



Business Central
Wireless Manager 2.1
Application
User Manual

December 2017
202-11633-03

350 E. 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.

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
202-11633-03	December 2017	We added Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network on page 59.
202-11633-02	July 2017	We added the following new features: • Support for captive portals that can provide paid-for access through vouchers (see Add a Captive Portal for Voucher Access to a WiFi Network on page 56). This new feature provides the following capabilities: - Capability to generate vouchers with a unique code to deploy paid-for guest WiFi service (see Sell, Generate, and Print a Voucher on page 141). - Capability to monitor the status of sold vouchers (see View the Status of Vouchers and Download All Vouchers on page 144). - Capability to invite clerk collaborators who can sell vouchers (see Invite a Manager, Customer, or Clerk to an Account on page 95). • Fast roaming (802.11r with 802.11k) for WiFi networks that are carried by 802.11ac access points (see Enable Fast Roaming for a WiFi Network on page 63). • Load balancing for a location with the option to specify the maximum number of clients that are allowed to connect to one type of access point model (see Manage Load Balancing for a Location on page 38). • Enhanced Auto RF management with the option to select individual corporate channels (see Run or Schedule Automatic Radio Frequency Management for a Location on page 36). • Registration of a NETGEAR device while adding the device to a location (see Add an Access Point to a Location on page 31 or to inventory (see Add a Device to Inventory Without Deploying It on page 79). • Capability to add an access point to inventory without deploying it to a location (see Add a Device to Inventory Without Deploying It on page 79).

Business Central Wireless Manager 2.1 Application

Publication Part Number	Publish Date	Comments
202-11633-02 (Continued)	July 2017 (Continued)	(Continued) • Capability to change the management VLAN ID for an access point (see Change the Management VLAN for an Access Point on page 74). • Enhanced device firmware upgrade management and status view with the following new capabilities: - Capability to let upgrades occur automatically when a new major firmware release is available (see Schedule to Upgrade Devices at a Location to the Latest Firmware Version on page 42). - Capability to select beta firmware for automatic upgrades (see Schedule to Upgrade Devices at a Location to the Latest Firmware Version on page 42). • Improved alarm categorization and alarm notification (see View Alarms for a Device, Claim Alarms, and Resolve Alarms on page 131). • Enhanced account management that restricts access of an application user with a customer role to read-only (see Invite a Manager, Customer, or Clerk to an Account on page 95). • Support for up to six custom fields for the splash page of a captive portal for free access (see Add a Captive Portal for Free Access to a WiFi Network on page 53).
202-11633-01	March 2016	First publication.

Contents

Chapter 1 Introduction to the Business Central Wireless Manager 2.1

Business Central Wireless Manager 2.1 Application Concepts.....	8
System Architecture Concepts.....	8
Service Location Concepts.....	8
Automatic Network Provisioning Concepts.....	9
Key Functions.....	10
Provisioning Functions.....	10
Configuring and Managing Functions.....	10
Location Functions.....	10
WiFi Network Functions.....	11
Access Point Functions.....	11
Monitoring Functions.....	11
Account Management Functions.....	11
Application Roles.....	12
Plan a Location With WiFi Networks and Hotspots.....	12
Determine the Location Requirements.....	13
Determine the Management VLAN.....	13
Plan the Client Authentication and Data Encryption.....	13
Plan the Hotspots With Free Access and Paid-For Access.....	14
Other Planning Considerations.....	14
Compatible NETGEAR WiFi Access Points.....	16
Definitions of Access Point Terms.....	17

Chapter 2 Get Started With Cloud Management

Add Your First Location.....	19
Add a First WiFi Network to a Location.....	20
Add a First Access Point to a Location.....	23

Chapter 3 Manage Locations

Add a Location.....	27
Add a WiFi Network to a Location.....	28
Add an Access Point to a Location.....	31
Change the Basic Settings for a Location.....	33
Manage the Radio and Antenna Settings for a Location.....	33
Run or Schedule Automatic Radio Frequency Management for a Location.....	36
Manage Load Balancing for a Location.....	38
Upgrade Firmware on Devices at a Location.....	40
Upgrade Devices at a Location to a Specific Firmware Version.....	40
Schedule to Upgrade Devices at a Location to the Latest Firmware Version...	42
Reboot a Location.....	44
Change the Device Credentials for a Location.....	45
Remove a Location.....	46

Chapter 4 Manage WiFi Networks

Change the Broadcast, Advertisement, and VLAN Settings for a WiFi Network...	48
Change the Authentication and Encryption for a WiFi Network.....	49
Add a Captive Portal for Free or Paid-For Access to a WiFi Network.....	52
Add a Captive Portal for Free Access to a WiFi Network.....	53
Add a Captive Portal for Voucher Access to a WiFi Network.....	56
Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network.....	59
Set Bandwidth Caps for a WiFi Network.....	62
Enable Fast Roaming for a WiFi Network.....	63
Enable Client Isolation for a WiFi Network.....	64
Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network.....	65
Remove a WiFi Network.....	66

Chapter 5 Manage Devices and Device Inventory

Change the Device Name.....	69
Add or Change Building and Floor Labels for a Device.....	69
Change the Radio and WiFi Settings for a Device.....	70
Change the IP and Management VLAN Settings for a Device.....	72
Configure a Static IP Address for an Access Point.....	72
Configure an Access Point as a DHCP Client.....	73
Change the Management VLAN for an Access Point.....	74
Reboot a Device.....	75
Remove a Device From a Location.....	76
Manage the Device Inventory.....	77
View the Device Inventory.....	77
Add a Device to Inventory Without Deploying It.....	79
Deploy a Device in Inventory at a Location.....	80
Decommission a Device From a Location and Keep It in Inventory.....	82
Remove a Device From Inventory.....	83

Chapter 6 Manage Accounts and Licenses

Accounts Overview.....	87
Licenses Overview.....	87
About the Trial Period.....	87
View the Trial Balance and Trial Expiration Date During the Trial Period.....	88
What Happens at the End of the Free Trial Period?.....	88
Create a New Account.....	89
Add a License to an Account.....	90
View License Information for an Account.....	92
Add a Location to an Account.....	93
Remove a Location From an Account.....	94
View the Devices Managed Under an Account.....	95
Invite a Manager, Customer, or Clerk to an Account.....	95
Accept an Invitation and Sign Up for and Activate a Manager, Customer, or Clerk Account.....	96
Remove a Manager, Customer, or Clerk From an Account.....	98
Change the Name for an Account.....	99

Business Central Wireless Manager 2.1 Application

Remove an Account.....	100
Change Your Account Email Address and Password.....	101

Chapter 7 Monitor Your Locations, Networks, and Devices

Overview of the Monitoring Options.....	103
View Alarms for Your Account, Claim Alarms, and Resolve Alarms.....	104
Set Up Email Notification Profiles for License Accounts and Locations.....	108
Change or Remove an Email Notification Profile.....	109
View the Status of All Locations and Devices Under Your Account.....	110
Monitor a Single Location.....	113
View WiFi Usage at a Location.....	113
View the Status of Devices at a Location.....	115
View Neighbor and Rogue Access Points at a Location.....	117
View Clients Connected at a Location.....	119
View the Event Logs for a Location.....	120
Monitor a Single WiFi Network at a Location.....	122
View Usage of a WiFi Network.....	122
View Clients Connected to a WiFi Network.....	124
View the Event Logs for a WiFi Network.....	125
View Captive Portal Sessions.....	127
Monitor a Single Device at a Location.....	128
View WiFi Usage on a Device.....	129
View Clients Connected to a Device.....	130
View Alarms for a Device, Claim Alarms, and Resolve Alarms.....	131
View the Event Logs for a Device.....	134

Chapter 8 Diagnostics and Troubleshooting

Download the Diagnostics File for an Access Point.....	138
Troubleshooting a WiFi Network.....	139

Appendix A Manage Vouchers With a Clerk User Account

Sell, Generate, and Print a Voucher.....	141
View the Status of Vouchers and Download All Vouchers.....	144

Appendix B Cloud-Managed Access Points

View the Access Point Inventory and Connection Status in the Application.....	148
View the Cloud Connection and Activity Status on a Cloud-Enabled Access Point.....	149
How the Configuration of a Cloud-Managed Access Point Can Be Changed....	151
Convert an Access Point From Cloud-Managed to Standalone.....	151

Appendix C Technical Specifications

Introduction to the Business Central Wireless Manager 2.1

1

This chapter provides an introduction to the NETGEAR Business Central Wireless Manager (BCWM) 2.1 application.

For more information about the BCWM 2.1 application, visit businesscentral.netgear.com.

For information about preparing your access points for cloud management and subscribing to the BCWM 2.1 application, see the *Business Central Wireless Manager How to Start Guide*, which you can download from downloadcenter.netgear.com.

This chapter includes the following sections:

- *Business Central Wireless Manager 2.1 Application Concepts* on page 8
- *System Architecture Concepts* on page 8
- *Key Functions* on page 10
- *Application Roles* on page 12
- *Plan a Location With WiFi Networks and Hotspots* on page 12
- *Compatible NETGEAR WiFi Access Points* on page 16
- *Definitions of Access Point Terms* on page 17

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

Note This manual uses the following conventions:

- *WiFi* and *wireless* are interchangeable terms.
 - A WiFi network provides access without a captive portal.
 - A hotspot is a WiFi network that provides access through a captive portal.
-

Business Central Wireless Manager 2.1 Application Concepts

The NETGEAR Business Central Wireless Manager (BCWM) 2.1 application is a cloud management application that you can access from any computer to centrally manage cloud-enabled NETGEAR access points. Using the BCWM 2.1 application, you can add, configure, and monitor WiFi networks in the cloud.

The BCWM 2.1 cloud management solution is intended primarily for small and medium-sized businesses and organizations, for example, retail and hospitality businesses and healthcare organizations. This manual is intended primarily for cloud network administrators.

In this manual, the BCWM 2.1 application is referred to as the *application*.

System Architecture Concepts

The application lets you manage multiple WiFi networks and NETGEAR WiFi access points (APs) over a secure connection using Secure Sockets Layer (SSL).

You can add existing and new access points to the application, which is based on access point licensing. You assign both networks and access points to a location.

You can set up multiple locations, each with its own networks and access points, and manage them from the application. By default, an account with a free trial subscription or paid-for subscription can support up to 4,000 access points.

Service Location Concepts

Service locations, in this manual referred to simply as *locations*, are physical addresses where WiFi networks and access points are installed. In the application, these locations can include multiple Layer 2 or Layer 3 network segments.

When you set up a location with one or more WiFi networks and assign access points to that location, the application automatically assigns the networks to the pool of access points for that location. That is, you do not assign a network to an access point. The application assigns the network automatically to one or more access points, depending on the number of WiFi networks and the number of access points at the location.

You can add multiple locations, for example, for branches and remote offices, which can be in different time zones. The application integrates Google Maps to display the locations. For each location, you can monitor its health, usage, and security, as well as its WiFi networks, building, floors, and access points. You can add a building label and a floor label to an access point that you assign to a location.

The following diagram shows the location-based hierarchy of the application.

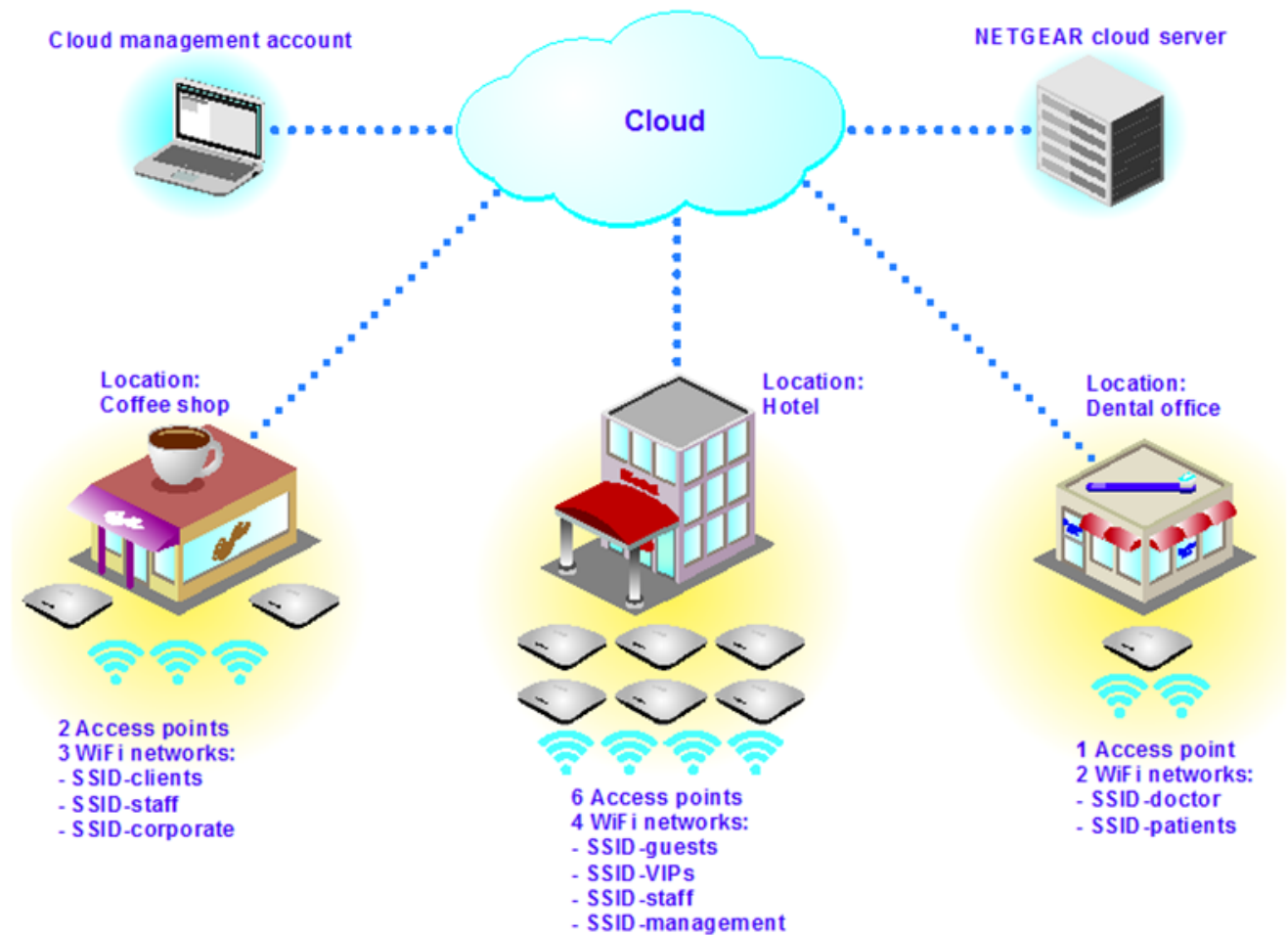


Figure 1. Locations with their access points and WiFi networks

Automatic Network Provisioning Concepts

With standalone access points, you add a WiFi network to an access point. With the application, the entire provisioning process is location based. You add a WiFi network to a location and you add an access point to the same location.

All networks configured at a location are automatically applied to all access points at that location. Typically, a single access point can support eight networks per radio. If an access point supports only a single radio, the application configures the networks only on that radio.

Optional building and floor labels can help you to organize your access points and you can group access points together by building and by floor.

Offline provisioning is possible. You can set up locations and WiFi networks while access points are offline. Then, add access points and assign them to locations, allowing the networks to go online.

Key Functions

The application provides key functions such as provisioning, configuring, managing, and monitoring.

Provisioning Functions

Provisioning lets you add locations, WiFi networks, and access points. Typically, you add a location, set up a WiFi network at the location, and bring the WiFi networks online by adding access points to the location. For more information, see [Get Started With Cloud Management](#) on page 18.

You could also start by adding access points to a temporary location and decommissioning them just to get them into inventory. (While decommissioned, access points do not use license credits.) Then, add locations, add WiFi networks to the locations, and bring the WiFi networks online by assigning the access points to the locations. For information about managing the inventory, see [Manage the Device Inventory](#) on page 77.

Configuring and Managing Functions

You can configure and manage features for each location, each WiFi network, and each access point.

Location Functions

For each location, you can configure and manage multiple features. For detailed configuration procedures, see [Manage Locations](#) on page 26, except where otherwise indicated in the following list.

You can configure and manage the following features:

- Add WiFi networks to the location.
For detailed configuration procedures, see [Manage WiFi Networks](#) on page 47.
- Add access points to the location.
For detailed configuration procedures, see [Manage Devices and Device Inventory](#) on page 68.
- Configure and manage global WiFi, access point, and security settings for the location, including the following components:
 - Automatic radio resource management (Auto RRM) for access point radios
 - Management of access point radios, including the WiFi mode, channel frequency, output power, channel bandwidth, Wi-Fi Multimedia (WMM) settings, maximum number of clients, and antenna settings
 - Radio broadcast on/off schedule
 - Access point credentials (that is, setting a global password for accessing the web management interfaces of cloud-managed access points)
 - Firmware management for access points

WiFi Network Functions

For each WiFi network that you set up at a location, you can configure and manage multiple features. For detailed configuration procedures, see [Manage WiFi Networks](#) on page 47.

You can configure and manage the following features:

- Set the security, including broadcast of the network name (SSID) and client separation for the WiFi network.
- Specify the tagged VLAN for the WiFi network.
- Select the radio (for dual-band access points) for the WiFi network.
- Manage the authentication and encryption for the WiFi network.
- Create a captive portal for free or paid-for access to the WiFi network.
- Set upload and download bandwidth caps for the WiFi network.
- Enable fast roaming for the WiFi network.
- Enable client isolation for the WiFi network.
- Set a radio broadcast on/off schedule for the WiFi network.

Access Point Functions

For each access point that you assign to a location, you can configure and manage multiple features. You can also decommission the access point from its current location and deploy it to a different location. For detailed configuration procedures, see [Manage Devices and Device Inventory](#) on page 68.

You can configure and manage the following features:

- Assign a name, building, and floor label to the access point.
- Manage the IP address settings for the access point, including the DHCP and DNS server settings.
- Configure the management VLAN (by default, VLAN 1) for the access point.
- Manage the radio settings for the access point, including the WiFi mode, channel frequency, output power, channel bandwidth, Wi-Fi Multimedia (WMM) settings, maximum number of clients, and antenna settings.

Monitoring Functions

Monitoring lets you display WiFi network and access point health; WiFi network and access point usage; WiFi network location maps; alarms and alarm trends; and statistics for networks, access points, traffic, clients, and neighboring access points. For detailed configuration procedures, see [Monitor Your Locations, Networks, and Devices](#) on page 102.

Account Management Functions

Account management lets you assign locations to license accounts, manage licenses, and invite application users (referred to as collaborators). For detailed configuration procedures, see [Manage Accounts and Licenses](#) on page 86.

Application Roles

The application supports the following roles for users who can log in to the application. These users are different from WiFi users and hotspot users who can connect to a network that is part of the cloud but who cannot log in to the application.

- **Owner.** A user who subscribed to the application and owns all license accounts that are set up under his or her application subscription. An owner can perform any action, including inviting collaborators (managers, customers, and clerks).
- **Manager.** A user who can perform most administrative functions. A manager (also referred to as a cloud network administrator) is authorized to perform many application functions for license accounts that he or she does *not* own.
Although a manager can set up his or her own new license account (and therefore become owner of that account), a manager can also access other license accounts (that is, accounts that were set up by other users) and can invite collaborators for other license accounts. However, a manager cannot add or remove a location from another license account, decommission or remove devices from a location for another license account, or entirely remove another license account.
- **Customer.** A user with read-only access to the license account to which he or she was invited, including all locations, WiFi networks, and access points that are assigned to that license account. Although a customer can set up his or her own license account (and therefore become owner of that account), a customer cannot access other license accounts to which he or she was not invited and cannot invite collaborators for other license accounts.
- **Clerk.** A user who can only sell, print, and email vouchers and monitor their use for paid-for captive portal access for the license account to which he or she was invited. A clerk is also referred to as a voucher clerk or hotspot clerk. As with other users, a clerk can set up his or her own license account (and therefore become owner of that account).

Owners, managers, customers, and clerks are referred to as collaborators.

Plan a Location With WiFi Networks and Hotspots

Before you set up a location with one or more large WiFi networks, plan accordingly and perform a site survey so that you can determine how many access points the location requires. Plan the types of network authentication and data encryption for WiFi access, the nature of hotspots, whether you need usage plans, and which user groups you must set up.

The following sections describe planning concepts:

- *Determine the Location Requirements* on page 13
- *Determine the Management VLAN* on page 13
- *Plan the Client Authentication and Data Encryption* on page 13
- *Plan the Hotspots With Free Access and Paid-For Access* on page 14
- *Other Planning Considerations* on page 14

Determine the Location Requirements

For each location, before you set up the location, configure the WiFi networks, and assign the access points, determine its requirements:

- Number of users that must be able to receive WiFi service over managed networks
- Type of security and encryption for the managed networks
- Number of users that must be able to receive WiFi service over a WiFi network or hotspot
- Type of security, encryption, and access for the WiFi network or hotspot
- Number of access points required to provide seamless coverage for all WiFi networks and hotspots through all buildings and floors of the location
- Number of licenses required to cover all access points at the location
- 802.11 frequency bands and channels that are optimal for WiFi usage

For each large location that you plan to set up, 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 clients, run a test to check connectivity between access points and clients.
- Identify potential RF obstructions and interference sources.
- Determine areas where denser coverage might be required because of heavier usage.

Determine the Management VLAN

To enable all access points at a location to connect over the Internet to the cloud, make sure that the management VLAN is set up correctly at the location and that all access points at the location use the correct management VLAN. The default management VLAN ID is ID 1. However, you can change the management VLAN for individual access points. For more information, see [Change the Management VLAN for an Access Point](#) on page 74.

Plan the Client Authentication and Data Encryption

A WiFi user must authenticate to the WiFi network to be able to access WiFi resources. A WiFi network can support several types of security methods, including those methods that require a RADIUS authentication server. The encryption option that is available depends on the authentication method that you selected. The following table lists the authentication and corresponding encryption methods that you configure through the application.

Table 1. Authentication and encryption options

Authentication Method	Type of Authentication	Encryption Options	Authentication Server
Open	None	None	None
WPA Personal	Network key (passphrase)	TKIP or TKIP+AES	None
WPA Enterprise	Shared secret (passphrase)	TKIP or TKIP+AES	RADIUS server

Plan the Hotspots With Free Access and Paid-For Access

A captive portal blocks clients from accessing a WiFi network until they are verified. Such a WiFi network is often referred to as a hotspot.

Plan the hotspots that you want to offer at a location. The type of hotspots that the application supports are hotspots that offer free access and hotspots that offer paid-for access with a voucher.

The application supports the following authentication methods for hotspots:

- **Click-through.** No authentication and no email address are required to click through to a hotspot.
- **Click-through with custom fields.** No authentication is required but other information can be required to click through to a hotspot. You can specify up to six fields to customize the required information, which can include a name, email address, mobile phone number, and so on.
- **Voucher.** A voucher number is required to sign in to a paid-for hotspot.

Note Although it is a less common approach, you could also use the voucher option to generate passwords for guest use in an office environment.

For more information, see [Add a Captive Portal for Free or Paid-For Access to a WiFi Network](#) on page 52.

Other Planning Considerations

The application functions with the following concepts:

- A WiFi network broadcasts in an entire location, not in an individual building or on a floor only.
- An access point might be configured with a label for a floor in a building at a location but carries all WiFi networks that broadcast at that location.
- All access points at a location function with the same WiFi and radio settings for that location (see [Manage WiFi Networks](#) on page 47 and [Manage the Radio and Antenna Settings for a Location](#) on page 33).

If you disable the broadcast of a WiFi network, the WiFi network stops broadcasting at the entire location. That is, you cannot stop a WiFi network from broadcasting in a particular building only or on a particular floor only. It's either on or off for the entire location. However, you can circumvent these limitations by setting up more than one location.

Business Central Wireless Manager 2.1 Application

Consider the following example:

In a single building (for example, a high-rise, multifloor tower) you want to use the application to manage the WiFi networks and hotspots through the cloud. The configuration of companies in the building varies: Some companies occupy an entire floor, some companies share a floor, and some companies occupy more than one floor. Each floor requires at least one access point and each company requires at least one WiFi network, but some floors require more access points and some companies require more WiFi networks. All companies are connected to the Internet through the same high-speed broadband WAN connection. The following three scenarios cover configuration options for the building:

- For a single company that occupies a single floor, you can do the following:
 1. Set up one location for the company.
 2. Add all access points that the company requires to the location.
 3. Add all WiFi networks that the company requires to the location.
If one or more simultaneous dual-band access points are assigned to the location, you can set up a maximum of 16 WiFi networks for the location.
- For a single company that occupies several floors, you can do the following:
 1. Set up one location for the company.
 2. Add all access points that the company requires to the location.
If the company is spread out over floors that are not adjacent, you must set up at least one access point per floor.
 3. Add floor labels to the access points.
Each floor label can represent the floor on which access points are located. Floor labels allow you to organize the access points by floors.
 4. Add all WiFi networks that the company requires to the location.
If the company is spread out over floors that are not adjacent, you must set up at least one WiFi network per floor.
If one or more simultaneous dual-band access points are assigned to the location, you can set up a maximum of 16 WiFi networks for the location.
- For different companies that share a single floor, you can do the following:
 1. Set up one location for the floor.
 2. Add a sufficient number of access points to the location so that the WiFi requirements for all companies on the floor are covered.
 3. For each company on the floor, add one or more WiFi networks to the location.
If one or more simultaneous dual-band access points are assigned to the location, you can set up a maximum of 16 WiFi networks for the location.

Compatible NETGEAR WiFi Access Points

Before the application can manage an access point, the access point must run the required firmware version that is cloud enabled. This release supports the following NETGEAR WiFi access points running cloud-enabled firmware:

- WAC730 ProSAFE 3x3 Dual-Band Wireless AC Access Point
- WAC720 ProSAFE 2x2 Dual-Band Wireless AC Access Point
- WNDAP660 ProSAFE Dual-Band Wireless-N Access Point
- 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

The following table lists the minimum required standalone firmware version that an access point must run for you to be able to upgrade the access point to the required cloud-enabled firmware version.

Table 2. Firmware requirements for upgrade to the cloud-enabled firmware version

Access Point Model	Minimum Required Standalone Firmware for Upgrade to Cloud-Enabled Firmware	Required Cloud-Enabled Firmware
WAC730 ProSAFE 3x3 Dual-Band Wireless AC Access Point	v3.1.1.0 or a later standalone version	v3.5.6.0 or later
WAC720 ProSAFE 2x2 Dual-Band Wireless AC Access Point	v3.1.1.0 or a later standalone version	v3.5.6.0 or later
WNDAP660 ProSAFE Dual Band Wireless-N Access Point	v2.0.5 or a later standalone version	v3.5.5.0 or later
WNDAP360 ProSAFE Dual Band Wireless-N Access Point	v2.1.12 or a later standalone version	v3.5.5.0 or later
WNDAP350 ProSAFE Dual Band Wireless-N Access Point	v2.1.9 or a later standalone version	v3.5.5.0 or later
WNAP320 ProSAFE Wireless-N Access Point	v2.1.6 or a later standalone version	v3.5.5.0 or later
WNAP210v2 ProSAFE Wireless-N Access Point	v2.1.5 or a later standalone version	v3.5.5.0 or later

If your access point runs a standalone firmware version that is earlier than the minimum required standalone firmware version, you first must upgrade the access point to the minimum required standalone firmware version *before* you can upgrade the access point to the required cloud-enabled firmware version.



CAUTION:

If you do not first upgrade to the minimum required standalone firmware version but attempt to upgrade directly to the required cloud-enabled firmware version, you might be locked out of the access point. In that situation, you must log in to the access point over an SSH connection with the user name **admin** and the password that is configured for the access point and issue the **restore-factory-default** command to reset the access point to factory default settings.

If your access point runs the minimum required standalone firmware version, you must load the required cloud-enabled firmware version onto the access point. Using the web management interface of the access

point, upgrade the access point to the cloud-enabled firmware version, and reset the access point to factory default settings. For more information about preparing your access points for cloud management, see the NETGEAR *Business Central Wireless Manager How to Start Guide*, which you can download from downloadcenter.netgear.com.

Once you perform the one-time cloud-enabled firmware upgrade for the access point, the application can centrally manage future firmware upgrades for the cloud-managed access point.

Note For more information about cloud-managed access points, see *Manage Devices and Device Inventory* on page 68.

Definitions of Access Point Terms

This manual uses the following definitions of access point terms:

- **Cloud-managed access point.** A NETGEAR access point that is installed at a location and is controlled by the application.
- **Neighbor access point.** An access point that is within the radio range of and discovered by a cloud-managed access point. The access point can be another cloud managed access point or an access point that is not cloud managed. The access point can be known, unknown, or rogue.
- **Rogue access point.** An access point that is broadcasting an SSID that is identical to the SSID of a cloud-managed access point. This type of rogue access point is also referred to as an evil twin. However, a cloud-managed access point can be rogue if it is deployed at another location or belongs to another user.
- **Known AP.** Either a NETGEAR access point that is cloud managed and that the application automatically classified as a known access point or another access point that is not cloud managed and that you or a collaborator classified as a known access point.
- **Unknown AP.** An unknown access point that is within the radio range of and discovered by a cloud managed access point and that you or a collaborator could mark as a known access point. A cloud-managed access point can be unknown if it is deployed at another location or belongs to another user.

Before you can manage WiFi networks in the cloud, you must set up a least one location, add one or more WiFi networks to the location, and add one or more access points to the location.

This chapter includes the following sections:

- *Add Your First Location* on page 19
- *Add a First WiFi Network to a Location* on page 20
- *Add a First Access Point to a Location* on page 23

Note For information about preparing your access points and subscribing to the BCWM application, see the NETGEAR *Business Central Wireless Manager How to Start Guide*, which you can download from downloadcenter.netgear.com.

Add Your First Location

Before you can add WiFi networks and access points, you must set up at least one location. For access points (and therefore WiFi networks) to become active, you must assign the location to a license account.

► To add your first location and assign it to a license account:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays and does not yet show any locations.
5. Click the **+ New Location** button.

The screenshot shows the 'Add a new Location' form with the following fields and steps:

- Step 1:** Search for the location you would like to add by its name or address. Location Search: Enter a name or address.
- Step 2:** Select the country for this location. Country: Select a country.
- Step 3:** Enter the details for your new location. Location Name, Contact Full Name, Contact Email.
- Step 4:** Enter the credentials to be used for devices at this location. Device Username: admin, Device Password: [password field with eye icon].
- Step 5:** Select an account for this location. Account: Select an account.

Buttons: Cancel, Save.

6. In the **Location Search** field, enter a name or address and select the location that Google search generates.
The location displays on the map.
7. Make sure that the correct country is selected from the **Country** menu.
When you complete the **Location Search** field, the country is automatically selected from the **Country** menu.
The selection from the **Country** menu determines the radio settings for access points at the location. Once the location is created, you cannot change the country selection.

Business Central Wireless Manager 2.1 Application

8. Enter the location name, contact name, and contact email address that you want to be associated with the location.
9. In the **Device Password** field, enter the password for accessing the web management interface of any cloud-managed access point that is assigned to the location.
Click the eye icon to make the password visible.

This password is pushed to all access points that you assign to the location.

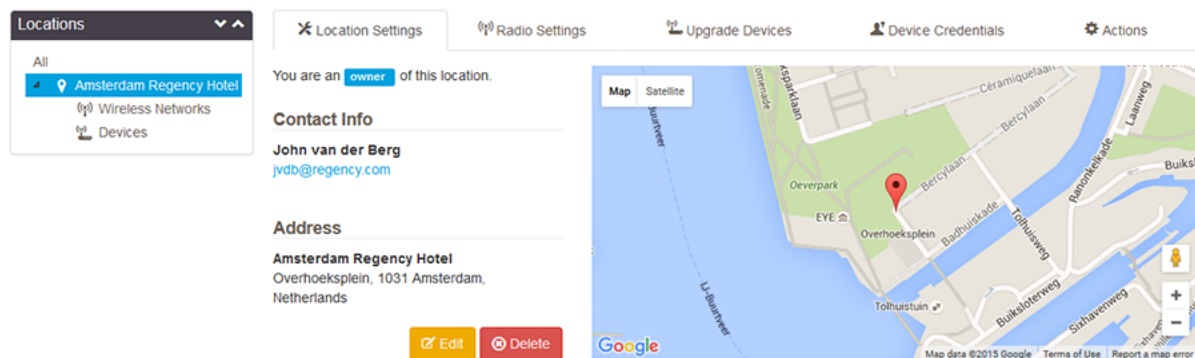
Note The Device Username field shows the fixed user name (**admin**) for accessing the web management interface of any cloud-managed access point that is assigned to the location. You cannot change this name.

10. From the **Account** menu, select the account to which the location must be assigned.

An account is a set of locations that are funded by the same license. Each location must be assigned to an account with an active license (which can be a trial license) for access points to be licensed and active. The **Accounts** menu lists the available license accounts. If you did not create a license account, only the default license account is available from the menu.

11. Click the **Save** button.

Your settings are saved. The location displays in the Locations tree on the left. Below the location in the tree, the **Wireless Networks** and **Devices** headings display.



Add a First WiFi Network to a Location

When you add a location (see [Add Your First Location](#) on page 19), the application automatically adds a **WiFi Networks** heading for the location in the Locations tree on the Configuration page, but you must define one or more WiFi networks that can broadcast at the location.

► To add a first WiFi network to a location:

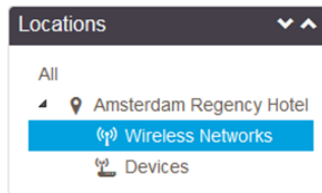
1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

Business Central Wireless Manager 2.1 Application

4. Select **Configuration**.

The Configuration page displays and shows the location that you added (see [Add Your First Location](#) on page 19).

5. In the Locations tree, click **Wireless Networks**.



The page displays the following message: There are no wireless networks configured for this location.

6. Click the **+ New Wireless Network** button.

7. In the **SSID** field, enter a WiFi network name (SSID).

You can use up to and including 32 ASCII printable (typeable) characters. Do not use extended ASCII characters, control ASCII characters, or ASCII characters that you compose with the Alt key on your keyboard.

By default, the application broadcasts the SSID. If you want to hide the SSID so that only users who know the SSID can access it, clear the **Broadcast SSID** check box.

8. From the **Bands** menu, select the WiFi band or bands.

The default setting is **2.4GHz and 5.0GHz Radios**, which applies to dual-band access points only. If an access point supports a single band only, the access point broadcasts on that band, unless your selection from the **Bands** menu disables that band.

9. To specify a tagged VLAN, select the **Specify a tagged VLAN** check box, and in the **VLAN ID** field, enter the VLAN ID.

Business Central Wireless Manager 2.1 Application

The VLAN ID is a 12-bit number that identifies the tagged VLAN. If the connection from the access points to the Internet gateway requires an IEEE 802.1Q VLAN tag, you must specify a VLAN ID. If multiple WiFi networks operate over the same physical Ethernet link, VLANs can provide isolation and separation.

10. From the **Authentication Type** menu, select the type of authentication:

- **Open.** You do not need to specify any additional information because the network functions without authentication and encryption.
- **WPA Personal.** In the **Password** field, you must specify the password that is required to access the network. You can enter up to 63 alphanumeric and special characters. The default encryption method is TKIP+AES, but you can select the **Change Data Encryption** check box and, from the **Data Encryption** menu, select **TKIP**.
- **WPA Enterprise.** You must specify a RADIUS profile and the network must be connected to a RADIUS server. For more information, see [Change the Authentication and Encryption for a WiFi Network](#) on page 49.

11. To assign a captive portal to the WiFi network, click the **+Add a Captive Portal** button.

For information about configuring a captive portal, see [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53.

12. To specify bandwidth caps, select the **Enable Bandwidth Caps** check box and adjust the upload and download bandwidth caps.

By default, the upload and download bandwidth caps are 1000 Kbps each. For each type of bandwidth cap, the minimum value is 64 Kbps and the maximum value is 10 Gbps.

13. If you select **WPA Personal** (with TKIP + AES) or **WPA Enterprise** from the **Authentication Type** menu, you can configure fast roaming (802.11r) for the WAC720 and WAC730 access points by doing the following:

a. Select the **Enable Fast Roaming** check box.

For more information about fast roaming and associated restrictions, see [Enable Fast Roaming for a WiFi Network](#) on page 63.

If you select the **Enable Fast Roaming** check box, the **Exchange Fast Roaming Info Over Wired Network** check box displays.

b. To enable fast roaming information to be exchanged over the wired network, select the **Exchange Fast Roaming Info Over Wired Network** check box.

If you enable fast roaming, by default, fast roaming information is exchanged over the WiFi network instead of the wired network.

14. To enable client isolation, select the **Enable Client Isolation** check box.

Note Enabling client isolation on a WiFi network for a location with 802.11ac access points enables client isolation for all WiFi networks for those access points.

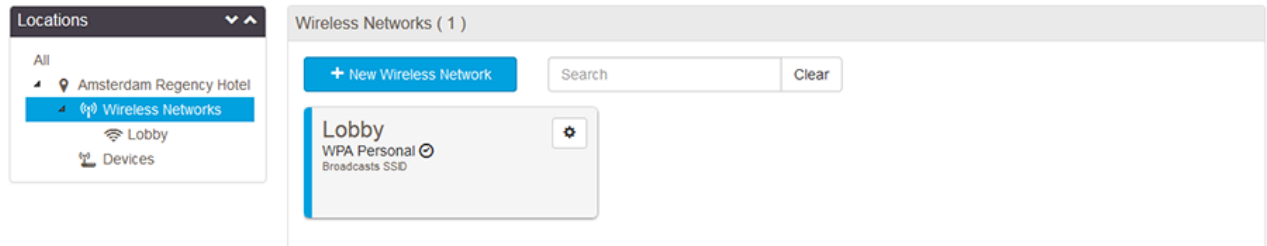
15. To set up a radio on/off broadcast schedule, select the **Create Schedule** check box.

Business Central Wireless Manager 2.1 Application

For information about configuring a radio on/off broadcast schedule, see [Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network](#) on page 65.

16. Click the **Save** button.

Your settings are saved. In the Locations tree on the left, the WiFi network displays under the **Wireless Networks** heading for the location.



Add a First Access Point to a Location

When you add a location (see [Add Your First Location](#) on page 19), the application automatically adds a **Devices** heading for the location in the Locations tree on the Configuration page, but you must add at least one access point that can carry the WiFi networks that you configure at the location.



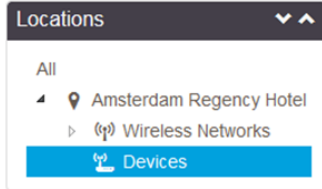
CAUTION:

If you add an access point to a location but do not add a WiFi network to the location, the access point continues to broadcast its default SSIDs and provides open networks without any security. Make sure that you add a WiFi network to the location (see [Add a First WiFi Network to a Location](#) on page 20) so that you can control WiFi security.

► **To add a first access point to a location:**

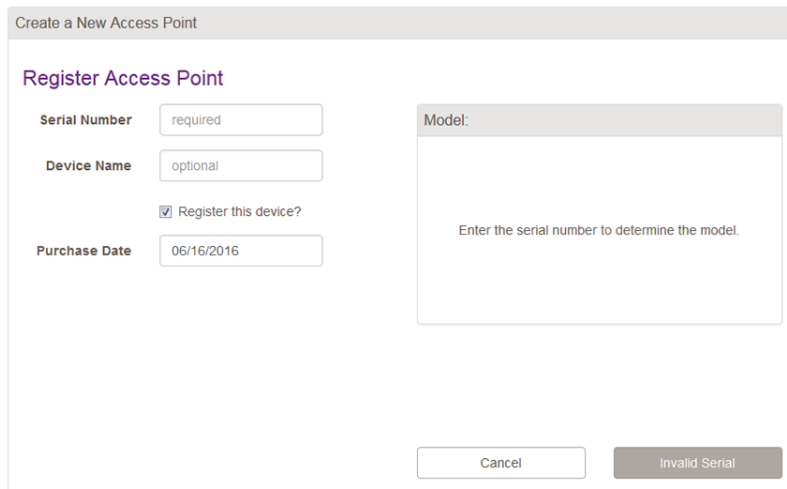
1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays and shows the location that you added (see [Add Your First Location](#) on page 19).

5. In the Locations tree, click **Devices**.



The page displays the following message: There are no devices configured for this location.

6. Click the **+ New Device** button.



7. In the **Serial Number** field, enter the precise serial number for the access point.
If you do not enter a correct serial number, you cannot add the access point to the network. After you enter a correct serial number, an image of the associated model displays in the **Model** field, and the gray **Invalid Serial** button changes into the **Save** button.
8. In the **Device Name** field, enter a name for the access point.
The name does not need to be the factory default name.
9. To register the access point with NETGEAR, keep the **Register this device** check box selected and enter your date of purchase in the **Purchase Date** field.
By default, the **Register this device** check box is selected. If you do not need or want to register the access point, clear the check box.
10. Click the **Save** button.
Your settings are saved. In the Locations tree on the left, the access point displays under the **Devices** heading for the location.

Business Central Wireless Manager 2.1 Application

Note the following about access point states:

- If the access point is not connected to the Internet, the application displays the status Waiting.
- If the location to which you added the access point is assigned to an unlicensed account, the access point displays the status Unlicensed and does not become active until you add a license to the account (see [Add a License to an Account](#) on page 90).

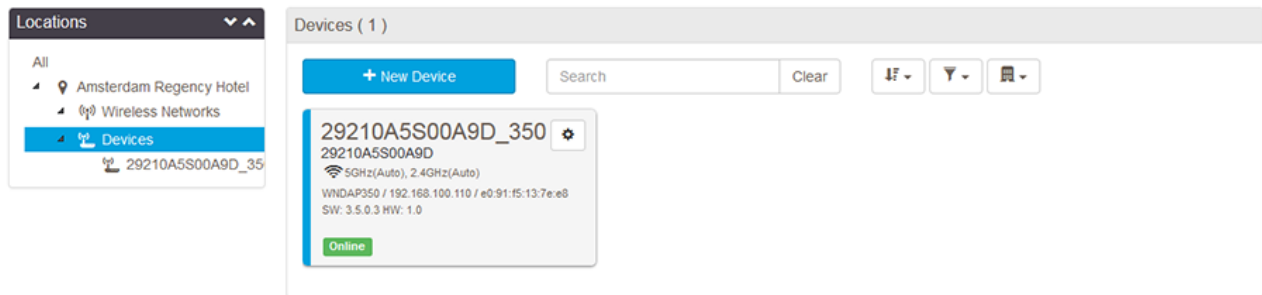


CAUTION:

If an access point remains unlicensed and is not active, it broadcasts its default SSIDs and provides open networks without any security. Make sure that the account to which you assigned the location is licensed so that the access point becomes active.

- If the access point is connected to the Internet and connects to the application for the first time, it might take between 5 and 10 minutes before the access point is connected and the application displays the status Online. During this period, the application might need to push the latest firmware to the access point, automatically reboot the access point, push the configuration to the access point, and automatically reboot the access point again.

The following figure shows the status Online.



Locations form the key building blocks of your cloud network. You can set up new and manage existing locations, add WiFi networks and access points to a location, manage radio settings for a location, and manage firmware and device credentials for all access points assigned to a location.

This chapter includes the following sections:

- [Add a Location](#) on page 27
- [Add a WiFi Network to a Location](#) on page 28
- [Add an Access Point to a Location](#) on page 31
- [Change the Basic Settings for a Location](#) on page 33
- [Manage the Radio and Antenna Settings for a Location](#) on page 33
- [Run or Schedule Automatic Radio Frequency Management for a Location](#) on page 36
- [Manage Load Balancing for a Location](#) on page 38
- [Upgrade Firmware on Devices at a Location](#) on page 40
- [Reboot a Location](#) on page 44
- [Change the Device Credentials for a Location](#) on page 45
- [Remove a Location](#) on page 46

Note For information about moving a location from one account to another account, see [Remove a Location From an Account](#) on page 94 and [Add a Location to an Account](#) on page 93.

Add a Location

A location is a physical address where WiFi networks and access points are installed. You can add multiple locations, for example, for branches and remote offices.

► **To add a location and assign it to a license account.**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. Click the **+ New Location** button.

Add a new Location

Step 1: Search for the location you would like to add by its name or address.

Location Search

Step 2: Select the country for this location.

Country

Step 3: Enter the details for your new location.

Location Name

Contact Full Name

Contact Email

Step 4: Enter the credentials to be used for devices at this location.

Device Username

Device Password

Step 5: Select an account for this location.

Account

6. In the **Location Search** field, enter a name or address and select the location that Google search generates.
The location displays on the map.
7. Make sure that the correct country is selected from the **Country** menu.
When you complete the **Location Search** field, the country is automatically selected from the **Country** menu.

The selection from the **Country** menu determines the radio settings for access points at the location. Once the location is created, you cannot change the country selection.

Business Central Wireless Manager 2.1 Application

8. Enter the location name, contact name, and contact email address that you want to be associated with the location.
9. In the **Device Password** field, enter the password for accessing the web management interface of any cloud-managed access point that is assigned to the location.
Click the eye icon to make the password visible.

This password is pushed to all access points that you assign to the location.

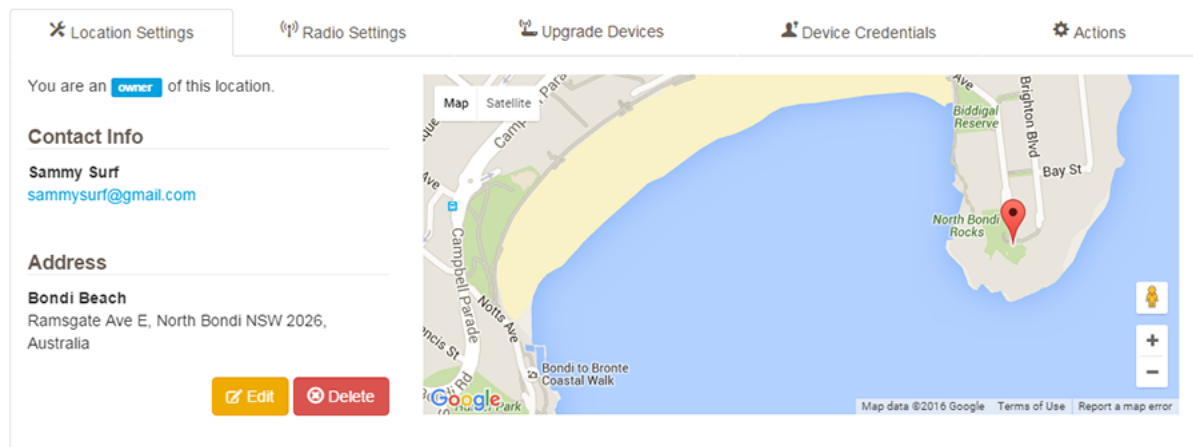
Note The Device Username field shows the fixed user name (**admin**) for accessing the web management interface of any cloud-managed access point that is assigned to the location. You cannot change this name.

10. From the **Account** menu, select the account to which the location must be assigned.

An account is a set of locations that are funded by the same license. Each location must be assigned to an account with an active license (which can be a trial license) for access points to be licensed and active. The **Accounts** menu lists the available license accounts. If you did not create a license account, only the default license account is available from the menu.

11. Click the **Save** button.

Your settings are saved. The location displays in the Locations tree on the left. Below the location in the tree, the **Wireless Networks** and **Devices** headings display.



Add a WiFi Network to a Location

You can add a WiFi network to a location. The WiFi network becomes active only after you add one or more access points to the location, the location is added to a license account, and the access points are in the active connected state.

► To add a WiFi network to a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.

Manage Locations

Business Central Wireless Manager 2.1 Application

3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. From the **Actions** menu, select **+ Add Wireless Network**.

Create a New Wireless Network

Advertisement

☒ Broadcast SSID?

SSID

Bands

☐ Specify a tagged VLAN

Authentication

Authentication Type

Captive Portal

[+ Add a Captive Portal](#)

Advanced Settings

☐ Enable Bandwidth Caps

☐ Enable Client Isolation

☐ Create Schedule

7. In the **SSID** field, enter a WiFi network name (SSID).
By default, the application broadcasts the SSID. If you want to hide the SSID so that only users who know the SSID can access it, clear the **Broadcast SSID** check box.
8. From the **Bands** menu, select the WiFi band or bands.
The options are **2.4GHz and 5.0GHz Radios**, **2.4GHz Radio only**, and **5.0GHz Radio only**. The default setting is **2.4GHz and 5.0GHz Radios**, which applies to dual-band access points only. If an access point supports a single band only, the access point broadcasts on that band, unless your selection from the **Bands** menu disables that band.
9. To specify a tagged VLAN, select the **Specify a tagged VLAN** check box, and in the **VLAN ID** field, enter the VLAN ID.
The VLAN ID is a 12-bit number that identifies the tagged VLAN. If the connection from the access point to the Internet gateway requires an IEEE 802.1Q VLAN tag, you must specify a VLAN ID. If multiple WiFi networks operate over the same physical Ethernet link, VLANs can provide isolation and separation.

Manage Locations

10. From the **Authentication Type** menu, select the type of authentication:

- **Open.** You do not need to specify any additional information because the network functions without authentication and encryption.
- **WPA Personal.** In the **Password** field, you must specify the password that is required to access the network. You can enter up to 63 alphanumeric and special characters. The default encryption method is TKIP+AES, but you can select the **Change Data Encryption** check box and, from the **Data Encryption** menu, select **TKIP**.
- **WPA Enterprise.** You must specify a RADIUS profile and the network must be connected to a RADIUS server. For more information about WPA Enterprise, see [Change the Authentication and Encryption for a WiFi Network](#) on page 49.

11. To assign a captive portal to the WiFi network, click the **+Add a Captive Portal** button.

For information about configuring a captive portal, see [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53.

12. To specify bandwidth caps, select the **Enable Bandwidth Caps** check box and adjust the upload and download bandwidth caps.

By default, the upload and download bandwidth caps are 1000 Kbps each. For each type of bandwidth cap, the minimum value is 64 Kbps and the maximum value is 10 Gbps.

13. To enable client isolation, select the **Enable Client Isolation** check box.

Note Enabling client isolation on a WiFi network for a location with 802.11ac access points enables client isolation for all WiFi networks for those access points.

14. If you select **WPA Personal** (with TKIP + AES) or **WPA Enterprise** from the **Authentication Type** menu, you can configure fast roaming (802.11r) for the WAC720 and WAC730 access points by doing the following:

a. Select the **Enable Fast Roaming** check box.

Although you can configure fast roaming regardless of the access points that you are deploying at a location, fast roaming applies only to the WAC720 and WAC730 access points and to clients that support fast roaming. If you enable fast roaming for a WiFi network that is broadcast on a WAC720 or WAC730 access point only, a client that does not support fast roaming cannot connect to the WiFi network. In such a situation, you could set up an additional WiFi network without fast roaming to serve the clients that do not support fast roaming.

If you select the **Enable Fast Roaming** check box, the **Exchange Fast Roaming Info Over Wired Network** check box displays.

b. To enable fast roaming information to be exchanged over the wired network instead of the WiFi network, select the **Exchange Fast Roaming Info Over Wired Network** check box.

The default setting is that fast roaming information is exchanged over the WiFi network instead of the wired network.

15. To set up a radio on/off broadcast schedule, select the **Create Schedule** check box.

For information about configuring a radio on/off broadcast schedule, see [Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network](#) on page 65.

16. Click the **Save** button.

Your settings are saved. In the Locations tree on the left, the WiFi network displays under the **Wireless Networks** heading for the location.

Add an Access Point to a Location

You can add an access point to location. The location must be assigned to a license account with an active license (see [Add a License to an Account](#) on page 90). Otherwise, the access point that you add remains in the unlicensed state and does not become active (which means that it broadcasts its default SSIDs and provides open networks without any security), preventing WiFi networks that you add to the location from coming up.



CAUTION:

If you add an access point to a location but do not add a WiFi network to the location, the access point continues to broadcast its default SSIDs and provides open networks without any security. Make sure that you add a WiFi network to the location (see [Add a WiFi Network to a Location](#) on page 28) so that you can control WiFi security.

► To add an access point to a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.

6. From the **Actions** menu, select **+ Add Device**.

Create a New Access Point

Register Access Point

Serial Number required

Device Name optional

☒ Register this device?

Purchase Date 06/16/2016

Model:

Enter the serial number to determine the model.

Cancel Invalid Serial

7. In the **Serial Number** field, enter the precise serial number for the access point.
If you do not enter a correct serial number, you cannot add the access point to the network. After you enter a correct serial number, an image of the associated model displays in the **Model** field, and the gray **Invalid Serial** button changes into the **Save** button.
8. In the **Device Name** field, enter a name for the access point.
The name does not need to be the factory default name.
9. To register the access point with NETGEAR, keep the **Register this device** check box selected and enter your date of purchase in the **Purchase Date** field.
By default, the **Register this device** check box is selected. If you do not need or want to register the access point, clear the check box.
10. Click the **Save** button.
Your settings are saved. In the Locations tree on the left, the access point displays under the **Devices** heading for the location.

Note the following about access point states (see [View the Access Point Inventory and Connection Status in the Application](#) on page 148):

- If the access point is not connected to the Internet, the application displays the status **Waiting**.
- If the location to which you added the access point is assigned to an unlicensed account, the access point displays the status **Unlicensed** and does not become active until you add a license to the account (see [Add a License to an Account](#) on page 90).



CAUTION:

If an access point remains unlicensed and is not active, it broadcasts its default SSIDs and provides open networks without any security. Make sure that the account to which you assigned the location is licensed so that the access point becomes active.

- If the access point is connected to the Internet and connects to the application for the first time, it might take between 5 and 10 minutes before the access point is connected and the application displays the status Online. During this period, the application might need to push the latest firmware to the access point, automatically reboot the access point, push the configuration to the access point, and automatically reboot the access point again.

Change the Basic Settings for a Location

You can change the basic settings for a location. These settings include the location address, location name, contact name, and contact email, and the access point credentials for the location (the device password).

► To change the settings for a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the orange **Edit** button.
The page adjusts and the fields become editable.
7. Change the information as needed.
8. Click the **Save** button.
Your settings are saved.

Manage the Radio and Antenna Settings for a Location

You can manage the radio settings that apply to all access points that are assigned to a location. The default settings often work well but situations might occur in which you want to change the settings. Managing the radio settings includes enabling or disabling a radio, changing the WiFi mode, changing the WiFi channel, changing the WiFi bandwidth, changing the transmission output power, changing the Wi-Fi Multimedia

Business Central Wireless Manager 2.1 Application

(WMM) settings, changing the maximum number of supported clients, and specifying the default internal or optional external antenna.

Note For information about managing the radio settings for an individual access point, see *Change the Radio and WiFi Settings for a Device* on page 70.

► To manage the radio settings for a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the **Radio Settings** tab.
The Configuration page displays the common radio settings.
7. Click the **Edit Radios** button.

The screenshot displays the 'Radio Settings' tab in the Business Central Wireless Manager 2.1 application. At the top, there are navigation tabs: 'Location Settings', 'Radio Settings' (selected), 'Upgrade Devices', 'Device Credentials', and 'Actions'. Below the tabs, there's a 'Radio Settings' section with a 'Save' button and a 'Cancel' button. A message indicates '* Radio has been modified'. The main part of the page is a table with columns: Access Point, Radio, Enabled, Band, Mode, Channel, Power, Bandwidth, WMM Mode, WMM Power Save, Max Clients, and Antenna. There are four rows of radio settings for different access points. Below the table, it says '4 Radios' and 'Country:'. The 'Auto RF' section is also visible, containing 'Channel Allocation' and 'Run Auto RF' options.

Access Point	Radio	Enabled	Band	Mode	Channel	Power	Bandwidth	WMM Mode	WMM Power Save	Max Clients	Antenna
29215A5W003C0 (BB_350_1)	WLAN0	☒	2.4GHz	g-n	Auto (1)	Full	Dynami	Yes	No	50	Internal
29215A5W003C0 (BB_350_1)	WLAN1	☒	5GHz	a-n	Auto (153)	Full	Dynami	Yes	No	50	Internal
200244NC0001A (BB_660_1)	WLAN0	☒	2.4GHz	g-n	Auto (6)	Full	Dynami	Yes	No	128	Internal
200244NC0001A (BB_660_1)	WLAN1	☒	5GHz	a-n	Auto (36)	Full	Dynami	Yes	No	128	Internal

4 Radios

Country:

Auto RF

Channel Allocation

	1	2	3	4	5	6	7	8	9	10	11
2.4GHz	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
5GHz	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Run Auto RF

☒ Run Auto RF Now

Schedule Auto RF

Run Auto RF:

Timezone: Australia/Sydney

For information about using automatic radio frequency (Auto RF) management, see *Run or Schedule Automatic Radio Frequency Management for a Location* on page 36.

Manage Locations

8. Change the settings:

- **Radio.** A nonconfigurable field that shows the radio number (WLAN0 or WLAN1) for the access point.
- **Enabled.** By default, the radio is enabled. To disable the radio, clear the check box.
- **Band.** A nonconfigurable field that shows the radio band that is associated with the WiFi mode.
- **Mode.** From the menu, select the WiFi mode for the radio. By default, the most advanced WiFi mode is selected.
- **Channel.** You can select a static channel from the menu. The supported channels depend on the region of operation for the access point. By default, cloud-managed access points autoconfigure their channels (that is, the channel setting is **Auto**).
- **Power.** By default, the transmission output for an access point is set to maximum power. From the menu, you can select a lower output power for each WiFi band that the access point supports. The supported output options are **Full, Half, Quarter, Eighth, Minimum**.
- **Bandwidth.** From the menu, select the WiFi bandwidth, which is also referred to as the channel width. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz. The supported WiFi bandwidths depend on the access point model.
- **WMM Mode.** By default, WMM is enabled, allowing time-dependent WiFi traffic such as video and audio to receive a higher priority than data WiFi traffic. You can disable WMM.
- **WMM Power Save.** By default, the WMM Power Save feature is enabled, increasing the efficiency and flexibility of data transmission and thereby allowing battery-powered equipment to save power. You can disable the WMM Power Save feature.
- **Max Clients.** A radio on a NETGEAR access point can typically support between 64 and 128 clients. However, allowing the maximum number of clients might not be the most suitable configuration for a site with a large number of clients. To prevent oversubscription and congestion and to improve throughput and latency, in the Max Clients column, for each radio, use the up and down arrows to specify the maximum number of allowed clients, or type a number in the field. For more information, see [Manage Load Balancing for a Location](#) on page 38.
- **Antenna.** By default, the setting is Internal. External antennas are optional accessories. If you select **External**, the configuration takes effect only if the access point is configured with one or more external antennas.

9. Click the **Save** button.

A pop-up window opens and displays a warning.

10. Click the **Save** button in the pop-up window.

Your settings are saved. Connected clients lose their connection momentarily while the access points reprograms their settings.

11. Click the **Dismiss** button.

The pop-up window closes.

Run or Schedule Automatic Radio Frequency Management for a Location

You can manage the radio settings that apply to all access points that are assigned to a location by running automatic radio frequency (Auto RF) management, which is also referred to as automatic radio resource management (Auto RRM). Auto RF management attempts to configure the optimum radio settings for the access points. You can either allocate all available channels to participate in Auto RF management or select specific channels only. You can run Auto RF management immediately or schedule it to run at time when you expect minimal WiFi traffic. (Running Auto RF management causes connected clients to momentarily lose connection.)

Note For information about managing the radio settings for an individual access point, see *Change the Radio and WiFi Settings for a Device* on page 70.

► To run or schedule Auto RF management for a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the **Radio Settings** tab.
The Configuration page displays the common radio settings.

Business Central Wireless Manager 2.1 Application

7. Click the **Edit Radios** button.

Radio Settings

Save Cancel * = Radio has been modified

Access Point	Radio	Enabled	Band	Mode	Channel	Power	Bandwidth	WMM Mode	WMM Power Save	Max Clients	Antenna
29210ASW003C0 (BB_350_1)	WLAN0	☒	2.4GHz	g-n	Auto (1)	Full	Dynami	Yes	No	50	Internal
29210ASW003C0 (BB_350_1)	WLAN1	☒	5GHz	a-n	Auto (153)	Full	Dynami	Yes	No	50	Internal
200244NC0001A (BB_660_1)	WLAN0	☒	2.4GHz	g-n	Auto (6)	Full	Dynami	Yes	No	128	Internal
200244NC0001A (BB_660_1)	WLAN1	☒	5GHz	a-n	Auto (36)	Full	Dynami	Yes	No	128	Internal

4 Radios Country:

Auto RF

Channel Allocation

	1	2	3	4	5	6	7	8	9	10	11
2.4GHz	All ☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
5GHz	36 ☒	40 ☒	44 ☒	48 ☒	153 ☒	157 ☒	161 ☒	165 ☒			

Run Auto RF [Run Auto RF Now](#)

Schedule Auto RF

Run Auto RF:

[Remove Schedule](#) [Save Schedule](#)

Timezone: Australia/Sydney

For information about manually changing the radio and WiFi settings for a location, see [Change the Radio and WiFi Settings for a Device](#) on page 70.

8. To allocate the channels that must participate in Auto RF management, do the following:
- To select or clear all available channels, click the **All** link under 2.4GHz, the **All** link under 5GHz, or both. By default, all available channels are selected, so the first time that you click an **All** link, all channels in the radio band are cleared.
 - To select or clear an individual channel, select or clear the check box that is associated with the channel.
9. To run Auto RF management immediately, do the following:
- Click the **Auto RF** button.
A pop-up window opens and displays a warning.
- 

WARNING:
Clients are disconnected when Auto RF management runs.
- Click the **Save** button.
Auto RF management runs and the new settings are saved.
 - Click the **Dismiss** button.

The pop-up window closes.

10. To schedule Auto RF management to run at a particular time, do the following:

- a.** Under Schedule Auto RF, click the Run Auto RF **Never** button.
A pop-up window displays a seven-day schedule.
- b.** Select the check boxes for the days on which you want Auto RF management to run, or select the **Every Day** check box.
A time field displays.
- c.** Click the time field.
The pop-up window with the seven-day schedule closes and another pop-up window displays options to specify a time.
- d.** Specify the time at which Auto RF management must run on the days that you selected.
Specify a time at which you expect a minimum number of clients to connect to the WiFi networks at the location, for example, 4 a.m.
- e.** To close the pop-up window, click the **x** icon in the pop-up window.
- f.** Click the **Save Schedule** button.
Your settings are saved. If the configuration was successful, the page displays the message *Successfully saved schedule*.
- g.** To remove the schedule and define another one, click the **Remove Schedule** button and repeat *Step a* through *Step f*.

Manage Load Balancing for a Location

All WiFi networks configured at a location are automatically applied to all access points at that location and therefore to all available radios at that location. Typically, a single access point can support eight networks per radio. If an access point supports only a single radio, the application configures the networks only on that radio.

By default, each access point supports the maximum number of clients that it is capable of. A radio on a NETGEAR access point can typically support between 64 and 128 clients. However, allowing the maximum number of clients might not be the most suitable configuration for a site with a large number of clients. You can decrease the maximum number of allowed clients to prevent oversubscription and congestion and to improve throughput and latency.

When you balance the client load over different types of access points at a location, take considerations such as the following into account:

- The total number of access points at the location
- The types of access points at the location
- The buildings and floors on which the access points are installed
- The number of expected clients at each building and floor

Business Central Wireless Manager 2.1 Application

► To manage load balancing for a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the **Radio Settings** tab.
The Configuration page displays the common radio settings.
7. Click the **Edit Radios** button.

Radio Settings

Save Cancel

* Radio has been modified

Access Point	Radio	Enabled	Band	Mode	Channel	Power	Bandwidth	WMM Mode	WMM Power Save	Max Clients	Antenna
29210A5W003C0 (BB_350_1)	WLAN0	☒	2.4GHz	g-n	Auto (1)	Full	Dynami	Yes	No	50	Internal
29210A5W003C0 (BB_350_1)	WLAN1	☒	5GHz	a-n	Auto (153)	Full	Dynami	Yes	No	50	Internal
20Q244NC0001A (BB_660_1)	WLAN0	☒	2.4GHz	g-n	Auto (6)	Full	Dynami	Yes	No	128	Internal
20Q244NC0001A (BB_660_1)	WLAN1	☒	5GHz	a-n	Auto (36)	Full	Dynami	Yes	No	128	Internal

4 Radios

Country:

Auto RF

Channel Allocation

	1	2	3	4	5	6	7	8	9	10	11
2.4GHz	All ☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
5GHz	36 ☒	40 ☒	44 ☒	48 ☒	153 ☒	157 ☒	161 ☒	165 ☒			

Run Auto RF

Run Auto RF Now

Schedule Auto RF

Run Auto RF: Never

Remove Schedule Save Schedule

Timezone: Australia/Sydney

8. In the Max Clients column, for each radio, use the up and down arrows to specify the maximum number of allowed clients, or type a number in the field.
The maximum number of clients that a radio can support is stated to the right of the field in which you can specify the number.
9. Click the **Save** button.
A pop-up window opens and displays a warning.
10. Click the **Save** button in the pop-up window.

Manage Locations

Your settings are saved. Connected clients lose their connection momentarily while the access points reprograms their settings.

11. Click the **Dismiss** button.

The pop-up window closes.

Upgrade Firmware on Devices at a Location

You can upgrade the firmware on one or several types of devices (that is, access point models) at a location. For each selected access point model, the firmware is upgraded for all access points of that model at the location.

You can upgrade the firmware immediately or schedule a firmware upgrade at time when you expect minimal WiFi traffic. (The firmware upgrade takes about four minutes, causing connected clients to lose connection during that period.)

For each access point model that you want to upgrade, either select to always upgrade to the latest firmware version when a new version is released or select a specific firmware version to upgrade to. For more information, see the following sections:

- *Upgrade Devices at a Location to a Specific Firmware Version* on page 40
- *Schedule to Upgrade Devices at a Location to the Latest Firmware Version* on page 42

If you scheduled a firmware upgrade, the upgrade occurs for major firmware releases only. The release designation consists of four digits separated by dots (1.2.3.4). A major firmware release is a release in which the third digit increases (1.2.**3**.4). For example, if access points at a location are running release 3.5.4.3 and release 3.5.4.6 is available, the scheduled firmware upgrade does not occur and you must upgrade manually. However, if access points at a location are running release 3.5.4.3 and release 3.5.5.0 is available, the scheduled firmware upgrade does occur.

Upgrade Devices at a Location to a Specific Firmware Version

You can upgrade the firmware on one or several types of devices (that is, access point models) at a location to a specific firmware version. For each selected access point model, the firmware is upgraded for all access points of that model at the location.

Although you can downgrade to an earlier firmware version, we still refer to this process as an upgrade for the sake of simplicity.

You can upgrade the firmware immediately or schedule a firmware upgrade at time when you expect minimal WiFi traffic. (The firmware upgrade takes about four minutes, causing connected clients to lose connection during that period.)

► **To upgrade or schedule to upgrade firmware on one or more types of devices at a location to a specific firmware version:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.

Business Central Wireless Manager 2.1 Application

The Monitoring page displays.

4. Select **Configuration**.

The Configuration page displays any existing locations.

5. In the Locations tree, click the location.

The Configuration page displays the settings for the selected location.

6. Click the **Upgrade Devices** tab.

Device Model	Number	Current Firmware Version	Upgrade Version	When to Upgrade
WNDAP660	1	3.5.12.0	Select a version	No upgrade scheduled
WNDAP350	1	3.5.12.0	Select a version	No upgrade scheduled

Timezone: Australia/Sydney

Save

7. To view the release notes for the current firmware version, do the following:

- In the Current Firmware Version column, click the green **i** (information) icon.
A pop-up window opens and displays the release notes.
- When you are done reading, scroll down, and click the **Close** button.
The pop-up window closes.

8. For the access point model that you want to upgrade (see the Device Model column), select a specific firmware version from the **Upgrade Version** menu.

You can either upgrade the firmware immediately or schedule the firmware to be upgraded at a particular time.

The upgrade occurs for *all* access points of that model at the location.

9. To upgrade the firmware immediately, do the following:

- Make sure that the **Now** radio button is selected in the When to Upgrade column.
- Click the **Save** button.
A pop-up window opens and displays a warning.
- Click the **Save Upgrade Settings** button.
Your settings are saved. If the configuration was successful, the page displays the message *Successfully saved upgrade settings*.
- Click the **Dismiss** button.
The pop-up window closes.

10. To schedule firmware to be upgraded at a particular date and time, do the following:

Manage Locations

- a. In the When to Upgrade column, select the **On Date** radio button.
A date and time field displays.
- b. Click the date and time field.
A pop-up window displays a monthly calendar.
- c. Select the month and day on which the upgrade must occur.
- d. Click the clock icon at the bottom of the pop-up window.
The pop-up window changes and displays options to specify a time.
- e. Specify the time at which the upgrade must occur.
Specify a time at which you expect a minimum number of clients to connect to the WiFi networks at the location, for example, 4 a.m.
- f. To close the pop-up window, click the **x** icon in the pop-up window.
You can also return to the calendar by clicking the calendar icon at the top of the pop-up window.
- g. Click the **Save** button.
A pop-up window opens and displays a warning.
- h. Click the **Save Upgrade Settings** button.
Your settings are saved. If the configuration was successful, the page displays the message *Successfully saved upgrade settings*.
- i. Click the **Dismiss** button.
The pop-up window closes.

Schedule to Upgrade Devices at a Location to the Latest Firmware Version

You can schedule to upgrade the firmware on one or several types of devices (that is, access point models) at a location to the latest firmware version. Such an upgrade recurs whenever a (major) firmware version is available. For each selected access point model, the firmware is upgraded for all access points of that model at the location.

You must schedule to upgrade the firmware at a particular time on one or more days in the week. We suggest that you do this at time when you expect minimal WiFi traffic. (The firmware upgrade takes about four minutes, causing connected clients to lose connection during that period.)

► To schedule a firmware upgrade to recur on one or more types of devices at a location to the latest firmware version:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.

Business Central Wireless Manager 2.1 Application

The Configuration page displays any existing locations.

5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the **Upgrade Devices** tab.

Device Model	Number	Current Firmware Version	Upgrade Version	When to Upgrade
WNDAP660	1	3.5.12.0	Select a version	No upgrade scheduled
WNDAP350	1	3.5.12.0	Select a version	No upgrade scheduled

Timezone: Australia/Sydney

[Save](#)

7. To view the release notes for the current firmware version, do the following:
 - a. In the Current Firmware Version column, click the green **i** (information) icon.
A pop-up window opens and displays the release notes.
 - b. When you are done reading, scroll down, and click the **Close** button.
The pop-up window closes.
8. For the access point model that you want to upgrade (see the Device Model column), select **Latest (recurring)** from the **Upgrade Version** menu to always upgrade to the latest firmware version when a new (major) version is released.

Device Model	Number	Current Firmware Version	Upgrade Version	When to Upgrade
WNDAP660	1	3.5.12.0	Latest (recurring)	Sun, Mon, Tue, Wed, Thu, Fri, Sat at 4:00 AM ☒
WNDAP350	1	3.5.12.0	Latest (recurring)	Sun, Mon, Tue, Wed, Thu, Fri, Sat at 4:00 AM ☒

Timezone: Australia/Sydney

[Save](#)

A day field and a time field display in the When to Upgrade column.

9. If you want to include beta firmware versions in the latest upgrades, select the check box next to the orange beta icon.
Beta firmware versions might be less stable than regular firmware versions.
10. Schedule to upgrade the firmware at a particular time on one or more days in the week by doing the following:

- a. Click the day field.
A pop-up window displays a seven-day schedule.
- b. Select the check boxes for the days on which you want upgrades to occur, or select the **Every Day** check box.
- c. Click the time field.
The pop-up window with the seven-day schedule closes and another pop-up window displays options to specify a time.
- d. Specify the time at which you want upgrades to occur.
Specify a time at which you expect a minimum number of clients to connect to the WiFi networks at the location, for example, 4 a.m.
An upgrade occurs only if a new (major) firmware version is available.
- e. To close the pop-up window, click the **x** icon in the pop-up window.
- f. Click the **Save** button.
A pop-up window opens and displays a warning.
- g. Click the **Save Upgrade Settings** button.
Your settings are saved. If the configuration was successful, the page displays the message *Successfully saved upgrade settings*.
- h. Click the **Dismiss** button.
The pop-up window closes.
The scheduled upgrade occurs for *all* access points of that model at the location.

Reboot a Location

You can reboot an entire location, that is, all access points at the location. The reboot process takes about two minutes, causing connected clients to lose connection during that period.

► To reboot all access points at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. From the Actions menu, select **Reboot Location**.
A pop-up window opens and displays a warning.

7. Click the **Reboot Location** button in the pop-up window.
All access points at the location are rebooted. After about two minutes, they come back online.
8. Click the **Dismiss** button.
The pop-up window closes.

Change the Device Credentials for a Location

You can change the device credentials (that is, the password; the user name is fixed) that you specified when you added the location. These credentials are required to access any access point that is assigned to the location, including access to the web management interface or access over an SSH connection.

Note If you remove an access point from the BCWM inventory, the access point device credentials are reset to their defaults (admin and password). For more information, see *Convert an Access Point From Cloud-Managed to Standalone* on page 151.

► To change the device credentials for a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the **Device Credentials** tab.
The Location-wide device credentials page displays. The Username field shows the fixed user name (admin). You cannot change this name.
7. To display the password, click the show/hide icon next to the password.
8. Click the **Edit** button.
The page adjusts and the **Password** field becomes editable.
9. Change the password.
10. Click the **Save** button.
Your settings are saved.

Remove a Location

You can remove a location that you no longer need. When you remove the location, all WiFi networks that you created for the location are removed and the access points that you assigned to the location are decommissioned and reset to factory defaults but do retain their IP settings and remain connected to the application. These access points do not convert to standalone mode but remain cloud-managed devices in inventory and you can deploy them at another location.

► To remove a location:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. Click the red **Delete** button.
A pop-up window displays a warning.
7. Click the **Delete** button in the pop-up window.
The location is removed.
8. Click the **Dismiss** button.
The pop-up window closes.

You assign WiFi networks to a location. Therefore, you first must set up a location and then you can add networks to that location (see [Add a WiFi Network to a Location](#) on page 28).

For each network, you can manage the WiFi settings, including the SSID and broadcast of the SSID, WiFi radio bands, tagged VLAN, authentication and encryption, captive portal, bandwidth caps, client separation, and radio on/off broadcast schedule.

This chapter includes the following sections:

- [Change the Broadcast, Advertisement, and VLAN Settings for a WiFi Network](#) on page 48
- [Change the Authentication and Encryption for a WiFi Network](#) on page 49
- [Add a Captive Portal for Free or Paid-For Access to a WiFi Network](#) on page 52
- [Set Bandwidth Caps for a WiFi Network](#) on page 62
- [Enable Fast Roaming for a WiFi Network](#) on page 63
- [Enable Client Isolation for a WiFi Network](#) on page 64
- [Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network](#) on page 65
- [Remove a WiFi Network](#) on page 66

Change the Broadcast, Advertisement, and VLAN Settings for a WiFi Network

You can change the network name (SSID) for a WiFi network, specify whether the SSID must be broadcast or is hidden, select the radio bands on which the access points broadcast, and specify a VLAN ID if the gateway connection requires a tagged VLAN.

► **To change the broadcast and advertisement settings for WiFi network at a location:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**.

Create a New Wireless Network

Advertisement

☒ Broadcast SSID?

SSID

Bands

☐ Specify a tagged VLAN

Authentication

Authentication Type

Captive Portal

[+ Add a Captive Portal](#)

Advanced Settings

☐ Enable Bandwidth Caps

☐ Enable Client Isolation

☐ Create Schedule

8. To disable broadcast of the SSID, clear the **Broadcast SSID** check box.

Business Central Wireless Manager 2.1 Application

By default, the SSID is broadcast. If you disable broadcast of the SSID (effectively, hide the SSID from users), only users who know the SSID can connect to the WiFi network. This is a method to enhance security.

9. To change the network name (SSID), enter a new name in the **SSID** field.
You can use up to and including 32 ASCII printable (typeable) characters. Do not use extended ASCII characters, control ASCII characters, or ASCII characters that you compose with the Alt key on your keyboard.
10. From the **Bands** menu, select the WiFi band or bands.
The options are **2.4GHz and 5.0GHz Radios**, **2.4GHz Radio only**, and **5.0GHz Radio only**. The default setting is **2.4GHz and 5.0GHz Radios**, which applies to dual-band access points only. If an access point supports a single band only, the access point broadcasts on that band, unless your selection from the **Bands** menu disables that band.
11. To specify a tagged VLAN, select the **Specify a tagged VLAN** check box, and in the **VLAN ID** field, enter the VLAN ID.
The VLAN ID is a 12-bit number that identifies the tagged VLAN. If the connection from the access points to the Internet gateway requires an IEEE 802.1Q VLAN tag, you must specify a VLAN ID. If multiple WiFi networks operate over the same physical Ethernet link, VLANs can provide isolation and separation.
12. Click the **Save** button.
A pop-up window opens and displays a warning.
13. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access points reprogram their settings.

Change the Authentication and Encryption for a WiFi Network

A cloud-managed WiFi network can function as an open network without authentication and encryption (which can work well for a public hotspot) or provide authentication and encryption through WPA Personal (WPA-PSK) or WPA Enterprise. For the latter form of WPA, authentication and accounting occur through a RADIUS server that you select for the WiFi network. You specify a primary and secondary RADIUS server. The application must be able to access these RADIUS servers.

If you select either form of WPA, both WPA and WPA2 devices can connect to the WiFi network, that is, the default encryption is TKIP+AES. You can select TKIP only, in which case WPA devices can connect to the WiFi network but WPA2 devices cannot.

Note NETGEAR access points that support 802.11ac and 802.11n devices support one RADIUS profile per WiFi network. However, NETGEAR access points that support 802.11n devices but do not support 802.11ac devices support a single RADIUS profile only for all WiFi networks. On an access point that supports a single RADIUS profile only, the last WPA Enterprise configuration that you specified for *any* WiFi network with WPA Enterprise applies to all WiFi networks with WPA Enterprise on the access point. If a location must support 802.11n devices, specify the same WPA Enterprise configuration for all WiFi networks at the location.



WARNING:

If you change the authentication method to WPA Personal or WPA Enterprise, connected clients lose their connection and must reconnect using the new authentication method.

► **To change the authentication and encryption settings for WiFi network at a location:**

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.

Business Central Wireless Manager 2.1 Application

- For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**.

Create a New Wireless Network

Advertisement

☒ Broadcast SSID?

SSID

Bands

☐ Specify a tagged VLAN

Authentication

Authentication Type

Captive Portal

[+ Add a Captive Portal](#)

Advanced Settings

☐ Enable Bandwidth Caps

☐ Enable Client Isolation

☐ Create Schedule

- From the **Authentication Type** menu, select the type of authentication:

- Open.** You do not need to specify any additional information because the network functions without authentication and encryption. This option can be useful for a public hotspot, in particular in combination with a captive portal (see [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53).
- WPA Personal.** In the **Password** field, you must specify the password that is required to access the network. You can enter up to 63 alphanumeric and special characters. The default encryption method is TKIP+AES, which allows both WPA and WPA2 devices to connect to the WiFi network. This encryption method works well for most WiFi networks. However, you can select the **Change Data Encryption** check box and from the **Data Encryption** menu, select **TKIP**. TKIP is an older and less secure encryption method that allows WPA devices to connect to the WiFi network but prevents WPA2 devices from connecting to the network. Use TKIP only if you expect only legacy devices to connect to the WiFi network.
- WPA Enterprise.**

Authentication

Authentication Type

On devices that only support a single Radius Profile, the last Radius Profile configuration to be made will apply to all Wireless Networks on those APs. The Netgear 11n APs support only one Radius profile for the device whereas the Netgear 11ac APs support a Radius Profile per Wireless network. If you have, or expect to have 11n APs at this location, you should enter the same radius server parameters for all wireless networks.

	Server IP Address	Secret Key	Port
Primary	Primary RADIUS Server	Shared Secret	1812
Secondary	Secondary RADIUS Server	Shared Secret	1812

Reauthentication Time

☒ Enable RADIUS Accounting

Radius Accounting Servers share the same IP addresses as the primary/secondary Authentication Servers with +1 port numbers.

☒ Change Data Encryption

Data Encryption

To configure WPA Enterprise, do the following:

- a. Configure the primary RADIUS server by entering its IP address, the shared secret (also referred to as the secret key, passphrase, or password), and the port number (the default is 1812) through which the application communicates with the RADIUS server.
 - b. As an option, configure the secondary RADIUS server by entering its IP address, the shared secret, and the port number (the default is 1812) through which the application communicates with the RADIUS server.
 - c. Specify the reauthentication time, which is period in minutes after which a client must reauthenticate with the RADIUS server.
The default is 3600 minutes. To disable reauthentication, enter **0**.
 - d. To enable RADIUS accounting, select the **Enable RADIUS Accounting** check box.
The RADIUS accounting servers use the same IP addresses as the RADIUS authentication servers but the port numbers are incremented by 1. That is, the default port number for the primary and secondary RADIUS accounting servers is 1813.
 - e. To change the encryption method, select the **Change Data Encryption** check box, and from the **Data Encryption** menu, select **TKIP**.
The default encryption method is TKIP+AES, which allows both WPA and WPA2 devices to connect to the WiFi network. This encryption method works well for most WiFi networks. TKIP is an older and less secure encryption method that allows WPA devices to connect to the WiFi network but prevents WPA2 devices from connecting to the network. Use TKIP only if you expect only legacy devices to connect to the WiFi network.
9. Click the **Save** button.
A pop-up window opens and displays a warning.
 10. Click the **Save** button in the pop-up window.
Your settings are saved. If you changed the authentication method to WPA Personal or WPA Enterprise, connected clients lose their connection and must reconnect using the new authentication method.

Add a Captive Portal for Free or Paid-For Access to a WiFi Network

A captive portal blocks clients from accessing a WiFi network until they are verified, at which point the captive portal can provide free or paid-for access to the WiFi network. Such a WiFi network is often referred to as a hotspot. You can require users to agree to user terms and you can redirect users to a specific website. You can add a captive portal to any WiFi network and specify captive portal settings that apply only to that WiFi network.

For more information, see the following sections:

- [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53
- [Add a Captive Portal for Voucher Access to a WiFi Network](#) on page 56
- [Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network](#) on page 59

Note Although a WiFi network with a captive portal often is set up as an open network, you *can* set up authentication and encryption for such a network in the same way that you can set it up for any other WiFi network. For more information, see [Change the Authentication and Encryption for a WiFi Network](#) on page 49.

Add a Captive Portal for Free Access to a WiFi Network

You can set up a captive portal for a WiFi network to offer either free access with click-through or free access with click-through and the requirement to provide information, for example, a name, company name, and email address. (You can customize the information fields.)

► To add a captive portal for free access to an existing WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network to which you want to add a captive portal, click the gear icon, and select **Edit Wireless Network**.
The page adjusts and the fields become editable.
8. Click the **+ Add a Captive Portal** button.
The Configure Your Captive Portal Splash Page pop-up window opens.
9. In the Splash Page section, from the **Type** menu, select select one of the following options:

Business Central Wireless Manager 2.1 Application

- **Click Through.** No authentication is required to click through.
- **Click Through w/Custom Fields.** For a captive portal user to be able to click through, the users must provide the information that you can specify in the Custom Fields section.

Configure Your Captive Portal Splash Page

Splash Page

Type: Click Through

Title:

Message:

Session

☐ Redirect users after login

Session Duration: 1 days

Image

Image File:

EULA

☒ Provide a EULA

EULA Text:

This usage agreement governs your use of the Internet services provided. The use of this hotspot is voluntarily given and may be rescinded without advanced notice. The user is not entitled to any compensation for damages, real or imagined, incurred while using the hotspot.

Note For information about the **Voucher** option, see [Add a Captive Portal for Voucher Access to a WiFi Network](#) on page 56. For information about the **Facebook WIFI** option, see [Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network](#) on page 59.

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

Setting	Description
Title	Enter a title for the splash page. Captive portal users do see this title.
Message	Enter a message for the captive portal users. The default message is <i>Please click 'Connect' for free Internet access.</i>
Redirect URL	To redirect the captive portal users to a website after login, select the Redirect users after login check box. In the field that displays, enter the website, beginning with http://.
Session Duration	Specify the session duration by entering a period in the left field and selecting a time unit from the right menu. By default, the session duration is 1 day.

(Continued)

Setting	Description
Custom Fields	The Enter a Custom Field field and the + Add Field button display only if the selection from the Type menu is Click Through w/Custom Fields. You can specify a maximum of six fields. For a captive portal user to be able to click through, the user must supply information in each field that you specify. To add a field, click the + Add Field button. To remove a field, click the – button.
Image	To add an image to the splash page, click the Browse button and navigate to and select an image from your computer. The maximum size for an image is 300 KB.
Image Alignment	This menu displays only if you select an image. From the Image Alignment menu, select the position of the image on the splash page (Middle , Left , or Right).
EULA	By default, the Provide a EULA check box is selected and the user can click the Terms of Use link on the splash page to view the default EULA. You can change the text of the EULA. You can also clear the Provide a EULA check box, in which case the EULA is not accessible to the user from the splash page.

- To preview the splash page, click the **Preview** button.

The splash page opens in a new tab.

**Fast Ferries
Access**



Welcome to Fast Ferries!
Please click continue for free
Internet access

Name

Company

Email

By clicking 'Connect', you agree to the [Terms of Use](#).

Connect

- Click the **Save** button.

The splash page is saved, the Configure Your Captive Portal Splash Page pop-up window closes, and the configuration page for the WiFi network displays again.

13. Click the **Save** button on the configuration page for the WiFi network.

Your settings are saved. The WiFi network becomes a hotspot that is accessible through the splash page. The access points reprogram their settings and are temporarily not available.

Add a Captive Portal for Voucher Access to a WiFi Network

You can set up a captive portal on a WiFi network to offer paid-for access through a voucher. You can specify the period and unit of time (minute, hour, day, or week) for a single voucher, and you can do so in various currencies. You can also specify if a single voucher allows access for a single or for several devices, and if access time is deducted only when devices are connected to the WiFi network or whether they are connected to the WiFi network or not.

► To add a captive portal for voucher access to an existing WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network to which you want to add a captive portal, click the gear icon, and select **Edit Wireless Network**.
The page adjusts and the fields become editable.
8. Click the **+ Add a Captive Portal** button.
The Configure Your Captive Portal Splash Page pop-up window opens.

Business Central Wireless Manager 2.1 Application

9. In the Splash Page section, from the **Type** menu, select **Voucher**.

Configure Your Captive Portal Splash Page

Splash Page

Type

Title

Message

Session

☐ Redirect users after login

Voucher

Cost per

Device Limit

Deduct Time

Image

Image File

EULA

☒ Provide a EULA

EULA Text

This usage agreement governs your use of the Internet services provided. The use of this hotspot is voluntarily given and may be rescinded without advanced notice. The user is not entitled to any compensation for damages, real or imagined, incurred while using the hotspot.

Note For information about the **Click Through** and **Click Through w/Custom Fields** options, see [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53. For information about the **Facebook WiFi** option, see [Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network](#) on page 59.

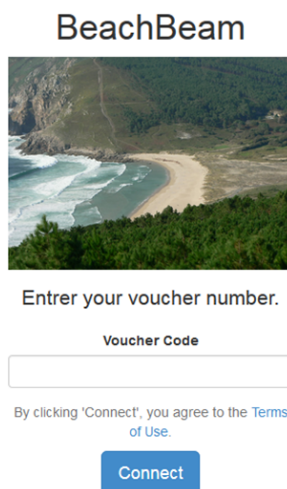
10. Configure the settings as described in the following table.

Setting	Description
Title	Enter a title for the splash page. Captive portal users do see this title.
Message	Enter a message for the captive portal users.
Redirect URL	To redirect the captive portal users to a website after login, select the Redirect users after login check box. In the field that displays, enter the website, beginning with http://.
Cost	The Cost option provides two menus and a field that let you define the cost of a single voucher: - From the left menu, select the currency. - In the middle field, enter the period that is associated with the unit of time, or use the up and down arrows to specify the period. - From the right menu, select the unit of time (minute, hour, day, or week).

(Continued)

Setting	Description
Device Limit	Enter or use the menu to specify the number of devices that are allowed WiFi access with a single voucher.
Deduct Time	From the menu, select one of the following options to specify how usage time is deducted from the voucher balance: only while connected. Usage time is deducted only when a device is connected to the WiFi network. whether connected or not. Usage time is connected from the moment that the voucher is issued and deducted whether or not a device is connected to the WiFi network.
Image	To add an image to the splash page, click the Browse button and navigate to and select an image from your computer. The maximum size for an image is 300 KB.
Image Alignment	This menu displays only if you select an image. From the Image Alignment menu, select the position of the image on the splash page (Middle , Left , or Right).
EULA	By default, the Provide a EULA check box is selected and the user can click the Terms of Use link on the splash page to view the default EULA. You can change the text of the EULA. You can also clear the Provide a EULA check box, in which case the EULA is not accessible to the user from the splash page.

11. To preview the splash page, click the **Preview** button.
The splash page opens in a new tab.



12. Click the **Save** button.

The splash page is saved, the Configure Your Captive Portal Splash Page pop-up window closes, and the configuration page for the WiFi network displays again.

13. Click the **Save** button on the configuration page for the WiFi network.

Your settings are saved. The WiFi network becomes a hotspot that is accessible through the splash page. The access points reprogram their settings and are temporarily not available.

Add a Captive Portal for Facebook Wi-Fi Access to a WiFi Network

You can set up a captive portal on a WiFi network to offer free access through check-in to a Facebook business page.

Note A captive portal that uses Facebook Wi-Fi access is available only for access point models WAC720 and WAC730.



ATTENTION:

After you add a captive portal for Facebook Wi-Fi, the associated portal splash page might not open under some circumstances, allowing users Internet access without logging in. This security limitation is implemented by Facebook Wi-Fi, not by NETGEAR. If a user opens a browser and attempts to access a website over HTTP (by default, over port 80), the user is directed to the splash page. However, if a user attempts to access a website that does not use HTTP, the splash page might not open and the user can access the website without logging in. For example, this situation occurs if a user opens a browser and accesses a secure website over HTTPS (by default, over port 443), or if an application uses HTTPS to send traffic to the Internet.

► To add a captive portal for Facebook Wi-Fi access to an existing WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.

Business Central Wireless Manager 2.1 Application

7. For the WiFi network to which you want to add a captive portal, click the gear icon, and select **Edit Wireless Network**.

The page adjusts and the fields become editable.

8. Click the **+ Add a Captive Portal** button.

The Configure Your Captive Portal Splash Page pop-up window opens.

9. In the Splash Page section, from the **Type** menu, select **Facebook WIFI**.

Configure Your Captive Portal Splash Page

Splash Page

Type: Facebook WIFI

Facebook WIFI Setup

Register

Gateway ID:

Verify Pairing

Page Name:

Save Cancel

Note For information about the **Click Through** and **Click Through w/Custom Fields** options, see [Add a Captive Portal for Free Access to a WiFi Network](#) on page 53. For information about the Voucher option, see [Add a Captive Portal for Voucher Access to a WiFi Network](#) on page 56.

10. In the Facebook WIFI Setup section, Click the **Register** button.

The application generates a gateway ID, which displays in the **Gateway ID** field. After you click the **Register** button, the button becomes the **Configure Page** button.

11. In the Facebook WIFI Setup section, click the **Configure Page** button.

If you are not yet logged in to a Facebook account, the Log in to Facebook page opens.

Business Central Wireless Manager 2.1 Application

12. If you are not yet logged in to a Facebook account, log in to a Facebook account by entering your user name and password for the Facebook account.

Facebook Wi-Fi Configuration
Circular Quay-Manly

Facebook Page
To use Facebook Wi-Fi you need to be the admin of a local business Page that has a valid location associated with it.
Select a Page ▾

Bypass Mode
Your customers always have the option to skip checking in. They can do this by clicking on a link that lets them skip check-in, or by entering a Wi-Fi code that you provide to them.

☒ Skip check-in link [?]
☐ Require Wi-Fi code [?]

Session Length
Select the length of time your customers will have Wi-Fi for after they check in.
Five hours ▾

Terms of Service
☐ Optional: Add your own Terms of Service [?]

[Visit Help Center](#) **Save Settings**

The name of the location and WiFi network for which you are setting up a captive portal display below Facebook Wi-Fi Configuration at the top of the page. (In the previous figure, Circular Quay-Manly.)

13. Configure the Facebook Wi-Fi settings:
- From the **Select a Page** menu, select a Facebook business page.
 - Select the bypass mode option:
 - To allow customers to skip check-in, select the **Skip check-in link** radio button. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in.
 - To require users to enter a WiFi code before they can gain WiFi access, select the **Require Wi-Fi code** radio button and type a WiFi code in the field that displays. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in by using the WiFi code.
 - From the **Session Length** menu, select the period after which users are automatically logged out.
 - To add terms of service to the Facebook check-in page, select the **Terms of Service** check box and type or copy the terms of service in the field that displays.
 - Click the **Save Settings** button.
The Facebook Wi-Fi settings are saved.
 - Close the Facebook Wi-Fi Configuration page.
14. In the Configure Your Captive Portal Splash Page pop-up window, click the **Verify Pairing** button.
The Facebook business page that you selected displays in the **Page Name** field.
15. Click the **Save** button.

The Facebook Wi-Fi portal is saved, the Configure Your Captive Portal Splash Page pop-up window closes, and the configuration page for the WiFi network displays again.

Under the **Type** menu, the **Edit Captive Portal** and **Remove Captive Portal** buttons now display.

16. Click the **Save** button on the configuration page for the WiFi network.

Your settings are saved. The WiFi network becomes a hotspot that is accessible through the Facebook splash page. The WAC720 and WAC730 access points reprogram their settings and are temporarily not available.

Set Bandwidth Caps for a WiFi Network

By default, a cloud-managed WiFi network does not impose bandwidth caps on either upload or download traffic. If you enable bandwidth control, the default upload and download bandwidth caps are 1000 Kbps each. For each type of bandwidth cap, you can customize the bandwidth caps with a minimum value of 64 Kbps and a maximum value of 10 Gbps. The actual bandwidth capacity depends on multiple factors such as the number of devices on the WiFi network, the signal strength of the WiFi work, and the physical Ethernet link of the access point.

► To change the broadcast and advertisement settings for WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**.
The page adjusts and the fields become editable.

8. Select the **Enable Bandwidth Caps** check box.

Advanced Settings

☒ Enable Bandwidth Caps

Minimum value is 64Kbps, Maximum value is 10 Gbps

Upload Bandwidth Cap Kbps

Download Bandwidth Cap Kbps

☐ Enable Client Isolation

☐ Create Schedule

9. In the **Upload Bandwidth Cap** and **Download Bandwidth Cap** fields, enter numeric values, click the + and – buttons to change the values, or use a combination of both methods to set the bandwidth values. All bandwidth values are expressed in Kbps.
10. Click the **Save** button.
A pop-up window opens and displays a warning.
11. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access points reprogram their settings.

Enable Fast Roaming for a WiFi Network

Fast roaming can improve voice quality while a client roams between two access points. For fast roaming to be effective, both the client and the access points must support fast roaming (802.11r), and the authentication and encryption method for the WiFi network must be WPA Personal (WPA-PSK) with TKIP + AES or WPA Enterprise (see [Change the Authentication and Encryption for a WiFi Network](#) on page 49).

Although you can configure fast roaming regardless of the access points that you are deploying at a location, fast roaming applies only to the WAC720 and WAC730 access points and to clients that support fast roaming. If you enable fast roaming for a WiFi network that is broadcast on a WAC720 or WAC730 access point only, a client that does not support fast roaming cannot connect to the WiFi network. In such a situation, you could set up an additional WiFi network without fast roaming to serve the clients that do not support fast roaming.

► To enable fast roaming for WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.

5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**.
The page adjusts and the fields become editable.

Note The **Enable Fast Roaming** check box displays only if the selection from the **Authentication Type** menu is **WPA Personal** or **WPA Enterprise**.

8. Select the **Enable Fast Roaming** check box.
The **Exchange Fast Roaming Info Over Wired Network** check box displays.
9. To enable fast roaming information to be exchanged over the wired network instead of the WiFi network, select the **Exchange Fast Roaming Info Over Wired Network** check box.
The default setting is that fast roaming information is exchanged over the WiFi network instead of the wired network.
10. Click the **Save** button.
A pop-up window opens and displays a warning.
11. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access points reprogram their settings.

Enable Client Isolation for a WiFi Network

Client isolation is an added security measure that prevents clients on a WiFi network from accessing computers that are connected to the network by a wired connection and from communicating with other clients on the same WiFi network. A public hotspot is one example of an environment in which you might want to enable client isolation.

► To enable client isolation for WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.

The Configuration page displays the settings for the selected location.

6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**.
The page adjusts and the fields become editable.
8. Select the **Client Isolation** check box.
9. Click the **Save** button.
A pop-up window opens and displays a warning.
10. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access points reprogram their settings.

Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network

A radio on/off broadcast schedule lets you specify when a WiFi network must be turned off and back on again. For example, you can set up a schedule that lets you turn off WiFi networks at night and during weekends to save energy and prevent unauthorized network use.

Note Both when you implement a radio on/off broadcast schedule and when a scheduled blockage begins or ends for a WiFi network, a momentary loss of connection occurs on all access points that serve the WiFi network. That is, even if a client is connected to another WiFi network for which the schedule is not implemented or for which the blockage does not begin or end, a momentary loss of connection still occurs if the WiFi network is served by the same access points that also serve the WiFi network for which the schedule is implemented or the blockage does begin or end.

► To set up or change a radio on/off broadcast schedule for a WiFi network at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.

Business Central Wireless Manager 2.1 Application

The Configuration page displays any existing WiFi networks.

7. For the WiFi network that you want to change, click the gear icon, and select **Edit Wireless Network**. The page adjusts and the fields become editable.

The nature of the check box for the schedule depends on whether you are setting up a new schedule or are changing an existing schedule.

8. To set up a new schedule, select the **Create Schedule** check box.
To change an existing schedule, select the **Edit Schedule** check box.
A pop-up window opens and displays a warning.
9. Click the **Create Schedule** button (or the **Edit Schedule** button) in the pop-up window.
The page displays a seven-day schedule with hours from 12 a.m. to 11 p.m. The time zone is adjusted for the location.
10. For each day that you want the radios to broadcast, in the day column (for example, the Monday column), click the time when you want the radios to begin broadcasting and drag to the time that you want broadcasting to end.

You can specify several broadcasting time slots during a single day.

Broadcasting can begin either at the top of the hour or 30 minutes past the hour. Broadcasting can end either 29 minutes and 59 seconds past the hour or 59 minutes and 59 seconds past the hour. A scheduled broadcasting time slot is shown by a blue color. Clicking again removes the scheduled time slot and the blue color.

The scheduled time is repeated every week.

Note As an example, to schedule the WiFi network to turn off every night at 9:00 p.m., turn on every morning at 5:30 a.m., and remain off during Saturday and Sunday, do the following: In the Monday column, click the 5:30 time and drag to the 8:30 time so that all times from 5:30 a.m. to 9:00 p.m. are shown in blue, and repeat this for each weekday.

11. Click the **Save** button.
A pop-up window opens and displays a warning.
12. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access points reprogram their settings. (See also the note at the beginning of this section.)

Remove a WiFi Network

You can remove a WiFi network that you no longer need.

► To permanently remove a WiFi network:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.

Business Central Wireless Manager 2.1 Application

The application login page displays.

3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.
The Configuration page displays any existing WiFi networks.
7. For the WiFi network that you want to change, click the gear icon, and select **Delete Wireless Network**.
A pop-up window displays a warning.
8. Click the **Delete** button in the pop-up window.
The WiFi network is removed.
9. Click the **Dismiss** button.
The pop-up window closes.

Manage Devices and Device Inventory

5

You assign devices (access points) to a location. Therefore, you first must set up a location, and then you can add access points to that location (see [Add an Access Point to a Location](#) on page 31).

For each access point, you can change the name, assign building and floor labels, change the IP address from a DHCP-assigned IP address to a static IP address or the other way around, and manage the radio settings for the access point (as opposed to the radio settings for a WiFi network that is served by the access point).

You can also manage the device inventory (all access points that are cloud managed), including adding devices to inventory without deploying them to a location, decommissioning devices from one location and redeploying them at another location, and removing devices from inventory altogether.

This chapter includes the following sections:

- [Change the Device Name](#) on page 69
- [Add or Change Building and Floor Labels for a Device](#) on page 69
- [Change the Radio and WiFi Settings for a Device](#) on page 70
- [Change the IP and Management VLAN Settings for a Device](#) on page 72
- [Reboot a Device](#) on page 75
- [Remove a Device From a Location](#) on page 76
- [Manage the Device Inventory](#) on page 77

Change the Device Name

When you first add an access point to a location, you must specify a device name, which does not need to be the default device name (usually in the format netgearXXXX, in which X can be a numeric or alphanumeric value). You can change that device name.

► To add or change the device name for an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. For the device that you want to change, click the gear icon, and select **Change Short Name**.
A pop-up window opens.
8. In the upper field, in which the existing name displays, enter a new name.
As an option, you can add a description in the lower field. (This description is not displayed on any monitoring pages.)
9. Click the **Save** button in the pop-up window.
Your settings are saved.

Add or Change Building and Floor Labels for a Device

To help you organize your access point by physical location, you can add building and floor labels to an access point.

► To add or change building and floor labels for an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. Select the access point.
The Configuration page displays the access point details.
8. Click one of the edit icons (✎).
The **Device Name**, **Building**, and **Floor** fields become editable.
9. Enter a building name, floor name, or both.
10. Click the **Save** button.
Your settings are saved.

Change the Radio and WiFi Settings for a Device

You can change the radio and WiFi settings that apply to a single access point that is assigned to a location, as opposed to changing the radio settings for the location, that is, for the entire pool of access points that is assigned to a location.

The default settings often work well but situations might occur in which you want to change the settings. Managing the radio and WiFi settings includes enabling or disabling a radio, changing the WiFi mode, changing the WiFi channel, changing the WiFi bandwidth, changing the transmission output power, changing the Wi-Fi Multimedia (WMM) settings, changing the maximum number of supported clients, and specifying the default internal or optional external antenna.

Note For information about manually changing the radio settings for a location, that is, for the entire pool of access points that are assigned to a location, see [Manage the Radio and Antenna Settings for a Location](#) on page 33.

► To configure a static IP address for an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.

Business Central Wireless Manager 2.1 Application

5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. Select the access point.
The Configuration page displays the access point details.
8. Click the **Radios** tab.
The radio settings display.
9. Click the **Edit Radios** button.

Radio	Enabled	Band	Mode	Channel	Power	Bandwidth	WMM Mode	WMM Power Save	Max Clients	Antenna
WLAN0	☒	2.4GHz	g-n	Auto (6)	Full	Dynami	Yes	No	128	Internal
WLAN1	☒	5GHz	a-n	Auto (36)	Full	Dynami	Yes	No	128	Internal

10. Change the settings as needed:

- **Radio.** A nonconfigurable field that shows the radio number (WLAN0 or WLAN1) for the access point.
- **Enabled.** By default, the radio is enabled. To disable the radio, clear the check box.
- **Band.** A nonconfigurable field that shows the radio band that is associated with the WiFi mode.
- **Mode.** From the menu, select the WiFi mode for the radio. By default, the most advanced WiFi mode is selected.
- **Channel.** You can select a static channel from the menu. The supported channels depend on the region of operation for the access point. By default, cloud-managed access points autoconfigure their channels (that is, the channel setting is **Auto**).
- **Power.** By default, the transmission output for an access point is set to maximum power. From the menu, you can select a lower output power for each WiFi band that the access point supports. The supported output options are **Full**, **Half**, **Quarter**, **Eighth**, **Minimum**.
- **Bandwidth.** From the menu, select the WiFi bandwidth, which is also referred to as the channel width. A wider channel improves the performance but some legacy devices can operate only in either 20 MHz or 40 MHz. The supported WiFi bandwidths depend on the access point model.
- **WMM Mode.** By default, WMM is enabled, allowing time-dependent WiFi traffic such as video and audio to receive a higher priority than data WiFi traffic. You can disable WMM.
- **WMM Power Save.** By default, the WMM Power Save feature is enabled, increasing the efficiency and flexibility of data transmission and thereby allowing battery-powered equipment to save power. You can disable the WMM Power Save feature.

Manage Devices and Device Inventory

- **Max Clients.** A radio on a NETGEAR access point can typically support between 64 and 128 clients. However, allowing the maximum number of clients might not be the most suitable configuration for a site with a large number of clients. From the menu, you can select a lower number to prevent oversubscription and congestion and to improve throughput and latency.
- **Antenna.** By default, the setting is **Internal**. External antennas are optional accessories. If you select **External**, the configuration takes effect only if the access point is configured with one or more external antennas.

11. Click the **Save** button.

A pop-up window opens and displays a warning.

12. Click the **Save** button in the pop-up window.

Your settings are saved. Connected clients lose their connection momentarily while the access point reprograms its settings.

13. Click the **Dismiss** button.

The pop-up window closes.

Change the IP and Management VLAN Settings for a Device

For any NETGEAR access point that the application supports, the access point functions as a DHCP client by default. If your network does not include a DHCP server or the network configuration requires a static IP address, you can set a static IP address configuration for an access point, including the gateway IP address and the DNS server IP addresses.

You can also change the management VLAN ID from its default VLAN ID 1 to another VLAN ID.

Configure a Static IP Address for an Access Point

If your network does not include a DHCP server or the network configuration requires a static IP address, you can set a static IP address configuration for an access point.

► To configure a static IP address for an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.

The Configuration page displays any existing access points.

7. Select the access point.

The Configuration page displays the access point details.

8. Click the **IP Settings** tab.

The configured IP settings display.

9. Click the **Edit IP Settings** button.

The **IP Settings** menu becomes available.

10. From the **IP Settings** menu, select **static**.

The fields become editable.

11. Enter the static IP address information, including the gateway and DNS server addresses.

12. Click the **Save** button.

A pop-up window opens and displays a warning.

13. Click the **Save** button in the pop-up window.

Your settings are saved. Connected clients lose their connection momentarily while the access point reprograms its settings.

14. Click the **Dismiss** button.

The pop-up window closes.

Configure an Access Point as a DHCP Client

For any NETGEAR access point that the application supports, the access point functions as a DHCP client by default. If the access point functions with a static IP configuration and you want to convert it to a DHCP client, follow this procedure. The application must be able to connect to a DHCP server.

► To configure an access point at a location as a DHCP client:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.

7. Select the access point.
The Configuration page displays the access point details.
8. Click the **IP Settings** tab.
The configured IP settings display.
9. Click the **Edit IP Settings** button.
The **IP Settings** menu becomes available.
10. From the **IP Settings** menu, select **DHCP**.
The fields are masked out.
11. Click the **Save** button.
A pop-up window opens and displays a warning.
12. Click the **Save** button in the pop-up window.
Your settings are saved. It might take several minutes before the access point receives an IP address from the DHCP server. Connected clients lose their connection momentarily while the access point reprograms its settings.
13. Click the **Dismiss** button.
The pop-up window closes.

Change the Management VLAN for an Access Point

For any NETGEAR access point that the application supports, the default management VLAN ID is ID 1. You can change this ID to any other VLAN ID that your network supports. Make sure that you enter a correct VLAN ID. Otherwise, the access point might become unreachable and you might need to reset the access point to factory default settings to recover it.

► To change the management VLAN ID for an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. Select the access point.

The Configuration page displays the access point details.

8. Click the **IP Settings** tab.
The configured IP and management VLAN settings display.
9. Click the **Edit IP Settings** button.
The **IP Settings** menu becomes available.
10. In the **Management VLAN** field, enter a new VLAN ID.
The default management VLAN ID is ID 1.
11. Click the **Save** button.
A pop-up window opens and displays a warning.
12. Click the **Save** button in the pop-up window.
Your settings are saved. Connected clients lose their connection momentarily while the access point reprograms its settings.
13. Click the **Dismiss** button.
The pop-up window closes.

Reboot a Device

You can reboot an access point at a location. The reboot process takes about two minutes, causing connected clients to lose connection during that period.

For information about rebooting a location, that is, the entire pool of access points that is assigned to a location, see [Reboot a Location](#) on page 44.

► To reboot an access point at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. For the access point that you want to reboot, click the gear icon, and select **Reboot Device**.
A pop-up window opens and displays a warning.

8. Click the **Reboot Location** button in the pop-up window.
The access point at the location is rebooted. After about two minutes, it comes back online.
9. Click the **Dismiss** button.
The pop-up window closes.

Remove a Device From a Location

You can remove an access point from a location. The access point resets to factory defaults and becomes a standalone access point. That is, the access point does not remain in inventory and is no longer cloud managed. If you want to keep the access point in inventory and cloud managed, do not remove (that is, delete) the access point, but decommission it from the location while preserving the IP settings (see *Decommission a Device From a Location and Keep It in Inventory* on page 82).



CAUTION:

If an access point is removed from a location, it is no longer managed by the application, resets to factory default settings, broadcasts its default SSIDs, and provides open networks without any security. If you do not want open networks, connect to the access point through its web management interface and implement WiFi security or disable the radios.

► To remove an access point from a location and from inventory:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. For the access point that you want to remove, click the gear icon, and select **Delete Device**.
A pop-up window opens and displays a warning.
8. Click the **Delete** button in the pop-up window.
The access point is removed from the location and from inventory.
9. Click the **Dismiss** button.

The pop-up window closes.

Manage the Device Inventory

The device inventory consists of cloud-managed access points that can be active and connected or not active but still connected.

The following sections describe how you can manage the device inventory:

- [View the Device Inventory](#) on page 77
- [Add a Device to Inventory Without Deploying It](#) on page 79
- [Deploy a Device in Inventory at a Location](#) on page 80
- [Decommission a Device From a Location and Keep It in Inventory](#) on page 82
- [Remove a Device From Inventory](#) on page 83

View the Device Inventory

The device inventory lets you view the inventory status, connection status, location, building, floor, and firmware version of all access points that were added to the application, whether active or not.

The device inventory consists of cloud-managed access points for which the inventory status can be one of the following:

- **Active.** The access point is connected to the application and is added to a location, and the location is assigned to a license account with an active license.
- **Provisioning.** The access point is either cloud managed or in the process of becoming cloud managed while the application is pushing a configuration.
- **Upgrading.** The access point is either cloud managed or in the process of becoming cloud managed while the application is pushing a firmware upgrade.
- **Rebooting.** The access point is either cloud managed or in the process of becoming cloud managed and is rebooting after the application pushed a configuration or a firmware upgrade to the access point.
- **Unlicensed.** Even though the access point is connected to the application, the access point is added to a location that is assigned to an unlicensed account. The access point does not become active until you add an active license to the account.
- **Decommissioning.** The application is in the process of decommissioning the access point from a location.
- **Decommissioned.** Even though the access point is connected to the application, the access point is not added to a location and is not active.

For each access point in inventory, the connection status can be one of the following:

- **Connected.** The access point is connected to the application. However, this does not mean that the access point is active.
- **Disconnected.** The access point was connected to the application but is now disconnected.

Business Central Wireless Manager 2.1 Application

- **Waiting.** The access point is added to a location and is waiting for a connection to the application.
- **Phoned home** (and a time indication). The access point is connected to the application but decommissioned (or undeployed).

► To view the device inventory:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Inventory**.

Role: owner		Status: All	Decommission	Delete	Deploy	New Device	
☐	Device	Inventory Status	Connection Status	☐ Location	Building	Floor	Software Version
☐	20Y2345R0005C (AP320-Upstairs-N...	Active	Connected	☐ Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
☐	20Y2345B00041 (AP320-Downstair...	Active	Connected	☐ Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
☐	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	☐ Netgear - Main Office			tailac_staging_1511.16.1936.112
☐	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	☐ Netgear - Main Office			continuous_15.11.10.2054.54
☐	2XX244NN0012F (AP660-Peets-Riv...	Active	Connected	☐ Peet's - Rivermark Plaza			continuous_15.11.16.1923.62
☐	2925345600355 (AP350-Peets-Airpo...	Active	Connected	☐ Peet's - San Jose Intl Ai...			continuous_15.11.10.2054.54
☐	4D815AER000AA (AP720-Peets-Air...	Active	Connected	☐ Peet's - San Jose Intl Ai...			tailac_staging_1601.05.2320.216
☐	4DA25AE300036 (AP730-Starbucks...	Active	Connected	☐ Starbucks - North First			tailac_staging_1511.16.1936.112
☐	2XX244NE00135 (AP-660-Starbucks...	Active	Connected	☐ Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The table on the Inventory page displays the access points that are in inventory, whether active, decommissioned, or in the process of being provisioned or decommissioned.

For more information, see the following sections:

- For information about adding an access point to inventory without deploying it, see [Add a Device to Inventory Without Deploying It](#) on page 79.
- For information about deploying an access point, see [Deploy a Device in Inventory at a Location](#) on page 80.
- For information about decommissioning an access point, see [Decommission a Device From a Location and Keep It in Inventory](#) on page 82.
- For information about removing an access point from inventory, see [Remove a Device From Inventory](#) on page 83.

Add a Device to Inventory Without Deploying It

You can add an access point to the inventory without immediately deploying it to a location. For example, you can add access points to the inventory, set up locations and WiFi networks, and then deploy the access points to the locations. You can also keep spare access points in the inventory so that you quickly can deploy an access point if one at a location fails.



CAUTION:

While an access point is in inventory but undeployed (decommissioned), the access point broadcasts its factory default SSIDs and provides open networks without any security. Because the access point is managed by the application, you cannot access its web management interface to implement security. Once you deploy the access point to a location, the security configurations of the WiFi networks at the location are pushed to the access point.

► To add an access point to inventory:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Inventory**.

Role:owner

Status: All

Decommission

Delete

Deploy

+ New Device

☐	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
☐	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
☐	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
☐	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tailac_staging_1511.16.1936.112
☐	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
☐	2XK244NN0012F (AP660-Peets-Riv...	Active	Connected	Peets - Rivermark Plaza			continuous_15.11.16.1923.62
☐	2925345600355 (AP350-Peets-Airpo...	Active	Connected	Peets - San Jose Intl AI...			continuous_15.11.10.2054.54
☐	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peets - San Jose Intl AI...			tailac_staging_1601.05.2320.216
☐	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tailac_staging_1511.16.1936.112
☐	2XK244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

6. Click the **+New Device** button.

Business Central Wireless Manager 2.1 Application

Create a New Access Point

Register Access Point

Serial Number required

Device Name optional

☒ Register this device?

Purchase Date 06/16/2016

Model:

Enter the serial number to determine the model.

Cancel Invalid Serial

7. In the **Serial Number** field, enter the precise serial number for the access point.
If you do not enter a correct serial number, you cannot add the access point to the inventory. After you enter a correct serial number, an image of the associated model displays in the **Model** field, and the gray **Invalid Serial** button changes into the **Save** button.
8. In the **Device Name** field, enter a name for the access point.
The name does not need to be the factory default name.
9. To register the access point with NETGEAR, keep the **Register this device** check box selected and enter your date of purchase in the **Purchase Date** field.
By default, the **Register this device** check box is selected. If you do not need or want to register the access point, clear the check box.
10. Click the **Save** button.
Your settings are saved. The access point is added to the inventory. Because the access point is not deployed at a location, the Inventory Status field in the table shows Decommissioned. After the access point reconnects to the application, the Connection Status field in the table shows Phoned home (and a time indication), which confirms that the access point is connected to the application.

Deploy a Device in Inventory at a Location

If an access point is in inventory and decommissioned, you can deploy it at a location. During the provisioning process, the application upgrades the access point to the cloud-managed firmware version for the location, reboots the access point, pushes the location settings to the access point, and reboots the access point again. This process might take between 5 and 10 minutes.

► To deploy one or more access points at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.

Manage Devices and Device Inventory

Business Central Wireless Manager 2.1 Application

The Monitoring page displays.

4. Select **Inventory**.

Role: owner	Status: All	Decommission	Delete	Deploy	New Device		
	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tallac_staging_1511.16.1936.112
	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
	2XX244NN0012F (AP660-Peets-Riv...	Active	Connected	Peet's - Rivermark Plaza			continuous_15.11.16.1923.62
	2925345600355 (AP350-Peets-Airpo...	Active	Connected	Peet's - San Jose Intl Ai...			continuous_15.11.10.2054.54
	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peet's - San Jose Intl Ai...			tallac_staging_1601.05.2320.216
	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tallac_staging_1511.16.1936.112
	2XX244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The table on the Inventory page displays the access points that are in inventory, whether active, decommissioned, or in the process of being provisioned or decommissioned.

6. To limit the access points in the table to the decommissioned ones, from the **Showing** menu, select **Decommissioned**.

The table on the Inventory page displays decommissioned access points only.

7. Select the check boxes for the access points that you want to deploy at the same location.

8. From the **Deploy** menu, select the location.

A pop-up window opens and lets you confirm your selection.

9. Click the **Deploy** button in the pop-up window.

The application starts the deployment process.

10. Click the **Dismiss** button.

The pop-up window closes.

After the access points are deployed, on the Monitoring page, the Inventory Status fields in the table shows Active and the Connection Status fields in the table shows Connected.

However, if the location to which you added the access points is assigned to an unlicensed account, the Inventory Status fields shows Unlicensed and the access points do not become active until you add a license to the account (see [Add a License to an Account](#) on page 90).



CAUTION:

If access points remain unlicensed and are not active, they broadcast their default SSIDs and provide open networks without any security. Make sure that the account to which you assigned the location is licensed so that the access points become active.

Decommission a Device From a Location and Keep It in Inventory

If an access point is assigned to a location and active, you can decommission it from the location. Upon decommissioning, the access point is reset to factory defaults but with a few configuration exceptions: The cloud mode remains enabled and you can choose to let the access point keep its IP address configuration or reset the IP address configuration to defaults. In either case, the access point remains cloud managed and in inventory. You can redeploy this access point by assigning it to another location. While decommissioned, the access point does not use license credits.

If you choose to reset the IP address configuration to defaults during the decommissioning process, the access point remains in inventory but you might need to reconfigure the access point before you can redeploy it. This option might be useful if the access point requires a static IP address configuration for the location to which you want to deploy it. In such a situation, you might need to access the web management interface of the access point, disable the access point for the cloud, specify a static IP address configuration, and reenabling the access point for the cloud before you can deploy the access point at the new location.



CAUTION:

While an access point is in inventory but decommissioned (undeployed), the access point broadcasts its factory default SSIDs and provides open networks without any security. Because the access point is managed by the application, you cannot access its web management interface to implement security. Once you deploy the access point to a location, the security configurations of the WiFi networks at the location are pushed to the access point.

► To decommission one or more access points from a location:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

Business Central Wireless Manager 2.1 Application

4. Select **Inventory**.

Role: owner	Status: All	Decommission	Delete	Deploy	New Device		
☐	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
☐	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
☐	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
☐	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tallac_staging_1511.16.1936.112
☐	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
☐	2XX244NN0012F (AP660-Peets-Riv...	Active	Connected	Peet's - Rivermark Plaza			continuous_15.11.16.1923.62
☐	2925345600355 (AP350-Peets-Airpo...	Active	Connected	Peet's - San Jose Intl Ai...			continuous_15.11.10.2054.54
☐	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peet's - San Jose Intl Ai...			tallac_staging_1601.05.2320.216
☐	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tallac_staging_1511.16.1936.112
☐	2XX244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The table on the Inventory page displays the access points that are in inventory, whether active, decommissioned, or in the process of being provisioned or decommissioned.

6. To limit the access points in the table to the active ones, from the **Showing** menu, select **Active**.

The table on the Inventory page displays active access points only.

7. Select the check boxes for the access points that you want to decommission.

The **Decommission** button becomes available.

8. Click the **Decommission** button.

A pop-up window opens and displays a warning.

9. To keep the IP address configurations after the access points are decommissioned, select the **Preserve IP Config** check box.

10. Click the **Decommission** button in the pop-up window.

The application start the decommissioning process.

11. Click the **Dismiss** button.

The pop-up window closes.

After the access points are decommissioned, the Inventory Status fields in the table show Decommissioned - IP (that is, if you preserved the IP configurations). After the access points reconnect to the application, the Connection Status fields in the table show Phoned home (and a time indication), which confirms that the access points are connected to the application.

Remove a Device From Inventory

You can remove an access point from inventory. The access point resets to factory defaults and becomes a standalone access point. That is, the serial number is removed from the application and the access point is no longer cloud managed. If you want to keep the access point in inventory and cloud managed, do not

Business Central Wireless Manager 2.1 Application

remove (that is, delete) the access point, but decommission it from the location (see *Decommission a Device From a Location and Keep It in Inventory* on page 82).



CAUTION:

If an access point is removed from inventory, it is no longer managed by the application, resets to factory default settings, broadcasts its default SSIDs, and provides open networks without any security. If you do not want open networks, connect to the access point through its web management interface and implement WiFi security or disable the radios.

► To remove one or more access points from inventory:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Inventory**.

Role: owner		Status: All	Decommission	Delete	Deploy	New Device	
☐	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
☐	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
☐	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
☐	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tallac_staging_1511.16.1936.112
☐	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
☐	2XX244NN0012F (AP660-Peets-Riv...	Active	Connected	Peet's - Rivermark Plaza			continuous_15.11.16.1923.62
☐	2925345600355 (AP350-Peets-Airpo...	Active	Connected	Peet's - San Jose Intl Ai...			continuous_15.11.10.2054.54
☐	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peet's - San Jose Intl Ai...			tallac_staging_1601.05.2320.216
☐	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tallac_staging_1511.16.1936.112
☐	2XX244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The table on the Inventory page displays the access points that are in inventory, whether active, decommissioned, or in the process of being provisioned or decommissioned.

6. To limit the access points in the table to the decommissioned ones, from the **Showing** menu, select **Decommissioned**.

The table on the Inventory page displays decommissioned access points only.

7. Select the check boxes for the access points that you want to remove from inventory.
The **Delete** button becomes available.

Manage Devices and Device Inventory

8. Click the **Delete** button.
A pop-up window opens and displays a warning.
9. Click the **Delete** button in the pop-up window.
The access points are removed from inventory.
10. Click the **Dismiss** button.
The pop-up window closes.

The application provides one default account. Unless you specify otherwise, all locations, licenses, and collaborators are added to the default account. However, you can set up multiple accounts (also referred to as license accounts) under the application. For managed service providers (MSPs), also referred to as value added resellers (VARs), working with multiple accounts allows for management of a variety of customers. For more information, see [Accounts Overview](#) on page 87.

This chapter includes the following sections:

- [Accounts Overview](#) on page 87
- [Licenses Overview](#) on page 87
- [About the Trial Period](#) on page 87
- [Create a New Account](#) on page 89
- [Add a License to an Account](#) on page 90
- [View License Information for an Account](#) on page 92
- [Add a Location to an Account](#) on page 93
- [Remove a Location From an Account](#) on page 94
- [View the Devices Managed Under an Account](#) on page 95
- [Invite a Manager, Customer, or Clerk to an Account](#) on page 95
- [Accept an Invitation and Sign Up for and Activate a Manager, Customer, or Clerk Account](#) on page 96
- [Remove a Manager, Customer, or Clerk From an Account](#) on page 98
- [Change the Name for an Account](#) on page 99
- [Remove an Account](#) on page 100
- [Change Your Account Email Address and Password](#) on page 101

Accounts Overview

If you sign up for a BCWM application account, you become the owner of the account. Under the umbrella of that account, you can set up multiple license accounts. The application provides one default license account under which all locations, licenses, and collaborators are placed. If you set up additional license accounts, you can specify the locations for each account, add licenses to each account, and invite managers and customers for each account.

If you manage a tenant account (that is, an account for a single business or organization), a single license account might be sufficient even if you set up multiple locations for that business or organization, or various conditions might require you set up multiple license accounts. Consider the example in which you manage the WiFi networks for a hotel chain with multiple locations in various countries:

- If you centrally manage the WiFi networks and access points for all individual properties in the hotel chain and the business cost of WiFi management is charged to a single department in the hotel chain, a single license account for the entire hotel chain is sufficient.
- If the business cost of WiFi management is charged to each individual property in the hotel chain, set up a license account for each property and add the required licenses to each license account.
- If each individual property in the hotel chain must be able to manage its own WiFi networks and access points through a collaborator, set up a license account for each location and add a collaborator account to each license account.

If you manage the WiFi networks and access points for multiple tenants (that is, separate businesses and organizations), you *do* want to set up a separate license accounts for each individual business and organization, even if that business or organization consists of a single location. Even though you use a single BCWM application account, all license accounts are segmented and secure, that is, data is confined within each partition.

Licenses Overview

A license consists of credits. Each access point that the application manages requires one credit per day. That is, each credit provides one access point with one day of cloud usage.

After all credits are used up, the licence must be renewed for you to continue to use the application.

For example, if you purchased 3 licenses for 10 access points for 3 years (resulting in a credit balance of 10,950 credits) and the application manages 24 access points per day, you must renew your licenses after 438 days. Another example: If you purchased 12 licenses for 1 access point for 1 year (resulting in a credit balance of 4,380 credits) and the application manages 6 access points per day, you must renew your licenses after 2 years (730 days).

You can purchases licenses in the form of license keys for 1, 10, or 50 access points for either 1 or 3 years.

About the Trial Period

The trial period starts when you set up and activate your BCWM subscription and lasts 90 days.

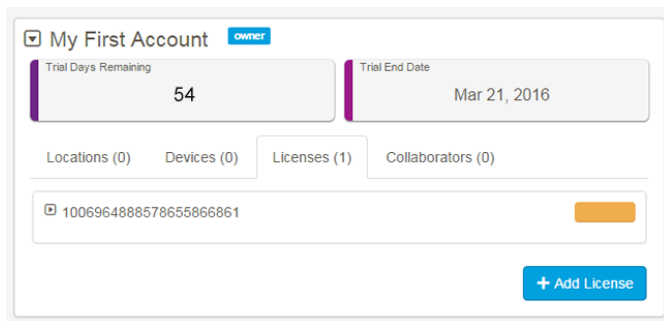
NETGEAR does not impose any special limits to the number of locations, networks, and access points that you can add during the trial subscription. An account with a free trial subscription or paid-for subscription can support up to 4,000 access points.

View the Trial Balance and Trial Expiration Date During the Trial Period

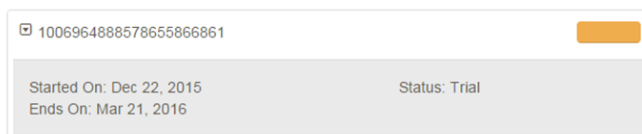
Your trial period starts when you subscribe to the application and lasts 90 days. At any time during the trial period, you can view how many days are left in the trial period and you can view the trial expiration date.

► To view the trial balance and expiration date:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default trial license account displays. By default, the **Locations** tab is selected.
5. Click the **Licenses** tab.



6. To display details about the trial license, click the triangle icon to the left of the license key.



For information about adding a purchased license to an account with a trial subscription, see [Add a License to an Account](#) on page 90.

What Happens at the End of the Free Trial Period?

Two weeks before the end of the trial period, the application displays alerts about the scheduled end of the trial period and you start to receive email messages notifying you of the pending end of the trial period. Before the end of the trial period, you can purchase access point licenses to continue with the application without service interruption. That is, you can convert your account with a free trial subscription to an account with a paid-for subscription. For more information, see [Add a License to an Account](#) on page 90.

If you decide not to purchase access point licenses, you eventually lose full access to the application and its WiFi networks, as follows:

- When the trial period ends, the one-month grace period starts. During this period, you are still granted full access to the application and can purchase and add access point licenses.
- When the grace period ends, the access points stop being managed by the application, are removed from inventory, reset to their factory default configuration, and start functioning in standalone mode. As a consequence, the cloud-managed WiFi networks no longer function. However, you can still access the application, add access point licenses, and reprovision the access points and WiFi networks. To use the access points after they are removed from the application, you can reprovision them on an account with a paid-for subscription (that is, an account with access point licenses), reprovision them with a NETGEAR hardware-based wireless controller platform, or manually reconfigure them for standalone service.

Note During the free trial period, you can provision an access point for a single BCWM account only. You cannot reprovision the same access point for another BCWM account, that is, you cannot set up successive accounts with trial subscriptions and keep adding the same access points to different accounts.

Create a New Account

If you manage one or more locations for a single business or organization (that is, you manage a tenant account), a single account might be sufficient. However, if you manage multiple businesses and organizations (that is, you manage multiple tenants), each with one or more locations, set up separate license accounts.

You can create multiple license accounts to which you can add locations (and therefore access points that are assigned to those locations), licenses, and collaborators.

► To create a new license account:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
5. At the top of the page, in the **New Account Name** field, enter a name for the account.
6. Click the **+ Create** button.
The new account displays.

For more information about configuring the new account, see the following sections:

- *Add a License to an Account* on page 90
- *Add a Location to an Account* on page 93
- *Invite a Manager, Customer, or Clerk to an Account* on page 95

Add a License to an Account

You can add one or more licenses to a single license account.

Note If you add a purchased license to a trial account, any remaining days in the trial period are forfeited. The license period starts on the day that you add the license.



CAUTION:

If you created multiple license accounts, make sure that you add the license to the correct license account. Once added, you cannot move the license to another license account.

► **To add a license to a license account:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
The Credits Available, Renewal Date, and Credits Used Per Day boxes display under the license account name.
5. For the license account to which you want to add a license, under the boxes described in the previous step, click the **Licenses** tab.
The page displays the active licenses for the license account. If you did not yet add any licenses, none are shown.
6. Click the **+ Add License** button.
A field displays.

Business Central Wireless Manager 2.1 Application

- Copy or type your license key in the field.

The screenshot shows the 'License Accounts (2)' form. At the top is a 'New Account Name' input field with a '+ Create' button. Below this is a card for 'SydneyWiFiMgmt' with an 'owner' tag. The card contains three input fields: 'Credits Available' (0), 'Renewal Date' (empty), and 'Credits Used Per Day' (empty). Below these are tabs for 'Locations (2)', 'Devices (2)', 'Licenses (0)', and 'Collaborators (1)'. At the bottom is a license key input field containing 'NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-3333' with green and red checkmark buttons.

- Click the green check icon.

The screenshot shows the 'License Accounts (2)' form after the license key has been added. The 'Credits Available' field now shows 365, the 'Renewal Date' field shows 'Jun 22, 2016', and the 'Credits Used Per Day' field shows 2. The 'Licenses (1)' tab is now active. The license key input field at the bottom now has a green bar to its right, indicating the license is valid.

The license is added and the following information is shown in the boxes:

- Credits Available.** The total number of available credits for *all* licenses added to the license account. (In the previous figure, only a single license is shown for the license account.)
- Renewal Date.** The date on which you run out of credits for the license account.
- Credits User Per Day.** The total number of credits that are consumed per day for the license account.
Only active access points consume credits. An access point that is in inventory but not assigned to a location does not consume credits.

In the previous figure, to the right of the license key, a green bar displays, indicating that the full license is still available and that no credits were used yet. If credits were used already, the bar would be orange.

View License Information for an Account

For each license account, you can view the license information.

► **To view license information for a license account:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.

The screenshot shows a web interface for a 'Default' license account. At the top, there are three summary boxes: 'Credits Available' with the value 1343, 'Renewal Date' with the value Jun 23, 2016, and 'Credits Used Per Day' with the value 9. Below these are four tabs: 'Locations (6)', 'Devices (9)', 'Licenses (4)', and 'Collaborators (8)'. The 'Licenses (4)' tab is selected, showing a list of four license keys. Each key is preceded by a checkbox and followed by a status indicator (a small orange or green bar). The license keys are: NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-8001, NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-8002, NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-8003, and NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-8004. At the bottom right of the list is a blue button labeled '+ Add License'.

The following information displays for the license account:

- **Credits Available.** The total number of available credits for *all* licenses added to the license account.
- **Renewal Date.** The date on which you run out of credits for the license account.
- **Credits User Per Day.** The total number of credits that are consumed per day for the license account.
Only active access points consume credits. An access point that is in inventory but not assigned to a location does not consume credits.

Note If you added more than one license account to the application, the credit and renewal date information that is shown for this license account does not apply to the other license accounts. Each license account provides its own credit and license information.

Business Central Wireless Manager 2.1 Application

To the right of the license key, either an orange bar or a green bar displays:

- **Orange bar.** The license is being used, that is, credits were used already.
- **Green bar.** The full license is still available, that is, no credits were used yet.

5. To display details about a license, click the triangle icon to the left of the license key.

☐ NG1234-AAAA-BBBB-CCCC-DDDD-EEEE-1111-2222-8001 

Date Added: Jan 8, 2016	SKU: WM1AP1YL-10000S
Date Activated: Jan 25, 2016	Credits Used: 117
Last Charged: Jan 25, 2016	Credits Remaining: 248
Expires On: Jan 8, 2017	Status: In Use

Add a Location to an Account

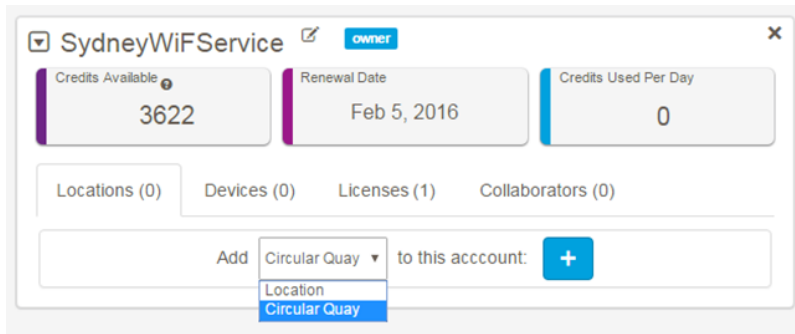
When you add a location, you must assign it to a license account. Therefore, you can add an existing location to a license account only if the location is no longer assigned to another license account because you removed the location from the other license account (see [Remove a Location From an Account](#) on page 94).

IMPORTANT:

If you do not add at least one license to the license account (see [Add a License to an Account](#) on page 90), access points that you add to the location remain in the unlicensed state, broadcast their default SSIDs, provide open networks without any security, and do not become active, preventing WiFi networks that you add to the location from coming up.

► To add a location to a license account:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays. By default, the **Locations** tab is selected.
5. For the license account to which you want to add a location, select the location from the **Add Location** menu.



Only unassigned locations display in the menu.

6. Click the blue + button.

The location is added and displays under the **Locations** tab. The devices that are assigned to the location display automatically under the **Devices** tab.

Remove a Location From an Account

If you want to add a location to another license account, you first must remove the location from the default license account or any other license account that it might be assigned to.



CAUTION:

If you remove a location from a license account but do not assign it to another license account, access points that you added to the location remain in the unlicensed state, broadcast their default SSIDs, provide open networks without any security, and do not become active, preventing WiFi networks that you added to the location from coming up.

► To remove a location from a license account:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays. By default, the **Locations** tab is selected.
5. For the license account from which you want to remove the location, click the **x** to the right of the location.
The location is removed from the license account but is added as a selection in the **Add Location** menu that is available for any license account.

If you want to add the location to another license account, simply select the location from the **Add Location** menu for that license account, and click the blue + button.

View the Devices Managed Under an Account

You cannot add devices to a license account. You can add devices to a location. When you assign a location to a license account, all devices that you added to the location are automatically assigned to the license account.

By default, all locations are assigned to the default license account. Therefore, by default, all devices are also assigned to the default license account.

► To view the devices that are managed under a license account:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
5. For the license account for which you want to view the managed devices, click the **Devices** tab.
The managed devices display.

Invite a Manager, Customer, or Clerk to an Account

The application supports the following roles for users who can log in to the application. These users are different from WiFi users and hotspot users who can connect to a network that is part of the cloud but who cannot log in to the application.

- **Owner.** A user who subscribed to the application and owns all license accounts that are set up under his or her application subscription. An owner can perform any action, including inviting collaborators (managers, customers, and clerks).
- **Manager.** A user who can perform most administrative functions. A manager (also referred to as a cloud network administrator) is authorized to perform many application functions for license accounts that he or she does *not* own.
Although a manager can set up his or her own new license account (and therefore become owner of that account), a manager can also access other license accounts (that is, accounts that were set up by other users) and can invite collaborators for other license accounts. However, a manager cannot add or remove a location from another license account, decommission or remove devices from a location for another license account, or entirely remove another license account.
- **Customer.** A user with read-only access to the license account to which he or she was invited, including all locations, WiFi networks, and access points that are assigned to that license account. Although a customer can set up his or her own license account (and therefore become owner of that account), a

customer cannot access other license accounts to which he or she was not invited and cannot invite collaborators for other license accounts.

- **Clerk.** A user who can only sell, print, and email vouchers and monitor their use for paid-for captive portal access for the license account to which he or she was invited. A clerk is also referred to as a voucher clerk or hotspot clerk. As with other users, a clerk can set up his or her own license account (and therefore become owner of that account).

Owners, managers, customers, and clerks are referred to as collaborators.

► To invite a collaborator to an account:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
5. For the license account for which you want to invite a collaborator, click the **Collaborators** tab.
Any existing collaborators for the license account display. (An owner of a license account is not a collaborator.)
6. Click the **Invite Collaborator** button.
7. From the **Select role** menu, select **Manager**, **Customer**, or **Clerk**, and in the field next to the menu, enter the email address of the collaborator.
8. Click the green check icon.
The collaborator is added to the license account and receives an invitation email message.

For information about how to accept an invitation and sign up for the application account, see [Accept an Invitation and Sign Up for and Activate a Manager, Customer, or Clerk Account](#) on page 96.

Accept an Invitation and Sign Up for and Activate a Manager, Customer, or Clerk Account

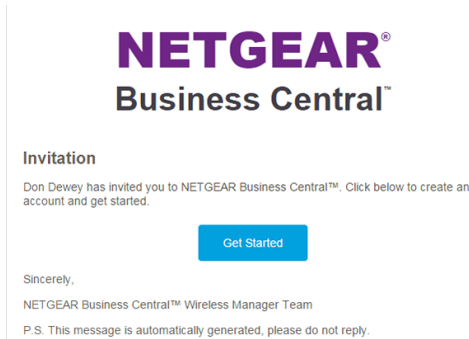
A user with an owner account or manager account can send an invitation email to invite someone to set up a manager, customer, or clerk account. A user with a customer account can send an invitation email to someone only to set up a clerk account. For information about these types of application users, which are referred to as collaborators, see [Application Roles](#) on page 12.

If you receive such an invitation, before you can access the application, you must accept the invitation, sign up for a user account, and activate the user account.

Business Central Wireless Manager 2.1 Application

► To accept an invitation and sign up for an activate a manager, customer, or clerk account:

1. Go to your email inbox and open the invitation email message.



Make sure that you are online.

2. Click the **Get Started** button in the email. message.

The Create Account page displays.

If the page does not display, open a browser and enter **<https://bc.qa.netgear.com/#/user/signup>** in the address bar.

A screenshot of the 'Create Account' web form. It contains several input fields: Email, Password, Confirm Password, First Name, Last Name, Company Name, Street Address, Apt. Suite, Bldg. (optional), City, State/Province/Region, Zip/Postal Code, Country, and Phone Number. Each field has a red asterisk indicating it is required. Below these fields is a 'Category' section with two radio buttons: 'Managed Service Provider' (selected) and 'End User'. A link for 'Terms and Conditions' is provided. At the bottom is a large 'Create Account' button with a user icon, and a smaller 'Login' link.

3. Complete all fields.

The password length can be from 6 to 128 symbols. Valid symbols are a–z, A–Z, and 0–9, and the following special characters:

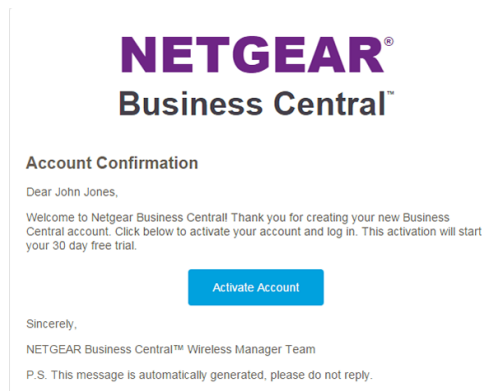
* ! @ # \$ % ^ & ()"

4. If you are a VAR, reseller, or managed service provider and you are managing one or more end user accounts, select the **Managed Service Provider** radio button. Otherwise, select the **End User** radio button.

Business Central Wireless Manager 2.1 Application

After you complete all fields, the **Create Account** button becomes available.

5. To view the terms and conditions, do the following:
 - a. Click the **Terms and Conditions** link.
The END USER LICENSE AGREEMENT FOR NETGEAR Cloud Management Platform page displays.
 - b. Scroll through and read the agreement, and if you agree, click the **Agree** button.
The page closes and the Create Account page displays again.
6. Click the **Create Account** button.
The *Welcome to Business Central!* message displays and an email message is sent to the email address that you specified.
7. Go to your email inbox and open the email message.



8. Click the **Activate Account** button in the email message.
The application login page displays again and shows the message *Email Confirmed. Please log in.* Your email address and password are entered automatically.
9. To log in to the application, click the **Login** button.
The Monitoring page displays.

Remove a Manager, Customer, or Clerk From an Account

You can remove a manager, customer, or clerk (referred to as collaborators) from an account if his or her involvement is no longer required.

► To remove a collaborator from an account:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.

The Monitoring page displays.

4. Select **Accounts**.

The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.

5. For the license account for which you want to remove a collaborator, click the **Collaborators** tab. Any existing collaborators for the license account display. (An owner of a license account is not a collaborator.)

6. To the right of the collaborator that you want to remove, click the **x**.
The collaborator is removed and can no longer log in to the BCWM.

Change the Name for an Account

You can change the name for an account that you added.

Note The default name for a trial license account is *My First Account*. You cannot change that name until you purchase a license and add it to the account.

► **To change the name for a license account:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
5. For the license account for which you want to change the name, click the edit icon .
The name becomes editable.
6. Enter a new name in the field.
7. Click the green check icon.
Your settings are saved.

Remove an Account

If absolutely required, you can remove a license account that you no longer need.



WARNING:

Deleting a license account is a serious operation! All licenses that you added to this account will be lost and the remaining balance of unused credits will be forfeited.

Locations that were added to the account are not deleted but can be added to another account. However, collaborator accounts are deleted.

Rather than entirely removing an account to which you added licenses, alternate solutions exist. Consider a situation in which a managed service provider (MSP) services a customer for which a license account exists and for which the MSP added a license, a location, and a collaborator. If the customer decides to stop service, rather than entirely removing the license account, the MSP can do the following:

- The MSP removes the customer as a collaborator from the license account.
- The MSP removes the customer's location (and customer's access points) from the license account.

Until the MSP decides to add a new customer and location to the license account, the license account remains idle and no license credits are used. In this way, the license account does not need to be removed and no unused credits are forfeited.

► **To remove a license account:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Accounts**.
The Accounts page displays the license accounts. If you did not create a license account, only the default license account displays.
5. To the right in the pane of the license account that you want to remove, click the **x**.
A pop-up window opens and displays a warning.
6. Click the **Delete** button in the pop-up window.
The license account is removed.

Change Your Account Email Address and Password

Your account settings include the email address and password to access the BCWM. You can change these settings.

► **To change your account email address and password:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the upper right of the page, click the menu with your name, and select **Account Settings**.
The Accounts Settings page displays.
5. Change the settings as needed:
 - **Current Password.** To make any changes on the page, enter your current password. To make the passwords on the page visible, click the **Show Passwords** button.
 - **New Email Address.** To change your current email address, enter a new email address.
 - **New Password.** To change your current password, enter a new password.
 - **Confirm New Password.** If you are changing your password, repeat the new password.
6. Click the **Save** button.
Your settings are saved.

Monitor Your Locations, Networks, and Devices

7

You can view summary and detailed information about all locations and about individual locations, WiFi networks, and devices that you manage under your account, including real-time and historical information, performance statistics, and traffic usage.

This chapter includes the following sections:

- *Overview of the Monitoring Options* on page 103
- *View Alarms for Your Account, Claim Alarms, and Resolve Alarms* on page 104
- *Set Up Email Notification Profiles for License Accounts and Locations* on page 108
- *Change or Remove an Email Notification Profile* on page 109
- *View the Status of All Locations and Devices Under Your Account* on page 110
- *Monitor a Single Location* on page 113
- *Monitor a Single WiFi Network at a Location* on page 122
- *Monitor a Single Device at a Location* on page 128

Overview of the Monitoring Options

The monitoring options of the application let you view the status of your WiFi networks and devices for all locations and for a specific location, WiFi network, and device. You can also view, claim, and resolve alarms for all locations or for a specific location and device. The following table shows the monitoring options, each of which is described in detail in this chapter.

Table 3. Monitoring options

Component and Drill Down	
All (See View the Status of All Locations and Devices Under Your Account on page 110.) • Device status (Online, Offline, Waiting, and Upgrading) for all locations • Alarm status (critical alarms and noncritical alarms) for all locations • Critical alarms for all locations • Location map for all locations	
Single Location	Usage (See View WiFi Usage at a Location on page 113.) • Number of connected clients • Total network usage • Usage per wireless network • Usage per radio band
	Health (See View the Status of Devices at a Location on page 115.) • Device status (Online, Offline, Waiting, and Upgrading) • Alarm status (critical alarms and noncritical alarms) • Critical alarms
	Neighborhood (See View Neighbor and Rogue Access Points at a Location on page 117.) • Number of neighbor access points • Number of rogue access points
	Connected clients (See View Clients Connected at a Location on page 119.)
	Event logs (See View the Event Logs for a Location on page 120.)

Table 3. Monitoring options (Continued)

Component and Drill Down	
Wireless networks	WiFi networks assigned to the location
Single wireless network	Usage (See View Usage of a WiFi Network on page 122.) - Number of connected clients - Wireless network usage
	Connected clients (See View Clients Connected to a WiFi Network on page 124.)
	Event logs (See View the Event Logs for a WiFi Network on page 125.)
	Captive portal sessions (See View Captive Portal Sessions on page 127.)
Devices	Devices assigned to the location
Single device	Usage (See View WiFi Usage on a Device on page 129.) - Number of connected clients - Average wireless usage over time per wireless network - Average wireless usage over time per radio
	Connected clients (See View Clients Connected to a Device on page 130.)
	Alarms (See View Alarms for a Device, Claim Alarms, and Resolve Alarms on page 131.)
	Event logs (See View the Event Logs for a Device on page 134.)

View Alarms for Your Account, Claim Alarms, and Resolve Alarms

You can view the alarms table for your account and filter the table by time, location, and whether or not alarms were claimed. You can also claim and resolve alarms.

Claiming or resolving an alarm means the following:

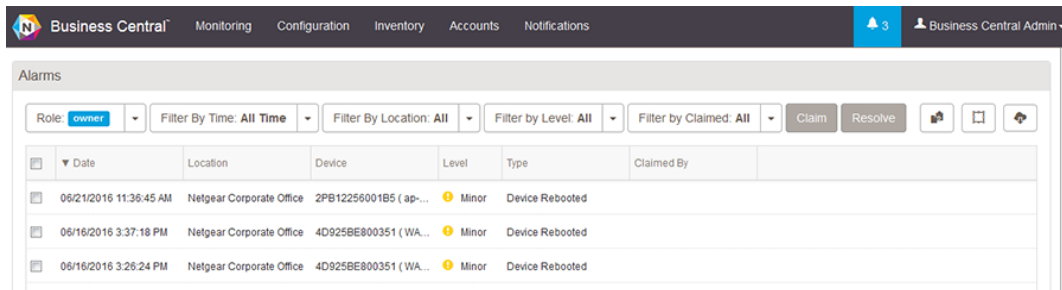
- **Claim an alarm.** You take responsibility for the alarm and can add an optional note. Others can open the pop-up window for the alarm and view the note. The alarm remains in the alarms table and the Claimed by field in the table shows your email address.
- **Resolve an alarm.** You mark the alarm as resolved and can add an optional resolution note. (A future release will support historical alarm tables in which you can view the resolution notes.) The alarm is removed from the alarms table.

Alarms are classified in four categories or severity levels: Critical (for example, a device disconnected), Major (for example, a device command failure occurred), Minor (for example, a device rebooted), and Info (for example, a device reconnected).

Business Central Wireless Manager 2.1 Application

► To view the alarms for your account, filter the alarms table, claim or resolve alarms, copy alarm table entries, or download the entire alarm table:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the top menu bar next to your name on the right, click the bell icon.
The total number of alarms for your account is stated next to the bell icon.



Date	Location	Device	Level	Type	Claimed By
06/21/2016 11:36:45 AM	Netgear Corporate Office	2PB12256001B5 (ap-...	Minor	Device Rebooted	
06/16/2016 3:37:18 PM	Netgear Corporate Office	4D925BE800351 (WA...	Minor	Device Rebooted	
06/16/2016 3:26:24 PM	Netgear Corporate Office	4D925BE800351 (WA...	Minor	Device Rebooted	

The table is sorted by the time the alarm occurred. You can resort the table by clicking a column heading.

5. To filter the alarms by type of user account, in the **Role** menu, select **owner**, **manager**, or **customer**.
The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Alarms page.
6. To filter the alarms table by time, in the **Filter by Time** menu, select **Last Hour**, **Last 24 Hours**, or **Last 72 Hours**.
By default, the selection is **All Time**.
7. To filter the alarms table by location, in the **Filter by Location** menu, select the location.
You can also search for a location. By default, the selection is **All** (locations).
8. To filter alarms by severity level, in the **Filter by Level** menu, select **All**, **Info**, **Minor**, **Major**, or **Critical**.
By default, alarms of all severity levels (**All**) are displayed.
9. To filter the table by claimed or unclaimed alarms, in the **Filter by Claimed** menu, select **Claimed** or **Unclaimed**.
By default, the selection is **All** (alarms).
10. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.

11. To claim alarms, do the following:

To claim a single alarm, do the following:

- a. Click the alarm row in the table.

2XX244NC0001A (B...

A Device reboot has been detected

⚠ This Alarm has not been resolved

[Go to Access Point](#)

Claim Optional notes...

Resolve Resolution message

Hide

- b. In the **Optional notes** field, enter a message for management purposes only.
- c. Click the **Claim** button in the pop-up window.
The pop-up window closes. The Claimed by field in the table shows your email address.

To claim several or all alarms simultaneously, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select groups of entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the **Claim** button above the table.
A pop-up window opens.
- c. Enter an optional message for management purposes only.
- d. Click the **Claim** button in the pop-up window.
The pop-up window closes. The Claimed by fields in the table shows your email address.

12. To resolve alarms, do the following:

To resolve a single alarm, do the following:

- a. Click the alarm row in the table.

2XX244NC0001A (B...

A Device reboot has been detected

Claimed by okaywhatnowthen3@gmail.com on
02/11/2016 1:20:07 PM (a few seconds ago)

Roland

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Resolve

Resolution message

Hide

The previous figure shows a claimed alarm. If the alarm was not claimed, the pop-up window would show both the **Claim** and **Resolve** buttons.

- b. In the **Resolution message** field, enter a message for management purposes only.
- c. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarm is removed from the table.

To resolve several or all alarms simultaneously, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select groups of entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the **Resolve** button above the table.
A pop-up window opens.
- c. Enter an optional message for management purposes only.
- d. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarms are removed from the table.

13. To copy some or all of the table entries, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select multiple entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the copy icon (, the leftmost icon).
The selected entries are placed on the Clipboard.

14. To download the entire table as a CSV file, do the following:

- a. Click the download icon (, the rightmost icon).
A pop-up window opens.
- b. Navigate to a location and save the file.

Set Up Email Notification Profiles for License Accounts and Locations

You can set up multiple email notification profiles that allow you to receive alarms that occur for specific license accounts, locations, or both.

► **To set up an email notification profile:**

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Notifications**.
The Notifications page displays.
5. Click the **+ New** button.

Create a new Notification

Contact Name This will be used to personalize alarm emails.

Email Address We will send emails to this address when an Alarm is triggered.

Notify On The filter controls which alarm types trigger notifications.

For which accounts do you want to receive license alerts?

☐	Account Name	Locations	Credits	Role
☐	My First Account	1	0	Owner
☐	SydneyWiFiService	0	0	Owner

For which locations do you want to receive alarms?

☐	Location	Location	Wireless Networks	Devices	Role
☐	Bondi Beach	Ramsgate Ave E, North Bondi NSW 2026, Australia	2	2	Owner
☐	Circular Quay	Circular Quay, Sydney NSW 2000, Australia	1	0	Owner

6. In the **Contact Name** field, enter your name.
7. In the **Email Address** field, enter the email address at which you want to receive notifications.
8. From the **Notify On** menu, select the severity levels of the alarms for which you want to be notified:
 - **All Alarms.** This is the default setting.
 - **Minor, Major, and Critical Alarms.**
 - **Major & Critical Alarms.**
 - **Critical Alarms Only.**
9. Select the check boxes for the license accounts and locations for which you want to receive notifications.

To receive notifications for all license accounts or all locations, select the check box in a table heading.

10. Click the **Save** button.

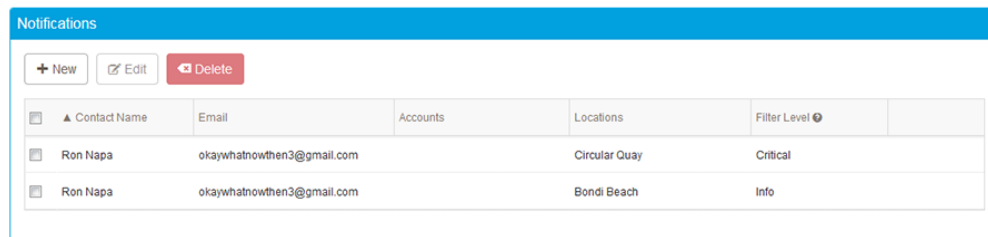
The email notification profile is saved and you start to receive email messages when alarms occur.

Change or Remove an Email Notification Profile

You can change or remove an email notification profile. However, you cannot select which types of alarms you will receive notifications for.

► To change or remove an email notification profile:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Notifications**.



☐	▲ Contact Name	Email	Accounts	Locations	Filter Level ⓘ	
☒	Ron Napa	okaywhatnowthen3@gmail.com		Circular Quay	Critical	
☒	Ron Napa	okaywhatnowthen3@gmail.com		Bondi Beach	Info	

5. Select the check box for a contact name.
6. To change an email notification profile, do the following:
 - a. Click the **Edit** button.
The Edit Notification page displays
 - b. Make the changes as needed.
 - c. Click the **Save** button.
7. To delete an email notification profile, do the following:
 - a. Click the **Delete** button.
A pop-up window opens and displays a warning.
 - b. Click the **Delete** button in the pop-up window.
The email notification profile is removed.

View the Status of All Locations and Devices Under Your Account

To give you a high-level overview of the status of all locations and devices under your account, you can monitor the following components for *all locations* together:

- Device status (Online, Offline, Waiting, and Upgrading)
- Alarm status (critical alarms and noncritical alarms)
- List of critical alarms for all locations
- Location map

Claiming or resolving an alarm means the following:

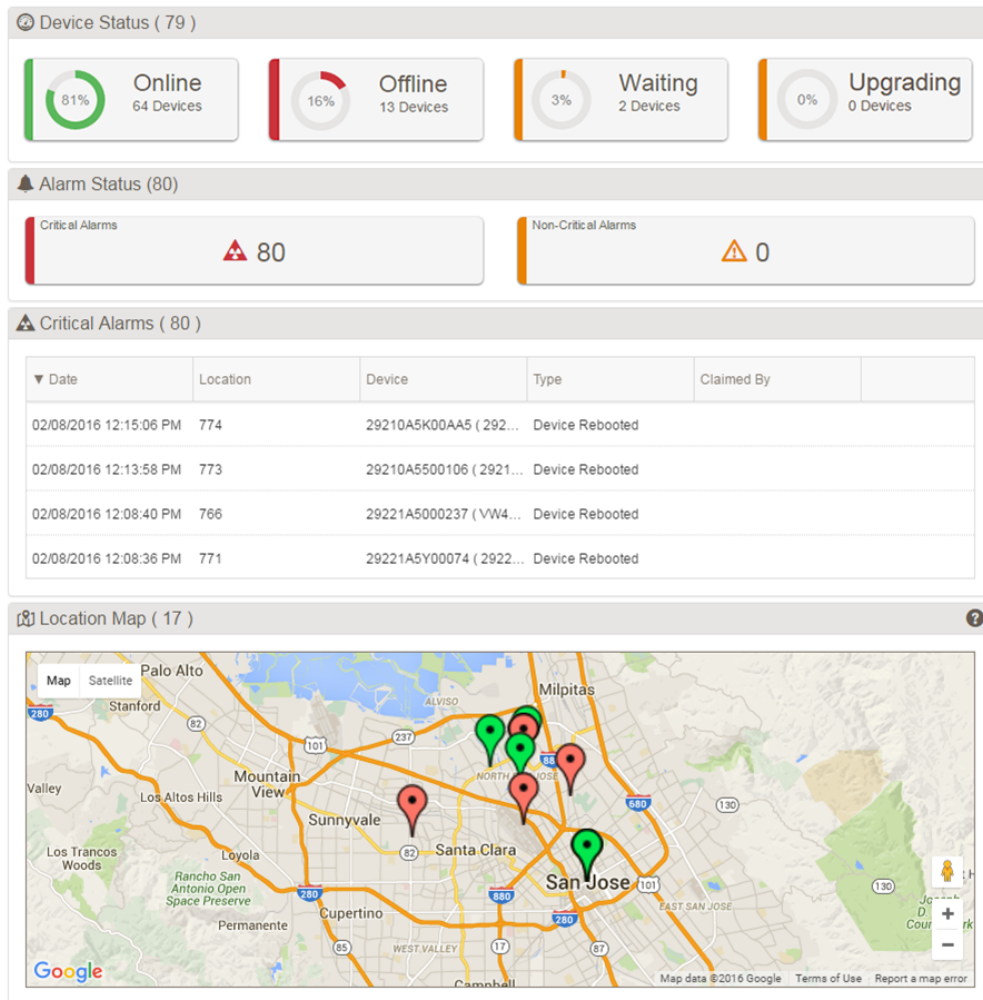
- **Claim an alarm.** You take responsibility for the alarm and can add an optional note. Others can open the pop-up window for the alarm and view the note. The alarm remains in the alarms table and the Claimed by field in the table shows your email address.
- **Resolve an alarm.** You mark the alarm as resolved and can add an optional resolution note. (A future release will support historical alarm tables in which you can view the resolution notes.) The alarm is removed from the alarms table.

► To view the status of all locations and networks under your account, claim an alarm, or resolve an alarm:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

Business Central Wireless Manager 2.1 Application

- At the very top of the Locations tree on the left, make sure that **All** is selected.



- Drill down for more detailed information as explained in the following table.

Component	Information
Device Status	The total number of devices that are managed under the BCWM account is stated. Click the Online, Offline, Waiting, or Upgrading tab to view a list of devices. Devices that are offline, waiting, or upgrading cannot broadcast WiFi networks. In the list of devices, click a device to view detailed information about the device. For more information, see Monitor a Single Device at a Location on page 128.
Alarm Status	The total number of alarms for devices that are managed under the BCWM account is stated. Click the Critical Alarms or Non-Critical Alarms tab to view a list of alarms. In the list of alarms, scroll down to view more alarms. Click an alarm to view more information about the alarm, claim the alarm (see Step 6), or resolve the alarm (see Step 7).

(Continued)

Component	Information
Critical Alarms	The total number of critical alarms for devices that are managed under the BCWM account is stated. View the same list of alarms and scroll down to view more alarms. Click an alarm to view more information about the alarm, claim the alarm (see Step 6), or resolve the alarm (see Step 7).
Location Map	The total number of locations that are managed under the BCWM account is stated. Each location is indicated by a marker. A green marker indicates that all devices at the location are up. A red marker indicates that one or more devices at the location are down. Click a marker to open a pop-up window with information. Click the location link in the pop-up window to view information about the location. For more information, see Monitor a Single Location on page 113.

6. To claim an alarm, do the following:

- a. Select the check box for the alarm.
- b. Click the **Claim** button.

2XX244NC0001A (B...

A Device reboot has been detected

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Claim

Optional notes...

Resolve

Resolution message

Hide

- c. In the **Optional notes** field, enter a message for management purposes only.
- d. Click the **Claim** button in the pop-up window.
The pop-up window closes. The Claimed by field in the table shows your email address.

7. To resolve an alarm, do the following:

- a. Select the check box for the alarm.
- b. Click the **Resolve** button.

2XX244NC0001A (B...

A Device reboot has been detected

Claimed by okaywhatnowthen3@gmail.com on
02/11/2016 1:20:07 PM (a few seconds ago)

Roland

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Resolve

Resolution message

Hide

- c. In the **Resolution message** field, enter a message for management purposes only.
- d. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarm is removed from the table.

Monitor a Single Location

You can the monitor the following components for a single location:

- **Usage.** Number of connected clients, total WiFi network usage, usage per WiFi network, and usage per radio band.
For more information, see [View WiFi Usage at a Location](#) on page 113.
- **Health.** Device status, alarms status, and critical alarms.
For more information, see [View the Status of Devices at a Location](#) on page 115.
- **Neighborhood.** Number of neighbor access points and number of rogue access points.
For more information, see [View Neighbor and Rogue Access Points at a Location](#) on page 117.
- **Connected clients.** Details about connected clients.
For more information, see [View Clients Connected at a Location](#) on page 119.
- **Event logs.** Details about events that occurred.
For more information, see [View the Event Logs for a Location](#) on page 120.

View WiFi Usage at a Location

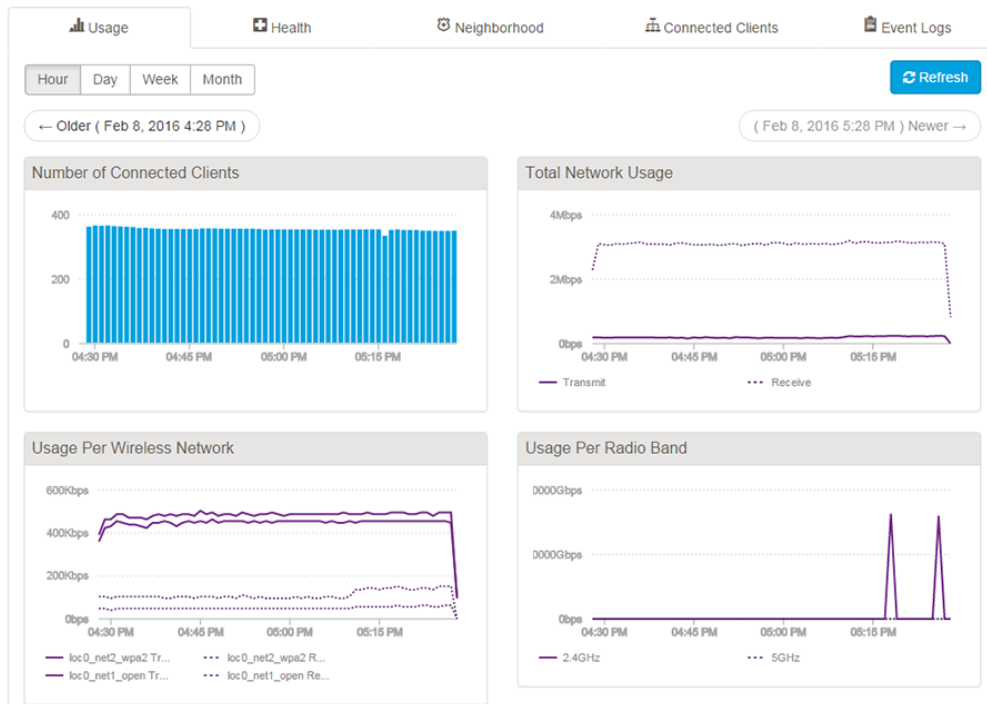
You can view the WiFi usage for a location, broken out into the following components:

- Number of connected clients at the entire location
- Total WiFi network usage at the entire location
- Usage per WiFi network
- Usage per radio band (2.4 GHz and 5 GHz)

Business Central Wireless Manager 2.1 Application

► To view WiFi usage at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click a location.
By default, the **Usage** tab is selected.



By default, the **Hour** button is selected.

5. To view information for a different period, click the **Day**, **Week**, or **Month** button.
6. To view information for a previous or following period (that is, hour, day, week, or month), click the **Older** button on the left or the **Newer** button on the right until you find the period for which you want to view information.
7. To see more information, point to a graph.

View the Status of Devices at a Location

You can view the status of devices (also referred to as the health status) at a location, broken out into the following components:

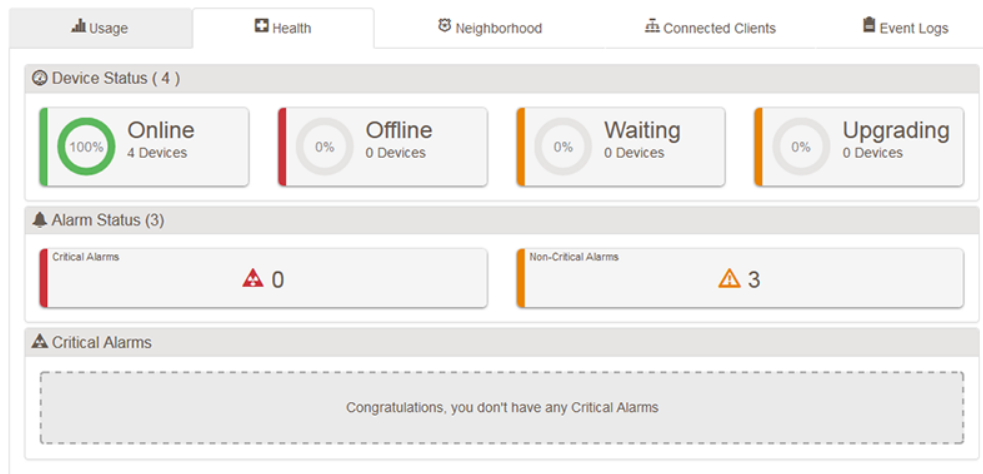
- Device status (Online, Offline, Waiting, and Upgrading)
- Alarm status (critical alarms and noncritical alarms)
- List of critical alarms

Claiming or resolving an alarm means the following:

- **Claim an alarm.** You take responsibility for the alarm and can add an optional note. Others can open the pop-up window for the alarm and view the note. The alarm remains in the alarms table and the Claimed by field in the table shows your email address.
- **Resolve an alarm.** You mark the alarm as resolved and can add an optional resolution note. (A future release will support historical alarm tables in which you can view the resolution notes.) The alarm is removed from the alarms table.

► To view the status of devices at a location, claim an alarm, or resolve an alarm:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
By default, the **Usage** tab is selected and WiFi usage information displays.
5. Click the **Health** tab.



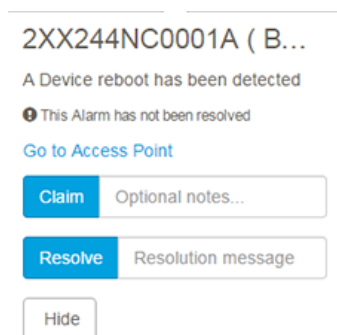
6. Drill down for more detailed information as explained in the following table.

Business Central Wireless Manager 2.1 Application

Component	Information
Device Status	The total number of devices that are managed at the location is stated. Click the Online, Offline, Waiting, or Upgrading tab to view a list of devices. Devices that are offline, waiting, or upgrading cannot broadcast WiFi networks. In the list of devices, click a device to view detailed information about the device. For more information, see Monitor a Single Device at a Location on page 128.
Alarm Status	The total number of alarms for devices at the location is stated. Click the Critical Alarms or Non-Critical Alarms tab to view a list of alarms. In the list of alarms, scroll down to view more alarms. Click an alarm to view more information about the alarm, claim the alarm (see Step 7), or resolve the alarm (see Step 8).
Critical Alarms	The total number of critical alarms for devices at the location is stated. View the same list of alarms and scroll down to view more alarms. Click an alarm to view more information about the alarm, claim the alarm (see Step 7), or resolve the alarm (see Step 8).

7. To claim an alarm, do the following:

- Select the check box for the alarm.
- Click the **Claim** button.



2XX244NC0001A (B...

A Device reboot has been detected

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Claim Optional notes...

Resolve Resolution message

Hide

- In the **Optional notes** field, enter a message for management purposes only.
- Click the **Claim** button in the pop-up window.
The pop-up window closes. The Claimed by field in the table shows your email address.

8. To resolve an alarm, do the following:

- a. Select the check box for the alarm.
- b. Click the **Resolve** button.

2XX244NC0001A (B...

A Device reboot has been detected

Claimed by okaywhatnowthen3@gmail.com on
02/11/2016 1:20:07 PM (a few seconds ago)

Roland

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Resolve Resolution message

Hide

- c. In the **Resolution message** field, enter a message for management purposes only.
- d. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarm is removed from the table.

View Neighbor and Rogue Access Points at a Location

You can view the details about neighbor and rogue access points at a location:

- **Neighbor access point.** An access point that is not cloud managed and that is a known or access point that is broadcasting a managed SSID or an unknown access point that is broadcasting an SSID.
- **Rogue access point.** An access point that is not cloud managed and that is broadcasting an SSID that is identical to the SSID of a cloud-managed access point. This type of rogue access point is also referred to as an evil twin.

You can mark an unknown neighbor access point or a rogue access point as a known access point.

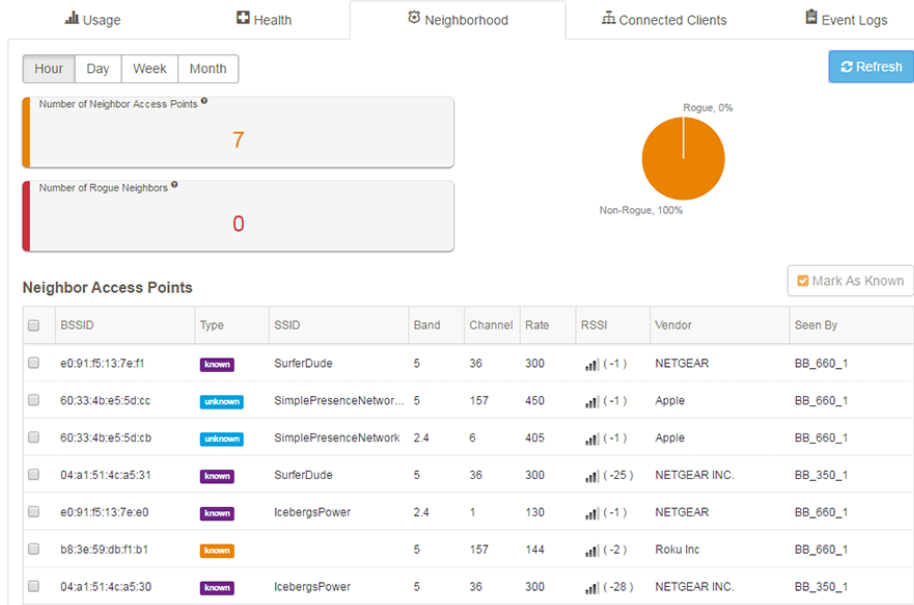
An access point that is cloud managed at the location is automatically marked as known.

► To view neighbor and rogue access points at a location and mark an unknown neighbor access point or a rogue access point as a known access point:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
By default, the **Usage** tab is selected and WiFi usage information displays.

Business Central Wireless Manager 2.1 Application

5. Click the **Neighborhood** tab.



By default, the **Hour** button is selected.

The number of neighbor access points and the number of rogue access points, if any, are stated.

The table is sorted by the time the access point was last detected. You can resort the table by clicking a column heading. The labels in the Type column mean the following:

- rogue** A rogue access point (none are shown in the previous figure).
- unknown** An unknown access point.
- known** A known access point that is cloud managed and that was automatically marked as known.
- known** A known access point that was manually marked as known.

- To view more table columns, point to the table and move the gray pop-up slider at the bottom of the table to the right.
- To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
- To view information for a different period, click the **Day**, **Week**, or **Month** button.
- To see more information, point to the graph.
- To mark one or more unknown or rogue access point as known access points, do the following:
 - Select the check boxes for the access points.
To select all unknown and rogue access points, select the check box in the table heading.
 - Click the **Mark as Known** button.
The label in the Type column changes from **unknown** or **rogue** to **known**.

View Clients Connected at a Location

You can view details about clients that are connected to the WiFi networks at a location. You can filter the information and search by client MAC address.

► To view details about clients that are connected to the WiFi networks at a location:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
By default, the **Usage** tab is selected and WiFi usage information displays.
5. Click the **Connected Clients** tab.

▼ Last Seen	MAC Address	Signal Strength	Usage (rx + tx)	Client IP Address	Access Point	Building
★ a minute ago	00:00:28:21:27:e8	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:f8	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:05	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:01	📶 (-48)	26 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:07	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:1a	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:0e	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:17	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:12	📶 (-48)	22 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ 2 minutes ago	00:00:02:d6:2c:90	📶 (-47)	25 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:02:d6:2c:84	📶 (-47)	30 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c4	📶 (-47)	211 KB	172.16.78.161	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:28:0f	📶 (-47)	26 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c7	📶 (-47)	197 KB	172.16.78.2	4DA156EM00011(AP11-8033ef)	

100 Connected Clients

By default, the **Hour** button is selected.

The table is sorted by the time the client was last detected. You can resort the table by clicking a column heading.

6. To view more table columns, point to the table and move the gray pop-up slider at the bottom of the table to the right.
7. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
8. To view information for a different period, click the **Day**, **Week**, or **Month** button.

9. To search and filter the table, take one of the following actions:
 - To search for a client by MAC address, do the following:
 - a. Click the drop-down button next to **All**.
A pop-up window opens.
 - b. In the **Search** field in the pop-up window, enter the MAC address or part of a MAC address of a client.
 - c. Select the check box next to the client MAC address.
The information in the table is limited to the selected client.
 - To filter the table and show a selected client only, select the check box next to the client MAC address.
You can repeat this action and add another selected client to the table.
10. For a large table, move through the table by clicking a page number button at the bottom right.

View the Event Logs for a Location

You can view the logs for events that occur on devices at a location. You can filter the information, search the events log, copy all or selected entries, and download the entire events log as a CSV file.

► To view the event logs for a location, copy entries, or download the entire events log:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
By default, the **Usage** tab is selected and WiFi usage information displays.

Business Central Wireless Manager 2.1 Application

5. Click the **Event Logs** tab.

Usage Health Neighborhood Connected Clients **Event Logs**

Hour Day Week Month

Client MAC Address Clear

Search Clear

Filter By Device: All

Access Point	Date	Message
4DA156EM0001...	02/08/2016 5:29:35 PM	hostapd[3069]: station: 00:00:02:d6:2c:92 deauthenticated
4DA156EM0001...	02/08/2016 5:29:35 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 deauthed from BSSID 50:6a:03:80:33:e1 reason 4: Disassociated due to inactivity
4DA156EM0001...	02/08/2016 5:27:00 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 associated with BSSID 50:6a:03:80:33:e1
4DA156EM0001...	02/08/2016 5:26:59 PM	hostapd[3069]: Assoc request from 00:00:02:d6:2c:92 BSSID 50:6a:03:80:33:e1 SSID loc0_net2_wpa2
4DA156EM0001...	02/08/2016 5:26:59 PM	hostapd[3069]: station: 00:00:02:d6:2c:92 deauthenticated
4DA156EM0001...	02/08/2016 5:26:59 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 deauthed from BSSID 50:6a:03:80:33:e1 reason 3: STA is leaving IBSS or ESS
4DA156EM0001...	02/08/2016 5:26:59 PM	hostapd[3069]: Assoc request from 00:00:02:d6:2c:92 BSSID 50:6a:03:80:33:e1 SSID loc0_net2_wpa2
4DA156EM0001...	02/08/2016 5:25:59 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 deauthenticated for reason 15: 4-way handshake timeout
4DA156EM0001...	02/08/2016 5:25:59 PM	hostapd[3069]: Station 00:00:02:d6:2c:92 had an authentication failure, reason 16
4DA156EM0001...	02/08/2016 5:25:55 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 associated with BSSID 50:6a:03:80:33:e1
4DA156EM0001...	02/08/2016 5:25:55 PM	hostapd[3069]: STA 00:00:02:d6:2c:92 associated with BSSID 50:6a:03:80:33:e1

500 Messages

1 2

By default, the **Hour** button is selected.

The table is sorted by the time the event occurred. You can resort the table by clicking a column heading.

6. To view more of the Message column, point to the table and move the gray pop-up slider at the bottom of the table to the right.
7. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
8. To view information for a different period, click the **Day**, **Week**, or **Month** button.
9. To search and filter the table, take one of the following actions:
 - To search by client MAC address, in the **Client MAC Address** field, enter the MAC address of the client.
The information in the table is limited to the selected client.
 - To search for a term in the message text, in the **Search** field, enter the term, IP address, or MAC address.
All occurrences of the term or address are highlighted in the table.
 - To search for an access point serial number, name, or part of a serial number or name, do the following:
 - a. Click the drop-down button next to **All**.
A pop-up window opens.
 - b. In the **Search** field in the pop-up window, enter the access point serial number, name, or part of the serial number or name.
 - c. Select the check box next to the access point serial number and name.

Business Central Wireless Manager 2.1 Application

The information in the table is limited to the selected access point.

- To filter the table and show a selected access point only, select the check box next to the access point serial number and name.
You can repeat this action and add another selected access point to the table.

10. To copy some or all of the table entries, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select multiple entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the copy icon (, the leftmost icon).
The selected entries are placed on the Clipboard.

11. To download the entire table as a CSV file, do the following:

- a. Click the download icon (, the rightmost icon).
A pop-up window opens.
- b. Navigate to a location and save the file.

12. For a large table, move through the table by clicking a page number button at the bottom right.

Monitor a Single WiFi Network at a Location

You can monitor the following components for a single WiFi network at a location:

- **Usage.** Number of connected clients and WiFi network usage.
For more information, see [View Usage of a WiFi Network](#) on page 122.
- **Connected clients.** Details about connected clients.
For more information, see [View Clients Connected to a WiFi Network](#) on page 124.
- **Event logs.** Details about events that occurred.
For more information, see [View the Event Logs for a WiFi Network](#) on page 125.
- **Captive portal (CP) sessions.** Details about clients that are connected to a captive portal.
For more information, see [View Captive Portal Sessions](#) on page 127.

View Usage of a WiFi Network

You can view the usage of a WiFi network at a location, broken out into the following components:

- Number of connected clients
- WiFi network usage

► To view usage of a WiFi network:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.

Business Central Wireless Manager 2.1 Application

The application login page displays.

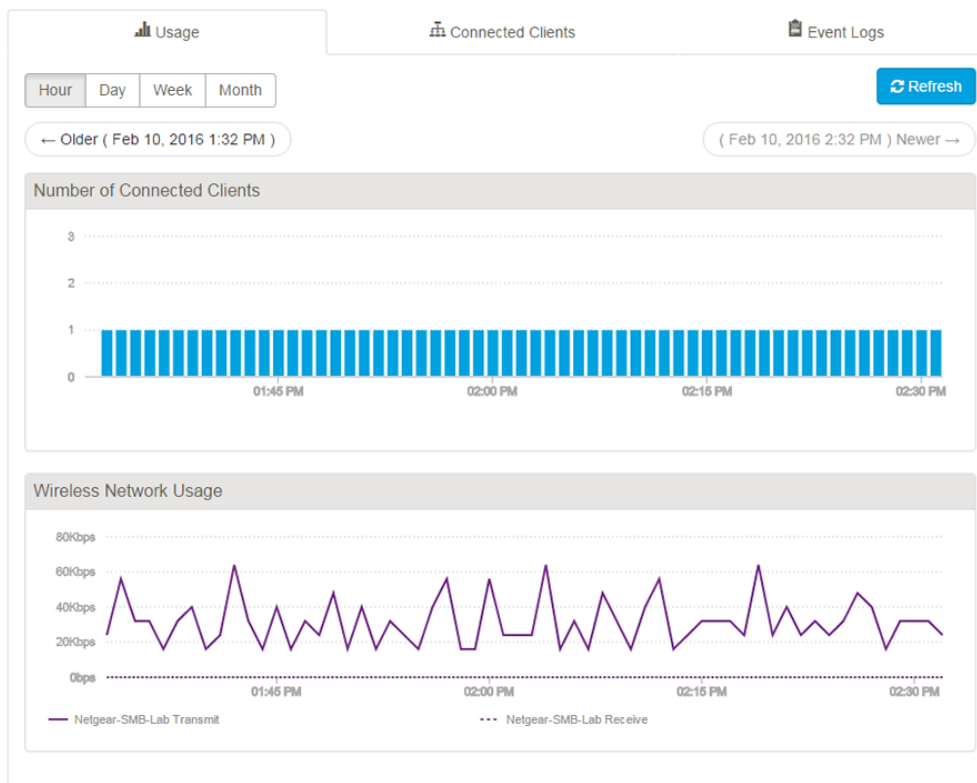
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

4. In the Locations tree on the left, click the location.

5. In the Locations tree, click **Wireless Networks**.
The Monitoring page displays any existing WiFi networks.

6. Select the WiFi network.

By default, the **Usage** tab is selected and WiFi usage information displays. If you configured a captive portal on the WiFi network, the page also displays the **CP Sessions** tab (not shown in the following figure), which lets you monitor active captive portal sessions.



By default, the **Hour** button is selected.

7. To view information for a different period, click the **Day**, **Week**, or **Month** button.
8. To view information for a previous or following period (that is, hour, day, week, or month), click the **Older** button on the left or the **Newer** button on the right until you find the period for which you want to view information.
9. To see more information, point to a graph.

View Clients Connected to a WiFi Network

You can view details about clients that are connected to a WiFi network at a location. You can filter the information and search by client MAC address.

► To view details about clients that are connected to a WiFi network:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Wireless Networks**.
The Monitoring page displays any existing WiFi networks.
6. Select the WiFi network.
By default, the **Usage** tab is selected and WiFi usage information displays. If you configured a captive portal on the WiFi network, the page also displays the **CP Sessions** tab (not shown in the following figure), which lets you monitor active captive portal sessions.
7. Click the **Connected Clients** tab.

▼ Last Seen	MAC Address	Signal Strength	Usage (rx + tx)	Client IP Address	Access Point	Building
★ a minute ago	00:00:28:21:27:e8	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:f8	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:d5	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:01	📶 (-48)	26 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:07	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:1a	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:0e	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:17	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:12	📶 (-48)	22 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ 2 minutes ago	00:00:02:d6:2c:90	📶 (-47)	25 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:02:d6:2c:84	📶 (-47)	30 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c4	📶 (-47)	211 KB	172.16.78.161	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:28:0f	📶 (-47)	26 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c7	📶 (-47)	197 KB	172.16.78.2	4DA156EM00011(AP11-8033ef)	

100 Connected Clients

By default, the **Hour** button is selected. The table is sorted by the time the client was last detected. You can resort the table by clicking a column heading.

8. To view more table columns, point to the table and move the gray pop-up slider at the bottom of the table to the right.
9. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
10. To view information for a different period, click the **Day**, **Week**, or **Month** button.
11. To search and filter the table, take one of the following actions:
 - To search for a client by MAC address, do the following:
 - a. Click the drop-down button next to **All**.
A pop-up window opens.
 - b. In the **Search** field in the pop-up window, enter the MAC address or part of the MAC address of the client.
 - c. Select the check box next to the client MAC address.
The information in the table is limited to the selected client.
 - To filter the table and show a selected client only, select the check box next to the client MAC address.
You can repeat this action and add another selected client to the table.
12. For a large table, move through the table by clicking a page number button at the bottom right.

View the Event Logs for a WiFi Network

You can view the logs for events that occur on a WiFi network at a location. You can filter the information, search the events log, copy all or selected entries, and download the entire events log as a CSV file.

► To view the event logs for a WiFi network, copy entries, or download the entire events log:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Wireless Networks**.
The Monitoring page displays any existing WiFi networks.
6. Select the WiFi network.
By default, the **Usage** tab is selected and WiFi usage information displays. If you configured a captive portal on the WiFi network, the page also displays the **CP Sessions** tab (not shown in the following figure), which lets you monitor active captive portal sessions.

7. Click the **Event Logs** tab.

Usage Connected Clients Event Logs

Hour Day Week Month

Client MAC Address Clear

Search Clear

Filter By Device: All

Access Point	Date	Message
2XX244NC0001...	02/10/2016 11:12:00 PM	udhcp[26385]: Lease of 192.168.100.115 obtained, lease time 600
2XX244NC0001...	02/10/2016 11:12:00 PM	udhcp[26385]: Sending renew...
29210A5W003C...	02/10/2016 11:11:17 PM	udhcp[3524]: Lease of 192.168.100.110 obtained, lease time 600
29210A5W003C...	02/10/2016 11:11:17 PM	udhcp[3524]: Sending renew...
2XX244NC0001...	02/10/2016 11:11:10 PM	kernel: ath_bstuck_tasklet-wifi1-(135209829): stuck beacon; resetting (bmiss count 18)
2XX244NC0001...	02/10/2016 11:07:00 PM	udhcp[26385]: Lease of 192.168.100.115 obtained, lease time 600
2XX244NC0001...	02/10/2016 11:07:00 PM	udhcp[26385]: Sending renew...
29210A5W003C...	02/10/2016 11:06:17 PM	udhcp[3524]: Lease of 192.168.100.110 obtained, lease time 600
29210A5W003C...	02/10/2016 11:06:17 PM	udhcp[3524]: Sending renew...
2XX244NC0001...	02/10/2016 11:02:06 PM	hostapd: wifi0vap1: STA c0:bd:d1:b0:f0:f1 WPA: group key handshake completed (RSN)
2XX244NC0001...	02/10/2016 11:01:59 PM	udhcp[26385]: Lease of 192.168.100.115 obtained, lease time 600
2XX244NC0001...	02/10/2016 11:01:59 PM	udhcp[26385]: Sending renew...

56 Messages

By default, the **Hour** button is selected.

The table is sorted by the time the event occurred. You can resort the table by clicking a column heading.

8. To view more of the Message column, point to the table and move the gray pop-up slider at the bottom of the table to the right.
9. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
10. To view information for a different period, click the **Day**, **Week**, or **Month** button.
11. To search and filter the table, take one of the following actions:
 - To search by client MAC address, in the **Client MAC Address** field, enter the MAC address of the client.
The information in the table is limited to the selected client.
 - To search for a term in the message text, in the **Search** field, enter the term, IP address, or MAC address.
All occurrences of the term or address are highlighted in the table.
 - To search for an access point serial number, name, or part of a serial number or name, do the following:

Business Central Wireless Manager 2.1 Application

- a. Click the drop-down button next to **All**.
A pop-up window opens.
 - b. In the **Search** field in the pop-up window, enter the access point serial number, name, or part of the serial number or name.
 - c. Select the check box next to the access point serial number and name.
The information in the table is limited to the selected access point.
- To filter the table and show a selected access point only, select the check box next to the access point serial number and name.
You can repeat this action and add another selected access point to the table.
12. To copy some or all of the table entries, do the following:
 - a. Select one table entry, use the **Shift** and **Ctrl** keyboard keys to select multiple entries, or click the toggle icon (, the middle icon) to select all entries.
 - b. Click the copy icon (, the leftmost icon).
The selected entries are placed on the Clipboard.
13. To download the entire table as a CSV file, do the following:
 - a. Click the download icon (, the rightmost icon).
A pop-up window opens.
 - b. Navigate to a location and save the file.
14. For a large table, move through the table by clicking a page number button at the bottom right.

View Captive Portal Sessions

If you configured a captive portal on a WiFi network, you can view information about active client sessions, if any exist. You can download the client session table as a CSV file.

► To view information about active client sessions or the client session table for a captive portal on a WiFi network:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Wireless Networks**.
The Monitoring page displays any existing WiFi networks.
6. Select the WiFi network.

Business Central Wireless Manager 2.1 Application

By default, the **Usage** tab is selected and WiFi usage information displays.

7. Click the **CP Sessions** tab.

Hour	Day	Week	Month								Refresh
Station Mac Address	Status	Start Time	Device Serial	Total Tx	Total Rx	Customer Name	Customer Email	Voucher Code			
C08D.D180.F0F1	authorized	Thu Jun 09 2016 16:40:18 GMT-0700 (Pa...	29211A5W113C0	2.05 MB	180 KB	JohnnyBillyworth	jbillyworth@aussie.com	3JA9FTPX			

By default, the **Day** button is selected. (The previous figure shows the **Month** button selected.) The table is sorted by the start time of the captive portal sessions. You can resort the table by clicking a column heading. The information that is displayed in the table depends on the nature of the captive portal (offering free access or paid-for access with a voucher).

8. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
9. To view information for a different period, click the **Hour**, **Week**, or **Month** button.
10. To download the client session table as a CSV file, do the following:
 - a. Click the download icon to the left of the **Refresh** button.
A pop-up window opens.
 - b. Navigate to a location and save the file.
11. For a large table, move through the table by clicking a page number button at the bottom right.

Monitor a Single Device at a Location

You can the monitor the following components for a single device at a location:

- **Usage.** Number of connected clients, average WiFi usage per WiFi network, and average WiFi usage per radio.
For more information, see [View WiFi Usage on a Device](#) on page 129.
- **Connected clients.** Details about connected clients.
For more information, see [View Clients Connected to a Device](#) on page 130.
- **Alarms.** Details about alarms that occurred.
For more information, see [View Alarms for a Device, Claim Alarms, and Resolve Alarms](#) on page 131.
- **Event logs.** Details about events that occurred.
For more information, see [View the Event Logs for a Device](#) on page 134.

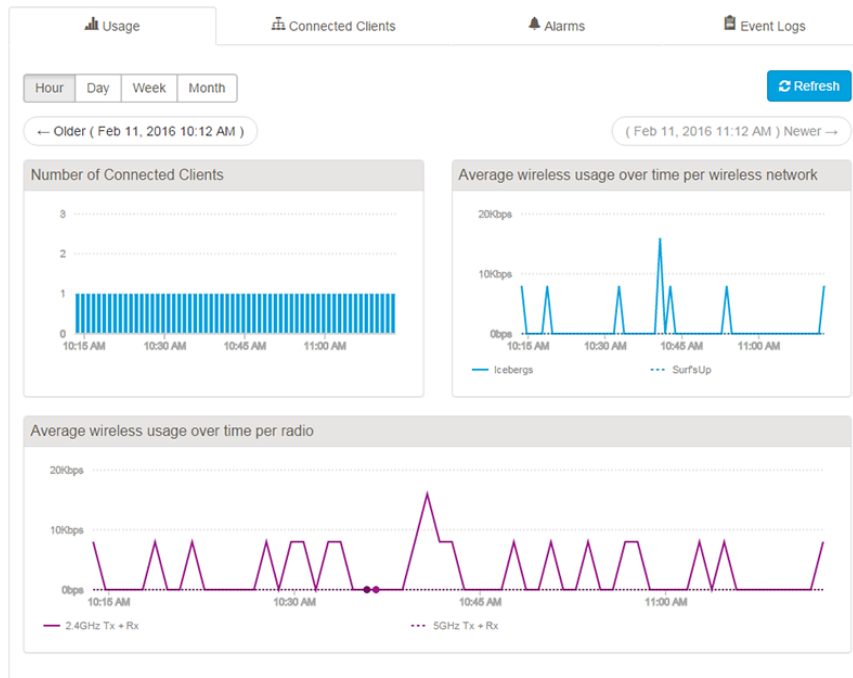
View WiFi Usage on a Device

You can view the WiFi usage on a device, broken out into the following components:

- Number of connected clients
- Average WiFi usage over time per WiFi network
- Average WiFi usage over time per radio

► To view usage of a WiFi network:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Devices**.
The Monitoring page displays any existing devices.
6. Select the device.
By default, the **Usage** tab is selected and WiFi usage information displays.



By default, the **Hour** button is selected.

7. To view information for a different period, click the **Day**, **Week**, or **Month** button.

Business Central Wireless Manager 2.1 Application

- To view information for a previous or following period (that is, hour, day, week, or month), click the **Older** button on the left or the **Newer** button on the right until you find the period for which you want to view information.
- To see more information, point to a graph.

View Clients Connected to a Device

You can view details about clients that are connected to a device at a location. You can filter the information and search by client MAC address.

► To view details about clients that are connected to a device:

- Open a browser on your computer.
- In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
- Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
- In the Locations tree on the left, click the location.
- In the Locations tree, click **Devices**.
The Monitoring page displays any existing devices.
- Select the device.
By default, the **Usage** tab is selected and WiFi usage information displays.
- Click the **Connected Clients** tab.

▼ Last Seen	MAC Address	Signal Strength	Usage (rx + tx)	Client IP Address	Access Point	Building
★ a minute ago	00:00:28:21:27:e8	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:f8	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:27:d5	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:01	📶 (-48)	26 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:07	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:1a	📶 (-48)	24 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:0e	📶 (-48)	25 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:17	📶 (-48)	23 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ a minute ago	00:00:28:21:28:12	📶 (-48)	22 KB	0.0.0.0	4DA156EW00019(AP14-8034ef)	
★ 2 minutes ago	00:00:02:d6:2c:90	📶 (-47)	25 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:02:d6:2c:84	📶 (-47)	30 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c4	📶 (-47)	211 KB	172.16.78.161	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:28:0f	📶 (-47)	26 KB	0.0.0.0	4DA156EM00011(AP11-8033ef)	
★ 2 minutes ago	00:00:28:21:27:c7	📶 (-47)	197 KB	172.16.78.2	4DA156EM00011(AP11-8033ef)	

100 Connected Clients

Business Central Wireless Manager 2.1 Application

By default, the **Hour** button is selected. The table is sorted by the time the client was last detected. You can resort the table by clicking a column heading.

8. To view more table columns, point to the table and move the gray pop-up slider at the bottom of the table to the right.
9. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
10. To view information for a different period, click the **Day**, **Week**, or **Month** button.
11. To search and filter the table, take one of the following actions:
 - To search for a client by MAC address, do the following:
 - a. Click the drop-down button next to **All**.
A pop-up window opens.
 - b. In the **Search** field in the pop-up window, enter the MAC address or part of the MAC address of the client.
 - c. Select the check box next to the client MAC address.
The information in the table is limited to the selected client.
 - To filter the table and show a selected client only, select the check box next to the client MAC address.
You can repeat this action and add another selected client to the table.
12. For a large table, move through the table by clicking a page number button at the bottom right.

View Alarms for a Device, Claim Alarms, and Resolve Alarms

You can view the alarms that occur on a device at a location. You can claim an alarm, mark an alarm as resolved, copy all or selected alarms, and download the entire alarm list as a CSV file.

Claiming or resolving an alarm means the following:

- **Claim an alarm.** You take responsibility for the alarm and can add an optional note. Others can open the pop-up window for the alarm and view the note. The alarm remains in the alarms table and the Claimed by field in the table shows your email address.
- **Resolve an alarm.** You mark the alarm as resolved and can add an optional resolution note. (A future release will support historical alarm tables in which you can view the resolution notes.) The alarm is removed from the alarms table.

Alarms are classified in four categories or severity levels: Critical (for example, a device disconnected), Major (for example, a device command failure occurred), Minor (for example, a device rebooted), and Info (for example, a device reconnected).

► To view the alarms for a device, claim or resolve alarms, copy alarm table entries, or download the entire alarm table:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.

Business Central Wireless Manager 2.1 Application

3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Devices**.
The Monitoring page displays any existing devices.
6. Select the device.
By default, the **Usage** tab is selected and WiFi usage information displays.
7. Click the **Alarms** tab.

☐	▼ Date	Location	Device	Level	Type	Claimed By
☐	05/16/2016 3:37:18 PM	Netgear Corporate Office	4D925BE800351 (WA...	Minor	Device Rebooted	
☐	05/16/2016 3:26:24 PM	Netgear Corporate Office	4D925BE800351 (WA...	Minor	Device Rebooted	

The table is sorted by the time the alarm occurred. You can resort the table by clicking a column heading.

8. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
9. To claims alarms, do the following:

To claim a single alarm, do the following:

- a. Click the alarm row in the table.

2XX244NC0001A (B...

A Device reboot has been detected

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Claim

Optional notes...

Resolve

Resolution message

Hide

- b. In the **Optional notes** field, enter a message for management purposes only.
- c. Click the **Claim** button in the pop-up window.

Business Central Wireless Manager 2.1 Application

The pop-up window closes. The Claimed by field in the table shows your email address.

To claim several or all alarms simultaneously, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select groups of entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the **Claim** button above the table.
A pop-up window opens.
- c. Enter an optional message for management purposes only.
- d. Click the **Claim** button in the pop-up window.
The pop-up window closes. The Claimed by fields in the table shows your email address.

10. To resolve alarms, do the following:

To resolve a single alarm, do the following:

- a. Click the alarm row in the table.

2XX244NC0001A (B...

A Device reboot has been detected

Claimed by okaywhatnowthen3@gmail.com on
02/11/2016 1:20:07 PM (a few seconds ago)

Roland

ⓘ This Alarm has not been resolved

[Go to Access Point](#)

Resolve

Resolution message

Hide

The previous figure shows a claimed alarm. If the alarm was not claimed, the pop-up window would show both the **Claim** and **Resolve** buttons.

- b. In the **Resolution message** field, enter a message for management purposes only.
- c. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarm is removed from the table.

To resolve several or all alarms simultaneously, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select groups of entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the **Resolve** button above the table.
A pop-up window opens.
- c. Enter an optional message for management purposes only.
- d. Click the **Resolve** button in the pop-up window.
The pop-up window closes. The alarms are removed from the table.

11. To copy some or all of the table entries, do the following:
 - a. Select one table entry, use the Shift and Ctrl keyboard keys to select multiple entries, or click the toggle icon (, the middle icon) to select all entries.
 - b. Click the copy icon (, the leftmost icon).
The selected entries are placed on the Clipboard.
12. To download the entire table as a CSV file, do the following:
 - a. Click the download icon (, the rightmost icon).
A pop-up window opens.
 - b. Navigate to a location and save the file.

View the Event Logs for a Device

You can view the logs for events that occur on a device at a location. You can search the events log, copy all or selected entries, and download the entire events log as a CSV file.

► To view the event logs for a device, copy entries, or download the entire events log:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. In the Locations tree on the left, click the location.
5. In the Locations tree, click **Devices**.
The Monitoring page displays any existing devices.
6. Select the device.
By default, the **Usage** tab is selected and WiFi usage information displays.

Business Central Wireless Manager 2.1 Application

7. Click the **Event Logs** tab.

The screenshot shows the 'Event Logs' tab in the Business Central Wireless Manager 2.1 application. At the top, there are four tabs: 'Usage', 'Connected Clients', 'Alarms', and 'Event Logs'. Below the tabs, there are filters for 'Hour', 'Day', 'Week', and 'Month'. There is also a 'Client MAC Address' field with a 'Clear' button and a 'Search' field with a 'Clear' button. To the right of the filters are three icons (a selection icon, a copy icon, and a refresh icon) and a 'Refresh' button. Below the filters is a table with two columns: 'Date' and 'Message'. The table contains several log entries, including lease timeouts and WPA group key handshakes. At the bottom of the table, there is a '28 Messages' indicator.

Date	Message
02/11/2016 12:36:26 PM	udhccp[3524]: Lease of 192.168.100.110 obtained, lease time 600
02/11/2016 12:36:26 PM	udhccp[3524]: Sending renew...
02/11/2016 12:31:26 PM	udhccp[3524]: Lease of 192.168.100.110 obtained, lease time 600
02/11/2016 12:31:26 PM	udhccp[3524]: Sending renew...
02/11/2016 12:26:26 PM	udhccp[3524]: Lease of 192.168.100.110 obtained, lease time 600
02/11/2016 12:26:26 PM	udhccp[3524]: Sending renew...
02/11/2016 12:21:26 PM	udhccp[3524]: Lease of 192.168.100.110 obtained, lease time 600
02/11/2016 12:21:26 PM	udhccp[3524]: Sending renew...
02/11/2016 12:20:13 PM	hostapd: wif0vap0: STA c0:bd:d1:b0:f0:f1 WPA: group key handshake completed (RSN)
02/11/2016 12:20:13 PM	hostapd: wif0vap0: STA c0:bd:d1:b0:f0:f1 WPA: received EAPOL-Key 2/2 Group with unexpected replay counter
02/11/2016 12:20:13 PM	hostapd: wif0vap0: STA c0:bd:d1:b0:f0:f1 WPA: EAPOL-Key timeout

By default, the **Hour** button is selected.

The table is sorted by the time the event occurred. You can resort the table by clicking a column heading.

8. To view more of the Message column, point to the table and move the gray pop-up slider at the bottom of the table to the right.
9. To view more table rows, point to the table and move the gray pop-up slider at the right of the table to the bottom.
10. To view information for a different period, click the **Day**, **Week**, or **Month** button.
11. To search the table, take one of the following actions:
 - To search by client MAC address, in the **Client MAC Address** field, enter the MAC address of the client.
The information in the table is limited to the selected client.
 - To search for a term in the message text, in the **Search** field, enter the term, IP address, or MAC address.
All occurrences of the term or address are highlighted in the table.

12. To copy some or all of the table entries, do the following:

- a. Select one table entry, use the Shift and Ctrl keyboard keys to select multiple entries, or click the toggle icon (, the middle icon) to select all entries.
- b. Click the copy icon (, the leftmost icon).
The selected entries are placed on the Clipboard.

13. To download the entire table as a CSV file, do the following:

Business Central Wireless Manager 2.1 Application

- a. Click the download icon (, the rightmost icon).
A pop-up window opens.
 - b. Navigate to a location and save the file.
14. For a large table, move through the table by clicking a page number button at the bottom right.

This chapter provides diagnostics and troubleshooting information.

The chapter includes the following sections:

- *Download the Diagnostics File for an Access Point* on page 138
- *Troubleshooting a WiFi Network* on page 139

Download the Diagnostics File for an Access Point

You can download the diagnostics file for an access point. If connectivity issues occur with the access point, analyzing the file might help you or NETGEAR support to find a solution.

► **To add or change building and floor labels for an access point at a location:**

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. For the device for which you want to download the diagnostics file, click the gear icon, and select **Download Diagnostics**.
The application retrieves the diagnostics file of the access point.
Depending on your browser settings a window might open or another action might occur.
8. Save the diagnostics file to your computer.
The name of the file includes the serial number of the access point and the date. The file extension is `.tar.gz`. An example is `244244N44001A_2016-02-15T23-44-18-4.tar.gz`.

Troubleshooting a WiFi Network

If a WiFi network does not broadcast at a location, check the following:

1. Did you add the location to which you added the WiFi network (and one or more access points) to a license account with an active license? If the account is unlicensed, the access points remain in the unlicensed state, preventing the WiFi network from coming up.
For more information, see the following sections:
 - [View the Access Point Inventory and Connection Status in the Application](#) on page 148
 - [Add a License to an Account](#) on page 90
2. Is any access point connected and active at the location?
For more information, see the following sections:
 - [View the Access Point Inventory and Connection Status in the Application](#) on page 148
 - [View the Cloud Connection and Activity Status on a Cloud-Enabled Access Point](#) on page 149
3. Is broadcast of the WiFi network disabled because a radio on/off broadcast schedule turned off the broadcast?
For more information, see [Set Up or Change a Radio On/Off Broadcast Schedule for a WiFi Network](#) on page 65.
4. Is the SSID of the WiFi network being broadcast or is it hidden?
For more information, see [Change the Broadcast, Advertisement, and VLAN Settings for a WiFi Network](#) on page 48.
5. Does the event log for the WiFi network indicate a specific reason why the WiFi network does not broadcast?
For more information, see [View the Event Logs for a WiFi Network](#) on page 125.

Manage Vouchers With a Clerk User Account

A

If you are assigned a clerk user account, you can sell, generate, and view the status of vouchers for a paid-for captive portal.

For information about signing up for a clerk account after you received an invitation email, see [Accept an Invitation and Sign Up for and Activate a Manager, Customer, or Clerk Account](#) on page 96.

This appendix includes the following sections:

- [Sell, Generate, and Print a Voucher](#) on page 141
- [View the Status of Vouchers and Download All Vouchers](#) on page 144

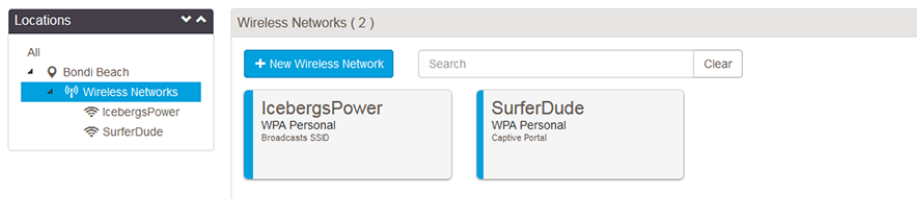
Sell, Generate, and Print a Voucher

As a clerk, you can sell a voucher, email it to the customer, and print it. You can also set the duration of the voucher and specify whether the expiration time of the voucher must be enforced.

As a clerk, you cannot change the price of a time unit (minute, hour, day, or week) for a voucher, nor can you specify whether usage time is being deducted only while the customer is connected to the WiFi network or regardless of the connection status. These settings are defined by the owner, manager, or customer of the location where the WiFi network with its captive portal is set up.

► To sell, generate, and print a voucher:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Wireless Networks**.



7. In the Locations tree, click the WiFi network.
You can also click the tab for the WiFi network. If a WiFi network is a captive portal, the tab states Captive Portal under the network name.

The settings page for the WiFi network displays. With a clerk user account, you can only view these settings, not modify them.

Business Central Wireless Manager 2.1 Application

8. Click the **Vouchers** tab.

Created	Customer Name	Customer Email	Code	Status	Start Time	Expire Time	Duration	Remaining	Cost
a few seconds ago	Tim Zonin	tzonin@greataccess.au	O90FLN58	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
a few seconds ago	Tim Zonin	tzonin@greataccess.au	EW2UYLCO	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
a few seconds ago	Tim Zonin	tzonin@greataccess.au	S30WNRJV	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
22 minutes ago	Ron Klaiker	rtklaiker@greataccess.au	IGHLOPVF	Created		Sat Jun 18 9:46 PM	1 day	24 hours	\$60.00
39 minutes ago	Marsha Marron	mmarron@xssydney.au	TV501W6L	Expired		Sat Jun 18 9:46 AM	1 day	0 minutes	\$60.00
41 minutes ago	Billy Boardman	bboardman@aussieco...	QVCE20LS	Created			2 hours	2 hours	\$5.00
41 minutes ago	Billy Boardman	bboardman@aussieco...	CVXLUNE5	Created			2 hours	2 hours	\$5.00

By default, the page shows the voucher table with vouchers that were sold during the past hour. You can click the **Day**, **Week**, or **Month** button to display vouchers that were sold during that period. If no vouchers were sold, the page does not show any.

9. Click the **Sell Vouchers** button.

Sell Vouchers

Customer Name:

Customer Email:

☐ Send Vouchers to Customer Email

Time Unit: Cost per hour: \$2.50

Duration:

Voucher time will be deducted only while connected

Number of Vouchers:

☐ Force Expiration

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

Setting	Description
Customer Name	Enter the name of the customer.
Customer Email	Enter the email address of the customer.
Send Vouchers to Customer Email	To send the voucher to the customer email address, select the Send Vouchers to Customer Email check box. When you click the Save button, the email is sent.
Time Unit	From the menu, select the time unit (minute , hour , day , or week). The voucher cost is nonconfigurable on this page and is automatically adjusted, depending on the time unit selected.

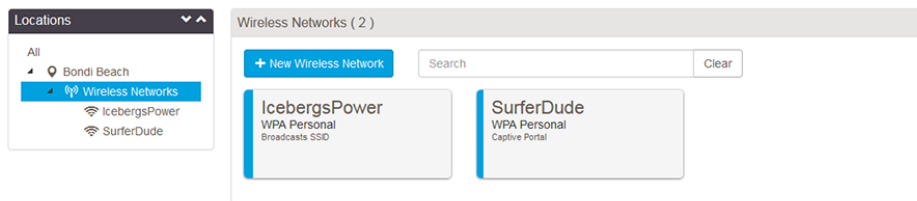
Manage Vouchers With a Clerk User Account

(Continued)

Setting	Description
Duration	Enter or specify the period that is associated with the unit of time.
Number of Vouchers	Enter the number of vouchers that you are selling to the customer.

11. If the voucher must expire on a particular day and time (which does not need to coincide with the duration of the voucher), do the following:
 - a. Select the **Force Expiration** check box.
The **Voucher Expires At** field becomes available.
 - b. Click the **Voucher Expires At** field.
A pop-up window displays a monthly calendar.
 - c. Select the month and day on which the voucher must expire.
 - d. Click the clock icon at the bottom of the pop-up window.
The pop-up window changes and displays options to specify a time.
 - e. Specify the time at which the voucher must expire.
 - f. To close the pop-up window, click the **x** icon in the pop-up window.
You can also return to the calendar by clicking the calendar icon at the top of the pop-up window.
12. Click the **Save** button.
Your settings are saved. The voucher is added to the voucher table and, if you specified so, sent to the email address of the customer.
13. To print one or more vouchers, do the following:

Business Central Wireless Manager 2.1 Application



7. In the Locations tree, click the WiFi network.

You can also click the tab for the WiFi network. If a WiFi network is a captive portal, the tab states Captive Portal under the network name.

The settings page for the WiFi network displays. With a clerk user account, you can only view these settings, not modify them.

8. Click the **Vouchers** tab.

Settings

Vouchers

Hour

Day

Week

Month

Sell Vouchers

▼ Created	Customer Name	Customer Email	Code	Status	Start Time	Expire Time	Duration	Remaining	Cost
a few seconds ago	Tim Zonin	tzonin@greataccess.au	O90FLN58	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
a few seconds ago	Tim Zonin	tzonin@greataccess.au	EW2UYLCO	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
a few seconds ago	Tim Zonin	tzonin@greataccess.au	S30WNRV	Created		Sun Jun 19 8:00 AM	1 day	24 hours	\$60.00
22 minutes ago	Ron Klaiker	rtaiker@greataccess.au	IGHLOPVF	Created		Sat Jun 18 9:46 PM	1 day	24 hours	\$60.00
39 minutes ago	Marsha Marron	mmarron@xssydney.au	TV501W6L	Expired		Sat Jun 18 9:46 AM	1 day	0 minutes	\$60.00
41 minutes ago	Billy Boardman	bboardman@aussieco...	QVCE20LS	Created			2 hours	2 hours	\$5.00
41 minutes ago	Billy Boardman	bboardman@aussieco...	CVXLUNE5	Created			2 hours	2 hours	\$5.00

By default, the page shows the voucher table with vouchers that were sold during the past hour. You can click the **Day**, **Week**, or **Month** button to display vouchers that were sold during that period. If no vouchers were sold, the page does not show any.

The following table describes the nonconfigurable information in the voucher table.

Setting	Description
Created	The time at which the voucher was created (sold).
Customer Name	The name of the customer.
Customer Email	The email address of the customer.
Code	The voucher code with which the customer can gain access to to the WiFi network.
Status	The status of the voucher (Created, Activated, or Expired).
Start Time	The time at which the voucher was activated by the customer.
Expiry Time	The time at which the voucher expires or expired.
Duration	The period that is associated with the unit of time for the voucher.

(Continued)

Setting	Description
Remaining	The remaining time balance on the voucher.
Cost	The total cost of the voucher.

9. To download all vouchers as a CSV file, do the following:
 - a. Click the download icon to the left of the **Sell Voucher** button.
 - b. Follow the directions of your browser to download and save the CSV file.

Cloud-Managed Access Points

B

This appendix includes the following sections:

- *View the Access Point Inventory and Connection Status in the Application* on page 148
- *View the Cloud Connection and Activity Status on a Cloud-Enabled Access Point* on page 149
- *How the Configuration of a Cloud-Managed Access Point Can Be Changed* on page 151
- *Convert an Access Point From Cloud-Managed to Standalone* on page 151

Note For information about preparing your NETGEAR WiFi access points for cloud management, see the *NETGEAR Business Central Wireless Manager How to Start Guide*, which you can download from downloadcenter.netgear.com.

The following sections also provide information about access points:

- *Compatible NETGEAR WiFi Access Points* on page 16
- *Definitions of Access Point Terms* on page 17

View the Access Point Inventory and Connection Status in the Application

The access point status is the cloud-management state of the access point in the application. The status is made up of two components:

- **Inventory status.** The inventory status can be one of the following:
 - **Active.** The access point is connected to the application and is added to a location, and the location is assigned to a license account with an active license.
 - **Provisioning.** The access point is either cloud managed or in the process of becoming cloud managed while the application is pushing a configuration.
 - **Upgrading.** The access point is either cloud managed or in the process of becoming cloud managed while the application is pushing a firmware upgrade.
 - **Rebooting.** The access point is either cloud managed or in the process of becoming cloud managed and is rebooting after the application pushed a configuration or a firmware upgrade to the access point.
 - **Unlicensed.** Even though the access point is connected to the application, the access point is added to a location that is assigned to an unlicensed account. The access point does not become active until you add an active license to the account.
 - **Decommissioning.** The application is in the process of decommissioning the access point from a location.
 - **Decommissioned.** Even though the access point is connected to the application, the access point is not added to a location and is not active.
- **Connection status.** The connection status can be one of the following:
 - **Connected.** The access point is connected to the application. However, this does not mean that the access point is active.
 - **Disconnected.** The access point was connected to the application but is now disconnected.
 - **Waiting.** The access point is added to a location and is waiting for a connection to the application.
 - **Phoned home** (and time indication). The access point is connected to the application but decommissioned (or undeployed).

► To view the access point inventory and connection status in the application:

1. Open a browser on your computer.
2. In the address bar, enter **<https://bc.netgear.com>**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.

Business Central Wireless Manager 2.1 Application

4. Select **Inventory**.

Role: owner	Status: All	Decommission	Delete	Deploy	New Device		
	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tallac_staging_1511.16.1936.112
	2925345800365 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
	2XX244NN0012F (AP660-Peets-Riv...	Active	Connected	Peet's - Rivermark Plaza			continuous_15.11.16.1923.62
	2925345600355 (AP350-Peets-Airpo...	Active	Connected	Peet's - San Jose Intl Ai...			continuous_15.11.10.2054.54
	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peet's - San Jose Intl Ai...			tallac_staging_1601.05.2320.216
	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tallac_staging_1511.16.1936.112
	2XX244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The Inventory Status and Connection Status fields display the cloud-management states of the access points.

View the Cloud Connection and Activity Status on a Cloud-Enabled Access Point

When an access point is cloud enabled, its web management interface is a restricted cloud management interface that shows the cloud connection status and cloud activity status.

► To view the cloud connection and activity status on a cloud-enabled access point:

1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Configuration**.
The Configuration page displays any existing locations.
5. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
6. In the Locations tree, under the location, click **Devices**.
The Configuration page displays any existing access points.
7. Select the access point.

Business Central Wireless Manager 2.1 Application

The Configuration page displays the access point details.

8. Next to LAN IP Address, click the IP address, which is a hyperlink.

If your computer is on the same network as the access point, the login window for the access point opens. If it does not, try changing your browser settings.

If your computer is *not* on the same network as the access point, do the following:

- a. Access the network that the access point is part of.
- b. Open a browser on your computer.
- c. In the address bar, enter the IP address of the access point.

9. Enter the user name and password.

Depending on your browser settings, the user name and password might be automatically entered. If they are not, the user name is **admin** and the password is specific to the location to which the access point is assigned.

If you do not know this password, do the following:

- a. In the Locations tree, click the location.
The Configuration page displays the settings for the selected location.
- b. Click the **Device Credentials** tab.
The Location-wide device credentials page displays.
- c. Click the show/hide password icon next to the password.
The password displays.

10. Click the **LOGIN** button.

The General page displays. The web management interface is the restricted cloud management interface.

When the access point is cloud enabled, the web management interface can indicate the cloud activation status and cloud connectivity status for the access point as described in the following table.

Setting		Description
Cloud Activation Status	Pending	The access point is not yet registered with the application and not yet cloud managed but is either waiting to be connected or in the process of being connected to the application. If you reset an access point to the factory default state, the access point restarts in the Pending state.
	Activated	The access point is registered with the application and is cloud managed.

(Continued)

Setting		Description
Cloud Connectivity Status	Connected	The access point is registered with the application, cloud managed, connected to the Internet, and connected to the application.
	Disconnected	Although the access point is registered with the application and is cloud managed, it is disconnected from the application. This situation could occur when a cable is unplugged, the Internet connection is down, a gateway cannot be reached, a DNS name cannot be resolved, and so on. If you reset an access point to the factory default state, the access point restarts in the Disconnected state.

How the Configuration of a Cloud-Managed Access Point Can Be Changed

The configuration of a cloud-managed access point can be changed in the following ways:

- **BCWM application.** The BCWM application can configure the access point settings but provides only a subset of the complete configurable settings of an access point.
- **Web management interface of the access point.** When an access point is cloud managed, its web management is in restricted mode, allowing you to configure only a few select settings.
- **CLI through an SSH, Telnet, or console session to the access point.** You can configure all access points settings through the CLI, using an SSH, Telnet, or console session to the access point (not all these access options are available on all access point models). However, when the BCWM application pushes a configuration to the access point (for example, after the access point restarts), all settings that you made through the CLI are overwritten and lost.
- **SNMP management station connected to the access point.** You can configure all access point settings through SNMP commands from an SNMP management station that is connected to the access point. However, when the BCWM application pushes a configuration to the access point (for example, after the access point restarts), all settings that you made through SNMP commands are overwritten and lost.

Convert an Access Point From Cloud-Managed to Standalone

You can convert an access point from a cloud-managed access point to a standalone access point. Once converted, the access point is running the same firmware version that was used for the cloud-managed mode but is now in standalone mode with a full rather than restricted web management interface.

► **To convert an access point from a cloud-managed access point to a standalone access point:**

1. Open a browser on your computer.
2. In the address bar, enter <https://bc.netgear.com>.

Business Central Wireless Manager 2.1 Application

The application login page displays.

3. Enter the email address and password for your BCWM and click the **Login** button.
The Monitoring page displays.
4. Select **Inventory**.

Role: owner	Status: All	Decommission	Delete	Deploy	New Device		
☐	Device	Inventory Status	Connection Status	Location	Building	Floor	Software Version
☐	2GY2345R0005C (AP320-Upstairs-N...	Active	Connected	Netgear - Demo Home	Main	2	continuous_15.11.16.1923.68
☐	2GY2345B00041 (AP320-Downstair...	Active	Connected	Netgear - Demo Home	Main	1	continuous_15.11.16.1923.68
☐	4D815AE400034 (AP720-2-SMB-Lab)	Active	Connected	Netgear - Main Office			tailac_staging_1511.16.1936.112
☐	2925345800065 (AP350-2-SMB-Lab)	Active	Connected	Netgear - Main Office			continuous_15.11.10.2054.54
☐	2XK244NN0012F (AP660-Peets-Riv...	Active	Connected	Peets - Rivermark Plaza			continuous_15.11.16.1923.62
☐	2925345600055 (AP350-Peets-Airpo...	Active	Connected	Peets - San Jose Intl Ai...			continuous_15.11.10.2054.54
☐	4D815AER000AA (AP720-Peets-Air...	Active	Connected	Peets - San Jose Intl Ai...			tailac_staging_1601.05.2320.216
☐	4DA25AE300036 (AP730-Starbucks...	Active	Connected	Starbucks - North First			tailac_staging_1511.16.1936.112
☐	2XK244NE00135 (AP-660-Starbucks...	Active	Connected	Starbucks - River Oaks ...			continuous_15.11.16.1923.62

5. To filter the devices that are displayed in the table on the Inventory page, from the **Role** menu, select the type of user account (**owner**, **manager**, or **customer**) that is associated with the inventory that you want to display.

The **Role** menu is meaningful if you are assigned more than one user account. For example, you might be the owner of one location, manager for another location, and customer for a third location. The type of role determines the actions that are available to you on the Inventory page.

The table on the Inventory page displays the access points that are in inventory, whether active, decommissioned, or in the process of being provisioned or decommissioned.

6. To limit the access points in the table to the decommissioned ones, from the **Showing** menu, select **Decommissioned**.

The table on the Inventory page displays decommissioned access points only.

7. Select the check boxes for the access points that you want to remove from inventory.
The **Delete** button becomes available.

8. Click the **Delete** button.
A pop-up window opens and displays a warning.

9. Click the **Delete** button in the pop-up window.
The access points are removed from inventory.

10. Click the **Dismiss** button.
The pop-up window closes.

11. Open a browser on your computer.
12. In the address bar, enter the IP address of the access point.

By default, the access point functions as a DHCP client. If the access point is installed in a network that includes a DHCP server, the IP address of the access point is issued by the DHCP server.

Business Central Wireless Manager 2.1 Application

If the access point is not connected to a DHCP server or is accessible only over its default IP address, do the following:

- a. Change the IP address of your computer to an IP address in the 192.168.0.x subnet, which is the subnet in which the access point's default IP address is located.

For example, change the computer's IP address to 192.168.0.210.

- b. Connect your computer to the access point with an Ethernet cable.
- c. In the address bar of the browser, enter the default IP address of the access point:

- **WAC730.** 192.168.0.100
- **WAC720.** 192.168.0.100
- **WNDAP660.** 192.168.0.100
- **WNDAP360.** 192.168.0.100
- **WNDAP350.** 192.168.0.237
- **WNAP320.** 192.168.0.100
- **WNAP210v2.** 192.168.0.236

A login window opens.

13. Enter the user name and password.

The user name is **admin**. The default password is **password**.

14. Click the **LOGIN** button.

If the Change Password page displays, go to Step 14.

If the General page displays, go to Step 15.

15. If the Change Password page displays, specify a new password by doing the following:

- a. In the **Current Password** field, enter the existing password, which is the default password.
- b. In the **New Password** and **Repeat New Password** fields, specify the new password.
- c. Click the **APPLY** button.

A login window opens again.

- d. Enter the user name and new password.

The user name is **admin**. The new password is the one that you just specified.

- e. Click the **LOGIN** button.

The General page displays.

16. On the General page, click the **No** radio button.

By default, the **Yes** radio button is selected, the access point is enabled for the cloud (even though it is disconnected from the cloud), and the access point functions with a restricted web management interface (only the **Configuration** and **Monitoring** main menu tabs display).

17. Click the **APPLY** button.

Business Central Wireless Manager 2.1 Application

The access point restarts with factory default settings but retains its IP configuration and management VLAN.



CAUTION:

The access point broadcasts its default SSIDs and provides open networks without any security. If you do not want open networks, implement WiFi security or disable the radios.

The access point is now ready for standalone operation with a full web management interface. If you log back in to reconfigure the access point, the Change Password page might display again (because the access point was reset to factory default settings), in which case you once again must specify a new password.

The following table lists the technical specifications of the application.

Table 4. Technical specifications

Item	Specification
System architecture and supported devices	WiFi management as a service: Cloud hosted with an embedded agent on NETGEAR cloud-managed access points For information about the supported access point and required firmware versions, see Compatible NETGEAR WiFi Access Points on page 16.
Browser support	The desktop versions of the following browsers: • Microsoft Internet Explorer 11 or later • Mozilla Firefox 15 or later • Google Chrome 15 or later • Apple Safari 5 or later • Microsoft Edge 13 or later
OS support	Any OS with one of the supported browsers
Management interface support	Desktop web management interface
Language support	English