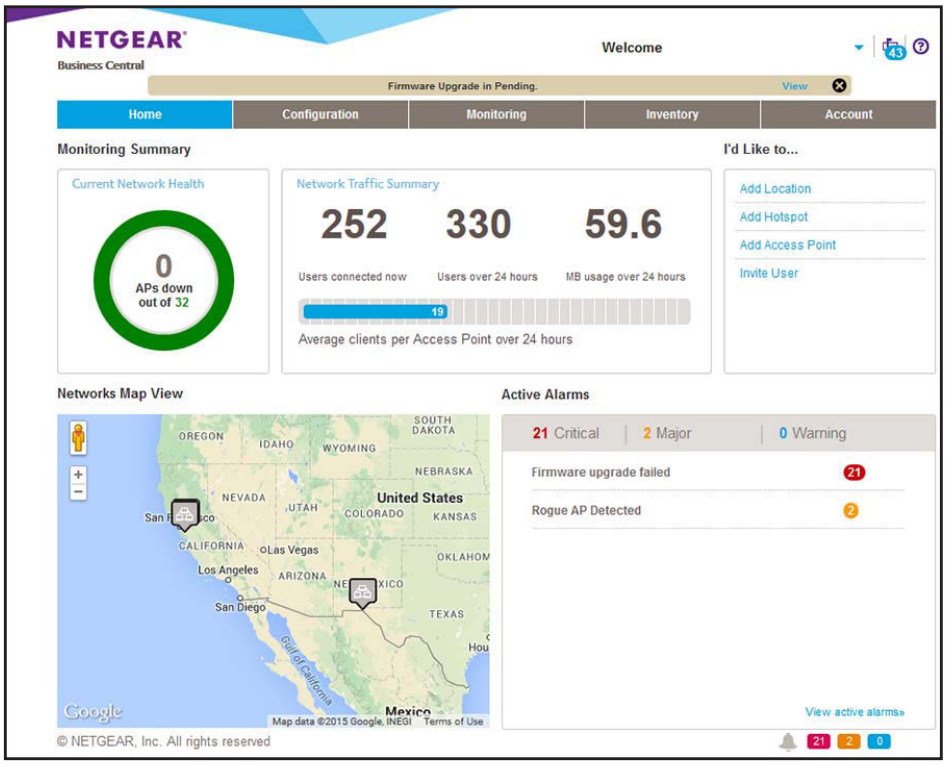
NETGEAR®

Business Central Wireless Manager Application

Quick Start Guide



June 2015
201-19279-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

For product updates and web support, visit *http://support.netgear.com*.

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

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
201-19279-01	June 2015	First publication of the Quick Start Guide

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

This quick 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 application.

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

The quick start guide includes the following sections:

- *Basic Concepts*
- *Prepare Your NETGEAR Wireless Access Points for Cloud Management*
- *Subscribe to the Business Central Wireless Manager*
- *Use the Get Started Wizard to Set Up a Location and WiFi Network*
- *Alternate Method: Set Up a Basic Location*
- *Monitor WiFi Traffic and Client Usage at a Location*

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

Basic Concepts

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

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

Note: In this manual, the BCWM 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.
- **Buildings and floors**. When you set up a location, the application automatically creates a default building (Building 1) and floor (Floor 1) for the location. You can add multiple buildings and floors to the location. In the application, these buildings and floors are logical groupings and, although they can, they do not need to correspond to physical locations or network segments.

  You assign an access point to a building or to a specific floor in a building. However, you add WiFi networks to the location, not to a building or floor.
- **Automatic network provisioning**. All networks configured at a location are automatically applied to 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 network automatically to one or more access points, depending on the number of networks and the number of access points at the location.
- **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.
- **Shared settings**. The application lets you set up global configurations (referred to as *shared settings*) for captive portal profiles, RADIUS server profiles, policy plans, user groups, hotspot users, and MAC ACLs. You can assign these to any location.
- **Monitoring**. You can display WiFi network and access point health; WiFi network and access point usage; WiFi network location maps; alarms and alarm trends; 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 manage licenses, add and invite application users, schedule maintenance slots, schedule access point firmware updates or run updates immediately, and back up and restore application settings.

Prepare Your NETGEAR Wireless 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 wireless access points running cloud-enabled firmware version 3.0.0.7 or later:

- WNAP210v2 ProSAFE Wireless-N Access Point
- WNAP320 ProSAFE Wireless-N Access Point
- WNDAP350 ProSAFE Dual Band Wireless-N Access Point
- WNDAP360 ProSAFE Dual Band Wireless-N Access Point
- WNDAP660 ProSAFE Dual Band Wireless-N Access Point

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

Table 1. Software requirements for upgrade to the cloud-enabled firmware version

Access Point Model	Minimum Required Standalone Firmware	Required Cloud-Enabled Firmware
WNAP210v2 ProSAFE Wireless-N Access Point	v2.1.4.8	v3.0.0.7 or later
WNAP320 ProSAFE Wireless-N Access Point	v2.1.6	v3.0.0.7 or later
WNDAP350 ProSAFE Dual Band Wireless-N Access Point	v2.1.9	v3.0.0.7 or later
WNDAP360 ProSAFE Dual Band Wireless-N Access Point	V2.1.12	v3.0.0.7 or later
WNDAP660 ProSAFE Dual Band Wireless-N Access Point	V2.0.5	v3.0.0.7 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.

Which Preparation Procedure Should You Follow?

Depending on the firmware version that your access point runs, to prepare your access point for cloud management, follow the procedure or procedures that are listed in the following table.

Table 2. Access point preparation procedures

Standalone Firmware	Preparation Procedures
Access point runs a standalone firmware *earlier* than the minimum required.	1. *Upgrade to the Minimum Required Standalone Firmware Version* 2. *Upgrade to the Required Cloud-Enabled Firmware Version and Enable the Access Point for the Cloud*
Access point runs the minimum required standalone firmware or later.	*Upgrade to the Required Cloud-Enabled Firmware Version and Enable the Access Point for the Cloud*
Access point runs standalone firmware 3.0.0.7 or later.	*Enable an Access Point Running Firmware Version 3.0.0.7 or Later for the Cloud*

Upgrade to the Minimum Required Standalone Firmware Version

Follow this procedure 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 *Table 1* on page 5).

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 and Enable the Access Point for the Cloud* on page 8.

If your access point already runs the minimum required standalone firmware version or later or runs firmware version 3.0.0.7 or later, skip this procedure.

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

1. Visit *support.netgear.com*.
2. Navigate to the support page for your access point and download the minimum required standalone firmware version for your access point (see *Table 1* on page 5).
3. Read the release notes before upgrading the software.
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:

   - **WNAP210v2**. 192.168.0.236
   - **WNAP320**. 192.168.0.100
   - **WNDAP350**. 192.168.0.237
   - **WNDAP360**. 192.168.0.100
   - **WNDAP660**. 192.168.0.100

A login window opens.

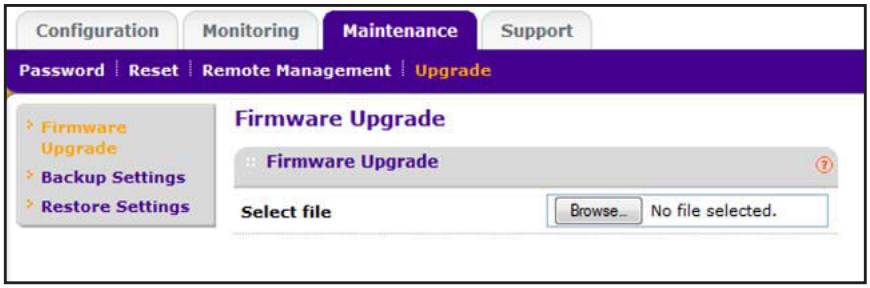
7. Enter the user name and password.

   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 upload. 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, do 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.
    c. Enter the user name and password.
    d. Click the **LOGIN** button.

       The General page displays.

    e. Select **Monitoring > System**.

       The **Firmware Version** field must state the new firmware version.

Upgrade to the Required Cloud-Enabled Firmware Version and Enable the Access Point for the Cloud

Follow this procedure if your access point runs the minimum required standalone firmware version (see *Table 1* on page 5) or a later version, but a version earlier than version 3.0.0.7.

You must load the required firmware onto the access point. Using the web management interface of the access point, upgrade the access point to the cloud-enabled firmware, reset the access point to factory default settings, and enable the access point for the cloud.

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.

If your access point already runs firmware version 3.0.0.7 or later, see *Enable an Access Point Running Firmware Version 3.0.0.7 or Later for the Cloud* on page 13.

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 *support.netgear.com*.
2. Navigate to the support page for your access point and download the cloud-enabled firmware version for your access point.
3. Read the release notes before upgrading the software.
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.

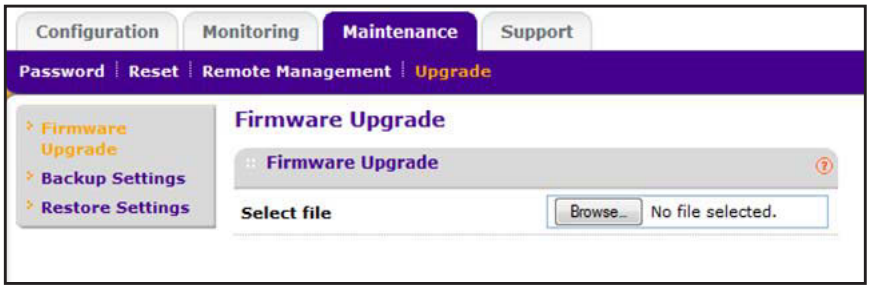
   b. Connect your computer to the access point with an Ethernet cable.
   c. In the address bar of the browser, enter the default IP address of the access point:

      - **WNAP210v2**. 192.168.0.236
      - **WNAP320**. 192.168.0.100
      - **WNDAP350**. 192.168.0.237
      - **WNDAP360**. 192.168.0.100
      - **WNDAP660**. 192.168.0.100

   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 upload. 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, specify a new password (the new firmware version requires you to do so), and reset the access point to factory default settings (see *Step 12* through *Step 14*).

12. Log back in to the access point and specify a new password:
    a. Open a browser on your computer.
    b. In the address bar, enter the IP address that is assigned to the access point.
    c. Enter the user name and password.

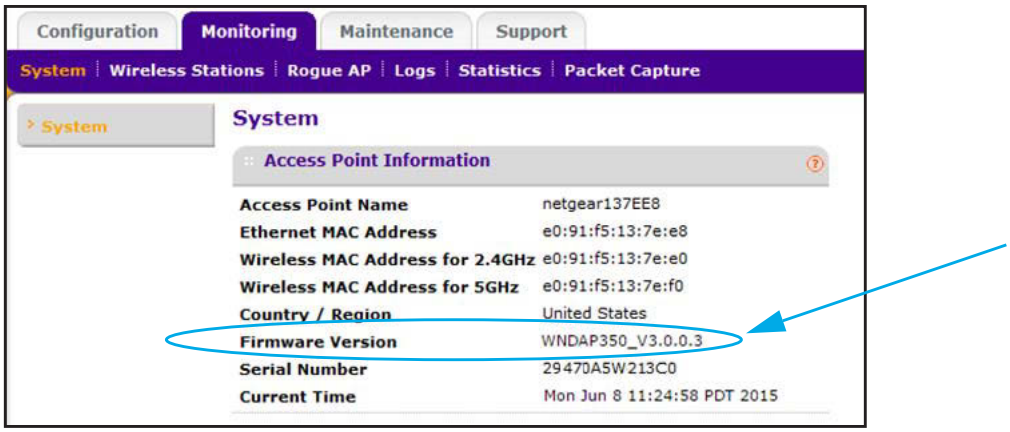
       The user name is **admin**. The default password is **password**.
    d. Click the **LOGIN** button.

       The Change Password page displays.
    e. In the **Current Password** field, enter **password**, which is the default password.
    f. In the **New Password** and **Repeat New Password** fields, specify the new password.
    g. Click the **APPLY** button.

       A login window opens.
    h. Enter the user name and new password.

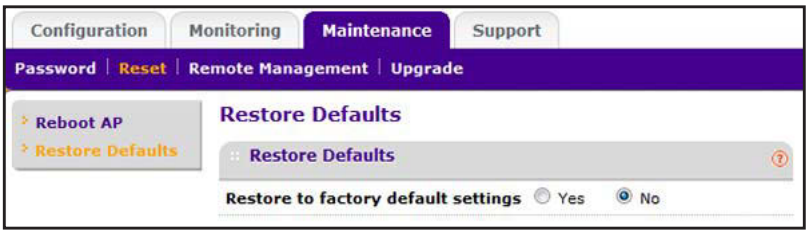
       The user name is **admin**. The new password is the one that you just specified.
    i. Click the **LOGIN** button.

       The General page displays.
13. To verify that the access point runs the new firmware version, select **Monitoring > System**.



The **Firmware Version** field must state the new firmware version.

14. Reset the access point to factory default settings:
    a. Select **Maintenance > Reset > Restore Defaults**.



    b. Select the **Yes** radio button.
    c. Click the **APPLY** button.

       The access point resets to factory defaults, retains the cloud-enabled software that you just uploaded, and restarts.

WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the reset. 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.

15. If the access point is not yet connected to the Internet, connect it to the Internet.

    You now must log back in to the access point again, once again specify a new password (the new firmware version requires you to do so), enable the access point for the cloud, and verify that the access point can reach an NTP server (see *Step 16* through *Step 18*).

16. Log back in to the access point and specify a new password:
    a. Open a browser on your computer.
    b. In the address bar, enter the IP address that is assigned to the access point.

Note: If you connected the access point to the Internet in *Step 15*, make sure that you enter the correct IP address, which is not the factory default IP address. 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.

c. Enter the user name and password.

The user name is **admin**. The default password is **password**.

d. Click the **LOGIN** button.

The Change Password page displays.

e. In the **Current Password** field, enter **password**, which is the default password.

f. In the **New Password** and **Repeat New Password** fields, specify the new password.

g. Click the **APPLY** button.

A login window opens.

h. Enter the user name and new password.

The user name is **admin**. The new password is the one that you just specified.

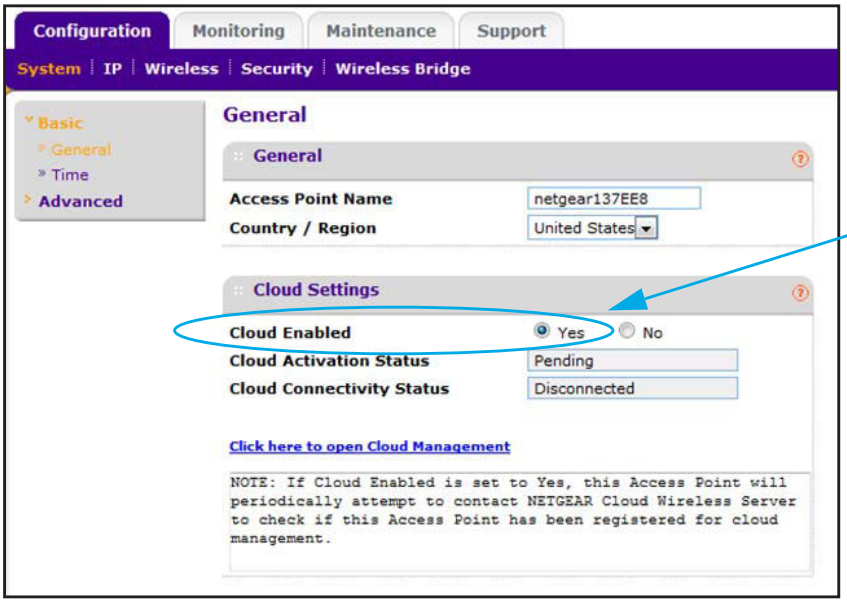
i. Click the **LOGIN** button.

The General page displays.

17. Enable the access point for the cloud:

a. Select **Configuration > System**.

b. Select the **Yes** radio button.

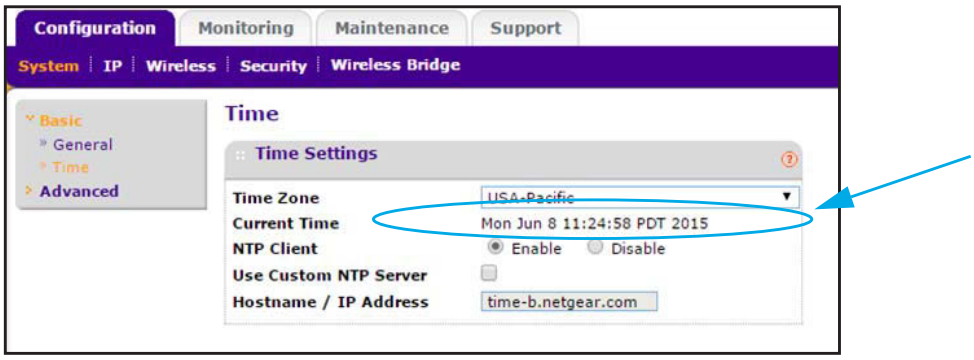


c. Click the **APPLY** button.

Your settings are saved.

The **Cloud Activation Status** field shows **Pending** and the **Cloud Connectivity Status** field shows **Disconnected**.

18. To verify that the access point can reach an NTP server and detect the correct time for the configured time zone, select **Configuration > System > Time**.



The **Current Time** field must show the correct time for the configured time zone. If it does, the access point is ready for cloud management by the application.

Enable an Access Point Running Firmware Version 3.0.0.7 or Later for the Cloud

Follow this procedure if you purchased a new access point that runs firmware version 3.0.0.7 or later.

If your access point runs the minimum required standalone firmware version (see *Table 1* on page 5) or a later version, but a version earlier than version 3.0.0.7, see *Upgrade to the Required Cloud-Enabled Firmware Version and Enable the Access Point for the Cloud* on page 8.

➢ **To enable an access point running firmware version 3.0.0.7 or later for the cloud:**

1. If the access point is not yet connected to the Internet, connect it to the Internet.

   Note: 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.

2. Open a browser on your computer.
3. In the address bar, enter the IP address that is assigned to the access point.

   Note: If you connected the access point to the Internet in *Step 1*, make sure that you enter the correct IP address. 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.

d. Enter the user name and password.

   The user name is **admin**. The default password is **password**.

e. Click the **LOGIN** button.

   The Change Password page displays.

4. Specify a new password:
   a. In the **Current Password** field, enter **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.

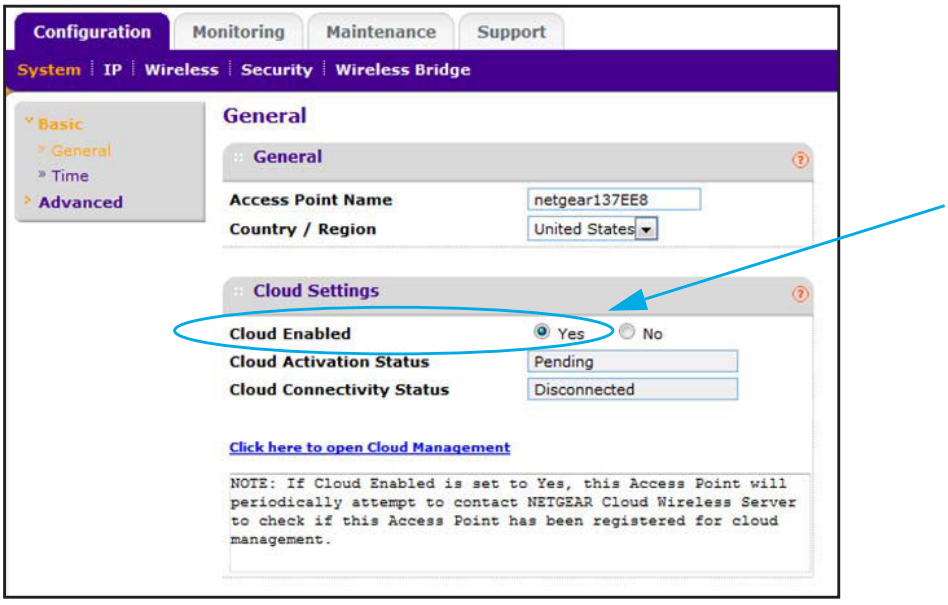
   d. Enter the user name and new password.

      The user name is **admin**. The new password is the one that you just specified.

   e. Click the **LOGIN** button.

      The General page displays.

5. Enable the access point for the cloud:
   a. Select **Configuration > System**.
   b. Select the **Yes** radio button.

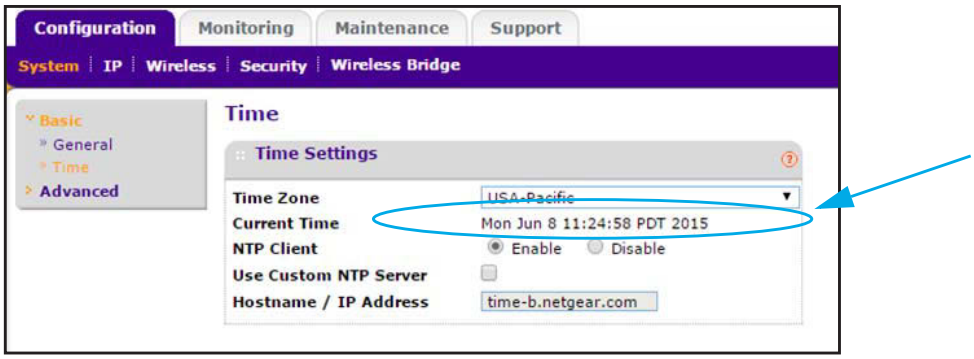


   c. Click the **APPLY** button.

      Your settings are saved.

      The **Cloud Activation Status** field shows **Pending** and the **Cloud Connectivity Status** field shows **Disconnected**.

6. To verify that the access point can reach an NTP server and detect the correct time for the configured time zone, select **Configuration > System > Time**.



The **Current Time** field must show the correct time for the configured time zone. If it does, the access point is ready for cloud management by the application.

Subscribe to the Business Central Wireless Manager

Before you can access the application, you must subscribe to the BCWM. You can use your existing MyNETGEAR account to subscribe to the BCWM. If you do not own a MyNETGEAR account, create one and subscribe to the BCWM.

NETGEAR offers you a free 90-day trial subscription. NETGEAR does not impose any special limits to the number of locations, networks, and access points[1] that you can add during the trial subscription.

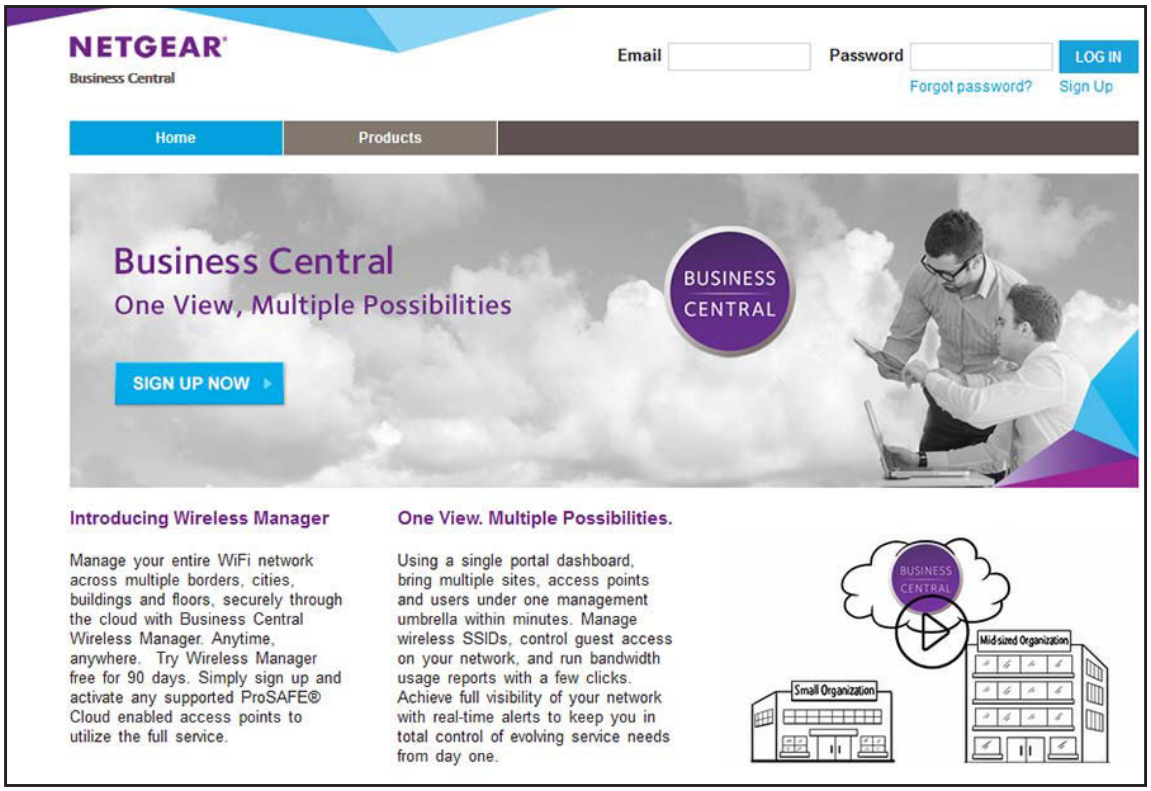
Use Your Existing MyNETGEAR Account to Subscribe to the BCWM

If you already own a MyNETGEAR account, use your existing MyNETGEAR account to subscribe to the BCWM.

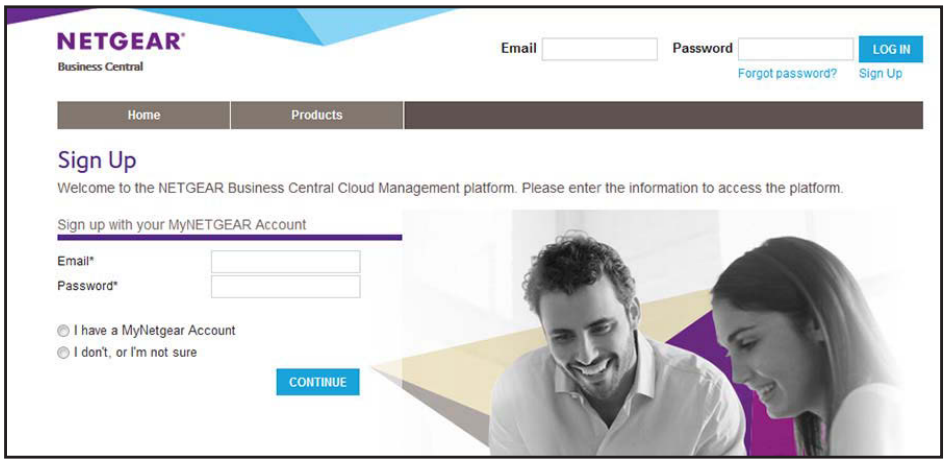
➢ **To use your existing MyNETGEAR account to subscribe to the BCWM:**

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

1. By default, an account with a free trial subscription or paid-for subscription can support up to 4,000 access points.

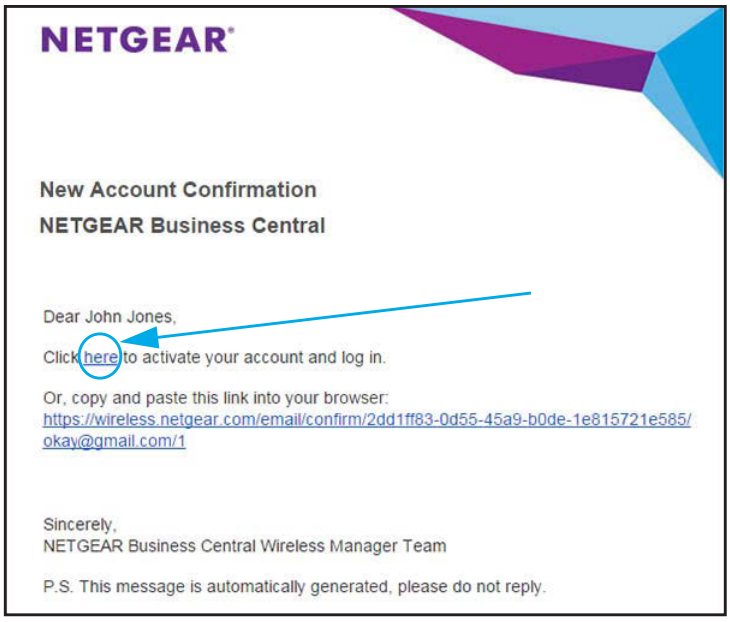


3. Click the **SIGN UP NOW** button.

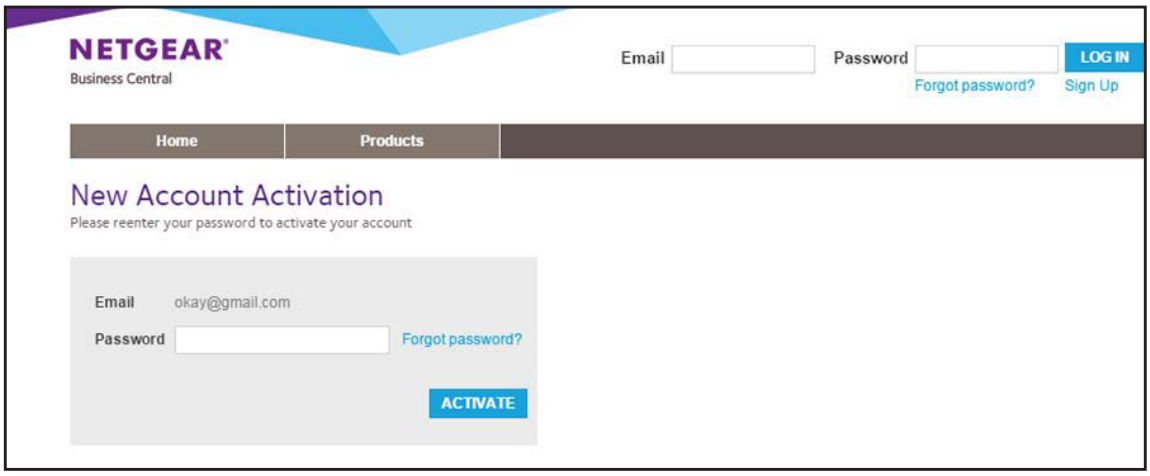


4. In the **Email** field, enter the email address for your existing MyNETGEAR account.
5. In the **Password** field, enter the password for your existing MyNETGEAR account.
6. Select the **I have a MyNetgear Account** radio button.
7. Click the **SIGN UP** button.

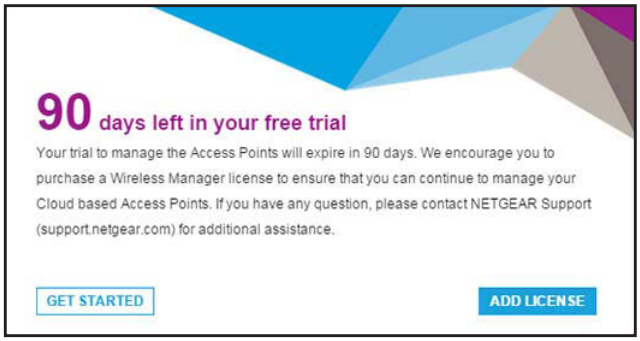
   If you signed up successfully, the Sign Up Was Successful page displays and NETGEAR sends you a confirmation email with a confirmation link.



8. Open the confirmation email and click the **here** link.



9. In the **Password** field, enter the password with which you set up your account.
10. Click the **ACTIVATE** button.



Your account is activated. You can log in immediately by clicking the **GET STARTED** button or add a license immediately by clicking the **ADD LICENSE** button. You can also close the page and log in later (see *Use the Get Started Wizard to Set Up a Location and WiFi Network* on page 21) or add a license later.

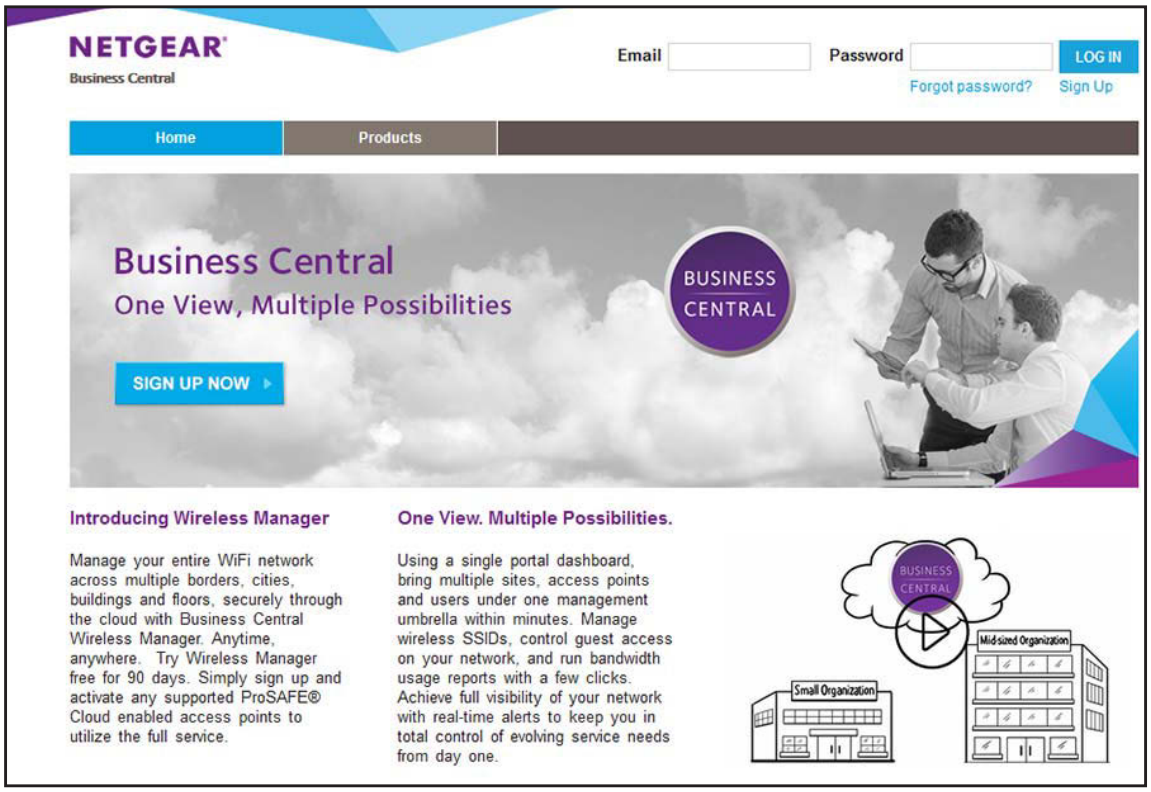
In addition, NETGEAR sends you an account trial start notification email.

Create a NETGEAR Account and Subscribe to the BCWM

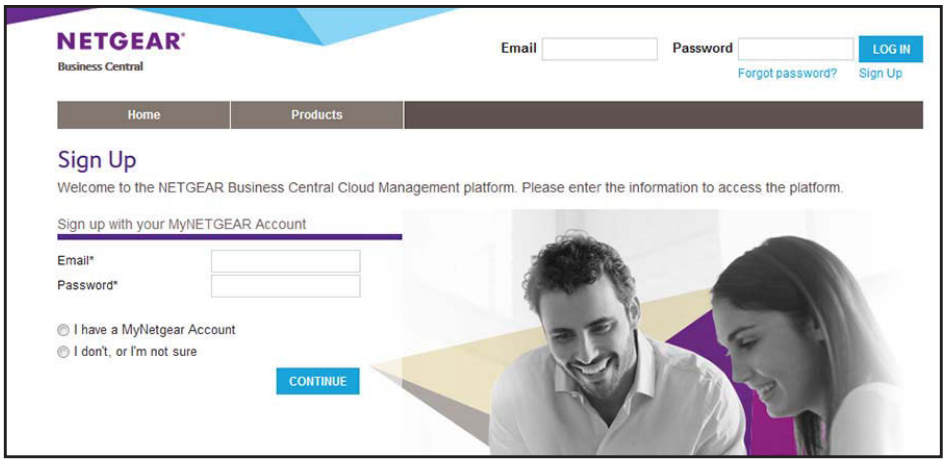
If you did not yet sign up for a MyNETGEAR account, create a new NETGEAR account and subscribe to the BCWM.

➢ **To create a NETGEAR account and subscribe to the BCWM:**

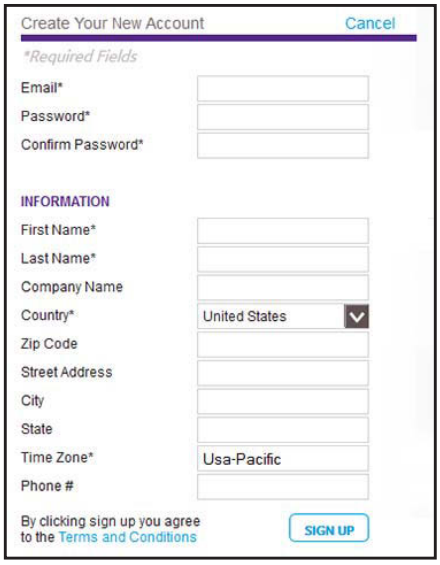
1. Open a browser on your computer.
2. In the address bar, enter **https://wireless.netgear.com**.



3. Click the **SIGN UP NOW** button.

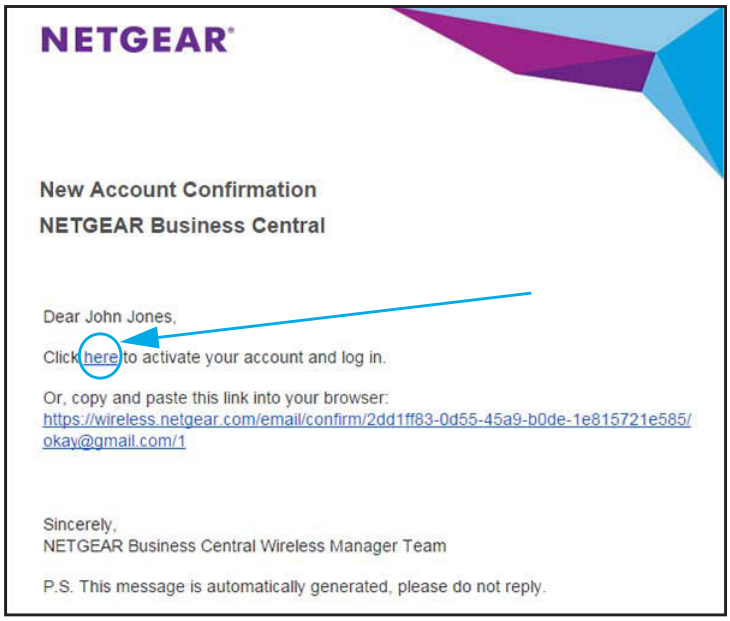


4. Select the **I don't, or I'm not sure** radio button.

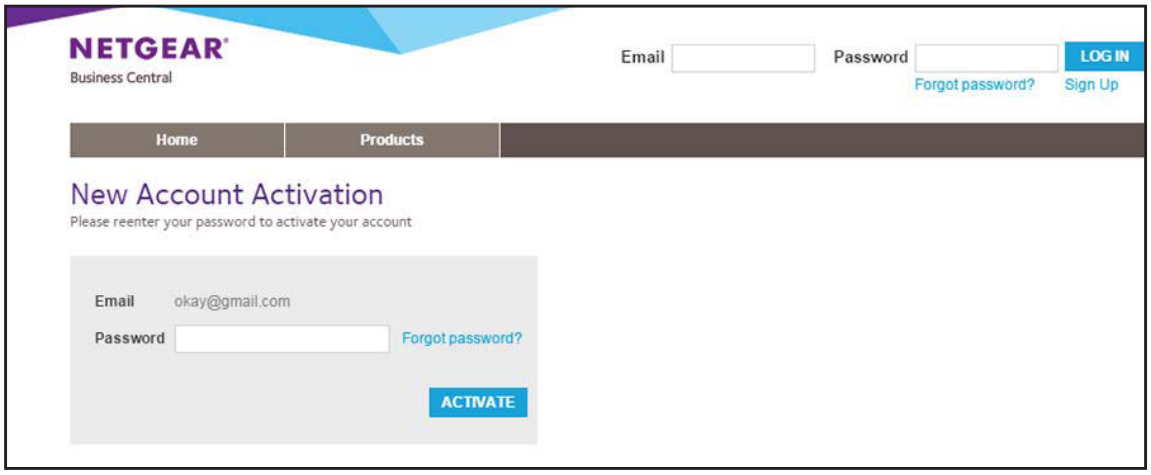


5. Enter your email address, specify and confirm a password, and enter all required and optional information.
6. To view the terms and conditions, click the **Terms and Conditions** link.
7. Click the **SIGN UP** button.

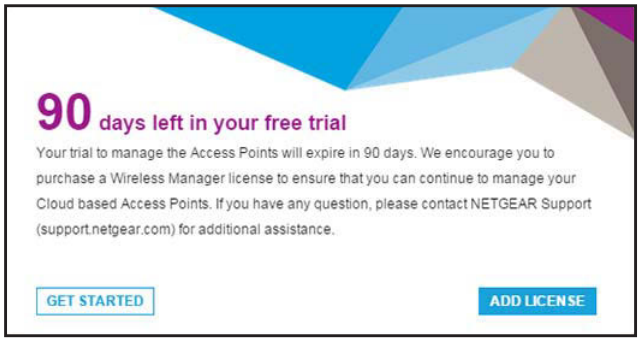
   If you signed up successfully, the Sign Up Was Successful page displays and NETGEAR sends you a confirmation email with a confirmation link.



8. Open the confirmation email and click the **here** link.



9. In the **Password** field, enter the password with which you set up your account.
10. Click the **ACTIVATE** button.



Your account is activated. You can log in immediately by clicking the **GET STARTED** button or add a license immediately by clicking the **ADD LICENSE** button. You can also close the page and log in later (see *Use the Get Started Wizard to Set Up a Location and WiFi Network* on page 21) or add a license later.

In addition, NETGEAR sends you an account trial start notification email.

Use the Get Started Wizard to Set Up a Location and WiFi Network

Before you can configure the application, you must use the Get Started wizard to set up at least one location and WiFi network. Setting up an access point during the Get Started wizard process is optional because you can also do that later.

If you prefer, you can add multiple access points to the application inventory *before* you initiate the Get Started wizard. For information about adding multiple access points to the application inventory, see the *Business Central Wireless Manager User Manual*, which you can download from *downloadcenter.netgear.com*.

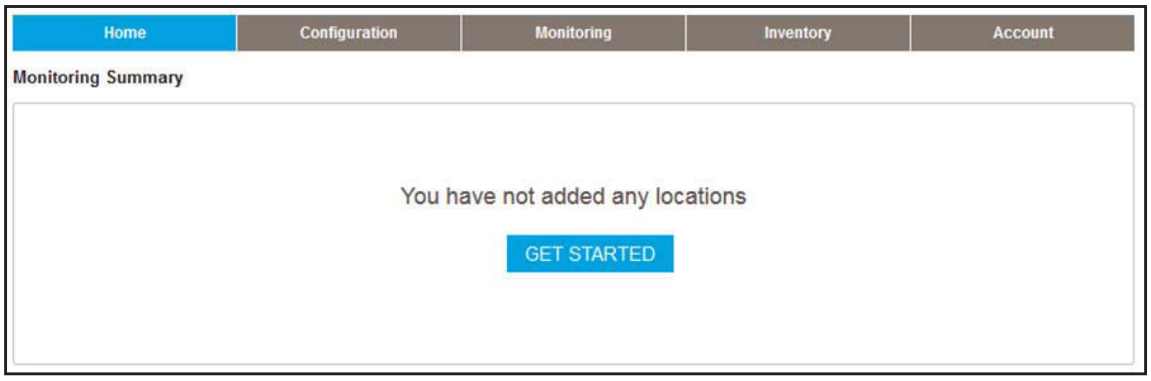
Note: If you already set up a location and WiFi network, the Get Started wizard no longer displays. Instead, see *Alternate Method: Set Up a Basic Location* on page 27.

Note: After five unsuccessful login attempts, your account is blocked for five minutes. While your account is being blocked, you can reset and redefine your account password, but the account remains blocked for five minutes. After five minutes, you can attempt to log in to your account with the new password.

➢ **To add a new location, network, and access point for the first time using the Get Started wizard:**

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

   The application login page displays.
3. Enter the email address and password for your BCWM account and click the **LOG IN** button.

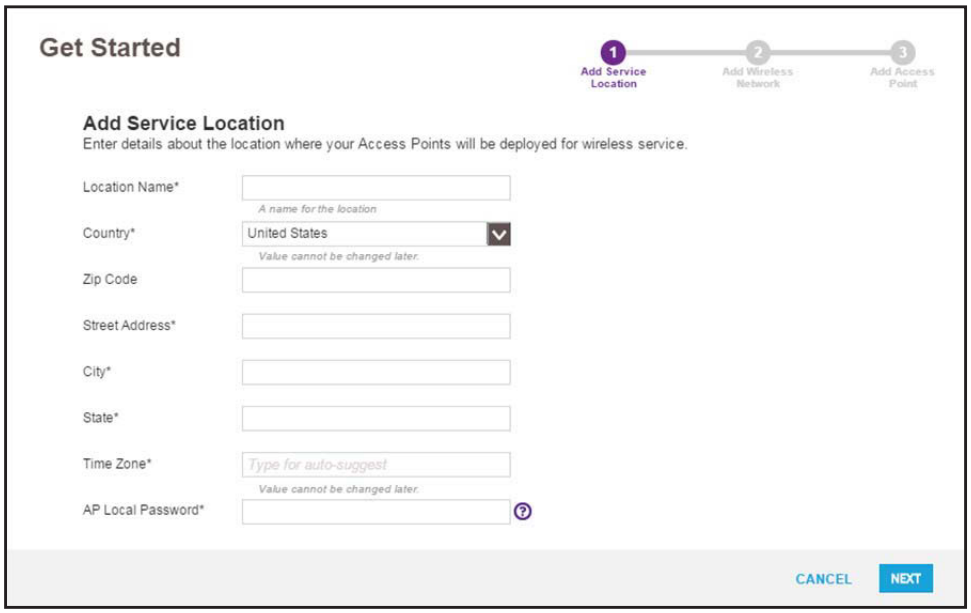


Except for adding access points to the application inventory and making changes to your account, no configuration options other than initiating the Get Started wizard are available to you. You must set up a location before you can configure and monitor networks and access points.

4. Click the **GET STARTED** button.

   The Get Started page displays. This page provides information only.

5. Click the **START** button.

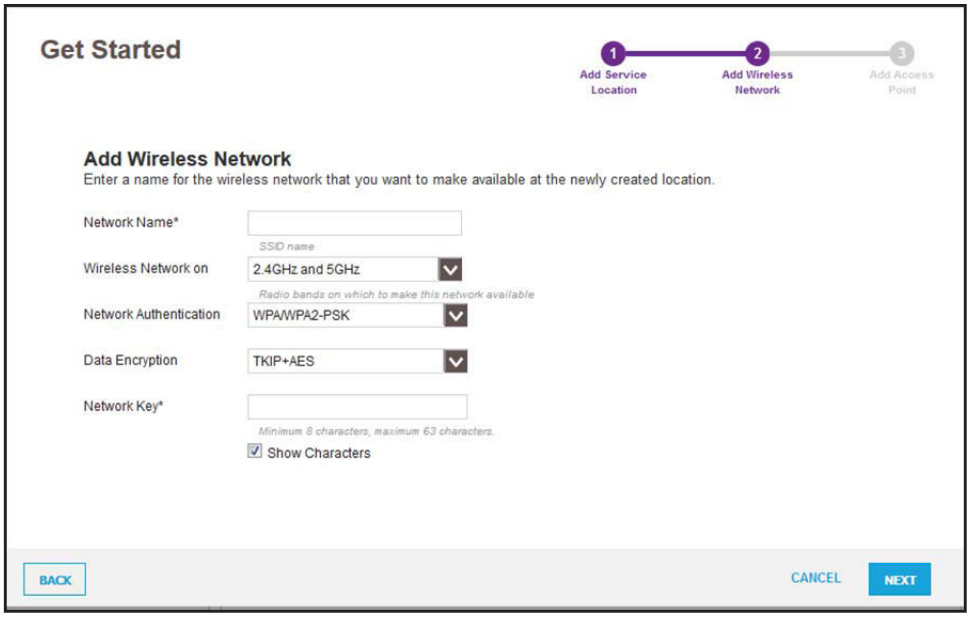


6. Specify a location name, complete the location address fields, select a time zone, and set the location-specific password for the access points that you can assign to the location.

   Note: Entering correct address information allows the location to be displayed on Google Maps.

Note: The password that you must set in this step is the password that you need when you want to access the web management interface of an individual cloud-managed access point or to access a cloud-managed access point over an SSH connection.

7. Click the **NEXT** button.



8. Configure the network settings:
   a. In the **Network Name** field, enter a WiFi network name (SSID).
   b. From the **Wireless Network on** menu, select the WiFi band or bands.

      Dual-band configurations apply only to access points that support both the 2.4 GHz and 5 GHz bands.

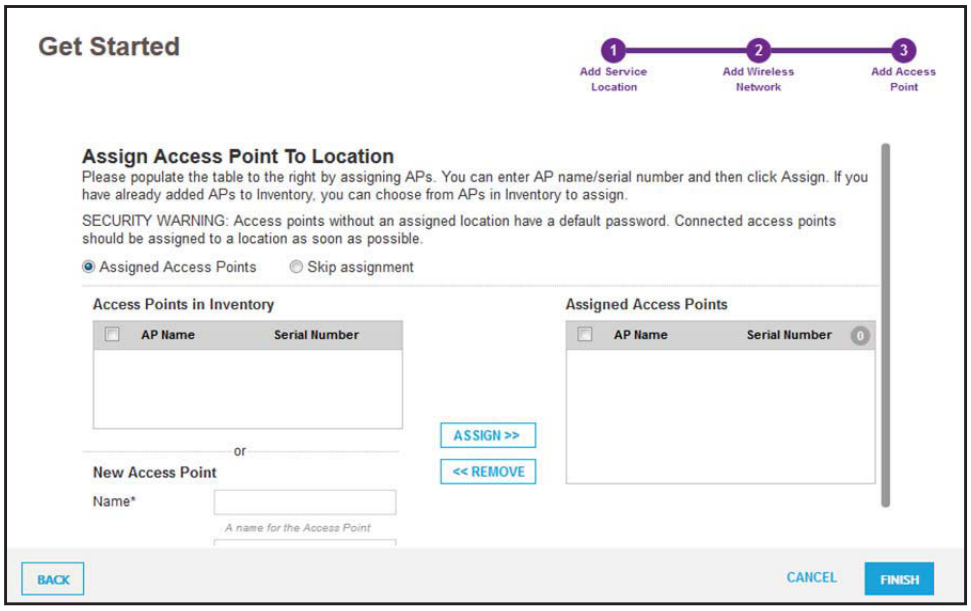
   c. From the **Network Authentication** menu, select the type of authentication.

      If you need advanced authentication, select one of the available options from the **Network Authentication** menu and complete the procedure. Then, configure the advanced authentication (see the *Business Central Wireless Manager User Manual*).

   d. From the **Data Encryption** menu, select the type of encryption.
   e. In the **Network Key** field, enter the network key that you want to use.

      You can enter up to 63 alphanumeric and special characters.

9. Click the **NEXT** button.



10. Decide if you do not want to add an access point, add and assign one or more new access points, or assign one or more access points that are already in the application inventory:

    - **Do not add an access point**. If you do not want to add an access point at this time, do the following:

      a. Click the **Skip Assignment** button.

      b. Continue with *Step 11*.

      Note: You can always add access points at a later time (see the *Business Central Wireless Manager User Manual*).

    - **Add and assign one or more new access point**s. To add and assign one or more new access points (that are not yet in the application inventory), do the following:

      a. In the **Name** field, enter the factory default name (which is not shown in the field) or enter a new name for the access point.

      b. Scroll down to the **Serial Number** field and enter the precise serial number for the access point.

      Note: Without entering the correct serial number, you cannot add the access point to the network.

      c. Click the **ASSIGN** button.

      The access point is moved to the Assigned Access Points table.

      d. To add another access point, repeat *Step a* through *Step c*.

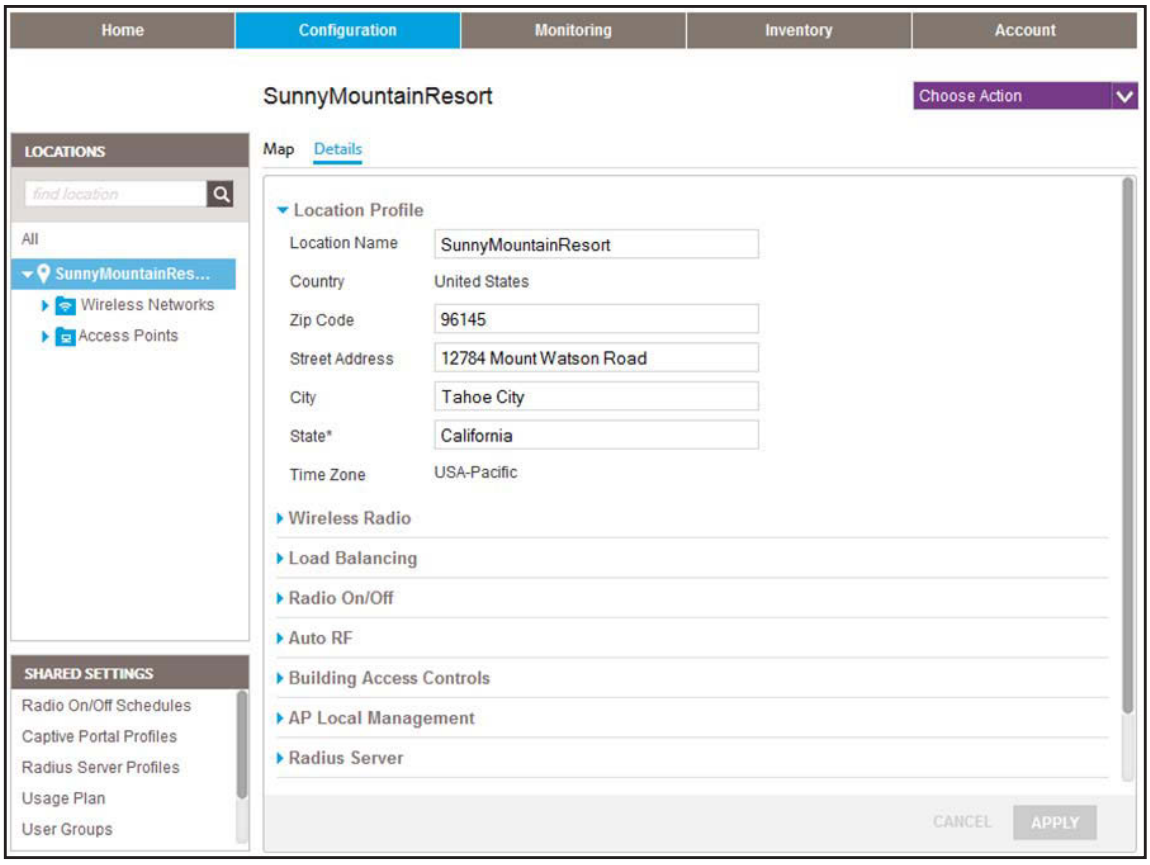
- **Assign one or more access points that are already in the application inventory**. To assign one or more access points that are already in the application inventory, do the following:

  a. In the Access Points In Inventory table, select the check boxes for the access points that you want to assign, or select the check box in the table header to assign all access points.

  b. Click the **ASSIGN** button.

  The access points are moved to the Assigned Access Points table.

11. Click the **FINISH** button.



On the left, the LOCATIONS tree displays, highlighting the location that you just added and showing the **Wireless Networks** heading and **Access Points** heading.

On the main page, the Location Profile section is expanded and displays the details of the location.

12. To verify the configuration of the WiFi network and access point (if you added any), do the following:

  a. In the LOCATIONS tree, click the **Wireless Networks** heading.

  The buildings that you just added displays.

  The WiFi network that you just added displays.

b. In the LOCATIONS tree, click the name of the WiFi network.

On the main page, the Network Name and Authentication section expands.

c. To view other details about the network, on the main page, click another section heading (for example, **Security**).

For information about how to change the network settings, see the *Business Central Wireless Manager User Manual*.

d. In the LOCATIONS tree, click the **Access Points** heading.

Building 1 displays. The application automatically added this default building when you set up the location.

e. In the LOCATIONS tree, click **Building 1**.

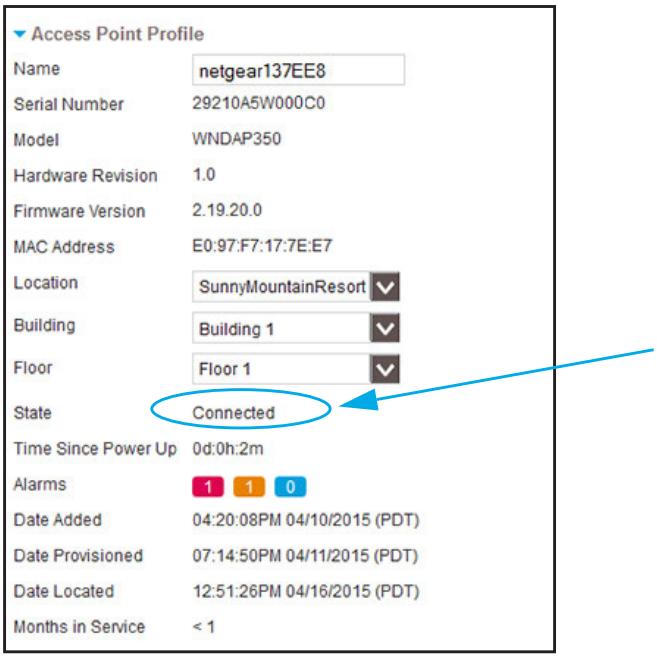
Floor 1 displays. The application automatically added this default floor when you set up the location.

f. In the LOCATIONS tree, click **Floor 1**.

The access points that you just added display.

g. To verify that a newly added access point is connected to the cloud, in the LOCATIONS tree, click the name of the access point.

The Access Point Profile section displays information about the access point.



If the access point is connected to the Internet, after you add the access point to the application, the application detects the access point, reconfigures it, and restarts it. This process takes time and the **State** field might display **Waiting for connection** for several minutes. After the process finishes, the **State** field displays **Connected**, and you can manage the access point in the cloud.

Note: Be aware that if the access point connects to the application for the first time, it might take between 5 and 10 minutes before the **State** field displays **Connected**. 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.

h. To view other details about the access point, on the main page, click another section heading (for example, **IP Setting**).

For information about how to change the access point settings, see the *Business Central Wireless Manager User Manual*.

i. To verify that another newly added access point is connected to the cloud, repeat *Step g* and *Step h*.

Alternate Method: Set Up a Basic Location

The following procedure describes how you can set up a basic location, add a single WiFi network, and add a single access point after the Get Started wizard is no longer available to you.

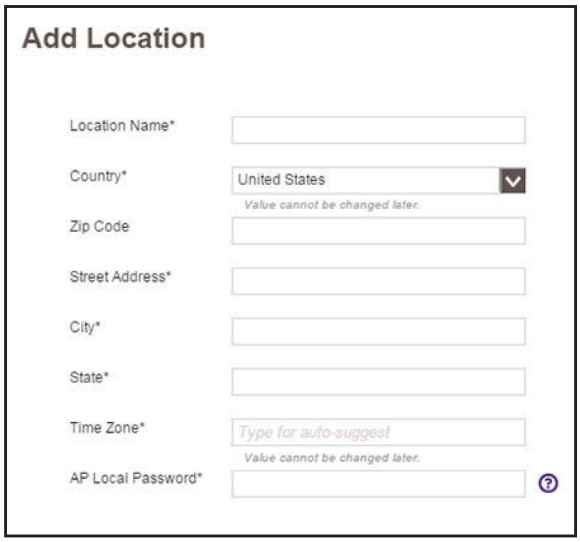
➢ **To set up a basic location, add a WiFi network, and add an access point:**

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

   The application login page displays.
3. Enter the email address and password for your BCWM account and click the **LOG IN** button.

   The Home page displays.
4. Select **Configuration**.

5. From the **Choose Action** menu, select **Add Location**.



6. Specify a location name, complete the location address fields, select a time zone, and set the location-specific password for the access points that you can assign to the location.

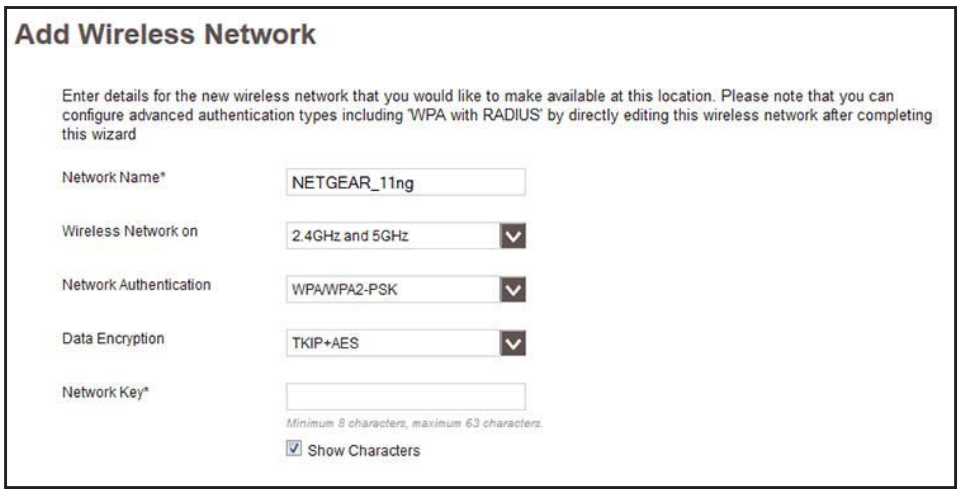
   Note: Entering correct address information allows the location to be displayed on Google Maps.

   Note: The password that you must set in this step is the password that you need when you want to access the web management interface of an individual cloud-managed access point or to access a cloud-managed access point over an SSH connection.

7. Click the **ADD THIS LOCATION** button.

   The application confirms the addition.

8. Click the **Add Wireless Network** link.



9. Configure the network settings:
   a. In the **Network Name** field, enter a WiFi network name (SSID).
   b. From the **Wireless Network on** menu, select the WiFi band or bands.

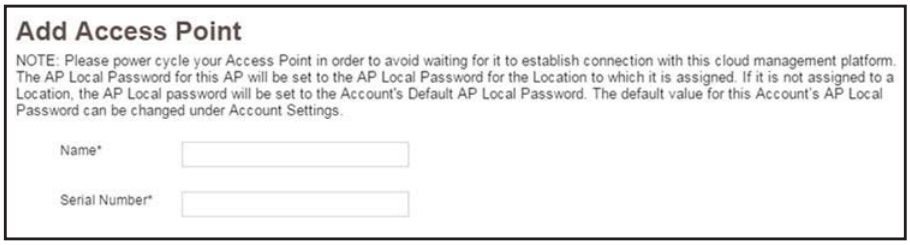
      For dual-band access points, you can select both bands to be active.

   c. From the **Network Authentication** menu, select the type of authentication.

      If you need advanced authentication, select one of the available options from the **Network Authentication** menu and complete the procedure. Then, configure the advanced authentication (see the *Business Central Wireless Manager User Manual*).

   d. From the **Data Encryption** menu, select the type of encryption.
   e. In the **Network Key** field, enter the network key that you want to use. You can enter up to 63 alphanumeric and special characters.
10. Click the **ADD THIS WIRELESS NETWORK** button.

    The application confirms the addition.
11. Click the **Add Access Point** link.



12. In the **Name** field, enter a name for the access point.
13. In the **Serial Number** field, enter the precise serial number for the access point.

    Note: Without entering the correct serial number, you cannot add the access point to the network.

14. Click the **ADD THIS ACCESS POINT** button.

    The Location Profile page displays, showing information about the new location.
15. To verify the configuration of the new location with its new WiFi network and access point, do the following:
    a. In the LOCATIONS tree on the left, click the name of the location that you just added.

       The **Wireless Networks** and **Access Points** headings display.

    b. Click the **Wireless Networks** heading.

       The WiFi network that you just added displays.

    c. In the LOCATIONS tree, click the name of the WiFi network.

       On the main page, the Network Name and Authentication section expands.

    d. To view other details about the network, on the main page, click another section heading (for example, **Security**).

For information about how to change the network settings, see the *Business Central Wireless Manager User Manual*.

e. In the LOCATIONS tree, click the **Access Points** heading.

Building 1 displays. The application automatically added this default building when you set up the location.

f. In the LOCATIONS tree, click **Building 1**.

Floor 1 displays. The application automatically added this default floor when you set up the location.

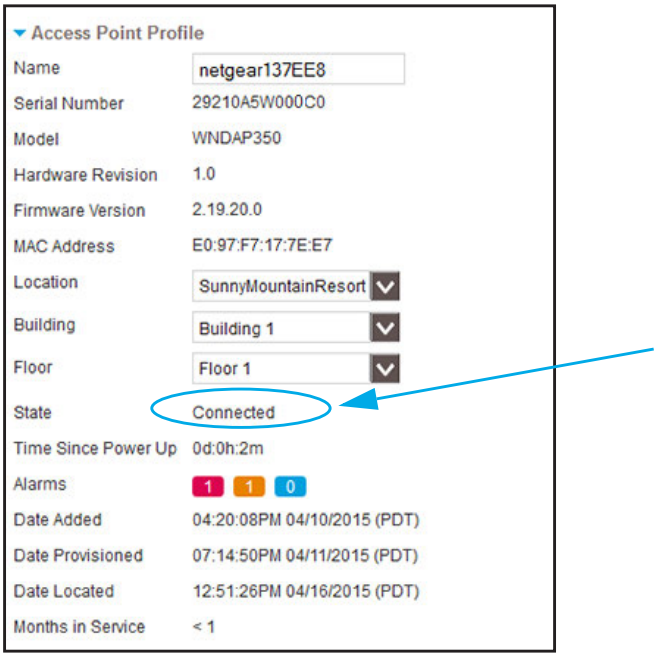
g. In the LOCATIONS tree, click **Floor 1**.

The access point that you just added displays.

h. In the LOCATIONS tree, click the name of the access point.

On the main page, the Access Point Profile section expands.

i. Verify that the access point is connected to the cloud.



If the access point is connected to the Internet, after you add the access point to the application, the application detects the access point, reconfigures it, and restarts it. This process takes time and the **State** field might display **Waiting for connection** for several minutes. After the process finishes, the **State** field displays **Connected**, and you can manage the access point in the cloud.

Note: Be aware that if the access point connects to the application for the first time, it might take between 5 and 10 minutes before the **State** field displays **Connected**. 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.

j. To view other details about the access point, on the main page, click another section heading (for example, **IP Setting**).

For information about how to change the access point settings, see the *Business Central Wireless Manager User Manual*.

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:**

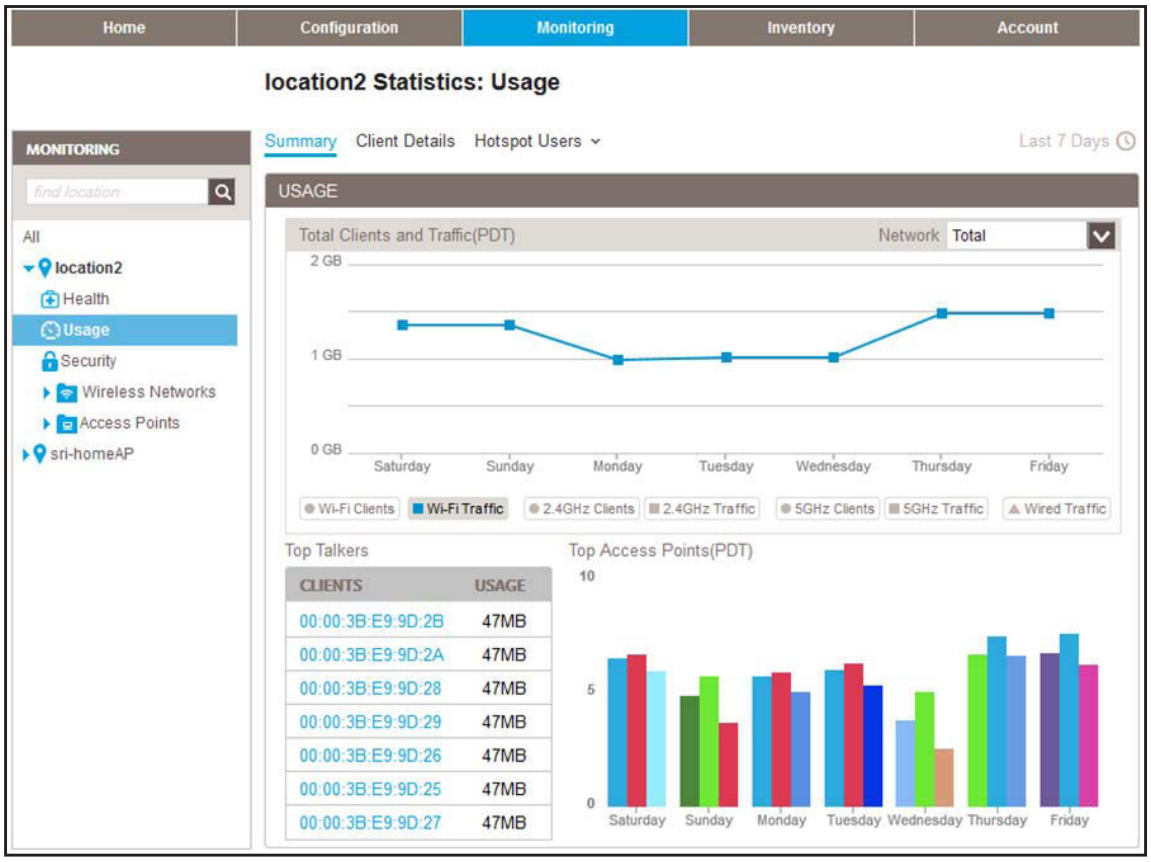
1. Open a browser on your computer.
2. In the address bar, enter **https://wireless.netgear.com**.

   The application login page displays.
3. Enter the email address and password for your BCWM account and click the **LOG IN** button.

   The Home page displays.
4. Select **Monitoring**.

   The Account Statistics page displays.
5. In the MONITORING tree on the left, click a location.

   The **Health**, **Usage**, **Security**, **Wireless Networks**, and **Access Points** icons display.
6. Click the **Usage** icon.

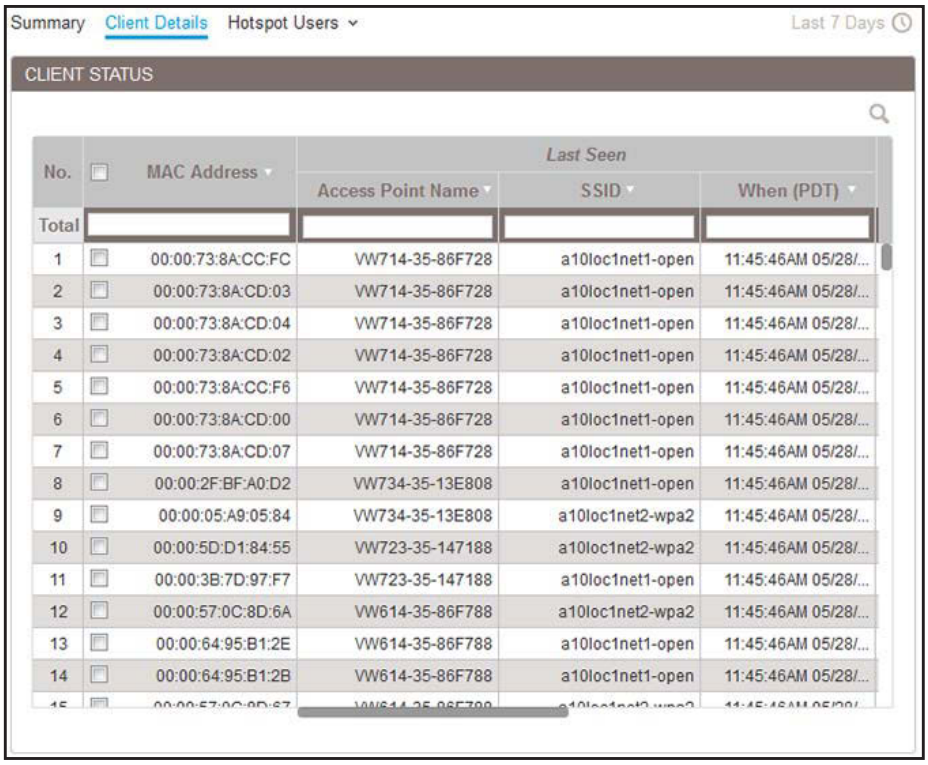


The page displays a graph for the total number of clients and amount of traffic at the location, a table with the top talkers (clients) at the location, and a graph for the top access points at the location. The previous figure shows the monitoring period as Last 7 Days and the information in the upper graph for the WiFi traffic for *all* networks at the location.

7. To select another monitoring period, click the clock icon at the right (Last 7 Days).

   You can select a monitoring period from one hour (that is, the last hour) to 30 days.

8. At the top of the page, select **Client Details**.



The page displays information about all WiFi clients that are or were connected to networks at the location. The columns in the table are self-explanatory. The previous figure shows the monitoring period as Last 7 Days.

9. To select which columns are shown in the table, do the following:
   a. To the right of the MAC Address column, right-click anywhere in the table header.

      A pop-up window displays.

   b. Select the check boxes for the columns that you want to be shown.

      The table adjusts.
10. To select another monitoring period, click the clock icon at the right (Last 7 Days).

    You can select a monitoring period from one hour (that is, the last hour) to 30 days. For this table, you can also select **Right Now** to display only the clients that are currently connected.
11. To view more table columns, move the slider at the bottom to the right.
12. To view more table rows, move the slider at the right to the bottom.
13. To sort the table, click a table header.
14. To search for a particular component and narrow the information that is shown in the table, do one of the following:
    - Type information in a field in the table header.
    - Make a selection from a menu in the table header.

- Use the search field above the table by doing the following:
  a. Click the magnifier icon in the upper right.

     The search field becomes available.

  b. Type information in the search field.
  c. Click the magnifier icon again.

     If a match is found, the results display in the table.

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