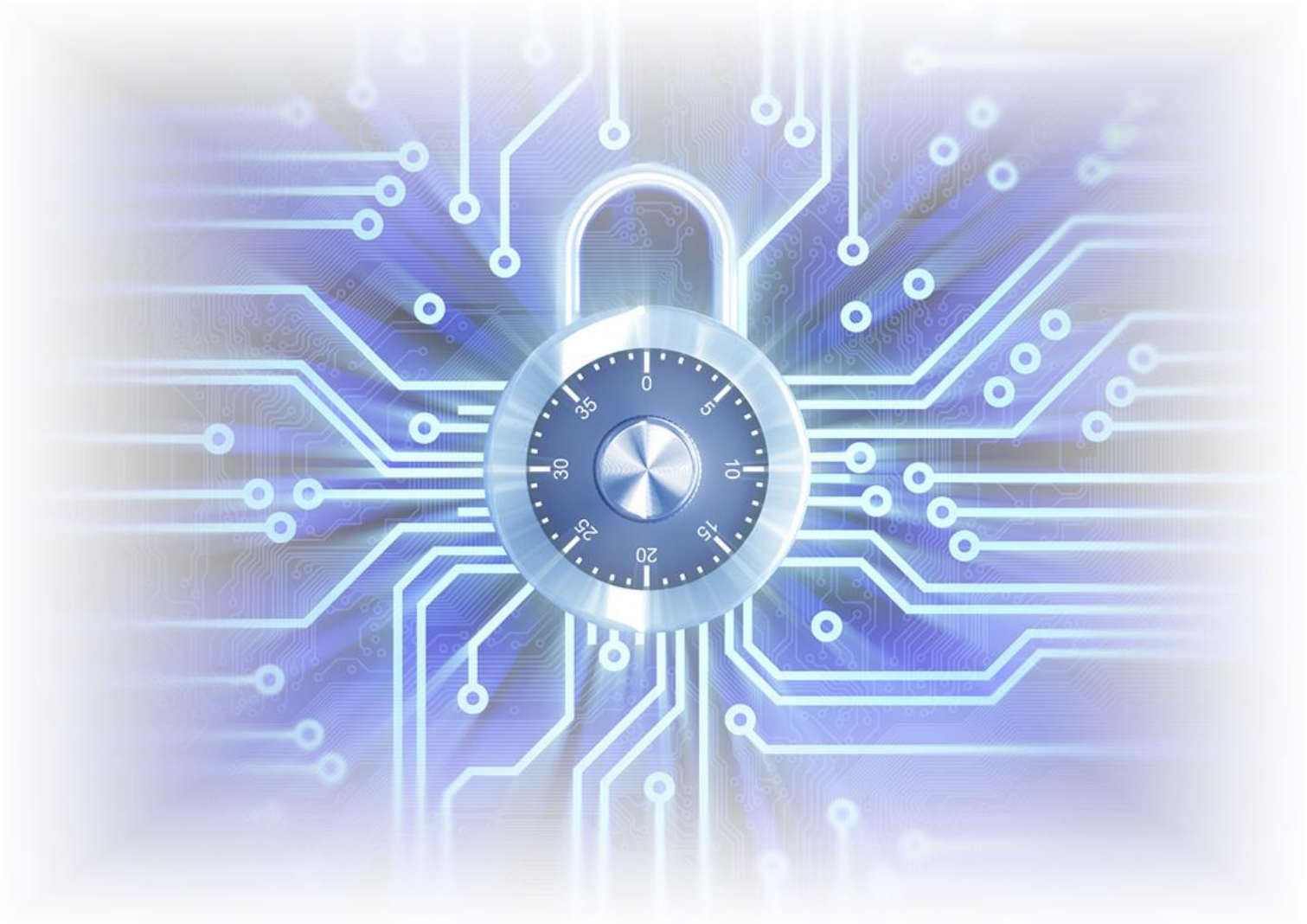


Security Best Practices

for an i-Vu® Express v8.5 system





Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

©2023 Carrier. All rights reserved.



Contents

Security best practices	1
Network separation	1
Internet connectivity scenarios.....	2
Network firewall.....	5
BACnet firewall.....	6
Users	12
i-Vu Express server	12
Appendix A: Glossary	13
Appendix B: Security checklist.....	14
Document revision history	15



Security best practices

Carrier 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 i-Vu® Express building automation systems.

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

Network separation

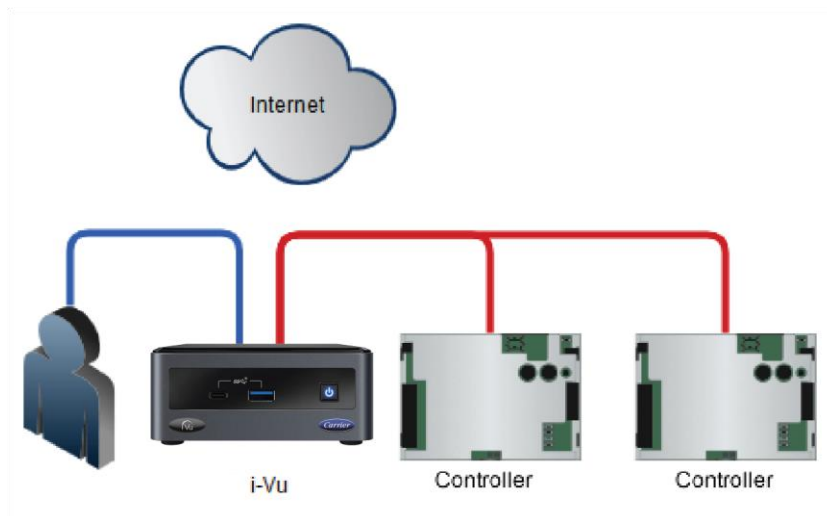
Standard BACnet is an intentionally open system that makes it easy to discover and control any device on its network. Because of this, you should design your system to minimize the users that have access to the server and controllers.

Because the i-Vu® web server, controllers, and users are on the same network, you must be aware that there is still a potential risk from insiders, such as the curious tinkerer, a student on an education system's network, or a disgruntled employee. For this reason, you may want to consider completely isolating the i-Vu network and its users.

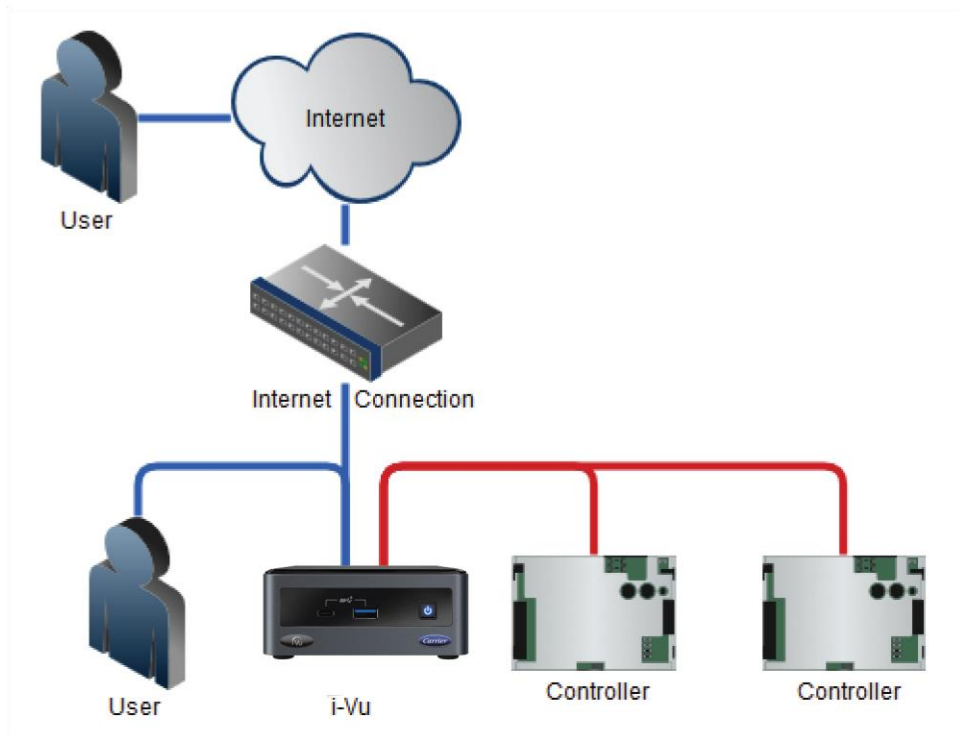
Internet connectivity scenarios

The i-Vu Express 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



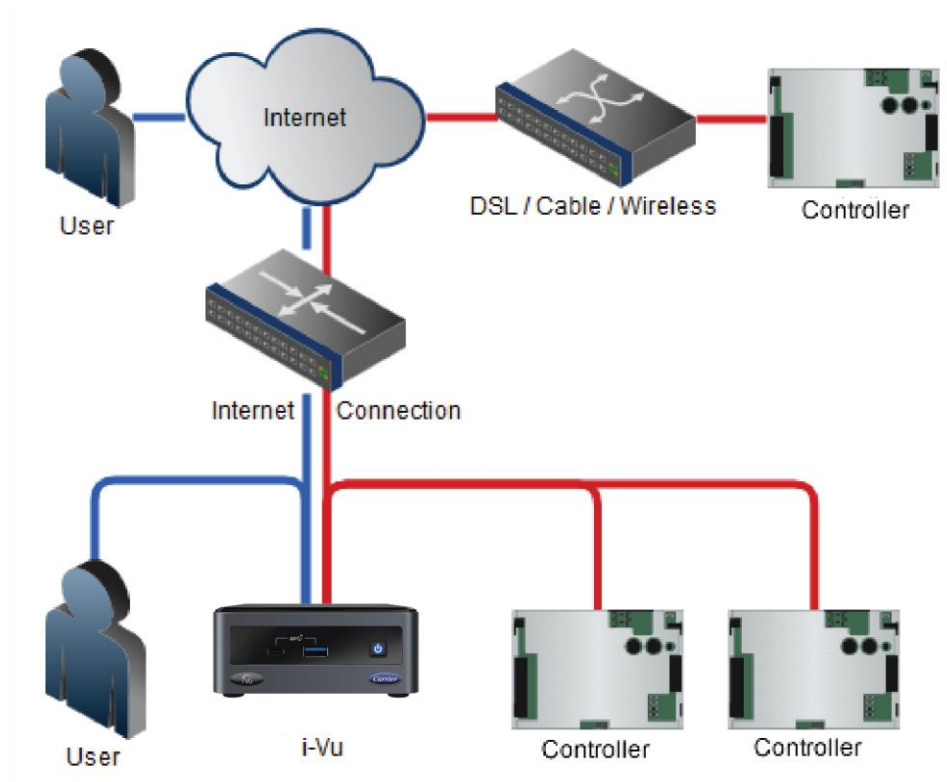
Do not permanently expose the i-Vu Express server or the BACnet network to the Internet. You can, however, allow users to access the i-Vu Express server through a secure VPN connection. If a NAT router or firewall is present on the LAN for other purposes, it should not have any ports forwarded to the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

Scenario B: Public Users - Medium risk

It is acceptable to permanently expose the i-Vu Express server on the Internet as long as:

- The BACnet network is not exposed.
- The NAT/Firewall device exposing the i-Vu Express system exposes only TCP ports 80 and 443 on the i-Vu Express 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 i-Vu Express 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 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 i-Vu® Express system only from devices whose public IP addresses are in the list. Often, the only address controllers need to talk to is the i-Vu Express server. The i-Vu Express 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.

Network firewall

Limit the ports opened through any firewall or NAT port forwarding to the minimum ports required. The i-Vu Express system uses the following ports:

Port	Transfer	Protocol/User	Use
53	TCP	DNS	Basic Network
53	UDP	DNS	Basic Network
5353	TCP	Multicast DNS (Avahi)	Basic Network
80 (default)	TCP	http (Web server)	Client/Server
1234	TCP	Chronyd	Basic Network
1234	UDP	Chronyd	Basic Network
443 (default)	TCP	https (Web server, Management Tool)	Client/Server
47806 (default)	TCP	Alarm Notification Client	Client/Server
47808	UDP	BACnet/IP	Server/i-Vu router
47808	TCP	Diagnostic Telnet *	Client/Server
47812	UDP	CCN/IP	i-Vu CCN router/Server
50005 50007 50008	UDP	Firmware CCN/IP	Server/i-Vu CCN router
50005 - 50008	UDP	Firmware CCN/IP	CCN router to CCN router

* 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.

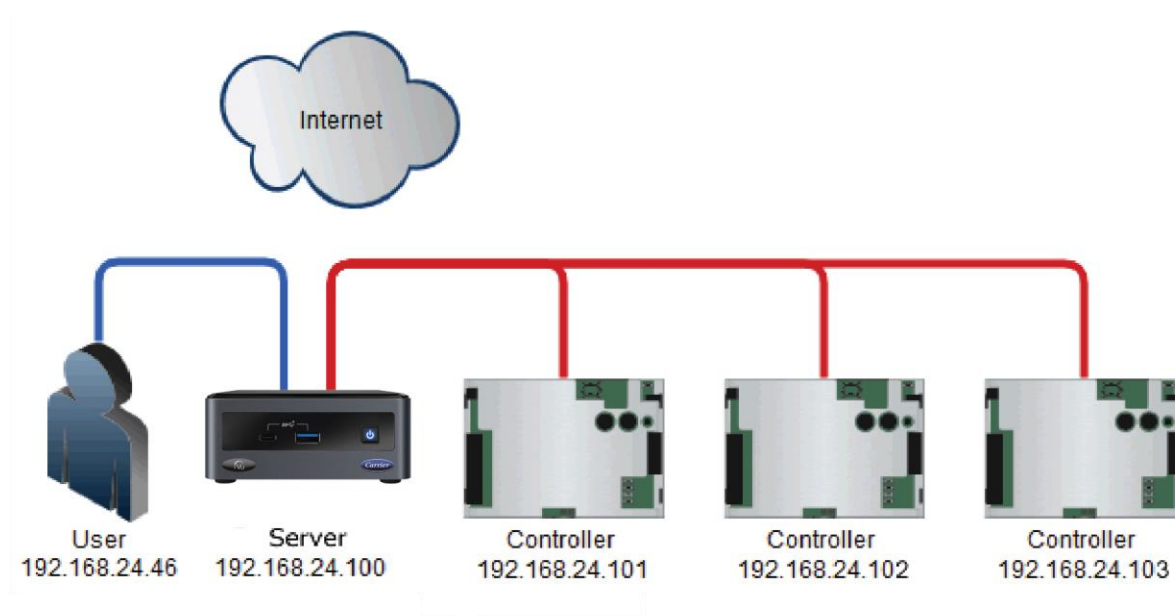
BACnet firewall

The v6-02 drivers for Carrier 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.

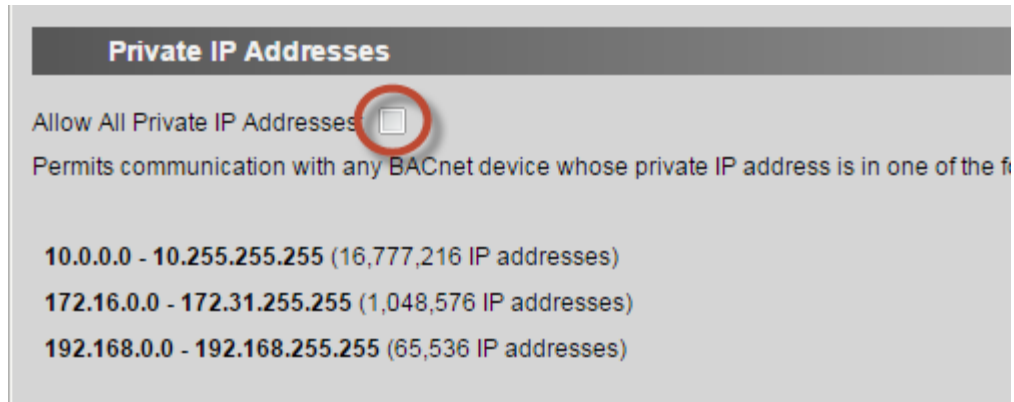


In this example, each controller's BACnet firewall should allow BACnet communication from the i-Vu® Express server's IP address and the controller's IP addresses. The user at 192.168.24.46 should not be allowed BACnet communication with the controllers.

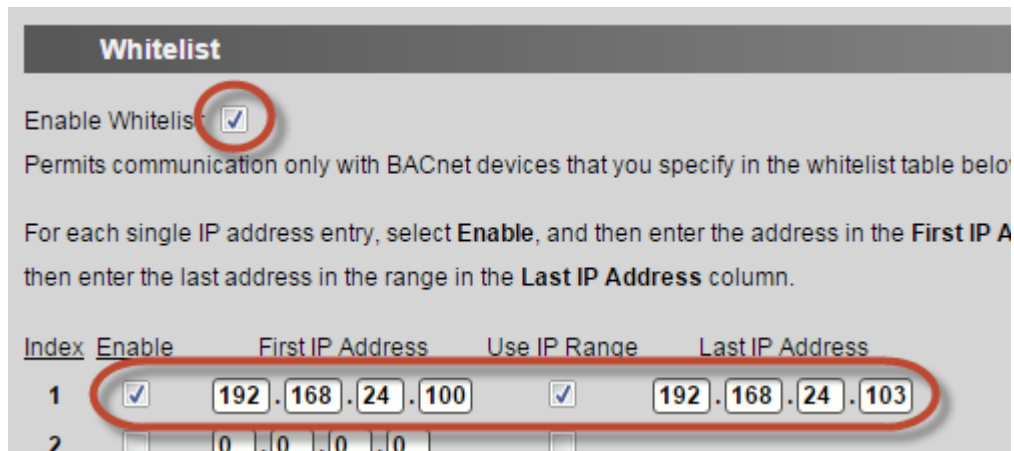
The server and controllers addresses fall within the private IP address range of 192.168.0.0 to 192.168.255.255, but restricting BACnet communication to all private IP addresses is not sufficient since that would allow communication from the user. So a whitelist must be created in the BACnet firewall.

To set up the BACnet firewall:

- 1 In the i-Vu® Express interface, right-click each controller and select **Driver Properties**.
- 2 Select **BACnet Firewall > Properties** tab.
- 3 Check **Enable BACnet firewall**.
- 4 Uncheck **Allow All Private IP Addresses**.



- 5 Check **Enable Whitelist**.
- 6 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.

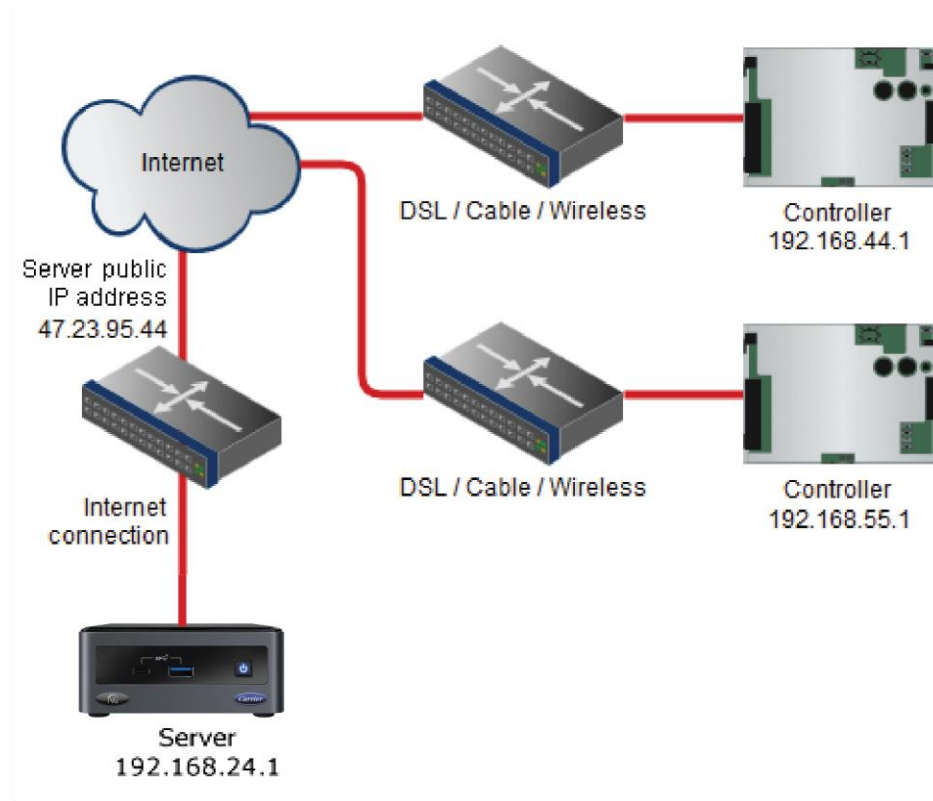


- 7 Click **Accept**.
- 8 Wait for the page to update, and then check **Confirm firewall settings**.

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 i-Vu® Express 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 i-Vu® Express interface, right-click each controller and select **Driver Properties**.
- 2 Select **BACnet Firewall > Properties** tab.
- 3 Check **Enable BACnet firewall**.
- 4 Uncheck **Allow All Private IP Addresses**.

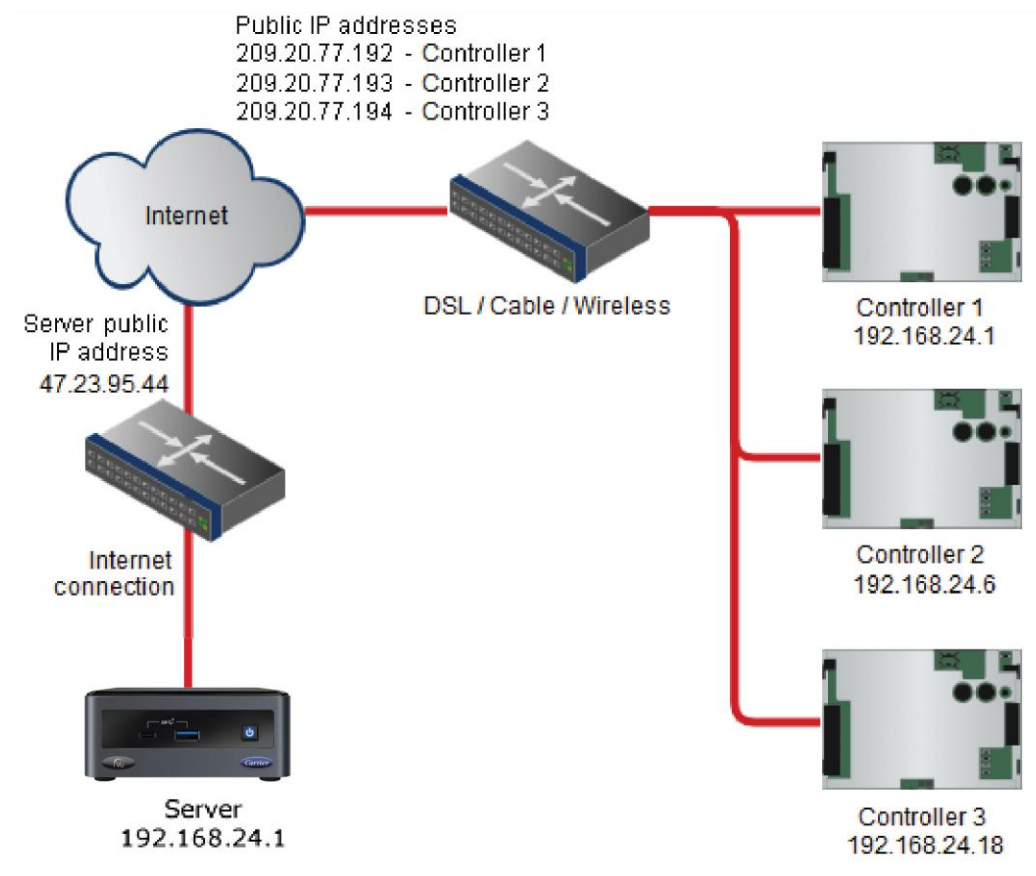
- 5 Check **Enable Whitelist**.
- 6 On the first row, check **Enable**, and then enter the address 47.23.95.44.

Index	Enable	First IP Address	Use IP Range	Last IP Address
1	<input checked="" type="checkbox"/>	47 . 23 . 95 . 44	<input type="checkbox"/>	
2	<input type="checkbox"/>	0 . 0 . 0 . 0	<input type="checkbox"/>	
3	<input type="checkbox"/>	0 . 0 . 0 . 0	<input type="checkbox"/>	

- 7 Click **Accept**.
- 8 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.

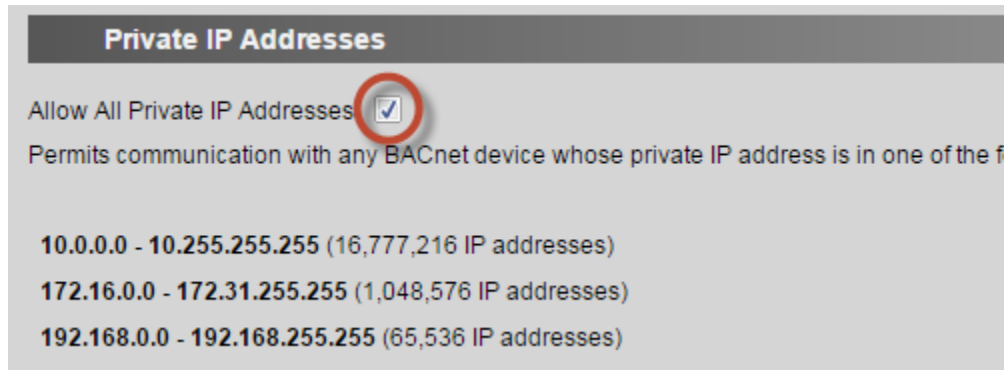


In this example, the controllers need to communicate with the i-Vu® Express server and each other. The controllers are the only devices on the site's private network, or other devices present are benign.

Each controller's BACnet firewall should allow BACnet communication with the i-Vu® Express 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 i-Vu® Express interface, right-click each controller and select **Driver Properties**.
- 2 Select **BACnet Firewall > Properties** tab.
- 3 Check **Enable BACnet firewall**.
- 4 Check **Allow All Private IP Addresses**.



Private IP Addresses

Allow All Private IP Addresses ☒

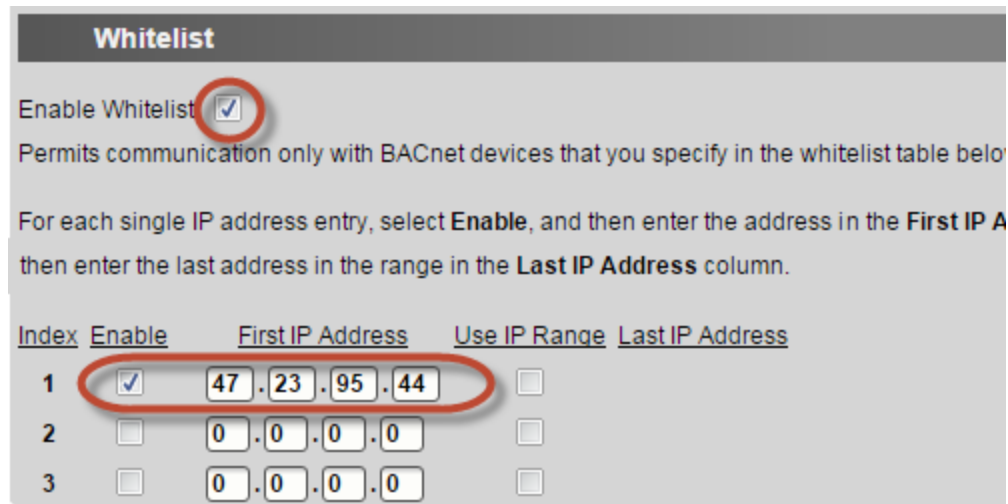
Permits communication with any BACnet device whose private IP address is in one of the following ranges:

10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)

192.168.0.0 - 192.168.255.255 (65,536 IP addresses)

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



Whitelist

Enable Whitelist ☒

Permits communication only with BACnet devices that you specify in the whitelist table below.

For each single IP address entry, select **Enable**, and then enter the address in the **First IP Address** column. If you want to specify a range of IP addresses, select **Use IP Range**, and then enter the last address in the range in the **Last IP Address** column.

Index	Enable	First IP Address	Use IP Range	Last IP Address
1	<input checked="" type="checkbox"/>	47 . 23 . 95 . 44	<input type="checkbox"/>	
2	<input type="checkbox"/>	0 . 0 . 0 . 0	<input type="checkbox"/>	
3	<input type="checkbox"/>	0 . 0 . 0 . 0	<input type="checkbox"/>	

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

Users

Follow the guidelines below to limit unauthorized user access.

- **Installer account**—A system has a default Installer user. If you upgraded from a pre-v6.5 system, change the Installer'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 v8.5, you will be required to change the name and add a password.
- **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 i-Vu Express system. Delete their account or change their password.
- **Auto Logoff**—Verify that the field **Log off operators after __ (HH:MM) of Inactivity** is enabled in System Options.
NOTE You can disable this for an individual user (for example, an account for a monitoring center).
- **Lock out users**—Verify that the field **Lock out operators for __ minutes after __ failed login attempts** is enabled.

i-Vu Express server

Protect the i-Vu Express server by keeping the i-Vu Express system up-to-date with the latest updates.

Appendix A: Glossary

BAS—A Building Automation System is a collection of BACnet and/or CCN devices, the i-Vu Express 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

- ☐ Determine the appropriate Internet connection scenario. See *Internet connectivity scenarios* (page 2).

If using Internet connectivity scenario A:

- ☐ Verify that IP addresses for the i-Vu Express 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 i-Vu Express server only exposes TCP ports 80 and/or 443.

If using Internet connectivity scenario C:

- ☐ Verify that the NAT router or firewall exposing the i-Vu Express 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 or each controller is protected by its internal BACnet firewall feature.
- ☐ Test the whitelist from a separate i-Vu Express 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 Installer login name and add a password.

After Commissioning

- ☐ On the **System Options > Security** tab, enable the Advanced password policy and set the minimum password length to at least 8 characters.

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

- ☐ **Log off operators after __ (HH:MM) of inactivity** is checked
- ☐ **Lock out operators for __ minutes after __ failed login attempts** is checked

System Maintenance

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

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*
		No updates yet	

* For internal use only

