



GigaCenter Quick Reference

1. Logging into the GigaCenter.....	1
2. Change the name and password of the wireless network.....	4
3. Connect to the wireless network.....	5
4. Change the “admin” user password.....	7
5. Block a website from being accessed.....	10
6. Restrict access to the Internet by time-of-day.....	12
7. Change the firewall security settings.....	13
8. Add Port Forwarding rules.....	15
9. Turn on “Remote Access”	16
10. Extending Wireless Coverage.....	18



1. Logging in to the Calix GigaCenter

- a. Connect an Ethernet cable between your computer and the Ethernet “1” port on your Gigacenter.
- b. From your browser, access the GigaCenter at <http://192.168.1.1>
- c. The following window should appear. If you receive a security warning, click on “Advanced” and choose to access the GigaCenter.
- d. Login using the user [admin] and the password listed on the Default Settings label on your GigaCenter, then click the “Login” button.

The image shows a web browser window displaying the login page for a "Residential Gateway". The title "Residential Gateway" is in a dark blue header. Below it, there are two input fields: "User Name:" followed by a text box containing a vertical cursor, and "Password:" followed by a text box. Below these fields is a blue "Login" button. The background of the page has a faint, stylized image of a person's head in profile.



e. The GigaCenter dashboard should now appear as follows:



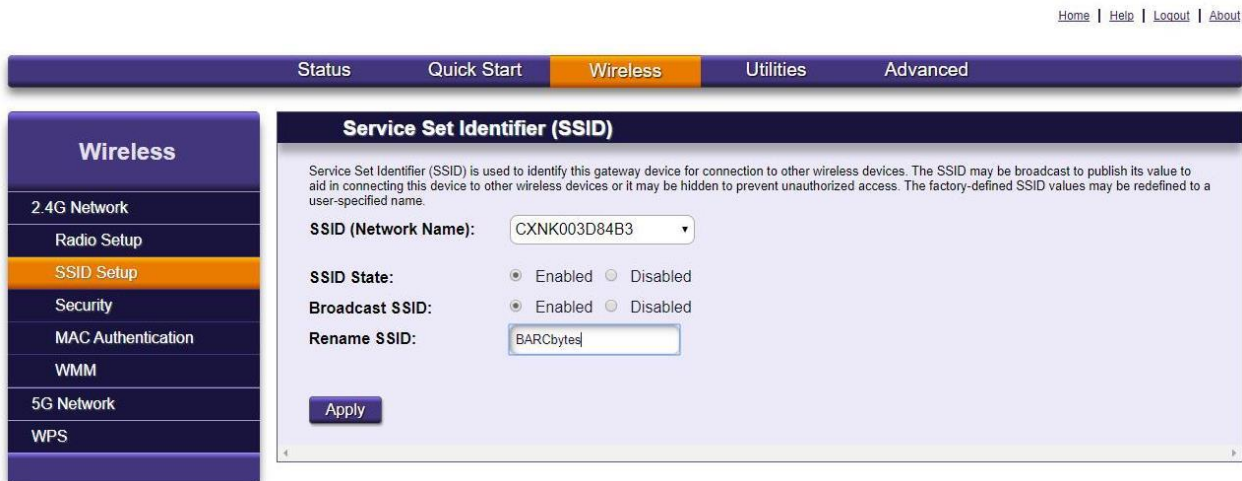


2. Change the name and password of the wireless network

- a. From the GigaConnect dashboard, click on the “Wireless” icon:




- b. From the “Wireless” column on the left under “2.4G Network,” click “SSID Setup.”



- c. Change the default “SSID (Network Name)” by typing the name you desire into the “Rename SSID” field, then click the “Apply” button.
- d. To change the wireless password, from the “Wireless” column on the left under “2.4G Network,” click “Security.”
- e. Click the circle adjacent to “Use Custom Security Key,” type in the desired new security key, and click “Apply.”
- f. Repeat steps “b” through “e” under the “5G Network” heading in the left column.



3. Connect to the wireless network

- a. Click on the wireless icon  on the right side of the task bar at the bottom of your screen.
- b. Click on the name of your wireless network.





- c. Ensure that “Connect automatically” is checked, then click “Connect”
- d. Press the “WPS” button on the side of the Calix GigaCenter. The connection may take as much as two minutes.

If you are unable to connect to the Gigacenter by pressing the “WPS” button, manually key in your password on the device you are trying to join to the network.

The steps listed above apply to a Windows OS. If you are trying to add a mobile phone or use a different OS on your computer (such as Apple or Linux) consult your vendor documentation on how to join that device to a wireless network.

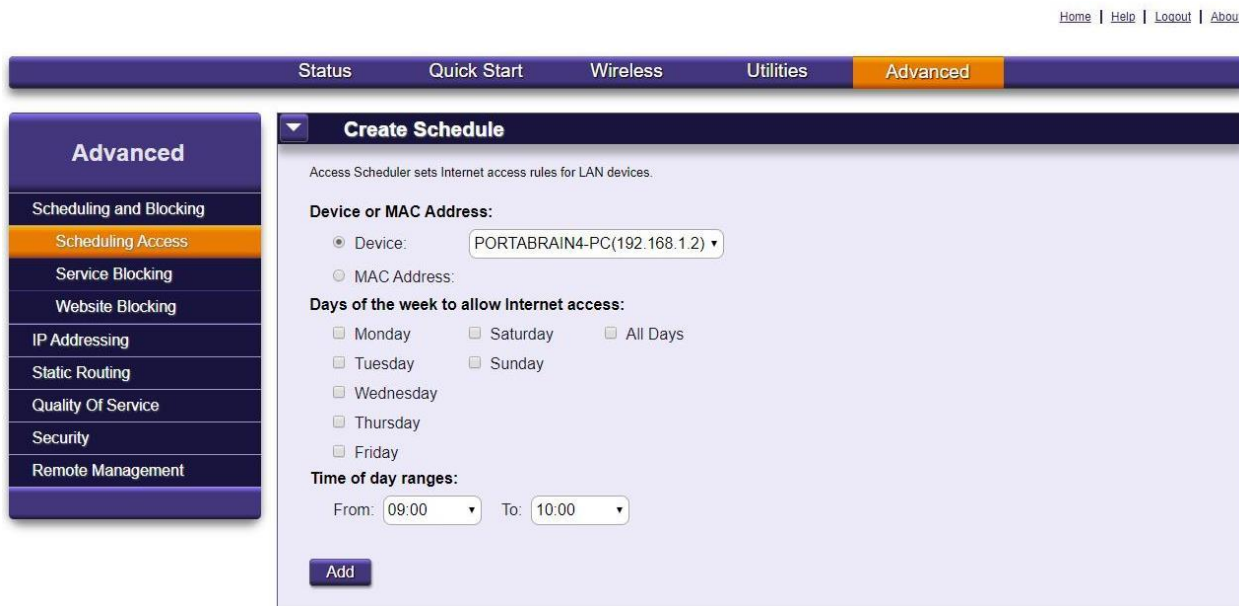


4. Change the “admin” user password

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



Or



- b. Click “Security” in the left column of your screen.
- c. Click the “Show” checkbox, then type the new password [“newpass” in this example].
- d. Click the Apply button at the bottom of the screen.



Status Quick Start Wireless Utilities **Advanced**

Advanced

- Scheduling and Blocking
- IP Addressing
- Static Routing
- Quality Of Service
- Security
- Administrator Credentials**
- Application Forwarding
- Port Forwarding
- Firewall
- DMZ Hosting
- UPnP
- Remote Management

Administrator Credentials

Administrator credentials prevent outsiders from accessing the gateway device's firmware settings. After creating a username and password, you will need to enter them before you can access the gateway device's configuration settings.

Credentials: ☒ Required ☐ Not Required

Administrator:

Username:

Password: ☒ Show

e. Click the “Ok” button in the “Residential Gateway” box.

Advanced - Security - Admin

192.168.1.1/html/advanced/security/advanced_security_admin.html

Home | Help | Logout | About

Status Quick Start Wireless Utilities **Advanced**

Advanced

- Scheduling and Blocking
- IP Addressing
- Static Routing
- Quality Of Service
- Security
- Administrator Credentials**
- Application Forwarding
- Port Forwarding
- Firewall
- DMZ Hosting
- UPnP
- Remote Management

Administrator Credentials

Administrator credentials prevent outsiders from accessing the gateway device's firmware settings. After creating a username and password, you will need to enter them before you can access the gateway device's configuration settings.

Credentials: ☒ Required ☐ Not Required

Administrator:

Username:

Password: ☒ Show

Residential Gateway

Re-login is needed after form applied.

f. Login with user “admin” and the new password for “Password.”



**Residential
Gateway**

User Name:

admin

Password:

Login

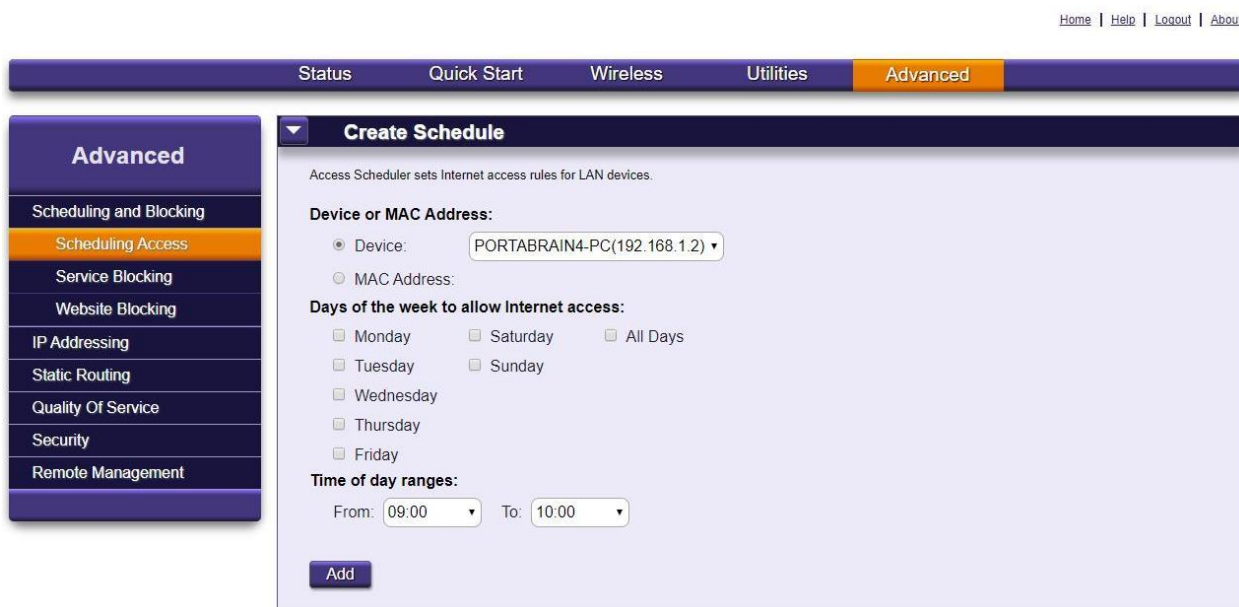


5. Block a website from being accessed

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



Or



- b. Click “Website Blocking” in the left column.



Status Quick Start Wireless Utilities Advanced

Advanced

Scheduling and Blocking

Scheduling Access

Service Blocking

Website Blocking

IP Addressing

Static Routing

Quality Of Service

Security

Remote Management

Website Blocking

Website blocking provides the ability to block specific websites per device or IP address.

Create New Association:

Website Address:

Note: Website Address can be written as "website.com", "www.website.com" or "http://www.website.com"

Associate Website With:

☒ Device

☐ IP Address

Apply
Cancel

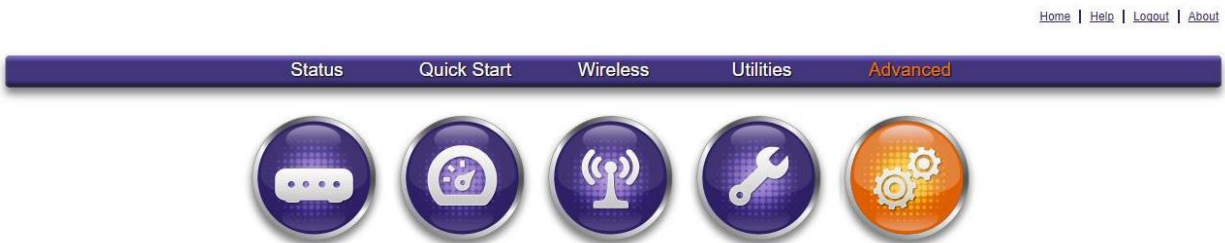
Device Name	IP Address	Website Blocked	Remove
No Entries Defined			

- c. Type in a website name, e.g. “badstuff.com” and click the “Apply button.

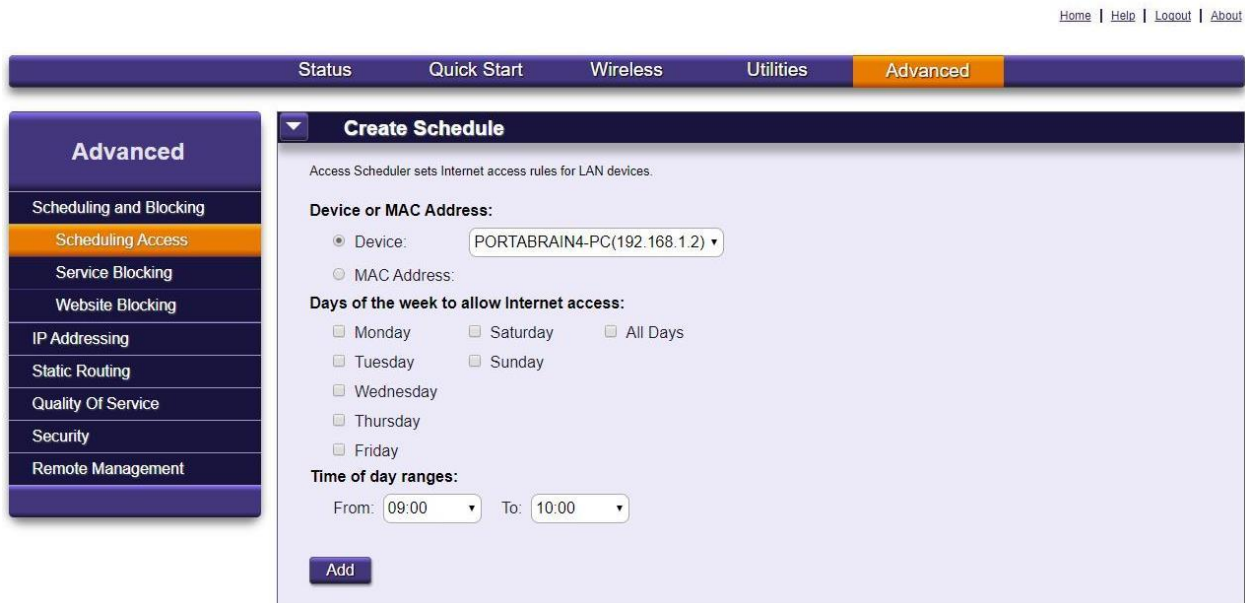


6. Restrict access to the Internet by time-of-day

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



Or



- b. From the “Create Schedule” screen, “Device” pull-down menu, choose the name of the computer you desire to restrict. Choose the days of the week to allow access, choose the “Time of day range, and click the “Add” button.

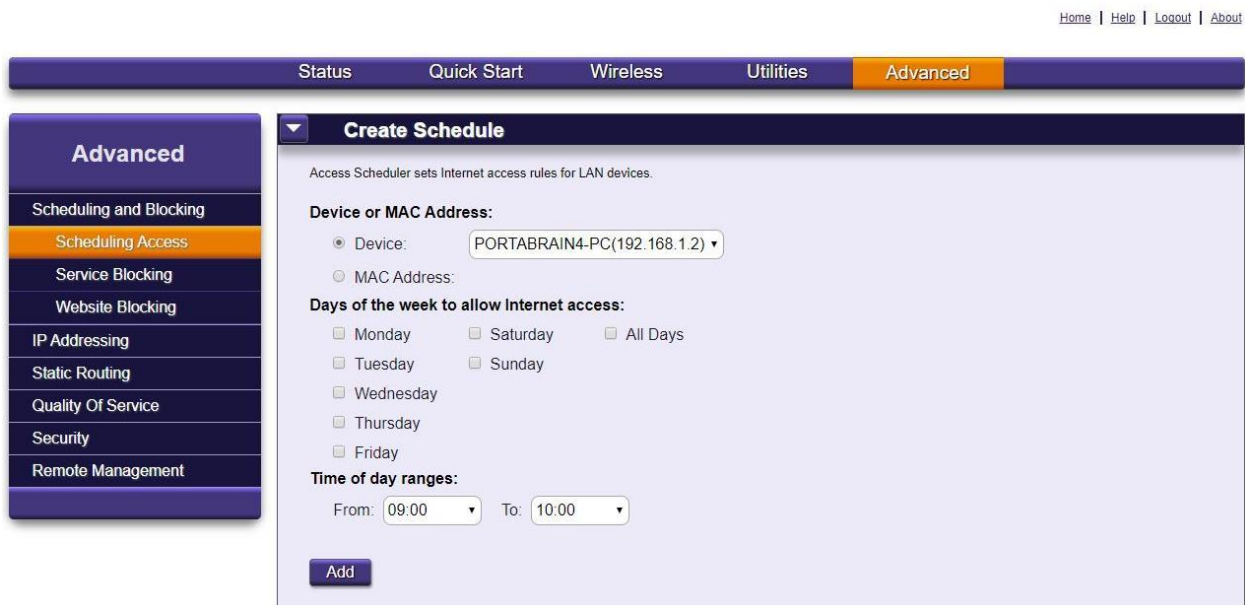


7. Change the firewall security settings

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



Or



- b. In the left column, click “Security, then click “Firewall.”



Status	Quick Start	Wireless	Utilities	Advanced
<div> <div> Advanced </div> <div> Scheduling and Blocking IP Addressing Static Routing Quality Of Service Security Administrator Credentials Application Forwarding Port Forwarding Firewall DMZ Hosting UPnP Remote Management </div> </div> <div> <div> Firewall </div> <div> <p>Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.</p> <p>Security Level:</p> <p> <input type="radio"/> Security Off No filtering of traffic in or traffic out. <input type="radio"/> Low Security Blocking of pre-defined traffic in per the Blocked Services settings. No blocking of traffic out. <input type="radio"/> Medium Security Blocking of pre-defined traffic in per the Blocked Services settings. No blocking of traffic out. (More limitation than first level.) <input checked="" type="radio"/> High Security Blocking of pre-defined traffic in per Blocked Services settings. Blocking of pre-defined traffic out per Blocked Services settings including DNS. </p> <p>Stealth Mode: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p> <p>When Stealth Mode is enabled, the device will not respond to all unsolicited WAN traffic including pings.</p> <p>Apply</p> </div> </div> <div> <div> Blocked Services </div> <div> </div> </div>				

c. Choose the desired “Security Level,” then click “Apply.”

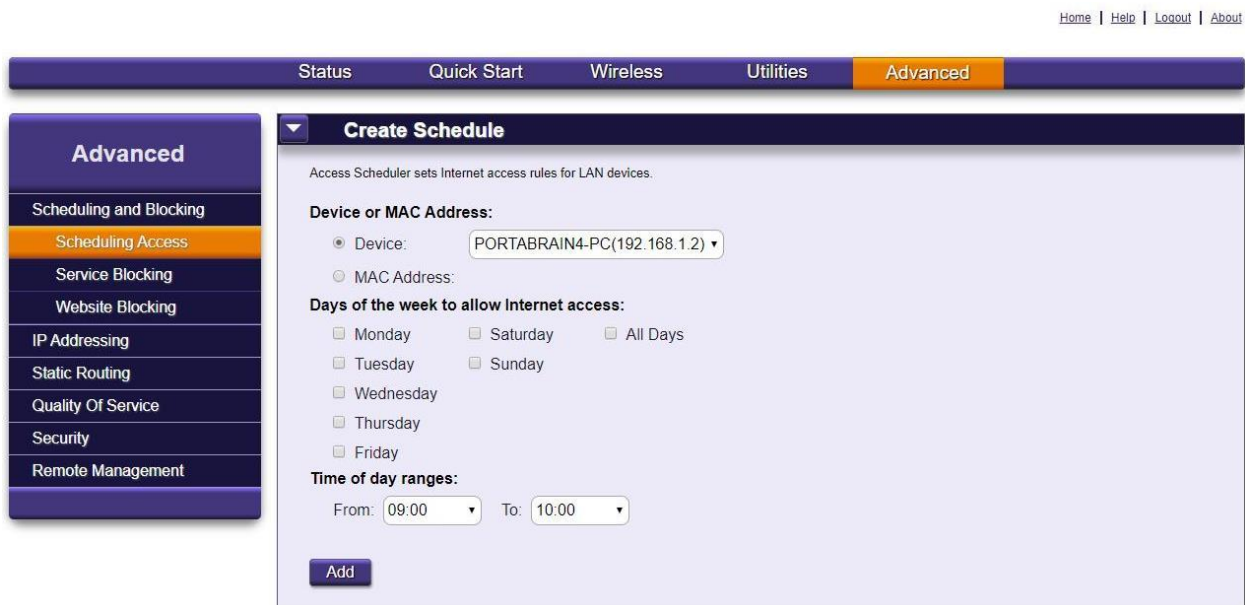


8. Add Port Forwarding rules

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



Or



- b. In the left column, click “Security, then click “Port Forwarding.”
- c. Click “Add,” key in the port forwarding rule parameters, then click “Apply.”
- d. Add additional port forwarding rules as desired.

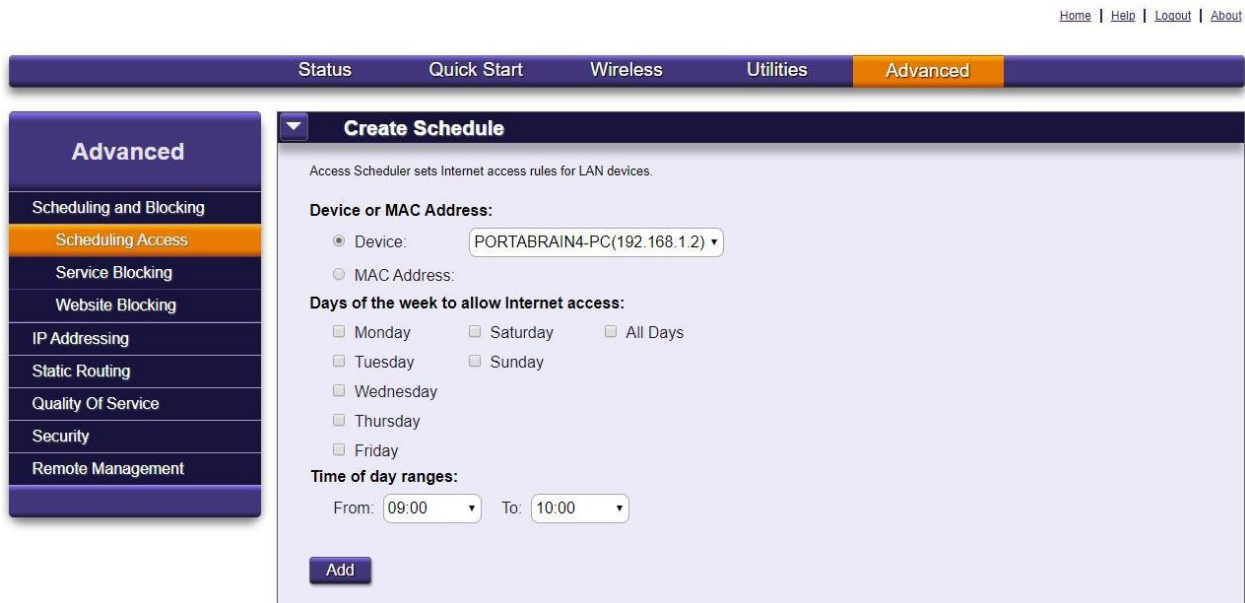


9. Turn on “Remote Access”

- a. Click the “Advanced” icon from the dashboard, or the “Advanced” button on the blue line near the top of the screen.



or



- b. In the left column, click “Security, then click “Remote Management.”
- c. Click “Enabled” for “Remote GUI State.”
- d. Determine your “WAN IP Address” by, e.g. accessing a site such as <http://www.dslreports.com/whatismyip>, type in that address in the “WAN IP Address” field, type in the port you will use for remote access, then click “Apply.”



- e. The WAN IP address is valid for up to three days (72 hours) when the GigaCenter is powered off, but will need to be re-determined and reentered if the previous WAN IP address has expired. The GigaCenter otherwise keeps the same IP address.



10. Extending wireless coverage using the Calix 804Mesh Dual Wi-Fi device

- a. Connect the power supply and plug in the Calix 804Mesh Dual Wi-Fi device in the part of the building you desire to extend wi-fi service. Once the power light and two of the Wi-Fi Backhaul lights are solid green (see sections “i” and “ii” below), press the “WPS” button on the back of the 804Mesh Dual Wi-Fi device until the four “WiFi Backhaul” lights are flashing green.
 - i. The optimum distance for the Calix 804E away from the Calix 844E or 844G will be indicated by two green lights only in the “WiFi Backhaul” lights. More lights than two indicate that the Calix 804Mesh Dual Wi-Fi device is too close to the Calix 844E or 844G. Less than two lights in the WiFi Backhaul lights indicate that the Calix 804Mesh Dual Wi-Fi device is too far away from the Calix 844E or 844G.
 - ii. Optimum distance from the Calix 844E or 844G to the Calix 804Mesh Dual Wi-Fi device is affected by the number and type of walls and other physical obstacles between the two devices.
- b. After pressing the “WPS” button on the back of the 804Mesh Dual Wi-Fi device, go to the operating ONT and ensure the green light adjacent to the “WPS” button is solid green. Press the “WPS” button on the ONT until the light flashes green.
- c. Wait until the WPS light is solid green.
- d. Go to the Calix 804 Mesh Dual Wi-Fi device. Examine the “WiFi Backhaul” lights to ensure that the conditions explained in sections a.i and a.ii above are met. Adjust the location of the Calix 804Mesh Dual Wi-Fi if the “WiFi Backhaul” lights indicate that you are too close or too far from the Calix 844E or 844G.