Security Best Practices

for a WebCTRL® v8.0 system

1150 Roberts Boulevard, Kennesaw, Georgia 30144
770-429-3000 Fax 770-429-3001 | www.automatedlogic.com

AutomatedLogic

 Verify that you have the most current version of this document. Go to **https://accounts.automatedlogic.com**, then select **Support** > **Download** > **Documents** > **WebCTRL security**. Important changes are listed in **Document revision history** at the end of this document.

Contents

Security best practices **1**
Network separation 1
Internet connectivity scenarios 2
Network firewall 6
BACnet firewall 7
Users 13
WebCTRL® server 14
Database server 14
Appendix A: Glossary **15**
Appendix B: Security checklist **16**
Document revision history **19**

Security best practices

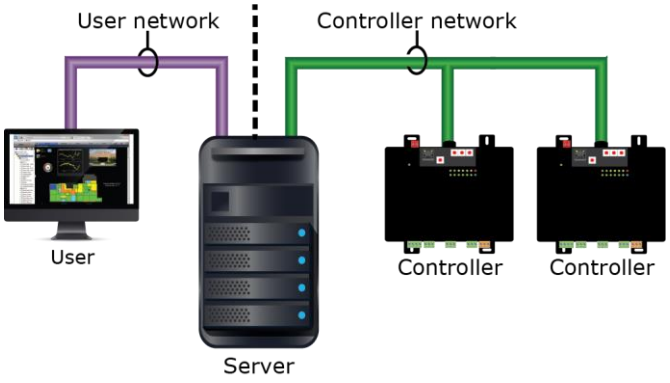
Automated Logic® takes the security of our systems very seriously and you play the biggest part in this by installing and configuring systems in a secure manner. We encourage you to establish security policies for your own company networks and all the systems you install and service.

Follow the best practices in this document when deploying WebCTRL® building automation systems.

Use the Security Checklist in Appendix B to track important security steps when designing, installing and commissioning WebCTRL® systems.

Network separation

Standard BACnet is an intentionally open system that makes it easy to discover and control any device on its network. Because of this, you should design your system to segregate users from the controller network by having two separate networks. For example, if the users are on a company's enterprise LAN, you would not want controllers on the LAN so that they are easy targets for misuse by anyone with access. Some of the biggest risks come from insiders such as the curious tinkerer, a student on an education system's network, or a disgruntled employee.



You can physically separate the user network and the BACnet network without any IP routing between them, or you can logically separate them at a switch using a Virtual Local Area Network (VLAN).

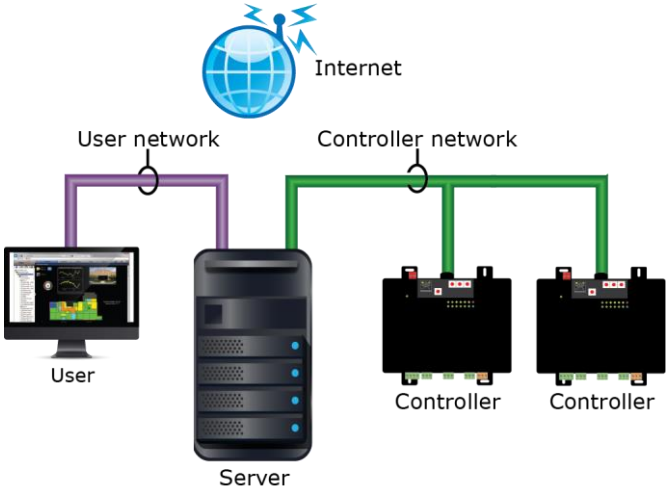
If you have dual NICs (Network Interface Cards), the WebCTRL® server must have a different IP address for each network:

- User network - Configure this IP address and subnet mask in SiteBuilder on the **Configure** > **Preferences** > **Web Server** tab.
- BACnet network - Configure this IP address and subnet mask in the WebCTRL® interface on the **Driver Properties** > **Connections** page > **Configure** tab.

Internet connectivity scenarios

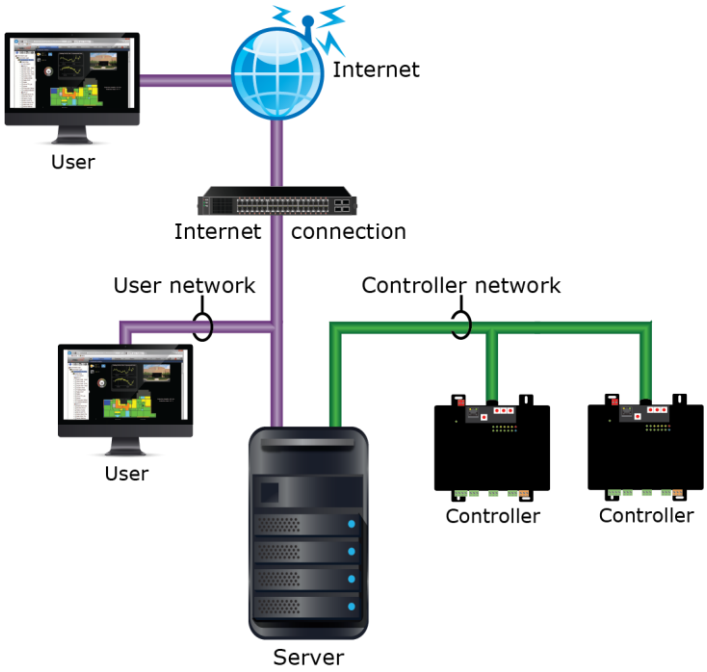
The WebCTRL® system's connection to the Internet may vary greatly based on the client's needs and IT capabilities. The following possible network scenarios are listed in order of DECREASING security.

Scenario A: Isolated Network - Low risk



Do not permanently expose the WebCTRL® server or the BACnet network to the Internet. You can, however, allow users to access the WebCTRL® server through a secure VPN connection. If a NAT router or firewall is present on the LAN for other purposes, it should not have any ports forwarded to the WebCTRL® server or any controllers.

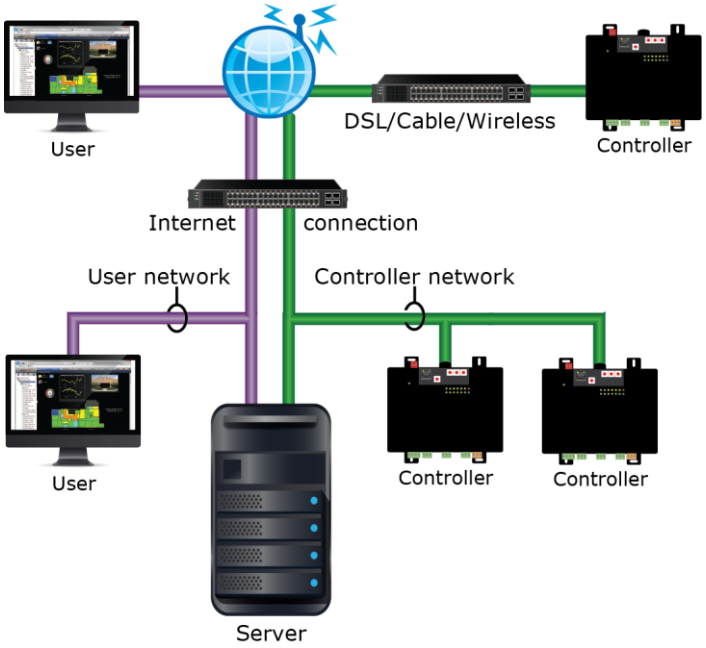
Scenario B: Public Users - Medium risk



It is acceptable to permanently expose the WebCTRL® server on the Internet as long as:

- The BACnet network is not exposed.
- The NAT/Firewall device exposing the WebCTRL® system exposes only TCP ports 80 and 443 on the WebCTRL® server.
- BACnet traffic on UDP port 47808 is not exposed.

Scenario C: Public Users with Distributed BACnet - High risk



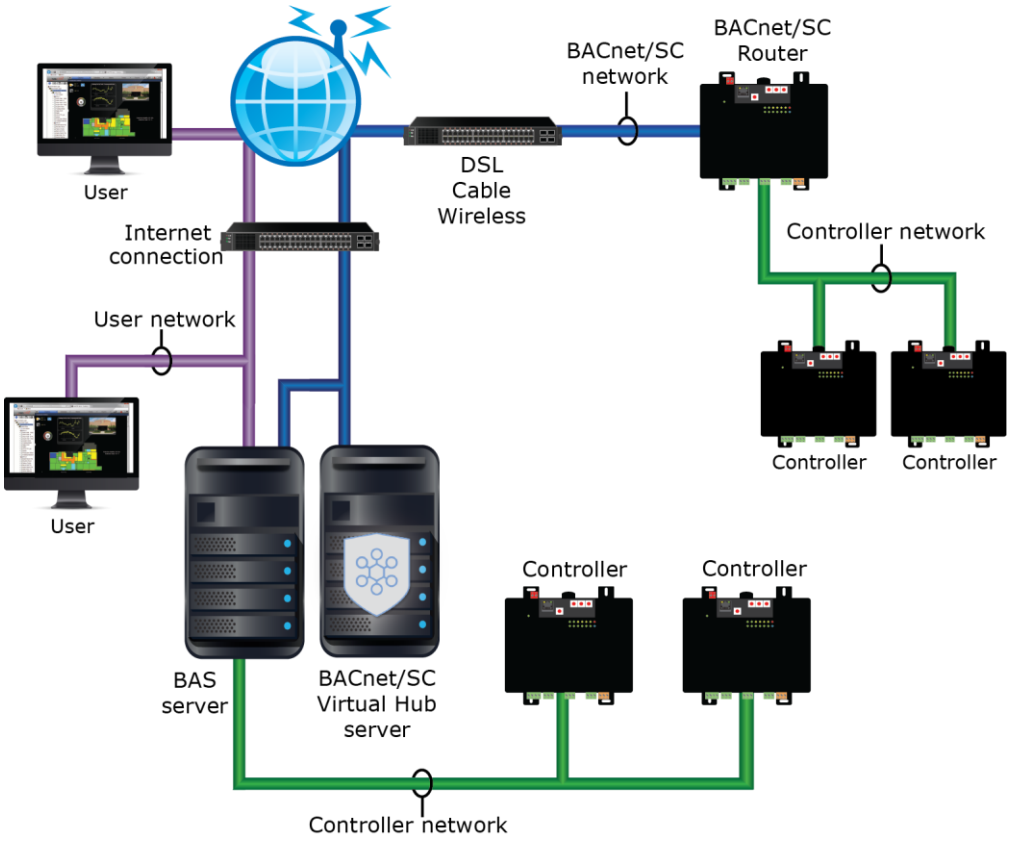
In this configuration, both users and BACnet controllers use a public network/Internet. Carefully plan this configuration to maximize security.

If the WebCTRL® server must connect to multiple sites over the Internet, connect them using a VPN to form a Wide Area Network that is secure (changing this to Scenario A).

If this is not possible, use the *BACnet Firewall feature* (page 7) in Ethernet-capable controllers, or protect controllers with a whitelist that your IT department can configure in each Internet connection device where the network connects to the Internet. The whitelist allows communication with your WebCTRL® system only from devices whose public IP addresses are in the list. Often, the only address controllers need to talk to is the WebCTRL® server. The WebCTRL® server firewall's whitelist will have to include the public address of all remote IP controllers.

DO NOT connect BACnet controllers to the Internet without at least whitelist protection! If you do, they could easily be discovered and modified by anyone on the Internet. If a BACnet router is connected to the Internet without protection, then the entire network connected to it is accessible.

Scenario D: Public Users with Distributed BACnet/SC - Low risk



BACnet Secure Connect, or BACnet/SC, is an industry standard way of securing BACnet communications over the internet without the need for VPNs. A BACnet/SC network consists of multiple nodes connecting through a central hub. This hub can be located on premises or hosted on the Internet. The figure above depicts the BACnet/SC Hub installed on premises.

Network firewall

Limit the ports opened through any firewall or NAT port forwarding to the minimum ports required. The WebCTRL® system uses the following ports:

Port	Transfer	Protocol/User	Use
80 (default)	TCP	http (Web server)	Client/Server
443 (default)	TCP	https (Web server)	Client/Server
443 (default)	TCP	wss (secure WebSocket for BACnet/SC)	Client
47806 (default)	TCP	Alarm Notification Client	Client/Server
47808	UDP	BACnet/IP	Server/Gateway
47808	TCP	Diagnostic Telnet *	Client/Server
47806	UDP	Legacy CMnet	Server/Gateway

* This functionality is off by default. You can start it using the `telnetd` console command.

Scenarios B or C in the previous section require TCP ports 80 and 443 to be exposed to the Internet for user access.

Scenario C also requires UDP port 47808 to be exposed for both the server and the controller's firewall. If you do this, you MUST use a whitelist to limit connectivity.

Scenario D may require configuration of an outgoing port for BACnet/SC traffic and/or an incoming port protecting a BACnet/SC Hub.

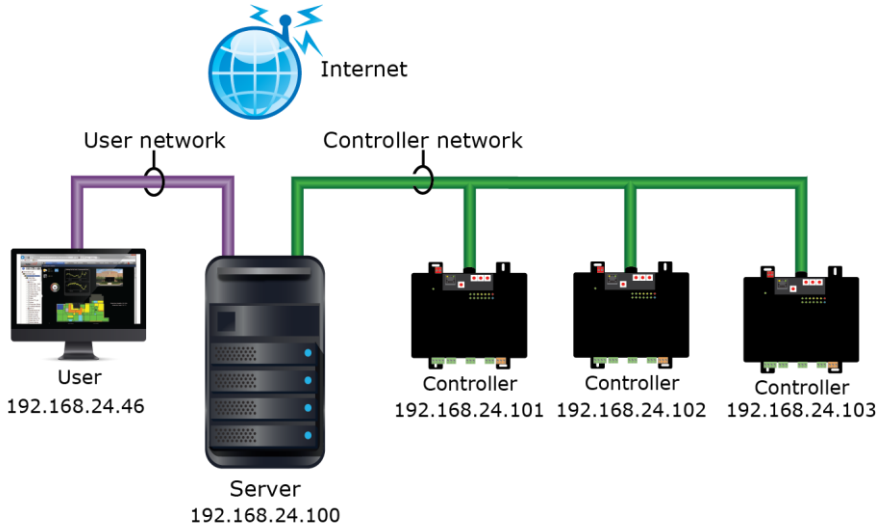
BACnet firewall

The v6-02 drivers for Automated Logic® controllers with Ethernet capability have a BACnet firewall feature that allows you to restrict BACnet/IP communication with the controller to all private IP addresses and/or to a whitelist of IP addresses that you define. This feature provides another layer of security for your system.

The following are examples of use cases for the BACnet firewall and instructions for setting it up.

Case 1: Isolated network

While an isolated network is secure from threats on the Internet, other users or devices on the local network can potentially interfere with controllers.



In this example, each controller's BACnet firewall should allow BACnet communication from the WebCTRL® server's IP address and the controller's IP addresses. The user at 192.168.24.46 should not be allowed BACnet communication with the controllers.

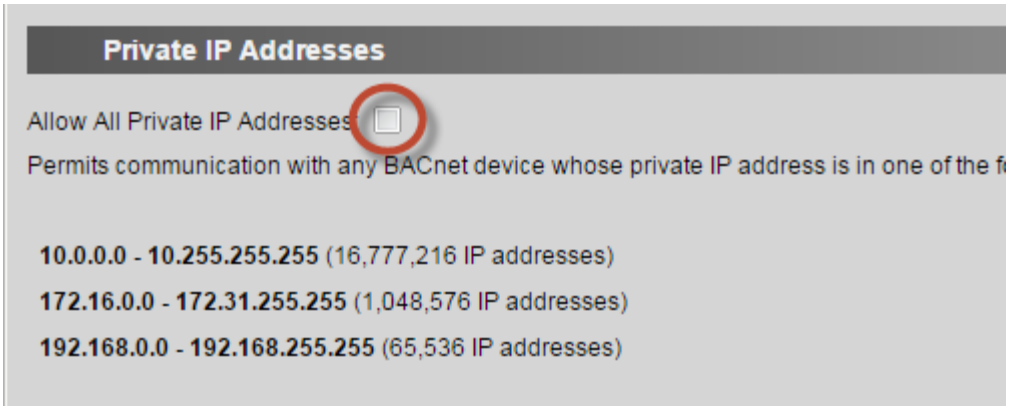
The server and controllers addresses fall within the private IP address range of 192.168.0.0 to 192.168.255.255, but restricting BACnet communication to all private IP addresses is not sufficient since that would allow communication from the user. So a whitelist must be created in the BACnet firewall.

To set up the BACnet firewall:

1 In the WebCTRL® interface, go to each controller's **Driver** > **BACnet Firewall** > **Properties** page.

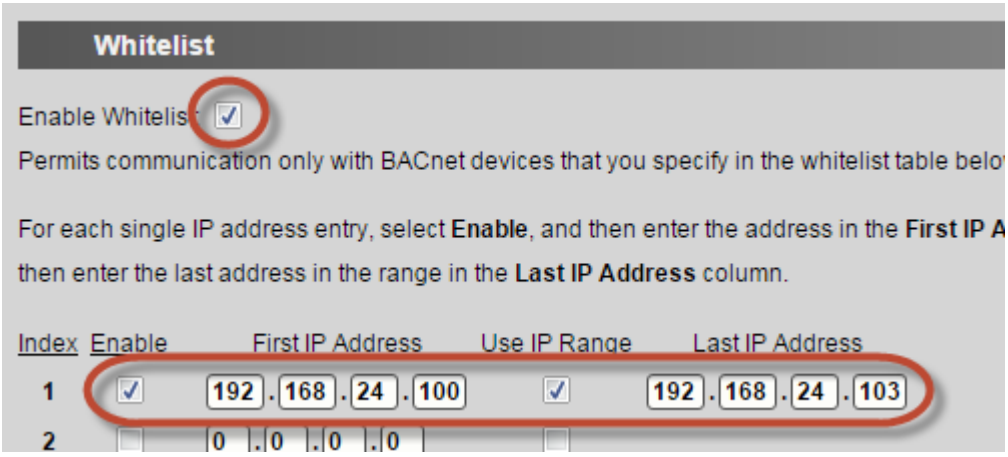
2 Check **Enable BACnet firewall**.

3 Uncheck **Allow All Private IP Addresses**.



4 Check **Enable Whitelist**.

5 On the first row, check **Enable**, check **Use IP Range**, and then enter the address range 192.168.24.100 through 192.168.24.103.



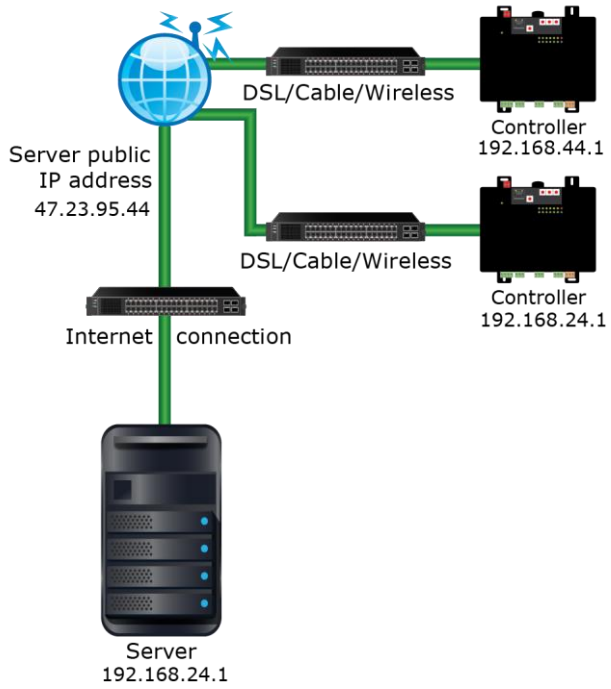
6 Click **Accept**.

7 Wait for the page to update, and then check **Confirm firewall settings**.

NOTE In this example, the server and controllers IP addresses are sequential so the whitelist could have an address range. If you anticipate future controller expansion, reserve extra sequential addresses so that you can simply expand the range in the BACnet firewall settings. If the IP addresses are not sequential, you must enter each IP address on a separate line and check **Enable**.

Case 2: Individual controllers exposed to the Internet

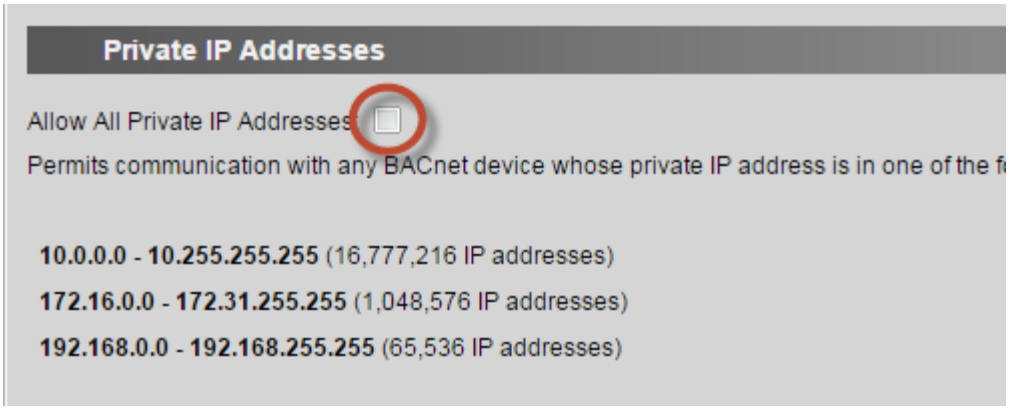
Controllers that are accessible on the Internet (for example, behind a DSL, cable, or wireless device) may not be protected by a network firewall or whitelist. This may be due to the network firewall's lack of capability or difficulty in setting it up.



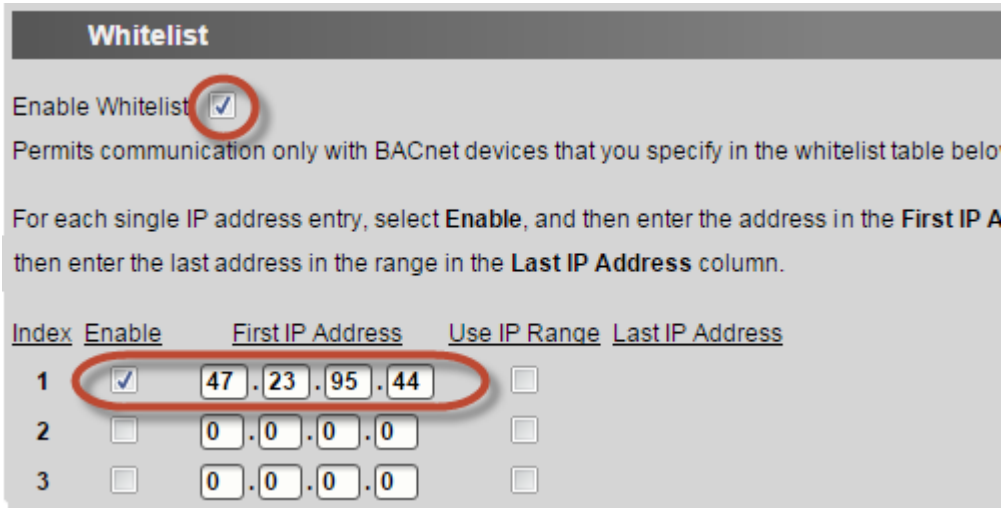
In this example, each controller needs to communicate with only the WebCTRL® server so their BACnet firewall's whitelist should have only the server's public IP address. The controllers do not need to communicate with each other.

To set up the BACnet firewall:

1. In the WebCTRL® interface, go to each controller's **Driver** > **BACnet Firewall** > **Properties** page.
2. Check **Enable BACnet firewall**.
3. Uncheck **Allow All Private IP Addresses**.



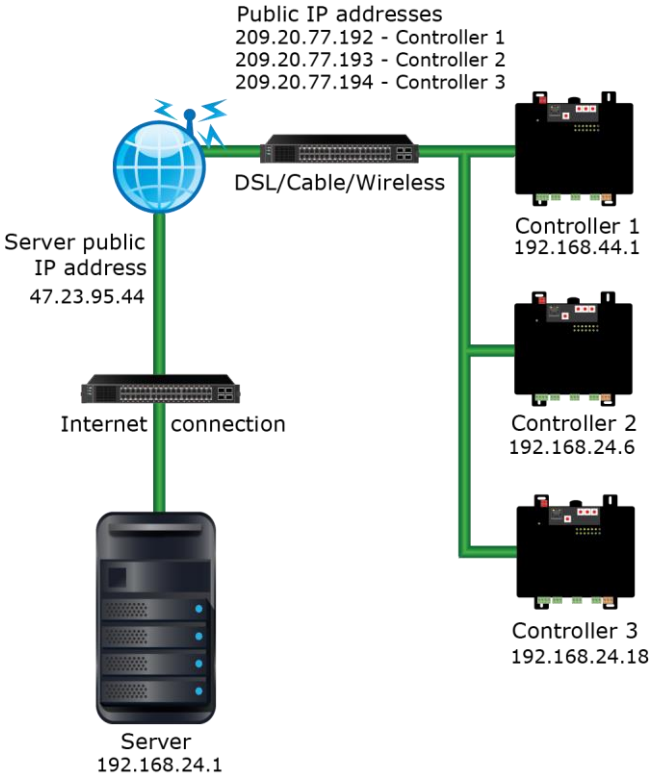
4. Check **Enable Whitelist**.
5. On the first row, check **Enable**, and then enter the address 47.23.95.44.



6. Click **Accept**.
7. Wait for the page to update, and then check **Confirm firewall settings**.

Case 3: Multiple controllers exposed to the Internet at one site

Multiple controllers that are accessible on the Internet (for example, behind a DSL, cable, or wireless device) may not be protected by a network firewall or whitelist. The controllers have private IP addresses, but it is their public IP addresses that are exposed to the Internet.

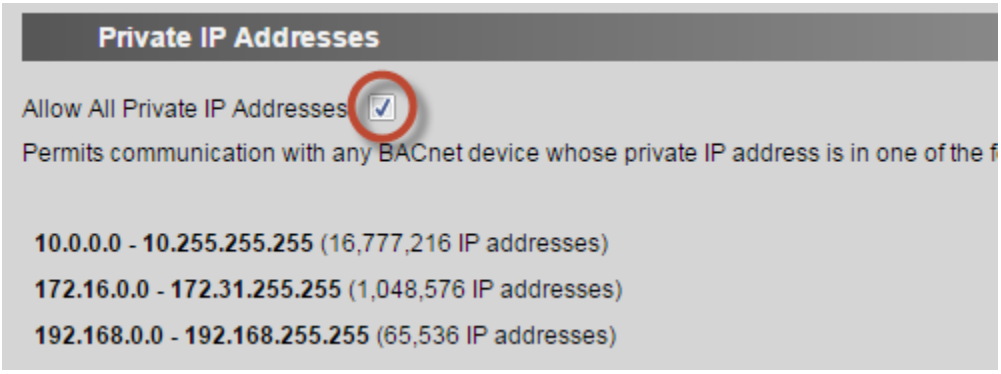


In this example, the controllers need to communicate with the WebCTRL® server and each other. The controllers are the only devices on the site's private network, or other devices present are benign.

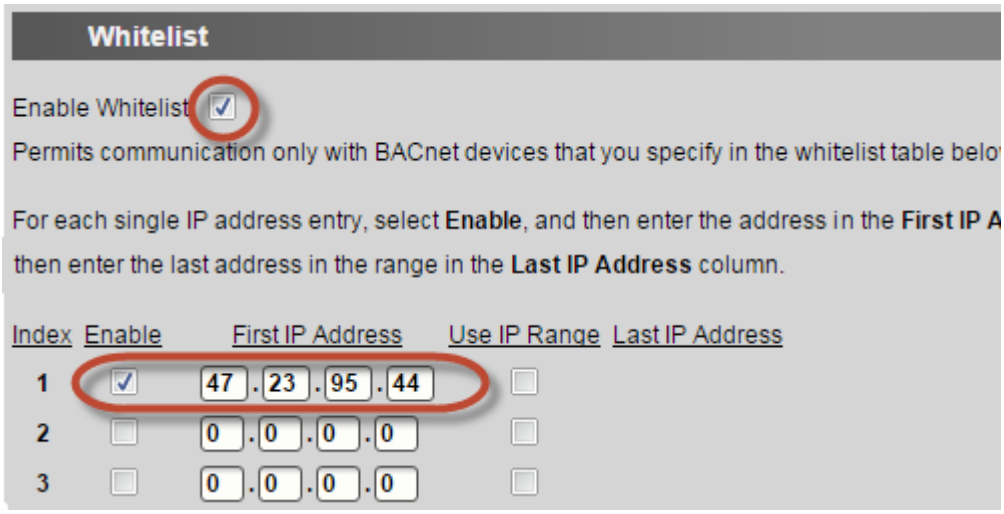
Each controller's BACnet firewall should allow BACnet communication with the WebCTRL® server's public IP address and with all private IP addresses so that the controllers can communicate with each other. The BACnet firewall prevents BACnet communication to the controller's public addresses.

To set up the BACnet firewall:

1. In the WebCTRL® interface, go to each controller's **Driver** > **BACnet Firewall** > **Properties** page.
2. Check **Enable BACnet firewall**.
3. Check **Allow All Private IP Addresses**.



4. Check **Enable Whitelist**.
5. On the first row, check **Enable**, and then enter the address 47.23.95.44.



6. Click **Accept**.
7. Wait for the page to update, and then check **Confirm firewall settings**.

Users

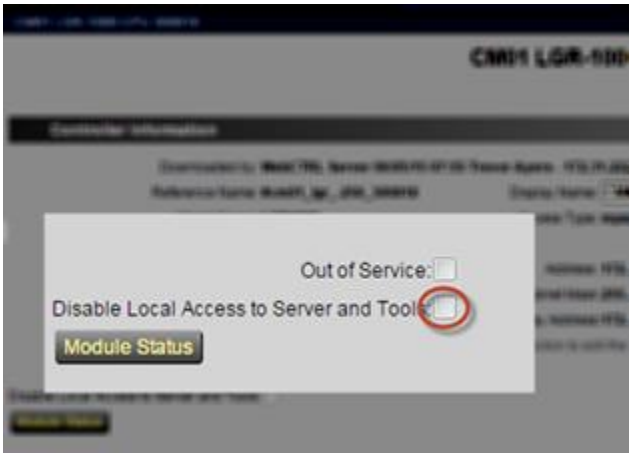
Follow the guidelines below to limit unauthorized user access.

- **Administrator account**—A system has a default Administrator user. If you upgraded from a pre-v6.5 system, change the Administrator's login name and add a password. DO NOT leave the password blank. DO NOT use the same password for multiple systems.
  NOTE When you create a new system in v6.5, you will be required to change the name and add a password.
- **Anonymous account**—A pre-v6.5 system had a default Anonymous user that required no user name or password. If you have not upgraded to v6.5, delete this user.
  NOTE The Anonymous user was removed from WebCTRL® v6.5.
- **Advanced password policy**—Enable the advanced password policy and require a minimum password length of at least 8 characters. This will disallow blank passwords.
- **No shared accounts**—Create a different account for each user. DO NOT create role-based accounts where multiple users log in with the same login name and password.
- **Delete old accounts**—Manage accounts when people no longer need access to the WebCTRL® system. Delete their account or change their password.
- **Auto Logoff**—Verify that **Log off operators after __ (HH:MM) of inactivity** is checked on the **System Settings** > **Security** tab.
  NOTE You can disable this for an individual user (for example, an account for a monitoring center).
- **Lock out users**—Verify that **Lock out operators for __ minutes after __ failed login attempts** is checked.
- **Location-dependent security**—Consider using the optional location-dependent security policy. For large systems with many users, you can restrict users to only the locations they should have access to.
- **LDAP/Active Directory Integration**—Consider using the optional LDAP/AD add-on. With this add-on, the WebCTRL® system uses the user accounts and validation of the customer's domain password system (for example, their Windows password). This also increases security because the company likely has a process for removing accounts when someone leaves the company. Contact Technical Support to find out how to get this add-on.

WebCTRL® server

Follow the guidelines below to protect the WebCTRL server.

- **Patches**—Keep the WebCTRL system and the operating system up-to-date with the latest patches.
- **Anti-virus protection—**Keep the WebCTRL server's anti-virus software and definitions up-to-date.
- **Single-use server**—WebCTRL software should be the only application running on the server. DO NOT put other applications on the same server.
- **HTTPS—**Use https:// with a certificate signed by a standard certificate authority, when possible. If using a self-signed certificate, install the server certificate on the client computers so users do not develop the bad habit of ignoring the "unsafe certificate" error.
- **Remote access**—After commissioning, uncheck **Allow remote file management** on the **System Settings** > **Security** tab.
- **Local Access**—After commissioning, check **Disable Local Access to Server and Tools** on the controller's **Properties** page. You can use Global modify to change this for all devices simultaneously.



Database server

Follow the database server vendor's best practices for a secure installation. This should include steps such as changing default accounts and passwords.

Configure the database server to accept connections only from the WebCTRL® system. Most database servers have a whitelist mechanism to facilitate this.

Appendix A: Glossary

BAS—A Building Automation System is a collection of BACnet devices, the WebCTRL server, and the network(s) they reside on.

LAN—A Local Area Network is a computer network that interconnects computers/devices within a limited area such as an office building.

Firewall—A device that restricts network traffic. Firewall functionality is often combined with IP Router functionality in a single device. A firewall is configured with rules to define what kind of traffic is allowed or blocked. Personal computers and servers have firewall functionality built into them.

IP router—An IP (Internet Protocol) device that connects two or more IP networks. Typically an IP router connects a local network to the larger enterprise/Internet network.

NAT router—An IP router that remaps IP addresses from one network to one or more IP addresses on another network. A NAT router is commonly used to connect devices on a private network to the Internet or enterprise network, and it often has firewall and port forwarding capabilities.

Port—A port is a 16 bit (0-65535) number associated with an IP address that defines an endpoint of a computer network connection. There are two types of ports, TCP and UDP. BACnet uses a UDP port. HTTP, HTTPS and Alarm Notification Client use TCP ports. To manage access to a port in a firewall, you must know its number and type.

Private IP address—An IP address in one of the following ranges:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

VLAN—A Virtual Local Area Network is partitioned and isolated by the IP network switch (or router). It is typically as effective as physically separating the network.

VPN—A Virtual Private Network is a method for extending a private network across a public network, such as the Internet. A VPN enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and they benefit from the functionality, security and management policies of the private network.

Whitelist—A list of IP addresses that are the only ones allowed through a firewall. Advanced firewall devices can have different whitelists for a given port or protocol.

Appendix B: Security checklist

Designing and Planning

- ☐ Separate user and BACnet networks either physically or with a VLAN.
- ☐ Determine the appropriate Internet connection scenario. See Internet connectivity scenarios.

Installing

If you have dual NICs:

- ☐ Enter the WebCTRL user network IP address and subnet mask in SiteBuilder on the **Configure** > **Preferences** > **Web Server** tab .
- ☐ Enter the WebCTRL BACnet network IP address and subnet mask in the WebCTRL interface on the **Connections** page > **Configure** tab.

If using Internet connectivity scenario A:

- ☐ Verify that IP addresses for the WebCTRL server and controllers are in one of the private IP address ranges.

If using Internet connectivity scenario B:

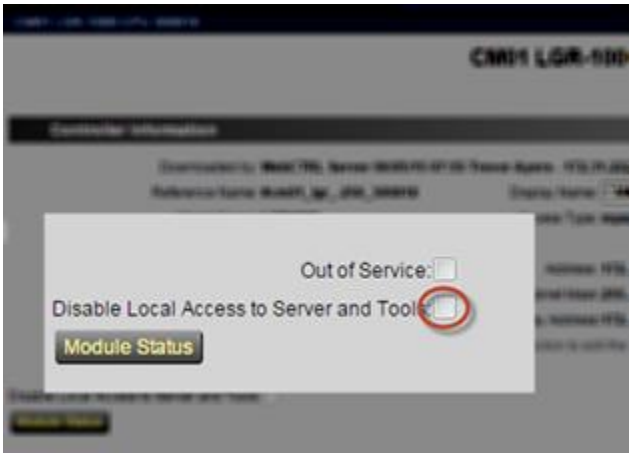
- ☐ Verify that controller IP addresses are in one of the private IP address ranges.
- ☐ Verify that the NAT router or firewall exposing the WebCTRL server only exposes TCP ports 80 and/or 443.

If using Internet connectivity scenario C:

- ☐ Verify that the NAT router or firewall exposing the WebCTRL server only exposes TCP ports 80 and/or 443, and UDP port 47808.
- ☐ Verify that each NAT router or firewall used (for both the server and each controller) has been configured with an appropriate whitelist of allowed IP addresses in your Internet connection device, or each controller is protected by its internal BACnet firewall feature.
- ☐ Test the whitelist protection from the Internet. Use a separate WebCTRL server on a public network by using a modstat like "modstat mac:0,b:1.2.3.4". Confirm you cannot access any of the system's controllers.
- ☐ Change the Administrator login name and add a password.
- ☐ If you are running a pre-v6.5 system, remove the Anonymous user account.
- ☐ Verify that the WebCTRL server's anti-virus software is up-to-date and is set to update automatically.
- ☐ Configure the database server to accept connections only from the WebCTRL application using a whitelist.

After Commissioning

- ☐ **Disable Local Access to Server and Tools** is checked on the controller's **Properties** page. You can use Global modify to change this for all controllers simultaneously.



- ☐ Enable the Advanced password policy and set the minimum password length to at least 8 characters.

On the **System Settings** > **Security** tab, verify that:

- ☐ **Allow remote file management** is not checked
- ☐ **Log off operators after __ (HH:MM) of inactivity** is checked
- ☐ **Lock out operators for __ minutes after __ failed login attempts** is checked

On SiteBuilder's **Configure** > **Preferences** > **Web Server** tab, verify that the following are not checked:

- ☐ Any **TLS Level** below **"TLS 1.3"**
- ☐ **Allow SOAP applications over HTTP**
- ☐ **Allow unsigned add-ons**

System Maintenance

- ☐ Install the latest software updates to keep the system current with the most recent security enhancements.

To quickly check security measures in place

In the WebCTRL® interface, use the Manual Command **sreview** to view your system's critical security compliance. These settings are described in more detail in the document above.

The **sreview** report displays the following:

Web Server	Possible responses	Recommendation for the most secure system
SSL Mode	**on**, **off**, or **both**	**on**
TLS in use	**on** or **off**	**true** (when SSL Mode is **on** or **both**)
TLS protocol	Version number	**TLS 1.3**
Allow unsigned add-ons	**true** or **false**	**false**
Allow SOAP over HTTP	**true** or **false**	**false**
Reads X-Forwarded-For Header	**true** or **false**	**false**

Certificate	Possible responses	Recommendation for the most secure system
Self-signed certificate in use	**true** or **false**	false
Certificate issued by	Distinguished Name of the certificate signer	certificate information, not a setting
Certificate expired	**true** or **false**	certificate information, not a setting
Certificate not yet valid	**true** or **false**	certificate information, not a setting
Certificate expires	date and time the certificate becomes invalid	certificate information, not a setting

	Possible responses	Recommendation for the most secure system
Email		
Secure SMTP enabled on email server	**true** or **false**	**true**
Passwords		
Password policy enforced	**true** or **false**	**true**
Software Updates		
Latest cumulative update applied: none or date	**none** or **date**	Keep the WebCTRL® system and the operating system up-to-date with the latest patches.

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
8/3/21	Internet Connectivity Scenarios	Added Scenario D	X-PM-LO-O
	Network Firewall	Added a row for BACnet/SC, note for Scenario D	X-PM-LO-O
	All network graphics	Graphics updated to show OptiFlex™ controllers	D

* For internal use only