the profile.

Network Authentication and Data Encryption Options

This section describes the detailed network authentication and data encryption options that you can select in the procedures that are described in *Configure a Profile in the Basic Profile Group* on page 123 and *Configure a Profile in an Advanced Profile Group* on page 130.

Table 10 on page 136 shows the data encryption options based on the network authentication that you select on the Edit Profile (Basic) or Edit Profile (Group-*X*) page, and the required configuration steps to implement the selected network authentication.

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

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 10. Network authentication and data encryption settings

Network Authentication Selection	Data Encryption Options	Configuration Steps
Open	None WEP	You can use an open system without any encryption or with WEP encryption: • **No encryption**. An open system without encryption is the default setting. No further authentication and encryption configuration is required. • **WEP encryption**. To configure an open system with WEP encryption, see the Shared Key and WEP information further down in this table.

Table 10. Network authentication and data encryption settings (continued)

Network Authentication Selection	Data Encryption Options	Configuration Steps
Shared Key	64-bit WEP 128-bit WEP 152-bit WEP	To configure Shared Key authentication with WEP: 1. From the **Data Encryption** menu, select a level of WEP encryption: - **64-bit WEP**. Uses 40/64-bit encryption. - **128-bit WEP**. Uses 104/128-bit encryption. - **152-bit WEP**. A proprietary mode that works only with other WiFi devices that support this mode. 2. To display the characters in the key fields, select the **Show Key** check box. 3. Select a key radio button (**Key1**, **Key2**, **Key3**, or **Key4**). 4. Enter a key in the corresponding field: - 64-bit WEP requires a key with 10 characters. - 128-bit WEP requires a key with 26 characters. - 152-bit WEP requires a key with 32 characters. **Note:** For information about requirements for WEP keys, see *Table 15* on page 362.
Legacy 802.1x	None	To configure legacy 802.1x authentication: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. 2. Select the **Local** or **External** radio button. 3. If you select the **External** radio button, select the authentication server that you wish to use from the menu.
WPA with Radius	TKIP TKIP + AES	To configure WPA authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. 2. From the **Data Encryption** menu, select the type of encryption: - **TKIP**. Supports Temporal Key Integrity Protocol (TKIP) only. - **TKIP + AES**. Supports both TKIP and Advanced Encryption Standard (AES). 3. Select the **Local** or **External** radio button. 4. If you select the **External** radio button, select the authentication server that you wish to use from the menu.

Table 10. Network authentication and data encryption settings (continued)

Network Authentication Selection	Data Encryption Options	Configuration Steps
WPA2 with Radius	AES TKIP + AES	To configure WPA2 authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. From the **Data Encryption** menu, select the type of encryption: - **AES**. Supports AES only. - **TKIP + AES**. Supports both TKIP and AES. 2. Select the **Local** or **External** radio button. 3. If you select the **External** radio button, select the authentication server that you wish to use from the menu.
WPA & WPA2 with Radius **Note:** Use this option if the network includes both WPA and WPA2 clients.	TKIP + AES	To configure WPA & WPA2 authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 139. 2. Select the **Local** or **External** radio button. 3. If you select the **External** radio button, select the authentication server that you wish to use from the menu. **Note:** The **Data Encryption** menu displays **TKIP + AES**, which is the only available option. Both TKIP and AES are supported.
WPA-PSK	TKIP TKIP + AES	To configure WPA-PSK authentication: 1. From the **Data Encryption** menu, select the type of encryption: - **TKIP**. Supports TKIP only. - **TKIP + AES**. Supports both TKIP and AES. 2. To display the characters in the **WPA Passphrase (Network Key)** field, select the **Show Passphrase** check box. 3. Type a passphrase of at least eight characters in the **WPA Passphrase (Network Key)** field. **Note:** For information about requirements for a WPA passphrase, see *Table 15* on page 362.

Table 10. Network authentication and data encryption settings (continued)

Network Authentication Selection	Data Encryption Options	Configuration Steps
WPA2-PSK	AES TKIP + AES	To configure WPA2-PSK authentication: 1. From the **Data Encryption** menu, select the type of encryption: - **AES**. Supports AES only. - **TKIP + AES**. Supports both TKIP and AES. 2. To display the characters in the **WPA Passphrase (Network Key)** field, select the **Show Passphrase** check box. 3. Type a passphrase of at least eight characters in the **WPA Passphrase (Network Key)** field. **Note:** For information about requirements for a WPA passphrase, see *Table 15* on page 362.
WPA-PSK & WPA2-PSK **Note:** Use this option if the network includes both WPA and WPA2 clients.	TKIP + AES	To configure WPA-PSK & WPA2-PSK authentication: 1. To display the characters in the **WPA Passphrase (Network Key)** field, select the **Show Passphrase** check box. 2. Type a passphrase of at least eight characters in the **WPA Passphrase (Network Key)** field. **Note:** The **Data Encryption** menu displays **TKIP + AES**, which is the only available option. Both TKIP and AES are supported. **Note:** For information about requirements for a WPA passphrase, see *Table 15* on page 362.

Manage Authentication Servers and Authentication Server Groups

You can set up internal and external authentication servers and server groups that the wireless controller can use for authentication.

Authentication Server Concepts

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 WiFi clients on the User Management page (see *Manage Users, Accounts, and Passwords* on page 230.)
- **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 must specify its configuration on the basic Authentication Server page (see *Configure Basic Authentication Server Settings* on page 141) 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:

- You must add the IP address of the wireless controller as a RADIUS client to the RADIUS server. All managed access points are then automatically known to the RADIUS server.
- For configuration guidelines for external MAC authentication, see *Guidelines for External MAC Authentication* on page 145.
- For configuration guidelines for external authentication of captive portal users, see *Manage Guest Network Access Through Guest Portals and Captive Portals* on page 218.

- **External LDAP server**. You can define one external LDAP server (commonly referred to as an Active Directory [AD] server). You must specify its configuration on the basic Authentication Server page (see *Configure Basic Authentication Server Settings* on page 141) 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.

Note: For authentication, you can configure and use a single LDAP server only. However, you can configure and use several RADIUS servers.

The settings that you specify on the Authentication Server page affect the selections that are available in the **Network Authentication** menu and the corresponding **Authentication Server** field on the Edit Profile page. For information about how to configure security profiles, see *Configure a Profile in the Basic Profile Group* on page 123 and *Configure a Profile in an Advanced Profile Group* on page 130.

Configure Basic Authentication Server Settings

Use the basic Authentication Server page 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 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. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

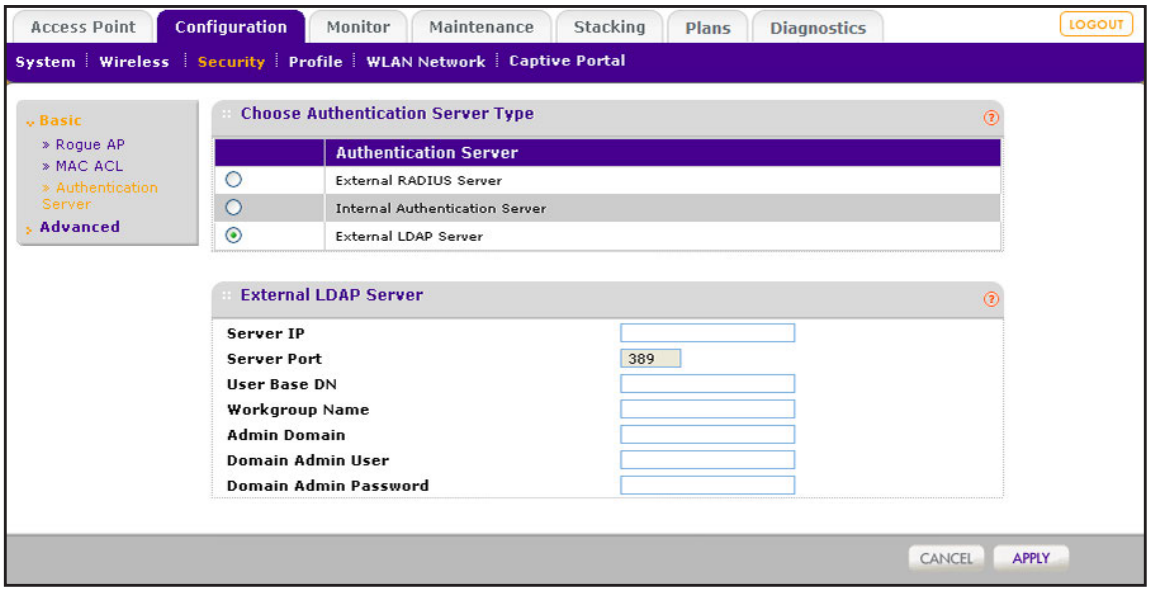
   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Basic > Authentication Server**.

   The basic Authentication Server page displays. The following figure shows the fields for an external LDAP server:



5. 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**
6. Configure the settings that correspond to the selected authentication server as described in the following table.

Setting	Description		
External RADIUS Server	Enable Authentication	Select the **Enable Authentication** check box to enable authentication.	
	Enable Accounting	Select the **Enable Accounting** check box to enable accounting.	
	Primary Server	Do the following for each server: 1. Specify the IP address. 2. Specify the port. The default port is **1812**. 3. Specify the shared secret.	For information about shared secret requirements, see *Table 15* on page 362.
	Secondary Server		
	Reauthentication time (Seconds)	Specify the time (in seconds) after which reauthentication occurs for all WiFi clients.	
	Update Global Key Every (Seconds)	To enable update of the global key: 1. Select the **Update Global Key Every (Seconds)** check box. 2. Specify the interval (in seconds) after which the global key is updated for all WiFi clients.	
Internal Authentication Server	Reauthentication Time (seconds)	Specify the time (in seconds) after which reauthentication occurs for all WiFi clients.	When you use the internal authentication server, set up WiFi clients on the User Management page. For information, see *Manage Users, Accounts, and Passwords* on page 230.
	Update Global Key Every (seconds)	To enable update of the global key: 1. Select the **Update Global Key Every (Seconds)** check box. 2. Specify the interval (in seconds) after which the global key is updated for all WiFi 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 port is **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. **Note:** For information about password requirements, see *Table 15* on page 362.	

7. Click the **Apply** button.

   The changes are saved.

For information about how to add an authentication server to a security profile in the basic profile group, see *Configure a Profile in the Basic Profile Group* on page 123.

For information about how to add an authentication server to a security profile in an advanced profile group, see *Configure a Profile in an Advanced Profile Group* on page 130.

Configure a RADIUS Authentication Server Group

For greater security flexibility, you can create up to eight external RADIUS servers to authenticate and account for different groups of users. After you 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 server group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

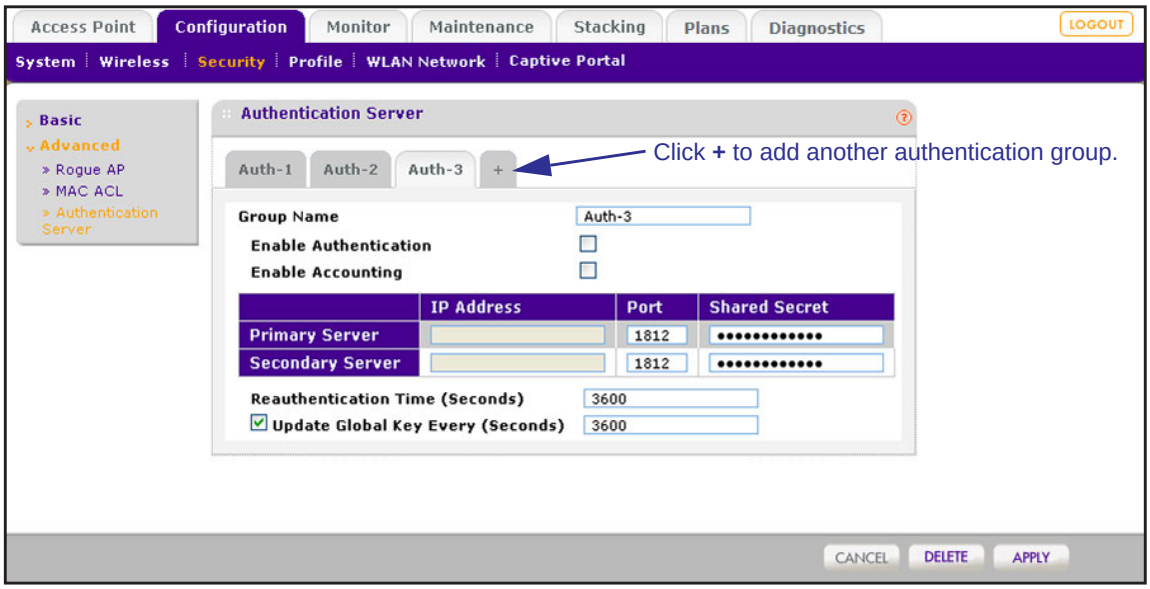
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Advanced > Authentication Server**.



5. Click the **+** button to create an additional authentication group.

The new authentication group displays on the advanced Authentication Server page, and the tab for the new authentication is automatically selected to let you configure the new group.

6. In the **Group Name** field, enter a unique name for the authentication group.

   By default, authentication groups are named **Auth-1**, **Auth-2**, **Auth-3**, and so on.

7. Specify the tasks for the accounting group by selecting one or both of the following check boxes:
   - **Enable Authentication**. Enables the authentication group to authenticate users.
   - **Enable accounting**. Enables the authentication group to perform accounting for users sessions.

8. Configure the external RADIUS server for the group.

   For information about setting up an external RADIUS server, see the table in the previous section, *Configure Basic Authentication Server Settings* on page 141.

9. Click the **Apply** button.

   The changes are saved.

For information about how to add a RADIUS authentication group to a security profile in the basic profile group, see *Configure a Profile in the Basic Profile Group* on page 123.

For information about how to add a RADIUS authentication group to a security profile in an advanced profile group, see *Configure a Profile in an Advanced Profile Group* on page 130.

Remove a RADIUS Authentication Server Group

You can remove a RADIUS authentication server group.

➢ **To remove a RADIUS authentication group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Advanced > Authentication Server**.

   The advanced Authentication Server page displays.

5. Click the tab for the RADIUS authentication group that you want to remove.
6. Click the **Delete** button.

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

Note the following external RADIUS server guidelines:

- For each MAC authentication client, you must 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, 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.

The wireless controller supports a maximum of 4,096 MAC addresses per SSID.

Note: You cannot add multicast or broadcast MAC addresses to a MAC access control list (ACL).

➢ **To set up basic MAC authentication ACL:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

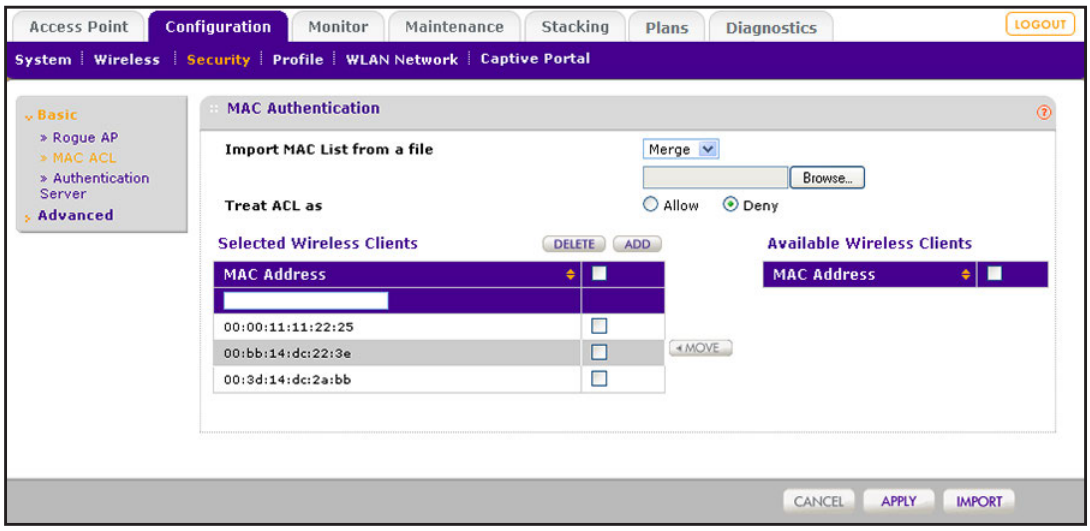
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Basic > MAC ACL**.



Note: As an option, you can import a list of MAC addresses from a file. For more information, see *Import a MAC List From a File* on page 147.

5. Next to Treat 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.
6. Add WiFi clients to the Selected Wireless Clients list through one of the following methods:
   - The MAC address that you want to add is in Available Wireless Clients list, which contains WiFi stations that are present in the vicinity of the access point:
     a. Select the MAC address from the Available Wireless Clients list.
     b. Click the **Move** button.
   - The MAC address that you want to add is not in Available Wireless Clients list:
     a. Enter the MAC address in the **MAC Address** field.
     b. Click the **Add** button.

7. Click the **Apply** button.

   The changes are saved.

Remove a MAC Address From a Wireless Client List

You can remove a MAC address from a wireless clients list.

➢ **To remove a MAC address from a wireless clients list:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Basic > MAC ACL**.

   The basic MAC Authentication page displays.

5. In the Selected Wireless Clients list, select the check boxes that correspond to the MAC addresses that you want to remove.
6. Click the **Delete** button.
7. Click the **Apply** button.

   The changes are saved.

For information about how to add a MAC ACL to a security profile in the basic profile group, see *Configure a Profile in the Basic Profile Group* on page 123.

For information about how to add a MAC ACL to a security profile in an advanced profile group, see *Configure a Profile in an Advanced Profile Group* on page 130.

Import a MAC List From a File

You can import a precompiled list of MAC addresses from a saved file. This file must 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 must 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. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

3. Enter your user name and password.
4. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

5. Select **Configuration > Security > Basic > MAC ACL**.

   The basic MAC Authentication page displays.

6. Click the **Browse** button, navigate to the file containing the list of MAC addresses, and select it.
7. Make one of the following selections from the **Import MAC List from a file** menu:
   - **Merge**. Merges the list of MAC addresses that you intend to import with the MAC addresses 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 the MAC addresses in the file that you intend to import.
8. Click the **Import** button.

   The wireless controller imports the MAC addresses that are in the text file into the Rogue List table.

9. Click the **Apply** button.

   The changes are saved.

Configure a Local MAC Authentication Group

For greater security flexibility, you can create up to eight 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.

The wireless controller supports a maximum of 4,096 MAC addresses per SSID.

Note: You cannot add multicast or broadcast MAC addresses to a MAC access control list (ACL).

➢ **To set up a MAC authentication group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

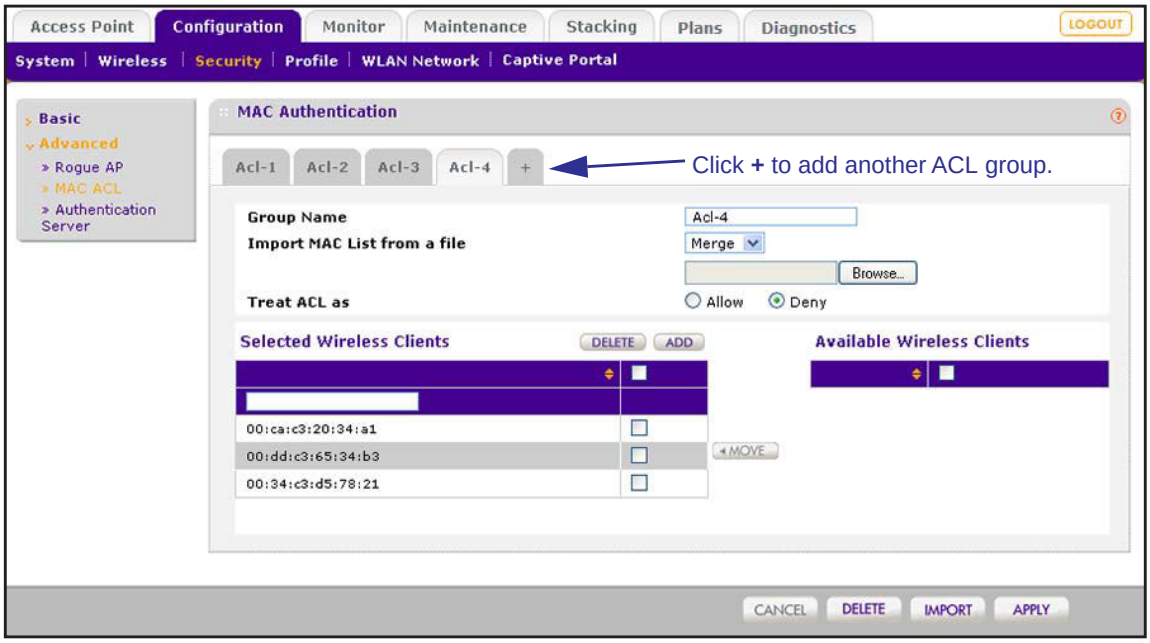
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Advanced > MAC ACL**.



5. Click the **+** button to create an additional ACL group.
6. The new ACL group displays on the advanced MAC Authentication page, and the tab for the new ACL is automatically selected to let you configure the new group.
7. In the **Group Name** field, enter a unique name for the ACL group.

   By default, profile groups are named **Acl-1**, **Acl-2**, **Acl-3**, and so on.

8. Compile the Selected Wireless Clients list.

   For information about how to compile a WiFi clients list, see *Configure Basic Local MAC Authentication Settings* on page 145.

9. Click the **Apply** button.

   The changes are saved.

For information about how to add a MAC authentication group to a security profile in the basic profile group, see *Configure a Profile in the Basic Profile Group* on page 123.

For information about how to add a MAC authentication group to a security profile in an advanced profile group, see *Configure a Profile in an Advanced Profile Group* on page 130.

Remove a Local MAC Authentication Group

You can remove a local ACL group.

➢ **To remove a local ACL group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Security > Advanced > MAC Authentication**.

   The advanced MAC Authentication page displays.
5. Click the tab for the ACL group that you want to remove.
6. Click the **Delete** button.

Select an ACL for a Profile in the Basic Profile Group

MAC authentication either allows or denies network access to clients on access point that are managed through a select profile in the basic profile group.

➢ **To select a local or external MAC ACL for a profile in the basic profile group:**

1. Configure a local MAC ACL or an external MAC ACL on an external RADIUS server.

   For more information about configuring a local MAC ACL, see *Configure Basic Local MAC Authentication Settings* on page 145 and *Configure a Local MAC Authentication Group* on page 148.

   For more information about configuring an external MAC ACL, see *Guidelines for External MAC Authentication* on page 145.
2. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
3. Enter your user name and password.

4. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

5. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) page displays.

6. Click the tab for the radio on which the profile is configured for which you want to select a MAC ACL.
7. Click the tab for the profile for which you want to select a MAC ACL.
8. On the Edit Profile page for the selected profile, next to MAC ACL, select a local or external MAC ACL:
   - **Local MAC ACL**:
     a. Select the **Local** radio button.
     b. From the **Local MAC ACL Group** menu, select a local MAC ACL.
   - **External MAC ACL**:
     a. Select the **External** radio button.
     b. From the **External Radius Server** menu, select the external RADIUS server on which the external MAC ACL is configured.
9. Click the **Apply** button.

   The changes are saved.

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

Select an ACL for a Profile in an Advanced Profile Group

MAC authentication either allows or denies network access to clients on access point that are managed through a select profile in the advanced profile group.

➢ **To select a local or external MAC ACL for a profile in an advanced profile group:**

1. Configure a local MAC ACL or an external MAC ACL on an external RADIUS server.

   For more information about configuring a local MAC ACL, see *Configure Basic Local MAC Authentication Settings* on page 145 and *Configure a Local MAC Authentication Group* on page 148.

   For more information about configuring an external MAC ACL, see *Guidelines for External MAC Authentication* on page 145.

2. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

3. Enter your user name and password.
4. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
5. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups page displays.
6. Click the tab for the profile group on which the profile is configured for which you want to select a MAC ACL.
7. Click the **Edit** button.

   The Edit Profile page displays.
8. Click the tab for the radio on which the profile is configured for which you want to select a MAC ACL.
9. Click the tab for the profile for which you want to select a MAC ACL.
10. On the Edit Profile page for the selected profile, next to MAC ACL, select a local or external MAC ACL:
    - **Local MAC ACL**:
      a. Select the **Local** radio button.
      b. From the **Local MAC ACL Group** menu, select a local MAC ACL.
    - **External MAC ACL**:
      a. Select the **External** radio button.
      b. From the **External Radius Server** menu, select the external RADIUS server on which the external MAC ACL is configured.
11. Click the **Apply** button.

    The changes are saved.

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

Discover and Manage Access Points

8

This chapter includes the following sections:

- *Access Point Discovery Guidelines*
- *Discover Access Points With the Discovery Wizard*
- *Manage the Managed AP List*
- *Assign Access Points to Buildings, Floors, and Advanced Profile Groups*

IMPORTANT:

Before you use the wireless controller to discover your access points and push the configurations to the access points, do the following:

1. Make sure that you register a sufficient number of licenses.

2. Determine which profiles and security you require.

3. If needed, set up authentication servers and MAC authentication.

4. Complete the configuration of the profiles that you intend to use.

These steps are described in *Register Your Licenses* on page 109 and in *Chapter 7, Manage Security Profiles and Profile Groups*.

Access Point Discovery Guidelines

You must 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 already deployed in a standalone configuration.

Both access points in the factory default state and deployed standalone access points run standalone firmware. For information about the minimum required standalone firmware versions, see *Supported NETGEAR Access Points* on page 26.

After the access points are discovered, you can add them to the Managed AP List, enabling the wireless controller to automatically upgrade the standalone firmware of the access points to managed-mode firmware. You can then use the wireless controller to configure, manage, and monitor the managed access points.

General Discovery Guidelines

An access point must run at least its initial firmware release or a newer version. For firmware requirements, see *Supported NETGEAR Access Points* on page 26. No other firmware requirements exist for the access point to function with the wireless controller.

Access points in the factory default state that are in the same Layer 2 network and are assigned the same IP address can still be discovered. Depending on the configuration of the DHCP server, these access points are discovered in parallel or sequentially.

Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 (vendor-specific information) with the IP address of the wireless controller. Whether you must enable option 43 on an *external* DHCP server in a Layer 2 network depends on the firmware version that the wireless controller is running:

- **Firmware version 4.x and earlier versions**. Option 43 must be enabled on an *external* DHCP server in a Layer 2 network.
- **Firmware version 5.x and later versions**. Option 43 is not required on an *external* DHCP server in a Layer 2 network.

Layer 3 Discovery Guidelines

The following are the requirements for autodiscovery of local access points across Layer 3 networks:

- Enable SNMP and SSH on all standalone access points. (This is the default setting for access points.)
- For all access points with a static IP address, access the web management interface of the access point and manually enter the IP address of the wireless controller in the **Controller IP** field. (This requirement does not apply to Layer 2 discovery.)
- Unblock UDP port number 7890 in the firewall.

- Assign each access point a unique IP address. (This requirement does not apply to Layer 2 discovery.) If two or more access points are assigned the same IP address, only one of them is discovered at a time. You must add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.
- Enable DHCP option 43 (vendor-specific information) on an *external* DHCP server. Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 with the IP address of the wireless controller.

  How you must configure DHCP option 43 depends on the type of external DHCP server:

  - **Layer 3 switch as a DHCP server**. If you use a Layer 3 switch as a 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 vendor-specific octets 02:04: must precede the hexadecimal address.

    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 add the vendor-specific octets, the complete address is 02:04:c0:a8:21:1b.

    In a configuration with stacked wireless controllers, use the octets that are shown in the following table.

    Table 11. Vendor-specific Octets

Number of Controllers	Octet
1 wireless controller	02:04
2 wireless controllers	02:08
3 wireless controllers	02:0c

    In a stacked configuration, to compose the address, start with the corresponding vendor-specific octet for the number of wireless controllers in the stack. 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 add the vendor-specific octet for a stack with three wireless controllers, the complete address is 02:0c:c0:a8:21:1b.

  - **Linux-based or Windows-based DHCP server**. If you use a Linux-based or Windows-based DHCP server, configure the IP address in decimal format and NETGEAR_WNC_AP as the vendor class identifier.

Remote Access Point Discovery Guidelines

The following guidelines apply to the discovery of remote access points:

- Enable SNMP and SSH on all standalone access points.
- Unblock the following ports in the firewall at the site where the wireless controller is located so that the remote access points can communicate with the wireless controller:
  - For models WC7600 and WC9500:
    - **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.
  - For models WC7500 and WC7600v2:
    - **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.
    - **TCP port 6670**. Used for communication and backward compatibility with access points that run an older firmware release.
    - **TCP port 6680**. Used for communication and backward compatibility with access points that run an older firmware release.
    - **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 datagram service.
    - **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 7000**. Used for Layer 3 roaming support.
    - **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.

  - **UDP port 7892**. Used for access point registration with the wireless controller after discovery.
  - **UDP port 7893**. Used for access point registration with the wireless controller during multicast discovery.
- 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.
- Convert access points behind a NAT router to managed access points and then install them behind the NAT router.
- Assign each access point an IP address. All access points that are the same model ship with the same default IP address. Except for access points in the factory default state that are in the same Layer 2 network at the remote site, if two or more access points are assigned the same IP address, then only one of them is discovered at a time. You must 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 must run at least its initial firmware release or a newer version. No other firmware requirements exist for the access point to function with the wireless controller.

  Tip: For management and monitoring purposes, make sure that you give 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 *Manage a Building and Floors for an RF Plan* on page 55. For information about assigning location, building, and floor names, see *Change Access Point Information on the Managed AP List* on page 168.

Limitations After Discovery

The following limitations apply after remote access points are 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 must 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.

Discover Access Points With the Discovery Wizard

The Discovery Wizard provides two methods to find access points that are not yet on the managed access point list. These methods are described in the following sections:

- *Discover Access Points in Factory Default State and Access Points in a Layer 2 Subnet*
- *Discover Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks*

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. Be sure that you set up security correctly (see *Chapter 7, Manage Security Profiles and Profile Groups*).

Discover Access Points in Factory Default State and Access Points in a Layer 2 Subnet

Access points in the factory default state are access points “out of the box” that were never employed. Access points in a Layer 2 subnet are access points that are installed and functioning in the same IP subnet as the wireless controller and that are connected to the wireless controller through a back-end Layer 2 switch.

Note: For information about DHCP option 43, see *General Discovery Guidelines* on page 154.

➢ **To discover access points in the factory default state and access points in a Layer 2 subnet:**

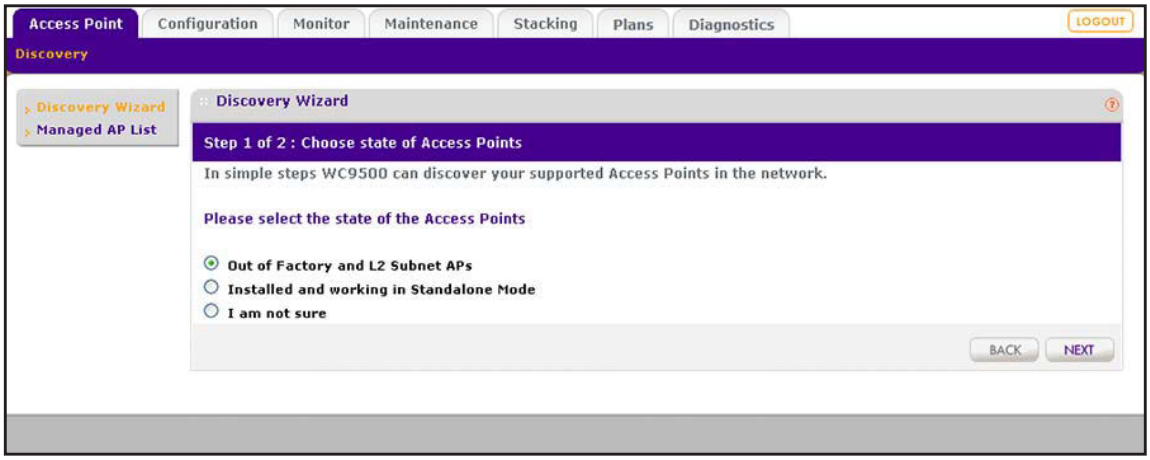
1. Open a web browser. In the browser’s address field, type the wireless controller’s IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller’s login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

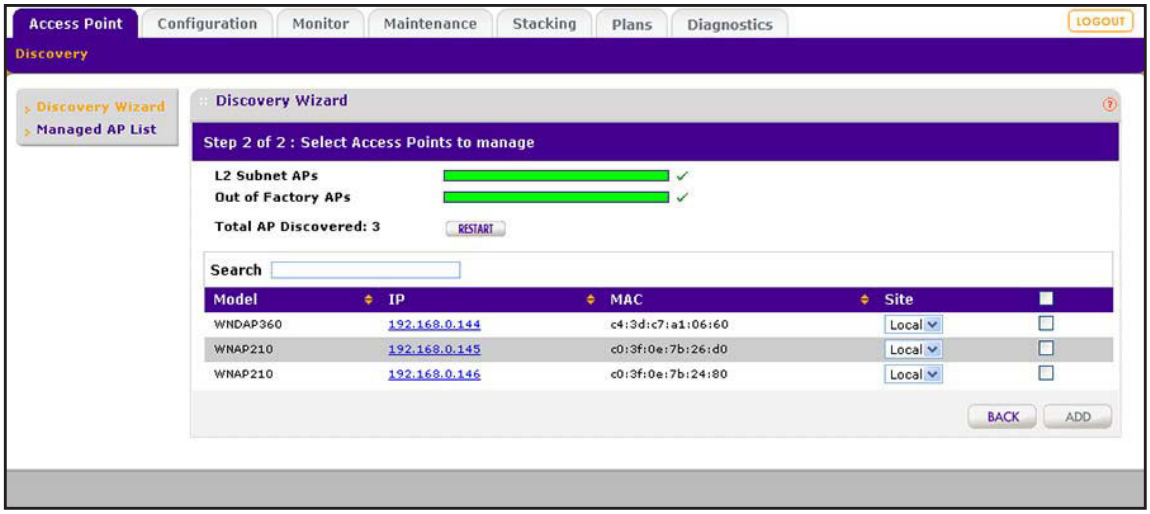
4. Select **Access Point > Discovery Wizard**.



5. Select the **Out of Factory and L2 Subnet APs** radio button.

Note: The **I am not sure** radio button directs you to the product documentation.

6. Click the **Next** button.



The wireless controller searches for NETGEAR products on the LAN based on MAC address and identifies which products are supported access point models. Progress bars show the progress of the discovery process.

When the discovery process is finished, the total number of access points is displayed and the table shows the access points that were discovered. For each access point, the table includes the model number, IP address, MAC address, and site.

7. To find an individual access point, enter information in the **Search** field.
8. To make sure that all the access points are listed, review the discovery results.

The effectiveness of the discovery process 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, discovery is simple.

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

- Access points that the wireless controller already manages 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 network.

  For information about how to discover access points in a different subnet, see *Discover Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks* on page 162.

- Access points that are in factory default mode but across a router are not detected.

  For information about how to discover access points across a router, see *Discover Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks* on page 162.

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

  For information about the wireless controller's DHCP server, see *Manage the DHCP Server* on page 105.

- For more information, see *Resolve Problems With Access Points* on page 355.

9. To run the discovery process again, click the **Restart** button.
10. To designate an access point as a remote access point, from the **Site** menu, select **Remote**.

    By default, all discovered access points are designated as **Local**. The **Remote** and **Local** designations are for organization only.

    Note: The wireless controller cannot discover remote access points over a site-to-site VPN connection or behind a remote NAT router without a VPN connection. To use an access point as a remote access point over a site-to-site VPN connection or behind a remote NAT router without a VPN connection, you must preprovision the access point and send it to the remote site for installation. For remote access points, the maximin WAN delay period is 100 millisecond.

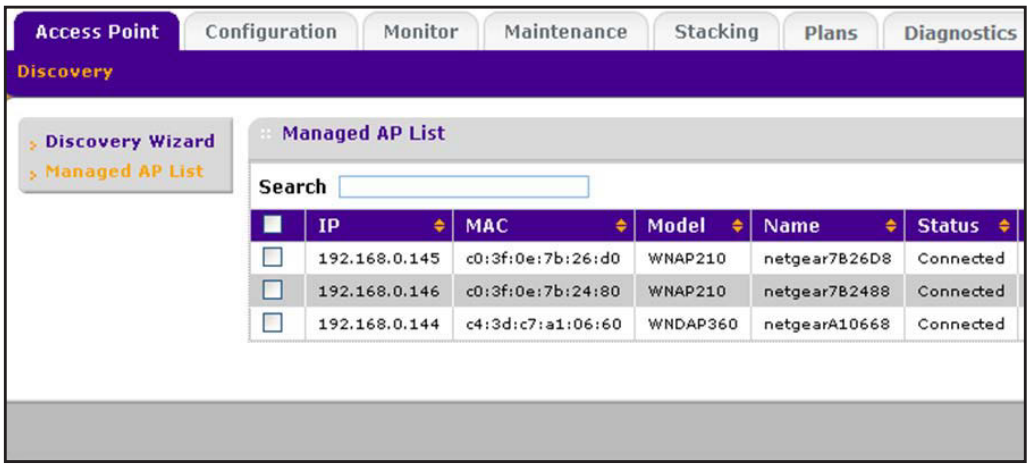
11. Either select individual access points to be added to the managed list or select all access points to be added to the managed list:
    - Select individual check boxes for discovered access points that you want to add to the managed list.
    - Select the check box in the upper right of the table heading to add all discovered access points to the managed list.

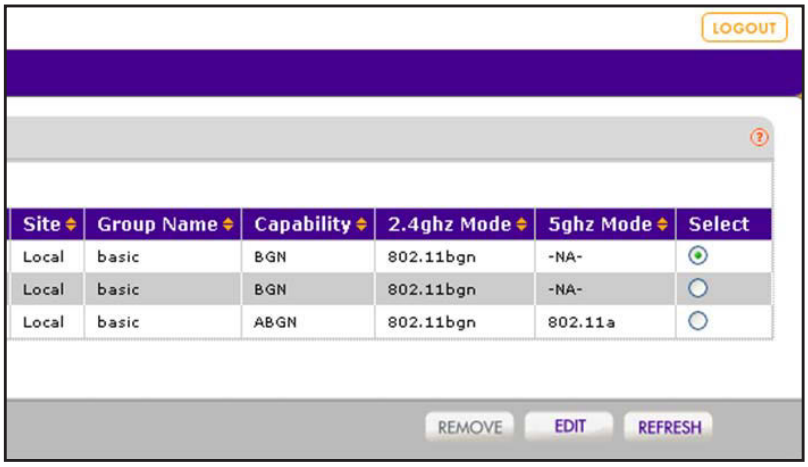
12. Click the **Add** button.

    Depending on the type of access points that were discovered, a page that lets you enter or ignore a login name and password might display.

13. If necessary, enter the login name and password.

    The Managed AP List page displays. Because this page is wide, it is shown in the following two figures.





After the access points are added to the Managed AP List, the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller, and the access points become managed access points. Depending on the number of access points that you add to the Managed AP List, this process might take several minutes.

By default, the access point upgrade process uses multicast. If you must configure a specific multicast IP address range for the upgrade process or disable multicast, see *Configure Multicast Firmware Upgrade for Access Points* on page 270.

If one or more access points do not transition to the Connected state (see the Status column in the Managed AP List), see *Resolve Problems With Access Points* on page 355.

For information about how to manage the Managed AP List, see *Manage the Managed AP List* on page 166.

Discover Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks

Access points that are installed and working in standalone mode in different Layer 3 networks are access points that do not function in the same subnet as the wireless controller but in different IP ranges and that are connected to the wireless controller through a router.

Note: Make sure that DHCP option 43 (vendor-specific information) is enabled on an *external* DHCP server. For more information, see *Layer 3 Discovery Guidelines* on page 154.

In a large WiFi network you might need to run the Discovery Wizard several times.

➢ **To discover access points in different Layer 3 networks:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

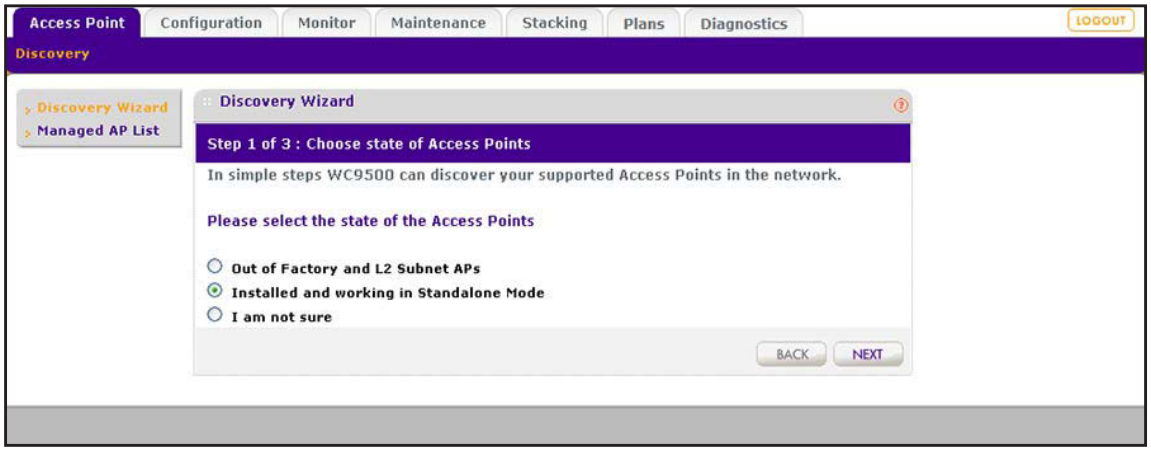
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

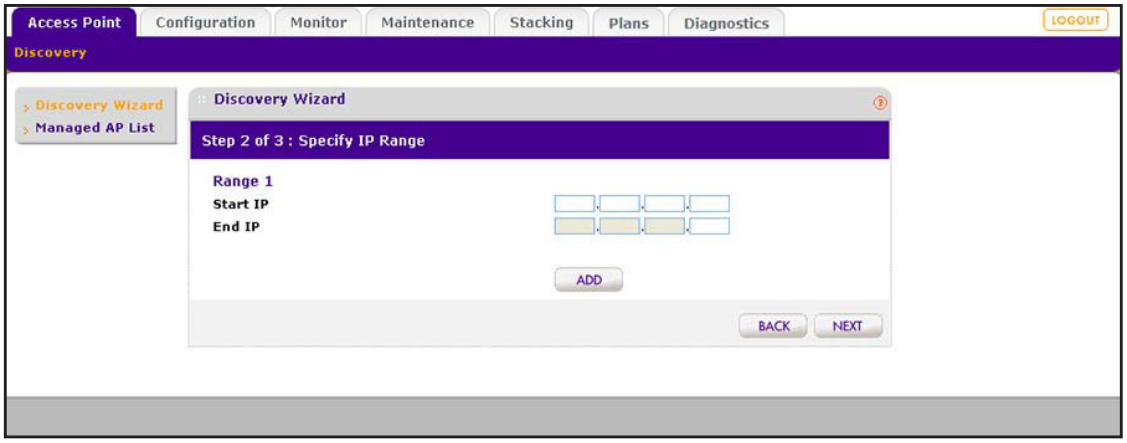
4. Select **Access Point > Discovery Wizard**.



5. Select the **Installed and working in Standalone Mode** radio button.

   Note: The **I am not sure** radio button directs you to the product documentation.

6. Click the **Next** button.



7. In the Range 1 section, fill in the **Start IP** and **End IP** fields.

   These IP addresses specify the range in which the wireless controller must discover access points.

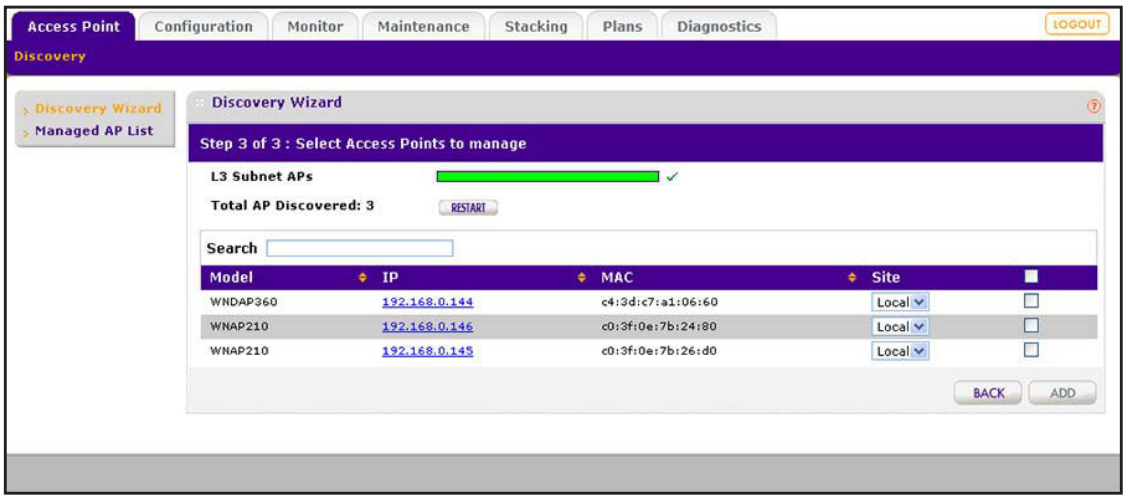
8. To add more IP address ranges for the wireless controller to search in, do the following:
   a. Click the **Add** button.

      The page adjusts to display a second set of **Start IP** and **End IP** fields.

   b. In the Range 2 section, fill in the **Start IP** and **End IP** fields.
   c. Click the **Add** button.

      The page adjusts to display a third set of **Start IP** and **End IP** fields.

   d. In the Range 3 section, fill in the **Start IP** and **End IP** fields.
9. Click the **Next** button.



The wireless controller searches for NETGEAR products on the LAN based on MAC address and then identifies which products are supported access point models. A progress bar show the progress of the discovery process.

When the discovery process is finished, the total number of access points is displayed and the table shows the access points that were discovered. For each access point, the table includes the model number, IP address, MAC address, and site.

10. To find an individual access point, enter information in the **Search** field.
11. To make sure that all the access points are listed, review the discovery results.

    The effectiveness of the discovery process 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, discovery is simple.

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

    - Access points that the wireless controller already manages are not in the discovery list.

      To view the Managed AP List, select **Access Point > Managed AP List**.

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

      For information about the wireless controller's DHCP server, see *Manage the DHCP Server* on page 105.

    - If more than one access point is assigned the same IP address, only one of them is discovered at a time.

      You must add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.

    - For more information, see *Resolve Problems With Access Points* on page 355.

12. To run the discovery process again, click the **Restart** button.
13. To designate an access point as a remote access point, from the **Site** menu, select **Remote**.

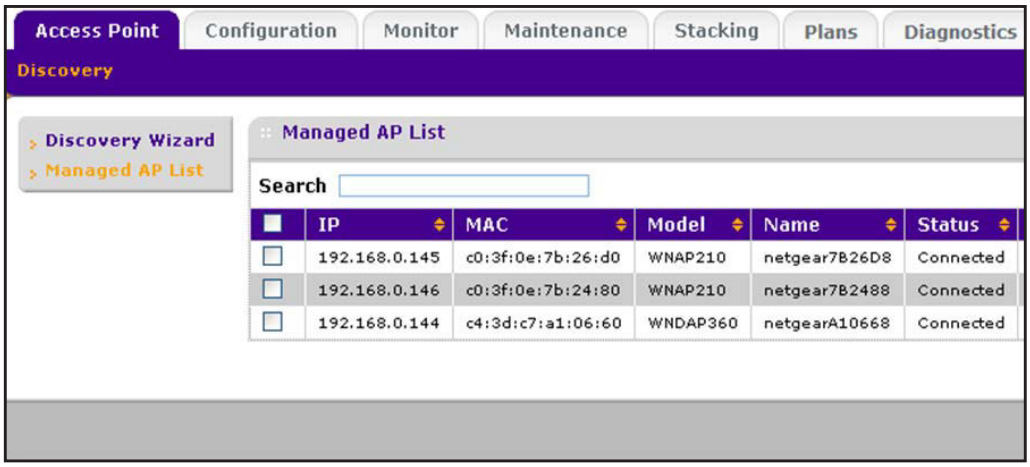
    By default, all discovered access points are designated as **Local**. The **Remote** and **Local** designations are for organization only.

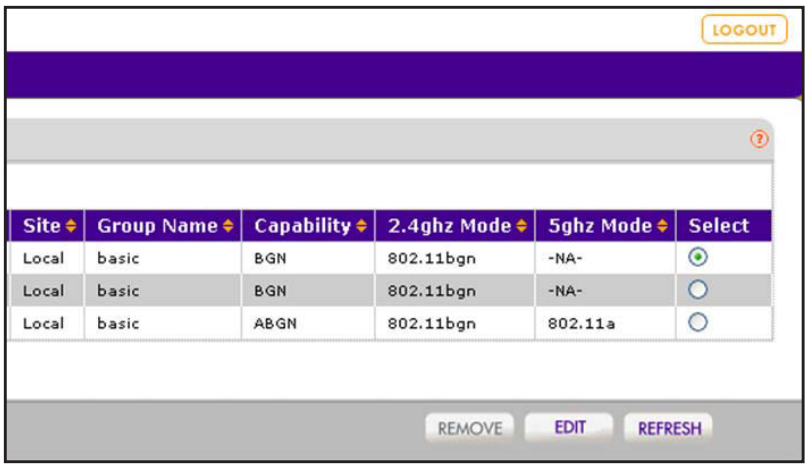
    Note: The wireless controller cannot discover remote access points over a site-to-site VPN connection or behind a remote NAT router without a VPN connection. To use an access point as a remote access point over a site-to-site VPN connection or behind a remote NAT router without a VPN connection, you must preprovision the access point and send it to the remote site for installation. For remote access points, the maximin WAN delay period is 100 millisecond.

14. Either select individual access points to be added to the managed list or select all access points to be added to the managed list:
    - Select individual check boxes for discovered access points that you want to add to the managed list.
    - Select the check box in the upper right of the table heading to add all discovered access points to the managed list.
15. Click the **Add** button.

    Depending on the type of access points that were discovered, a page that lets you enter or ignore a login name and password might display.
16. If necessary, enter the login name and password.

    The Managed AP List page displays. Because this page is wide, it is shown in the following two figures.





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

on the number of access points that you add to the Managed AP List, this process might take several minutes.

By default, the access point upgrade process uses multicast. If you must configure a specific multicast IP address range for the upgrade process or disable multicast, see *Configure Multicast Firmware Upgrade for Access Points* on page 270.

If one or more access points do not transition to the **Connected** state (see the Status column in the Managed AP List), see *Resolve Problems With Access Points* on page 355.

For information about how to manage the Managed AP List, see *Manage the Managed AP List* on page 166.

Manage the Managed AP List

After you add discovered access points to the Managed AP List, you can view the status of the access points on the list, change information for selected access point on the list, and remove access points from the list.

View the Managed AP List

The managed AP List displays the status, IP addresses, MAC addresses, model numbers, names, and other information for the managed access points.

➢ **To view the status and other information for managed access points:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

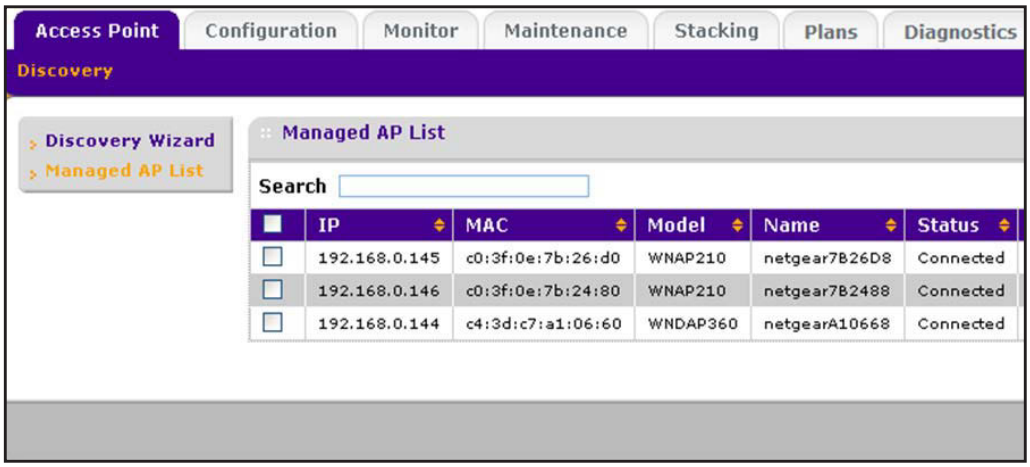
   The wireless controller's login window opens.

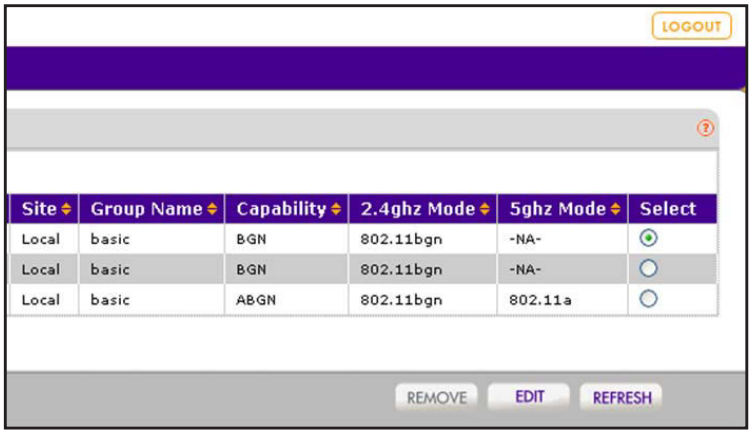
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Access Point > Managed AP List**.

   The Managed AP List page displays. Because this page is wide, it is shown in the following two figures.





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

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.

Item	Description
Status	Shows one of the following states: • **Authentication in progress**. This state occurs during the discovery and upgrade process of a standalone access point when the wireless controller logs in to the access point using the access point's password. This state can last several minutes. • **Firmware upgrade**. This state occurs after the access point receives the firmware file when the access point upgrades to the new firmware. This state can last several minutes. • **AP is rebooting**. This state occurs after the firmware upgrade process completes when the access point reboots. • **Applying configurations**. This state occurs after the wireless controller upgrades the firmware on the access point when the wireless controller pushes the WiFi configurations to the access point. • **Connecting**. This state occurs when the wireless controller attempts to establish a management connection with the access point. Make sure that a DHCP server is enabled in the network. Otherwise, the access point remains in the **Connecting** state and does not transition to the **Connected** state. • **Connected**. This state indicates that the firmware upgrade of the access point was successful, the WiFi configurations were pushed to the access point, and the access point is managed by the wireless controller. • **Not Connected**. This state indicates that the wireless controller cannot communicate with the access point at the configured IP address. The wireless controller attempts to log in to access points each minute. If the error is temporary, the state automatically changes to **Connected**. If the error is prolonged, verify the access point's IP address and network connectivity. For more information, see *Resolve Problems With Access Points* on page 355.
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote. For more information about designating an access point as local or remote, see *Discover Access Points With the Discovery Wizard* on page 158.
Group Name	The default group is **basic**. For information about changing the group for an access point, see *Change Access Point Information on the Managed AP List* on page 168.
Capability	The WiFi modes that the access point supports. **Note:** Capability information lets you determine which access points are 802.11n mode capable but function in 802.11g mode.
2.4ghz Mode	The access point's WiFi modes that function in the 2.4 GHz band.
5ghz Mode	The access point's WiFi modes that function in the 5 GHz band.

Change Access Point Information on the Managed AP List

For each individual access point, you can change the general information, IP settings, and VLAN settings, you can switch between the internal and external antenna (if the access point supports an external antenna), and you can enter location information.

➢ **To change the information for an access point on the Managed AP List:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

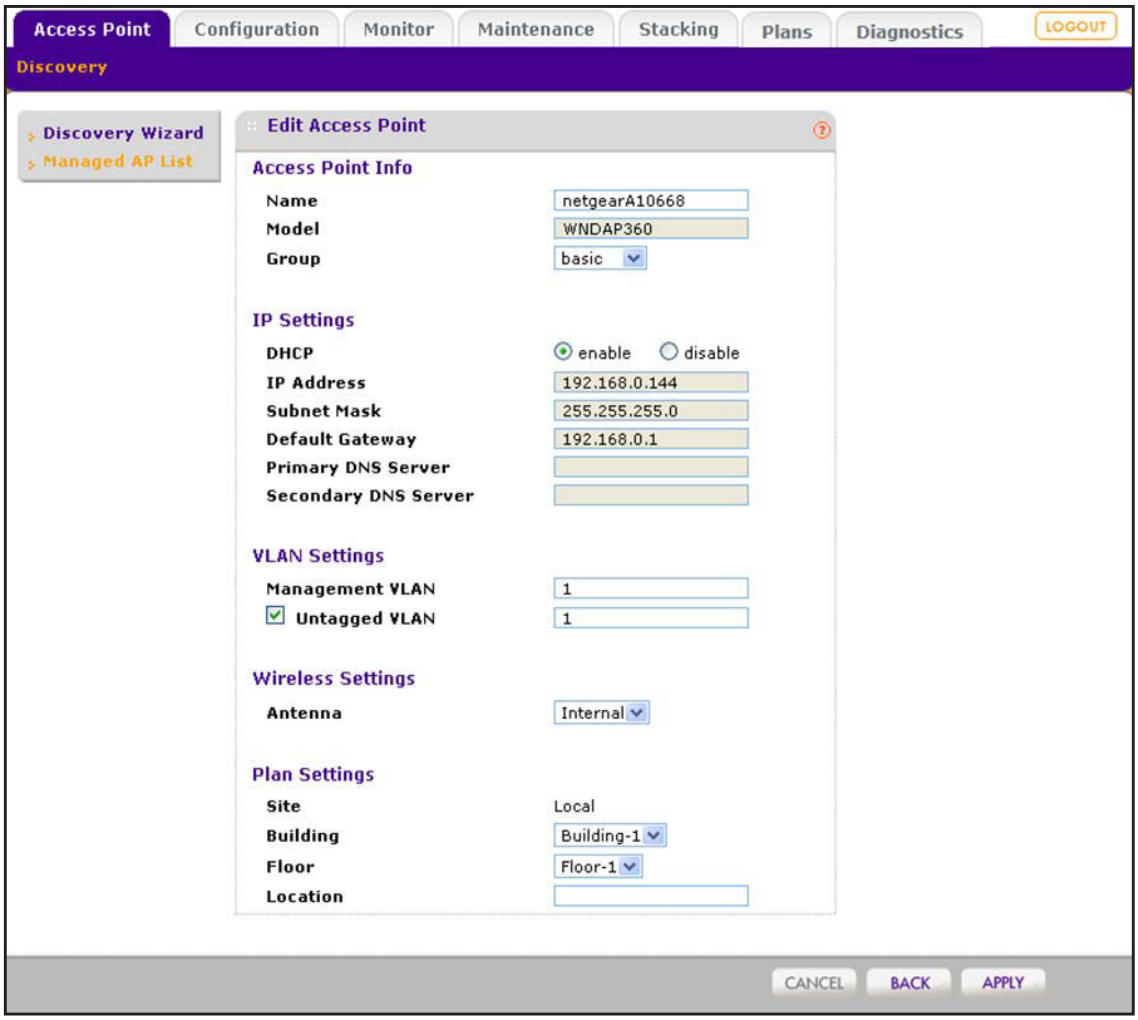
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Access Point > Managed AP List**.

   The Managed AP List page displays.

5. Select the access point that you want to change by selecting its radio button in the Edit column of the Managed AP List.
6. Click the **Edit** button.



7. Configure the settings as described in the following table.

Setting	Description
Access Point Info section	
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 changed.
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 set up profile groups, you can assign the access point to another profile group by selecting one from the menu. You can also change the group assignment later on the WLAN Group Assignment page. For more information, see *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172.
IP Settings 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. The following are the functions of the radio buttons: • **enable**. By default, the **enable** radio button is selected, allowing the access point to function as a DHCP client. The IP Settings fields are masked out, preventing you from changing the IP settings. • **disable**. Select the **disable** radio button to disable the access point's DHCP client. The IP Settings fields become available, allowing you to change the IP settings, including changes to the access point's IP address.	
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.
VLAN Settings section	
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 *Management VLAN* on page 35 and *Management VLAN Concepts* on page 101.
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.

Setting	Description
Wireless Settings section	
Antenna	You can specify which antenna the access point uses by making a selection from the menu: • **Internal**. The access point uses its internal antenna. • **External**. The access point uses its external antenna or antennas. External antennas are optional antennas that do not come standard with an access point.
Plan Settings section	
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote. For more information about designating an access point as local or remote, see *Discover Access Points With the Discovery Wizard* on page 158.
Building	Select a building from the menu. By default, the building designation is **Building-1**. For information about how to set up a custom building, see *Manage a Building and Floors for an RF Plan* on page 55.
Floor	Select a floor from the menu. By default, the floor designation is **Floor-1**. For information about how to set up a custom floor, see *Manage a Building and Floors for an RF Plan* on page 55.
Location	Enter a name that is meaningful to you.

8. Click the **Apply** button.

   The changes are saved.

9. Click the **Back** button.

   The Managed AP List page displays. Changes that you made on the Edit Access Point page are displayed in the table.

10. If the changes do not display in the table, click the **REFRESH** button.

Remove Access Points From the Managed AP List

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 reboot the access point.

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

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Access Point > Managed AP List**.

   The Managed AP List page displays.
5. Select the radio button to the right of the access point that you want to remove.
6. Click the **Remove** button.

Assign Access Points to Buildings, Floors, and Advanced Profile Groups

By default, all access points are automatically assigned to the basic profile group. However, you can assign access points to an advanced profile group. For information about how to create advanced profile groups, see *Add an Advanced Profile Group* on page 128.

By default, all access points are automatically assigned to the default building (Building-1) and default floor (Floor-1). However, you can assign access points to a custom building, custom floor, or both. For information about how to set up a custom building with custom floors, see *Manage a Building and Floors for an RF Plan* on page 55.

You can assign multiple access points simultaneously to a particular profile group, building, and floor.

Note: Access point profile group, profile group, and WLAN group are terms that are interchangeable.

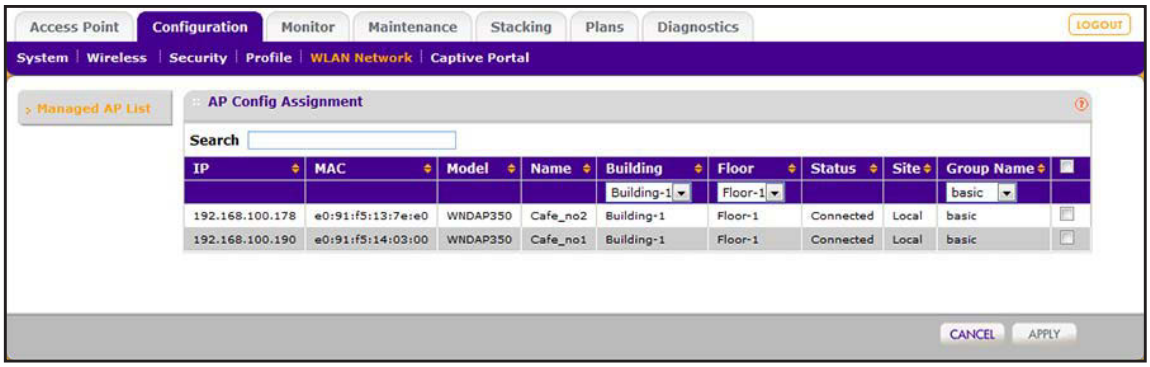
➢ **To view the default assignments and assign one or more access points to a building, floor, another profile group, or a combination of these:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > WLAN Network**.



The settings are described in the following table.

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 to which the access point is assigned. For information about selecting a building, see *Step 6*. By default, the building designation is **Building-1**. For information about how to set up a custom building, see *Manage a Building and Floors for an RF Plan* on page 55.
Floor	The floor to which the access point is assigned. For information about selecting a floor, see *Step 7*. By default, the floor designation is **Floor-1**. For information about how to set up a custom floor, see *Manage a Building and Floors for an RF Plan* on page 55.
Status	Shows one of the following states: • **Authentication in progress**. This state occurs during the discovery and upgrade process of a standalone access point when the wireless controller logs in to the access point using the access point's password. This state can last several minutes. • **Firmware upgrade**. This state occurs after the access point receives the firmware file when the access point upgrades to the new firmware. This state can last several minutes. • **AP is rebooting**. This state occurs after the firmware upgrade process completes when the access point reboots. • **Applying configurations**. This state occurs after the wireless controller upgrades the firmware on the access point when the wireless controller pushes the WiFi configurations to the access point. • **Connecting**. This state occurs when the wireless controller attempts to establish a management connection with the access point. Make sure that a DHCP server is enabled in the network. Otherwise, the access point remains in the **Connecting** state and does not transition to the **Connected** state.

Setting	Description
Status (continued)	• **Connected**. This state indicates that the firmware upgrade of the access point was successful, the WiFi configurations were pushed to the access point, and the access point is managed by the wireless controller. • **Not Connected**. This state indicates that the wireless controller cannot communicate with the access point at the configured IP address. The wireless controller attempts to log in to access points each minute. If the error is temporary, the state automatically changes to **Connected**. If the error is prolonged, verify the access point's IP address and network connectivity. For more information, see *Resolve Problems With Access Points* on page 355.
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote. For more information about designating an access point as local or remote, see *Discover Access Points With the Discovery Wizard* on page 158.
Group Name	The profile group to which the access point is assigned. For information about selecting a group, see *Step 8*. By default, the group designation is **basic**. For information about creating profile groups and their associated security profiles, see *Manage Security Profiles for Advanced Profile Groups* on page 128.

Tip: To view all members of a profile group, sort the access points by profile group. You do this by clicking the icon next to the Group Name header in the table.

5. Take one of the following actions:
   - Assign a single access point to another group, or building, floor, or a combination of these by selecting the check box to the right of the access point.
   - Assign a selection of access points to another group, building, or floor, or a combination of these by selecting the check boxes to the right of the access points.
   - Assign all access points to another group, building, or floor, or a combination of these by selecting the check box in the upper right of the table heading.
6. Select the building from the **Building** menu in the table heading.
7. Select the floor from the **Floor** menu in the table heading.
8. Select the group name from the **Group Name** menu in the table heading.
9. Click the **Apply** button.

   The changes are saved.

   The access points are assigned to the selected group, building, and floor.

Configure WiFi and QoS Settings

9

This chapter includes the following sections:

- *Basic and Advanced WiFi and QoS Configuration Concepts*
- *Configure the Radio*
- *Configure WiFi Settings*
- *Configure Channels*
- *Specify Radio Frequency Management*
- *Manage the Preferred Bands*
- *Manage Quality of Service for an Advanced Profile Group*
- *Manage Load Balancing*
- *Manage Rate Limiting*
- *Manage the LED Behavior*

Basic and Advanced WiFi and QoS Configuration Concepts

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 WiFi and Quality of Service (QoS) settings. Before you configure the WiFi settings, read *Basic and Advanced Setting Concepts* on page 32.

- **Basic WiFi settings**. If you use the basic configuration model, the following WiFi and QoS settings apply to all profiles in the basic profile group:
  - Basic radio on/off schedule
  - Basic WiFi settings for each radio in the basic profile
  - Basic RF management
  - Basic rate limiting for each radio in the basic profile
  - Basic preferred band settings for the WNDAP620 access points
- **Advanced WiFi settings**. If you use the advanced configuration model, you can configure the following WiFi and QoS settings separately for each profile group that you created:
  - Advanced radio on/off schedules for up to eight profile groups
  - Advanced WiFi settings for each radio in up to eight profile groups
  - Advanced QoS settings for each radio in up to eight profile groups
  - Advanced RF management for up to eight profile groups
  - Advanced rate limiting for each radio in up to eight profile groups
  - Advanced preferred band settings for the WNDAP620 access points
- **Global WiFi settings**. The following WiFi 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.

Configure the Radio for the Basic Profile Group

➢ **To schedule the radio for the basic profile group:**

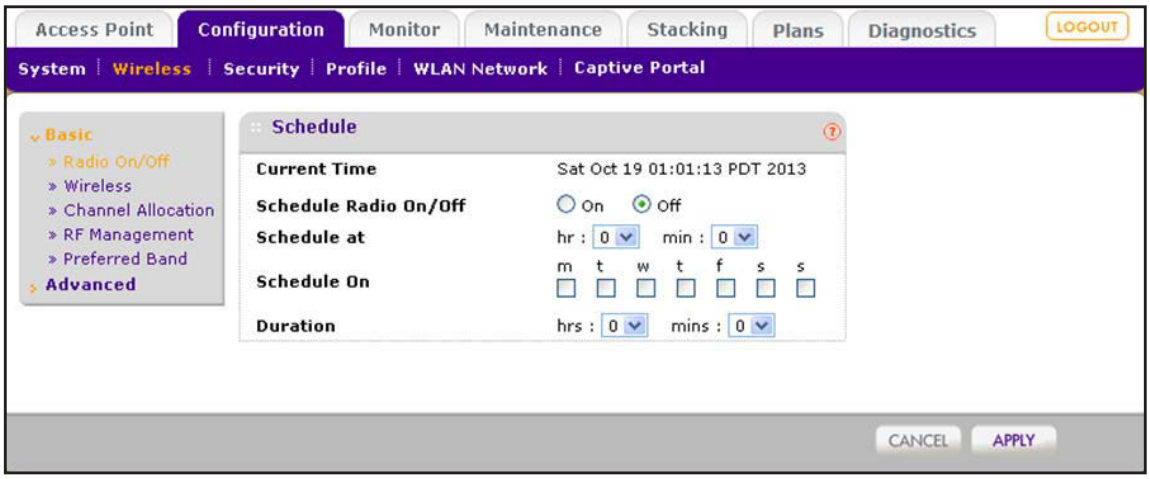
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Wireless > Basic > Radio On/Off**.



5. Configure the settings as described in the following table.

Setting	Description
Current Time	This field 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 **On** radio button or when it is off by selecting the **Off** radio button.
Schedule at	From the menus, 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 menus, select the duration (in hours and minutes) that the radio must be either on or off.

6. Click the **Apply** button.

   The changes are saved.

Configure the Radio for an Advanced Profile Group

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 an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

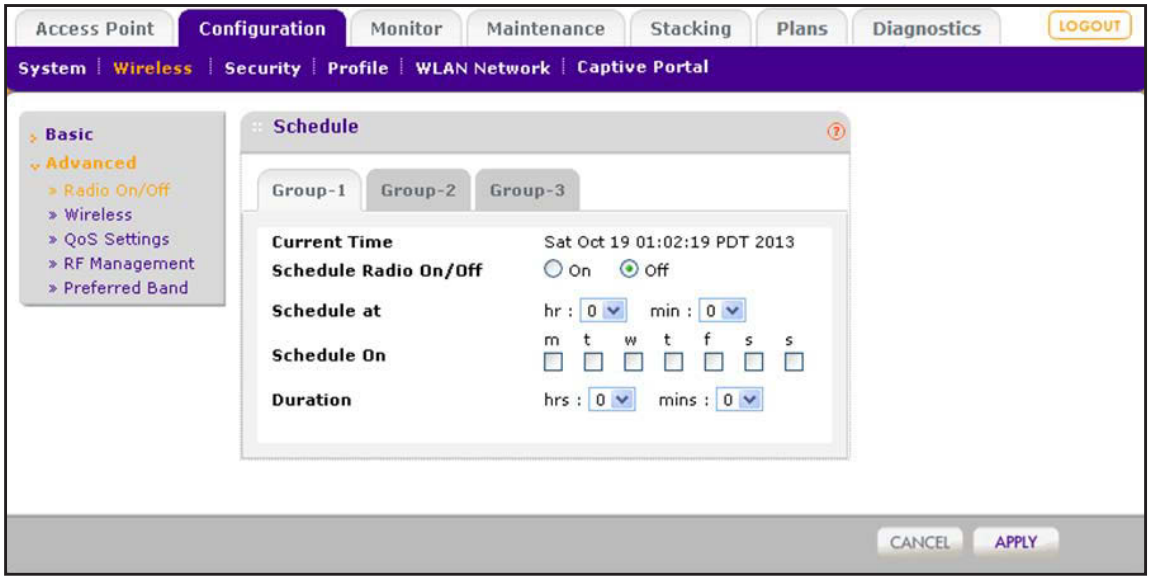
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > Radio On/Off**.



5. Click the tab for the profile group for which you want to configure the radio.
6. Configure the settings as described in the following table.

Setting	Description
Current Time	This field 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 **On** radio button or when it is off by selecting the **Off** radio button.
Schedule at	From the menus, 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 menus, select the duration (in hours and minutes) that the radio must be either on or off.

7. Click the **Apply** button.

   The changes are saved.

Configure WiFi Settings

During initial setup, you entered your country and region in the General Settings page (see *Configure the General Settings* on page 99). Based on your location and environment, the wireless controller determined the best WiFi settings for the discovered access points and pushed these settings to your managed access points.

IMPORTANT:

Unless your network and environment require that you use other WiFi settings, we recommend that you leave the WiFi settings as they are.

Typically, the default WiFi settings do not need adjustment. Override the WiFi settings only if a specific need exists, such as when the settings that a device vendor specifies are different from the default settings. You can configure WiFi settings for the basic profile group and for advanced profile groups (see *Configure WiFi Settings for an Advanced Profile Group* on page 185).

Configure WiFi Settings for the Basic Profile Group

Two requirements exist for you to be able to configure the WiFi settings on the Basic Wireless Settings page:

- You must disable automatic channel allocation for the radio on the Channel Allocation page. For information about channel allocation, see *Configure Channels* on page 191.
- At least one access point must be assigned to the profile group for the radio for which you want to configure the WiFi settings.

➢ **To configure WiFi settings for the basic profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

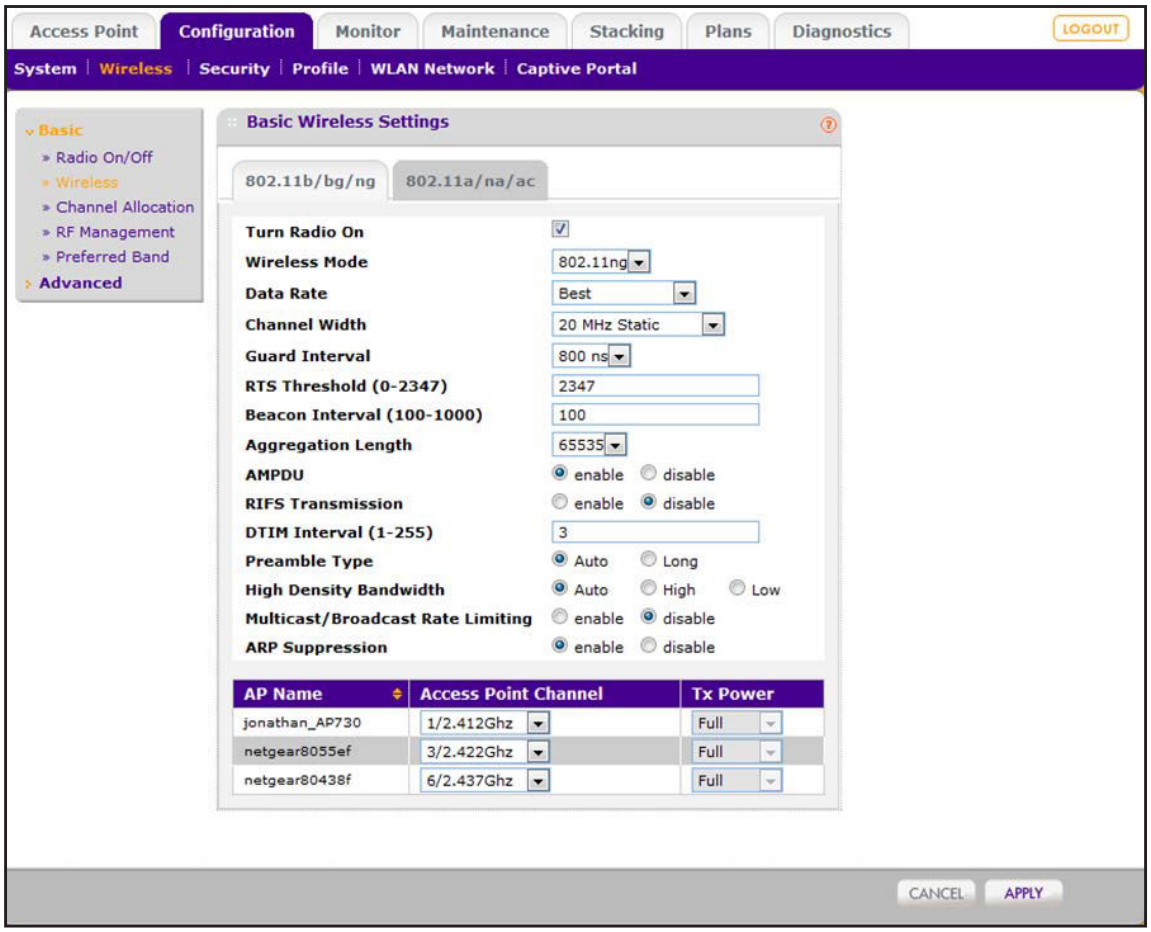
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Basic > Wireless**.



5. Click the tab for the radio for which you want to configure the WiFi settings.
6. Select the **Turn Radio On** check box.

   The WiFi settings become accessible and you can configure them. If you cannot select the **Turn Radio On** check box, see the requirements are the beginning of this section.

7. Configure the settings as described in the following table.

Setting	Description
Wireless Mode	The selections that are available depend on the selected radio mode. From the menu select the wireless mode: • 802.11b/bg/ng mode: - **802.11b**. - **802.11bg**. - **802.11ng**. This is the default setting. • 802.11a/na/ac mode: - **802.1a**. - **802.11na**. - **802.1na/ac**. This is the default setting. **Note:** 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.
Data Rate	From the menu, select the available transmit data rates of the WiFi network. **Note:** You can select the data rate only if the setting from the **Channel Width** menu is **20 MHz Static**. **Note:** If the setting from the **Channel Width** menu is **20 MHz Static** and you select **802.11na/ac** from the **Wireless Mode** menu, you can set separate data rates for 802.11na and 802.11ac devices.
Channel Width (802.11ng and 802.11na/ac only)	From the menu, select the channel width: • **20 MHz Static**. This is the default setting if the selection from the **Wireless Mode** menu is **802.11ng**. • **20/40 MHz Dynamic**. • **20/40/80 MHz Dynamic**. This is the default setting if the selection from the **Wireless Mode** menu is **802.1na/ac**. This setting is an option for 802.11na/ac devices only and does not apply to 802.11ng devices. A wider channel improves the performance, but some legacy devices can operate only with a 20 MHz channel width.
Guard Interval (802.11ng and 802.11na/ac only)	From the menu, 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.
RTS Threshold (0-2347)	Enter the size of the Request to Send (RTS) threshold packet. 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 must send an RTS threshold packet to the receiving station, and must wait for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.

Setting	Description
Beacon Interval (100-1000)	Enter the time interval for each beacon transmission that allows the access point to synchronize the WiFi network.
Aggregation Length (802.11ng and 802.11na/ac only)	Enter the maximum length of aggregated MAC protocol data unit (AMPDU) packets. Larger aggregation lengths could lead to better network performance. Aggregation is a mechanism used to achieve higher throughput. The default setting depends on the selection from the **Wireless Mode** menu: • If the selection from the **Wireless Mode** menu is **802.11ng** or **802.11na**, the default setting is 65535. • If the selection from the **Wireless Mode** menu is **802.11na/ac**, the default setting is 1048575.
AMPDU (802.11ng and 802.11na/ac only)	Select the **enable** radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabled is the default setting. Enabling AMPDU could lead to better network performance. Select the **disable** radio button to disable this option.
RIFS Transmission (802.11ng and 802.11na/ac only)	Select the **enable** radio button to enable the reduced interframe space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS could lead to better network performance. Select the **disable** radio button to disable this option. Disabled is the default setting.
DTIM Interval (1-255)	Enter the delivery traffic indication message (DTIM) or the data beacon rate that you want to use. The message period of the beacon delivery traffic indication is set in multiples of beacon intervals.
Preamble Type	Select one of the following radio buttons to specify the preamble type: • **Auto**. Automatically handles both long and short preambles. A short transmit preamble provides better performance. **Auto** is the default setting. • **Long**. Enables a long transmit preamble to provide a more reliable connection or a slightly longer range.
High Density Bandwidth (802.11ng and 802.11na/ac only)	Select the bandwidth type: • **Auto**. Automatically handles both high-density bandwidth (that is, high throughput) and low-density bandwidth (that is, extended range) environments. **Auto** is the default setting. • **High**. Enables a high bandwidth setting for dense environments in which multiple clients in a relatively small space require high bandwidth. One example of such an environment is a classroom in which multiple students stream video on individual WiFi devices. • **Low**. Enables a low bandwidth setting for sparse environments in which multiple clients are spread out over a relatively large space and do not require high bandwidth. One example of such an environment is a large office floor with multiple workers who do not all access the Internet or intranet simultaneously.

Setting	Description
Multicast/Broadcast Rate Limiting	Select the **enable** radio button to enable multicast and broadcast rate limiting, which can increase bandwidth and minimize interference. To configure the maximum packet rate, enter a packet rate in the **Multicast/Broadcast Rate Limiting Packet Count** field. By default, the wireless controller uses the following maximum packets rates: • For the 2.4 Ghz radio, up to 63 packets per second. • For the 5 GHz radio, up to radio 300 packets per second. Select the **disable** radio button to disable multicast and broadcast rate limiting. Disabled is the default setting.
ARP Suppression	Select the **enable** radio button to enable Address Resolution Protocol (ARP) suppression. ARP suppression decreases the management traffic that the wireless controller must handle. ARP suppression is enabled by default and applies to the wired interface only. With ARP suppression enabled, if the IP addresses of all WiFi clients that are associated with an access point are known, the wireless controller handles ARP requests in the following ways: • A packet with a known IP address is forwarded to its destination. • A packet with an unknown IP address is dropped. With ARP suppression enabled, if the IP address of at least one WiFi client that is associated with an access point is not known, the wireless controller broadcasts (that is, floods) the ARP requests into the WiFi network. Select the **disable** radio button to disable ARP suppression.

8. Click the **Apply** button.

   The changes are saved.

Override Channel and Transmission Power in the Basic Profile Group

The table on the Basic Wireless Settings page 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.

After you configure the WiFi settings for the basic profile group (see *Configure WiFi Settings for the Basic Profile Group* on page 179), you can change the channel, the transmission power, or both for individual access points in the basic profile group.

For you to be able to configure these settings in the table, two requirements exist:

- **Channel**. To enable the **Access Point Channel** menu in the table, you must disable automatic channel allocation on the Channel Allocation page (see *Configure Channels* on page 191).
- **Transmission power**. To enable the **Tx Power** menu in the table, you must disable automatic Tx power control on the basic RF Management page (see *Configure Radio Frequency Management for the Basic Profile Group* on page 195).

➢ **To override the channel and transmission power for individual access points in a security profile of the basic profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

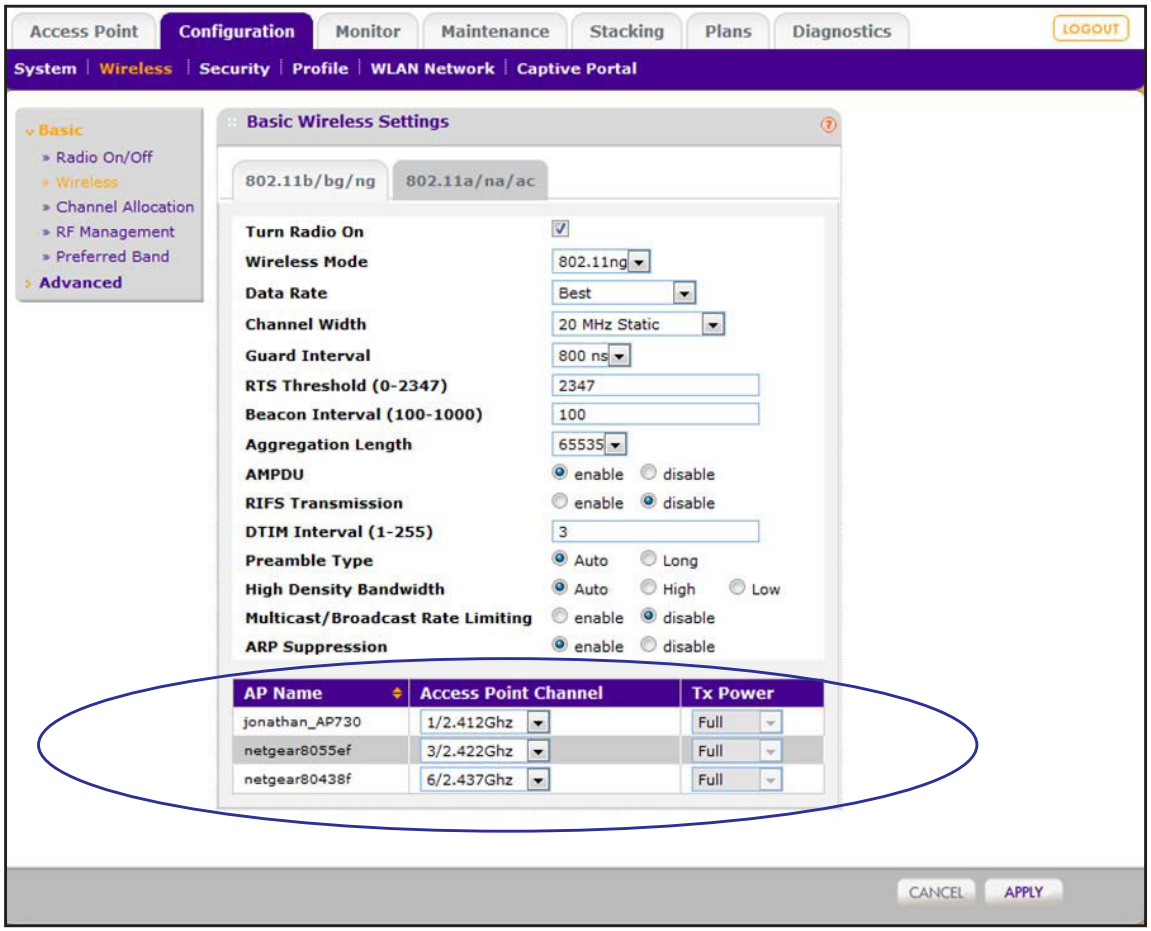
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Basic > Wireless**.



5. Click the tab for the radio for which you want to configure the WiFi settings.

6. Configure the settings in the table at the bottom of the page as described in the following table.

Setting	Description
AP Name	The name of the access point.
Access Point Channel	Override these settings only if a specific need exists. From the menu, select a channel and frequency for the access point to operate in. **Note:** Changing a channel might temporarily affect the traffic on the access point. **Note:** 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, the channel and frequency are set to the ones providing the highest performance. For more information, see *Configure Channels* on page 191.
Tx Power	From the menu, select the transmission power of the access point. **Note:** By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management page. For more information, see *Configure Radio Frequency Management for the Basic Profile Group* on page 195.

7. Click the **Apply** button.

   The changes are saved.

Configure WiFi Settings for an Advanced Profile Group

Two requirements exist for you to be able to configure the WiFi settings on the Advanced Wireless Settings page:

- You must disable automatic channel allocation for the radio on the Channel Allocation page. For information about channel allocation, see *Configure Channels* on page 191.
- At least one access point must be assigned to the profile group for the radio for which you want to configure the WiFi settings.

➢ **To configure WiFi settings for an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

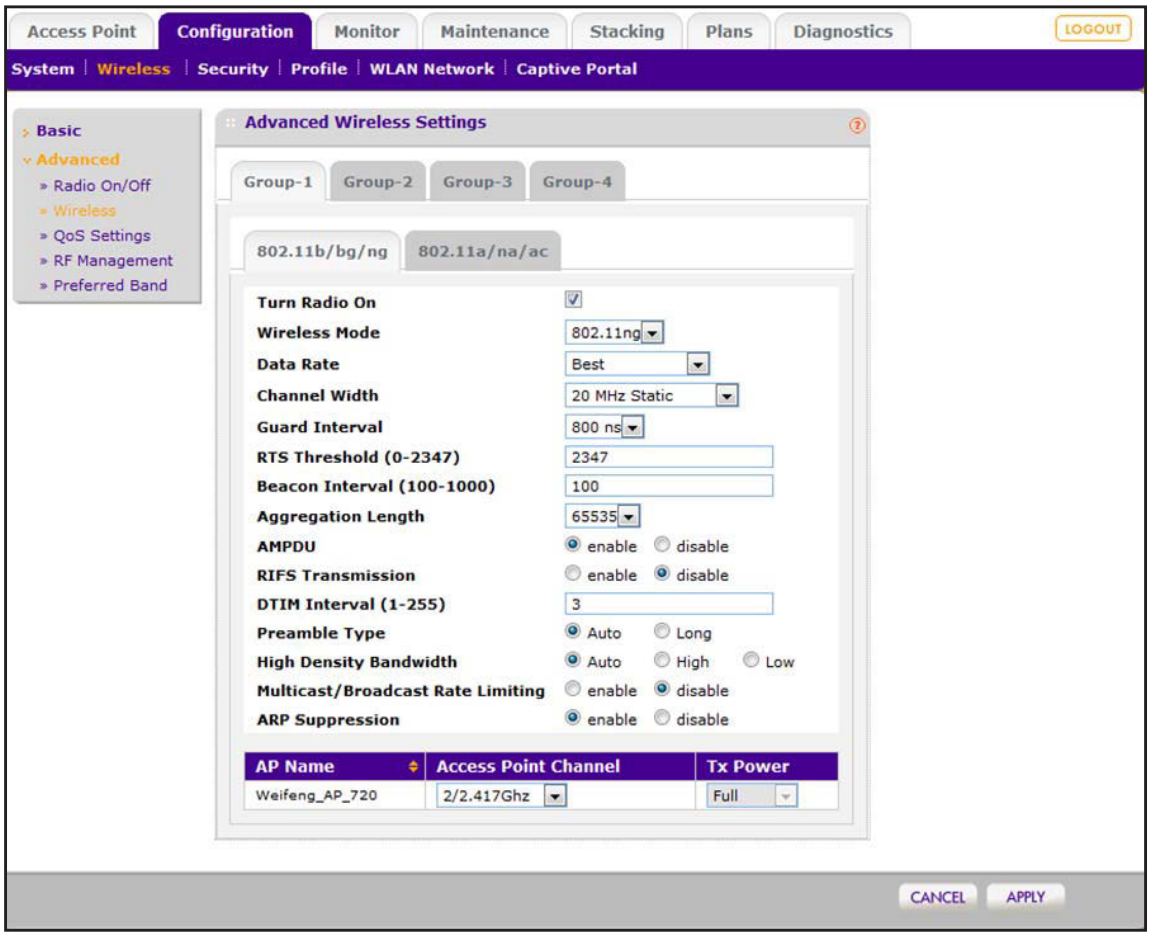
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > Wireless**.



5. Click the tab for the profile group for which you want to configure the WiFi settings.
6. Click the tab for the radio for which you want to configure the WiFi settings.
7. Select the **Turn Radio On** check box.

   The WiFi settings become accessible and you can configure them. If you cannot select the **Turn Radio On** check box, see the requirements are the beginning of this section.
8. Configure the settings as described in the following table.

Setting	Description
Wireless Mode	The selections that are available depend on the selected radio mode. From the menu select the wireless mode: • 802.11b/bg/ng mode: - **802.11b**. - **802.11bg**. - **802.11ng**. This is the default setting. • 802.11a/na/ac mode: - **802.1a**. - **802.11na**. - **802.1na/ac**. This is the default setting. **Note:** 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.
Data Rate	From the menu, select the available transmit data rates of the WiFi network. **Note:** You can select the data rate only if the setting from the **Channel Width** menu is **20 MHz Static**. **Note:** If the setting from the **Channel Width** menu is **20 MHz Static** and you select **802.11na/ac** from the **Wireless Mode** menu, you can set separate data rates for 802.11na and 802.11ac devices.
Channel Width (802.11ng and 802.11na/ac only)	From the menu, select the channel width: • **20 MHz Static**. This is the default setting if the selection from the **Wireless Mode** menu is **802.11ng**. • **20/40 MHz Dynamic**. • **20/40/80 MHz Dynamic**. This is the default setting if the selection from the **Wireless Mode** menu is **802.1na/ac**. This setting is an option for 802.11na/ac devices only and does not apply to 802.11ng devices. A wider channel improves the performance, but some legacy devices can operate only with a 20 MHz channel width.
Guard Interval (802.11ng and 802.11na/ac only)	From the menu, 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.
RTS Threshold (0-2347)	Enter the size of the Request to Send (RTS) threshold packet. 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 must send an RTS threshold packet to the receiving station, and must wait for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.

Setting	Description
Beacon Interval (100-1000)	Enter the time interval for each beacon transmission that allows the access point to synchronize the WiFi network.
Aggregation Length (802.11ng and 802.11na/ac only)	Enter the maximum length of aggregated MAC protocol data unit (AMPDU) packets. Larger aggregation lengths could lead to better network performance. Aggregation is a mechanism used to achieve higher throughput. The default setting depends on the selection from the **Wireless Mode** menu: • If the selection from the **Wireless Mode** menu is **802.11ng** or **802.11na**, the default setting is 65535. • If the selection from the **Wireless Mode** menu is **802.11na/ac**, the default setting is 1048575.
AMPDU (802.11ng and 802.11na/ac only)	Select the **enable** radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabled is the default setting. Enabling AMPDU could lead to better network performance. Select the **disable** radio button to disable this option.
RIFS Transmission (802.11ng and 802.11na/ac only)	Select the **enable** radio button to enable the reduced interframe space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS could lead to better network performance. Select the **disable** radio button to disable this option. Disabled is the default setting.
DTIM Interval (1-255)	Enter the delivery traffic indication message (DTIM) or the data beacon rate that you want to use. The message period of the beacon delivery traffic indication is set in multiples of beacon intervals.
Preamble Type	Select one of the following radio buttons to specify the preamble type: • **Auto**. Automatically handles both long and short preambles. A short transmit preamble provides better performance. **Auto** is the default setting. • **Long**. Enables a long transmit preamble to provide a more reliable connection or a slightly longer range.
High Density Bandwidth (802.11ng and 802.11na/ac only)	Select the bandwidth type: • **Auto**. Automatically handles both high-density bandwidth (that is, high throughput) and low-density bandwidth (that is, extended range) environments. **Auto** is the default setting. • **High**. Enables a high bandwidth setting for dense environments in which multiple clients in a relatively small space require high bandwidth. One example of such an environment is a classroom in which multiple students stream video on individual WiFi devices. • **Low**. Enables a low bandwidth setting for sparse environments in which multiple clients are spread out over a relatively large space and do not require high bandwidth. One example of such an environment is a large office floor with multiple workers who do not all access the Internet or intranet simultaneously.

Setting	Description
Multicast/Broadcast Rate Limiting	Select the **enable** radio button to enable multicast and broadcast rate limiting, which can increase bandwidth and minimize interference. To configure the maximum packet rate, enter a packet rate in the **Multicast/Broadcast Rate Limiting Packet Count** field. By default, the wireless controller uses the following maximum packets rates: • For the 2.4 Ghz radio, up to 63 packets per second. • For the 5 GHz radio, up to radio 300 packets per second. Select the **disable** radio button to disable multicast and broadcast rate limiting. Disabled is the default setting.
ARP Suppression	Select the **enable** radio button to enable Address Resolution Protocol (ARP) suppression. ARP suppression decreases the management traffic that the wireless controller must handle. ARP suppression is enabled by default and applies to the wired interface only. With ARP suppression enabled, if the IP addresses of all WiFi clients that are associated with an access point are known, the wireless controller handles ARP requests in the following ways: • A packet with a known IP address is forwarded to its destination. • A packet with an unknown IP address is dropped. With ARP suppression enabled, if the IP address of at least one WiFi client that is associated with an access point is not known, the wireless controller broadcasts (that is, floods) the ARP requests into the WiFi network. Select the **disable** radio button to disable ARP suppression.

9. Click the **Apply** button.

   The changes are saved.

Override Channel and Transmission Power in an Advanced Profile Group

The table on the Advanced Wireless Settings page shows the access points that are managed in the profiles of an advanced profile group and to which the channel allocation and advanced RF management settings apply.

After you configure the WiFi settings for an advanced profile group (see *Configure WiFi Settings for an Advanced Profile Group* on page 185), you can change the channel, the transmission power, or both for individual access points in an advanced profile group.

For you to be able to configure these settings in the table, two requirements exist:

- **Channel**. To enable the **Access Point Channel** menu in the table, you must disable automatic channel allocation on the Channel Allocation page (see *Configure Channels* on page 191).
- **Transmission power**. To enable the **Tx Power** menu in the table, you must disable automatic Tx power control on the advanced RF Management page (see *Configure Radio Frequency Management for an Advanced Profile Group* on page 197).

➢ **To override the channel and transmission power for individual access points in a security profile of an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

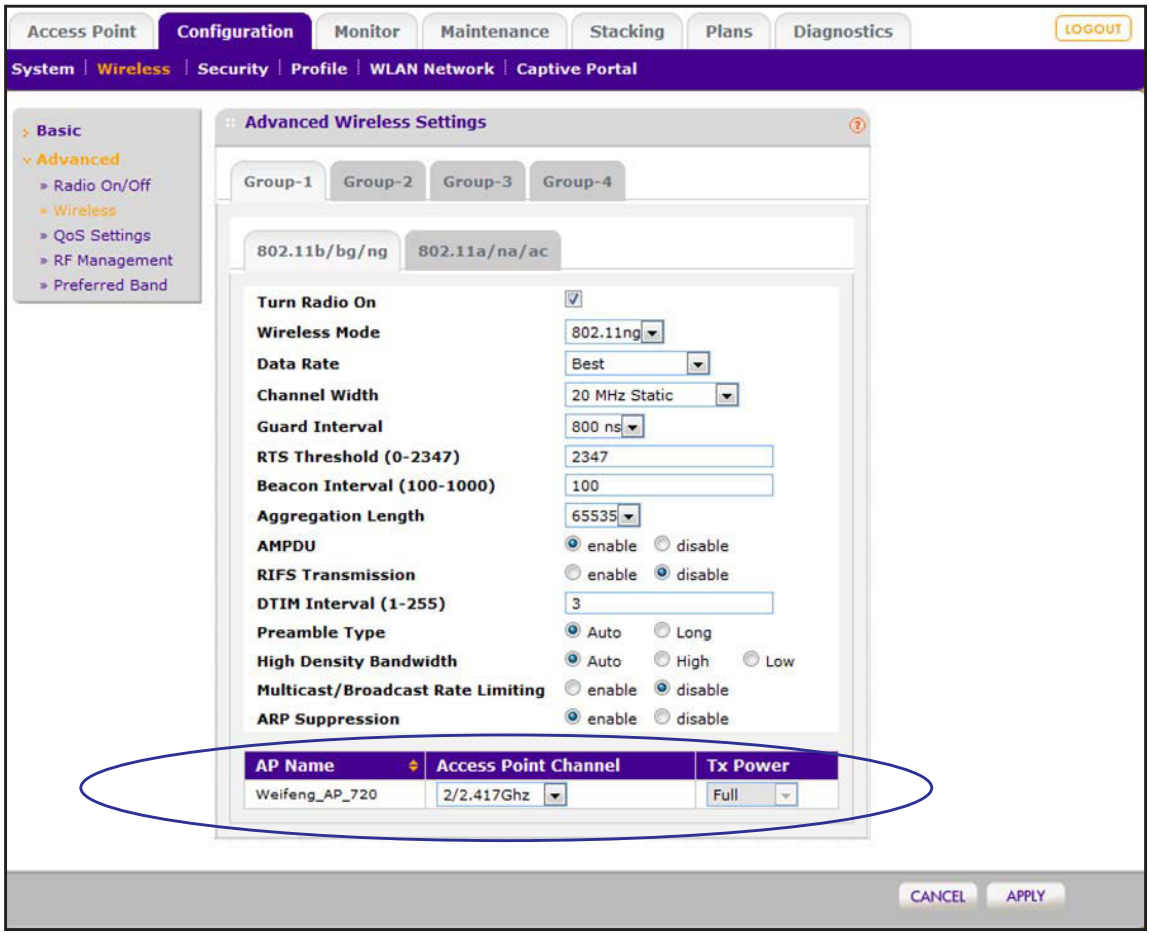
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > Wireless**.



5. Click the tab for the profile group for which you want to configure the WiFi settings.
6. Click the tab for the radio for which you want to configure the WiFi settings.

7. Configure the settings in the table at the bottom of the page as described in the following table.

Setting	Description
AP Name	The name of the access point.
Access Point Channel	Override these settings only if a specific need exists. From the menu, select a channel and frequency for the access point to operate in. **Note:** Changing a channel might temporarily affect the traffic on the access point. **Note:** 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, the channel and frequency are set to the ones providing the highest performance. For more information, see *Configure Channels* on page 191.
Tx Power	From the menu, select the transmission power of the access point. **Note:** By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management page. For more information, see *Configure Radio Frequency Management for an Advanced Profile Group* on page 197.

8. Click the **Apply** button.

   The changes are saved.

Configure Channels

CAUTION:

Do not disable channel allocation unless you are debugging or an extreme situation occurred 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. The wireless controller collects this information over the previous 24 hours and uses this information to determine the best possible channel for the access point.

Note: The wireless controller determines available channels based on the country or region that you specified on the General Settings page (see *Configure the General Settings* on page 99).

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

To adhere to best practices when adjusting channel allocation, we recommend 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.

Channel allocation is a global feature that applies to all access points. (If you disable channel allocation, it is globally disabled for all access points.) The allocated channels also 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.

However, you *can* override the general channel allocation settings for individual access points on the Basic Wireless Settings page and on the Advanced Wireless Settings page. For more information, see:

- *Override Channel and Transmission Power in the Basic Profile Group*
- *Override Channel and Transmission Power in an Advanced Profile Group*

➢ **To change the channel allocation:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

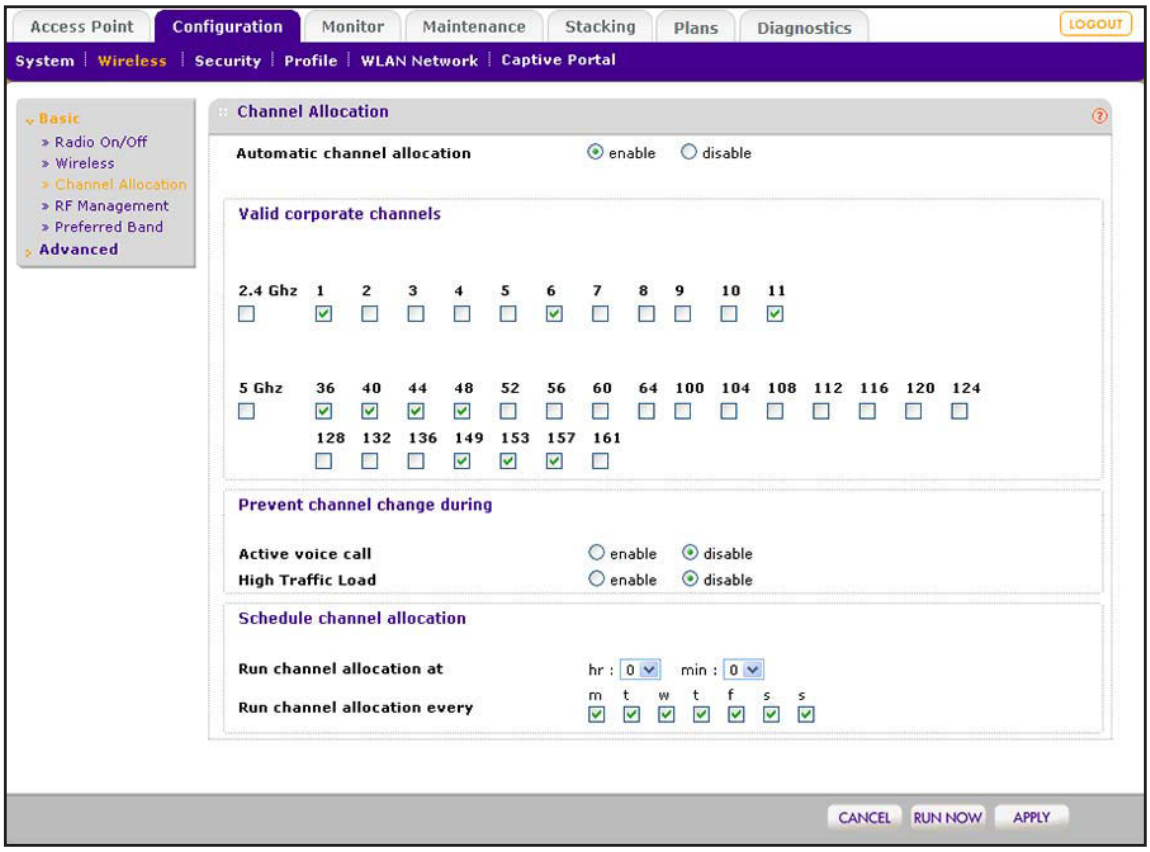
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Basic > Channel Allocation**.



5. Configure the settings as described in the following table.

Setting	Description
Automatic channel allocation	Ensure that the **enable** 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 **disable** radio button.
Valid corporate channels	Specify the WiFi band by selecting the **2.4 GHz** or **5 GHz** check box. For each WiFi band, the following applies: • You can remove one or more channels from the list of available channels by clearing their check boxes. For example, you might want to avoid interference with competing equipment such as in a medical environment in which medical devices use a specific channel. • You cannot add channels. The wireless controller determines available channels based on the country or region that you specified on the General Settings page (see *Configure the General Settings* on page 99).

Setting	Description	
Prevent channel change during **Note:** 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 **enable** radio button to prevent channel changes during voice calls. Select the **disable** radio button to allow channel changes during voice calls. Disabled is the default setting.
	High Traffic Load	Select the **enable** radio button to prevent channel changes during a high traffic load. Select the **disable** radio button to allow channel changes during a high traffic load. Disabled is the default setting.
Schedule channel allocation **Note:** We recommend 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 menus, select the hour and minutes when the channel allocation must run.
	Run channel allocation every	Select the check boxes to specify the day or days when the channel allocation must run.

IMPORTANT:

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

6. To run channel allocation immediately, click the **Run Now** button.

   The selected channels are applied to the managed access points. This option is useful when you add a new access point or change your network.

7. Click the **Apply** button.

   The changes are saved. If enabled, the channel allocation occurs according to the configured schedule.

Specify Radio Frequency Management

Radio frequency (RF) management lets you specify the transmission power settings, WLAN healing settings, and band steering settings.

Radio Frequency Concepts

Radio frequency (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 wireless controller by an access point.

WLAN healing is a special feature of RF management. When you use WLAN healing, if an access point goes down or loses connectivity, other access points share its load to avoid a

coverage hole. In such a situation, the other access points increase their transmit power. WLAN healing is configured per security profile group and is active among access points that share a common security configuration.

You can configure centralized RF management for the basic profile group on the basic RF Management page. If you use advanced profile groups, you can use the advanced RF Management page to customize settings for each advanced profile group.

WLAN Healing Concepts

The wireless controller supports automatic WLAN healing through the following features:

- **Automatic channel allocation**. Enables the wireless controller to distribute an access point channel automatically across the access points on a floor to reduce interference. Automatic channel allocation considers interference and the traffic load on the access point, 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 automatic channel allocation, including the option to skip automatic channel allocation during a heavy traffic load or voice activity, see *Configure Channels* on page 191.
- **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, we recommend the following:

- Configure the WLAN self-healing wait time to a value greater than the access point reboot time, which is usually one minute. Set an appropriate wait time to allow for fluctuations in the power of nearby access points when access points are rebooted.
- The number of neighbors to participate in WLAN self-healing must not be large (three to four usually suffices in most deployments). Keep the number of participants low to prevent too many access points from increasing power for a single failed access point.

Configure Radio Frequency Management for the Basic Profile Group

You can configure the WiFi transmission power, WLAN healing, and band steering for the basic profile group.

➢ **To configure RF management for access points in the basic profile group:**

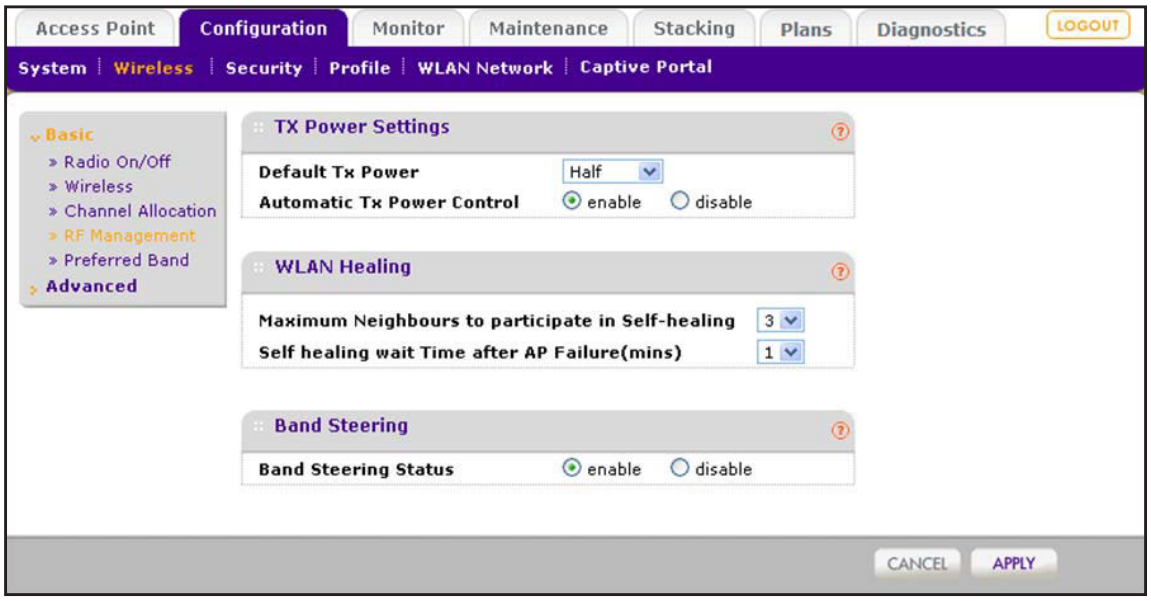
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Basic > RF Management**.



5. Configure the settings as described in the following table.

Setting	Description
TX Power Settings	
Default Tx Power	Make a selection from the menu to specify how the transmission (Tx) power is configured on the access points: **Full**, **Half**, **Quarter**, **Eighth**, or **Minimum**. By default, the selection from the menu is **Half**. When automatic Tx power control is enabled, the selection from the menu is used as the initial power level for the access points.
Automatic Tx Power Control	Select the **enable** radio button to enable automatic Tx power control: • 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. • When coverage areas overlap, the access point's Tx power is automatically decreased below default level. By default, automatic Tx power control is enabled. Select the **disable** radio button to disable automatic Tx power control.
WLAN Healing	
Maximum Neighbors to Participate in Self-healing	From the menu, 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. By default, the selection from the menu is **3**.

Setting	Description
Self healing wait Time after AP Failure	From the menu, 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 less than one minute. By default, the selection from the menu is **1**. Entering a value greater than the access point reboot time allows for fluctuations in the power of nearby access points when access points are rebooted.
Band Steering	
Band Steering Status	Select the **enable** radio button to enable band steering to the 5 GHz band for access points that support dual bands simultaneously. If band steering is enabled, the wireless controller identifies WiFi clients that are dual-band capable and can force them to connect to the 5 GHz band rather than 2.4 GHz band. WiFi clients that are already connected to the 2.4 GHz band can be forced into the 5 GHz band. In general, the 5 GHz band provides more channels, provides more bandwidth, and causes less interference for WiFi clients. By default, the **disable** radio button is selected, and band steering is disabled. **Note:** Load balancing can steer clients to stronger access points. For more information, see *Manage Load Balancing* on page 205.

6. Click the **Apply** button.

   The changes are saved.

Configure Radio Frequency Management for an Advanced Profile Group

You can configure the WiFi transmission power, WLAN healing, and band steering for advanced profile groups.

➢ **To configure RF management for access points in an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

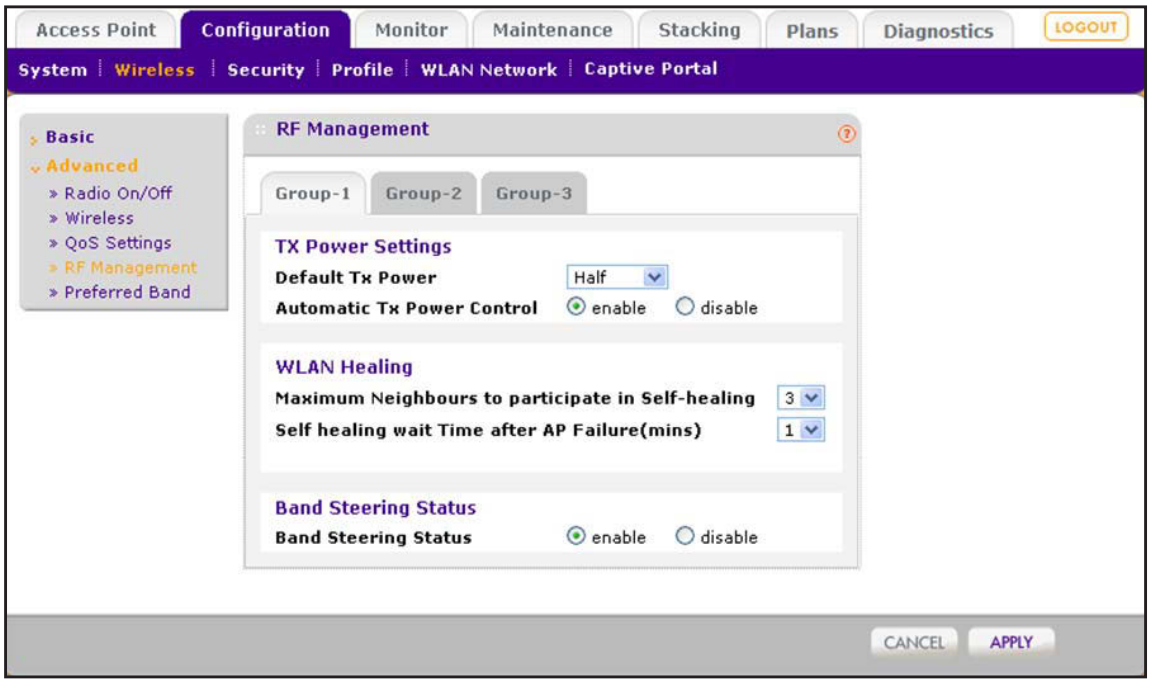
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > RF Management**.



5. Click the tab for the profile group for which you want to configure RF management.
6. Configure the settings as described in the following table.

Setting	Description
TX Power Settings	
Default Tx Power	Make a selection from the menu to specify how the transmission (Tx) power is configured on the access points: **Full**, **Half**, **Quarter**, **Eighth**, or **Minimum**. By default, the selection from the menu is **Half**. When automatic Tx power control is enabled, the selection from the menu is used as the initial power level for the access points.
Automatic Tx Power Control	Select the **enable** radio button to enable automatic Tx power control: • 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. • When coverage areas overlap, the access point's Tx power is automatically decreased below default level. By default, automatic Tx power control is enabled. Select the **disable** radio button to disable automatic Tx power control.
WLAN Healing	
Maximum Neighbors to Participate in Self-healing	From the menu, 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. By default, the selection from the menu is **3**.

Setting	Description
Self healing wait Time after AP Failure	From the menu, 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 less than one minute. By default, the selection from the menu is **1**. Entering a value greater than the access point reboot time allows for fluctuations in the power of nearby access points when access points are rebooted.
Band Steering	
Band Steering Status	Select the **enable** radio button to enable band steering to the 5 GHz band for access points that support dual bands simultaneously. If band steering is enabled, the wireless controller identifies WiFi clients that are dual-band capable and can force them to connect to the 5 GHz band rather than 2.4 GHz band. WiFi clients that are already connected to the 2.4 GHz band can be forced into the 5 GHz band. In general, the 5 GHz band provides more channels, provides more bandwidth, and causes less interference for WiFi clients. By default, the **disable** radio button is selected, and band steering is disabled. **Note:** Load balancing can steer clients to stronger access points. For more information, see *Manage Load Balancing* on page 205.

7. Click the **Apply** button.

   The changes are saved.

Manage the Preferred Bands

This feature applies to WNDAP620 access points only. The WNDAP620 access point can function in either the 802.11b/bg/ng band or the 802.11a/na band, but does not support concurrent band operation. The preferred band feature lets you switch between the bands. The selected band applies to all WNDAP620 access points in one profile group.

Note: WNDAP620 access points are supported on models WC7600 and WC9500 but not on models WC7500 and WC7600v2.

Configure the Preferred Band for WNDAP620 Access Points in the Basic Profile Group

For WNDAP620 access points that are members of the basic profile group, you can configure the preferred band that the access points operate in.

➢ **To configure the preferred band for WNDAP access points in the basic profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

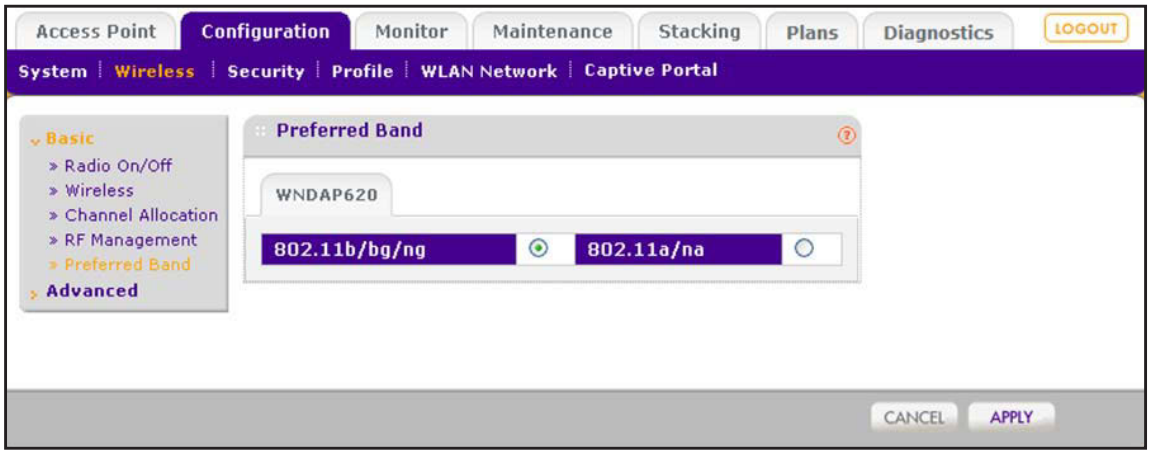
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Basic > Preferred Band**.



5. Select one of the following radio buttons:
   - **802.11b/bg/ng**. The WNDAP620 access points function in the combined 802.11b, 802.11bg, and 802.11ng band. By default, the **802.11b/bg/ng** radio button is selected.
   - **802.11a/na**. The WNDAP620 access points function in the combined 802.11a and 802.11na band.
6. Click the **Apply** button.

   The changes are saved. All WNDAP620 access points in the basic profile group now operate in the selected band.

Configure the Preferred Band for WNDAP620 Access Points in an Advanced Profile Group

For WNDAP620 access points that are members of an advanced profile group, you can configure the preferred band that the access points operate in.

➢ **To configure the preferred band for WNDAP access points in an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

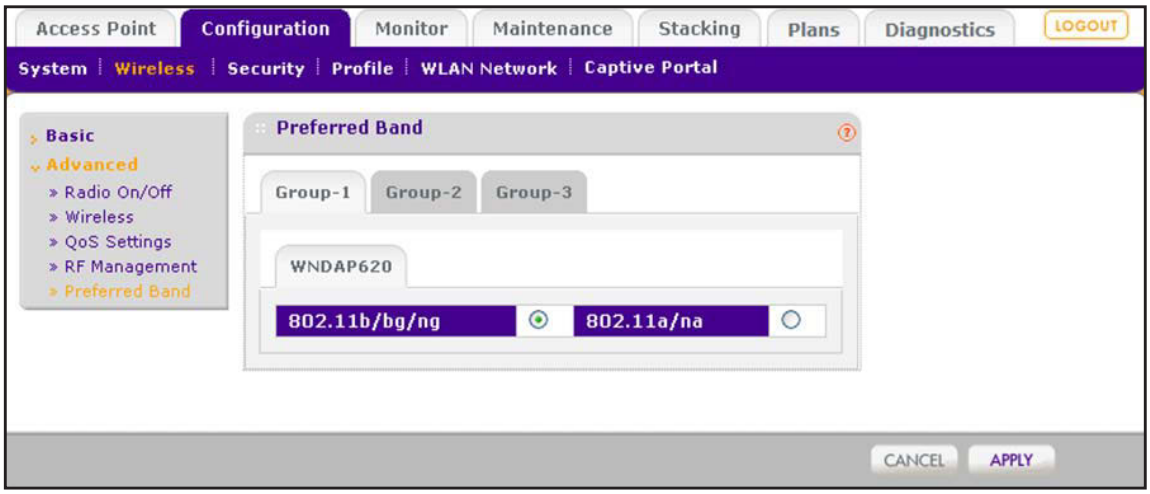
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > Preferred Band**.



5. Select one of the following radio buttons:
   - **802.11b/bg/ng**. The WNDAP620 access points function in the combined 802.11b, 802.11bg, and 802.11ng band. By default, the **802.11b/bg/ng** radio button is selected.
   - **802.11a/na**. The WNDAP620 access points function in the combined 802.11a and 802.11na band.
6. Click the **Apply** button.

   The changes are saved. All WNDAP620 access points in the selected advanced profile group now operate in the selected band.

Manage Quality of Service for an Advanced Profile Group

Quality of Service (QoS) management lets you fine-tune priorities for different types of traffic.

Quality of Service Concepts

Quality of Service (QoS) works by default for the advanced profile groups. Change QoS only if a specific reason exists, such as when specifications of a device vendor require you to use different QoS 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 WiFi medium access is enabled automatically. QoS settings on the access point control downstream traffic that flows from the access point to the client station (*AP* Enhanced Distributed Channel Access [EDCA] parameters) and the upstream traffic that flows from the client station to the access point (*Station* EDCA parameters).

The Advanced QoS Settings page lets you change the QoS settings per profile group and per radio for upstream traffic flowing from the station (that is, the WiFi 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.

Configure Quality of Service for a Profile Group

You can configure Quality of Service (QoS) settings for each advanced profile group.

➢ **To configure the QoS settings for a profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

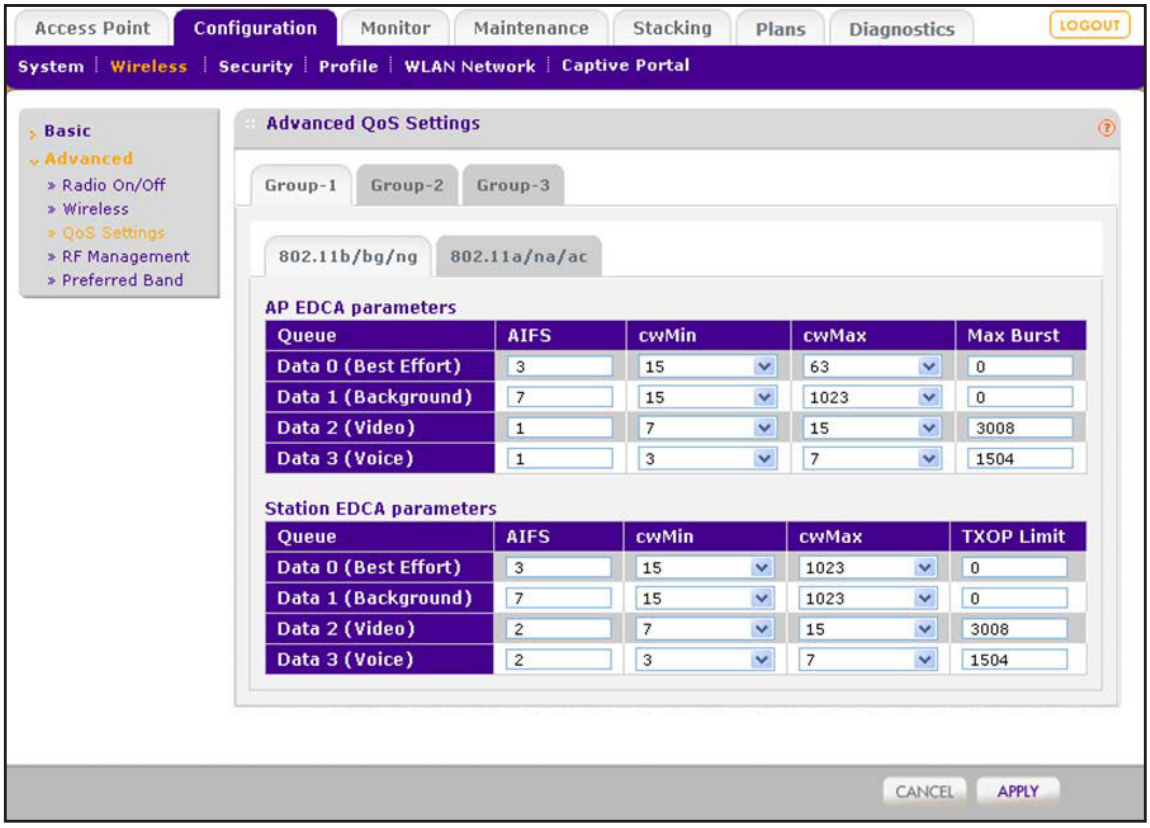
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Wireless > Advanced > QoS**.



5. Click the tab for the profile group for which you want to configure the QoS settings.
6. Click the tab for the radio for which you want to configure the QoS settings.
7. Configure the settings as described in the following table.

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">AIFS</td><td colspan="2">Specify a wait time (in milliseconds) for data frames. Valid values for arbitration inter-frame space (AIFS) are 1 through 255.</td></tr>
<tr><td>The following are the default values for the AP EDCA parameters:
• Data 0 (Best Effort). 3
• Data 1 (Background). 7
• Data 2 (Video). 1
• Data 3 (Voice). 1</td><td>The following are the default values for the Station EDCA parameters:
• Data 0 (Best Effort). 3
• Data 1 (Background). 7
• Data 2 (Video). 2
• Data 3 (Voice). 2</td></tr>
<tr><td rowspan="2">CwMin</td><td colspan="2">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 1023. The value for the minimum contention window (CwMin) must be lower than the value for the maximum contention window (CwMax).</td></tr>
<tr><td>The following are the default values for the AP EDCA parameters:
• Data 0 (Best Effort). 15
• Data 1 (Background). 15
• Data 2 (Video). 7
• Data 3 (Voice). 3</td><td>The following are the default values for the Station EDCA parameters:
• Data 0 (Best Effort). 15
• Data 1 (Background). 15
• Data 2 (Video). 7
• Data 3 (Voice). 3</td></tr>
<tr><td rowspan="2">CwMax</td><td colspan="2">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 1023. The value for the maximum contention window (CwMax) must be higher than the value for minimum contention window (CwMin).</td></tr>
<tr><td>The following are the default values for the AP EDCA parameters:
• Data 0 (Best Effort). 63
• Data 1 (Background). 1023
• Data 2 (Video). 15
• Data 3 (Voice). 7</td><td>The following are the default values for the Station EDCA parameters:
• Data 0 (Best Effort). 1023
• Data 1 (Background). 1023
• Data 2 (Video). 15
• Data 3 (Voice). 7</td></tr>
<tr><td rowspan="2">Max Burst
Note: AP EDCA parameters only</td><td colspan="2">Specify (in milliseconds) the maximum burst length allowed for packet bursts on the WiFi network.
A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0 through 8192. The maximum burst length applies only to AP EDCA parameters.</td></tr>
<tr><td colspan="2">The following are the default values for the AP EDCA parameters:
• Data 0 (Best Effort). 0
• Data 1 (Background). 0
• Data 2 (Video). 3008
• Data 3 (Voice). 1504</td></tr>
</table>

Setting	Description
TXOP Limit **Note:** Station EDCA parameters only	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.
	The following are the default values for the Station EDCA parameters: • **Data 0 (Best Effort). 0** • **Data 1 (Background). 0** • **Data 2 (Video). 3008** • **Data 3 (Voice). 1504**

8. Click the **Apply** button.

   The changes are saved.

Manage Load Balancing

Load balancing lets you balance WiFi clients over the managed access points of one model, taking the following aspects into account:

- The maximum number of clients that can connect to the access point model.
- The received signal strength indicator (RSSI) of the WiFi clients.

Load Balancing Concepts

Load balancing allows the wireless controller to distribute access point clients (the “load”) equally among the access points that it manages. You configure load balancing per type of access point model and per radio. By default, load balancing is disabled.

When a client discovers an access point using probe requests or sends association frames, the access point determines whether to accept the client based on the number of clients that are already connected, the signal strength of the clients that are already connected, and the signal strength of the client that attempts to connect.

The wireless controller performs load balancing based on the following criteria:

- **Maximum number of clients**. If more than the maximum number of clients that you allow on a radio of an access point attempt to associate, the clients are pushed to another access point.

  If you want a good distribution of clients between the access points, set the maximum number of clients to a low value (compared to, for example, the total number of clients in an office or on a floor).

- **Signal strength or RSSI**. Signal strength determines speed. For a client that is far away from an access point, the data rate is much lower than for a client that is in closer proximity to the access point. The distant client requires more time to transmit or receive data, and the delay could be too long. You can give a threshold for signal strength, which is specified as a percentage, from 0 percent to a maximum of 75 percent.

RSSI percentages translate into the following power levels in dBm:

- RSSI of 0% = –95 dBm (load balancing is disabled)
- RSSI of 25% = –81 dBm
- RSSI of 50% = –68 dBm
- RSSI of 75% = –55 dBm

In situations in which the throughput expectation is high, if you want only clients *near* an access point to associate with the access point, 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 fewer access points are available, set the RSSI to a lower value.

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

Configure Load Balancing

You can configure load balancing for each model of the managed access points.

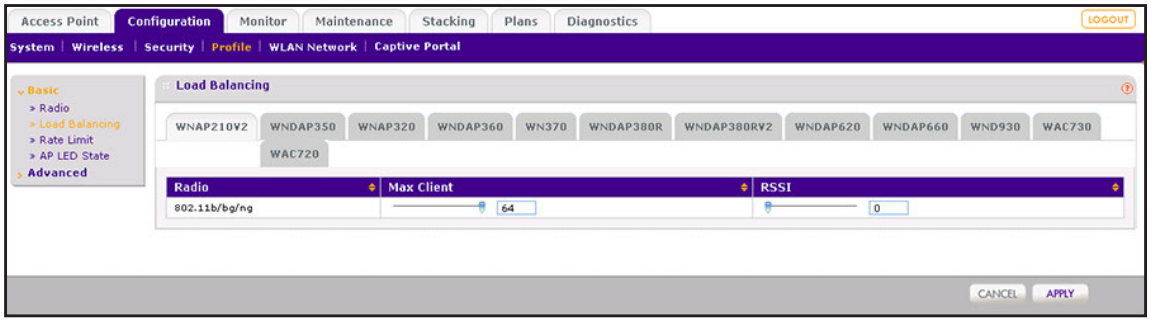
➢ **To configure load balancing for all access points of one model:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Profile > Basic > Load Balancing**.



5. Click the tab for the access point model for which you want to configure load balancing.

6. Configure the settings as described in the following table.

Setting	Description
Max Client	Drag the slider to specify or enter the maximum number of WiFi 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 of clients that a radio of an access point can support.
RSSI	Drag the slider to specify or enter the minimum signal quality in percentage (**0** to **75** percent) expected from the WiFi clients that connect to the access points. A value of **0** means that this check is not enforced and load balancing is disabled. RSSI percentages translate into the following power levels in dBm: • RSSI of 0% = –95 dBm (load balancing is disabled) • RSSI of 25% = –81 dBm • RSSI of 50% = –68 dBm • RSSI of 75% = –55 dBm

7. Click the **Apply** button.

   The changes are saved.

   If you want to configure load balancing for all access points of another model, repeat the procedure for that model.

Manage Rate Limiting

Rate limiting lets you manage how the available bandwidth is distributed among the profiles in a profile group on a radio of a managed access point.

Rate Limiting Concepts

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

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

For example, within one profile group, if four profiles use the 802.11b/bg/ng mode and two profiles use the 802.11a/na/ac 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/ac 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/ac 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. Configuring 0 percent effectively disables rate limiting for that profile. A setting of 0 percent can work well for profiles that are used for management, administration, or testing.

Configure Rate Limiting for the Basic Profile Group

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

➢ **To configure rate limiting for the basic profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

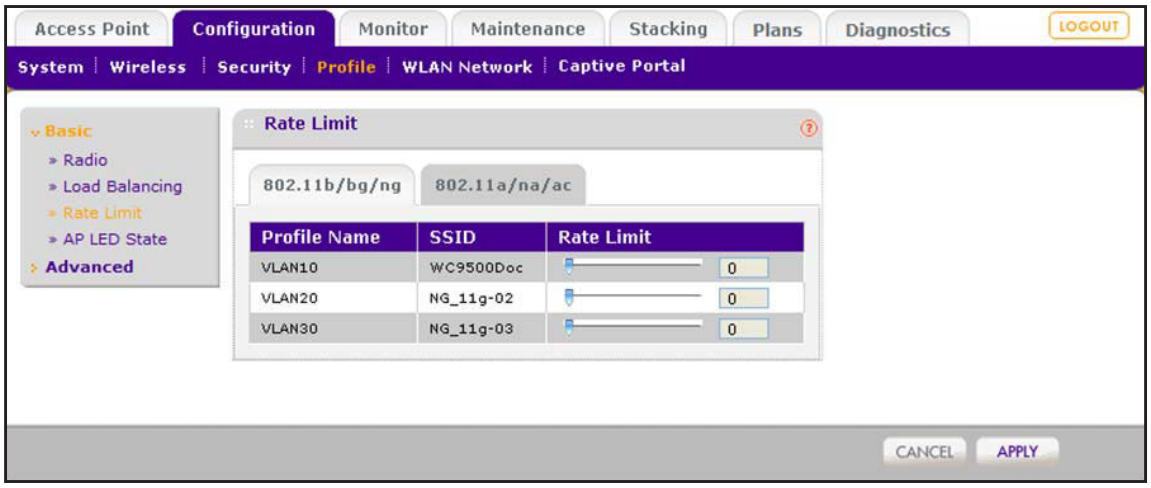
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Basic > Rate Limit**.



   The page provides a tab for each WiFi radio.

5. Click the tab for the radio for which you want to configure rate limiting.
6. For each profile on a WiFi radio, specify the rate limit as a percentage.

   You can drag the sliders to adjust the values in the **Rate Limit** fields to the right of the sliders. Make sure that the total percentages of all profiles on one WiFi radio do not exceed 100 percent.

7. Click the **Apply** button.

   The changes are saved.

Configure Rate Limiting for an Advanced Profile Group

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

➢ **To configure rate limiting for an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

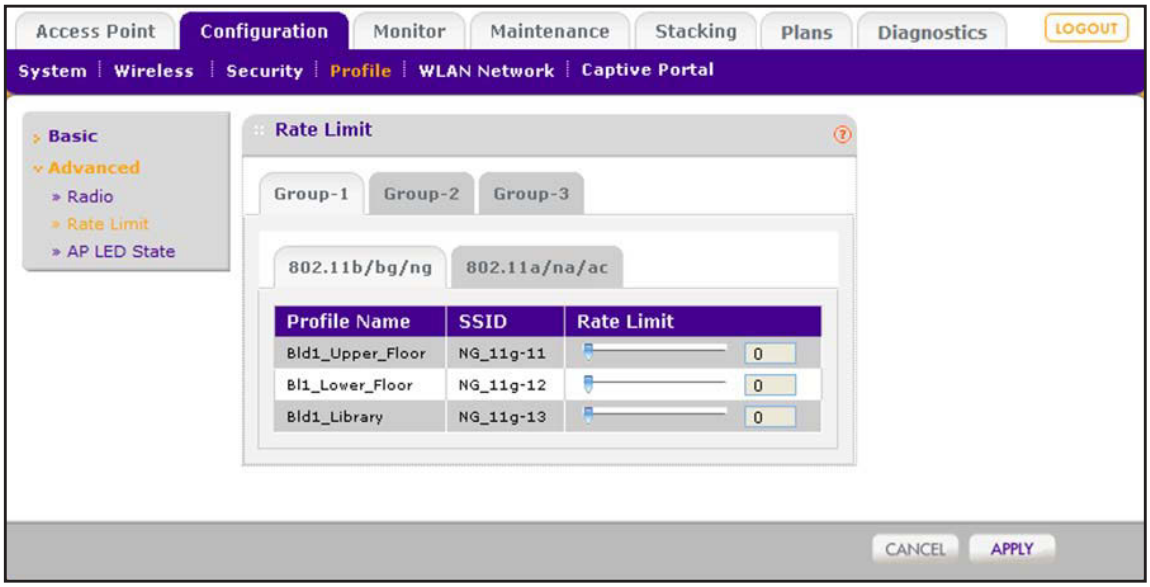
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Advanced > Rate Limit**.



   The page provides a tab for each group. For each group, the page provides a tab for each WiFi radio.

5. Click the tab for the profile group for which you want to configure rate limiting.
6. Click the tab for the radio for which you want to configure rate limiting.

7. For each profile on a WiFi radio in the selected profile group, specify the rate limit as a percentage.

   You can drag the sliders to adjust the values in the **Rate Limit** fields to the right of the sliders. Make sure that the total percentages of all profiles on one WiFi radio in the selected profile group do not exceed 100 percent.

8. Click the **Apply** button.

   The changes are saved.

Manage the LED Behavior

Note: This feature is supported for access point models WN370, WAC720, and WAC730 only.

You can manage the LED behavior of WN370, WAC720, and WAC730 access points by enabling all LEDs (which is the default setting), by enabling the Power LED only, or by disabling all LEDs. You can configure a different setting for each model access point that supports management of the LED behavior.

This feature is useful if an access point is installed in a hotel guest room and you want to make sure that guests are not disturbed by the blue light of the LEDs.

Manage the LED Behavior for the Basic Profile Group

You can manage the LED behavior of WN370, WAC720, and WAC730 access points that support the basic profile group.

➢ **To manage the LED behavior of WN370, WAC720, or WAC730 access points that support the basic profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

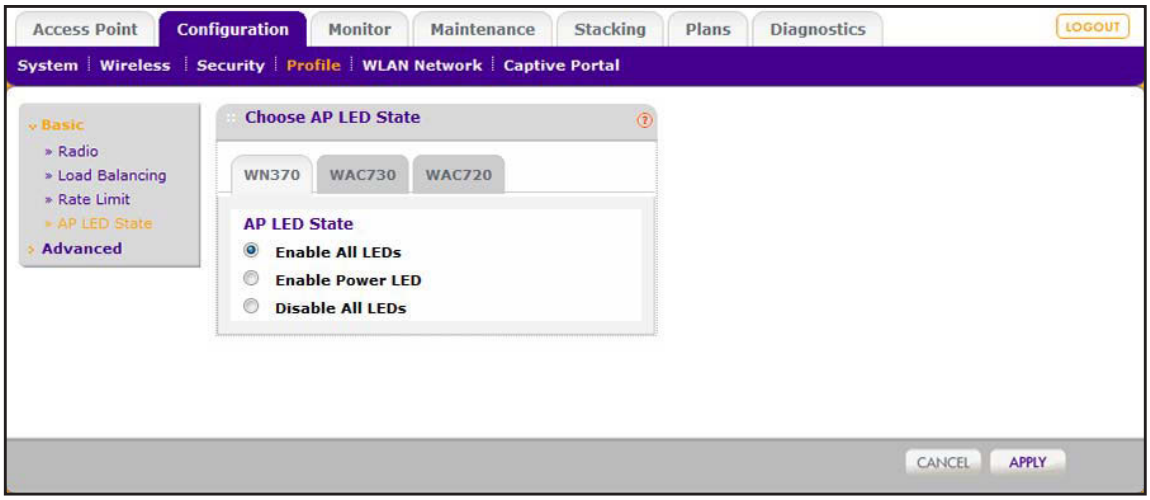
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Profile > Basic > AP LED State**.



5. Select the tab for the model access point that you want to configure.
6. Select a radio button:
   - **Enable all LEDs**. All LEDs function normally. This is the default selection.
   - **Enable Power LED**. Only the Power LED functions and the other LEDs are off.
   - **Disable All LEDs**. All LEDs are off.
7. Click the **Apply** button.

   The changes are saved.

Manage the Behavior for an Advanced Profile Group

For each advanced profile group, you can manage the LED behavior of WN370, WAC720, and WAC730 access points that support the profile group.

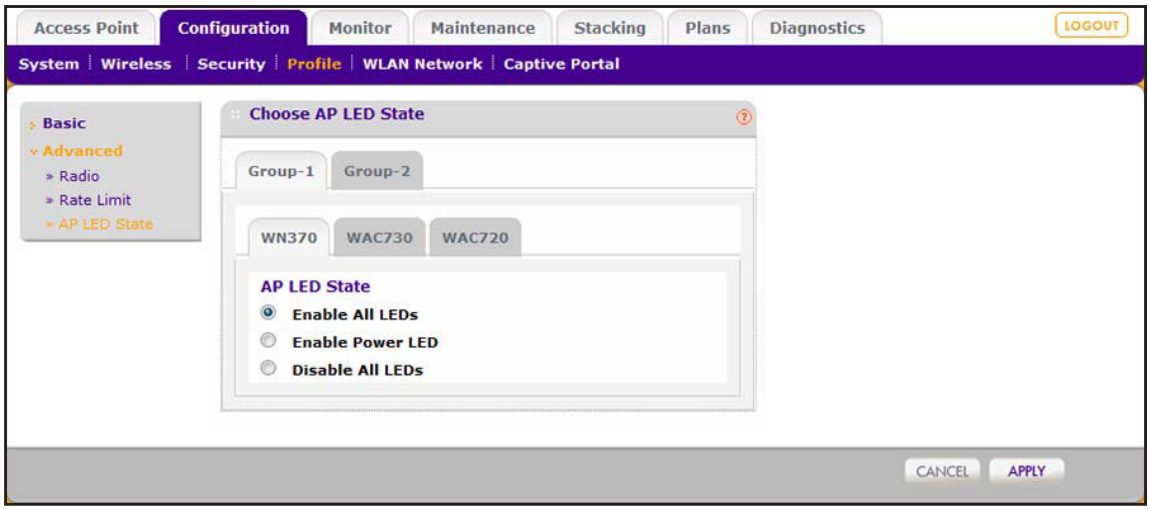
➢ **To manage the LED behavior of WN370, WAC720, or WAC730 access points that support an advanced profile group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Profile > Advanced > AP LED State**.



The page provides a tab for each group.

5. Click the tab for the profile group for which you want to manage the LED behavior.
6. Select the tab for the model access point that you want to configure.
7. Select a radio button:
   - **Enable all LEDs**. All LEDs function normally. This is the default selection.
   - **Enable Power LED**. Only the Power LED functions and the other LEDs are off.
   - **Disable All LEDs**. All LEDs are off.
8. Click the **Apply** button.

   The changes are saved.

Manage Rogue Access Points, Guest Network Access, and Users

10

This chapter includes the following sections:

- *Manage Rogue Access Points*
- *Manage Guest Network Access Through Guest Portals and Captive Portals*
- *Manage Users, Accounts, and Passwords*

Manage Rogue Access Points

The wireless controller can detect rogue access points in your network, you can classify the detected rogue access points, and you can import a list of known access points.

Rogue Access Point Concepts

Rogue access point detection is disabled by default on the wireless controller. If you want to detect rogue access points, you must enable rogue access point detection. Scanning might affect the service availability of the access point temporarily.

An access point is defined as rogue if:

- The access point's radio basic service set identifier (BSSID) is detected by any of the managed access points.
- The access point transmits 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).

The wireless controller can detect and maintain a maximum of 512 access points, both neighboring and rogue access points.

Note: If enabled, basic rogue AP detection and advanced rogue AP detection apply to all profiles, whether in the basic profile group or in any of the advanced profile groups.

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 *Classify Rogue Access Points* on page 215).

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

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

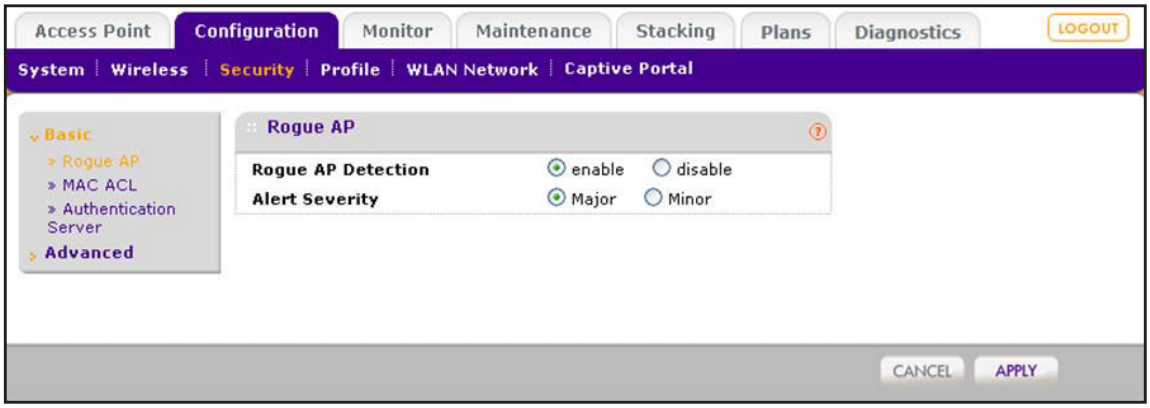
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Basic > Rogue AP**.



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

5. Next to Rogue AP Detection, select the **enable** radio button.
6. Next to Alert Severity, select the severity of the alarm when a rogue access point is detected:
   - **Major**. A major alarm is triggered.
   - **Minor**. A minor alarm is triggered.
7. Click the **Apply** button.

   The changes are saved.

   Because the neighboring and rogue access points are detected during off-channel scans, it typically takes about 30 minutes after the rogue AP detection is enabled for the neighbor and rogue access points to be detected on one channel.

   Once the neighbor and rogue access points are detected, the wireless controller populates the known list (that is, the database with known access points) and unknown list (that is, the database with unknown access points).

Classify Rogue Access Points

You can identify what could be access points from neighboring businesses that are known. As you identify access points, mark them as known or unknown so that the wireless controller does not keep finding them and flagging them. Marking the access points can help you to identify your own equipment that must be managed and the rogue access points that must be detected. A rogue access point acquired both a WiFi and a LAN connection. A neighbor is an access point with only a WiFi connection, not a LAN connection.

➢ **To view and classify rogue access points:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

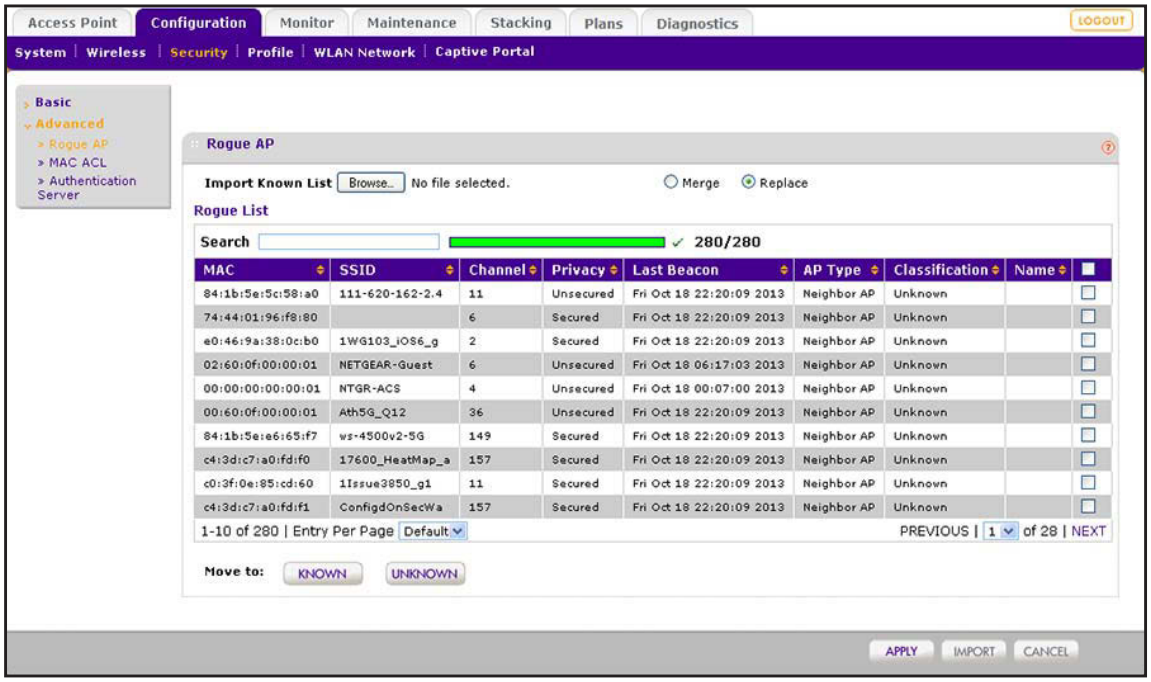
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Security > Advanced > Rogue AP**.



The page displays the Rogue List, which shows all detected rogue access points with essential information, including information about their last beacon. If the Rogue List contains many entries that are spread out over several pages, click the **Next** button or the **Previous** button to scroll through the Rogue List.

Note: As an option, you can import a list of access points from a file. For more information, see *Import a List of Known Access Points From a File* on page 217.

5. Classify the access points in the Rogue List:

   a. Do one of the following:

   - Select one or more check boxes that correspond to the access points.
   - Select all access points 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.
   - **Unknown**. Moves the selected access points to the unknown list.

6. For each known access point, enter a name in the Name column.

   A name allows access points to be more easily identified.

7. Click the **Apply** button.

   The changes are saved.

Import a List of Known Access Points From a File

You can import a list of known access points from a saved file. Create a text file that includes the MAC address of each access point, 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 must 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. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

3. Enter your user name and password.
4. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

5. Select **Configuration > Security > Advanced > Rogue AP**.

   The advanced Rogue AP page displays.

6. Click the **Browse** button, navigate to the file containing the list of known access points, and select it.
7. 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 the access points that are already present in the Rogue List.
   - **Replace**. Replaces the access points that are present in the Rogue List with the access points in the file that you intend to import.

8. Click the **Import** button.

   The wireless controller imports the MAC addresses that are in the text file into the Rogue List table.

9. Click the **Apply** button.

   The changes are saved.

Manage Guest Network Access Through Guest Portals and Captive Portals

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

Note: The URL for the portal is http://<*IP address*>/guest_access/index.php in which <*IP address*> is the IP address of the wireless controller.

Portal Concepts

You can configure multiple guest portals and assign a portal to a security profile in the basic profile group or a security profile in an advanced profile group. The wireless controller pushes a portal configuration to the SSID of a managed access point.

The wireless controller supports two types of portal settings:

- **Guest portal**. Use a guest portal if all WiFi 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 a captive portal if WiFi users must supply their login name and password before being allowing access the network. You must define user names and passwords for these users (see *Manage Users, Accounts, and Passwords* on page 230). Captive portal authentication is typically used for hotspot users and paying guests such as hotel guests who purchase access time for an Internet connection.

  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.

  You can configure the basic portal as a guest portal or a captive portal (see *Configure a Basic Guest Portal or Captive Portal* on page 219) and you can configure up to eight portals (any combination of guest portals and captive portals) as part of the advanced portal group (see *Configure an Advanced Guest Portal or Captive Portal* on page 224).

Note: If the network authentication uses an external RADIUS server, you cannot configure captive portal authentication. 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 must be Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK (see *Network Authentication and Data Encryption Options* on page 136).

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 WiFi 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-Input-Gigawords

Configure a Basic Guest Portal or Captive Portal

You can configure a basic guest portal or captive portal with a local or external authentication server.

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

➢ **To configure a basic guest portal or captive portal:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

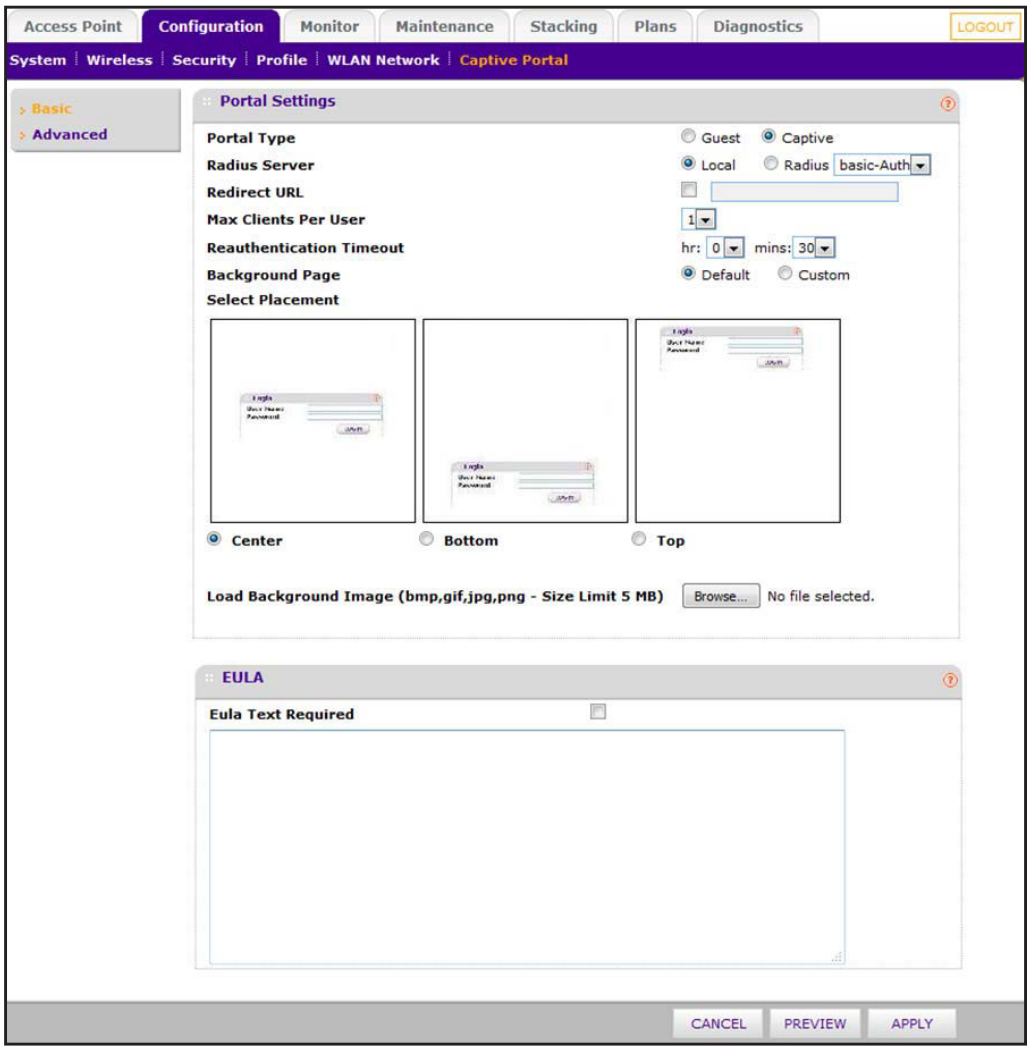
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

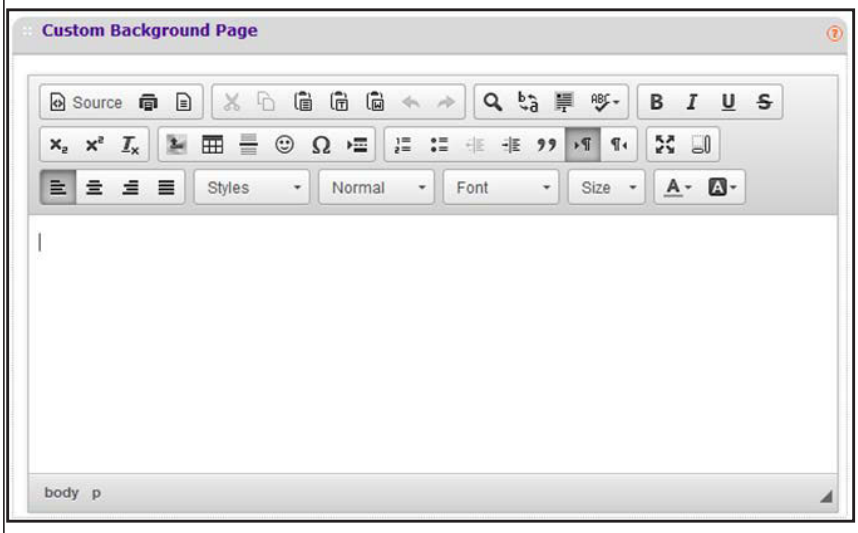
4. Select **Configuration > Captive Portal > Basic**.

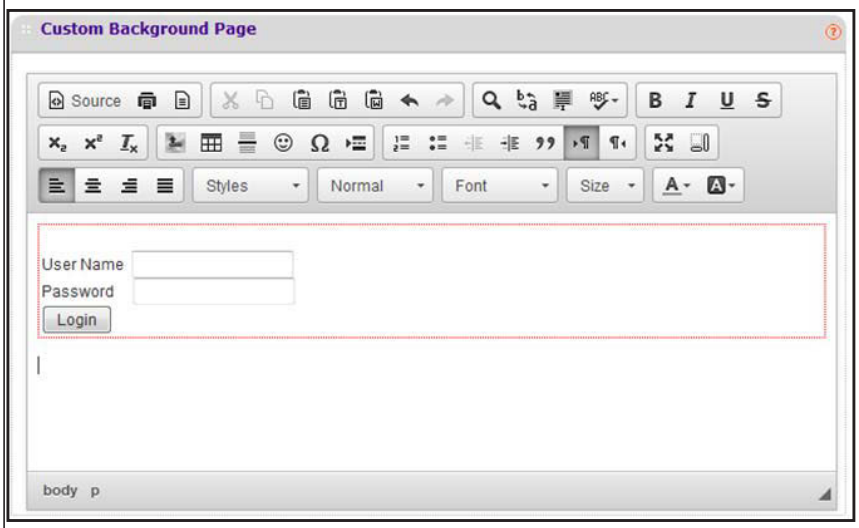


The previous figure shows the settings for a captive portal. The settings for a guest portal are identical, except for the RADIUS server settings, which you cannot configure for a guest portal.

5. Configure the settings as described in the following table.

Setting	Description
Portal Settings section	
Portal Type	Select one of the following radio buttons: • **Guest**. A guest portal with a field for entering an email address. Guests do not need to provide a password and can get unlimited access to the network. You do not need to configure guest accounts. • **Captive**. 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 menu display. For information about how to configure captive portal users and accounts, see *Manage Users, Accounts, and Passwords* on page 230.
Radius Server **Note:** This setting is for a captive portal only.	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Select an external authentication server from the menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 139.
Redirect URL	To redirect traffic to a URL after successful captive authentication, select the check box and enter the URL. By default, traffic is not redirected.
Max Clients Per User	Specify the number of clients that a single captive portal user can open with the same the login information. The default setting is 1. The maximum number of clients that you can select from the menu is 5.
Reauthentication Timeout	Specify the period after which a user who was idle must be reauthenticated. The minimum period is 30 minutes. The maximum period that you can select through the menus is 24 hours.
Select Placement	Click the **Center**, **Bottom**, or **Top** button to specify the location of the login prompt on the login page.

Setting	Description
Background Page	You can either select a background image or configure a custom background page. To navigate to and select an image file for the background of the login page, do the following: 1. Keep the Background Page **Default** radio button selected. 2. Next to Load Backgrounds Image, click the **Browse** button. 3. Navigate to and select an image file. You can use a `.bmp`, `.gif`, `.jpg`, or `.png` image. To configure a custom background page with the default login option, do the following: 1. Select the Background Page **Custom** radio button. The Login Panel radio buttons display. 2. Keep the Login Panel **Default** radio button selected. The default login panel for a guest portal provides an email field and a login button. The default login panel for a captive portal provides a user name and password field and a login button. 3. Scroll down to the Custom Background Page section and click in anywhere the window. The icons display.  4. Use the icons to compose your custom background.

Setting	Description
Login Panel	You can either keep the default login panel or configure a custom login panel. The default login panel for a guest portal provides an email field and a login button. The default login panel for a captive portal provides a user name and password field and a login button. You can customize the login panel to suit your needs. For example, for a captive portal login panel for a hotel, you could change the user name to a room number. To configure a custom background page with a custom login panel, do the following: 1. Select the Background Page **Custom** radio button. The Login Panel radio buttons display. 2. Select the Login Panel **Custom** radio button. 3. Scroll down to the Custom Background Page section. The icons display automatically.  4. Use the icons to compose both your custom background page and login panel.
EULA section	
EULA Text Required	Select the **EULA Text Required** check box if you want to present the end-user license agreement (EULA) on the guest login page or captive portal login page so users can view the EULA before they log in. Enter the EULA text in the text field.

6. To display the portal settings that you configured, click the **Preview** button.

   The URL for the captive portal is http://<IP address>/guest_access/index.php, in which <IP address> is the IP address of the wireless controller.

   The default URL for the captive portal is http://192.168.0.250/guest_access/index.php.

7. Click the **Apply** button.

   The changes are saved.

8. Assign the captive portal or guest portal to a security profile in the basic profile group, in an advanced profile group, or in both:
   - **Basic profile group**. Assign the captive portal or guest portal to a security profile in the basic profile group:
     a. Select **Configuration > Profile > Basic > Radio**.

        The Edit Profile (Basic) page displays.

     b. Click the tab for the radio for which you want to assign the portal.
     c. Click the tab for the profile to which you want to assign the portal.
     d. In the Authentication Settings section of the page, select the **Captive Portal** check box.

        The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.

     e. Click the **Apply** button.

        The changes are saved.
   - **Advanced profile group**. Assign the captive portal or guest portal to a security profile in an advanced profile group:
     a. Select **Configuration > Profile > Advanced > Radio**.

        The Profile Groups page displays.

     b. Click the tab for the profile group for which you want to assign the portal.
     c. Click the **Edit** button.

        The Edit Profile page displays.

     d. Click the tab for the radio for which you want to assign the portal.
     e. Click the tab for the profile to which you want to assign the portal.
     f. In the Authentication Settings section of the page, select the **Captive Portal** check box.

        The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.

     g. Click the **Apply** button.

        The changes are saved.

Configure an Advanced Guest Portal or Captive Portal

As part of the advanced portal group, you can configure up to eight portals (any combination of guest portals and captive portals) with local or external authentication servers.

You can assign any portal, including the basic portal, to *any* profile, whether in the basic profile group or in an advanced profile group.

➢ **To configure an advanced guest portal or captive portal:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

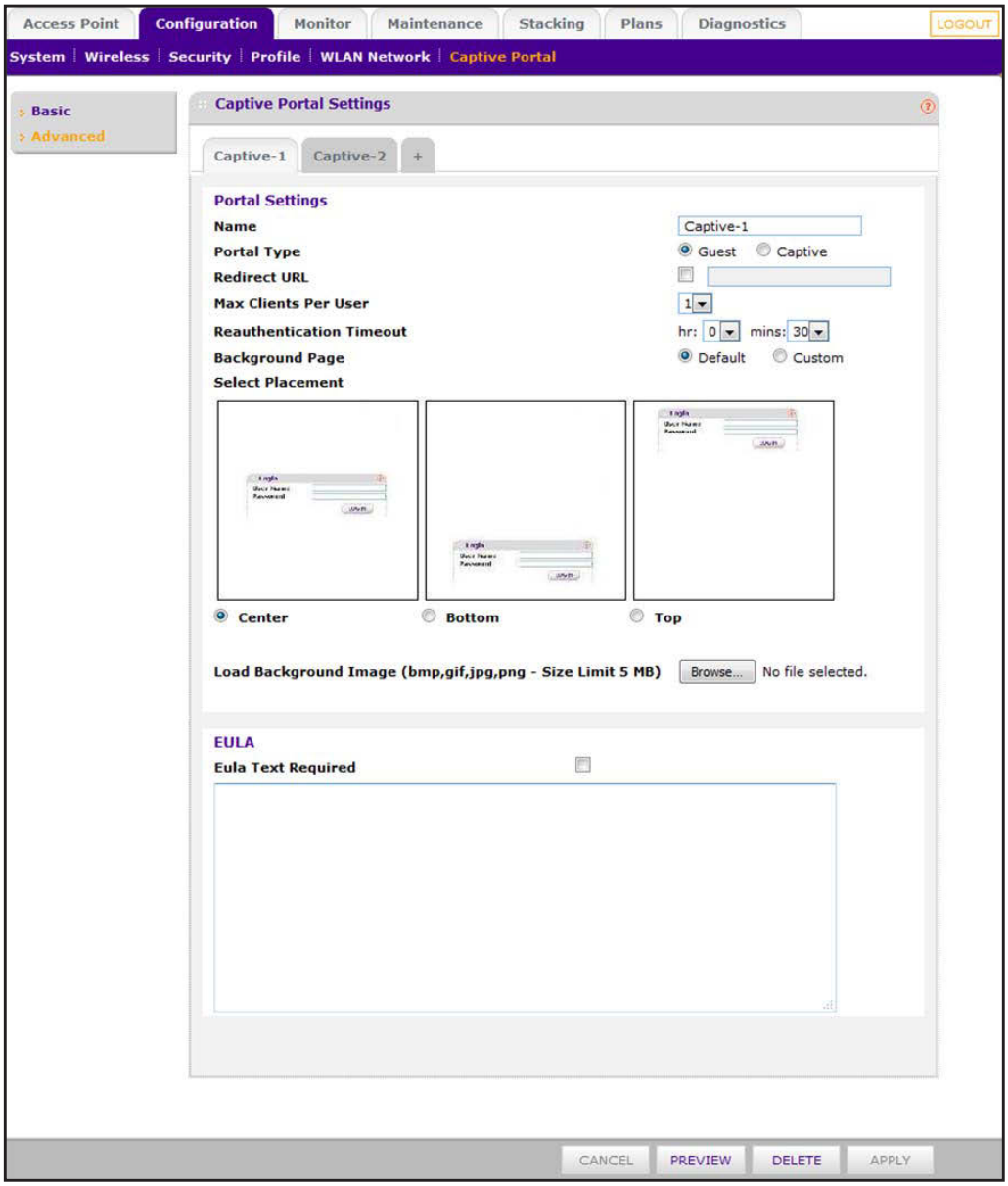
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Configuration > Captive Portal > Advanced**.



The previous figure shows the settings for a captive portal. The settings for a guest portal are identical, except for the RADIUS server settings, which you cannot configure for a guest portal.

5. Click the **+** button to create an additional portal.

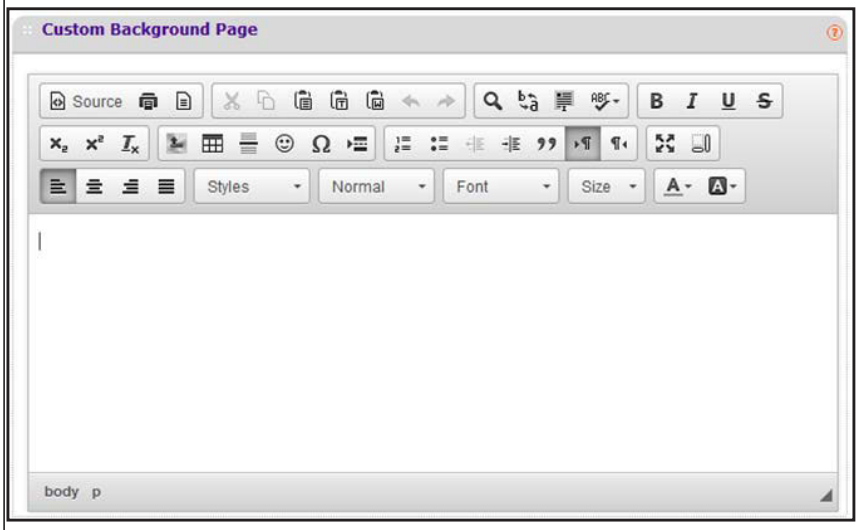
   The new portal displays on the advanced Captive Portal Settings page, and the tab for the new portal is automatically selected to let you configure the new group.

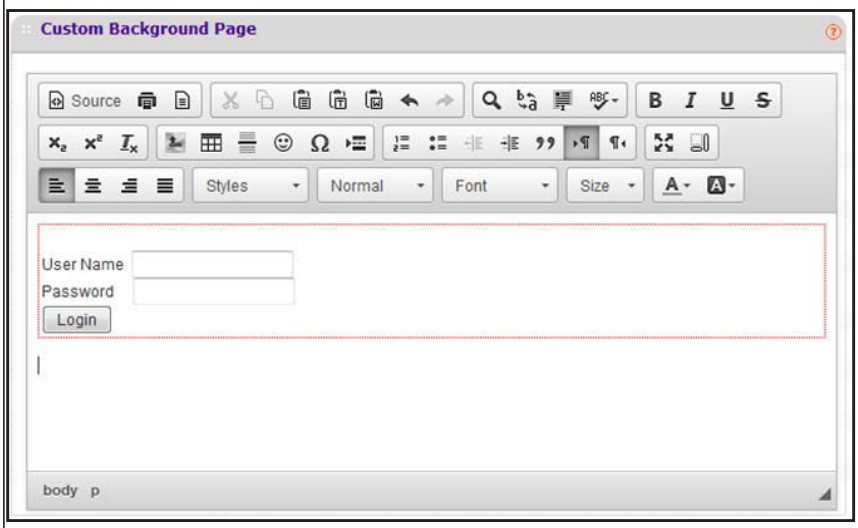
6. In the **Name** field, enter a unique name for the portal.

   By default, portals are named **Captive-1**, **Captive-2**, **Captive-3**, and so on.

7. Configure the settings as described in the following table.

Setting	Description
Portal Settings section	
Portal Type	Select one of the following radio buttons: • **Guest**. A guest portal with a field for entering an email address. Guests do not need to provide a password and can get unlimited access to the network. You do not need to configure guest accounts. • **Captive**. 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 menu display. For information about how to configure captive portal users and accounts, see *Manage Users, Accounts, and Passwords* on page 230.
Radius Server **Note:** This setting is for a captive portal only.	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Select an external authentication server from the menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 139.
Redirect URL	To redirect traffic to a URL after successful captive authentication, select the check box and enter the URL. By default, traffic is not redirected.
Max Clients Per User	Specify the number of clients that a single captive portal user can open with the same the login information. The default setting is 1. The maximum number of clients that you can select from the menu is 5.
Reauthentication Timeout	Specify the period after which a user who was idle must be reauthenticated. The minimum period is 30 minutes. The maximum period that you can select through the menus is 24 hours.
Select Placement	Click the **Center**, **Bottom**, or **Top** button to specify the location of the login prompt on the login page.

Setting	Description
Background Page	You can either select a background image or configure a custom background page. To navigate to and select an image file for the background of the login page, do the following: 1. Keep the Background Page **Default** radio button selected. 2. Next to Load Backgrounds Image, click the **Browse** button. 3. Navigate to and select an image file. You can use a `.bmp`, `.gif`, `.jpg`, or `.png` image. To configure a custom background page with the default login option, do the following: 1. Select the Background Page **Custom** radio button. The Login Panel radio buttons display. 2. Keep the Login Panel **Default** radio button selected. The default login panel for a guest portal provides an email field and a login button. The default login panel for a captive portal provides a user name and password field and a login button. 3. Scroll down to the Custom Background Page section and click in anywhere the window. The icons display.  4. Use the icons to compose your custom background.

Setting	Description
Login Panel	You can either keep the default login panel or configure a custom login panel. The default login panel for a guest portal provides an email field and a login button. The default login panel for a captive portal provides a user name and password field and a login button. You can customize the login panel to suit your needs. For example, for a captive portal login panel for a hotel, you could change the user name to a room number. To configure a custom background page with a custom login panel, do the following: 1. Select the Background Page **Custom** radio button. The Login Panel radio buttons display. 2. Select the Login Panel **Custom** radio button. 3. Scroll down to the Custom Background Page section. The icons display automatically.  4. Use the icons to compose both your custom background page and login panel.
EULA section	
EULA Text Required	Select the **EULA Text Required** check box if you want to present the end-user license agreement (EULA) on the guest login page or captive portal login page so users can view the EULA before they log in. Enter the EULA text in the text field.

8. To display the portal settings that you configured, click the **Preview** button.

   The URL for the captive portal is http://<IP address>/guest_access/index.php, in which <IP address> is the IP address of the wireless controller.

   The default URL for the captive portal is http://192.168.0.250/guest_access/index.php.

9. Click the **Apply** button.

   The changes are saved.

10. Assign the captive portal or guest portal to a security profile in the basic profile group, in an advanced profile group, or in both:
    - **Basic profile group**. Assign the captive portal or guest portal to a security profile in the basic profile group:
        a. Select **Configuration > Profile > Basic > Radio**.

           The Edit Profile (Basic) page displays.
        b. Click the tab for the radio for which you want to assign the portal.
        c. Click the tab for the profile to which you want to assign the portal.
        d. In the Authentication Settings section of the page, select the **Captive Portal** check box.

           The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.
        e. Click the **Apply** button.

           The changes are saved.
    - **Advanced profile group**. Assign the captive portal or guest portal to a security profile in an advanced profile group:
        a. Select **Configuration > Profile > Advanced > Radio**.

           The Profile Groups page displays.
        b. Click the tab for the profile group for which you want to assign the portal.
        c. Click the **Edit** button.

           The Edit Profile page displays.
        d. Click the tab for the radio for which you want to assign the portal.
        e. Click the tab for the profile to which you want to assign the portal.
        f. In the Authentication Settings section of the page, select the **Captive Portal** check box.

           The **Captive Portal** check box displays only when you select **Open System**, **Shared Key**, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK & WPA2-PSK** from the **Network Authentication** menu.
        g. Click the **Apply** button.

           The changes are saved.

Remove a Portal

You can remove a portal.

➢ **To remove a portal:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Captive Portal > Advanced**.

   The Captive Portal Settings page displays.
5. Click the tab for the portal.
6. Click the **Delete** button.

   The portal is removed.

Manage Users, Accounts, and Passwords

The wireless controller supports different types of users and accounts. You can add, change, and remove users and accounts.

User and Account Concepts

The wireless controller supports three types of users: management users, WiFi users (WiFi clients), and captive portal users. *All* of these users must 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 WiFi network.

- **Management users**. These users are allowed access to the wireless controller's web management interface. The wireless controller supports four types of management users:
  - **Administrators**. Administrative users (admins) with read and write capabilities. These users can change the configuration of the wireless controller.
  - **Read-only users**. These users are allowed 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 users**. 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 users**. 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 266).
- **WiFi users**. Users with credentials to access the WiFi network. These users do not need to use the captive portal or the guest portal to access the WiFi network, nor is their access subject to expiration.
- **Captive portal users**. Users with credentials to access the captive portal and who are granted temporary access or access without 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 WiFi access is available and the amount that is charged for it.

Note: For information about password requirements, see *Table 15* on page 362.

Add a Management User

You can add an administrator, a user with read-only access to the wireless controller's web management interface, a user who can provision captive portal users only, and a user who can manage licenses only.

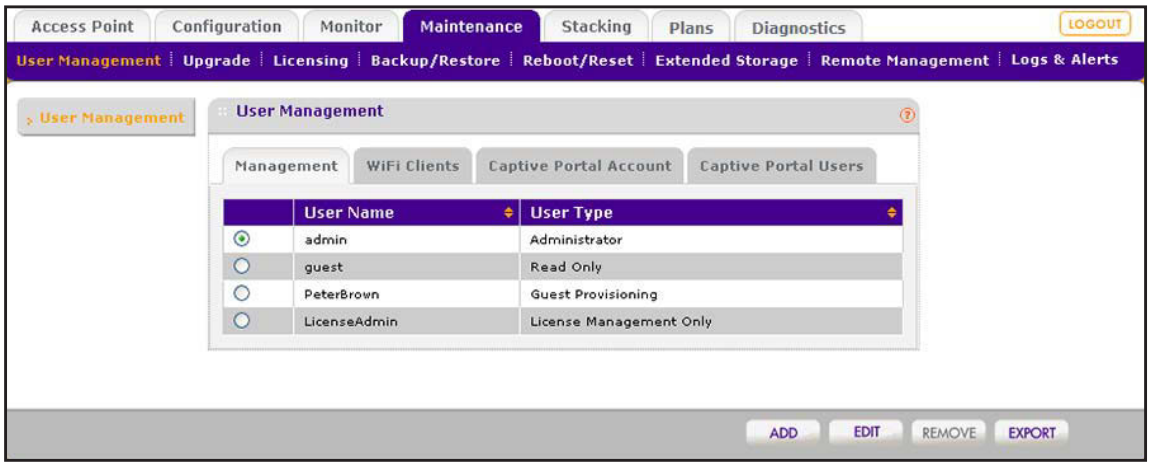
➢ **To add a management user:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Maintenance > User Management**.



The previous figure contains some account examples.

5. Click the **Add** button.

6. Configure the user settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
User Type	From the menu, select the type of user, which determines the users's access to the wireless controller's web management interface. • **Administrator**. Full access with read and write capabilities. • **Read Only**. Read-only access that is restricted to the **Monitor** and **Help** main navigation tabs. • **Guest Provisioning**. Access that is restricted to the **User Management** configuration menu tab under the **Maintenance** main navigation tab. • **License Management Only**. Access that is restricted to the **License** configuration menu tab under the **Maintenance** main navigation tab.
Password	Enter a password in the **Password** field. Confirm the password in the **Confirm Password** field.

7. Click the **Apply** button.

The changes are saved. The user is added to the table on the User Management page.

Add a WiFi User

You can add a user who is allowed to access the WiFi network but who does not need to go through the captive portal or the guest portal. (The web management interface refers to WiFi users as *WiFi clients*.)

➢ **To add a WiFi user:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

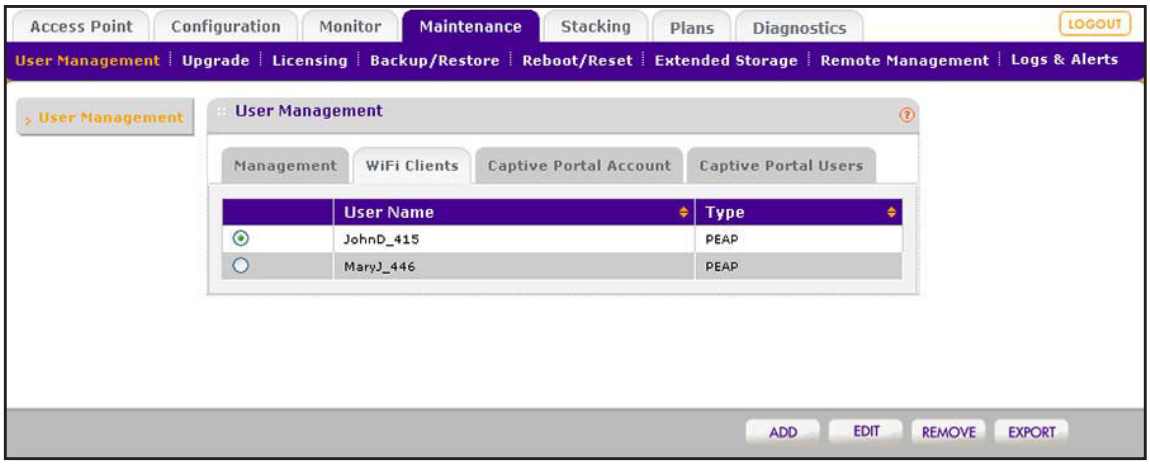
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

   The User Management page displays with the **Management** tab and associated page in view.

5. Click the **WiFi Clients** tab.



   The previous figure contains some account examples.

6. Click the **Add** button.

7. Configure the client settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
Password	Enter a password in the **Password** field. Confirm the password in the **Confirm Password** field.
Authentication Type	From the menu, select one of the following protocols: • **EAP**. Extensible Authentication Protocol. • **PEAP**. Protected EAP.

8. Click the **Apply** button.

   The changes are saved. The client is added to the table on the User Management page.

Add a Captive Portal Account

If you configure a captive portal (see *Configure a Basic Guest Portal or Captive Portal* on page 219), you can add a captive portal account.

Note: If you configure a guest portal, you cannot add a captive portal account.

➢ **To add a captive portal account:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

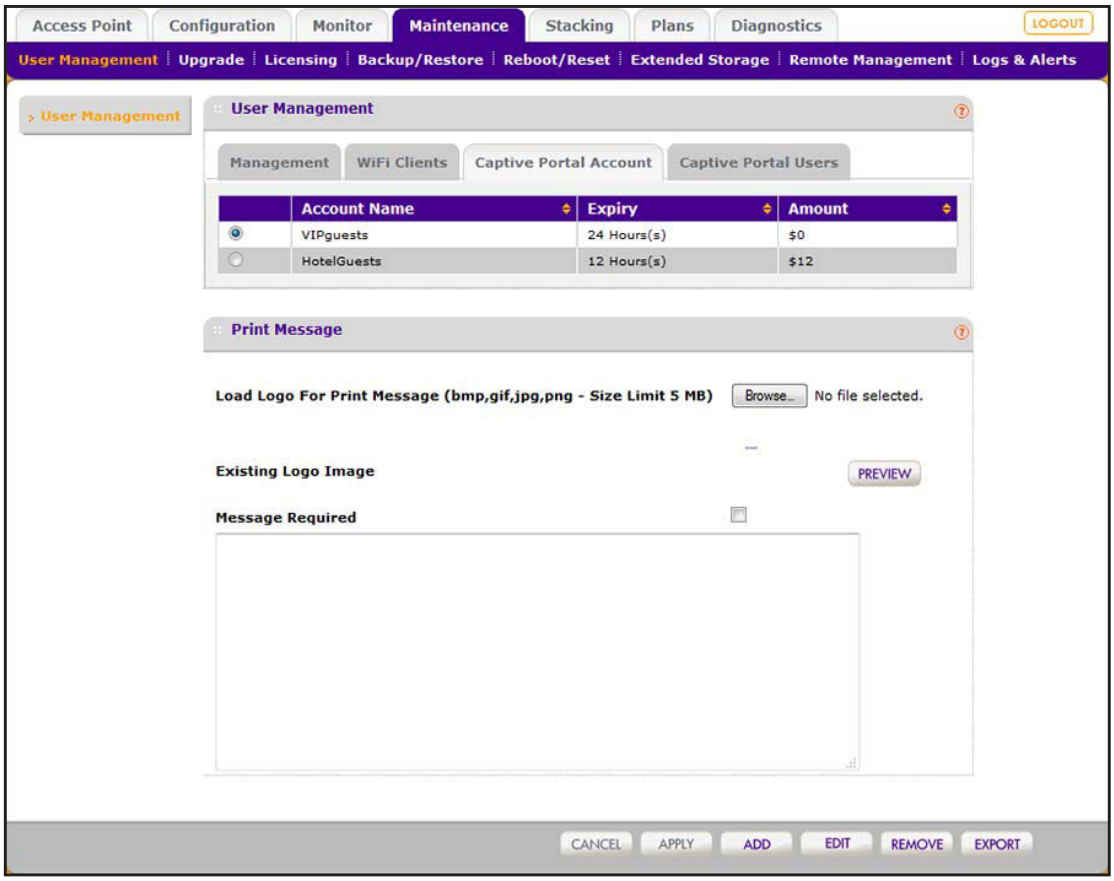
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

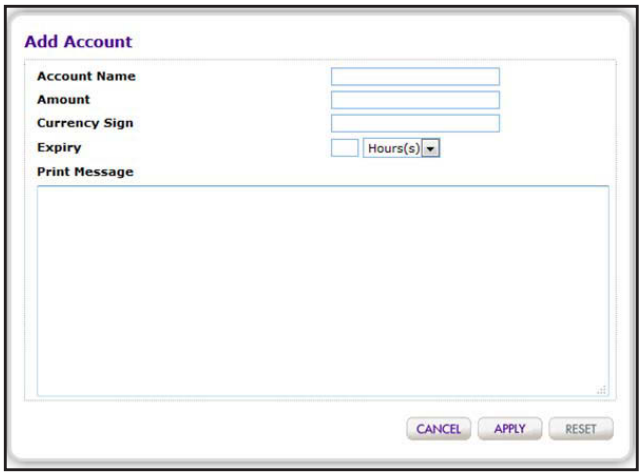
   The User Management page displays with the **Management** tab and associated page in view.

5. Click the **Captive Portal Account** tab.



The previous figure contains some account examples.

6. Click the **Add** button.



7. Configure the account settings as described in the following table.

Setting	Description
Account Name	Enter a unique account name. Only alphanumerical characters and underscore characters (_) are supported.
Amount	Enter the total amount that is charged for the period during which access is available. Enter whole numbers only.
Currency Sign	Enter the currency that is associated with the amount.
Expiry	From the menu, select one of the following periods, and enter a valid number in the field to the left of the menu: • **Hour(s)**. The expiration period is measured in one or more hours. • **Day(s)**. The expiration period is measured in one or more days. • **Week(s)**. The expiration period is measured in one or more weeks. • **Month(s)**. The expiration period is measured in one or more months.
Print Message	To convey a message to the captive portal user, enter a text.

8. Click the **Apply** button.

   The changes are saved. The account is added to the table on the User Management page.

Add a Logo and Message on Captive Portal User Information

If you configure a captive portal (see *Configure a Basic Guest Portal or Captive Portal* on page 219), you can add a logo and message that display if you print captive portal user information.

The logo displays on all printed captive portal user information (see *Add a Captive Portal User* on page 238 and *Add Multiple Captive Portal Users Simultaneously* on page 240). You can specify whether the message displays on all printed captive portal user information.

Note: If you configure a guest portal, you cannot add a logo or message.

➢ **To add a logo and message on printed captive portal user information:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

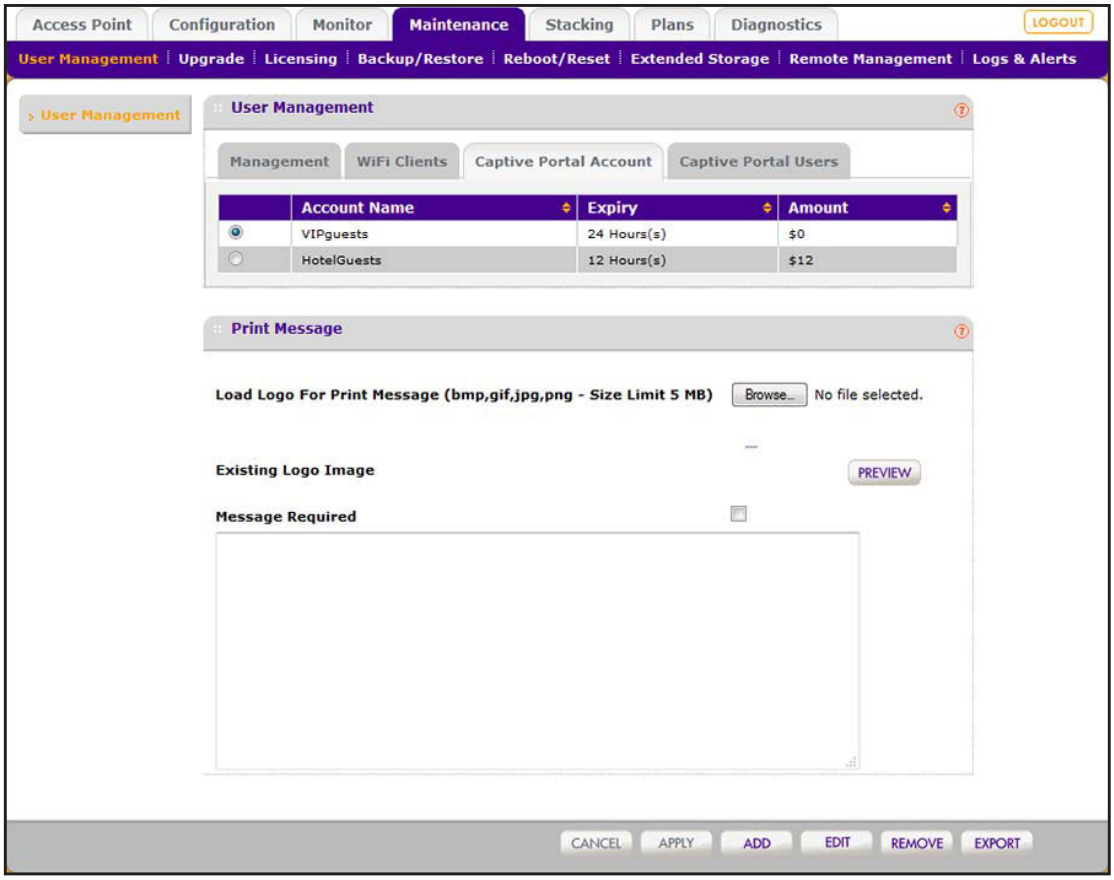
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

   The User Management page displays with the **Management** tab and associated page in view.

5. Click the **Captive Portal Account** tab.



The previous figure contains some account examples.

6. To load a logo that displays on the print message, click the **Browse** button, and follow the directions of your browser to navigate to the logo and select it.

   You can upload a logo in `.bmp`, `.gif`, `.jpg`, or `.png` format. The maximum size for the file is 5 MB.

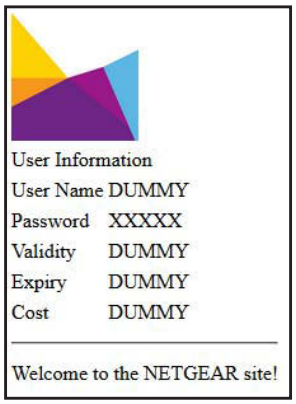
7. To specify a message, in the field below the **Message Required** check box, enter the message.
8. To specify that the message must be printed, select the **Message Required** check box.

   If you do not select the **Message Required** check box, the message is not printed.

9. Click the **Apply** button.

   The changes are saved. The uploaded logo displays to the left of the **PREVIEW** button.

10. To preview the logo and message, click the **PREVIEW** button.



Add a Captive Portal User

If you configure a captive portal (see *Configure a Basic Guest Portal or Captive Portal* on page 219), you can add a captive portal user.

Note: If you configure a guest portal, you cannot add a captive portal user.

➢ **To add a captive portal user:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

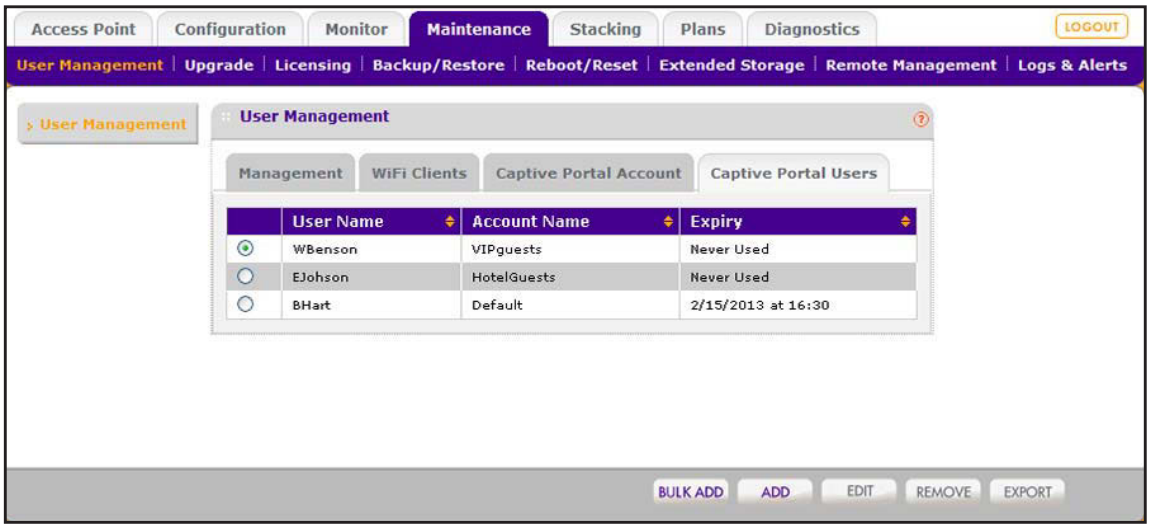
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

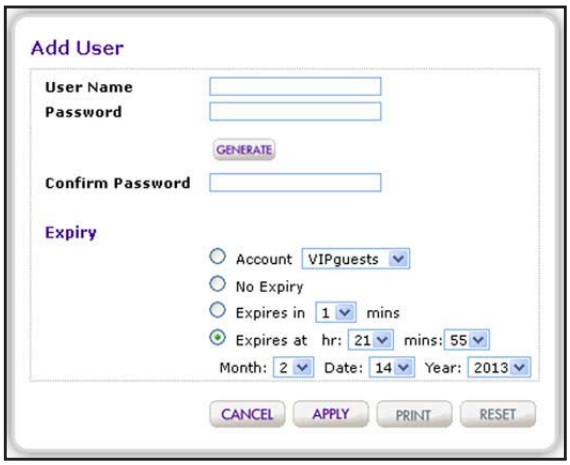
   The User Management page displays with the **Management** tab and associated page in view.

5. Click the **Captive Portal Users** tab.



The previous figure contains some account examples.

6. Click the **Add** button.



7. Configure the user settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
Password	Use one of the following methods to populate the password fields. **Method 1:** 1. Enter a password in the **Password** field. 2. Confirm the password in the **Confirm Password** field. **Method 2:** Click the **Generate** button. A password is generated automatically.

Setting	Description
Expiry	Select one of the following radio buttons: • **Account**. Select a captive portal account from the menu. WiFi access expires according to the expiration period that is specified for the selected account (see *Add a Captive Portal Account* on page 234). • **No Expiry**. WiFi access does not expire. • **Expires in**. WiFi access expires in less than one hour. From the **mins** menu, select in how many minutes (from 1–59) access expires. • **Expires at**. WiFi access expires at a date and time that you specify by making selections from the following menus: **hr**, **mins**, **Month**, **Date**, and **Year**.

8. Click the **Apply** button.

   The changes are saved. The user is added to the table on the User Management page.

9. To print the captive user information, click the **Print** button.
10. Click the **Close** button.

    The pop-up window closes.

Add Multiple Captive Portal Users Simultaneously

If you configure a captive portal (see *Configure a Basic Guest Portal or Captive Portal* on page 219), you can add multiple (up to 256) captive portal users simultaneously.

Note: If you configure a guest portal, you cannot add captive portal users.

➢ **To add a multiple captive portal users simultaneously:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

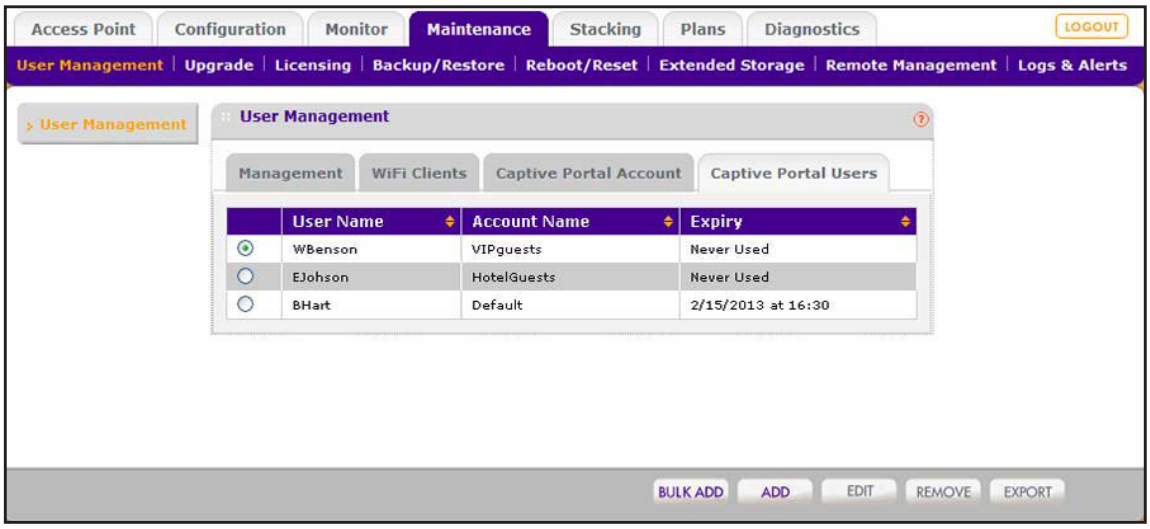
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

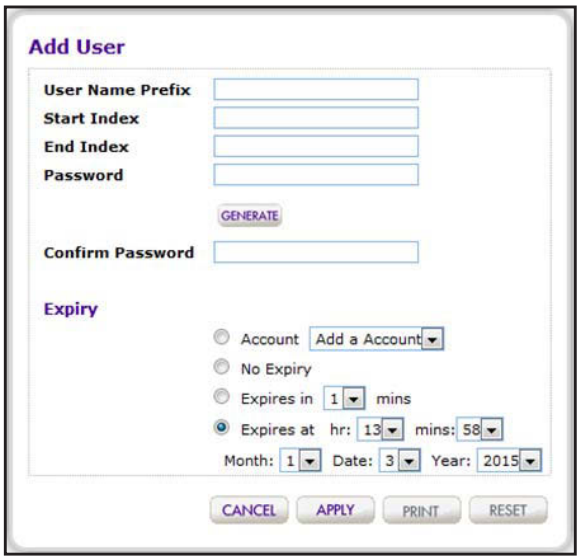
   The User Management page displays with the **Management** tab and associated page in view.

5. Click the **Captive Portal Users** tab.



The previous figure contains some account examples.

6. Click the **Bulk Add** button.



7. Configure the user settings as described in the following table.

Setting	Description
User Name Prefix	Enter a user name prefix. Only alphanumerical characters and underscore characters (_) are supported. **Note:** As an example, if you want to add 17 captive portal users for a group of conference guests that are booked in a hotel under the name Johnson, enter Johnson_. Then, for the start index, enter 1, and for the end index, enter 17. The captive portal accounts are added under the names Johnson_1, Johnson-2, and so on through Johnson_17.
Start Index	Enter the start index number.

Setting	Description
End Index	Enter the end index number, which determines how many captive portal users are added.
Password	Use one of the following methods to populate the password fields. **Method 1:** 1. Enter a password in the **Password** field. 2. Confirm the password in the **Confirm Password** field. **Method 2:** Click the **Generate** button. A password is generated automatically. **Note:** All captive portal users that you are adding through this procedure must use the same password. However, after you add the users, you can change the password for an individual user to a unique password (see *Change the Settings for a User or Account* on page 242).
Expiry	Select one of the following radio buttons: • **Account**. Select a captive portal account from the menu. WiFi access expires according to the expiration period that is specified for the selected account (see *Add a Captive Portal Account* on page 234). • **No Expiry**. WiFi access does not expire. • **Expires in**. WiFi access expires in less than one hour. From the **mins** menu, select in how many minutes (from 1–59) access expires. • **Expires at**. WiFi access expires at a date and time that you specify by making selections from the following menus: **hr**, **mins**, **Month**, **Date**, and **Year**.

8. Click the **Apply** button.

   The changes are saved. The users are added to the table on the User Management page.

9. To print the user information, click the **Print** button.
10. Click the **Close** button.

    The pop-up window closes.

Change the Settings for a User or Account

You can change the settings for a user or an account.

➢ **To change the settings for a user or an account:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

   The User Management page displays with the **Management** tab and associated page in view.

5. Click one of the following tabs:
   - **Management**
   - **WiFi Clients**
   - **Captive Portal Account**
   - **Captive Portal Users**
6. Select the radio button that corresponds to the user or account that you want to change.
7. Click the **Edit** button.

   A pop-up window opens.

8. Change the user or account settings.
9. Click the **Apply** button.

   The settings are saved in the table on the User Management page.

Remove Users or Accounts

You can change or remove one or more users or accounts. However, you cannot remove a captive portal account with which one or more captive portal users are associated. Before you can remove the account, you first must assign the users to another account.

➢ **To remove one or more users or accounts:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > User Management**.

   The User Management page displays with the **Management** tab and associated page in view.

5. Click one of the following tabs:
   - **Management**
   - **WiFi Clients**
   - **Captive Portal Account**
   - **Captive Portal Users**
6. Take one of the following actions:
   - For management users, WiFi clients, or captive portal accounts, select the radio button that correspond to the user or account that you want to remove.
   - For captive portal users, select one or more check boxes that correspond to the users that you want to remove.
7. Click the **Remove** button.

   The users or accounts are removed from the table.

Export a List of Users or Accounts

You can export a list of users or account as a comma-separated values (CSV) file.

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

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Maintenance > User Management**.

   The User Management page displays with the **Management** tab and associated page in view.
5. Click one of the following tabs:
   - **Management**
   - **WiFi Clients**
   - **Captive Portal Account**
   - **Captive Portal Users**
6. Click the **EXPORT** button.

   The selected list is opened or saved as a zipped CSV file to a location that you specify.
7. To complete the procedure, follow the directions of your browser.

11 Maintain the Wireless Controller and Access Points

This chapter includes the following sections:

- *Manage the Configuration File or Upgrade the Firmware*
- *Reboot the Wireless Controller*
- *Reset the Wireless Controller*
- *Manage External Storage*
- *Manage Remote Access*
- *Specify Session Time-Outs*
- *Save the Logs*
- *View Alerts and Events*
- *Manage Licenses*
- *Reboot Access Points*
- *Configure Multicast Firmware Upgrade for Access Points*

Manage the Configuration File or Upgrade the Firmware

This section includes the following subsections:

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

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, cleared to factory default settings, and replaced by a newer version (upgraded).

Back Up the Configuration File

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.

➢ **To back up the configuration file and save a copy of the current settings:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

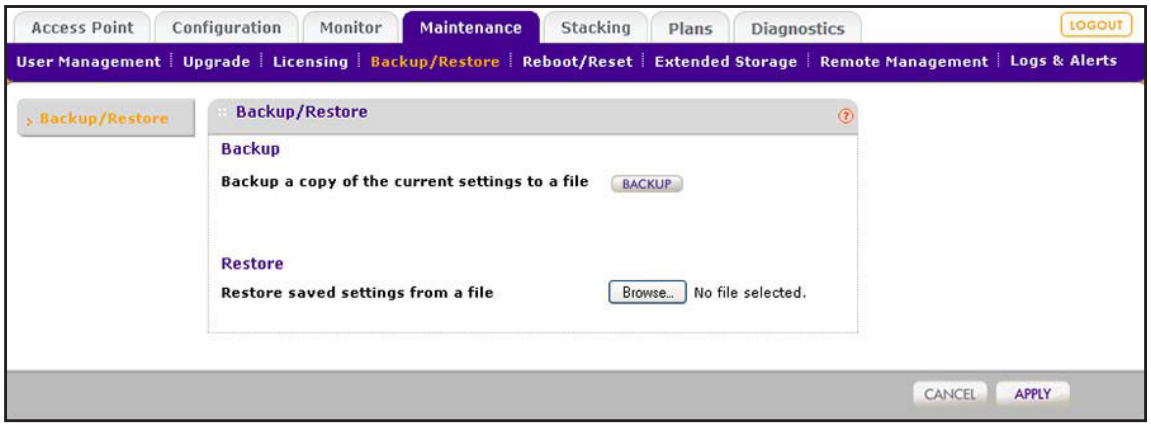
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Backup/Restore**.



5. Click the **Backup** button.

A dialog box displays, showing the file name of the backup file. The backup file is in the following format: `backup.tgz`.

6. To save the configuration file, follow the instructions of your browser.

Restore the Configuration File

Restore only settings that were backed up from a WC7500, WC7600, WC7600v2, WC9500 wireless controller. (You cannot restore settings on a WC7500, WC7600, WC7600v2, WC9500 wireless controller that were backed up from a WC7520 or WC7600 wireless controller.)

➢ **To restore the configuration file from a backed-up file:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Backup/Restore**.

   The Backup/Restore page displays.

5. Click the **Browse** button.
6. Navigate to the saved configuration file.

WARNING:

When you click the Apply button to 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 Status LED turns green, wait a few more seconds before you do anything.

7. Click the **Apply** button.

   The configuration file is loaded onto the wireless controller, and the wireless controller reboots.

Upgrade the Firmware

The wireless controller provides two methods for upgrading its firmware:

- Scheduled, automatic update
- Manual update

To enable you to switch the wireless controller from one firmware version to another, the wireless controller provides two boot partitions. You can configure the wireless controller to download firmware from a TFTP or FTP server and upgrade the firmware on the wireless controller when it is least disruptive. You can also download firmware manually to a computer and upload it to the wireless controller from a local file.

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. To find out if you must reconfigure the wireless controller, see the release notes for the firmware version.

IMPORTANT:

If your wireless controller runs a 3.x or 4.x firmware version and you want to upgrade to a 5.x version, you must upgrade the firmware by using a TFTP or FTP server. You cannot upgrade the firmware from a local file.

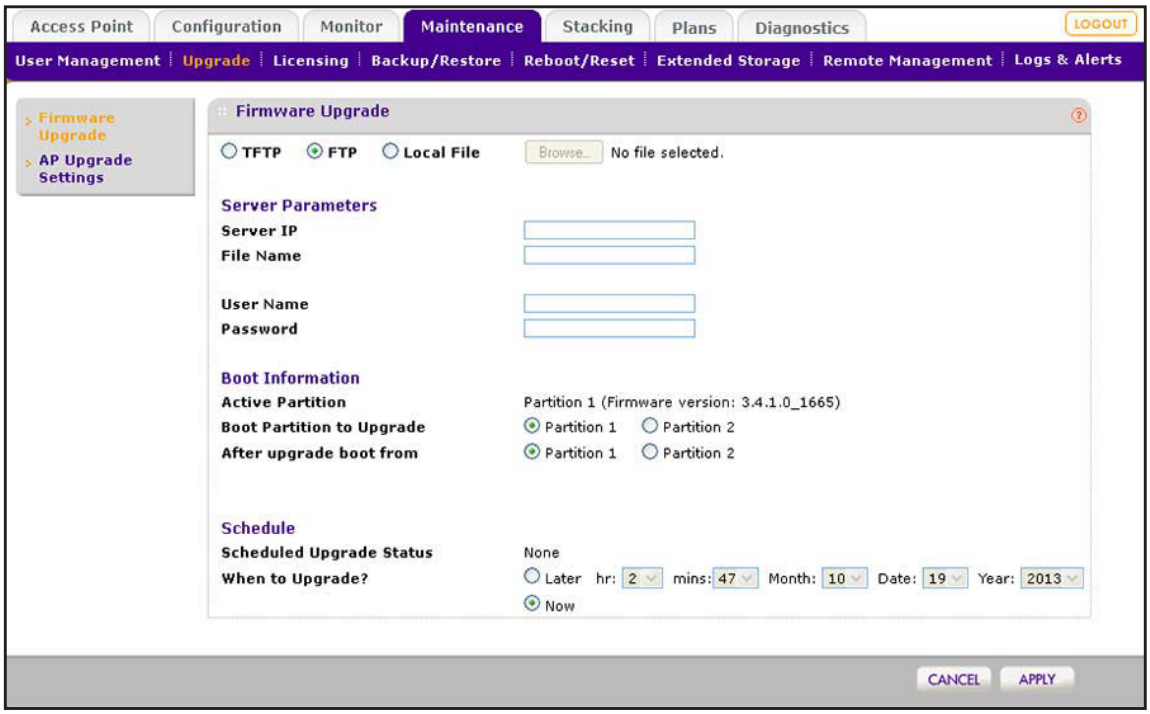
➢ **To upgrade the firmware:**

1. Download the firmware from NETGEAR:
   a. Visit the NETGEAR support page for the WC7500, WC7600, WC7600v2, WC9500 wireless controller at *http://support.netgear.com/product/WC9500*.
   b. Download the firmware and save it on your computer or on a network server.
2. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
3. Enter your user name and password.
4. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
5. Select **Maintenance > Upgrade > Firmware Upgrade**.



The previous figure shows the fields that display when you select the **FTP** radio button. When you select the **TFTP** or **Local File** radio button, fewer fields are shown.

6. Configure the settings as described in the following table.

Setting	Description
TFTP, FTP, or Local File	Select one of the following radio buttons to specify from which location the upgrade must occur. The page adjusts to display the fields that are required for each upgrade location. • **TFTP**. Upgrade from a TFTP server. The **Server IP** and **File Name** server parameters fields display. • **FTP**. Upgrade from an FTP server. The **Server IP, File Name**, **User Name**, and **Password** server parameters fields display. • **Local File**. Upgrade from a local file that you downloaded. The server parameter fields do not display, but the **Browse** button becomes available. To select the firmware upgrade file from your computer, follow the directions of your browser. **Note:** If your WiFi controller runs a 3.x or 4.x firmware version and you want to upgrade to a 5.x version, you must upgrade the firmware by using a TFTP or FTP server. You cannot upgrade the firmware from a local file.
Server Parameters section (TFTP and FTP only)	
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.

Setting	Description
Password (FTP only)	Enter the password to access the FTP server.
Boot Information section	
Active Partition	This field 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 must be saved.
After upgrade boot from	Select the radio button for the partition from which the wireless controller must reboot after the firmware is upgraded.
Schedule section	
Schedule Update Status	This field is an informational field that displays when the firmware upgrade occurs. If no update is scheduled, the field displays **None**.
When to Upgrade?	Select when the firmware upgrade must occur: • **Later**. Make selections from the menus to specify the date and time when the upgrade must occur. • **Now**. The upgrade occurs immediately after you click the **Apply** button.

WARNING:

When you click the Apply button and the Now radio button is selected to upgrade the firmware immediately, 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 Status LED turns green, wait a few more seconds before you do anything.

7. Click the **Apply** button.

   Unless you scheduled the firmware upgrade for a particular time, the firmware is upgraded immediately, and the wireless controller reboots.

8. To verify that the wireless controller is running the latest firmware, do the following:

   a. Select **Monitor > Network > Controller**.

      The Controllers page displays.

   b. Verify the firmware version in the Version column.

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

Reboot the Wireless Controller

The Reboot/Reset Controllers page lets you reset the wireless controller.

➢ **To reboot the wireless controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

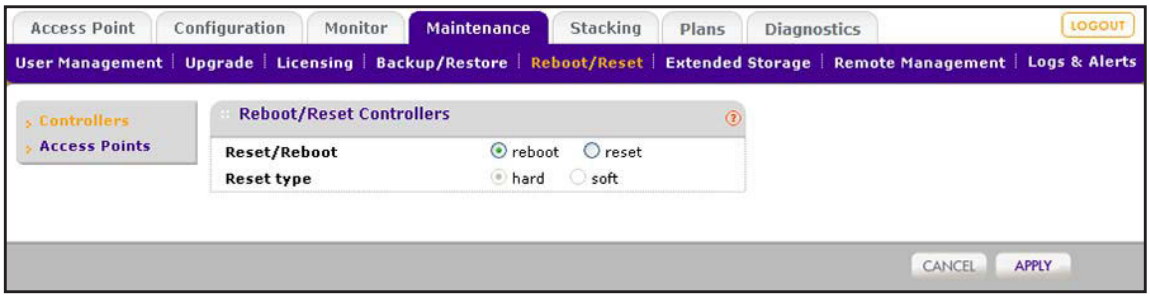
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Reboot/Reset > Controllers**.



5. Select the **reboot** radio button.
6. Click the **Apply** button.

   The wireless controller reboots. The reboot process is complete after several minutes when the Status LED on the front panel turns green.

Reset the Wireless Controller

You can perform a hard or soft reset of the wireless controller:

- **Hard reset**. The settings of the wireless controller are restored to factory default settings. This reset is the same as the reset that occurs when you press the **Reset** button on the front panel.
- **Soft reset**. Saves the IP and VLAN addresses and managed access point list but clears all other settings such as profiles, profile groups, and authentication servers.

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

➢ **To reset the wireless controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Reboot/Reset > Controllers**.

   The Reboot/Reset Controllers page displays.

5. Select the **reset** radio button.
6. Select one of the following radio buttons to specify a hard reset or soft reset:
   - **hard**. Restores the factory default settings to the wireless controller. The factory default settings are listed in *Appendix A, Factory Default Settings, Technical Specifications, and Passwords Requirements*.
   - **soft**. Clears all settings except for the IP and VLAN addresses and managed access point list.

WARNING:

If you select the hard radio button and you click the Apply button, 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 Status LED turns green, wait a few more seconds before you do anything.

7. Click the **Apply** button.

   The configuration file is restored according to the selection that you made, and the wireless controller reboots.

Manage External Storage

The Extended Storage page 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.

Note: Do not reboot the wireless controller while an external storage device is connected. Doing so causes the wireless controller to halt in the boot process. First, disconnect the external storage device. Then, reboot the wireless controller.

➢ **To mount an external storage device and view information about the device or unmount an external storage device:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

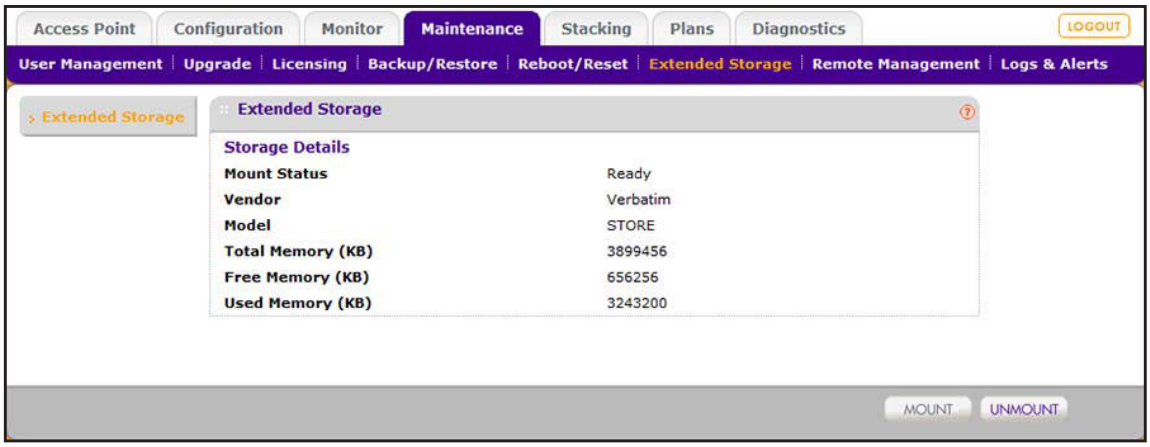
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Extended Storage**.



   The previous figure shows information about an attached USB memory stick.

5. Mount or unmount the external storage device:
   - To mount the external storage device, do the following:
     a. Attach the external storage device to the USB port on the front panel of the wireless controller.
     b. Click the **Mount** button.

        The storage details become visible on the Extended Storage page.
   - To unmount the external storage device, do the following:
     a. Click the **Unmount** button.
     b. Remove the external storage device from the USB port.

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.

You can configure the wireless controller through SNMP, except for the following features:

- Guest access management
- RF management
- Stacking management

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

➢ **To enable and configure SNMP:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

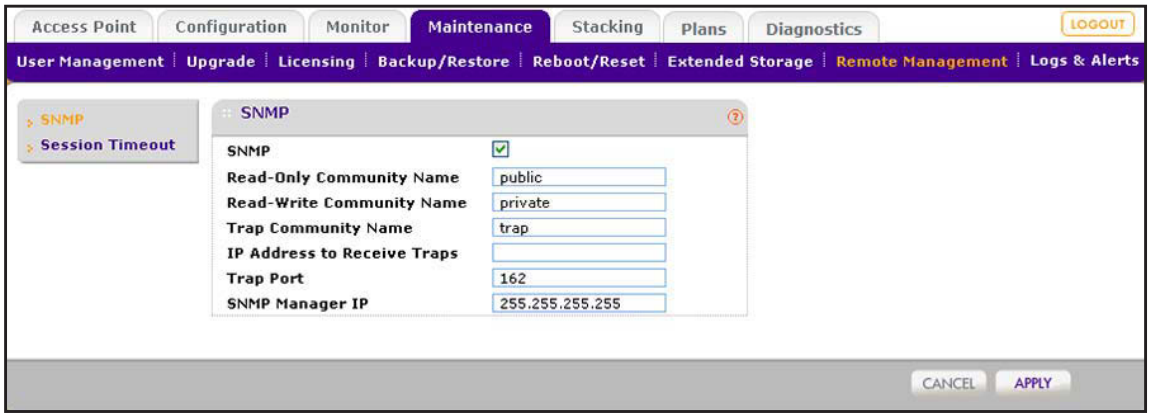
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Remote Management > SNMP**.



5. Enable SNMP and configure the settings as described in the following table.

Setting	Description
SNMP	Select the **SNMP** 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. To allow any SNMP manager to access the wireless controller, keep this field blank.

6. Click the **Apply** button.

   The changes are saved.

Specify Session Time-Outs

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

➢ **To specify the length of the HTTP session time-out for the wireless controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

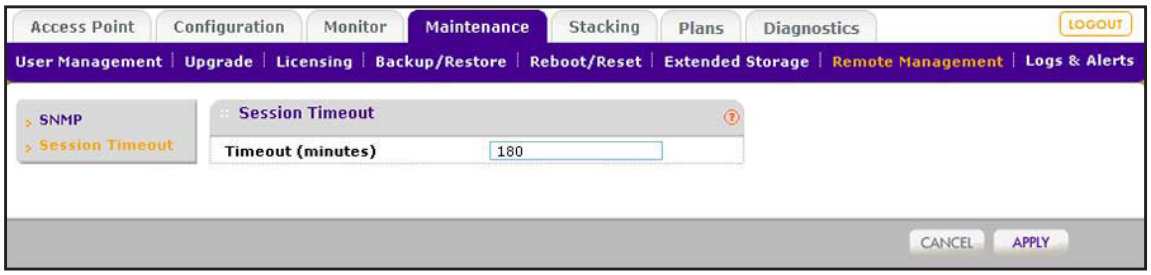
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Remote Management > Session Timeout**.



5. In the **Timeout (minutes)** field, specify number of minutes before an active HTTP login session expires.

   The default session time-out is **5** minutes.

6. Click the **Apply** button.

   The changes are saved.

Save the Logs

You can save the system logs that are collected on the wireless controller. You can also save the logs for an individual access point.

If a problem or failure occurs, the system logs along with backed-up configuration settings could help determine the cause.

Save the System Logs

You can save the system logs to a zipped log file on your computer.

The information that is stored in the system logs depends on the log settings. For information about how to configure which information is recorded and stored in the logs, see *Configure the Event Tracing Log Settings* on page 113.

➢ **To save the system logs:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

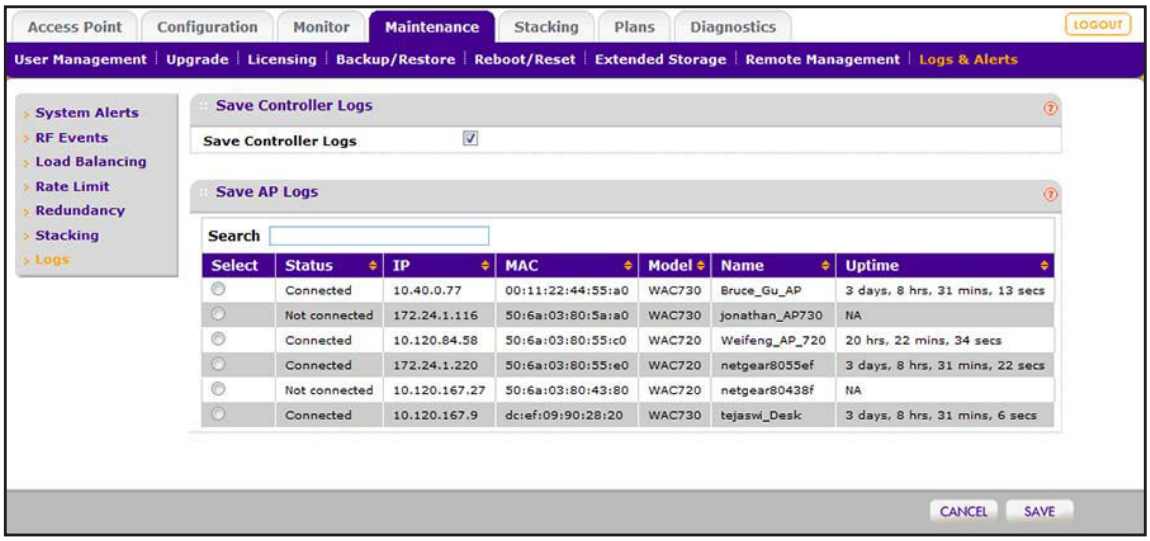
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > Logs**.



5. Select the **Save Controller Logs** check box.
6. Click the **Save** button.
7. Follow the directions of your browser.

   The default name of the zipped log file is *IP address*-WC7600-Logs.tgz, in which *IP address* is the IP address of the wireless controller.

Save and Clear the Logs for an Access Point

You can save the logs for a managed access point to a zipped log file on your computer. After you save the logs, they are automatically deleted from the access point.

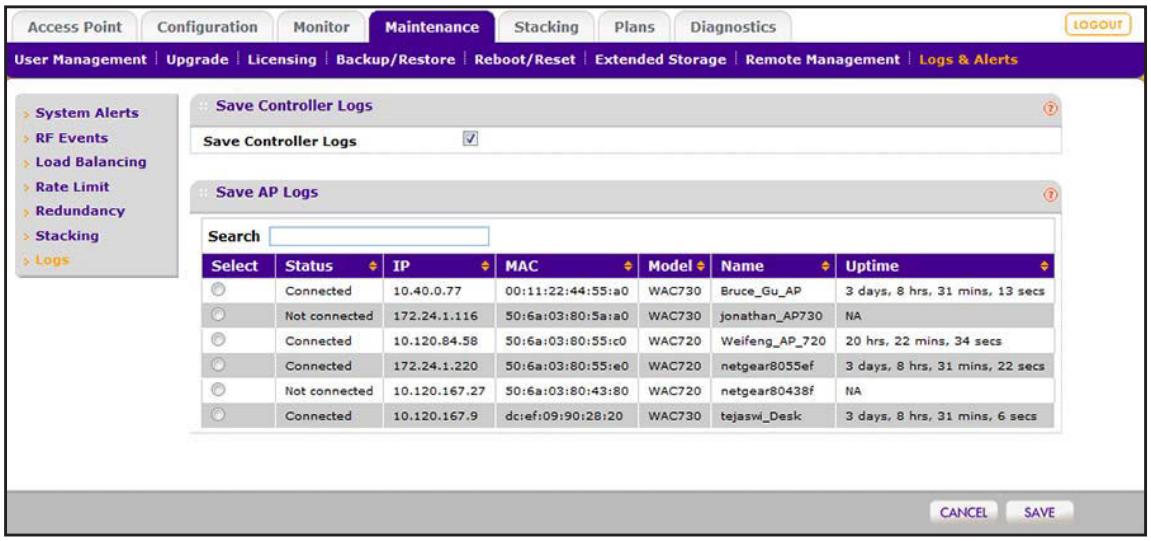
➢ **To save and clear the logs for a managed access point:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Maintenance > Logs & Alerts > Logs**.



5. To search the table with access points, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
6. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
7. Select the radio button that corresponds to the access point for which you want to save the logs.

CAUTION:

After you save the logs, they are automatically deleted from the access point.

8. Click the **Save** button.
9. Follow the directions of your browser.

   The default name of the zipped log file is ap_logs_*XX_XX_XX_XX_XX_XX*.tgz, in which *XX_XX_XX_XX_XX_XX* is the MAC address of the access point.

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, and a firmware upgrade.
- **RF events**. Radio frequency events such as a change of channel or a managed access point going down.
- **Load balancing events**. Load-balancing events such as a bad RSSI for a client, or the violation of a load-balancing threshold.
- **Rate limiting events**. 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 events**. Stacking events such as a slave wireless controller coming up or going down, or two wireless controllers synchronizing.

Alerts and events indicate the alarm severity level (minor, normal, major, or critical), provide a description, and show the date and time that the alerts or events was recorded.

View System Alerts

The wireless controller generates alerts for system events such as an access point coming up or being shut down, the wireless controller coming up or being shut down, and a firmware upgrade.

➢ **To view system alerts:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

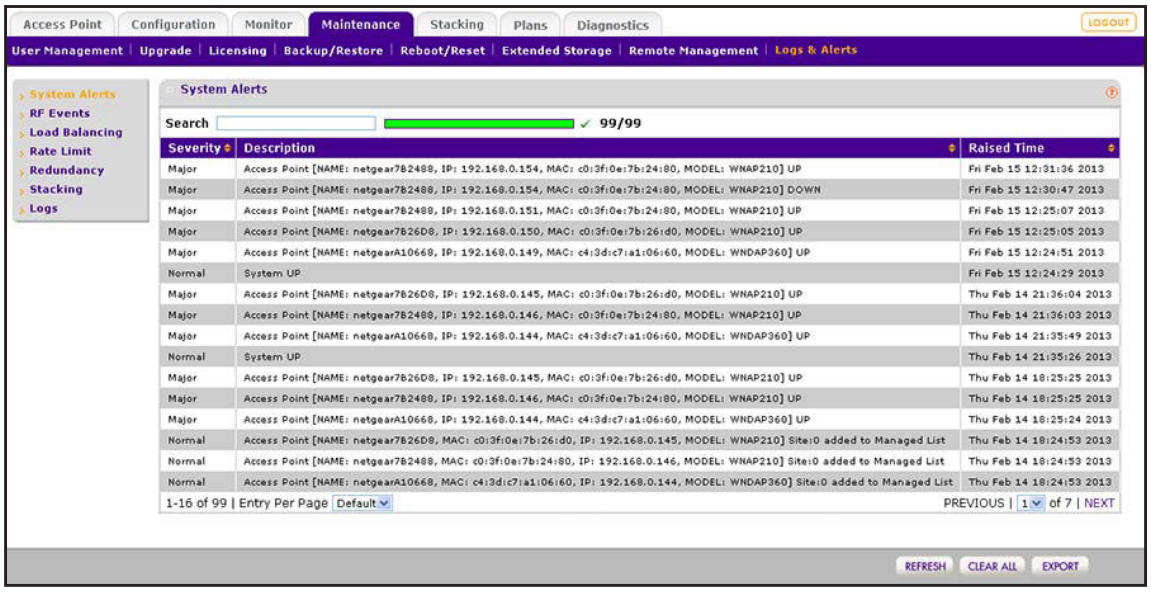
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > System Alerts**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest alerts onscreen, click the **REFRESH** button.
7. To save the alerts to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all alerts from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the alerts before you clear them.

View Radio Frequency Events

The wireless controller generates alerts for radio frequency (RF) events such as a change of channel or a managed access point going down.

➢ **To view RF events:**

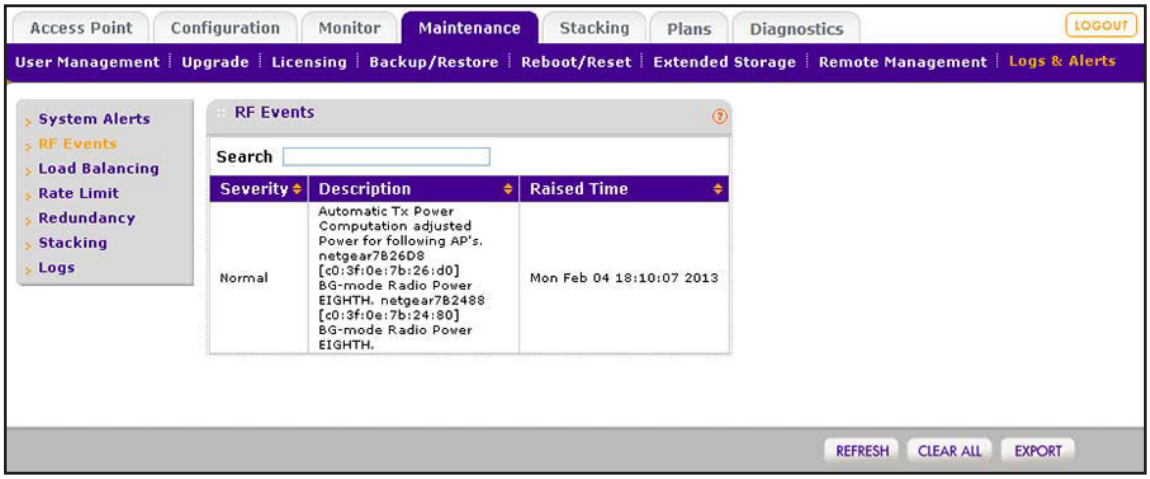
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > RF Events**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest events onscreen, click the **REFRESH** button.
7. To save the events to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all events from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the events before you clear them.

View Load-Balancing Events

The wireless controller generates alerts for load-balancing events such as a bad RSSI for a client, or the violation of a load-balancing threshold.

➢ **To view load-balancing events:**

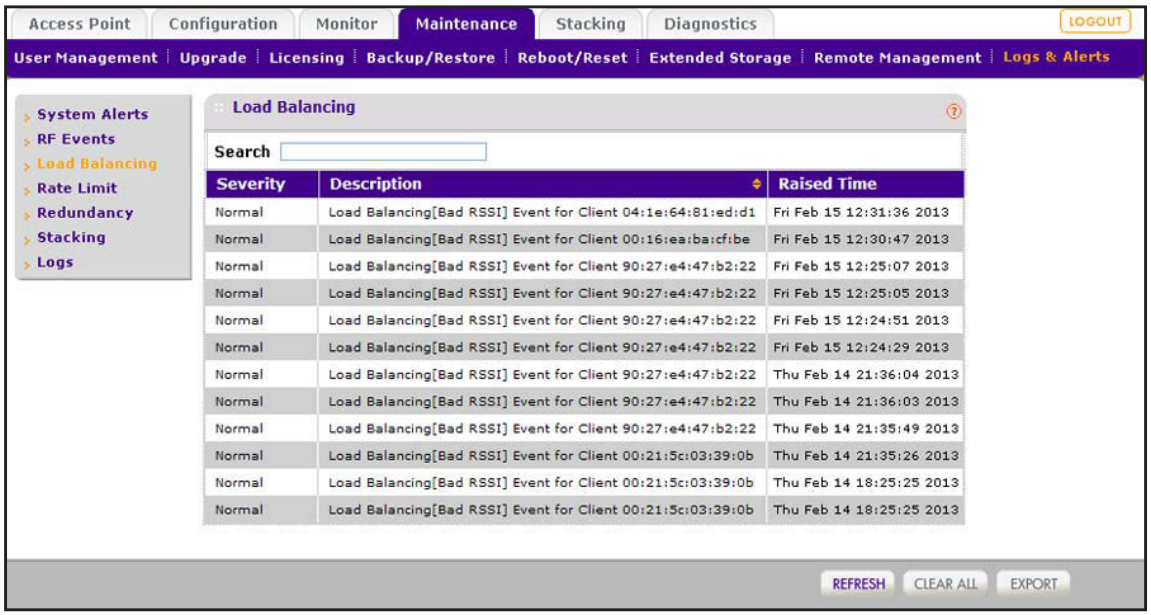
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > Load Balancing**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest events onscreen, click the **REFRESH** button.
7. To save the events to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all events from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the events before you clear them.

View Rate-Limit Events

The wireless controller generates alerts for rate-limit events such as the violation of a rate-limit threshold.

➢ **To view rate-limit events:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

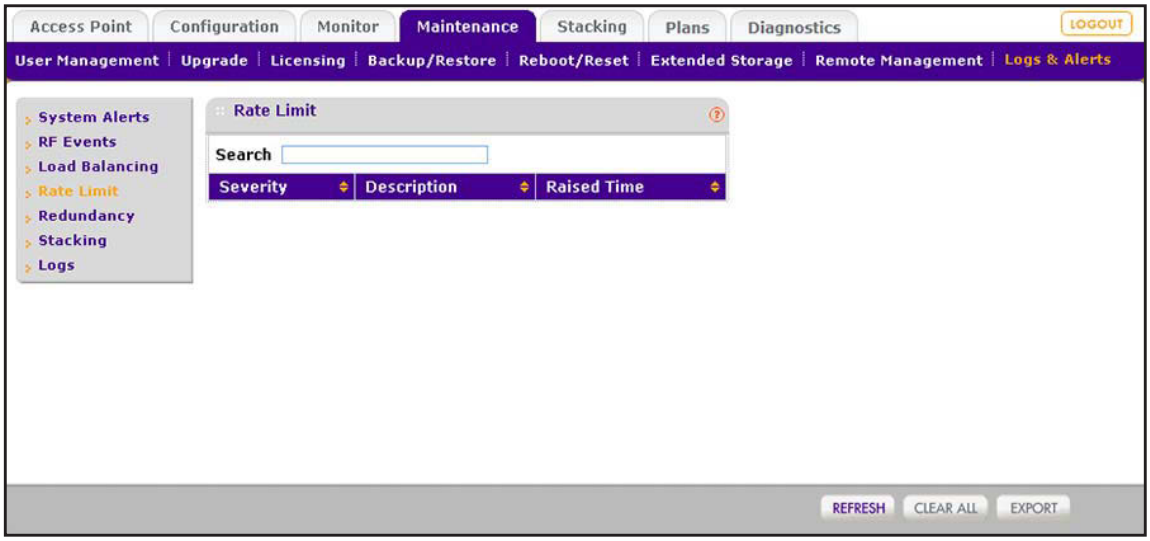
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > Rate Limit**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest events onscreen, click the **REFRESH** button.
7. To save the events to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all events from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the events before you clear them.

View Redundancy Events

The wireless controller generates alerts for redundancy events such as the redundant wireless controller coming up or going down, or a failover to another wireless controller.

➢ **To view redundancy events:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

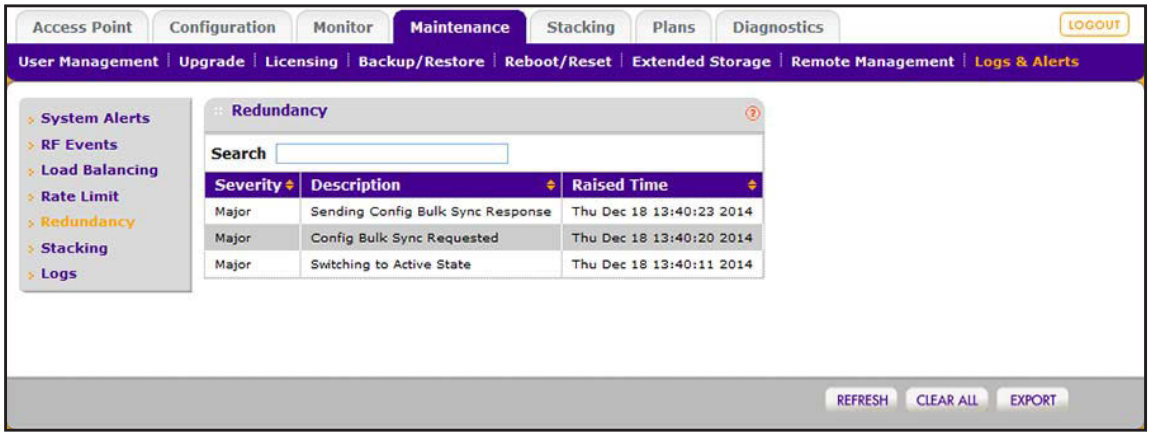
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > Redundancy**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest events onscreen, click the **REFRESH** button.
7. To save the events to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all events from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the events before you clear them.

View Stacking Events

The wireless controller generates alerts for stacking events such as a slave wireless controller coming up or going down, or two wireless controllers synchronizing.

➢ **To view stacking events:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

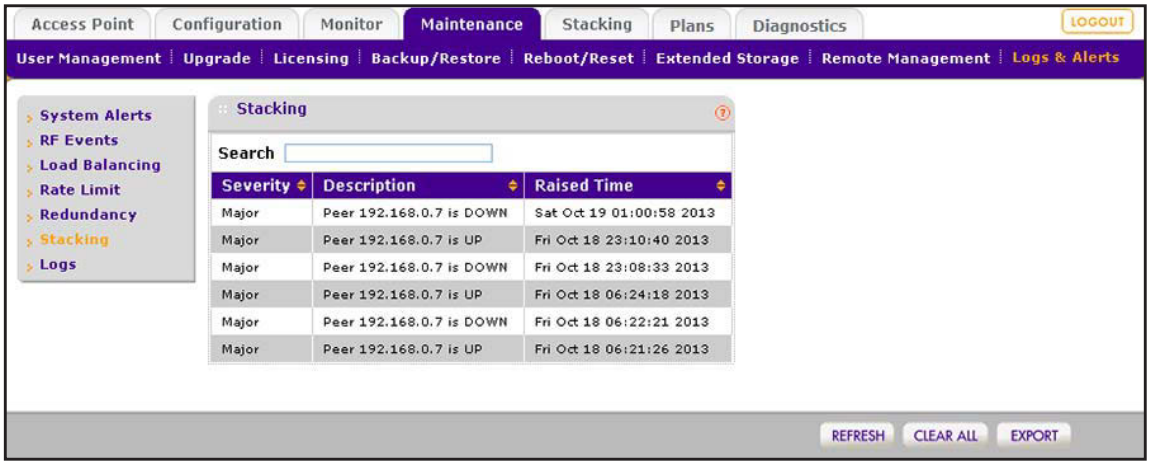
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Logs & Alerts > Stacking**.



5. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
6. To display the latest events onscreen, click the **REFRESH** button.
7. To save the events to your computer, click the **EXPORT** button and follow the directions of your browser.
8. To clear all events from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the events before you clear them.

Manage Licenses

The License page allows you to import, register, and view the licenses that you require for your network. For more information about licenses, see *Licenses* on page 16.

The License page provides four tabs:

- **Inventory**. Provides an overview of your licenses. For information, see *View Your Licenses* on page 266.
- **Server Settings**. Allows you to configure the server settings to import your licenses. For information, see *Configure the License Server Settings* on page 109.
- **Registration**. Allows you to register your licenses. For information, see *Register Your Licenses With the License Server* on page 110.
- **Advanced**. Lets you retrieve your licenses. This page displays relevant information only if you receive a replacement unit from NETGEAR and install the unit. Under normal circumstances, you do not need this page. For information, see *Retrieve Your Licenses* on page 268.

View Your Licenses

When your licenses are installed and registered, you can view them on the Inventory page.

➢ **To view your licenses:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

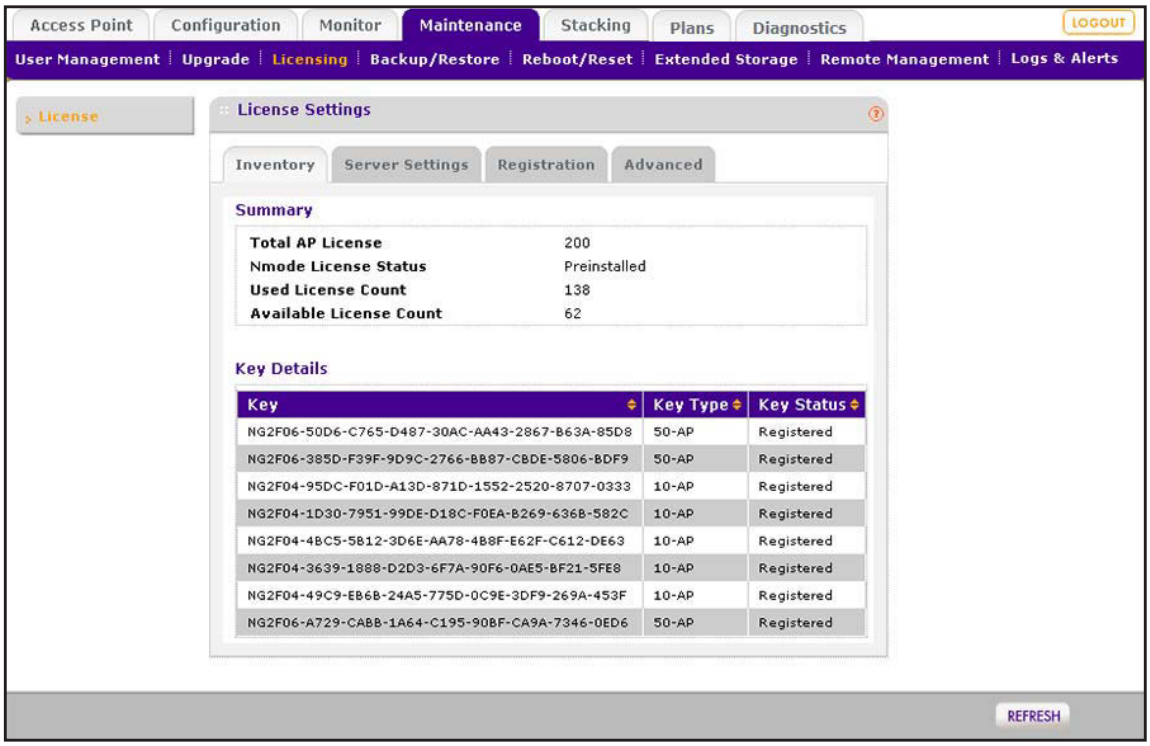
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Licensing**.
5. Click the **Inventory** tab.



The following table describes the fields of the page.

Setting	Description
Summary section	
Total AP License	The number of access points that your licenses support.
Nmode License Status	Availability of the 802.11n mode license. (This license is available by default, indicated by either **Preinstalled** or **Available**.)
Used License Count	The number of access points that are used from the total number that your licenses support.
Available License Count	The number of access points that are still available from the total number that your licenses support.
Key Details section	
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**).

6. To refresh your license information onscreen, click the **REFRESH** button.

Retrieve Your Licenses

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

➢ **To retrieve licenses after you receive a replacement unit from NETGEAR:**

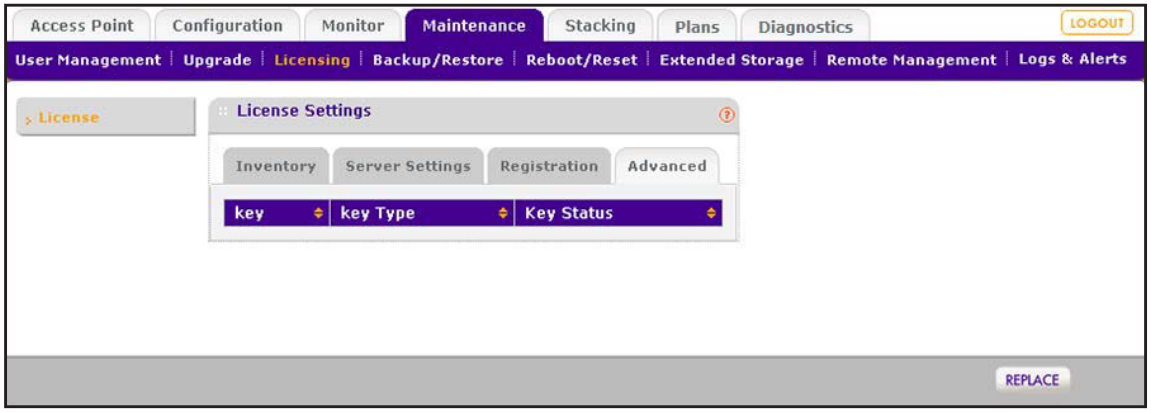
1. Make sure that the wireless controller is connected to the Internet.
2. Make sure that the DNS servers are configured correctly.

   For information about configuring DNS servers, see *Manage the IP, VLAN, and Link Aggregation Settings* on page 101.
3. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
4. Enter your user name and password.
5. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
6. Select **Maintenance > Licensing**.
7. Click the **Advanced** tab.



8. Click the **Replace** button.

   The wireless controller connects to the license update server and retrieves your licenses.

Reboot Access Points

Under normal circumstances, you do not need to reboot an access point. If a problem occurs with an access point, you can reboot it to see if this resolves the problem.

➢ **To reboot an access point:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

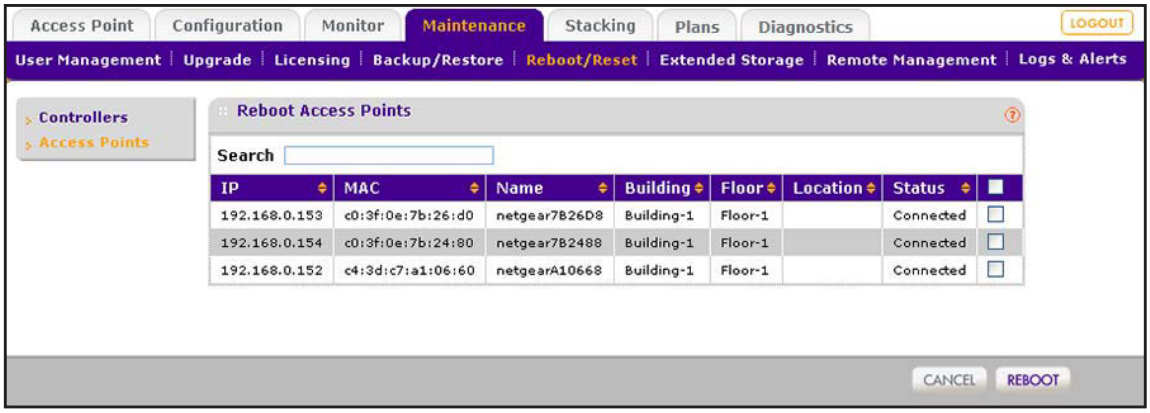
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Maintenance > Reboot/Reset > Access Points**.



5. To find the access point that you want to reboot, in the **Search** field, enter the IP address, MAC address, model, or name of the access point, or enter other information to narrow down the information that is displayed in the table.

   The table displays only the access point or access points that match the information that you entered in the **Search** field.

6. Take one of the following actions:
   - Select a single access point by selecting the check box to the right of the access point.
   - Make a selection of access points by selecting the check boxes to the right of the access points.
   - Select all access points by selecting the check box in the upper right of the table heading.
7. Click the **Reboot** button.

   The selected access point or access points are rebooted.

Configure Multicast Firmware Upgrade for Access Points

When you add access points to the managed list (see *Chapter 8, Discover and Manage Access Points*), the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller. By default, this firmware upgrade process uses multicast, which allows all access points to be upgraded simultaneously. If you prefer, you can disable multicast and let the wireless controller use unicast for the firmware upgrade process (see *Disable Multicast Firmware Upgrade* on page 271). Also, if the multicast firmware upgrade process fails three times, the wireless controller automatically switches to the unicast firmware upgrade process.

With the default multicast firmware upgrade process, the wireless controller distributes multicast IP addresses to the access points, enabling them to join the multicast group and to receive the firmware upgrade.

Change the Multicast Firmware Upgrade Settings

By default, the wireless controller uses IP range 239.255.0.0–239.255.0.255 for the multicast firmware upgrade process. If your network requires that the wireless controller uses a different multicast IP range, you can configure the IP range on the AP Upgrade Settings page.

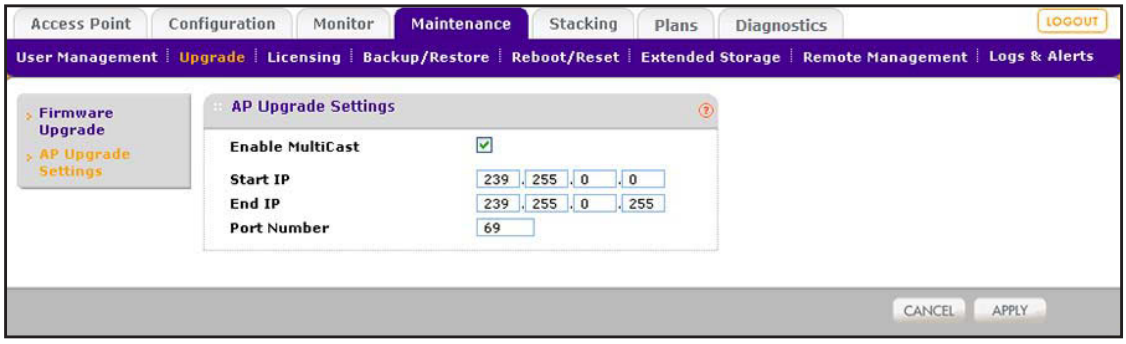
➢ **To configure another multicast IP address range and port for the firmware upgrade process:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Maintenance > Upgrade > AP Upgrade Settings**.



5. Configure the settings as described in the following table.

Setting	Description
Start IP	Enter the start IP address of the multicast range that the wireless controller must use.
End IP	Enter the end IP address of the multicast range that the wireless controller must use.
Port Number	Enter the port number that the wireless controller must use. The default number is **69**.

6. Click the **Apply** button.

   The changes are saved.

Disable Multicast Firmware Upgrade

There might be network configurations in which you cannot use multicast. If you disable multicast on the AP Upgrade Setting page, the firmware upgrade process uses unicast, which is a slower process because the firmware upgrade is applied to groups of access points instead of simultaneously to all access points. The time that the unicast firmware upgrade process takes depends on the network load and on the type of Ethernet interface to which the wireless controller is connected.

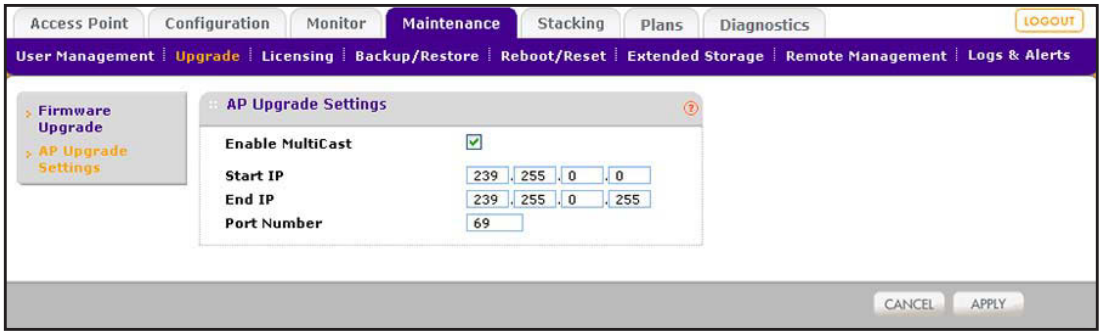
➢ **To disable multicast firmware upgrade for access points:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Maintenance > Upgrade > AP Upgrade Settings**.



5. Clear the **Enable Multicast** check box.

   This check box is selected by default.
6. Click the **Apply** button.

   The changes are saved.

12 Manage Stacking and Redundancy

This chapter includes the following sections:

- *Stacking Concepts*
- *Configure a Stack of Wireless Controllers*
- *Remove a Wireless Controller From a Stack*
- *Select Which Wireless Controller in a Stack to Configure*
- *Manage Redundancy for a Single Controller*
- *Manage a Redundancy Group With N:1 Redundancy*
- *Replace a Redundant Controller*
- *Remove a Redundancy Group*

Note: Model WC7500 does not support stacking and redundancy.

Note: *Master* and *slave* refers to the relationship between controllers in a stack. *Primary* and *redundant* (or *primary* and *secondary*) refers to the relationship between controllers in a redundant configuration.

Stacking Concepts

The wireless controller supports stacking of up to three units for management of up to 150 access points (models WC7600 and WC7600v2) or 600 access points (model WC9500) through purchased licensing (see *Licenses* on page 16).

In a stack, one wireless controller functions as the master controller, and the other two wireless controllers function as slave controllers.

The following figure shows a stacked configuration with WC9500 wireless controllers in which you can manage up to 600 access points:

Figure 17. WC9500 stacking configuration

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

The following procedure described the high-level configuration steps to set up a stack.

➢ **To set up a stack:**

1. Configure the master controller, including the system settings, profiles, security settings, and WiFi settings.
2. On each slave controller, configure the system settings only.
3. On the master controller, enable stacking and add all slave controllers to the stack.
4. On the master controller, synchronize the configurations to the slave controllers.

   The profiles, security settings, WiFi settings, administrative user name and password, and firmware image of the master controller are synchronized to the slave controllers. The managed AP list of the master controller is not synchronized.
5. On each slave controller, run the Discovery Wizard to discover the access points that the slave controller must manage and add them to the managed AP list for the slave controller.

After you configure the stack, you can change profiles, security settings, and WiFi settings on the master controller, synchronize these changes with the slave controllers, and let the slave controllers push the changes to the individual access points that they manage. For ease of management, you can configure location-based profiles on the master controller and assign a location to each slave controller.

Stacking allows WiFi 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.

The master and slave controllers in a stack support the following capacities:

- **Master controller**. You can perform the following tasks:
  - Manage the slave controllers
  - Perform RF planning for the slave controllers
  - Configure the entire network, including access point discovery and license reinforcement
  - Monitor the entire network
  - Push new a firmware image to the slave controllers
- **Slave controller**. You can perform the following tasks:
  - Configure the subnetwork
  - Monitor the subnetwork
  - Upgrade the firmware image on the slave controller only
  - Perform access point discovery for the subnetwork
  - Reinforce licenses for the subnetwork

Note: A single WC9500 wireless controller that does not function in a stack can manage up to 300 access point; a single WC9500 wireless controller in a stack can manage up to 200 access points.
If a WC9500 wireless controller does not function in a stack and manages *more* than 200 access points and you add the WC9500 wireless controller to a stack, all access points are removed from its managed list. The access points are removed because of the reduction in maximum capacity from 300 to 200 access points.
You must let the WC9500 wireless controllers in the stack rediscover the access points and add them to the managed lists of several WC9500 wireless controllers in the stack.

Configure a Stack of Wireless Controllers

A stack can consist of up to three wireless controllers, one of which is the master controller and two of which are slave controllers.

The following procedure assumes that you already configured the system settings, profiles, security settings, and WiFi settings on the master controller, and that you already configured the system settings on the slave controller.

➢ **To create a stack by adding a slave controller to a wireless controller that functions as the master controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

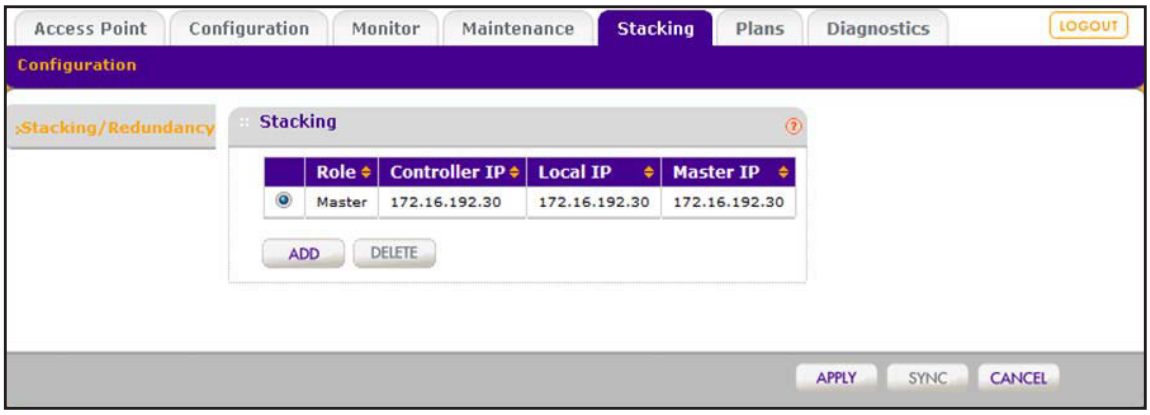
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

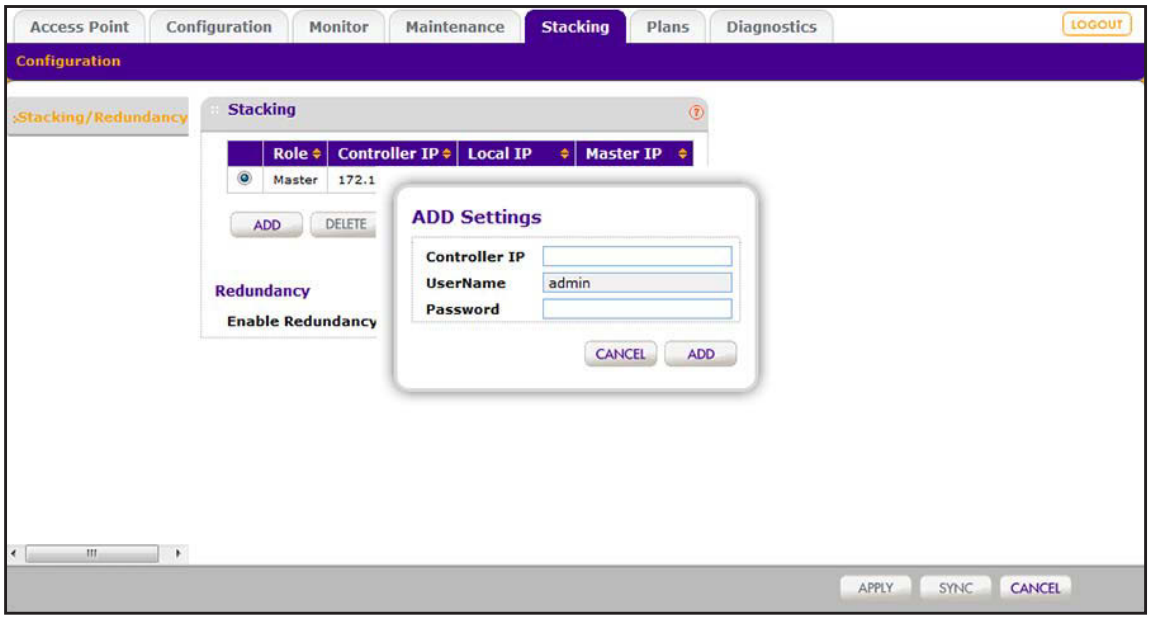
   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.



   The Stacking table shows the master wireless controller with its IP addresses.

5. Click the **Add** button.

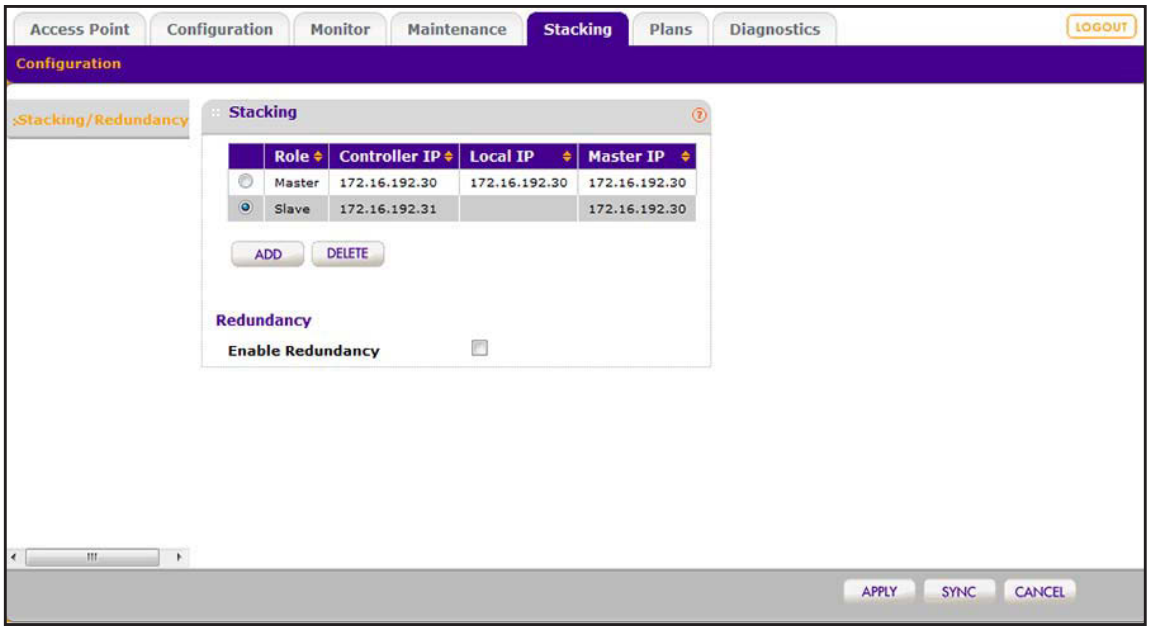


6. Configure the settings for the slave controller as described in the following table.

Setting	Description
Controller IP	Enter the IP address of the slave controller. This is the address that you use to log in to the slave controller's web management interface.
UserName	The user name is a nonconfigurable field that displays the user name with which you log in to the web management interface of the slave controller. By default, the user name is admin.
Password	Enter the password with which you log in to the web management interface of the slave controller. If you did not yet personalize the password, enter **password** for the password.

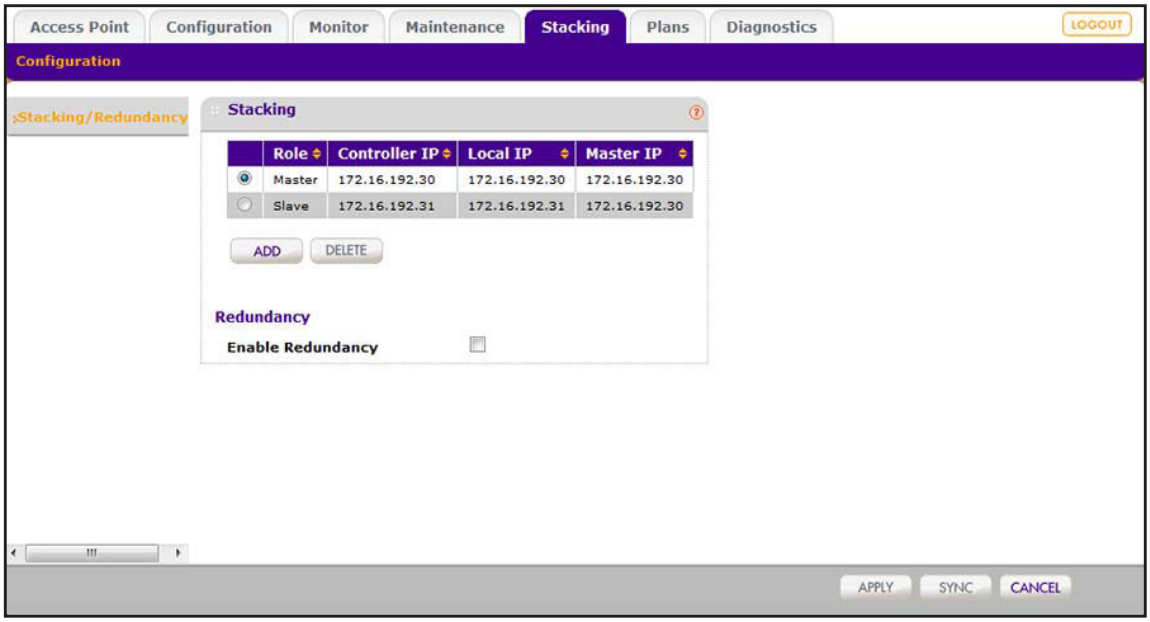
7. Click the **Add** button.

   The wireless controller is added to the Stacking table but the local IP address for the slave controller is not yet shown.



8. Click the **Apply** button.

   The changes are saved. After the configuration of the master controller synchronizes with the slave controller, the stack is established.



The Stacking table shows the following fields:

Setting	Description
Role	The role or function that the wireless controller provides in the stack: either **Master** or **Slave**.
Controller IP	The IP address of the wireless controller. In a stacking configuration, the controller IP address is identical to the local IP address.
Local IP	The local IP address of the wireless controller in the stacking group. This IP address remains constant. The role of the wireless controller (that is, master or slave) does not affect the local IP address.
Master IP	The IP address of the master in the stack.

9. To add another wireless controller, repeat *Step 5* through *Step 8*.
10. To synchronize the profiles, captive portals, and user management settings of the master controller to a slave controller in the stack, do the following:
    a. In the Stacking table, select the radio button for the slave controller that you want to synchronize.
    b. Click the **Sync** button.
    c. Confirm that you want to allow the slave controller to reboot.

    After synchronization, the slave controller reboots.
11. Select **Monitor > Network > Summary**.

    The Summary page displays for the network.

    Note: The web management interface displays an additional **Network** menu tab with the network Summary page in view. The network Summary page displays information about the stacking configuration.

12. Click the **REFRESH** button.

    The Summary page displays the new stacking information.

Note: On a 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. For information about selecting which controller to configure, see *Select Which Wireless Controller in a Stack to Configure* on page 280.

Remove a Wireless Controller From a Stack

You can remove a wireless controller from a stack.

➢ **To remove a wireless controller from a stack:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

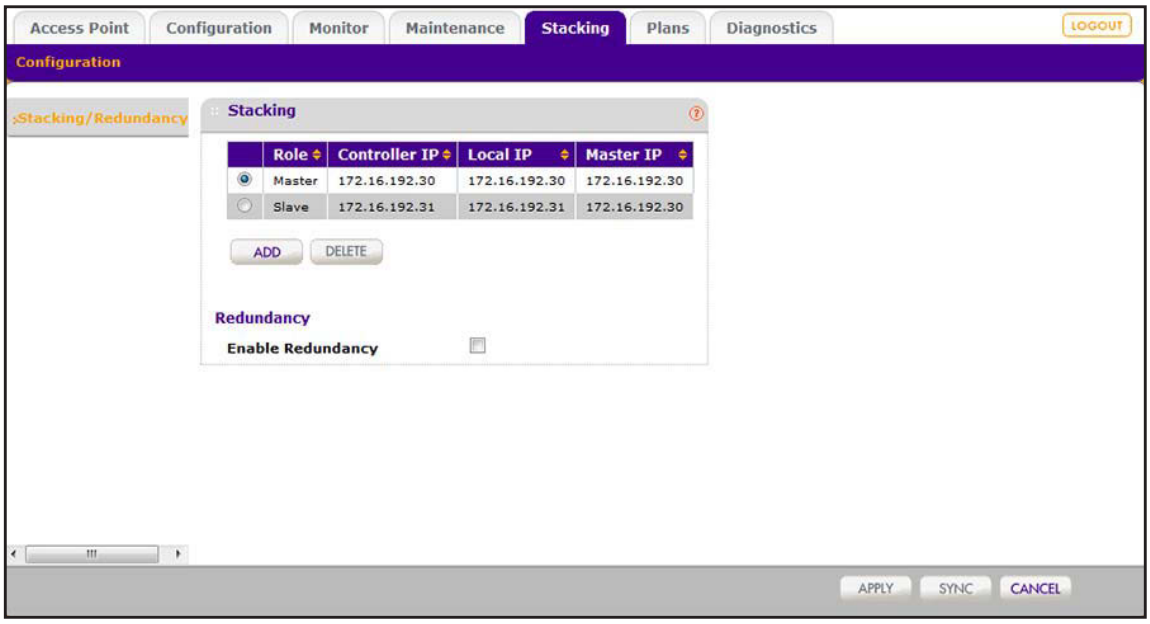
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.



5. In the Stacking table, select the radio button for the slave controller that you want to remove.

   Note: You cannot remove the master controller.

6. Click the **Delete** button.

   The slave controller is removed from the stack.

7. Click the **Apply** button.

   The changes are saved. The master controller and former slave controllers reboot. Depending on the number of controllers in the stack, the stack is either decreased in size and now consists of two instead of thee controllers, or removed entirely.

Select Which Wireless Controller in a Stack to Configure

After you add one or more wireless controllers to the stack, most pages of the web management interface display a controller selection menu at the top. This menu lets you select the wireless controller that you want to configure.

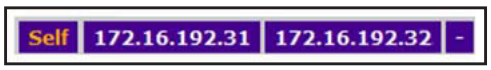


Figure 18. Controller selection menu with three wireless controllers in stack

In the previous figure, Self indicates the wireless controller that you are configuring through the web management interface. Self is shown in orange font. The two IP addresses (172.16.192.31 and 172.16.192.32) indicate the other wireless controllers in the stack. These IP addresses are shown in white font. A selected controller is shown in orange font. Other controllers in the stack that are not selected are shown in white font.

The following procedure is an example of how to select a wireless controller in a stack to configure the basic radio on/off settings. After you select a wireless controller to configure, this selection carries through to other pages of the web management interface until you select to configure another wireless controller in the stack.

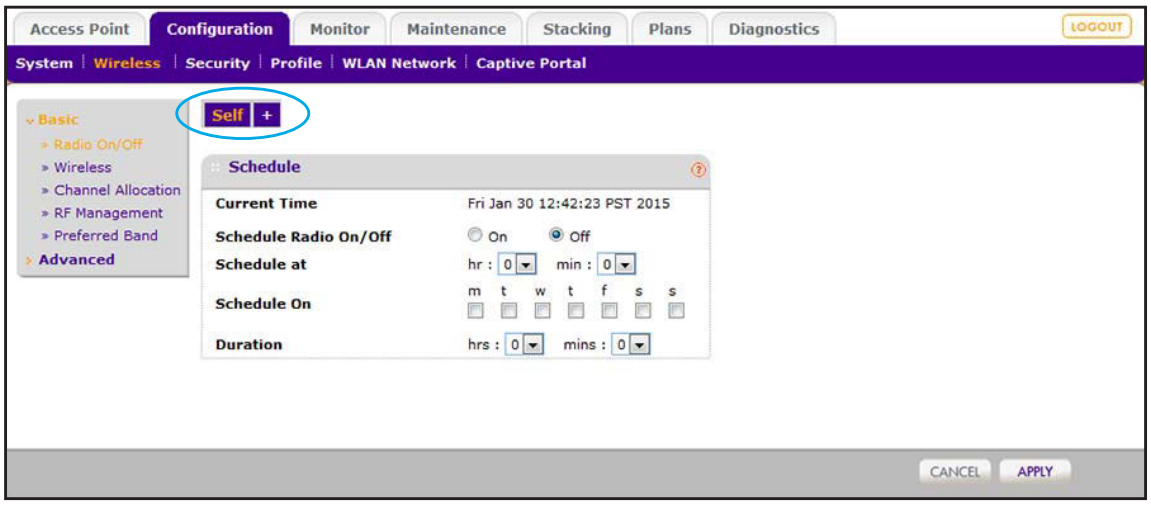
➢ **To select a wireless controller for configuration in a stack with two controllers:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

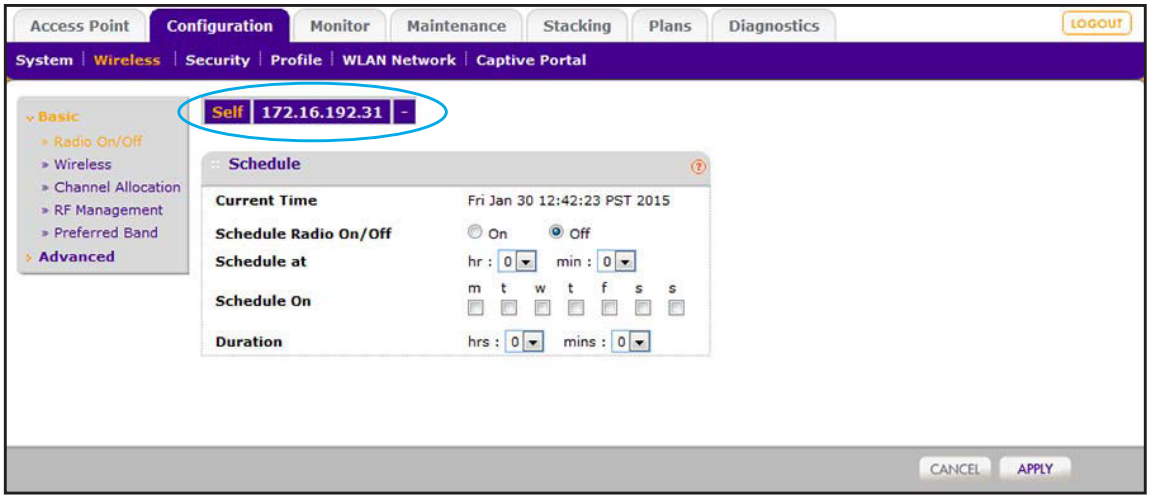
   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Configuration > Wireless > Basic > Radio On/Off**.



The controller selection menu shows Self in orange font as the wireless controller that you are accessing through the web management interface.

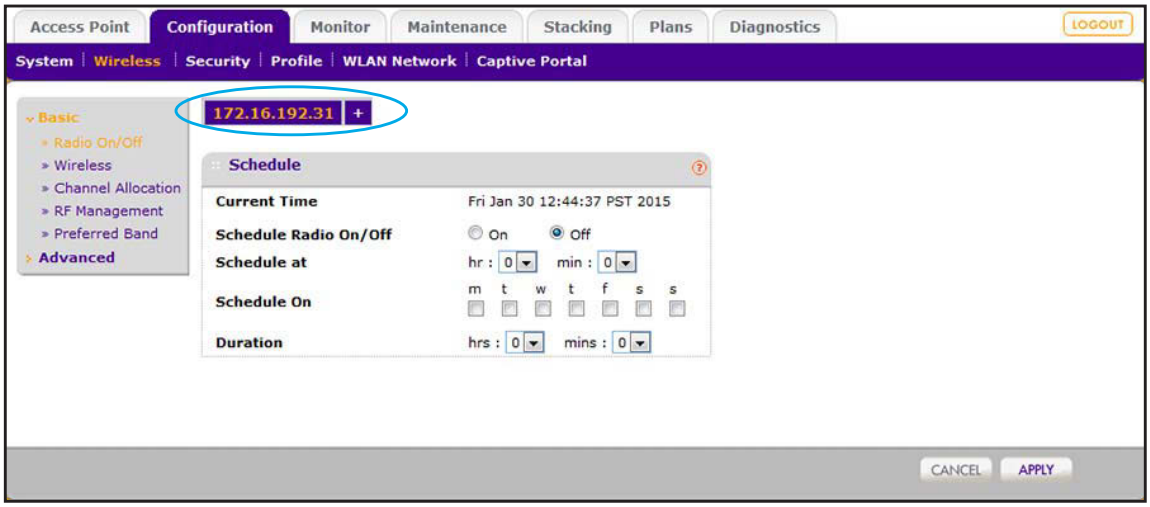
5. In the controller selection menu, next to Self, click the **+** button.



The IP address of the other wireless controller in the stack displays in white font in the controller selection menu.

6. In the controller selection menu, click **172.16.192.31**, which is the IP address of the other wireless controller in the stack.

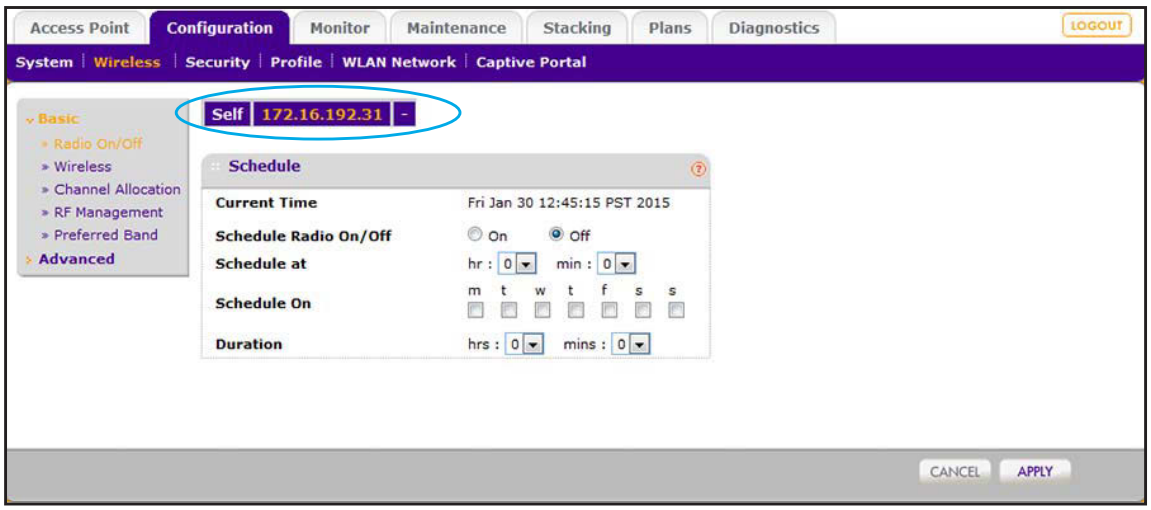
The web management interface accesses the other wireless controller in the stack.



The controller selection menu shows the IP address of the other wireless controller in the stack in orange font on the left. Self is no longer shown.

Note: If you select another page in the web management interface, the controller selection menu continues to shows the IP address of the other wireless controller as the one being configured.

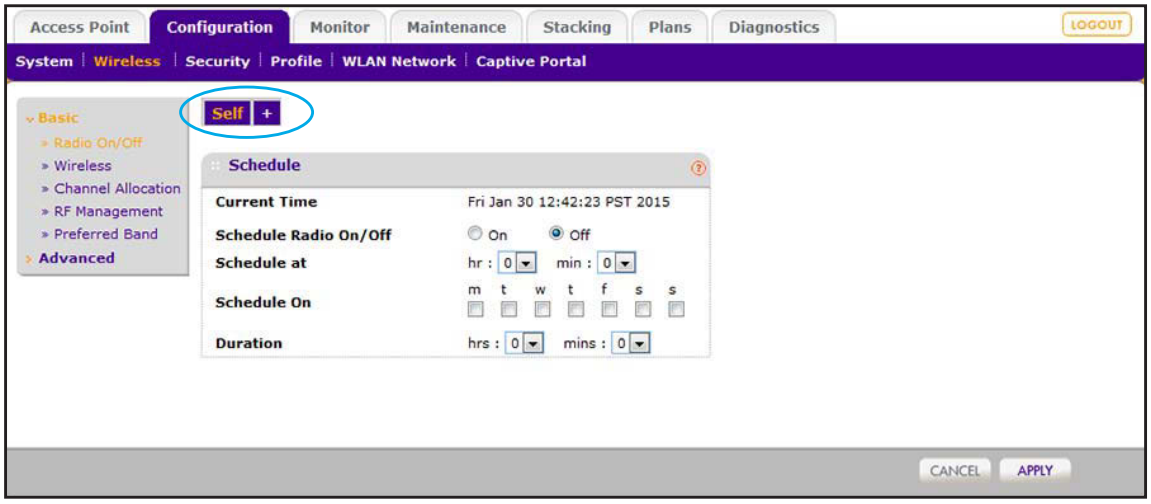
7. To change back to the original wireless controller, in the controller selection menu next to the IP address (172.16.192.31), click the **+** button.



In the controller selection menu, Self displays in white font to the left of the IP address of the other wireless controller in the stack.

8. In the controller selection menu, click **Self**.

The web management interface accesses the original wireless controller in the stack.



The controller selection menu once again shows Self in orange font. The IP address of the other wireless controller in the stack is no longer shown.

Manage Redundancy for a Single Controller

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

For information about N:1 redundancy, see *Manage a Redundancy Group With N:1 Redundancy* on page 289.

VRRP Redundancy Concepts

You can configure two controllers to form a redundancy group. You then designate one controller in the redundancy group as the primary controller (the master) and the other wireless controller as the redundant controller (the secondary 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.

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

Requirements and Restrictions for 1:1 Redundancy

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

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

Example of a 1:1 Redundancy Configuration

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

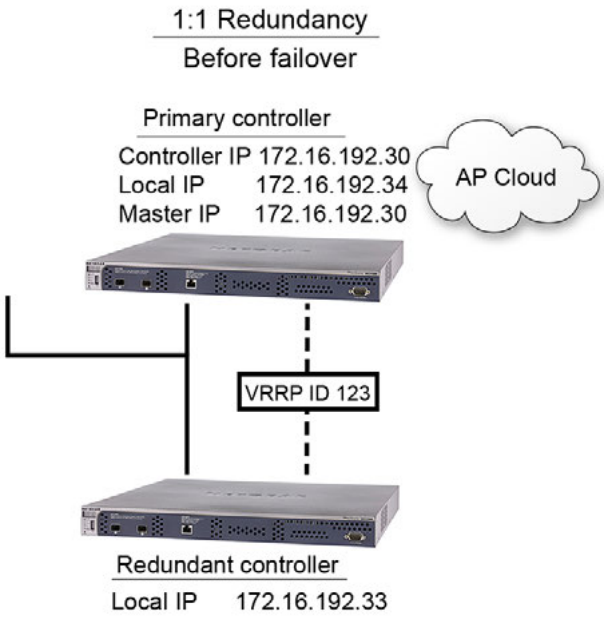


Figure 19. Primary and redundant controllers before a failover

The following figure shows the settings on the Stacking/Redundancy page before a failover occurs.

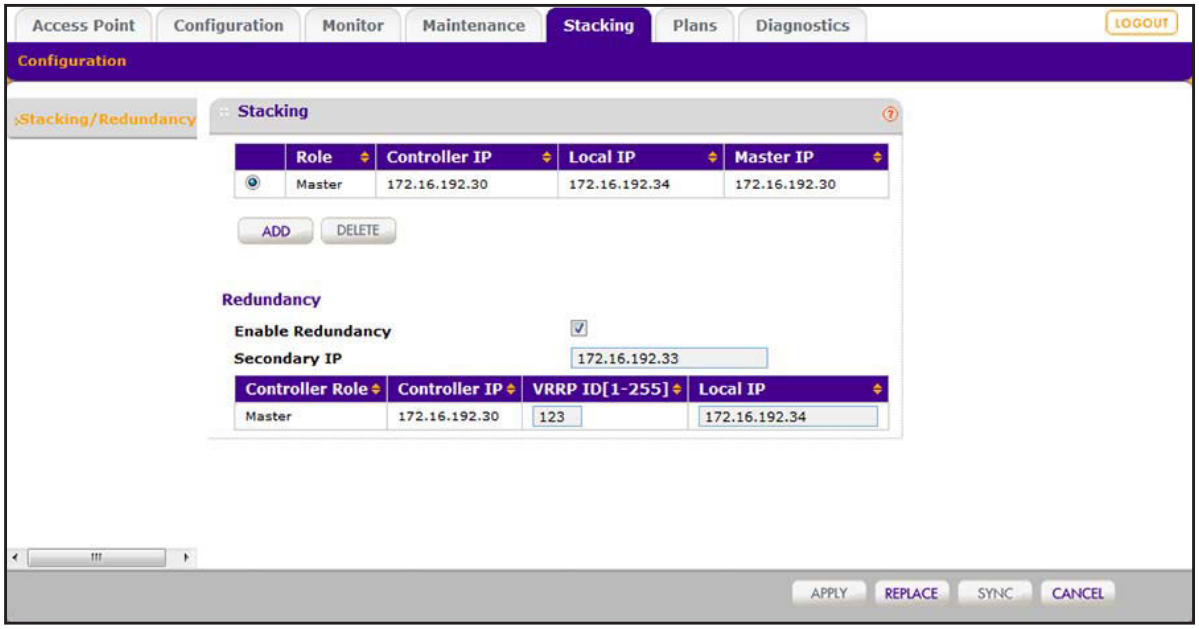


Figure 20. Stacking/Redundancy page before a failover

The following figure shows a configuration with a primary controller and a redundant controller *after* a failover occurred in which the primary controller went down and the redundant controller became the active controller.

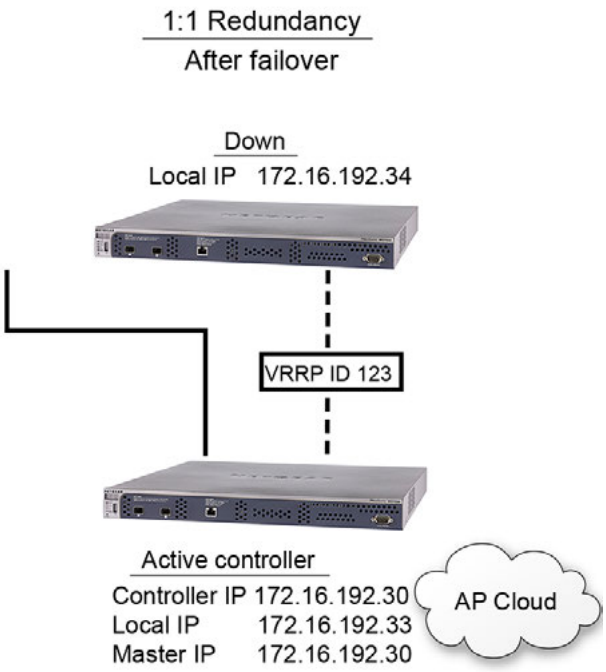


Figure 21. Primary and redundant controllers after a failover

Configure a Single Controller With Redundancy

To enable 1:1 redundancy, configure the secondary IP address (that is, the IP address for the redundant controller), the VRPP ID for the connection between the primary and the redundant controller, and the local IP address for the primary controller. Both controllers require matching licenses. If licenses do not match, redundancy cannot be established. For additional requirements, see *Requirements and Restrictions for 1:1 Redundancy* on page 283.

➢ **To configure a single controller with redundancy:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

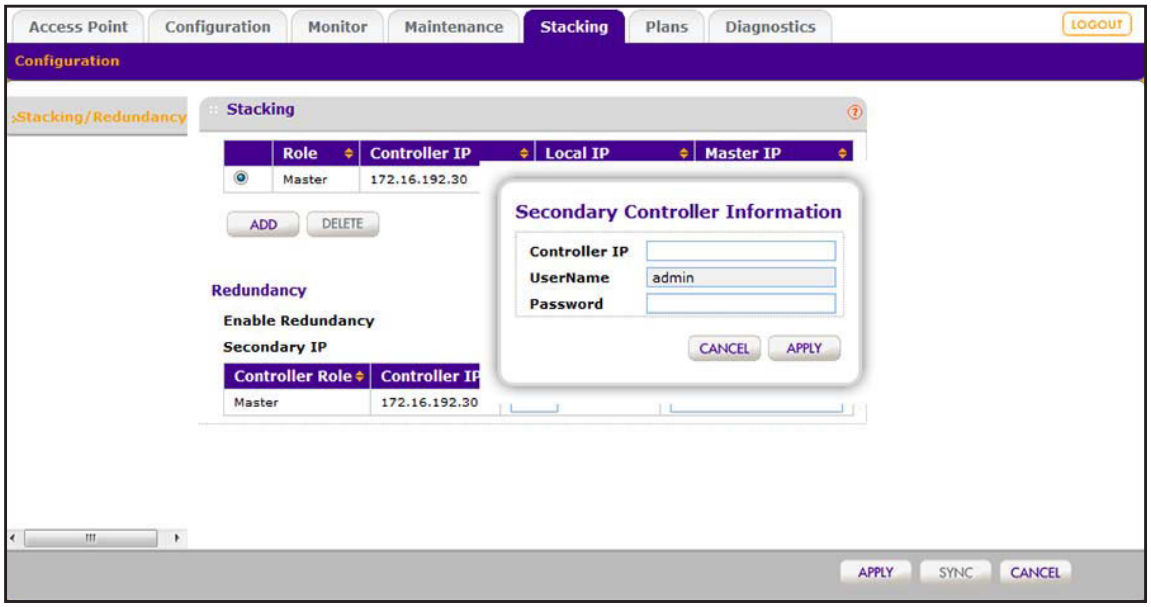
   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.

The Stacking/Redundancy page displays.

5. Select the **Enable Redundancy** check box.

   The Redundancy page expands to display the Redundancy table and the Secondary Controller Information pop-up window opens.

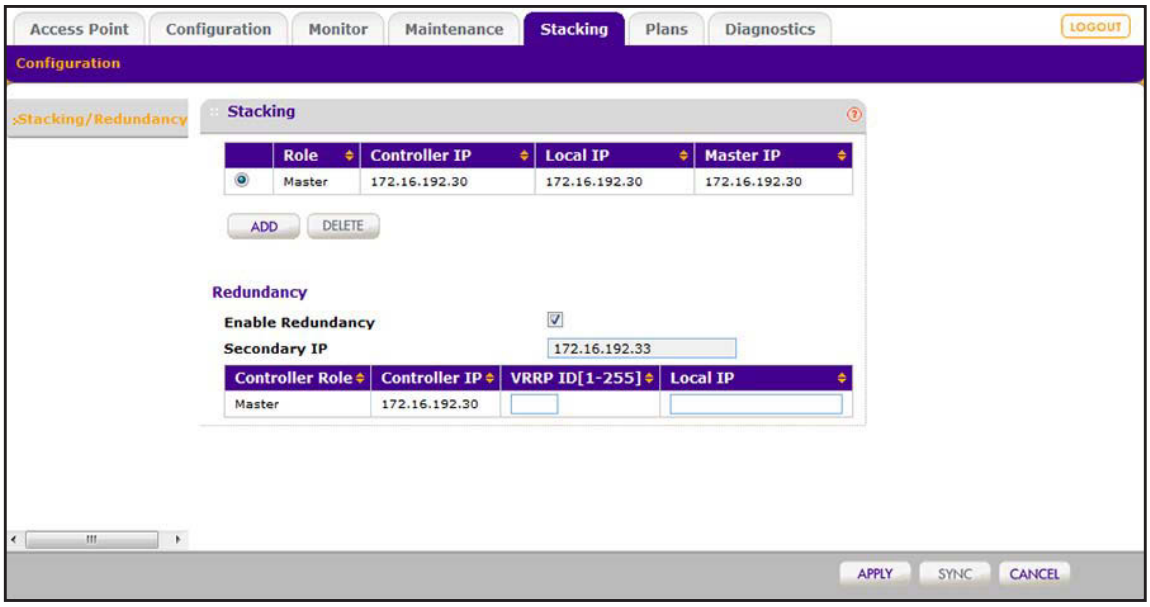


6. Configure the settings for the redundant controller (that is, the secondary controller) as described in the following table.

Setting	Description
Controller IP	Enter the IP address of the redundant controller. This is the address that you use to log in to the redundant controller's web management interface.
UserName	The user name is a nonconfigurable field that displays the user name with which you log in to the web management interface of the redundant controller. By default, the user name is admin.
Password	Enter the password with which you log in to the web management interface of the redundant controller. If you did not yet personalize the password, enter **password** for the password.

7. Click the **Apply** button.

   The changes are saved. The **Secondary IP** field displays the IP address of the redundant controller (that is, the secondary controller).



8. Configure the VRRP ID and local IP address of the primary controller (that is, the master) as described in the following table.

   These settings are required so that the primary controller and redundant controller can establish a redundancy group.

   The following table also includes descriptions of the nonconfigurable fields.

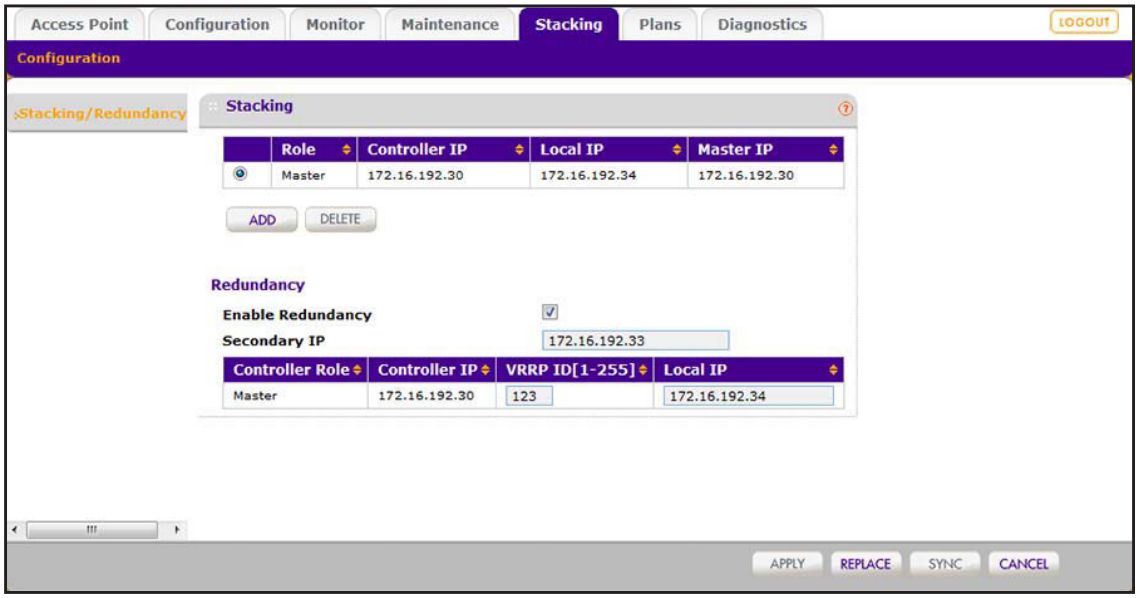
Setting	Description
Controller Role	This is a nonconfigurable field that shows that the role of the primary controller. In a 1:1 redundancy configuration, by default, the role is master.
Controller IP	This is a nonconfigurable field that shows the IP address of the primary controller. This IP address is the address that you use to log in to the primary controller's web management interface. **Note:** The controller IP address of the primary controller (the master) is also the master IP address.
VRRP ID [1-255]	For the primary controller, enter a number from **1** through **255** as the VRRP ID. This number must be unique and not assigned to any other device in the network.
Local IP	For the primary controller, enter a local IP address. If a failover occurs, this IP address remains assigned to the primary controller and does *not* transfer to the redundant controller to let you identify the primary controller before and after the failover. You must enter an IP address that is not assigned to any other device.

WARNING:

Enabling redundancy causes the redundancy process on the primary wireless controller to restart, which might temporarily affects traffic on the managed access points in the network.

9. Click the **Apply** button.

   The changes are saved. After the configuration of the primary controller synchronizes with the redundant controller, redundancy goes into effect.

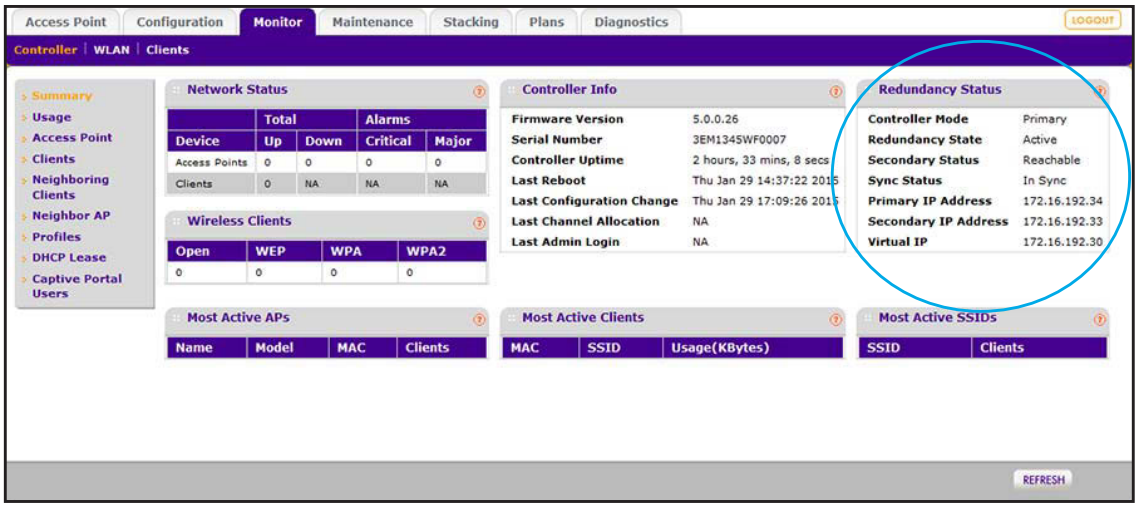


10. Select **Monitor > Controller > Summary**.

    The Summary page displays for the controller.

11. Click the **REFRESH** button.

    The Summary page displays the new redundancy information.



Manage a Redundancy Group With N:1 Redundancy

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

For information about 1:1 redundancy, see *Manage Redundancy for a Single Controller* on page 283.

VRRP N:1 Redundancy Concepts

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.

The controllers that are served by the redundant controller must function in a stack in which one controller is the master and the other controllers are the slaves. However, in relation to the redundant controller (also referred to as the secondary controller), both the master and the slaves function as primary controllers because the redundant controller can take over for the master or for any of the slaves.

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

Each controller in the redundancy group is assigned a unique controller IP address and a unique local IP address. Local addresses remain constant so that a controller can always be identified before and after a failover. If a 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 occurs, redundancy no longer exists 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, WiFi 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 must be in the same management VLAN and IP subnet.
- The primary controllers must be stacked.
- If three or four controllers are in the same redundancy group, you must configure one controller as the redundant controller and all other controllers as primary controllers.
- All controllers in the redundancy group must run the same firmware version. If the firmware versions do not match, redundancy does not work.
- The licenses on the redundant controller must match those on the primary controller that supports the largest number of licenses. For example, in a redundancy group with two primary controllers, if one primary controller supports a license for 10 access points and the other primary controller supports a license for 50 access points, the redundant controller must support a license for 50 access points. If the licenses do not match, redundancy does not work.
- For the relationship of each primary controller with the redundant controller, you must configure a unique VRRP ID that is also different from any other VRRP IDs that might be used for other purposes in the network. You also must 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.

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 occurs.

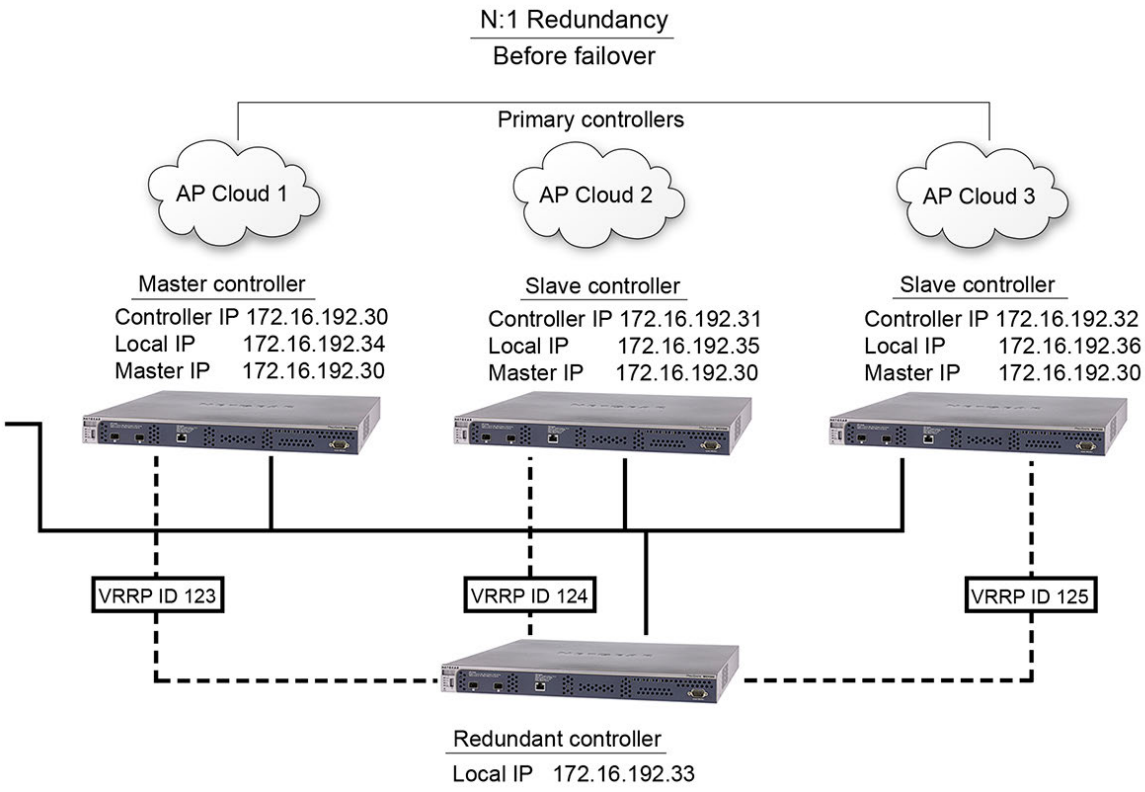


Figure 22. Primary and redundant controllers in an N:1 configuration before a failover

The following figure shows the N:1 settings on the Redundancy page before a failover occurs.

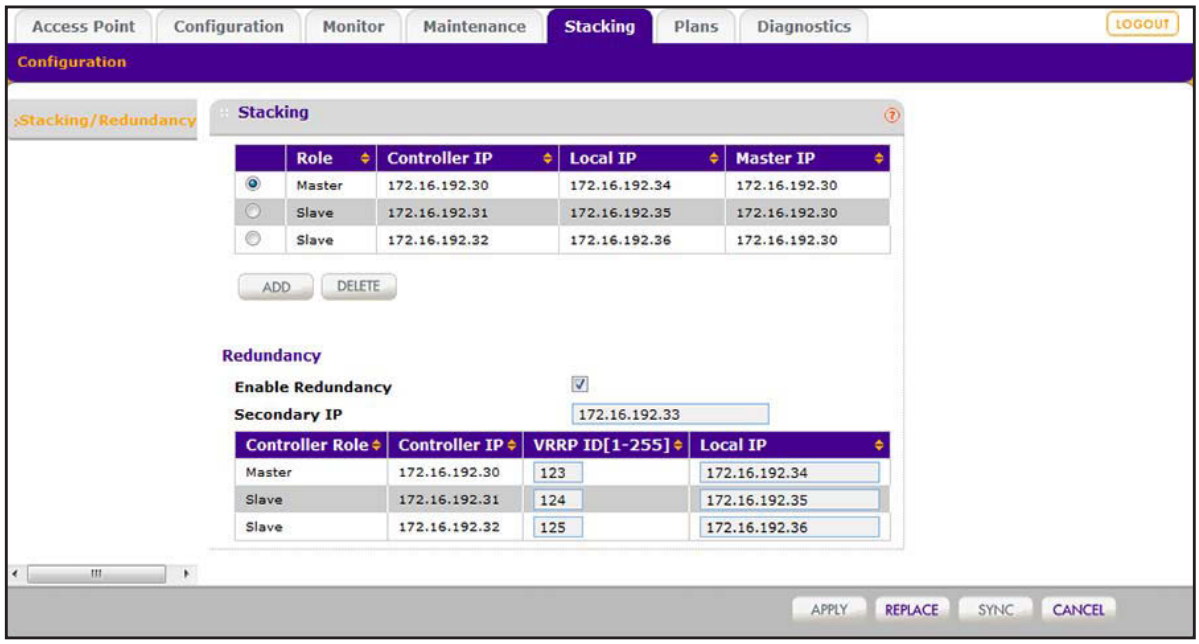


Figure 23. Redundancy page for an N:1 configuration before a failover

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

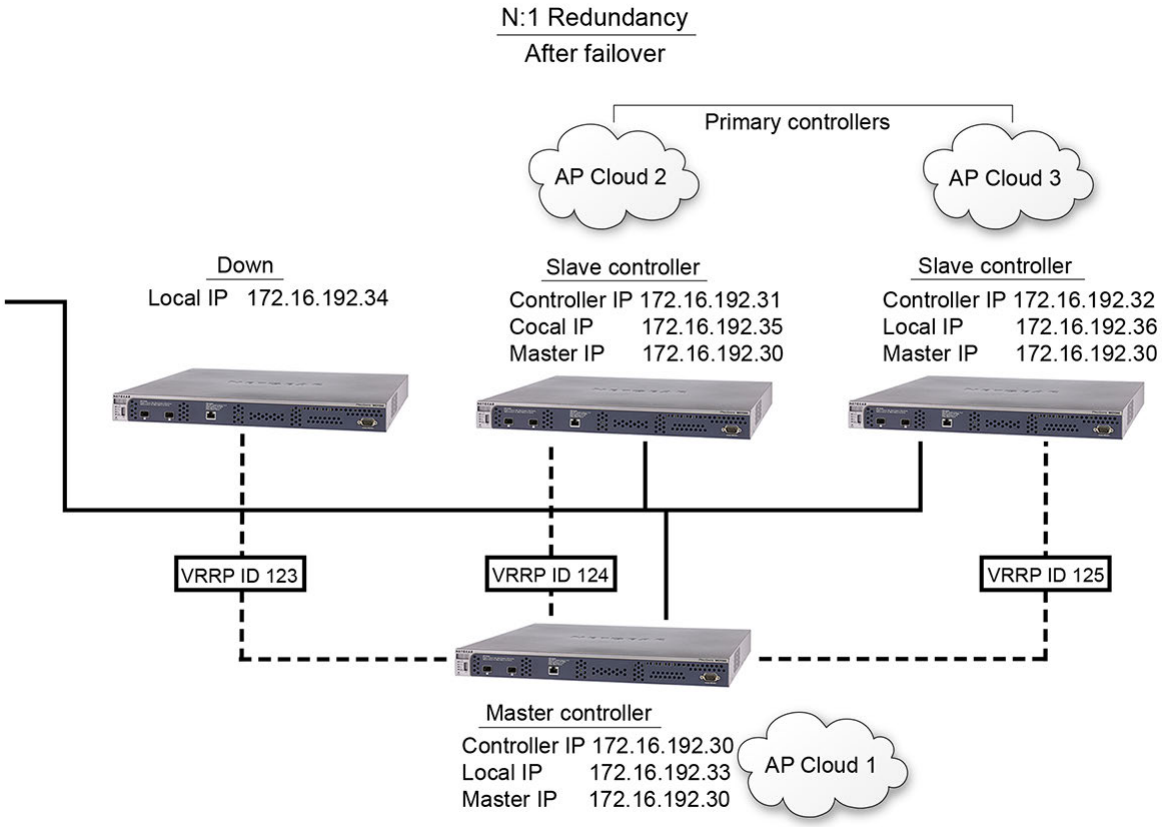


Figure 24. Primary and redundant controllers in an N:1 configuration after a failover

Configure a Redundancy Group With N:1 Redundancy

To enable N:1 redundancy, configure the redundancy settings on the primary controllers (the master and one or two slaves) and on the redundant controller (the secondary controller) that serves all primary controllers. All controllers require matching licenses. If licenses do not match, redundancy cannot be established. For additional requirements, see *Requirements and Restrictions for N:1 Redundancy* on page 290.

An N:1 redundancy group includes two or three primary controllers that usually operate as a stack:

- To configure redundancy for a stack of two controllers, you need three controllers: Two primary controllers (one master and one slave) and one redundant controller that serves both primary controllers.
- To configure redundancy for a stack of three controllers, you need four controllers: Three primary controllers (one master and two slaves) and one redundant controller that serves the three primary controllers.

For information about configuring a stack of controllers, see *Configure a Stack of Wireless Controllers* on page 275.

➢ **To configure N:1 redundancy for a stack of three controllers:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

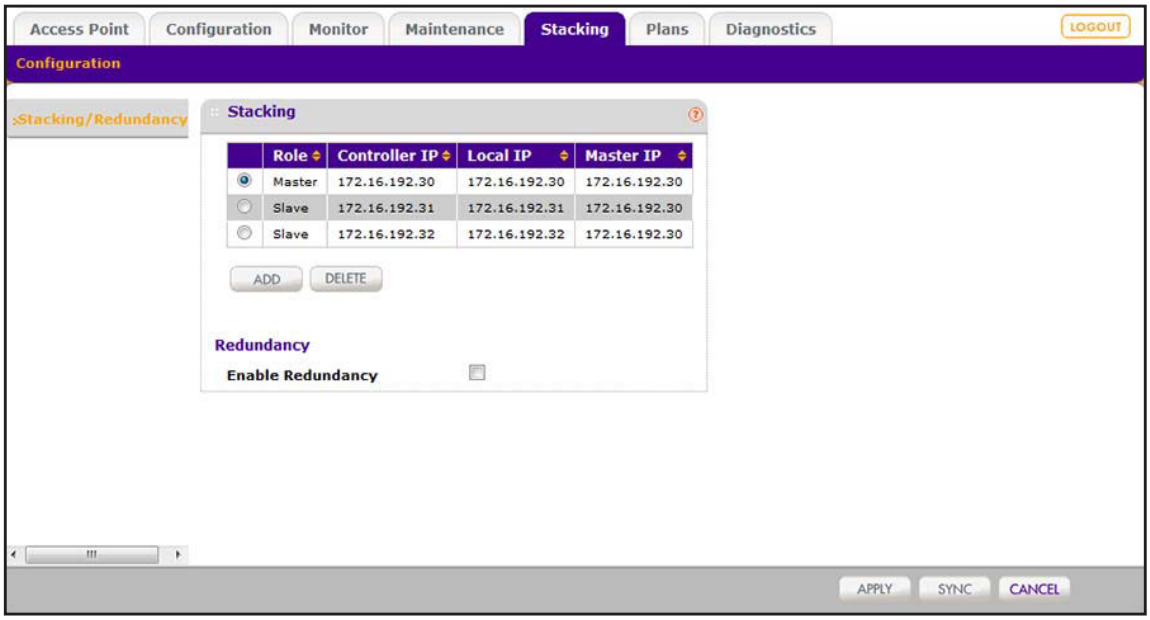
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

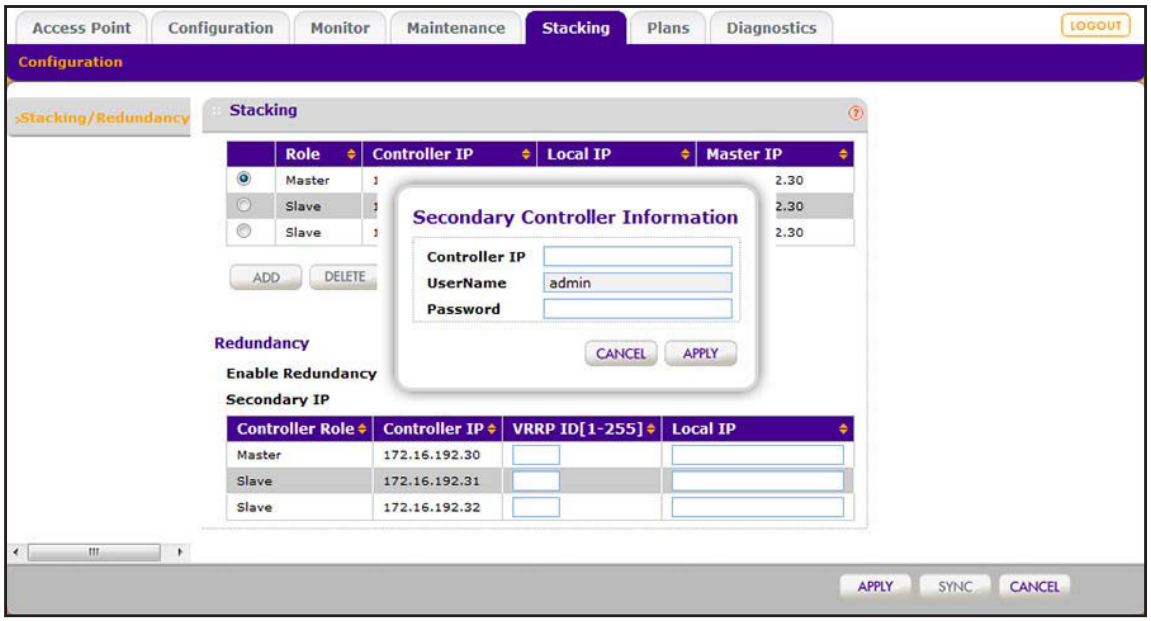
   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.



   The page displays the stacking configuration.

5. Select the **Enable Redundancy** check box.

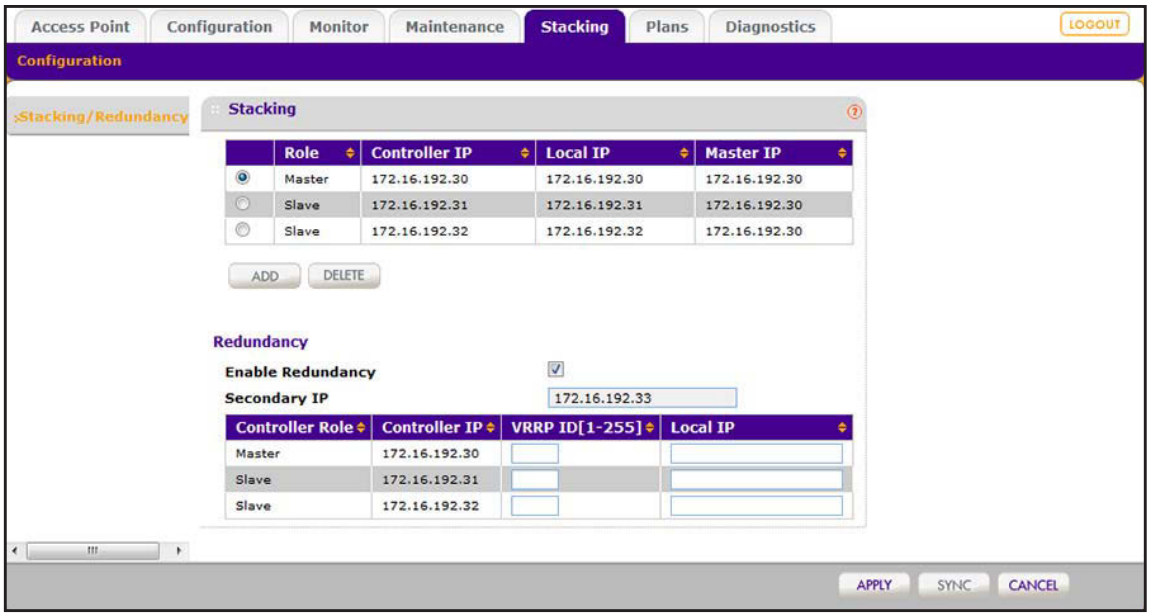


6. Configure the settings for the redundant controller (that is, the secondary controller) as described in the following table.

Setting	Description
Controller IP	Enter the IP address of the redundant controller. This is the address that you use to log in to the redundant controller's web management interface.
UserName	The user name is a nonconfigurable field that displays the user name with which you log in to the web management interface of the redundant controller. By default, the user name is admin.
Password	Enter the password with which you log in to the web management interface of the redundant controller. If you did not yet personalize the password, enter **password** for the password.

7. Click the **Apply** button.

   The changes are saved. The **Secondary IP** field displays the IP address of the redundant controller (that is, the secondary controller).



8. Configure the VRRP ID and local IP address of all primary controllers (that is, the master and the slaves) as described in the following table.

   These settings are required so that the primary controllers and redundant controller can establish a redundancy group.

   The following table also includes descriptions of the nonconfigurable fields.

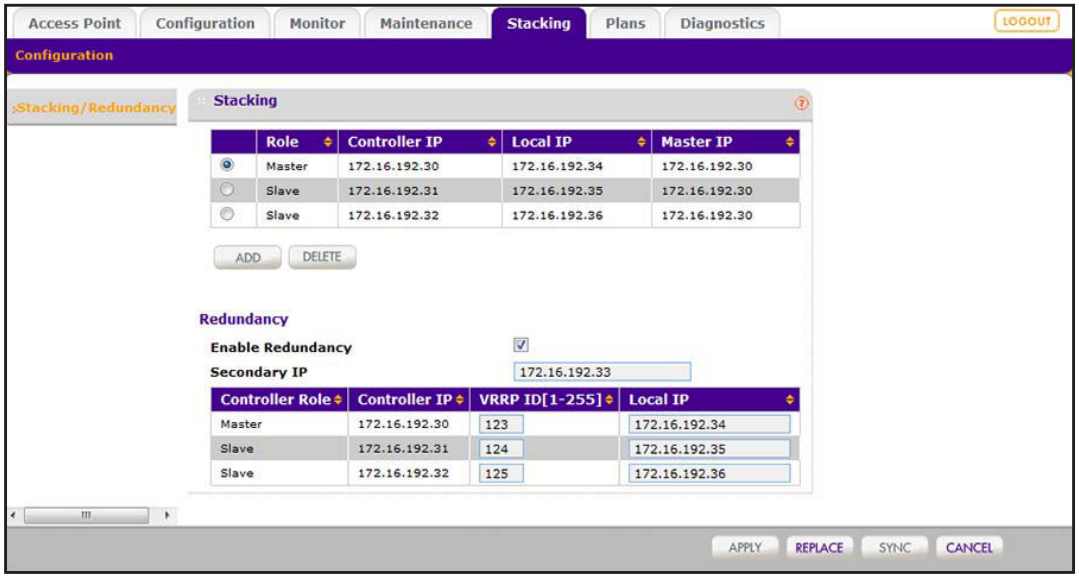
Setting	Description
Controller Role	This is a nonconfigurable field that shows that the role of the primary controller. The role is either master (for the master in the stack) or slave (for the slaves in the stack).
Controller IP	This is a nonconfigurable field that shows the IP address of the primary controller. This IP address is the address that you use to log in to the primary controller's (master's or slave's) web management interface and was established when you configured the stack (see *Configure a Stack of Wireless Controllers* on page 275). **Note:** The controller IP address of the master in the stack is also the master IP address for the redundancy configuration.
VRRP ID [1-255]	For each primary controller, enter a number from **1** through **255** as the VRRP ID. For each primary controller, this number must be unique and not assigned to any other device in the network.
Local IP	For each primary controller, enter a local IP address. If a failover occurs, this IP address remains assigned to the primary controller and does *not* transfer to the redundant controller to let you identify the primary controller before and after the failover. For each primary controller, you must enter an IP address that is not assigned to any other device.

WARNING:

Enabling redundancy causes the redundancy process on the primary wireless controller to restart, which might temporarily affects traffic on the managed access points in the network.

9. Click the **Apply** button.

   The changes are saved. After the configuration of the primary controller that functions as the master in the stack synchronizes with the redundant controller, redundancy goes into effect.

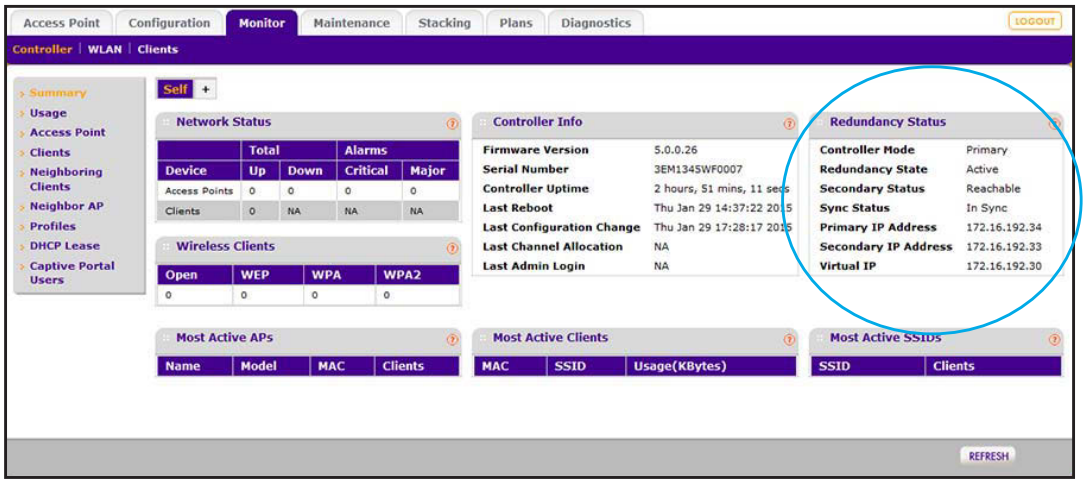


10. Select **Monitor > Controller > Summary**.

    The Summary page displays for the controller.

11. Click the **REFRESH** button.

    The Summary page displays the new redundancy information.



Replace a Redundant Controller

After you configure redundancy, you can replace the redundant controller with another one. Even if you change only the password of the redundant controller, use the replace tool.

➢ **To replace a redundant controller:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

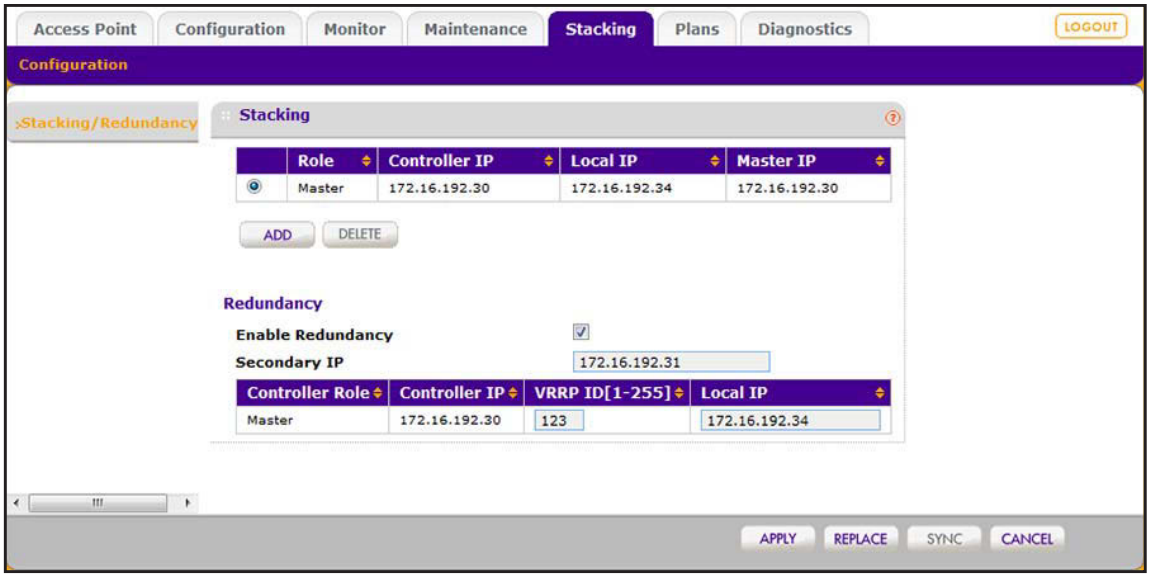
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

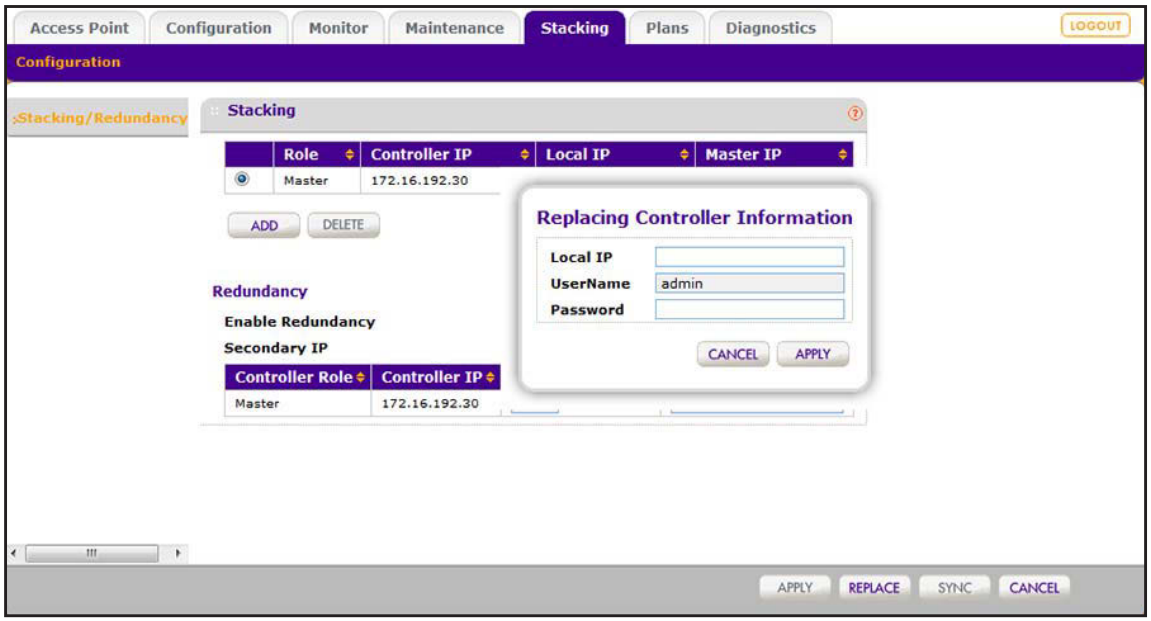
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.



5. Click the **Replace** button.



6. Configure the settings as described in the following table.

Setting	Description
Controller IP	Enter the IP address of the redundant controller. This is the address that you use to log in to the redundant controller's web management interface.
UserName	The user name is a nonconfigurable field that displays the user name with which you log in to the web management interface of the redundant controller. By default, the user name is admin.
Password	Enter the password with which you log in to the web management interface of the redundant controller. If you did not yet personalize the password, enter **password** for the password.

7. Click the **Apply** button.

   The changes are saved. The **Secondary IP** field displays the IP address of the redundant controller (that is, the secondary controller).

Remove a Redundancy Group

You can remove an existing redundancy group. In a 1:1 redundancy group, the primary controller is returned to a standalone configuration without redundancy. In a N:1 redundancy group, the primary controllers are returned to a stacked configuration without redundancy.

After you remove a redundant controller, reset the redundant controller to its factory default configuration before you use the controller in another configuration.

➢ **To remove a redundancy group:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

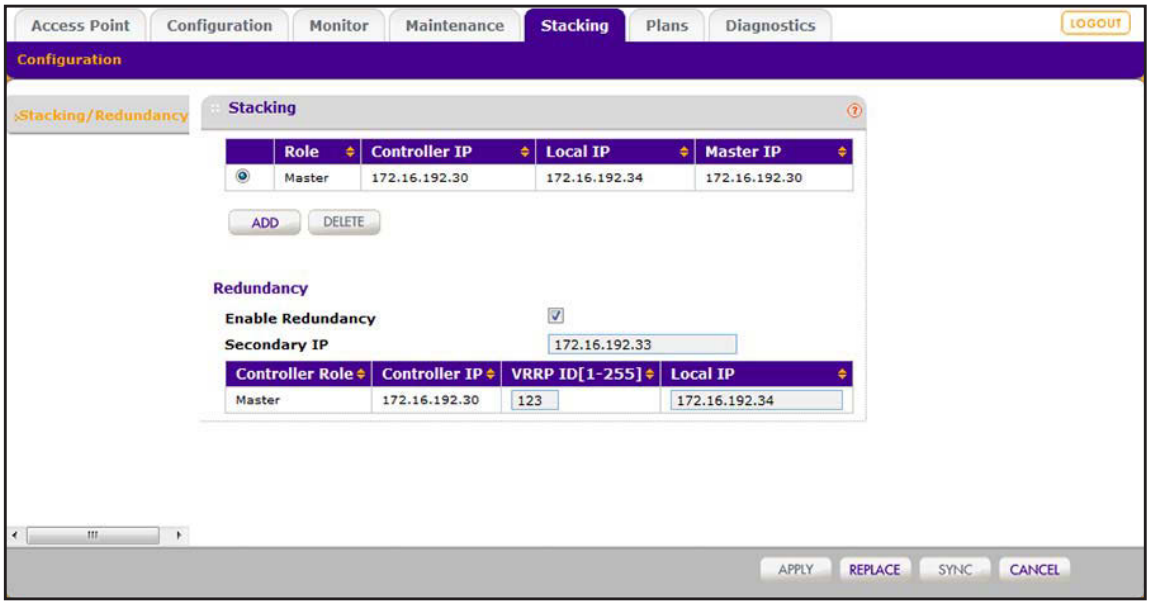
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Stacking**.



5. Clear the **Enable Redundancy** check box.
6. Click the **Apply** button.

   The changes are saved. Each controller in the redundancy group reboots. Redundancy is no longer provided.

Monitor the WiFi Network and Its Components

13

This chapter includes the following sections:

- *Monitor the Network*
- *Monitor the Wireless Controller*
- *Monitor the SSIDs on the Wireless Controller*
- *Monitor Local Clients in the Network*

Note: The information that is shown in the figures in this chapter is not always consistent. That is, the information in one figure might be for a different network configuration than the information in another figure.

Monitor the Network

Note: The **Network** configuration menu tab displays under the **Monitor** main navigation menu tab *only* if you configured stacking. If you did not configure stacking, see *Monitor the Wireless Controller* on page 316.

Note: Monitoring the network does not apply to the WC7500. For this model, see *Monitor the Wireless Controller* on page 316.

You can view a summary of the status of all wireless controllers *in the network* and their components and view individual components:

- **Summary**. See *View the Network Summary Page*.
- **Controllers**. *View the Wireless Controllers in the Network*.
- **Access Points**. See *View the Access Points in the Network*.
- **Clients**. See *View the Clients in the Network*.
- **Profiles**. See *View the Profiles in the Network*.

View the Network Summary Page

The wireless controller Summary page provides the status of the controller stack, the network status, and an overview of the rogue access points.

If you configured stacking and log in to the web management interface, the network Summary page displays. However, if you did not configure stacking, the wireless controller Summary page displays (see *View the Wireless Controller Summary Page* on page 316).

➢ **To view the network Summary page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

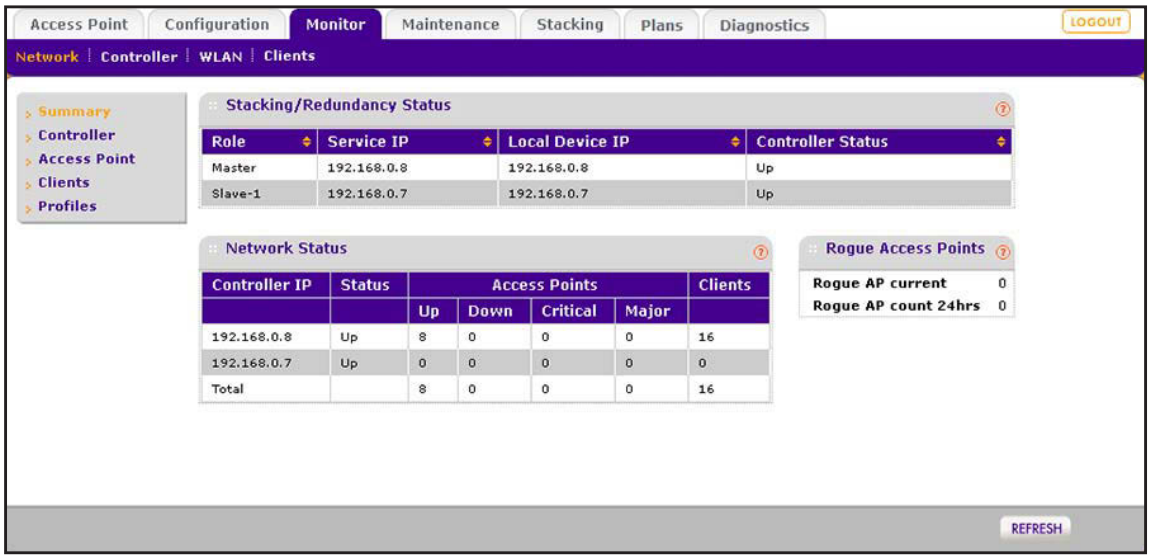
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Network > Summary**.



The following table describes the fields of the Stacking/Redundancy Status table, the Network Status table, and the Rogue Access Points section of the page.

Item	Description
Stacking/Redundancy Status	
Role	The role of the wireless controller in a stacking configuration (**Master** or **Slave**).
Service IP	The service IP address of the wireless controller. In a stacking configuration, the service IP address is identical to the local IP address.
Local Device IP	The local IP address of the wireless controller in the stacking group. This IP address remains constant. The role of the wireless controller (that is, master or slave) does not affect the local IP address.
Controller Status	The state of the wireless controller in the stack (**Up** or **Down**).
Network Status	
Controller IP	The IP address of each wireless controller in the network.
Status	The status of each wireless controller in the network (**Up** or **Down**).

Item		Description
Access Points	Up	The number of access points that a wireless controller manages and that are running correctly. This number is shown for each wireless controller in the stack and for all wireless controllers together.
	Down	The number of access points that a wireless controller manages but cannot ping. This number is shown for each wireless controller in the stack and for all wireless controllers together.
	Critical	The number of access points that a wireless controller manages and can ping, but either cannot log in to or for which the wireless controller detected that the access points are different from the ones that were configured. This number is shown for each wireless controller in the stack and for all wireless controllers together.
	Major	The number of access points that a wireless controller manages but for which the wireless controller detected that the configuration differs from the one that is in its own configuration. This situation can occur if an access point runs outdated firmware or the wireless controller changed the configuration while the access point was down or offline. This number is shown for each wireless controller in the stack and for all wireless controllers together.
Clients		The number of WiFi clients that each wireless controller in the stack manages, and the total number of WiFi clients that all wireless controllers in the stack manage.
Rogue Access Points		
Rogue AP current		The total number of unique rogue and unmanaged neighboring access points that are detected 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.

5. To sort the Stacking/Redundancy Status table, click the double triangle icon or single triangle icon at the top right of a column.
6. To display the latest information onscreen, click the **REFRESH** button.

View the Wireless Controllers in the Network

You can monitor the stacking configuration of the wireless controllers in the network.

➢ **To view the network Controllers page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

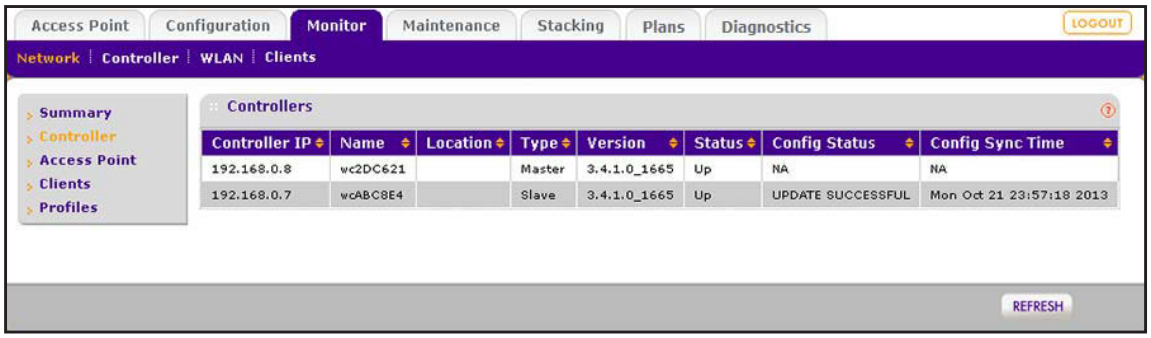
   The wireless controller's login window opens.

2. Enter your user name and password.

3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Network > Controller**.



   The following table explains the fields of the Controllers table on the network Controllers page.

Item	Description
Controller IP	The IP address of the wireless controller.
Name	The name of the wireless controller (see *Configure the General Settings* on page 99).
Location	The location of the wireless controller (see *Configure the General Settings* on page 99).
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**). **Note:** This field applies only for a wireless controller that functions as a slave.
Config Sync Time	The time that the wireless controller synchronized its firmware. **Note:** This field applies only for a wireless controller that functions as a slave.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To display the latest information onscreen, click the **REFRESH** button.

View the Access Points in the Network

You can monitor all managed access points in the network and see which wireless controller manages a particular access point.

➢ **To view the network Access Point page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

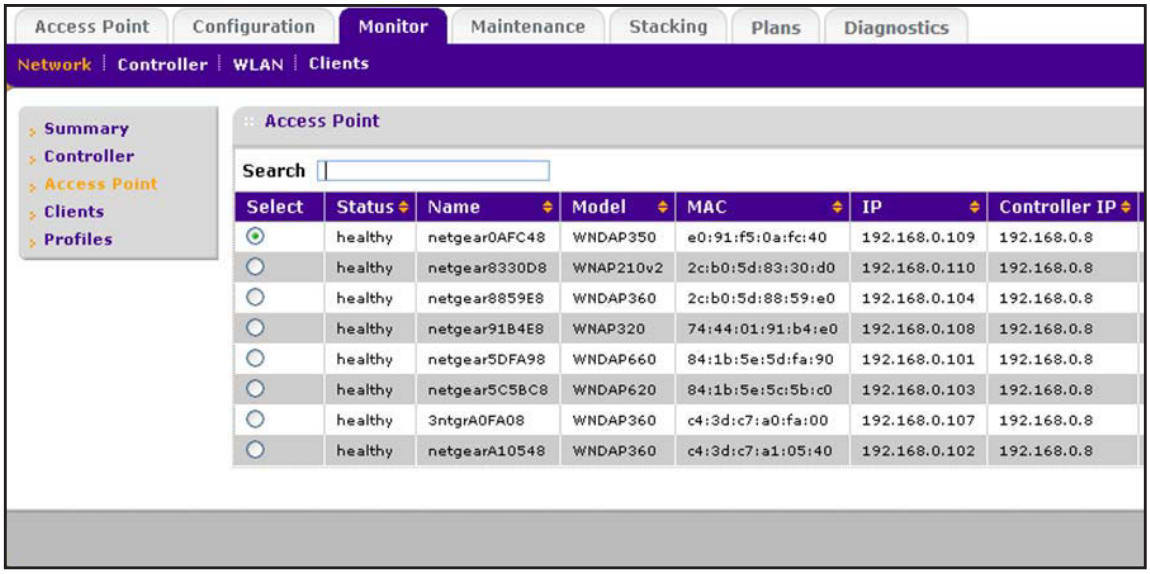
   The wireless controller's login window opens.

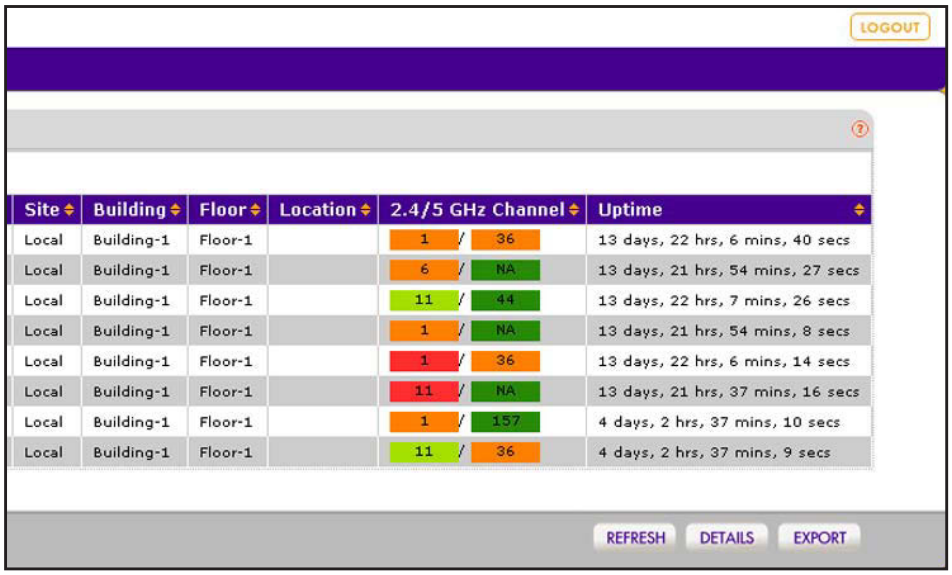
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Network > Access Point**.

   The Access Point page displays. Because this page is a wide page, it is shown in the following two figures.





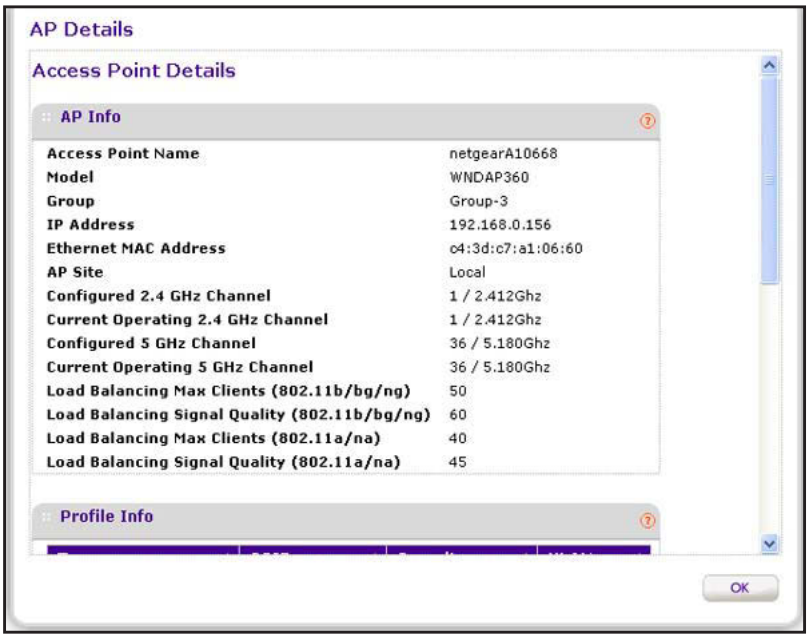
The following table describes the fields of the Access Point page.

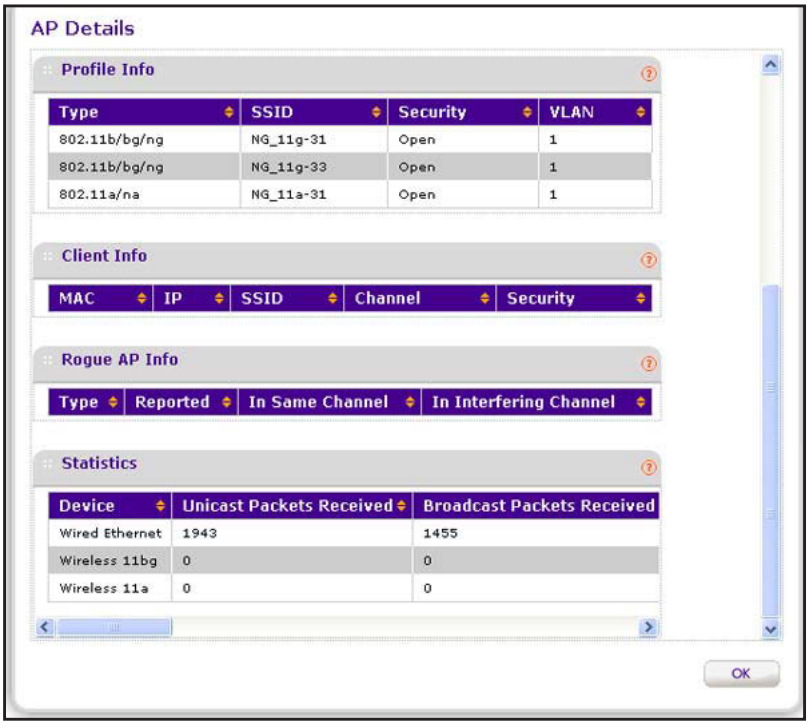
Item	Description
Select	The radio button that lets you select the access point.
Status	The status of the access point (**healthy** or **down**).
Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168).
Model	The model of the access point.
MAC	The MAC address of the access point.
IP	The IP address of the access point.
Controller IP	The IP address of the wireless controller that manages the access point.
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote. For more information about designating an access point as local or remote, see *Discover Access Points With the Discovery Wizard* on page 158.
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168).

Item	Description
2.4/5 GHz Channel	The active 2.4 GHz or 5 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation. The color coding specifies the channel utilization on each radio and means the following: • **Green**. 0–40 percent utilization. • **Light green**. 41–60 percent utilization. • **Orange**. 61–80 percent utilization. • **Red**. 81–100 percent utilization. • **NA**. The radio does not support the band.
Uptime	The period since the access point was last restarted.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.
10. To display details about an access point, do the following:
    a. Select the radio button that corresponds to the access point for which you want to see the details.
    b. Click the **Details** button.

       The AP Details pop-up window opens. Because this window is tall and you must scroll through it, the window is shown in the following two figures.





The following table describes the fields of the AP Details pop-up window.

Item	Description
AP Info	
This information is self-explanatory.	
Profile Info 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/ac**).
SSID	The WiFi 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.
Client Info The information that displays depends on the type and security of the connection between the client and the access point. For each WiFi client that is connected to the selected access point, some or all of the following information displays:	
MAC	The MAC address of the WiFi client.
IP	The IP address of the client.
Channel	The channel that the WiFi client is using to connect to the access point.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Rogue AP Info For all rogue and unmanaged neighboring access points combined that the selected managed access point detected, 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/ac**).
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.
Statistics	
For each type of usage (**Wired Ethernet**, **Wireless 11ng**, **Wireless 11bg**, **Wireless 11b**, **Wireless 11ac**, **Wireless 11na**, **Wireless 11a**, or a combination), statistics about transmitted and received packets and bytes display for the selected access point. The actual statistics are self-explanatory. **Note:** To see all fields of the table on the AP Details page, scroll to the right.	

11. Click the **OK** button.

    The AP Details pop-up window closes, and the network Access Point page displays again.

View the Clients in the Network

You can view all clients that are connected to managed access points and see which wireless controller manages a particular access point.

➢ **To view the Clients page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

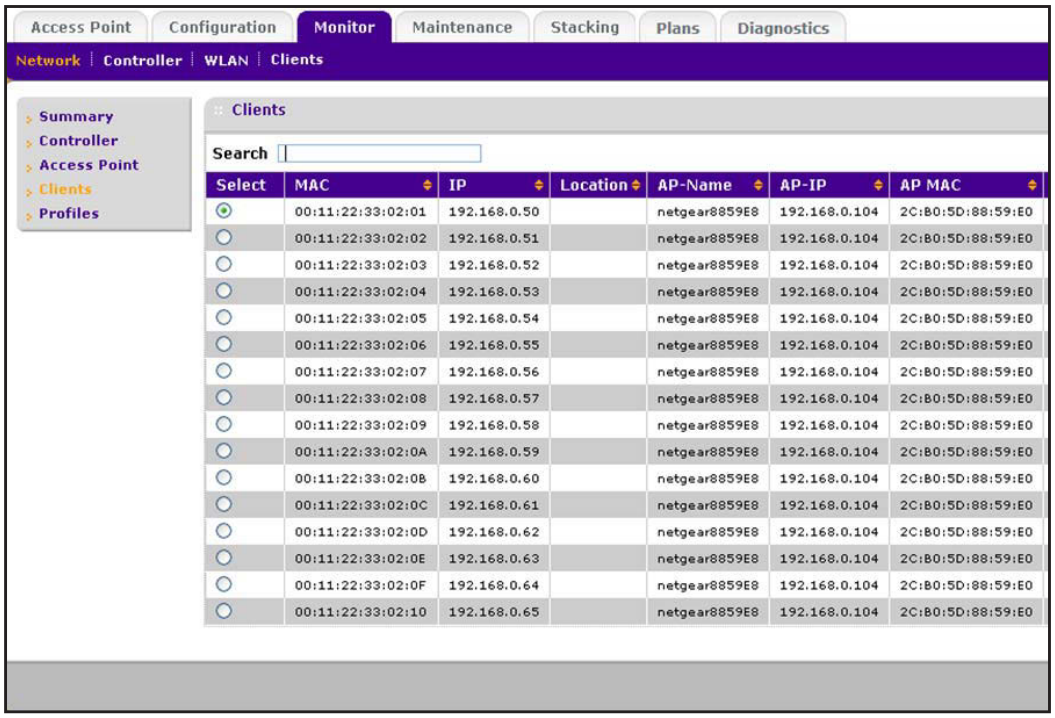
   The wireless controller's login window opens.

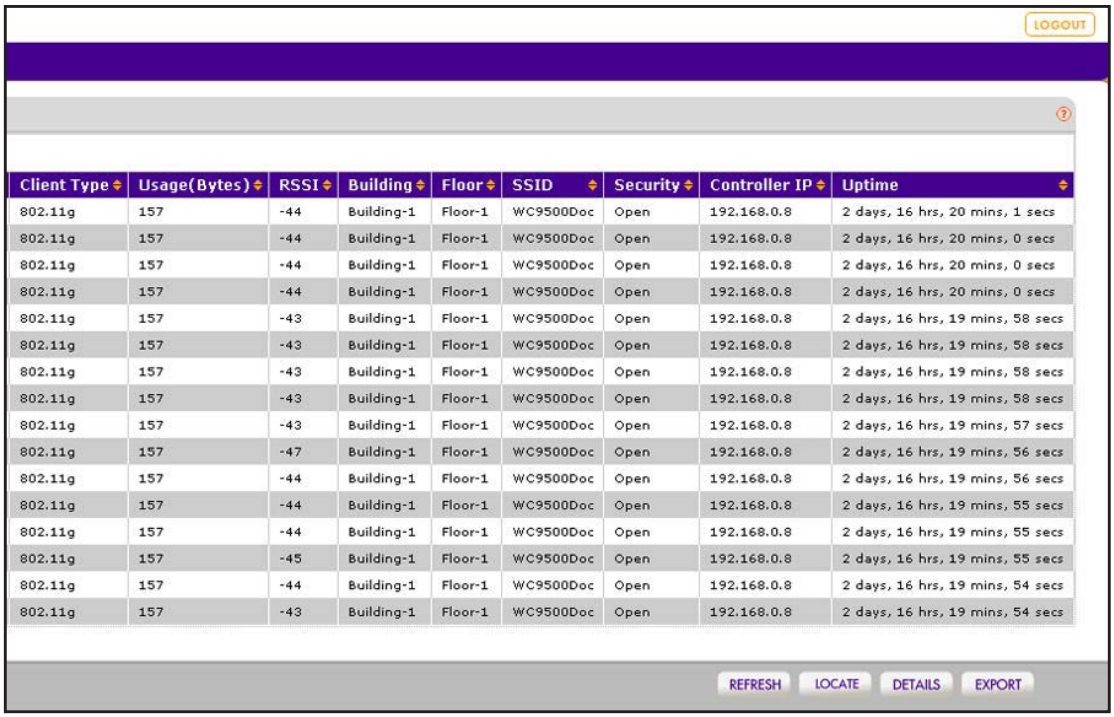
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Network > Clients**.

   The Clients page displays. Because this page is a wide page, it is shown in the following two figures.





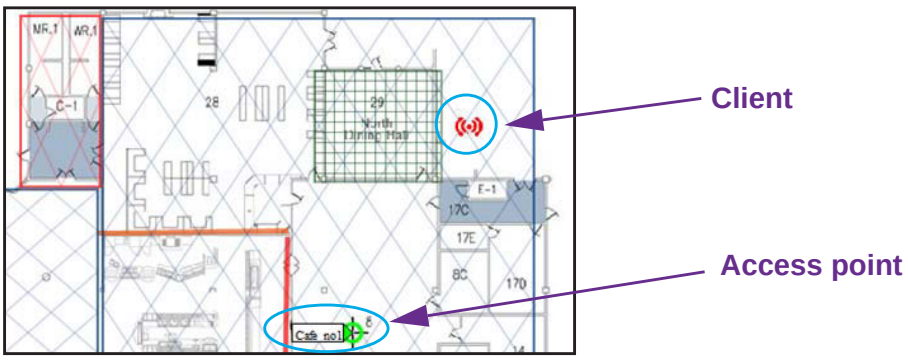
The following table describes the fields of the Clients page.

Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the WiFi client.
IP	The IP address of the WiFi client. Note the following: • If clients and the access point to which they are connected are in the same VLAN, all receive an IP address from the same DHCP server. • If clients and the access point to which they are connected are not in the same VLAN, you must provide a DHCP server for the client VLAN. • If clients are not connected to any DHCP server, IP addresses in the 169.254.x.x. range are assigned automatically.
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-IP	The IP address of the access point to which the WiFi client is connected.
AP-MAC	The MAC address of the access point to which the WiFi client is connected.
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).
Usage (KBytes)	The traffic usage of the WiFi client in KB.

Item	Description
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**) that the WiFi 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 WiFi client is connected.
Uptime	The period that the client is connected to the wireless controller.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To locate a client on a deployed floor plan, do the following:
   a. Select the radio button that corresponds to the client that you want to locate.
   b. Click the **Locate** button.

      The selected client displays on the floor plan and is indicated by a red icon.



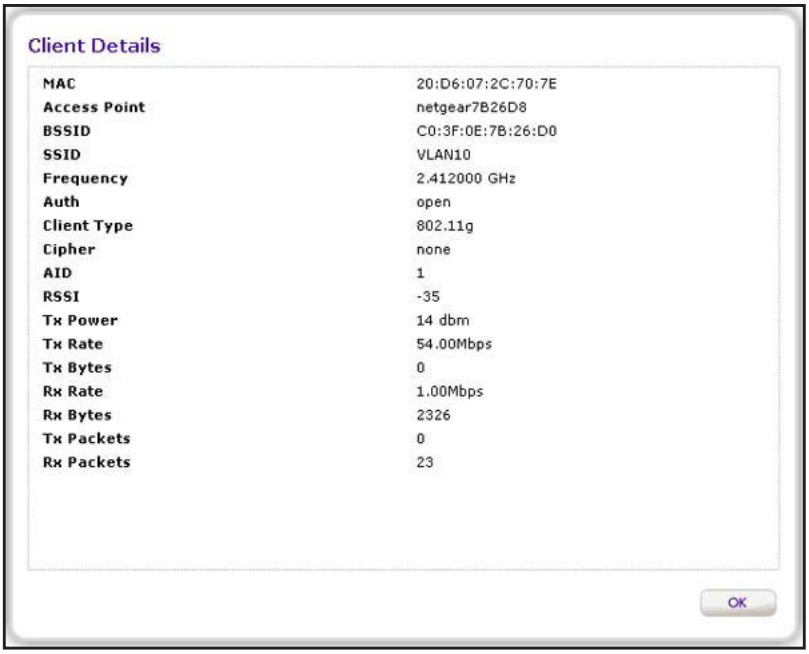
c. To display details about the client, point to the client.

   A pop-up window opens and displays details about the client.

d. To close the floor plan, click the **Back** button.

   The Clients page displays again.

10. To export the table, do the following:
    a. Click the **EXPORT** button.
    b. To save the file, follow the directions of your browser.
11. To display details about a client, do the following:
    a. Select the radio button that corresponds to the clients for which you want to see the details.
    b. Click the **Details** button.



The following table describes the fields of the Client Details pop-up window.

Item	Description
MAC	The MAC address of the WiFi client.
Access Point	The name of the access point to which the WiFi client is connected.
BSSID	The MAC address of the access point's radio to which the WiFi client is connected.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Frequency	The channel frequency that the WiFi client is using to connect to the access point.

Item	Description
Auth	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).
Cipher	The type of encryption that the WiFi client is using (**None**, **WEP**, **AES**, **TKIP**, or **TKIP + AES**).
AID	The association ID of the client.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Tx Power	The transmit power of the WiFi client.
Tx Rate	The transmit rate in Mbps of the WiFi client.
Tx Bytes	The number of bytes that the WiFi client transmitted.
Rx Rate	The receive rate in Mbps of the WiFi client.
Rx Bytes	The number of bytes that the WiFi client received.
Tx Packets	The number of packets that the WiFi client transmitted.
Rx Packets	The number of packets that the WiFi client received.

12. Click the **OK** button.

    The Client Details pop-up window closes, and the Clients page displays again.

View the Profiles in the Network

You can view all security profiles on the managed access points and see which wireless controller manages a particular access point.

➢ **To view the network Profiles page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

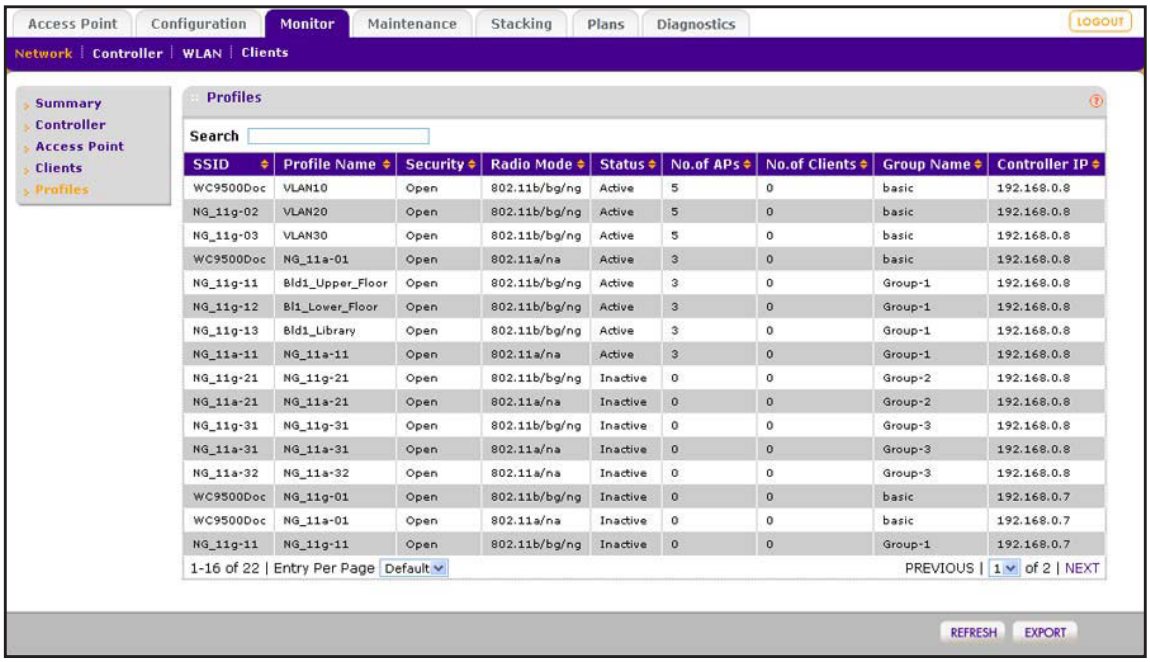
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Network > Profiles**.



The following table describes the fields of the Profiles page.

Item	Description
SSID	The WiFi network SSID for the security profile.
Profile Name	The name of 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/ac**).
Status	The status of the security profile (**Active** or **Inactive**).
No.of APs	The number of access points that are attached to the security profile.
No.of Clients	The number of clients that are attached (through the access points) to the security profile.
Group Name	The name of the group of which the security profile is a member.
Controller IP	The IP address of the wireless controller that manages the access point on which the profile is configured.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.

7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

Monitor the Wireless Controller

You can view a summary of the status of a wireless controller and its components and view individual components:

- **Summary**. See *View the Wireless Controller Summary Page*.
- **Usage**. See *View Wireless Controller Usage*.
- **Access Points**. See *View Access Points That the Wireless Controller Manages*.
- **Clients**. See *View Clients on Access Points That the Wireless Controller Manages*.
- **Neighboring Clients**. See *View Neighboring Clients That the Wireless Controller Detects*.
- **Neighboring APs**. See *View Neighboring Access Points That the Wireless Controller Does Not Manage*.
- **Profiles**. See *View Security Profiles That the Wireless Controller Manages*.
- **DHCP Lease**. See *View DHCP Leases That Are Provided by the Wireless Controller*.
- **Captive Portal Users**. See *View Captive Portal Users on Access Points That the Wireless Controller Manages*.
- **Guest Email List**. See *View the Guest Email Address Database for Access Points That the Wireless Controller Manages*.

View the Wireless Controller Summary Page

You can view an overview of the activity on the wireless controller.

When you log in to the web management interface, the wireless controller Summary page displays. However, if you configured stacking, the network Summary page displays (see *View the Network Summary Page* on page 301).

➢ **To view the wireless controller Summary page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

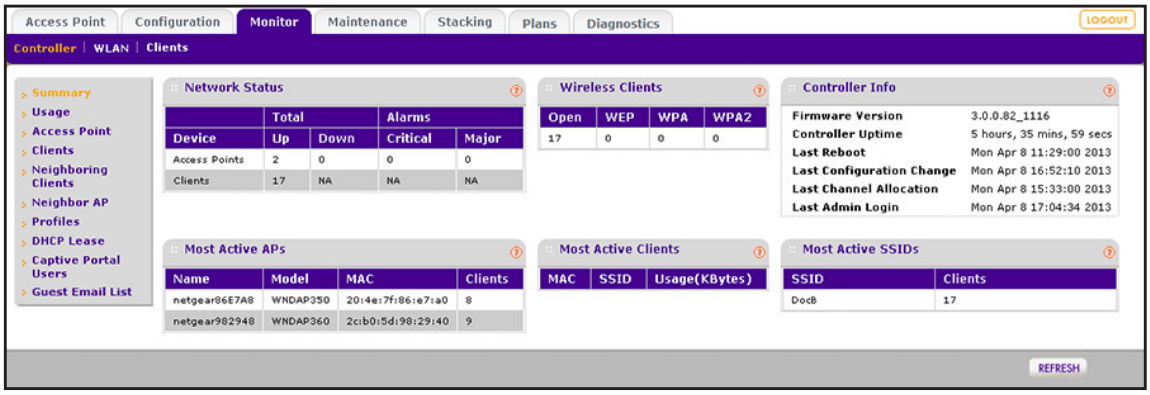
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Summary**.



The following table describes the fields of the Network Status, Wireless Clients, Most Active APs, Most Active Clients, and Most Active SSIDs tables of the page. The Controller Info section is self-explanatory.

Note: If you configure redundant controllers, the page also displays information about the status of the redundancy configuration. This information is self-explanatory.

Item		Description
Network Status		
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 detected that these devices 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.

Item	Description
Wireless Clients	
Open	The number of WiFi clients that are connected to managed access points using security profiles configured with open mode.
WEP	The number of WiFi clients that are connected to managed access points using security profiles configured with WEP.
WPA	The number of WiFi clients that are connected to managed access points using security profiles configured with WPA.
WPA2	The number of WiFi clients that are connected to managed access points using security profiles configured with WPA2.
Most Active APs For the most active access points, the following information displays:	
Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168).
Model	The model of the access point.
MAC	The MAC address of the access point.
Clients	The number of clients that are associated with the access point.
Most Active Clients For the most active clients, the following information displays:	
MAC	The MAC address of the WiFi client.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Usage (KBytes)	The traffic usage of the WiFi client in KB.
Most Active SSIDs For the most active SSIDs, the following information displays:	
SSID	The name of the WiFi network SSID.
Clients	The number of clients that are using the SSID.

5. To sort a table, click the double triangle icon or single triangle icon at the top right of a column.
6. To display the latest information onscreen, click the **REFRESH** button.

View Wireless Controller Usage

The page displays graphics that show the access point usage, SSID usage, and number of clients on the wireless controller.

Note: The Java plug-in is required to display the graphics.

➢ **To view the Usage page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Usage**.

Data for the 2.4 GHz network (for the combined 802.11b, 802.11bg, and 802.11ng modes) is shown in purple; data for the 5 GHz network (for the combined 802.11a, 802.11na, and 802.11ac modes) is shown in green. The page shows the following graphs:

- **AP Usage**. Displays the 2.4 GHz and 5 GHz traffic usage in MB for access points.
- **SSID Usage**. Displays the 2.4 GHz and 5 GHz traffic usage in MB for SSIDs.
- **Number of Clients**. Displays the total number of clients, number of clients in the 2.4 GHz network, and number of clients in the 5 GHz network over a period.

5. To display the latest information onscreen, click the **REFRESH** button.

View Access Points That the Wireless Controller Manages

You can monitor all access points that the wireless controller manages.

➢ **To view the Access Point page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

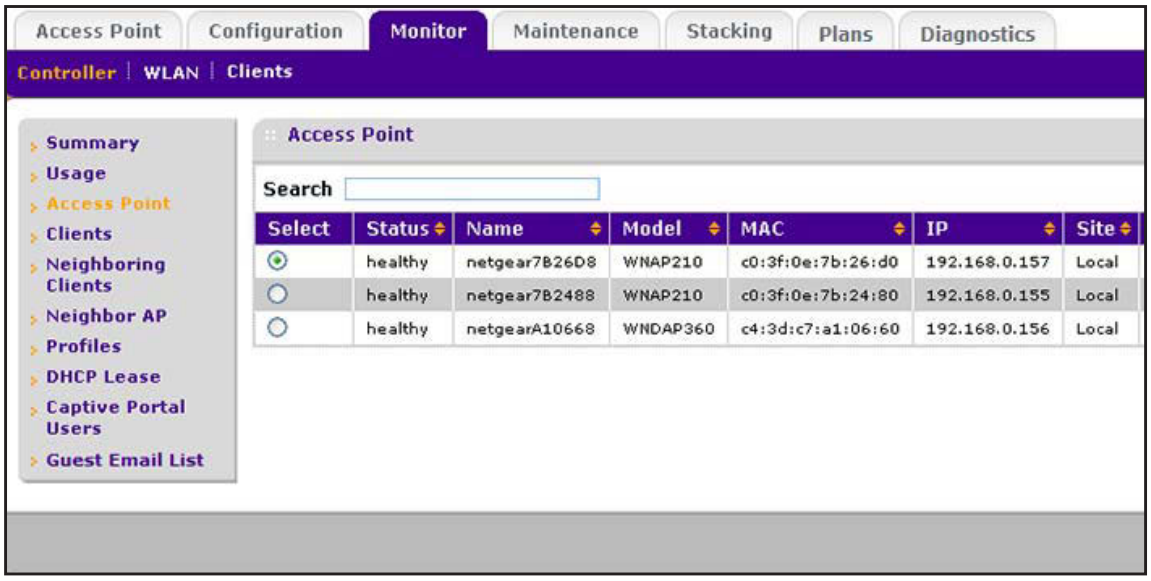
   The wireless controller's login window opens.

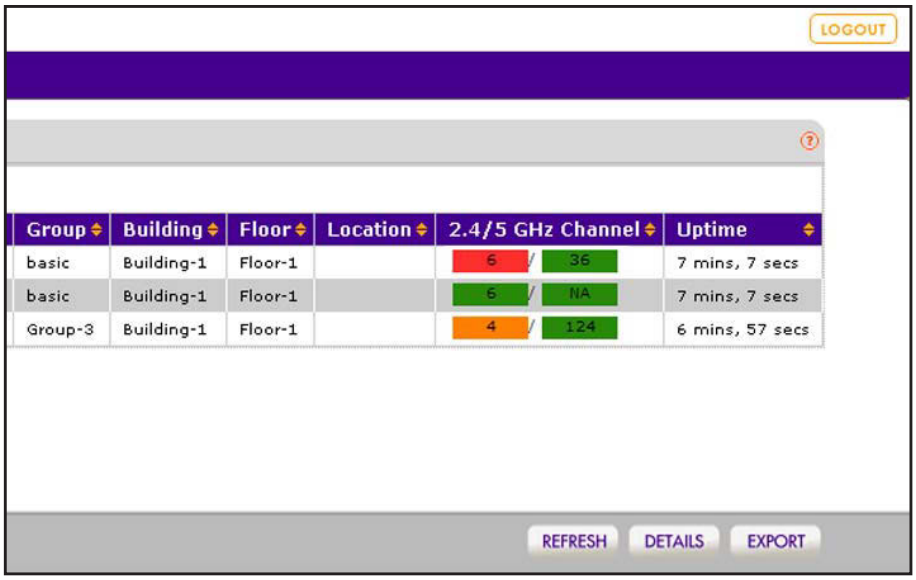
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Access Point**.

   The Access Point page displays. Because this page is a wide page, it is shown in the following two figures.





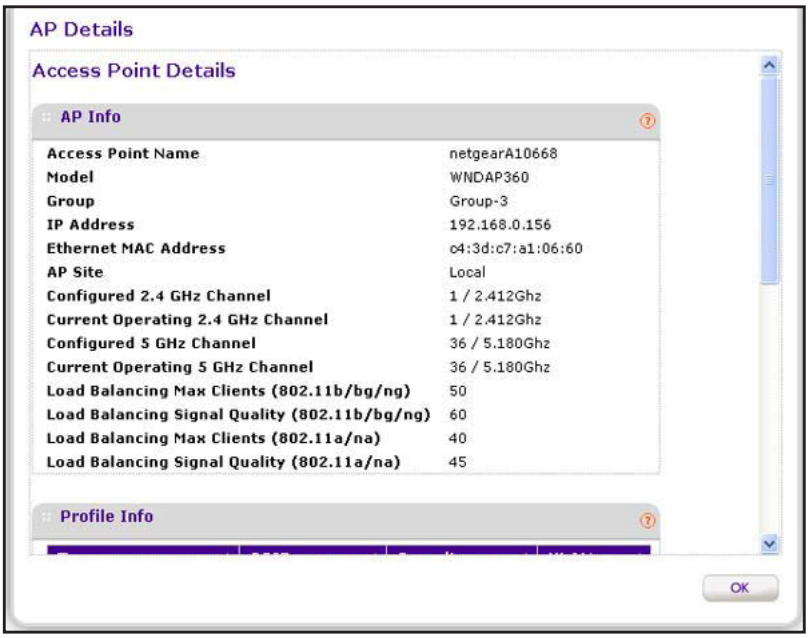
The following table describes the fields of the Access Point page.

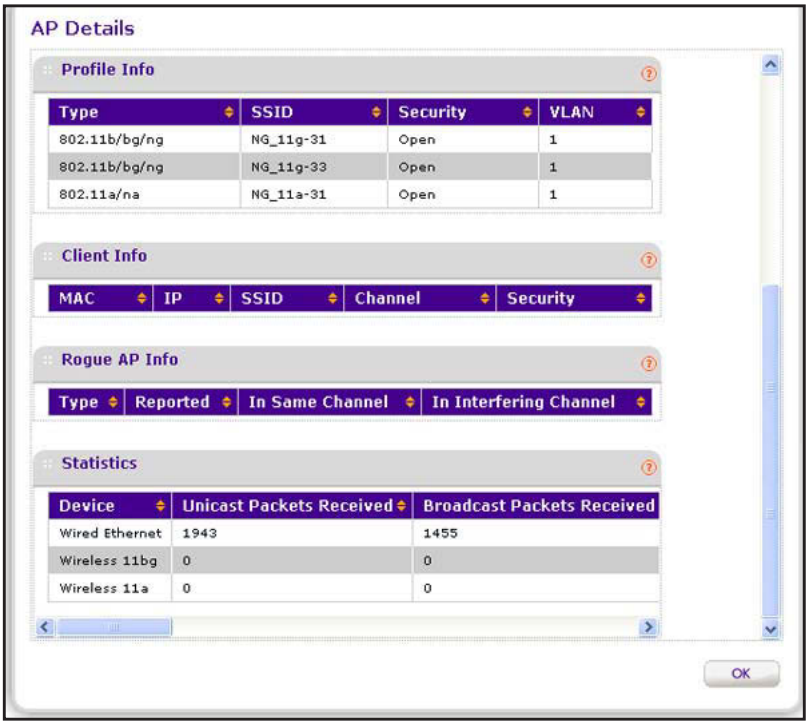
Item	Description
Select	The radio button that lets you select the access point.
Status	The status of the access point (**healthy** or **down**).
Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168).
Model	The model of the access point.
MAC	The MAC address of the access point.
IP	The IP address of the access point.
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote. For more information about designating an access point as local or remote, see *Discover Access Points With the Discovery Wizard* on page 158.
Group	The profile group to which the access point is assigned (see *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168).

Item	Description
2.4/5 GHz Channel	The active 2.4 GHz or 5 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation. The color coding specifies the channel utilization on each radio and means the following: • **Green**. 0–40 percent utilization. • **Light green**. 41–60 percent utilization. • **Orange**. 61–80 percent utilization. • **Red**. 81–100 percent utilization. • **NA**. The radio does not support the band.
Uptime	The period since the access point was last restarted.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.
10. To display details about an access point, do the following:
    a. Select the radio button that corresponds to the access point for which you want to see the details.
    b. Click the **Details** button.

       The AP Details pop-up window opens. Because this window is tall and you must scroll through it, the window is shown in the following two figures.





The following table describes the fields of the AP Details pop-up window.

Item	Description
AP Info	
This information is self-explanatory.	

Item	Description
Profile Info 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/ac**).
SSID	The WiFi 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.
Client Info The information that displays depends on the type and security of the connection between the client and the access point. For each WiFi client that is connected to the selected access point, some or all of the following information displays:	
MAC	The MAC address of the WiFi client.
IP	The IP address of the client.
Channel	The channel that the WiFi client is using to connect to the access point.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Rogue AP Info For all rogue and unmanaged neighboring access points combined that the selected managed access point detected, 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/ac**).
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.
Statistics	
For each type of usage (**Wired Ethernet**, **Wireless 11ng**, **Wireless 11bg**, **Wireless 11b**, **Wireless 11ac**, **Wireless 11na**, **Wireless 11a**, or a combination), statistics about transmitted and received packets and bytes display for the selected access point. The actual statistics are self-explanatory. **Note:** To see all fields of the table on the AP Details page, scroll to the right.	

11. Click the **OK** button.

    The AP Details pop-up window closes, and the Access Point page displays again.

View Clients on Access Points That the Wireless Controller Manages

You can view all clients that are connected to access points that the wireless controller manages.

➢ **To view the Clients page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

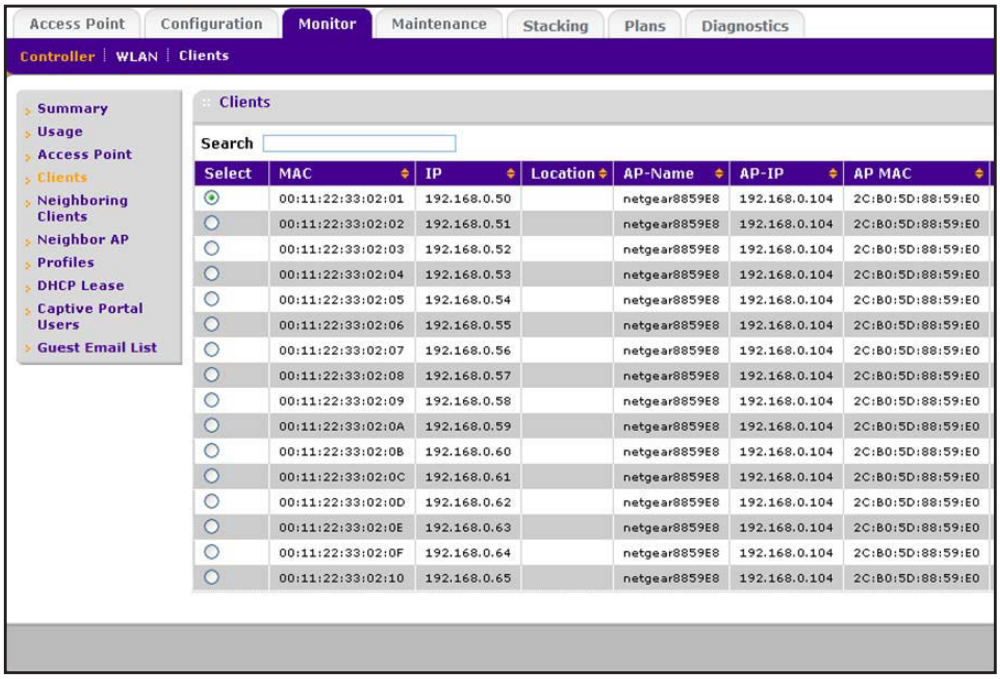
   The wireless controller's login window opens.

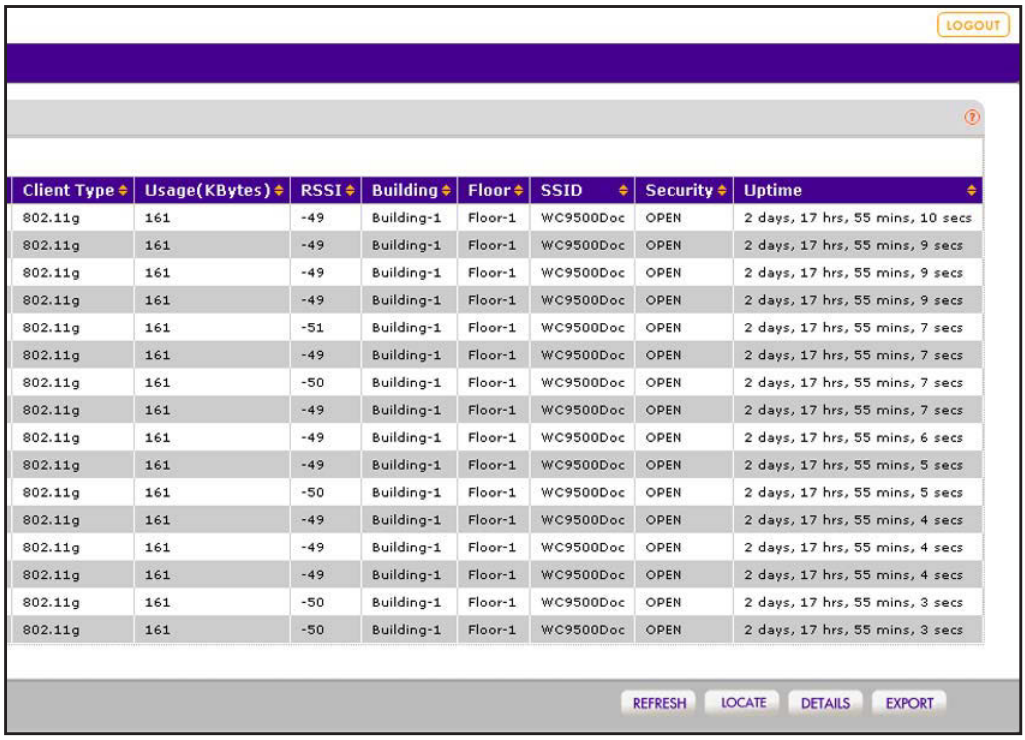
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Clients**.

   The Clients page displays. Because this page is a wide page, it is shown in the following two figures.



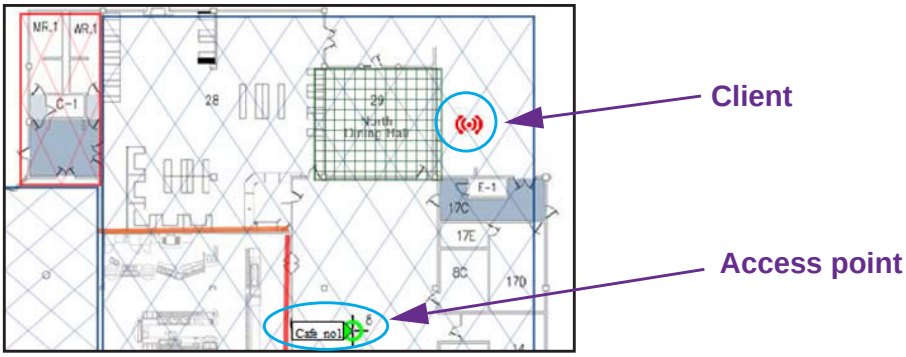


The following table describes the fields of the Clients page.

Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the WiFi client.
IP	The IP address of the WiFi client. Note the following: • If clients and the access point to which they are connected are in the same VLAN, all receive an IP address from the same DHCP server. • If clients and the access point to which they are connected are not in the same VLAN, you must provide a DHCP server for the client VLAN. • If clients are not connected to any DHCP server, IP addresses in the 169.254.x.x. range are assigned automatically.
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-IP	The IP address of the access point to which the WiFi client is connected.
AP-MAC	The MAC address of the access point to which the WiFi client is connected.
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).

Item	Description
Usage (KBytes)	The traffic usage of the WiFi client in KB.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**) that the WiFi client is using to connect to the access point.
Uptime	The period that the client is connected to the wireless controller.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To locate a client on a deployed floor plan, do the following:
   a. Select the radio button that corresponds to the client that you want to locate.
   b. Click the **Locate** button.
      The selected client displays on the floor plan and is indicated by a red icon.



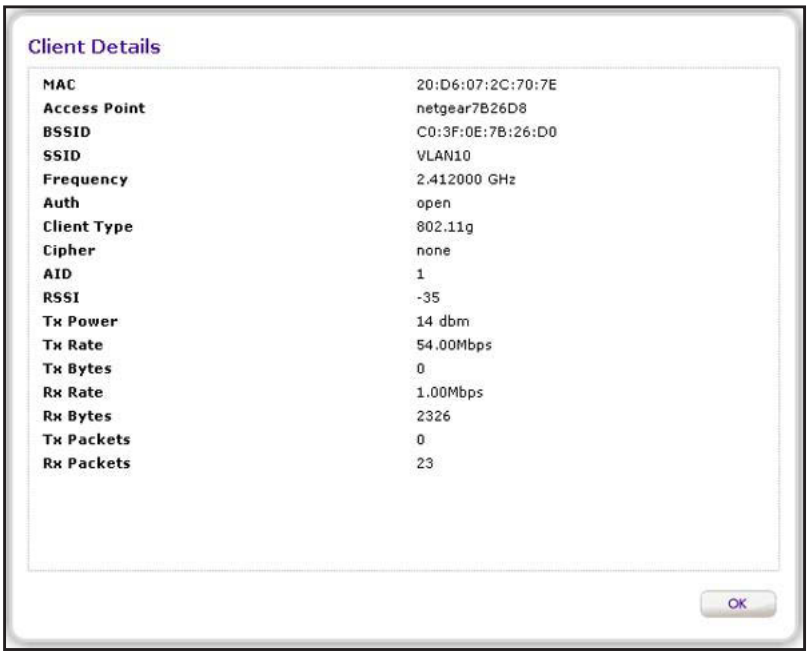
   c. To display details about the client, point to the client.

A pop-up window opens and displays details about the client.

d. To close the floor plan, click the **Back** button.

The Clients page displays again.

10. To export the table, do the following:
    a. Click the **EXPORT** button.
    b. To save the file, follow the directions of your browser.
11. To display details about a client, do the following:
    a. Select the radio button that corresponds to the clients for which you want to see the details.
    b. Click the **Details** button.



The following table describes the fields of the Client Details pop-up window.

Item	Description
MAC	The MAC address of the WiFi client.
Access Point	The name of the access point to which the WiFi client is connected.
BSSID	The MAC address of the access point's radio to which the WiFi client is connected.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Frequency	The channel frequency that the WiFi client is using to connect to the access point.

Item	Description
Auth	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).
Cipher	The type of encryption that the WiFi client is using (**None**, **WEP**, **AES**, **TKIP**, or **TKIP + AES**).
AID	The association ID of the client.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Tx Power	The transmit power of the WiFi client.
Tx Rate	The transmit rate in Mbps of the WiFi client.
Tx Bytes	The number of bytes that the WiFi client transmitted.
Rx Rate	The receive rate in Mbps of the WiFi client.
Rx Bytes	The number of bytes that the WiFi client received.
Tx Packets	The number of packets that the WiFi client transmitted.
Rx Packets	The number of packets that the WiFi client received.

12. Click the **OK** button.

    The Client Details pop-up window closes, and the Clients page displays again.

View Neighboring Clients That the Wireless Controller Detects

You can monitor clients that the wireless controller detects and that are attached to known or rogue access points.

➢ **To view the Neighboring Clients page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

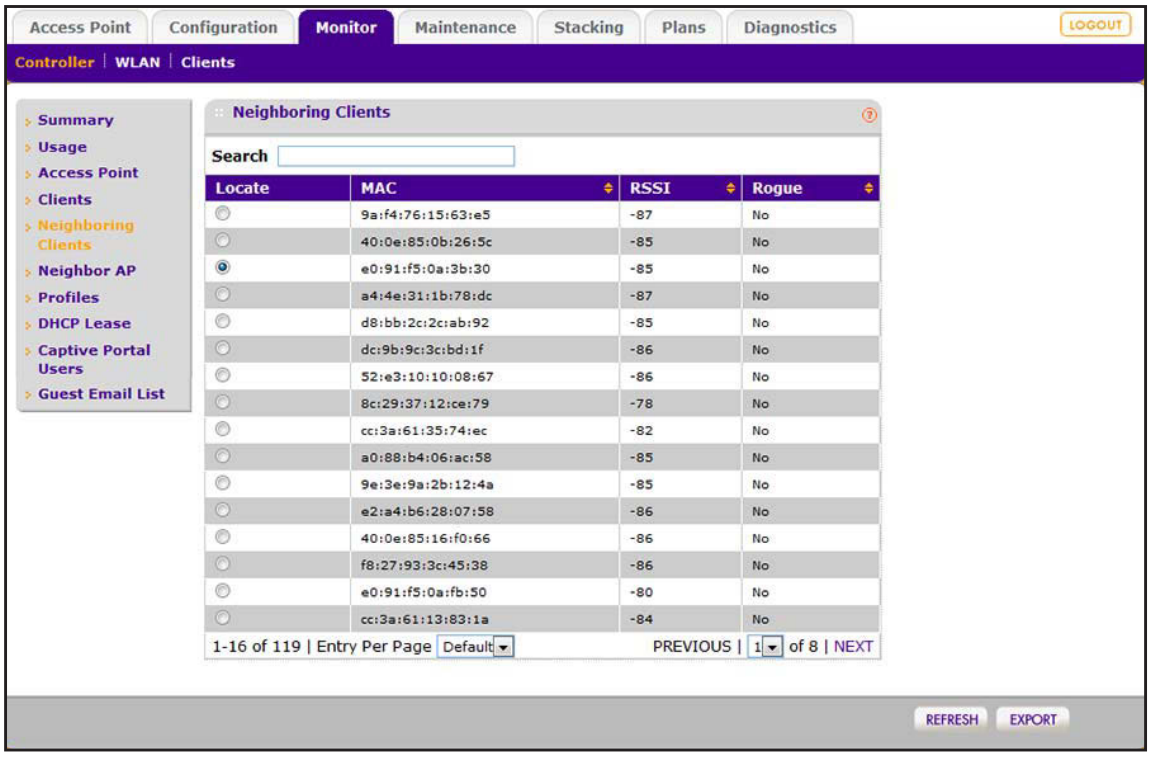
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Neighboring Clients**.



The following table describes the fields of the Neighboring Clients page.

Item	Description
Location	This radio button is nonfunctional.
MAC	The MAC address of the neighboring client.
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.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.

9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

View Neighboring Access Points That the Wireless Controller Does Not Manage

You can monitor the access points that the wireless controller detects but does not manage.

➢ **To view the Rogue AP page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

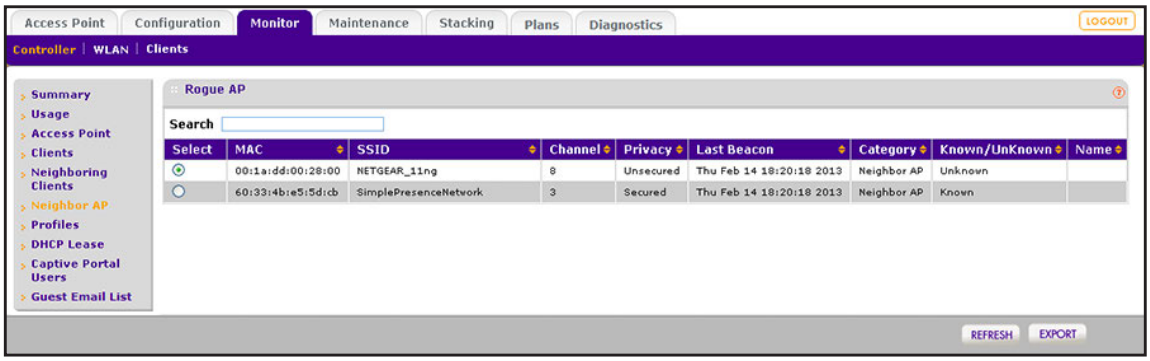
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Neighbor AP**.



The following table describes the fields of the Rogue AP page.

Item	Description
Select	The radio button that lets you select the access point.
MAC	The MAC address of the rogue access point.
SSID	The WiFi network SSID that the rogue access point is using.
Channel	The channel that the access point is using.
Privacy	The security of the access point (**Secured** or **Unsecured**).
Last Beacon	The last beacon that the access point transmitted.

Item	Description
Type	The category that the access point belongs to (**Neighbor AP** or **Rogue AP**).
Classification	The status of the access point (**Known** or **Unknown**).
Name	The name of the access point, if a name is assigned.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**
8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

View Security Profiles That the Wireless Controller Manages

You can monitor all security profiles on the access points that the wireless controller manages.

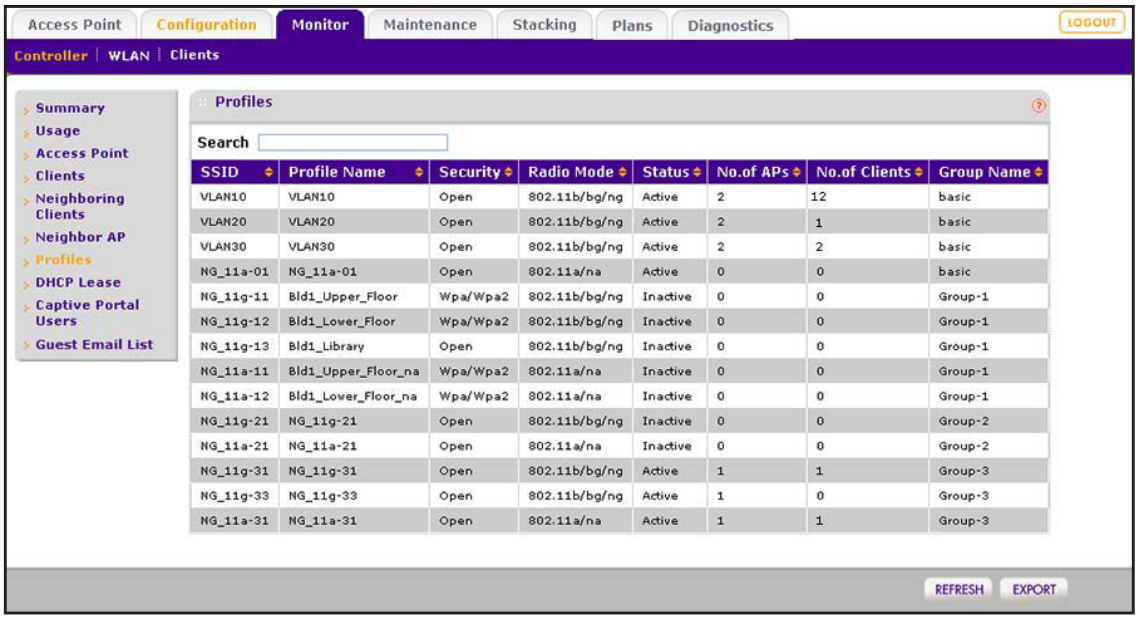
➢ **To view the Profiles page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Monitor > Controller > Profiles**.



The following table describes the fields of the Profiles page.

Item	Description
SSID	The WiFi network SSID for the security profile.
Profile Name	The name of 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/ac**).
Status	The status of the security profile (**Active** or **Inactive**).
No.of APs	The number of access points that are attached to the security profile.
No.of Clients	The number of clients that are attached (through the access points) to the security profile.
Group Name	The name of the group of which the security profile is a member.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.

8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

View DHCP Leases That Are Provided by the Wireless Controller

You can view the current DHCP clients that were allocated IP addresses by the DHCP server on the wireless controller.

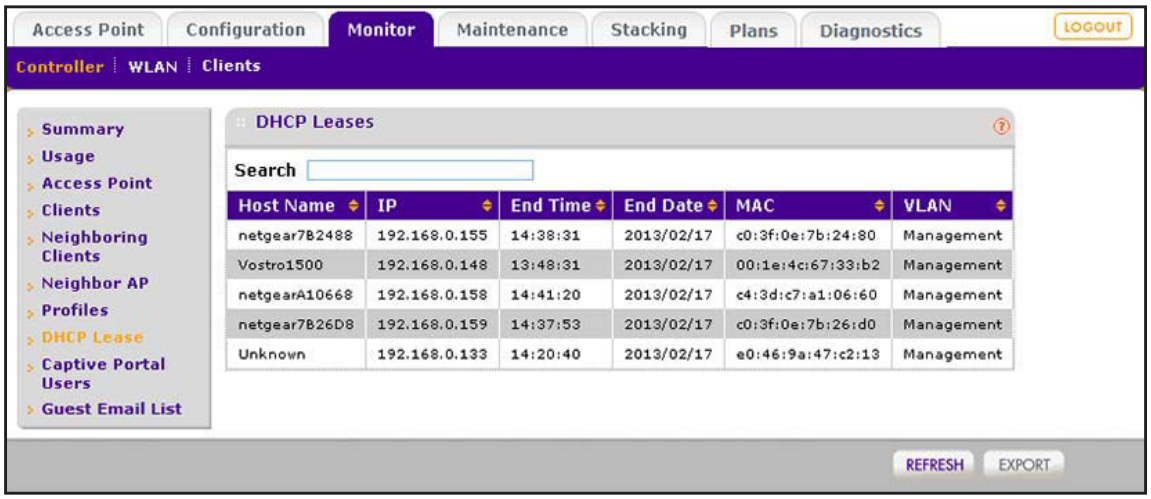
➢ **To view the DHCP Leases page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Monitor > Controller > DHCP Lease**.



The following table describes the fields of the DHCP Leases page.

Item	Description
Host Name	The host name of the DHCP client.
IP	The IP address that is allocated to the DHCP client.

Item	Description
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 name or number that the DHCP server and DHCP client are using to connect.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To export the table, do the following, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

View Captive Portal Users on Access Points That the Wireless Controller Manages

You can view the current guests and users that are logged in to a captive portal on the access points that the wireless controller manages.

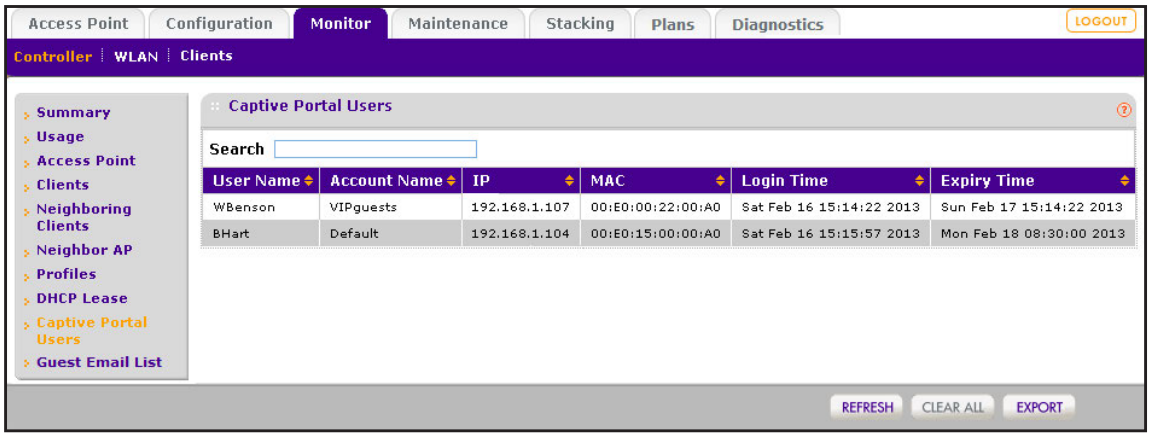
➢ **To view the Captive Portal Users page:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Monitor > Controller > Captive Portal Users**.



The following table describes the fields of the Captive Portal Users page.

Item	Description
User Name	The login name of the user.
Account Name	The account name, if any, that is associated with the user.
IP	The IP address of the user.
MAC	The MAC address of the device with which the user is logged in.
Login Time	The time that the user logged in.
Expiry Time	The time when the login access expires.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To clear all information from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the information before you clear the information.
10. To export the table, do the following:
    a. Click the **EXPORT** button.
    b. To save the file, follow the directions of your browser.

View the Guest Email Address Database for Access Points That the Wireless Controller Manages

You can view the email addresses of users who are or were logged in through a guest portal. The email address database can contain a maximum of 12,000 entries.

➢ **To view the guest email address database:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

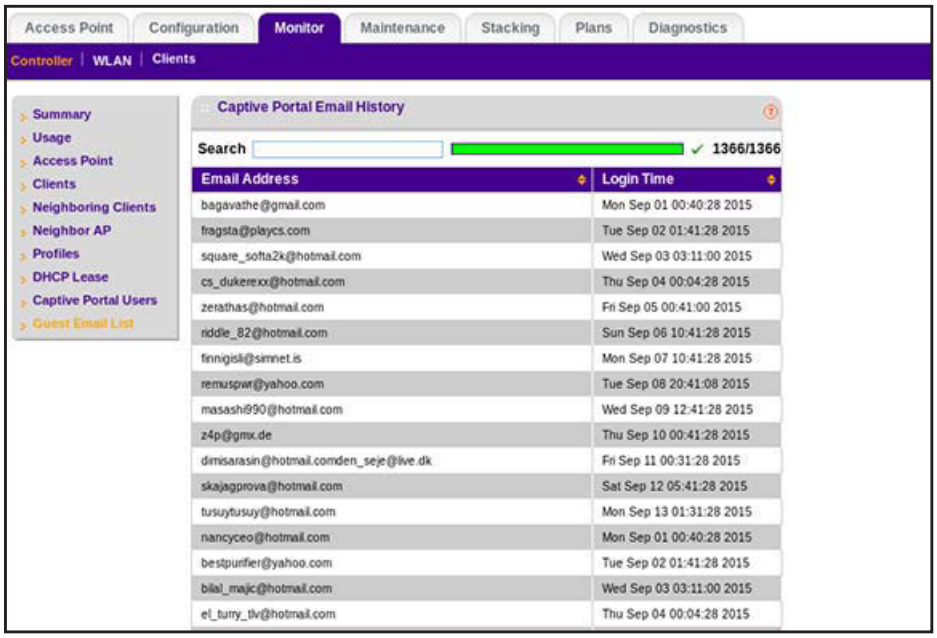
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Controller > Guest Email List**.

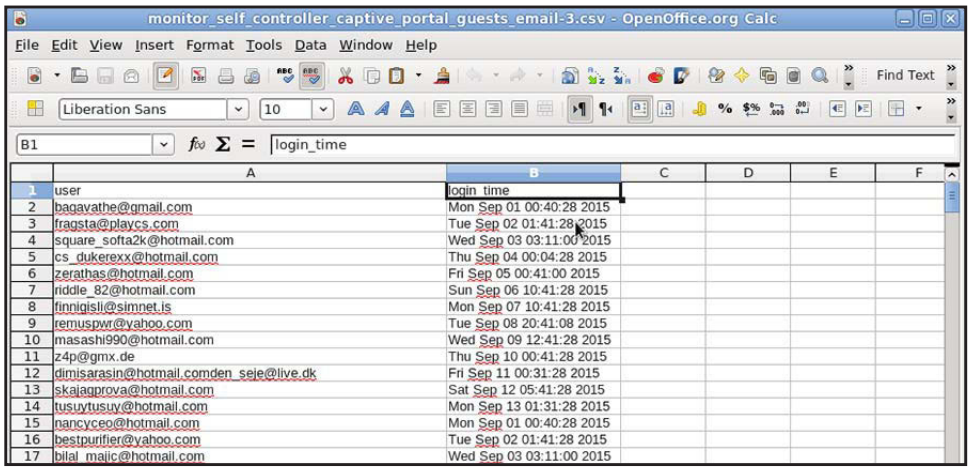


   The table shows the user email addresses and the date and time that the user logged in.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.

7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.
9. To clear all information from the page and from memory, click the **CLEAR ALL** button.

   We recommend that you save the information before you clear the information.
10. To export the table, do the following:
    a. Click the **EXPORT** button.



	A	B	C	D	E	F
1	user	login_time				
2	bagavathe@gmail.com	Mon Sep 01 00:40:28 2015				
3	fragsta@playcs.com	Tue Sep 02 01:41:28 2015				
4	square_softa2k@hotmail.com	Wed Sep 03 03:11:00 2015				
5	cs_dukerexx@hotmail.com	Thu Sep 04 00:04:28 2015				
6	zerathas@hotmail.com	Fri Sep 05 00:41:00 2015				
7	riddle_82@hotmail.com	Sun Sep 06 10:41:28 2015				
8	finnigisli@simnet.is	Mon Sep 07 10:41:28 2015				
9	remuspwr@yahoo.com	Tue Sep 08 20:41:08 2015				
10	masashi990@hotmail.com	Wed Sep 09 12:41:28 2015				
11	z4p@gmx.de	Thu Sep 10 00:41:28 2015				
12	dimisarasin@hotmail.comden_seje@live.dk	Fri Sep 11 00:31:28 2015				
13	skajaqprova@hotmail.com	Sat Sep 12 05:41:28 2015				
14	tusuytusuy@hotmail.com	Mon Sep 13 01:31:28 2015				
15	nancyceo@hotmail.com	Mon Sep 01 00:40:28 2015				
16	bestpurifier@yahoo.com	Tue Sep 02 01:41:28 2015				
17	bilal_majic@hotmail.com	Wed Sep 03 03:11:00 2015				

    b. To save the file, follow the directions of your browser.

Monitor the SSIDs on the Wireless Controller

You can monitor all access points that function in an SSID.

➢ **To monitor an active SSID in the network:**

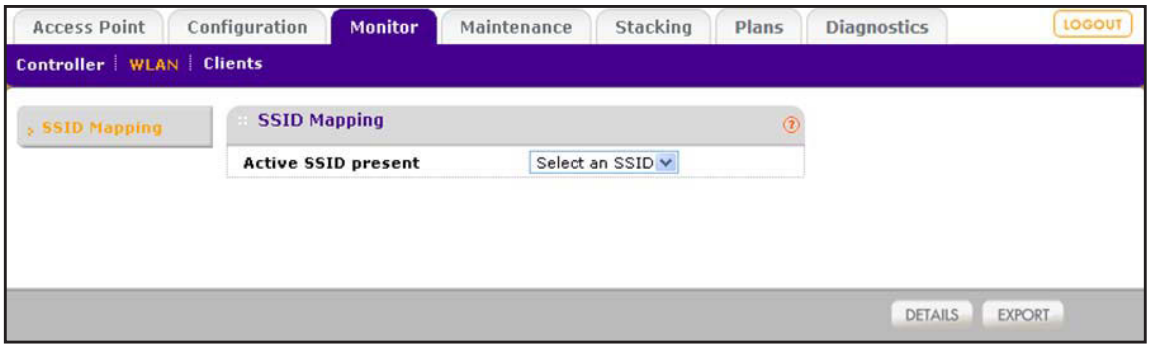
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

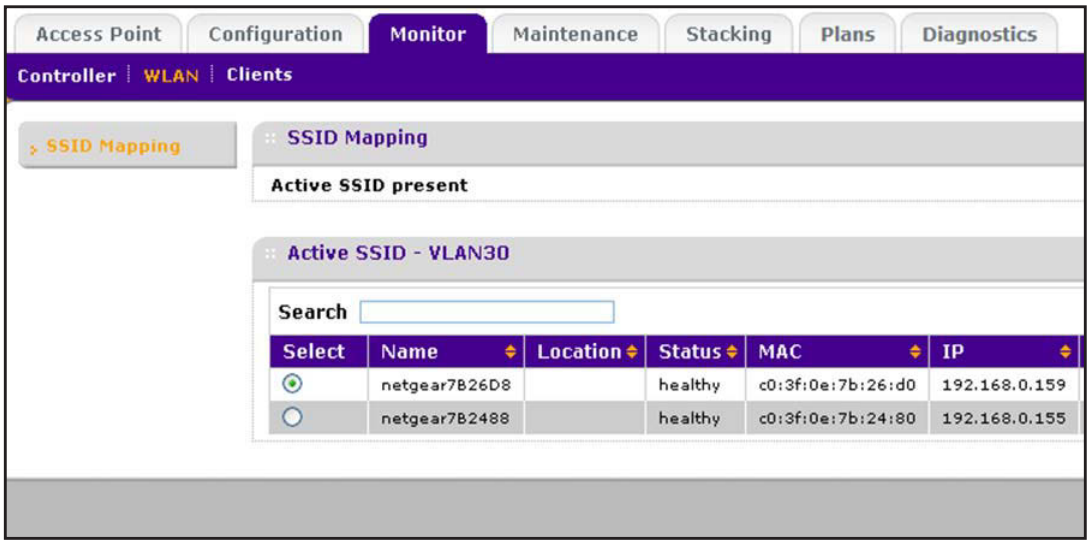
   The wireless controller's web management interface opens and displays the Summary page.

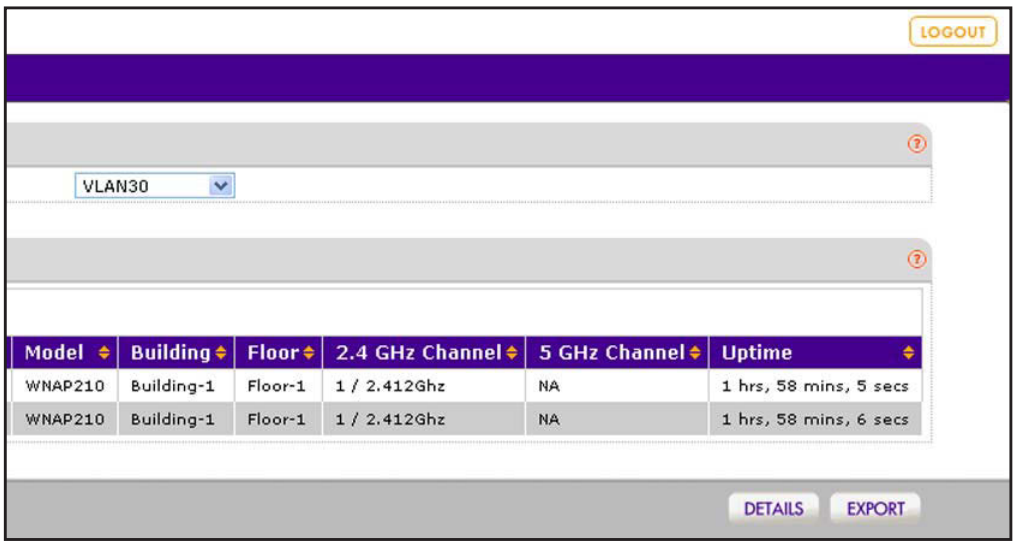
4. Select **Monitor > WLAN**.



5. From the **Active SSID** present menu, select an SSID.

   The Active SSID table for the selected SSID displays. Because this page is a wide page, it is shown in the following two figures.





The following table describes the fields of the SSID Mapping page.

Item	Description
Select	The radio button that lets you select the access point.
Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168).
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168).
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.
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
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.

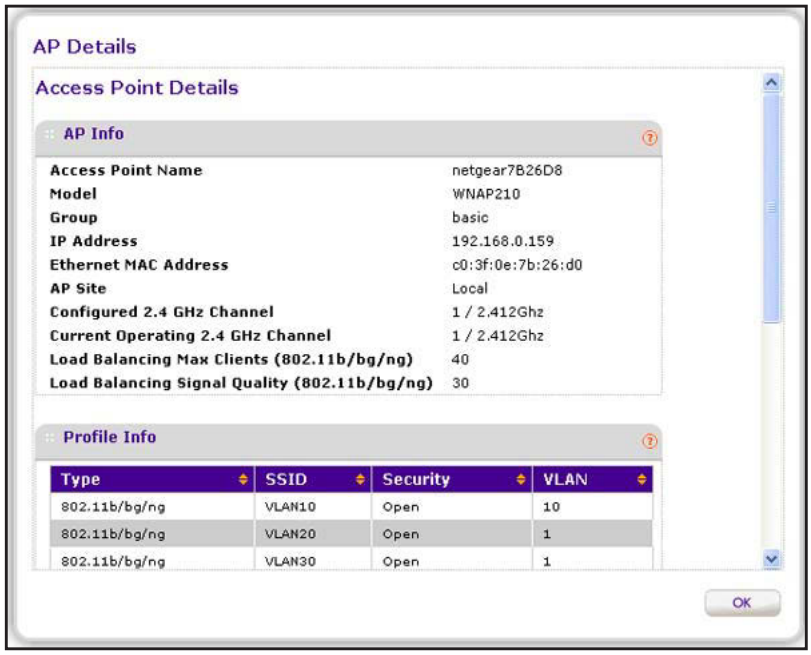
6. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
7. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
8. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

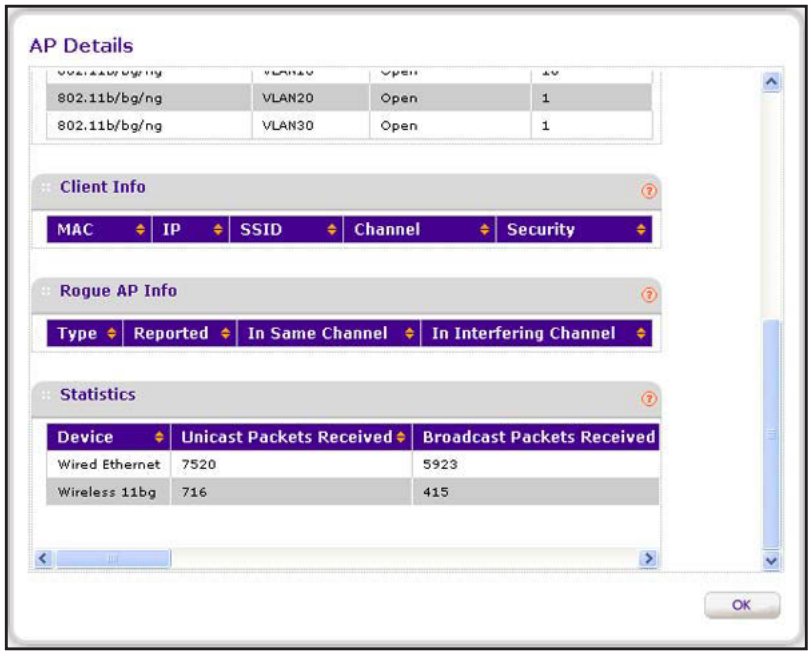
10. To display details about an access point, do the following:

    a. Select the radio button that corresponds to the access point for which you want to see the details.

    b. Click the **Details** button.

    The AP Details pop-up window opens. Because this window is tall and you must scroll through it, the window is shown in the following two figures.





The following table describes the fields of the AP Details pop-up window.

Item	Description
AP Info	
This information is self-explanatory.	
Profile Info 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/ac**).
SSID	The WiFi 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.
Client Info The information that displays depends on the type and security of the connection between the client and the access point. For each WiFi client that is connected to the selected access point, some or all of the following information displays:	
MAC	The MAC address of the WiFi client.
IP	The IP address of the client.
Channel	The channel that the WiFi client is using to connect to the access point.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Rogue AP Info For all rogue and unmanaged neighboring access points combined that the selected managed access point detected, 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/ac**).
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.

Item	Description
In Interfering Channel	The total number of detected rogue access points in the interfering channel.
Statistics	
For each type of usage (**Wired Ethernet**, **Wireless 11ng**, **Wireless 11bg**, **Wireless 11b**, **Wireless 11ac**, **Wireless 11na**, **Wireless 11a**, or a combination), statistics about transmitted and received packets and bytes display for the selected access point. The actual statistics are self-explanatory. **Note:** To see all fields of the table on the AP Details page, scroll to the right.	

11. Click the **OK** button.

    The AP Details pop-up window closes, and the SSID Mapping page displays again.

Monitor Local Clients in the Network

You can monitor the clients that were accepted into the WiFi network, the clients that were denied access to the WiFi network, and the clients that are roaming in the network:

- **Accepted clients**. See *Monitor Accepted Clients*.
- **Blacklisted clients**. See *Monitor Blacklisted Clients*.

Monitor Accepted Clients

You can monitor all clients that were accepted into the network by all wireless controllers in the network.

➢ **To view the accepted clients in the network:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

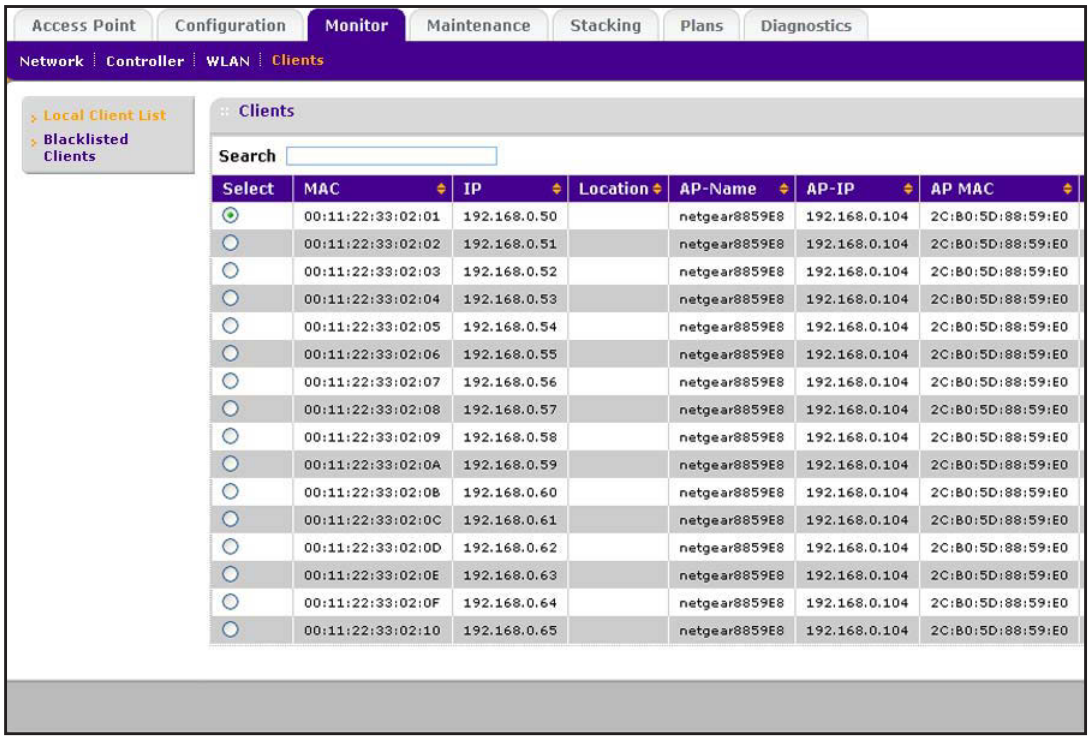
   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

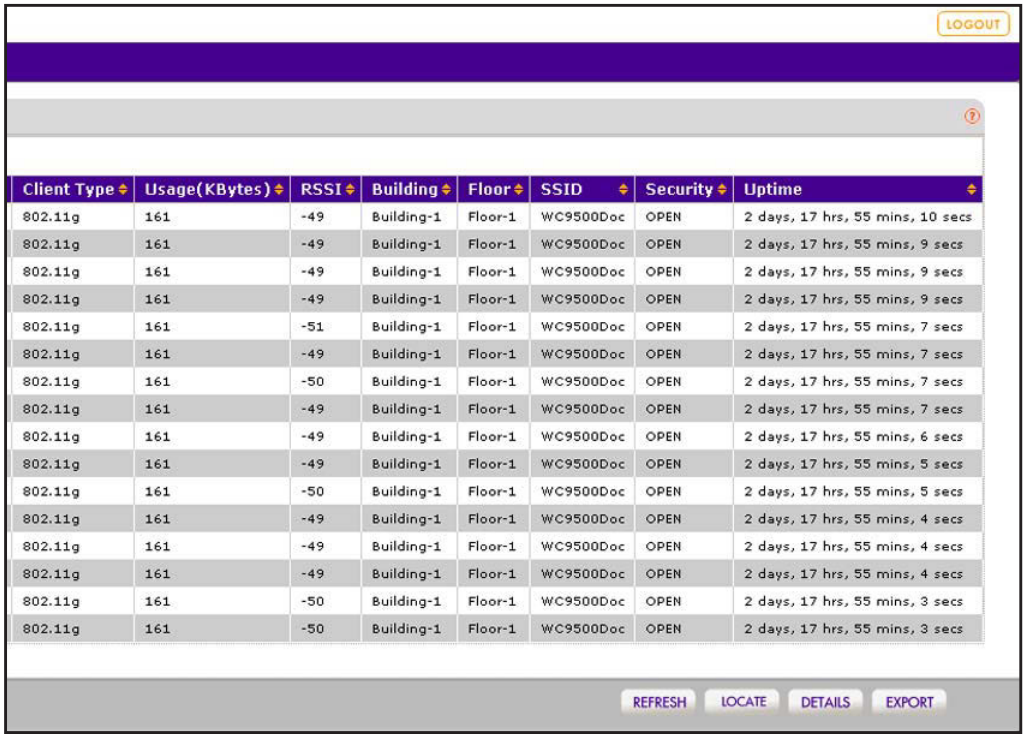
   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Monitor > Clients > Local Client List**.

   The Clients page displays. Because this page is a wide page, it is shown in the following two figures.



Select	MAC	IP	Location	AP-Name	AP-IP	AP MAC
◉	00:11:22:33:02:01	192.168.0.50		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:02	192.168.0.51		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:03	192.168.0.52		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:04	192.168.0.53		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:05	192.168.0.54		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:06	192.168.0.55		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:07	192.168.0.56		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:08	192.168.0.57		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:09	192.168.0.58		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0A	192.168.0.59		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0B	192.168.0.60		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0C	192.168.0.61		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0D	192.168.0.62		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0E	192.168.0.63		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:0F	192.168.0.64		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0
○	00:11:22:33:02:10	192.168.0.65		netgear8859E8	192.168.0.104	2C:B0:5D:88:59:E0



Client Type	Usage(KBytes)	RSSI	Building	Floor	SSID	Security	Uptime
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 10 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 9 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 9 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 9 secs
802.11g	161	-51	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 7 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 7 secs
802.11g	161	-50	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 7 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 7 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 6 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 5 secs
802.11g	161	-50	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 5 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 4 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 4 secs
802.11g	161	-49	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 4 secs
802.11g	161	-50	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 3 secs
802.11g	161	-50	Building-1	Floor-1	WC9500Doc	OPEN	2 days, 17 hrs, 55 mins, 3 secs

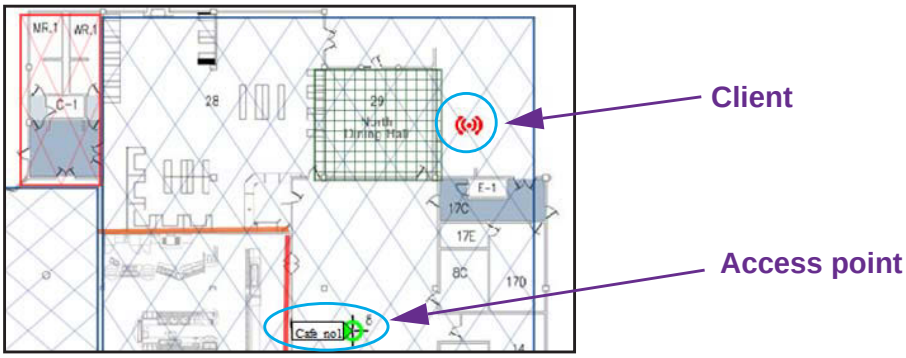
Note: The **Network** configuration menu tab displays under the **Monitor** main navigation menu tab *only* if you configured stacking.

The following table describes the fields of the Clients table on the Local Client List page.

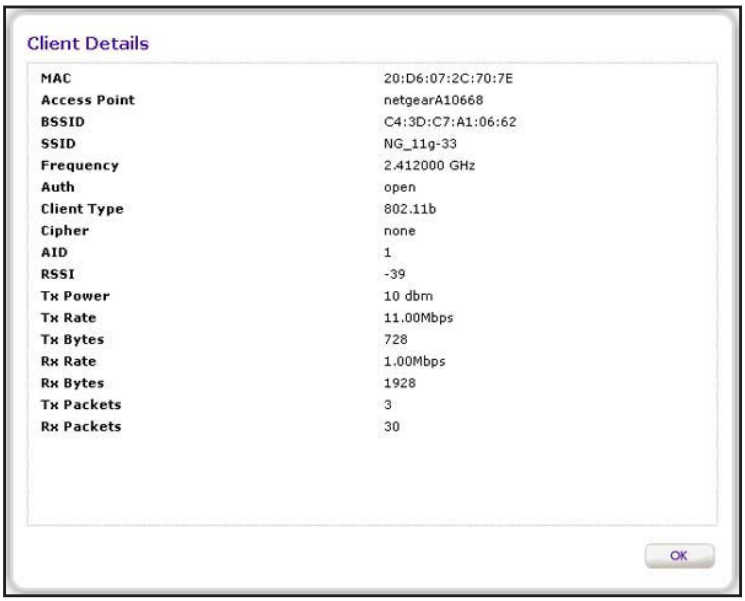
Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the WiFi client.
IP	The IP address of the WiFi client.
Location	The location of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client is connected.
AP-IP	The IP address of the access point to which the WiFi client is connected.
AP MAC	The MAC address of the access point to which the WiFi client is connected.
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).
Usage (KBytes)	The traffic usage of the WiFi client in KB.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Building	The building to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
Floor	The floor to which you assigned the access point (see *Change Access Point Information on the Managed AP List* on page 168 or *Assign Access Points to Buildings, Floors, and Advanced Profile Groups* on page 172).
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Security	The security mode (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**) that the WiFi client is using to connect to the access point.
Uptime	The period that the client is connected to the wireless controller.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To display the latest information onscreen, click the **REFRESH** button.

9. To locate a client on a deployed floor plan, do the following:
   a. Select the radio button that corresponds to the client that you want to locate.
   b. Click the **Locate** button.
      The selected client displays on the floor plan and is indicated by a red icon.



   c. To display details about the client, point to the client.
      A pop-up window opens and displays details about the client.
   d. To close the floor plan, click the **Back** button.
      The Local Client List page displays again.
10. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.
11. To display details about a client, do the following:
   a. Select the radio button that corresponds to the clients for which you want to see the details.
   b. Click the **Details** button.



The following table describes the fields of the Client Details pop-up window.

Item	Description
MAC	The MAC address of the WiFi client.
Access Point	The name of the access point to which the WiFi client is connected.
BSSID	The MAC address of the access point's radio to which the WiFi client is connected.
SSID	The WiFi network SSID that the WiFi client is using to connect to the access point.
Frequency	The channel frequency that the WiFi client is using to connect to the access point.
Auth	The security mode that the WiFi client is using to connect to the access point (**Open**, **WEP**, **WPA**, **WPA2**, or **WPA/WPA2**).
Client Type	The wireless mode that the WiFi client is using to connect to the access point (**802.11ng**, **802.11bg**, **802.11b**, **802.11ac**, **802.11na**, or **802.11a**).
Cipher	The type of encryption that the WiFi client is using (**None**, **WEP**, **AES**, **TKIP**, or **TKIP + AES**).
AID	The association ID of the client.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Tx Power	The transmit power of the WiFi client.
Tx Rate	The transmit rate in Mbps of the WiFi client.
Tx Bytes	The number of bytes that the WiFi client transmitted.
Rx Rate	The receive rate in Mbps of the WiFi client.
Rx Bytes	The number of bytes that the WiFi client received.
Tx packets	The number of packets that the WiFi client transmitted.
Rx Packets	The number of packets that the WiFi client received.

12. Click the **OK** button.

    The Client Details pop-up window closes, and the Local Client List page displays again.

Monitor Blacklisted Clients

You can monitor all clients that were denied access to the network by all wireless controllers in the network.

Note: Monitoring of blacklisted clients is supported on models WC7600 and WC9500 but not on models WC7500 and WC7600v2.

The wireless controller places the following types of clients on the black list:

- Clients for which an authentication failure occurred because they are included in a MAC ACL that denies them access.
- Clients for which an authentication failure occurred, for example, because an incorrect password was entered or a RADIUS server denied them access.

  If the client connects with the correct authentication information, the client is cleared from the black list after 10 seconds.
- Clients that attempt to connect to an access point for which load balancing is enabled and that reached its maximum number of devices allowed per radio.
- Clients that attempt to connect to an access point for which load balancing is enabled and that reached its RSSI threshold.

Note: If a client continues to attempt to connect to an access point with a weak signal (that is, with a weak RSSI), the client is allowed to connect while remaining on the black list. In such a situation, we recommend that you investigate the coverage and other environmental factors in the area in which the client and access point are located.

Blacklisted clients are allowed to attempt to connect again 10 seconds after their previous attempt. If the reason that a client is blacklisted is addressed, for example, the security key is corrected, the client is allowed to connect and (in most cases) removed from the black list.

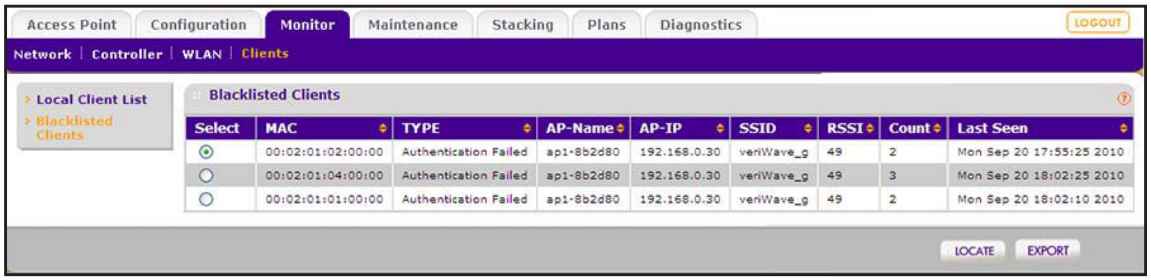
➢ **To view the blacklisted clients in the network:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Monitor > Clients > Blacklisted Clients**.



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

The following table describes the fields of the Blacklisted Clients table on the Blacklisted Clients page.

Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the WiFi client.
TYPE	The reason why the WiFi client was denied access.
AP-Name	The name of the access point (see *Change Access Point Information on the Managed AP List* on page 168) to which the WiFi client was denied access.
AP-IP	The IP address of the access point to which the WiFi client was denied access.
SSID	The WiFi network SSID to which the WiFi client attempted to connect.
RSSI	The received signal strength indicator (RSSI) of the WiFi client.
Count	The number of times that the WiFi client attempted to connect.
Last Seen	The last time that the WiFi client attempted to connect.

5. To sort the table, click the double triangle icon or single triangle icon at the top right of a column.
6. To search the table, in the **Search** field, enter the information that you are looking for, such as an IP address or MAC address.
7. If the table contains many entries, navigate through the table by using the following buttons and menu that display at the bottom of the table:
   - To move to the next page, click the **Next** button.
   - To move to the previous page, click the **Previous** button.
   - To change the number of entries onscreen, from the **Entry Per Page** menu, select **20**, or **40**, or **60**, and so on, or **All**.
8. To locate a blacklisted client on a deployed floor plan, do the following:
   a. Select the radio button that corresponds to the blacklisted client that you want to locate.
   b. Click the **Locate** button.

      The selected blacklisted client displays on the floor plan and is indicated by a red icon.
   c. To display details about the blacklisted client, point to the client.

      A pop-up window opens and displays details about the client.
   d. To close the floor plan, click the **Back** button.

      The Blacklisted Client page displays again.
9. To export the table, do the following:
   a. Click the **EXPORT** button.
   b. To save the file, follow the directions of your browser.

14 Troubleshooting and Diagnostics

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 Reset Button to Restore Default Settings*
- *Resolve Problems With Date and Time*
- *Resolve Network Problems*
- *Resolve Problems With Access Points*
- *Use the Diagnostic Tools on the Wireless Controller*

Troubleshoot Basic Functioning

After you turn on power to the wireless controller, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is lit green and that the Status LED is lit yellow.
2. After approximately two minutes, verify the following:
   a. The Status LED is lit green.
   b. The left Ethernet port LED is lit for any local port that is connected.

   If the port's left LED is lit, a link is established to the connected device. If the 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 yellow. 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 Is Not Lit

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, a hardware problem might exist. Contact NETGEAR technical support.

Status LED Never Turns Off

When the wireless controller is powered on, the Status LED is lit yellow for approximately two minutes and then turns green when the wireless controller completes its initialization. If the Status LED remains yellow, a fault occurred within the wireless controller.

If the Status LED is yellow more than several minutes after power-up, try the following:

- Turn off the power, and 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**. For more information, see *Reboot the Wireless Controller* on page 251.

If the error persists, a hardware problem might exist. Contact NETGEAR technical support.

Ethernet Port LEDs Are Not Lit

If the Ethernet 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 computer on your local network, try to isolate the problem. You can most likely solve the problem by following the suggestions that are described in the following sections.

Check the Ethernet Cabling

Check the Ethernet connection between the computer and the wireless controller as described in the previous section (see *Ethernet Port LEDs Are Not Lit*).

Check the IP Address Configuration

Make sure that your computer's IP address is on the same subnet as the wireless controller. If you are using the recommended addressing scheme, make sure that your computer is assigned a static IP address of 192.168.0.210 and a subnet of 255.255.255.0.

Note: If your computer'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 computer to the wireless controller and reboot your computer.

If the wireless controller's IP address changed and you do not know the current IP address, reset the wireless controller's configuration to factory default settings. The factory default IP address of the wireless controller is 192.168.0.250. For more information, see *Reboot the Wireless Controller* on page 251.

If you do not want to revert to the factory default settings and lose your configuration settings, you could use one of the following methods to discover the IP address of the wireless controller:

- 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.
- Run an IP scanner application in your network to discover the IP address of the wireless controller.
- Connect a serial cable between a computer and the wireless controller, and use the `ifconfig` command to discover the IP address of the wireless controller.

Check the Internet Browser

If the Ethernet cabling and IP address configuration are fine, the Internet browser might prevent you from accessing the web management interface. Check the following:

- Make sure that you are using the http://address login rather than the https://address login.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button 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 that you make 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 page, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. It is possible that the changes occurred but that the old settings remain in the web browser's cache.

After you upgrade the firmware, if the browser does not display the latest features of the web management interface, clear the browser's cache, and refresh the page.

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 troubleshoot a TCP/IP network by using the ping utility in your computer.

You can ping the wireless controller from your computer to verify that the LAN path to your wireless controller is set up correctly.

➢ **To ping the wireless controller from a computer running Windows:**

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 the **OK** button.

   A message like the following one displays:

   ```
   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, one of the following problems might be occurring:

- Wrong physical connections

  Make sure that the Ethernet LEDs are lit. If they are off, follow the instructions in *Ethernet Port LEDs Are Not Lit* on page 351.

- 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 Reset Button to Restore Default Settings

If you can access the wireless controller, you can use the Reboot/Reset Controllers page (the path is **Maintenance > Backup/Restore**) to perform a soft or hard reset (see *Reboot the Wireless Controller* on page 251).

If you can no longer access the wireless controller, press the **Reset** button on the front panel to restore the factory default settings.

➢ **To clear all data and restore the factory default values:**

1. Press and hold the **Reset** button for about eight seconds until the Status LED turns on and begins to blink.
2. Release the **Reset** button. The reboot process is complete after several minutes when the Status 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.

Resolve Problems With Date and Time

The Time Settings page displays the current date and time of day (see *Manage the Time Settings* on page 100). 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 did not yet successfully reach a network time server. Verify that the wireless controller can reach the Internet. After you configure the wireless controller, wait at least five minutes and check the date and time again.

Resolve Network Problems

If a network loop occurs, make sure that you did not connect a GBIC and the Ethernet port on the wireless controller (or two GBICs on the wireless controller) to the same network switch. Make only a single connection from a wireless controller to a network switch.

Resolve Problems With Access Points

If you encounter access point discovery or connection problems, the information in this section might help you to resolve these problems.

Resolve Discovery Problems

If the wireless controller does not discover any or all access points, check the configuration of the wireless controller and access points.

For all access points, check the following:

- Make sure that the wireless controller is connected to the LAN (see *Ethernet Port LEDs Are Not Lit* on page 351).
- Make sure that you enter 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 Guidelines* on page 154).
- Make sure that the access points run at least their initial firmware release or a newer version. For firmware requirements, see *Supported NETGEAR Access Points* on page 26.

For local access points that are installed across a Layer 3 network, check the following:

- Enable SNMP and SSH on all standalone access points. (This is the default setting for access points.)
- Unblock UDP port number 7890 in the firewall.
- Assign each access point a unique IP address. (This requirement does not apply to access points in the factory default state that are in the same Layer 2 network.) If two or more access points are assigned the same IP address, only one of them is discovered at a time. You must add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.
- Enable DHCP option 43 (vendor-specific information) on an *external* DHCP server. Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 with the IP address of the wireless controller.

For more information, see *Access Point Discovery Guidelines* on page 154.

Resolve Connection Problems

If the Power LED of an access point blinks amber, the access point lost its connection to the wireless controller. In this situation, check the network connectivity between the access point and the wireless controller.

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 a DHCP server issues, either a DHCP server in the network or a DHCP server that is configured on the wireless controller. This change occurs to ensure that each managed access point is assigned a unique IP address.

If the network does not include a 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 the network does not include a DHCP server, configure one on the wireless controller (see *Manage the DHCP Server* on page 105). When a DHCP server becomes available, the access point can transition from the Connecting state to the Connected state.

If you assign a static IP address to the wireless controller and then use the web management interface of a discovered access point to configure a static IP address for the access point and enter the wireless controller's static IP address, the access point attempts to reach the wireless controller only at the provided static IP address. If the IP address of the wireless controller changes, the access point can no longer reach the wireless controller. In such a situation, reset the access point to factory default settings. Doing so removes the static IP address of the wireless controller from the access point configuration.

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. The default rogue access point detection interval is 30 minutes. This interval is not configurable.

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.

Ping an Access Point

You can ping an access point to see if the wireless controller can reach the access point.

➢ **To ping an access point:**

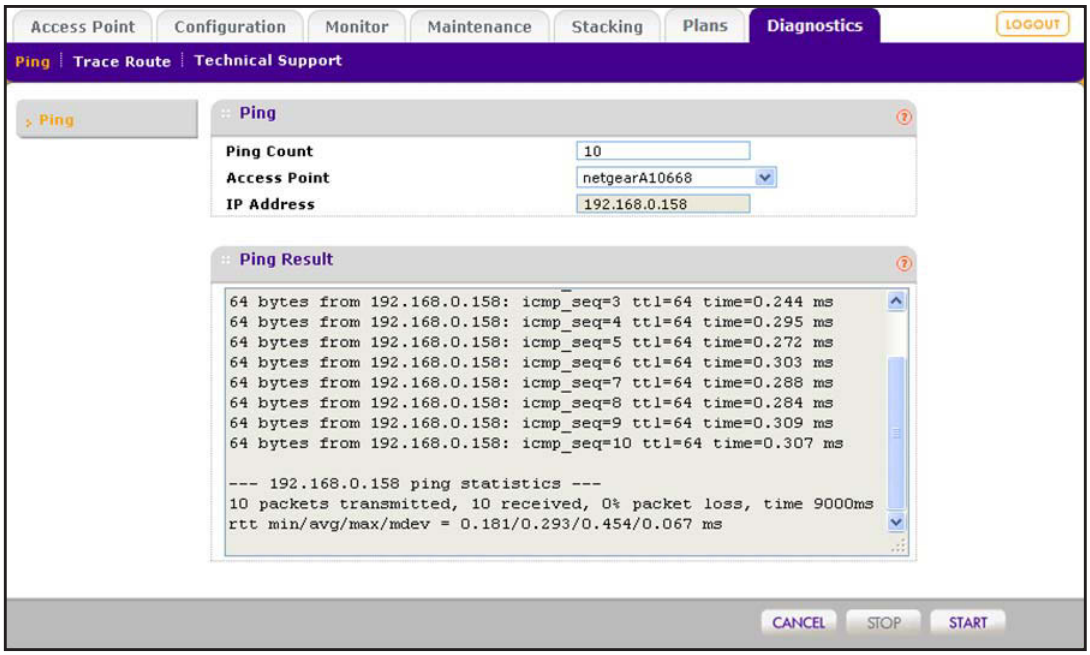
1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.

2. Enter your user name and password.
3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.
4. Select **Diagnostics > Ping**.



5. In the **Ping Count** field, enter the number of ping packets to be sent.

   The default number is 10.
6. From the **Access Point** menu, select the access point to be pinged.

   After you make your selection, the IP address of the access point displays in the **IP Address** field.
7. Click the **Start** button.

   The results are shown in the **Ping Result** field.

Trace a Route to an Access Point

You can trace a route to verify the route from the wireless controller to an access point.

➢ **To trace a route to an access point:**

1. Open a web browser. In the browser's address field, type the wireless controller's IP address.

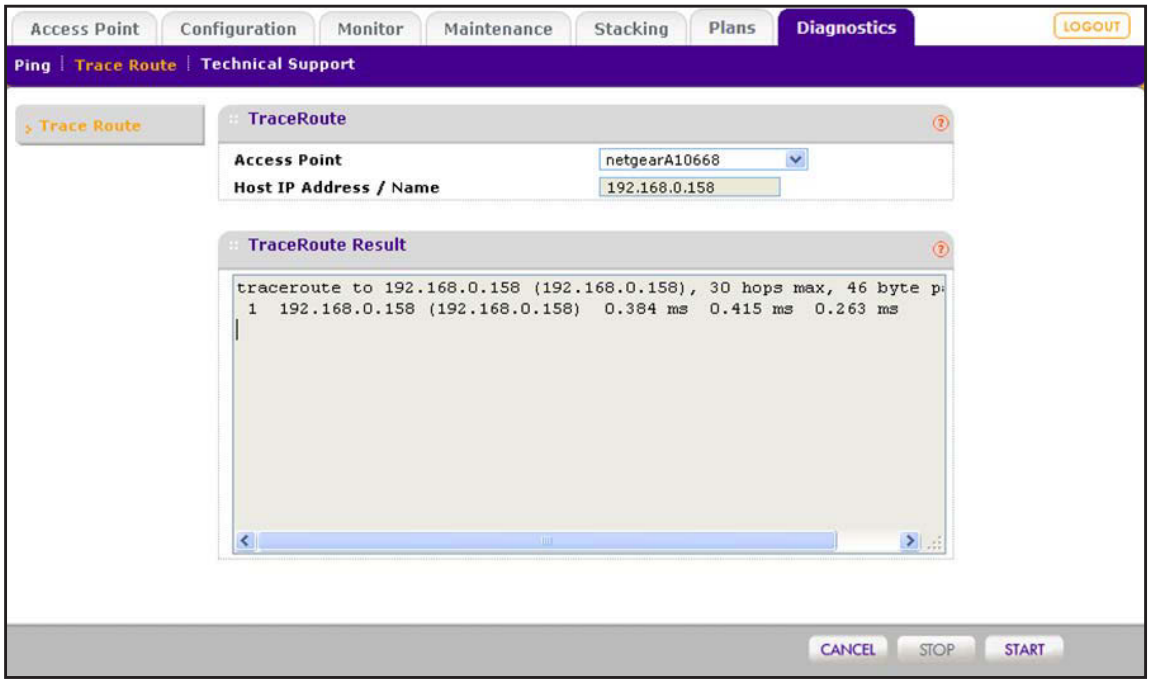
   By default, the IP address is 192.168.0.250.

   The wireless controller's login window opens.
2. Enter your user name and password.

3. Click the **Login** button.

   The wireless controller's web management interface opens and displays the Summary page.

4. Select **Diagnostics > Trace Route**.



5. From the **Access Point** menu, select the access point for which you want to trace the route.

   After you make your selection, the IP address of the access point displays in the **IP Address** field.

6. Click the **Start** button.

   The results are shown in the **TraceRoute Result** field.

Factory Default Settings, Technical Specifications, and Passwords Requirements

A

This appendix includes the following sections:

- *Factory Default Settings*
- *Technical Specifications Models WC7500 and WC7600v2*
- *Technical Specifications Models WC7600 and WC9500*
- *Password Requirements*

Factory Default Settings

You can restore the wireless controller to its factory default settings on the Reboot/Reset Controllers page (see *Reboot the Wireless Controller* on page 251) or by using the Reset button on the front panel (see *Use the Reset Button to Restore Default Settings* on page 354). The wireless controller returns to the factory configuration settings that are shown in the following table.

Table 12. Factory default settings for the wireless controller

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
	DHCP server pools	None
	Time zone	USA Pacific Standard Time (PST)
	Time zone adjusted for daylight saving time	Enabled
	SNMP	Enabled

Technical Specifications Models WC7500 and WC7600v2

The following table lists the technical and physical specifications for models WC7500 and WC7600v2.

Table 13. Technical and physical specifications models WC7500 and WC7600v2

Feature	Default Setting
Electrical specifications	• 100–240V, 3A, 50–60 Hz AC input • Typical power consumption 12 W
Dimensions (W x H x D) cm	44 cm x 4.5 cm x 26.3 cm (Fits in a 1U rack)
Dimensions (W x H x D) in.	17.3 in. x 1.7 in. x 10.3 in. (Fits in a 1U rack)
Weight	7.9 kg (3.6 lb)
Operating temperatures	0° to 45°C (32° to 113°F)
Operating humidity	10% minimum to 90% maximum relative humidity

Table 13. Technical and physical specifications models WC7500 and WC7600v2 (continued)

Feature	Default Setting
Storage temperatures	–20° to 70°C (–4° to 158°F)
Storage humidity	5% minimum to 95% maximum relative humidity, noncondensing
Safety and EMI	UL, FCC, CE, RCM, CCC, VCCI, KCC, BIS
Environmental	WEEE, RoHS, REACH

For a list of all features and capabilities of the wireless controller, see the datasheet:

- For the WC7500, visit *support.netgear.com/product/WC7500*.
- For the WC7600v2, visit *support.netgear.com/product/WC7600*.

Technical Specifications Models WC7600 and WC9500

The following table lists the technical and physical specifications for models WC7600 and WC9500.

Table 14. Technical and physical specifications models WC7600 and WC9500

Feature	Default Setting
Electrical specifications	• 100–240V, 5A, 47–63 Hz AC input • Typical power consumption 82.3 W
Dimensions (W x H x D) cm	43 cm x 4.3 cm x 44 cm (Fits in a 1U rack)
Dimensions (W x H x D) in.	16.92 in. x 1.7 in. x 17.32 in. (Fits in a 1U rack)
Weight	• With one power supply: 6.32 kg (13.94 lb) • With an optional second power supply: 7.57 kg (16.68 lb)
Operating temperatures	0° to 45°C (32° to 113°F)
Operating humidity	10% minimum to 90% maximum relative humidity
Storage temperatures	–20° to 70°C (–4° to 158°F)
Storage humidity	5% minimum to 95% maximum relative humidity, noncondensing
Safety and EMI	UL, FCC, CE, RCM, CCC, VCCI, KCC, BIS
Environmental	WEEE, RoHS, REACH

For a list of all features and capabilities of the wireless controller, see the datasheet:

- For the WC7600, visit *support.netgear.com/product/WC7600*.
- For the WC9500, visit *support.netgear.com/product/WC9500*.

Password Requirements

The following table lists the password requirements.

Table 15. Password requirements

Web Management Interface Path		User Type or Data Encryption	Restrictions		Section in This Manual
			Allowed Characters	Length	
Select **Maintenance > User Management**.		• Administrator • Read Only • Guest Provisioning • License Management Only	Alphanumerics and special characters (see footnote 1)	Up to 31	See *Manage Users, Accounts, and Passwords* on page 230.
1. Select **Maintenance > User Management**. 2. Click the **Captive Portal Users** tab.		Captive portal user	Alphanumerics and special characters	Up to 31	
1. Select **Maintenance > User Management**. 2. Click the **WiFi Clients** tab.		WiFi user	Alphanumerics only	Up to 31	
Basic profile: 1. Select **Configuration > Profile > Basic > Radio**. 2. Select a profile. 3. Make a selection from the Network Authentication menu.	Shared Key	64-bit WEP	Hexadecimal	10 fixed	See *Manage Security Profiles for the Basic Profile Group* on page 123.
		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 15. Password requirements (continued)

Web Management Interface Path		User Type or Data Encryption	Restrictions		Section in This Manual
			Allowed Characters	Length	
Advanced profile: 1. Select **Configuration > Profile > Advanced > Radio**. 2. Select a group. 3. Click **Edit**. 4. Select a profile. 5. Make a selection from the Network Authentication menu.	Shared Key	64-bit WEP	Hexadecimal	10 fixed	See *Manage Security Profiles for Advanced Profile Groups* on page 128.
		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			
Select **Configuration > Security > Authentication Server**.	External RADIUS Server	Shared Secret	Alphanumerics and special characters	Up to 127	See *Manage Authentication Servers and Authentication Server Groups* on page 139.
	External LDAP Server	Domain Admin User	Alphanumerics and special characters	Up to 32	

1. *If your admin password contains special characters (for example, P, !, @, #, $, %, or ^) and you upgrade the firmware from version 4.x to version 5.x, you first must change the password to one with alphanumeric characters only (for example, password4285) before you upgrade the firmware. Make sure that you back up the configuration before you upgrade the firmware. After you successfully upgrade the firmware to version 5.x, you can change the password back to your original password with special characters.*

Index

Numerics

1 to 1 redundancy 283–288
2.4 GHz and 5 GHz channels 193
802.11 wireless modes 181, 187
802.1Q VLAN header 35, 102

A

AC power supply
    WC7500 and WC7600v2 20
    WC7600 and WC9500 23
access denied, clients 349
access point logs, saving and clearing 257
access point profile groups
    adding advanced groups 128
    assigning access points to 172
    basic and advanced, described 33
    channels and transmission power, overriding 183, 189
    profiles, adding and configuring 123, 130
    QoS, configuring 202
    radio, turning on and off 176
    rate limiting, configuring 207
    RF management, configuring 194
    wireless settings, configuring 179
access points
    adding 161, 165
    antennas, configuring 171
    autodiscovery 153
    channel allocation
        automatic 191–194
        manual 185, 191
    DHCP client, disabling 170
    discovery 154
    dual-band 29, 33, 120, 207
    factory default state, autodiscovery 158
    firmware, minimum version 26
    floor and building settings 171
    IP addresses 170
    IP subnet 158, 160
    known and unknown 217
    local 154, 164, 168
    managed status 168
    models, supported 26
    pinging 356
    rebooting 269
    remote 160, 164, 168
    RF planning, adding and managing 75
    rogue
        detecting and managing 214
        viewing in the network 303
        viewing on the managed access point 309, 324, 342
        viewing on the wireless controller 331
    standalone mode
        autodiscovery 163
        returning to 171
    supported models 26
    tracing a route 357
    troubleshooting 355
    Tx power
        automatically controlling 196, 198
        manually controlling 185, 191
        overriding 183, 189
    viewing
        on the wireless controller 306, 321
        security profiles 309, 324, 342
        statistics 309, 324, 343
    VLAN settings 170
access, remote 254
accounts, captive portal 230
active SSIDs, viewing 340
active voice calls, preventing channel allocation 194
Address Resolution Protocol (ARP) suppression 183, 189
Advanced Encryption Standard (AES) 137
advanced profile groups
    adding groups 128
    assigning access points to 172
    channels and transmission power, overriding 189
    described 33
    LED behavior, configuring 211
    profiles, adding and configuring 130
    QoS, configuring 202
    radio, turning on and off 177
    rate limiting, configuring 209

RF management, configuring 197
wireless settings, configuring 185
advanced settings, described 32, 120
AES (Advanced Encryption Standard) 137
aggregated MAC protocol data unit (AMPDU) 182, 188
aggregation length 182, 188
aggregation, links 102
AIFS (arbitration inter-frame space) 204
alarms
settings 117
viewing in the network 303
viewing on the wireless controller 317
alerts, viewing and saving 259
AMPDU (aggregated MAC protocol data unit) 182, 188
antennas
RF planning, adding and managing 78
specifying internal or external 171
supported models 30
application requirements, RF planning 52
arbitration inter-frame space (AIFS) 204
architecture, advanced profile group 34
ARP (Address Resolution Protocol) suppression 183, 189
authentication
certificates 112
external
MAC authentication 126, 133, 145
RADIUS and LDAP servers 137, 139–142, 221, 226
internal 142
methods supported 37
servers 139
auto planning advisor, RF planning 69
autodiscovery, access points 153
automatic channel allocation and transmission power, WLAN healing 195

B

back panel components
WC7500 and WC7600v2 20
WC7600 and WC9500 22
background QoS queue 202
backing up the configuration 246
band steering 197, 199
bandwidth, low and high density 182, 188
basic profile group
assigning access points to 172
channels and transmission power, overriding 183
described 33
LED behavior, configuring 210
profiles, adding and configuring 123
radio, scheduling 176
rate limiting, configuring 208
RF management, configuring 195
wireless settings, configuring 179
basic service set identifier (BSSID) 214
basic settings, described 32, 120
beacon interval 182, 188
best effort QoS queue 202
blacklisted clients, viewing in the network 349
bottom label
WC7500 and WC7600v2 20
WC7600 and WC9500 23
broadcast rate limiting 183, 189
broadcasting SSID 125, 132
browsers
requirements, RF planning 52
supported 91
troubleshooting 353
BSSID (basic service set identifier) 214
buildings, RF planning 55

C

cabling, troubleshooting 351
calls, preventing channel allocation 194
captive portal
accounts and users, adding 234–242
accounts and users, viewing 335
configuring 218–230
enabling 133
guest email address database, viewing 337
users, adding multiple simultaneously 240
certificates, authentication 112
channel allocation
automatic 191–194
manual 185, 191
channel width 181, 187
classify rogue access points 215
client separation 125, 132
client VLANs 36, 41
clients, DHCP 170
clients, viewing
accepted in the network 345
blacklisted in the network 349
neighboring in the network 330
on the access point 309, 324, 342
on the wireless controller 311, 318, 326
clients, wireless, maximum number 205
color coding, channels 307, 322
community names, SNMP 255

compliance, regulatory
WC7500 and WC7600v2 361
WC7600 and WC9500 361
configuration file, restoring 247
configuration roadmaps 93–96
configuration, backing up and restoring 246–247
connection problems, troubleshooting 356
connectivity test 35
console port
WC7500 and WC7600v2 19
WC7600 and WC9500 22
contents, package 18
controller models 11
controller selection, stacking 280
corporate channels 193
counter
WC7500 and WC7600v2 19
WC7600 and WC9500 22
country and region of operation 100
customer information, licenses 111
CwMin and CwMax (minimum or maximum contention window) 204

D

data encryption
configuring 125, 132
supported methods 37
data rate 181, 187
date, troubleshooting 354
default profile group. See basic profile group.
default settings 360
default settings, resetting
WC7500 and WC7600v2 19, 251
WC7600 and WC9500 22, 251
delivery traffic indication message (DTIM) interval 182, 188
denied access, clients 349
detecting rogue access points 214
DHCP client, access points 170
DHCP leases, viewing 334
DHCP option 43 155, 355
DHCP server
described 36
settings 106
diagnostic tools 356
digital counter
WC7500 and WC7600v2 19
WC7600 and WC9500 22
dimensions
WC7500 and WC7600v2 360
WC7600 and WC9500 361
discovering access points 154
discovery problems, troubleshooting 355
DNS servers 104
DTIM (delivery traffic indication message) interval 182, 188
dual-band access points 29, 33, 120, 207

E

EAP (Extensible Authentication Protocol) 234
electrical specifications
WC7500 and WC7600v2 360
WC7600 and WC9500 361
email address database, viewing 337
email notification server 117
encryption, methods supported 37
end-user license agreement (EULA) 223, 228
Ethernet port
WC7500 and WC7600v2 19
WC7600 and WC9500 22
Ethernet port LEDs
described 25
troubleshooting 351
EULA (end-user license agreement) 223, 228
event tracing 114
Extensible Authentication Protocol (EAP) 234
external antennas 171
external authentication
MAC authentication 126, 133, 145
RADIUS and LDAP servers 137, 139–142, 221, 226
external storage 252

F

factory default settings, wireless controller 360
factory default state, access point autodiscovery 158
failover, redundancy 283, 289
Fan LED, described 24
fans
WC7500 and WC7600v2 20
WC7600 and WC9500 23
features, overview 13–15
firmware
minimum version for access points 26
multicast, using for access point upgrade 270
upgrading, wireless controller 248
version, viewing 304
floors, RF planning
adding 55

heat map, deployed floor plan 87
scaling 59
FTP server, firmware upgrade 249

G

GBICs (gigabit interface converters) 22
guard interval 181, 187
guest email address database, viewing 337
guest portal, configuring 218–230
GUI, troubleshooting 352

H

hard reset 251, 354
healing, WLAN 195
heat maps, deployed floor plan 87
high density bandwidth 182, 188
high traffic load, preventing channel allocation 194
hotspot users 218
humidity
WC7500 and WC7600v2 360
WC7600 and WC9500 361

I

interference sources 35
internal antennas 171
internal authentication server 142
internal RADIUS server 139
inventory, licenses 266
inventory, RF planning 83
IP addresses
access points 170
DHCP server assignment 107
license server 110
local address
redundancy setting 287, 295
stacking setting 278
master controller, stacking 278
multicast range 271
primary controller, redundancy 287, 295
secondary controller, redundancy 286, 294
slave controller, stacking 276
SNMP manager 255
syslog server 116
TFTP and FTP servers 249
wireless controller 104
IP settings
access points 170
wireless controller 104
IP subnets
access points 158, 160
LAN 104
troubleshooting 355

K

keys, licenses 112, 267
known rogue access points 217

L

label, bottom
WC7500 and WC7600v2 20
WC7600 and WC9500 23
LAG (link aggregation group) 104
LAN path, troubleshooting 353
LAN port
WC7500 and WC7600v2 19
WC7600 and WC9500 22
LAN port LEDs
described 25
troubleshooting 351
Layer 2 subnet, access point autodiscovery 158
Layer 3 access point autodiscovery 154, 162
LDAP server 137, 140–142, 221, 226
LEDs
startup procedure 91
troubleshooting 351
legacy 802.1x authentication 137
levels, logging 114–116
licenses
managing 266–268
number and types required 16
redundancy group, matching 283, 290
registering 109–112
link aggregation 102
link aggregation group (LAG) 104
load balancing 205
load balancing logs, viewing and saving 261
local access points 154, 164, 168
local IP address
redundancy settings 287, 295
stacking settings 278
location, placement wireless controller 97
logs
configuring 113
saving 256
low density bandwidth 182, 188

M

MAC authentication 145
MAC authentication groups 148
managed AP list 166
managed status, access points 168
management users, adding 231
management VLANs 35, 41, 101
master controller, stacking 274, 278
maximum burst length 204
maximum number, wireless clients 205
memory partition 250
minimum and maximum contention window (CwMin or CwMax) 204
models
  access points supported 26
  antennas supported 30
  wireless controllers 11
multicast rate limiting 183, 189
multicast, firmware upgrade process 270

N

N to 1 redundancy 289–296
neighboring clients, viewing 330
network authentication 125, 132
network performance, troubleshooting 356
network status, viewing summary 302
noncoverage zone, RF planning 60
notification server, emails 117
NTP (Network Time Protocol), client and server 101

O

obstacles, RF planning 61
obstruction areas, RF planning 64
option 43, DHCP 154

P

package contents 18
partition, memory 250
password requirements 362
passwords
  restoring default 354
  users 230
physical specifications 360–361
pinging, access points 356
planning, system 35
PoE (Power over Ethernet), access points 29
port requirements, RF planning 52
portals, configuring 218–230
ports and slots
  WC7500 and WC7600v2 18
  WC7600 and WC9500 21
Power LED
  described 24
  troubleshooting 351
power level, transmission 100
power supply
  WC7500 and WC7600v2 20
  WC7600 and WC9500 23
preamble type 182, 188
preferred wireless band 199
preventing channel allocation 194
primary controller, redundancy 287, 295
product label
  WC7500 and WC7600v2 20
  WC7600 and WC9500 23
profile groups. See
  access point profile groups.
  advanced profile groups.
  basic profile group.
profiles. See security profiles.

Q

QoS (quality of service) 202

R

rack-mounting 97
radio band steering 197, 199
radio frequency (RF)
  logs, viewing and saving 260
  management 194
  obstructions 35
  planning 51
radio, turning on and off 176
RADIUS authentication server groups 143
RADIUS servers 137, 139–142, 221, 226
rate limit logs, viewing and saving 263
rate limiting 207
rebooting
  access points 269
  wireless controller 251, 354
received signal strength indication (RSSI), load balancing 205
redirecting traffic, captive portals 221
reduced interframe space (RIFS) transmission 182, 188
redundancy logs, viewing 264
redundancy status, viewing 302

redundancy, managing 283—299
redundant controller 286, 294
registering licenses 109—112
registration keys, licenses 112, 267
regulatory compliance
  WC7500 and WC7600v2 361
  WC7600 and WC9500 361
remote access 254
remote access points 160, 164, 168
reports, RF planning 86
requirements
  1 to 1 redundancy 283
  N to 1 redundancy 290
requirements Layer 3 autodiscovery 154
Reset button
  WC7500 and WC7600v2 19
  WC7600 and WC9500 22
resetting
  factory defaults 19, 22, 251, 354
  passwords 354
  wireless controller 251
restoring the configuration file 247
RF (radio frequency)
  logs, viewing and saving 260
  management 194
  obstructions 35
  planning 51
RF planning
  access points, adding and managing 75
  antennas, adding and managing 78
  overview and requirements 52
RIFS (reduced interframe space) transmission 182, 188
roadmaps for configuration 93—96
rogue access points
  detecting and managing 214
  viewing
    in the network 303
    on the managed access point 309, 324, 342
    on the wireless controller 318, 331
RSSI (received signal strength indication), load balancing 205
RTS threshold 181, 187

S

scalability and features, wireless controller models 12
scaling, floors 59
scheduling
  channel allocation 194
  firmware updates, wireless controller 250
  radio 176
SD card slot, WC7500 and WC7600v2 19
second power supply, WC7600 and WC9500 23
secondary controller, redundancy 286, 294
security profiles
  configuring
    advanced profile groups 130
    basic profile group 123
  managing 120
  viewing on the access point 309, 324, 342
  viewing on the wireless controller 315, 333
self, controller selection 280
self-healing 196, 198
server, licenses 109
service set ID (SSID) 125, 132
session time-out 255
SFP slot LEDs, WC7600 and WC9500, described 25
SFP slots, WC7600 and WC9500 22
shared key requirements (RADIUS) 362
signal quality 73
signal strength 205
slave controller, stacking 274, 276
slots and ports
  WC7500 and WC7600v2 18
  WC7600 and WC9500 21
sniffer 352
SNMP, enabling 254
soft reset 251
software
  minimum version for access points 26
  multicast, using for access point upgrade 270
  upgrading, wireless controller 248
  version, viewing 304
spectrum analysis 35
SSID (service set ID or wireless network name) 125, 132
Stack Master LED, described 25
stacking logs, viewing 265
stacking status, viewing 302
stacking, managing 273—282
standalone mode, access points
  autodiscovery 163
  returning to 171
standby link, aggregation 104
Status LED
  described 24
  troubleshooting 351
steering, radio bands 197, 199
storage, external 252
subnet masks
  access point 170
  DHCP server 107

wireless controller 104
support, NETGEAR 16
suppression, ARP 183, 189
syslog server 115
system alerts, viewing and saving 259
system logs, saving 256
system planning 35

T

tagged VLANs 102
TCP/IP network, troubleshooting 353
technical specifications 360–361
technical support 2
temperatures
WC7500 and WC7600v2 360
WC7600 and WC9500 361
Temporal Key Integrity Protocol (TKIP) 137
TFTP server, firmware upgrade 249
time and time zone
configuring 101
troubleshooting 354
TKIP (Temporal Key Integrity Protocol) 137
tracing a route 357
tracing events 114
traffic redirecting, captive portals 221
transmission opportunity (TXOP) limit 205
transmission power
automatically controlling 196, 198
country specification 100
manually controlling 185, 191
overriding 183, 189
trap port, SNMP 255
trial license 16
troubleshooting
access points 355
basic functioning 351
configuration settings, using sniffer 352
connection problems 356
date 354
diagnostic tools 356
discovery problems 355
GUI 352
LAN path 353
LEDs 351
network performance 356
pinging access points 356
resetting factory default settings 354
TCP/IP network 353
time and time zone 354
tracing an access point route 357
web management interface 352
Tx power
automatically controlling 196, 198
country specification 100
manually controlling 185, 191
overriding 183, 189
TXOP (transmission opportunity) limit 205

U

unicast, firmware upgrade process 270
unknown rogue access points 217
untagged VLANs 102, 170
upgrading firmware, wireless controller 248
URL redirecting, captive portals 221
USB port
WC7500 and WC7600v2 19
WC7600 and WC9500 22
users, managing 230

V

VAR information, licenses 111
video QoS queue 202
Virtual Router Redundancy Protocol (VRRP) 283, 289
VLANs
clients 36, 41
DHCP server 106
management 35, 41, 101
security profiles 125, 132
settings, access points 170
untagged 102, 170
voice calls, preventing channel allocation 194
voice QoS queue 202
VRRP (Virtual Router Redundancy Protocol) 283, 289
VRRP ID 287, 295

W

web management interface, troubleshooting 352
weight
WC7500 and WC7600v2 360
WC7600 and WC9500 361
WEP encryption 137
WEP key requirements 362
WiFi auto planning advisor 69
WiFi coverage zone, RF planning 60
WiFi coverage, RF planning 82
WiFi inventory, RF planning 83
WiFi users, adding 233
WINS servers 104

wired connection, stacking 273
wireless bands
  preferred 199
  usage, viewing 319
wireless blacklisted clients, viewing 349
wireless client separation 125, 132
wireless clients, maximum number 205
wireless clients, viewing
  accepted in the network 345
  blacklisted in the network 349
  neighboring in the network 330
  on the access point 309, 324, 342
  on the wireless controller 311, 318, 326
wireless controller models 11
wireless controller, viewing
  active SSIDs 340
  captive portal accounts and users 335
  DHCP leases 334
  guest email address database 337
  in the network 304
  managed access points 320
  managed clients 325
  neighboring access points 331
  neighboring clients 329
  profiles 332
  summary 316
  usage 319
wireless modes 181, 187
wireless network name (SSID) 125, 132
wireless settings 175
wizard, access point discovery 154
WLAN group assignment 172
WLAN healing 195
WMM (Wi-Fi multimedia) 202
WNAP and WNDAP access points 26
WPA and WPA2 authentication 137—139
WPA passphrase requirements 362