



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

MORE BYTE BARC connects

- 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.

Residential Gateway		
	User Name:	
	Password:	
	Login	



e. The GigaCenter dashboard should now appear as follows:

Home | Help | Loqout | About





2. Change the name and password of the wireless network

a. From the GigaConnect dashboard, click on the "Wireless" icon:

Home Help Logout About



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

Home | Help | Logout | About

	Status	Quick Start	Wireless	Utilities	Advanced			
Wireless	Servi	ce Set Identifi	er (SSID)					
Wireless	Service Set Identifier (SSID) is used to identify this gateway device for connection to other wireless devices. The SSID may be broadcast to publish its value to aid in connection this device to other wireless devices or it may be bidden to prevent unauthorized access. The factory defined SSID values may be redefined to							
2.4G Network	user-specified n	iame.	,		,			
Radio Setup	SSID (Netwo	ork Name):	XNK003D84B3	<u> </u>				
SSID Setup	SSID State:	۲	Enabled 🔍 Disab	led				
Security	Broadcast	SSID:	Enabled O Disab	led				
MAC Authentication	Rename SS	ID:	ARCbytes					
WMM								
5G Network	Apply							
WPS								
	4							

- 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.

.สป้	Mobile Turned	e Broadband (1 off	Connection	
(h.	Secure	d		
<i>M</i>	Secure	d		
(k.	Secure	d		
(k	BARCB Secure	ytes d	1	
(k	Secure	d		
Netw	vork set	tings		
<i>M</i> . Wi-Fi		다 Airplane mode	.utl Cellular	('j') Mobile hotspot







- 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.

						Home Help Lodout About
	Status	Quick Start	Wireless	Utilities	Advanced	
			Y	Ø	ø	
	Status	Quick Start	Wireless	Utilities	Advanced	Home Help Locout Abd
	_					
Advanced	Access Schedu	e Schedule	o for LAN devices.			
Scheduling and Blocking	Device or M	AC Address:				
Scheduling Access	Device	PORTABRA	NN4-PC(192.168.1.2)	•		
Service Blocking	MAC A	Address:				
Website Blocking	Days of the	week to allow Interne	et access:			
IP Addressing	🔲 Monda	ay 📃 Saturday	All Days			
Static Routing	🔲 Tuesd	ay 🔲 Sunday				
Quality Of Service	Wedne	esday				
Security	Thurso	day				
Remote Management	Time of day	ranges:				
	From: 0	9:00 • To: 10	• 00			
	Add					

- 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.



					71373115533			
	Admini	strator Creden	tials					
Auvanceu	Administrator crede enter them before	entials prevent outsiders f you can access the gatew	rom accessing the gateway /ay device's configuration se	device's firmware setting attings.	s. After creating a usernam	e and password, you will need to		
Scheduling and Blocking								
IP Addressing	Credentials:	Required	Not Required					
Static Routing	Administrator Credentials Administrator credentials prevent outsiders from acce enter them before you can access the gateway device Credentials: Required Not Re Administrator: Username: admin Password: newpass Apply							
IP Addressing Static Routing Quality Of Service Security Administrator Credentials	Autimistrator							
Security	Username:	admin						
Administrator Credentials	Password:	newpass	Shc	W				
Application Forwarding								
Port Forwarding	Apply							
Firewall								
DMZ Hosting	<u></u>							
UPnP								

e. Click the "Ok" button in the "Residential Gateway" box.

Remote Management

C 192.168.1.1/html/advanced/se	ecurity/advanced_security_a	admin.html				☆
For quick access, place your bookmarks here	e on the bookmarks bar. Impor	t bookmarks now				
						Home Help Logout About
	Status	Quick Start	Wireless	Utilities	Advanced	
	Adminis	trator Creden	tials			
Advanced	Administrator creder	nt			r creating a usernam	e and password, you will need to
Scheduling and Blocking	enter them before yo	R	esidential Ga	iteway		
IP Addressing	Credentials:	Re-login is ne	eded after form applie	he		
Static Routing		1 to login is no	succe and round applie			
Quality Of Service	Administrator:	-				
Security	Username:					
Administrator Credentials	Password:	(
Application Forwarding				Ok Cancel		
Port Forwarding	Apply					
Firewall						
DMZ Hosting	<u>.</u>					P.
LID D						

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

		MORE BY	
DA	PC		
DA			
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.



b. Click "Website Blocking" in the left column.

	MORE BYTE
	BARC connects Vilities Advanced
Advanced	Website Blocking Website blocking provides the ability to block specific websites per device or IP address.
Scheduling and Blocking Scheduling Access	Create New Association:
Service Blocking Website Blocking	Website Address: Note: Website Address can be written as "website.com", "www.website.com" or "http://www.website.com"
IP Addressing	Associate Website With:
Static Routing	O Device All Devices
Quality Of Service	IP Address
Security	
Remote Management	Apply Cancel
	Device Name IP Address Website Blocked Remove No Entries Defined
	4

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.



 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.



b. In the left column, click "Security, then click "Firewall."



Home | Help | Logout | About



	Status Qu	ick Start	Wireless	Utilities	Advanced		
	_						_
Advanced	Firewall						
Advanced	Activating the firewall is op	otional. When the fir	ewall is activated, security	is enhanced, but some n	etwork functionality will be	lost.	
Scheduling and Blocking	Security Level:						
IP Addressing	Security Off	No filtering o	f traffic in or traffic out.				
Static Routing	Low Security	Blocking of p	re-defined traffic in per	the Blocked Services	settings. No blocking of	traffic out.	
Quality Of Service	,	Disaking of p	re defined traffic in per	the Blacked Capitana	ettings. No blocking of	traffic out /Mars limitation than	
Security	Medium Securit	first level.)	re-defined traffic in per	the blocked Services	settings. No blocking of	traine out.(More limitation than	
Administrator Credentials	 High Security 	Blocking of p Services sett	re-defined traffic in per ings including DNS.	Blocked Services setti	ngs. Blocking of pre-def	ined traffic out per Blocked	
Application Forwarding							
Port Forwarding	Stealth Mode:	Enabled	Disabled				
Firewall	When Stealth Mode is	s enabled, the devic	e will not respond to all un	soliciated WAN traffic inc	luding pings.		
DMZ Hosting	Apply						
UPnP							
Remote Management	1						•
	Blocked Se	rvices					

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.



- 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.



- 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
 <u>http://www.dslreports.com/whatismyip</u>, 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 Caliz 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.
 - 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 is 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.