



Business Central Wireless Manager 2.1 Application

How to Start Guide

July 2016
202-11632-02

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.

Contents

Chapter 1 Prepare Your Access Points, Subscribe, and Get Started

- Basic Concepts.....5
- Prepare Your NETGEAR WiFi Access Points for Cloud Management.....6
 - Upgrade to the Required Cloud-Enabled Firmware Version.....7
 - Upgrade an Access Point From BCWM 1.0 to BCWM 2.0 or a Later BCWM Version.....12
- Subscribe to the BCWM 2.0 or a Later BCWM Version.....16
- Set Up a Location With a WiFi Network and Access Point.....18
 - Add Your First Location.....18
 - Add a First WiFi Network to a Location.....20
 - Add a First Access Point to a Location.....23
- Monitor WiFi Traffic and Client Usage at a Location.....25

Appendix A Upgrade to the Minimum Required Standalone Firmware Version

Prepare Your Access Points, Subscribe, and Get Started 1

This how to start guide provides information about how to prepare your access points for cloud management, how to subscribe to the NETGEAR Business Central Wireless Manager (BCWM), and how to get started with the BCWM 2.1 application.

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

For extensive configuration procedures, see the *Business Central Wireless Manager 2.1 User Manual*, which you can download from downloadcenter.netgear.com.

This chapter includes the following sections:

- *Basic Concepts* on page 5
- *Prepare Your NETGEAR WiFi Access Points for Cloud Management* on page 6
- *Subscribe to the BCWM 2.0 or a Later BCWM Version* on page 16
- *Set Up a Location With a WiFi Network and Access Point* on page 18
- *Monitor WiFi Traffic and Client Usage at a Location* on page 25

Note In this manual, *WiFi* and *wireless* are exchangeable terms.

Note The BCWM 2.1 application supports 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
-

Basic 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 multiple WiFi networks in the cloud.

The BCWM cloud management solution is intended primarily for single or multisite small and medium-sized businesses, K–12 education, small to medium hospitalities, retailers, and healthcare organizations.

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

The BCWM application functions with the following basic concepts:

- **Service locations.** With the application, the entire provisioning process is service location based. Access points and WiFi networks are installed at physical addresses that are referred to as service locations, or simply locations. In the application, these locations are logical locations and can span multiple Layer 2 or Layer 3 network segments.
- **Automatic network provisioning.** All WiFi networks configured at a location are automatically supported by all access points at that location. With standalone access points, you add a WiFi network to an access point. With managed access points, the application assigns the WiFi network automatically to one or more access points, depending on the number of WiFi networks and the number of access points at the location.
For access points that you assign to a location, you can attach building labels and floor labels to them. However, these are just labels for organization.
- **Offline location and network provisioning.** You can set up locations and WiFi networks while offline. Then, add access points and assign them to locations, allowing the networks to go online.
- **Location-based radio management.** For each location independently, you can manage the radio settings for individual or all access points and run or schedule automatic resource management for all access points.
- **Location-based firmware management.** For each location independently, you can run or schedule firmware updates for individual or all access points and reboot all access points or schedule to reboot them.
- **Monitoring.** You can display WiFi network and access point health; WiFi network and access point usage; WiFi network location maps; alarms; statistics for networks, access points, traffic, and clients; and neighboring access points, with the option to classify access points into known and unknown.
- **Application account management.** You can add accounts to the application, assign licenses to an account, assign locations to an account, assign access points to an account, and add and invite application users to an account.

Prepare Your NETGEAR WiFi Access Points for Cloud Management

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

If your access point runs a standalone firmware version that is not cloud enabled, consult the following table.

Table 1. 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

The 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. Note the following about upgrades:

- If your access point does run the minimum required standalone firmware version or a later standalone firmware version, you can upgrade directly to the required cloud-enabled firmware. For more information, see [Upgrade to the Required Cloud-Enabled Firmware Version](#) on page 7.
- In the unlikely situation that 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. For more information, see Appendix A, [Upgrade to the Minimum Required Standalone Firmware Version](#) on page 27.



CAUTION:

If your access point runs a standalone firmware version that is earlier than the minimum required standalone firmware version and you attempt to upgrade directly to the required cloud-enabled firmware version, you might be locked out of the access point's web management interface. 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 is already cloud-managed by the BCWM 1.0 application, you can upgrade it to a state in which it can be cloud-managed by the BCWM 2.0 application or a later version of the application. For more information, see [Upgrade an Access Point From BCWM 1.0 to BCWM 2.0 or a Later BCWM Version](#) on page 12.

Note The upgrade procedures in this guide describe and include screen shots of the traditional web management interface that is supported on most NETGEAR access points. However, the WAC720 and WAC730 access points use a newer style web management interface. The steps and screen shots for that interface are similar but not identical to the traditional interface.

Upgrade to the Required Cloud-Enabled Firmware Version

Follow this procedure if your access point runs the minimum required standalone firmware version (see the table in [Prepare Your NETGEAR WiFi Access Points for Cloud Management](#) on page 6) or a later version, but a version earlier than version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0).

If the access point runs firmware version 3.0.x.x or a later version but a version earlier than version 3.5.5.0, by default, the access point is enabled for the cloud and you first must disable the cloud mode before you can manually upgrade the firmware. This requirement does not apply to the WAC720 and WAC730 access points.

Log in to the access point's web management interface and perform the following steps:

1. If the access point runs firmware version 3.0.x.x or a later version but a version earlier than version 3.5.5.0, disable the cloud mode. (This step does not apply to the WAC720 and WAC730 access points.)
2. Upgrade the access point to the cloud-enabled firmware version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version.
3. If you want the access point to become ready for cloud management, make sure that the access point is connected to the Internet.
4. Reset the access point to factory default settings.

These steps are described in detail in the following procedure.

After you perform this one-time firmware upgrade for the access point and the access point becomes cloud managed, the application can centrally manage future firmware upgrades for the access point.

IMPORTANT:

After you upgrade an access point to the cloud-enabled firmware, you must reset the access point to factory default settings as described in the following procedure.

► To upgrade an access point to the required cloud-enabled firmware version and enable the access point for the cloud:

1. Visit the support website at netgear.com/support.
2. Navigate to the page for your access point and download firmware version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version.
3. Read the release notes before upgrading the firmware.
4. If the access point does not receive power through Power over Ethernet (PoE), apply power to the access point and wait for the access point to complete its startup procedure.
5. Open a browser on your computer.
6. 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.

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.

7. Enter the user name and password.
The user name is **admin**. The default password is **password**.
8. Click the **LOGIN** button.
The General page displays.

Business Central Wireless Manager 2.1 Application

If the access point runs firmware version 3.0.x.x or a later version but a version earlier than version 3.5.5.0, you must disable the cloud mode before you can upgrade the firmware. (This requirement does not apply to the WAC720 and WAC730 access points.)

If the access point provides a full web management interface, go to Step 10.

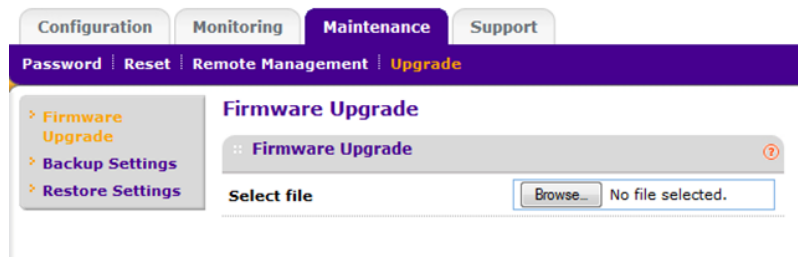
9. To disable the cloud mode and log back in to the access point, do the following:
 - a. On the General Page, next to Cloud Enabled, select the **No** radio button.
 - b. Click the **Apply** button.

The access point restarts with factory default settings but retains its IP configuration and management VLAN.
 - c. Open a browser on your computer.
 - d. In the address bar, enter the IP address that is assigned to the access point.
 - e. Enter the user name and password.

The user name is **admin**. The default password is **password**.
 - f. Click the **LOGIN** button.

The General page displays. The access point now provides a full web management interface.

10. Select **Maintenance > Upgrade**.



11. Click the **Browse** button, navigate to the firmware file on your computer, and select the firmware file.

The firmware displays to the right of the **Browse** button.
12. Click the **APPLY** button.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting.

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, the access point restarts.

You now must log back in to the access point, might need to specify a new password, and must reset the access point to factory default settings (see the following steps).

Note When the access point runs firmware version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version, by default, the access point is enabled for the cloud and operates with a limited web management interface (only the **Configuration** and **Monitoring** menu tabs display).

13. Log back in to the access point by doing the following:

- a.** Open a browser on your computer.
- b.** In the address bar, enter the IP address that is assigned to the access point.
A login window opens.
- c.** Enter the user name and password.
The user name is **admin**. The default password is **password**.
- d.** Click the **LOGIN** button.
If the Change Password page displays, go to Step 14.
If the General page displays, go to Step 15.

14. 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.

Business Central Wireless Manager 2.1 Application

- On the General page, verify that the **Yes** radio button is selected and that the Firmware Version field states the new firmware version.

The screenshot shows the 'Configuration' tab selected, with a sub-tab 'System'. Under 'System', the 'General' section is active. The 'Cloud Settings' section has 'Cloud Enabled' set to 'Yes' (radio button selected), 'Cloud Activation Status' set to 'Pending', and 'Cloud Connectivity Status' set to 'Disconnected'. A link 'Click here to open Cloud Management' is present. Below this is a note: 'NOTE: If Cloud Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Cloud Wireless Server to check if this Access Point has been registered for cloud management.' The 'Access Point Information' section displays the following details:

Access Point Name	netgear4CA528
Ethernet MAC Address	04:A1:51:4C:A5:28
Wireless MAC Address for 2.4GHz	04:A1:51:4C:A5:20
Wireless MAC Address for 5GHz	04:A1:51:4C:A5:30
Ethernet LLDP	Enabled
Band Steering to 5GHz	Disabled
Country / Region	United States
Firmware Version	3.5.1.3
Serial Number	2XXXXXX0001A
Current Time	Tue Feb 2 19:31:05 UTC 2016

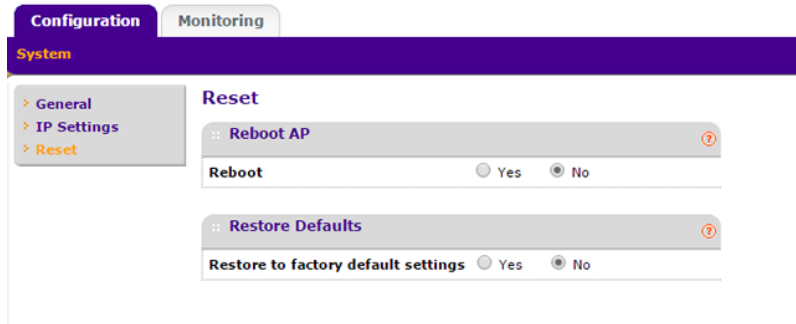
- If the access point is not yet connected to the Internet and you want it to become ready for cloud management, connect it to the Internet.

Wait several minutes. The access point must get an Internet connection and reach an NTP server.

Note You can also connect the access point to the Internet later. In that case, skip this step and the following step. After you reset the access point to factory default settings as described in Step 18, the access point is not ready for cloud management until you connect it to the Internet.

- To verify that the access point can reach an NTP server, make sure that the Current Time field on the General page (see the previous figure) shows the correct time for the configured time zone.
- Reset the access point to factory default settings by doing the following:

- a. Select **Reset**.
(The full path is **Configuration > System > Reset**.)



- b. Next to Restore to factory default settings, select the **Yes** radio button.
- c. Click the **APPLY** button.
- The access point restarts with factory default settings but retains its IP configuration and management VLAN.
- The access point is now ready for cloud management by the BCWM 2.0 application or a later version of the application. For information about how to add an access point to the application, see [Add a First Access Point to a Location](#) on page 23.

Upgrade an Access Point From BCWM 1.0 to BCWM 2.0 or a Later BCWM Version

You can upgrade an access point that is cloud-managed by the BCWM 1.0 application to a state in which it can be cloud-managed by the BCWM 2.0 application or a later version of the application.

Log in to the access point's web management interface and perform the following steps:

1. Disable the access point for the cloud, which causes the access point to reset to factory default settings.
2. Upgrade the access point firmware to version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version.
3. Make sure that the access point is connected to the Internet.

These steps are described in detail in the following procedure.

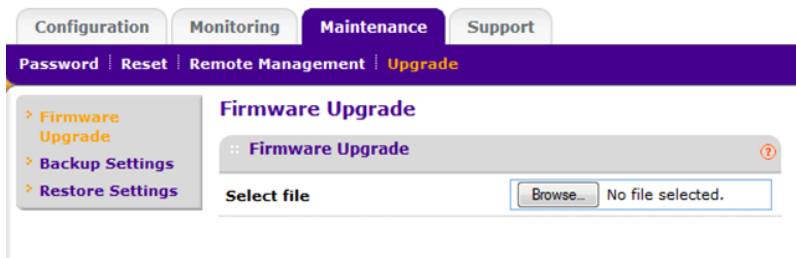
Note If you already know the IP address and password of the access point that you want to access, you can skip Step 1 and Step 2 in the following procedure and start with Step 3.

► **To upgrade an access point that is cloud-managed by the BCWM 1.0 application to a state in which it can be cloud-managed by the BCWM 2.0 application or a later version of the application:**

1. To view the IP address of the access point in the BCWM 1.0 application, do the following:
 - a. Open a browser on your computer.
 - b. In the address bar, enter **https://wireless.netgear.com**.
The application login page displays.
 - c. Enter the email address and password for your BCWM 1.0 account and click the **LOG IN** button.
 - d. The Home page displays.
 - e. Select **Inventory**.
All access point configurations display. By default, the configurations are sorted by access point name.
 - f. On the right side of the page, click the access point configuration for which you want to view the IP address.
The Access Point Profile section displays information about the access point.
 - g. Scroll down and click the **IP Settings** heading.
The IP address displays. Take note of the IP address, which you will need in Step 7.
2. To view the password of the access point in the BCWM 1.0 application, do the following:
 - a. Select **Configuration**.
The All Locations page displays.
 - b. In the LOCATIONS tree on the left, click the location to which the access point is assigned.
The Location Profile page displays.
 - c. On the right side of the page, click the **AP Local Management** heading.
The AP Local Management section expands.
 - d. To display the current password, select the **Show Characters** check box.
Take note of the password, which you will need in Step 8.
3. Visit the support website at netgear.com/support.
4. Navigate to the page for your access point and download firmware version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version.
5. Read the release notes before upgrading the firmware.
6. Open a browser on your computer.
7. In the address bar, enter the IP address of the access point.
Use the IP address that you determined in Step 1.
A login window opens.
8. Enter the user name and password.
The user name is **admin**. Use the password that you noted in Step 2.

9. Click the **LOGIN** button.
The General page displays.
10. Disable the access point for the cloud by doing the following:
 - a. Next to Cloud Enabled, select the **No** radio button.
 - b. Click the **APPLY** button.
The access point restarts with a full web management interface and factory default settings, but retains its IP configuration and management VLAN.
You now must log back in to the access point, might need to specify a new password, and must upgrade the firmware (see the following steps).
11. Log back in to the access point by doing the following:
 - a. Open a browser on your computer.
 - b. In the address bar, enter the IP address of the access point.
Because the access point retained its IP configuration, use the same IP address as the one that you used in Step 7.
A login window opens.
 - c. Enter the user name and password.
The user name is **admin**. The default password is **password**.
 - d. Click the **LOGIN** button.
If the Change Password page displays, go to Step 12.
If the General page displays, go to Step 13.
12. 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.

13. Select **Maintenance > Upgrade**.



14. Click the **Browse** button, navigate to the firmware file on your computer, and select the firmware file that you downloaded in Step 4.

The firmware displays to the right of the **Browse** button.

15. Click the **APPLY** button.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting.

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, the access point restarts.

16. To verify that the access point runs the new firmware version, is enabled for the cloud, and is connected to the Internet, log back in to the access point by doing the following:
- Open a browser on your computer.
 - In the address bar, enter the IP address of the access point.
Because the access point retained its IP configuration, use the same IP address as the one that you used in Step 7.
A login window opens.
 - Enter the user name and password.
The user name is **admin**. The password is either the default password (**password**) or the password that you specified in Step 12.
 - Click the **LOGIN** button.
The General page displays.

Business Central Wireless Manager 2.1 Application

Note When the access point runs firmware version 3.5.5.0 (or for the WAC720 and WAC730 access points, version 3.5.6.0) or a later version, by default, the access point is enabled for the cloud and operates with a limited web management interface (only the **Configuration** and **Monitoring** menu tabs display).

17. On the General page, verify that the **Yes** radio button is selected, that the **Firmware Version** field states the new firmware version, and that the **Current Time** field shows the correct time for the configured time zone.

The screenshot shows the 'Configuration' tab selected, with the 'Monitoring' tab also visible. The 'System' menu is open, showing 'General', 'IP Settings', and 'Reset'. The 'General' page is displayed, featuring two main sections: 'Cloud Settings' and 'Access Point Information'. In the 'Cloud Settings' section, 'Cloud Enabled' is set to 'Yes' (radio button selected), 'Cloud Activation Status' is 'Pending', and 'Cloud Connectivity Status' is 'Disconnected'. A link 'Click here to open Cloud Management' is present. A note states: 'NOTE: If Cloud Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Cloud Wireless Server to check if this Access Point has been registered for cloud management.' The 'Access Point Information' section lists various details: Access Point Name (netgear4CA528), Ethernet MAC Address (04:A1:51:4C:A5:28), Wireless MAC Address for 2.4GHz (04:A1:51:4C:A5:20), Wireless MAC Address for 5GHz (04:A1:51:4C:A5:30), Ethernet LLDP (Enabled), Band Steering to 5GHz (Disabled), Country / Region (United States), Firmware Version (3.5.1.3), Serial Number (2XXXXXX0001A), and Current Time (Tue Feb 2 19:31:05 UTC 2016).

Cloud Settings	
Cloud Enabled	☒ Yes ☐ No
Cloud Activation Status	Pending
Cloud Connectivity Status	Disconnected

[Click here to open Cloud Management](#)

NOTE: If Cloud Enabled is set to Yes, this Access Point will periodically attempt to contact NETGEAR Cloud Wireless Server to check if this Access Point has been registered for cloud management.

Access Point Information	
Access Point Name	netgear4CA528
Ethernet MAC Address	04:A1:51:4C:A5:28
Wireless MAC Address for 2.4GHz	04:A1:51:4C:A5:20
Wireless MAC Address for 5GHz	04:A1:51:4C:A5:30
Ethernet LLDP	Enabled
Band Steering to 5GHz	Disabled
Country / Region	United States
Firmware Version	3.5.1.3
Serial Number	2XXXXXX0001A
Current Time	Tue Feb 2 19:31:05 UTC 2016

The access point is now ready for cloud management by the BCWM 2.0 application or a later version of the application. For information about how to add an access point to the application, see [Add a First Access Point to a Location](#) on page 23.

Subscribe to the BCWM 2.0 or a Later BCWM Version

Before you can access the application, you must subscribe to the BCWM 2.0 or a later BCWM version.

Note If you already own an account for the BCWM 1.0, you must sign up again and create a new account for the BCWM 2.0 or a later BCWM version. *Do not use your BCWM 1.0 account for the BCWM 2.0 or a later BCWM version.*

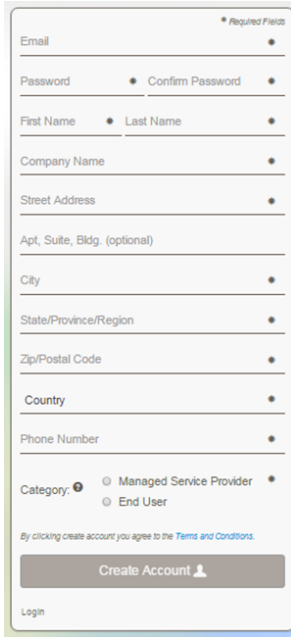
NETGEAR offers you a free 90-day trial subscription. NETGEAR does not impose any special limits on the number of locations, networks, and access points that you can add during the trial subscription.

Prepare Your Access Points, Subscribe, and Get Started

Business Central Wireless Manager 2.1 Application

► To subscribe to the BCWM 2.0 or a later BCWM version:

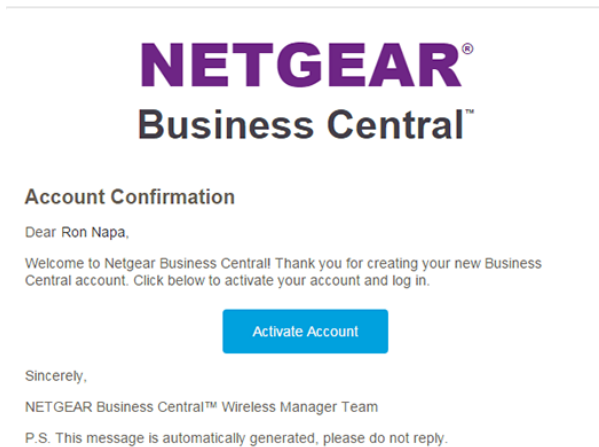
1. Open a browser on your computer.
2. In the address bar, enter **https://bc.netgear.com**.
The application login page displays.
3. Click the **Create Account** link.

A screenshot of the 'Create Account' form in the Business Central Wireless Manager 2.1 application. The form is titled 'Create Account' and includes a 'Login' link at the bottom. 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 small asterisk indicating it is a required field. There is also a 'Category' section with two radio buttons: 'Managed Service Provider' and 'End User'. Below the form, there is a line of text: 'By clicking create account you agree to the Terms and Conditions.' and a 'Create Account' button with a user icon.

4. 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:
* ! @ # \$ % ^ & ()"
5. 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.
After you complete all fields, the **Create Account** button becomes available.
6. 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.
7. 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.

Prepare Your Access Points, Subscribe, and Get Started

8. Go to your email inbox and open the email message.



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

Set Up a Location With a WiFi Network and Access Point

The following procedures describe how you can set up a basic location, add a single WiFi network, and add a single access point. Setting up a complex location with multiple WiFi networks and multiple access points is just an extension of these procedures: You simply add more WiFi networks and access points to the location.

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.

Business Central Wireless Manager 2.1 Application

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

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.
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.

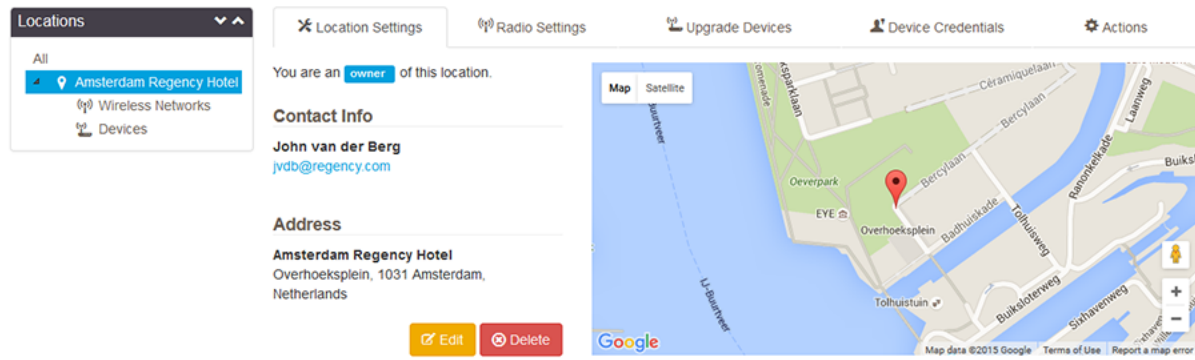
10. From the **Account** menu, select the account to which the location must be assigned.
An account is a set of locations that are funded by the same license. Each location must be assigned to an account with an active license (which can be a trial license) for access points to be licensed and

Business Central Wireless Manager 2.1 Application

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.

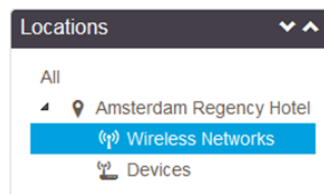


Add a First WiFi Network to a Location

When you add a location (see [Add Your First Location](#) on page 18), 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.
4. Select **Configuration**.
The Configuration page displays and shows the location that you added (see [Add Your First Location](#) on page 18).
5. In the Locations tree, click **Wireless Networks**.



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

Business Central Wireless Manager 2.1 Application

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

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

- 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.
- 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 points supports a single band only, the access points broadcasts on that band, unless your selection from the **Bands** menu disables that band.
- 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.
- 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.

Business Central Wireless Manager 2.1 Application

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 the *Business Central Wireless Manager 2.1 User Manual*, which you can download from downloadcenter.netgear.com.

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 the *Business Central Wireless Manager 2.1 User Manual*.

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 the *Business Central Wireless Manager 2.1 User Manual*.

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.

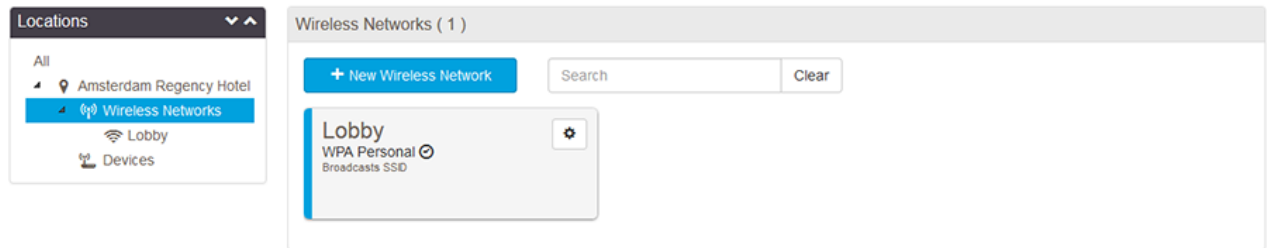
15. To set up a radio on/off broadcast schedule, select the **Create Schedule** check box.

For information about setting up a radio on/off broadcast schedule, see the *Business Central Wireless Manager 2.1 User Manual*.

16. Click the **Save** button.

Business Central Wireless Manager 2.1 Application

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 18), 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.

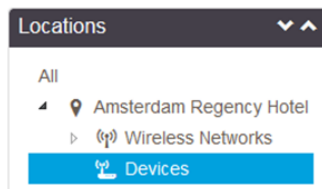


CAUTION:

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 18).
5. In the Locations tree, click **Devices**.



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

Business Central Wireless Manager 2.1 Application

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

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:

- 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. For more information, see the *Business Central Wireless Manager 2.1 User Manual*.

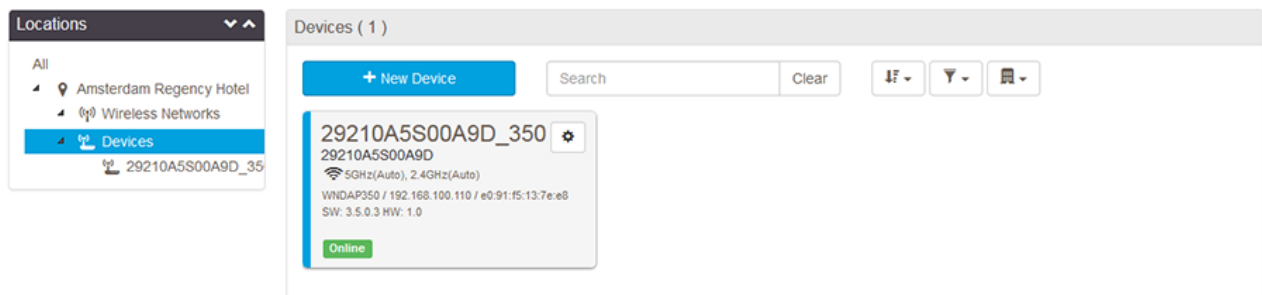
Business Central Wireless Manager 2.1 Application



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.



Monitor WiFi Traffic and Client Usage at a Location

After you set up a location, add one or more WiFi networks to the location, and assign one or more access points to the location, WiFi clients can access the networks. The application lets you monitor the WiFi traffic and client usage at the location.

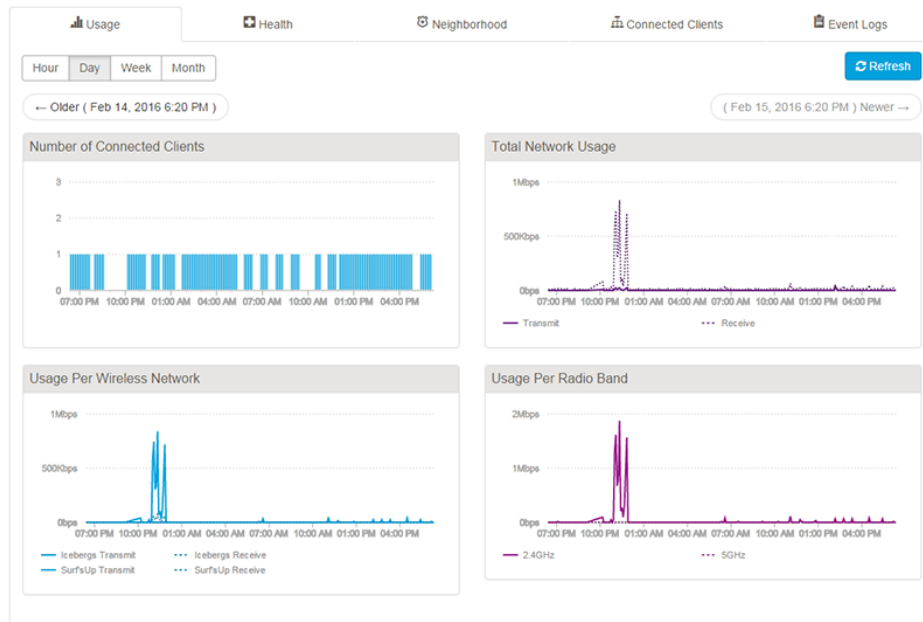
► To view a summary of WiFi traffic during the last 24 hours and details about current WiFi client usage at a location:

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.
The **Usage**, **Health**, **Neighborhood**, **Connected Clients**, and **Event Logs** tabs display. By default, the **Usage** tab is selected.

The page displays information about the number of connected clients, Ethernet network usage, WiFi network usage, and radio usage for the entire location. By default, the **Hour** button is selected.
5. Click the **Day** button.

Business Central Wireless Manager 2.1 Application

The information is restricted to the last 24 hours.



6. Click the **Connected Clients** tab.

The page displays detailed information about the connected clients for the entire location.

7. Click the **Day** button.

The information is restricted to the last 24 hours.

The screenshot displays the 'Connected Clients' tab of the Business Central Wireless Manager 2.1 application. The interface includes a navigation bar with tabs for Health, Usage, Neighborhood, Connected Clients, and Event Logs. Below the navigation bar, there are time range selectors for Hour, Day, Week, and Month, and a Refresh button. The main content area contains a table of connected clients.

▼ Last Seen	MAC Address	Signal Strength	Usage (rx + tx)	Client IP Address	Access Point	Building	Floor	SSID	Radio
★ 2 minutes ago	78:31:c1:62:c5:75	📶 (-89)	55.50 MB	192.168.10.166	2925345800365(AP350-2-SMB-Lab)			AP-360-2-Calvin	wlan1 (5GHz)
★ 2 minutes ago	6c:ad:f8:f2:66:65	📶 (0)	116.45 MB	0.0.0.0	4D815AE400034(AP720-2-SMB-Lab)			Netgear-SMB-Lab	wlan0 (2.4GH...
★ 2 minutes ago	ac:d1:b8:16:56:b5	📶 (-42)	2.79 GB	192.168.10.159	2925345800365(AP350-2-SMB-Lab)			Netgear-SMB-Guest	wlan0 (2.4GH...
★ 2 minutes ago	00:1d:e0:55:54:d9	📶 (-73)	1.73 GB	192.168.10.205	2925345800365(AP350-2-SMB-Lab)			Netgear-SMB-Lab	wlan1 (5GHz)
22 minutes ago	ac:d1:b8:f2:25:53	📶 (0)	1.06 GB	0.0.0.0	4D815AE400034(AP720-2-SMB-Lab)			Netgear-SMB-Guest	wlan0 (2.4GH...
5 hours ago	00:1b:77:cf:a4:5e	📶 (-60)	96.49 MB	192.168.10.176	2925345800365(AP350-2-SMB-Lab)			AP-360-2-Calvin	wlan1 (5GHz)

For more information about the BCWM 2.1 application and extensive information about monitoring procedures, see the *Business Central Wireless Manager 2.1 User Manual*, which you can download from downloadcenter.netgear.com.

Upgrade to the Minimum Required Standalone Firmware Version

A

Follow the procedure in this appendix *only* if your access point does not yet run the minimum standalone version that is required to upgrade the access point to the cloud-enabled firmware version (see the table in *Prepare Your NETGEAR WiFi Access Points for Cloud Management* on page 6).

Using the web management interface of the access point, upgrade the access point to the minimum required standalone firmware. When you are done, continue with the procedure that is described in *Upgrade to the Required Cloud-Enabled Firmware Version* on page 7.

► To upgrade an access point to the minimum required standalone firmware version:

1. Visit netgear.com/support.
2. Navigate to the support page for your access point and download the minimum required standalone firmware version for your access point.
For more information, see the table in *Prepare Your NETGEAR WiFi Access Points for Cloud Management* on page 6.

3. Read the release notes before upgrading the firmware.
4. If the access point does not receive power through Power over Ethernet (PoE), apply power to the access point and wait for the access point to complete its startup procedure.
5. Open a browser on your computer.
6. 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.

If the access point is not connected to a DHCP server or is accessible only over its default IP address, do the following:

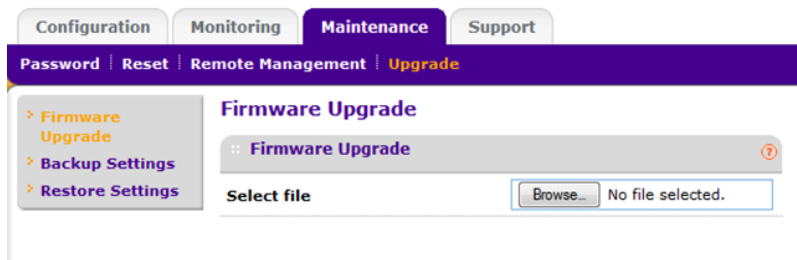
- a. Change the IP address of your computer to an IP address in the 192.168.0.x subnet, which is the subnet in which the access point's default IP address is located.
For example, change the computer's IP address to 192.168.0.210.
- b. Connect your computer to the access point with an Ethernet cable.
- 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

Business Central Wireless Manager 2.1 Application

- **WNAP320.** 192.168.0.100
- **WNAP210v2.** 192.168.0.236

A login window opens.

7. Enter the user name and password.
The user name is **admin**. The default password is **password**.
8. Click the **LOGIN** button.
The General page displays.
9. Select **Maintenance > Upgrade**.



10. Click the **Browse** button, navigate to the firmware file on your computer, and select the firmware file.
The firmware displays to the right of the **Browse** button.
11. Click the **APPLY** button.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting.

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, the access point restarts.

12. To verify that the access point runs the new firmware version, log back in to the access point by doing the following:
 - a. Open a browser on your computer.
 - b. In the address bar, enter the IP address that is assigned to the access point.
A login window opens.
 - c. Enter the user name and password.
The user name is **admin**. The default password is **password**.
 - d. Click the **LOGIN** button.
If the Change Password page displays, go to Step 13.
If the General page displays, go to Step 14.

13. 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.

14. Select **Monitoring > System**.

The Firmware Version field states the new firmware version.

Continue with the procedure that is described in *Upgrade to the Required Cloud-Enabled Firmware Version* on page 7.