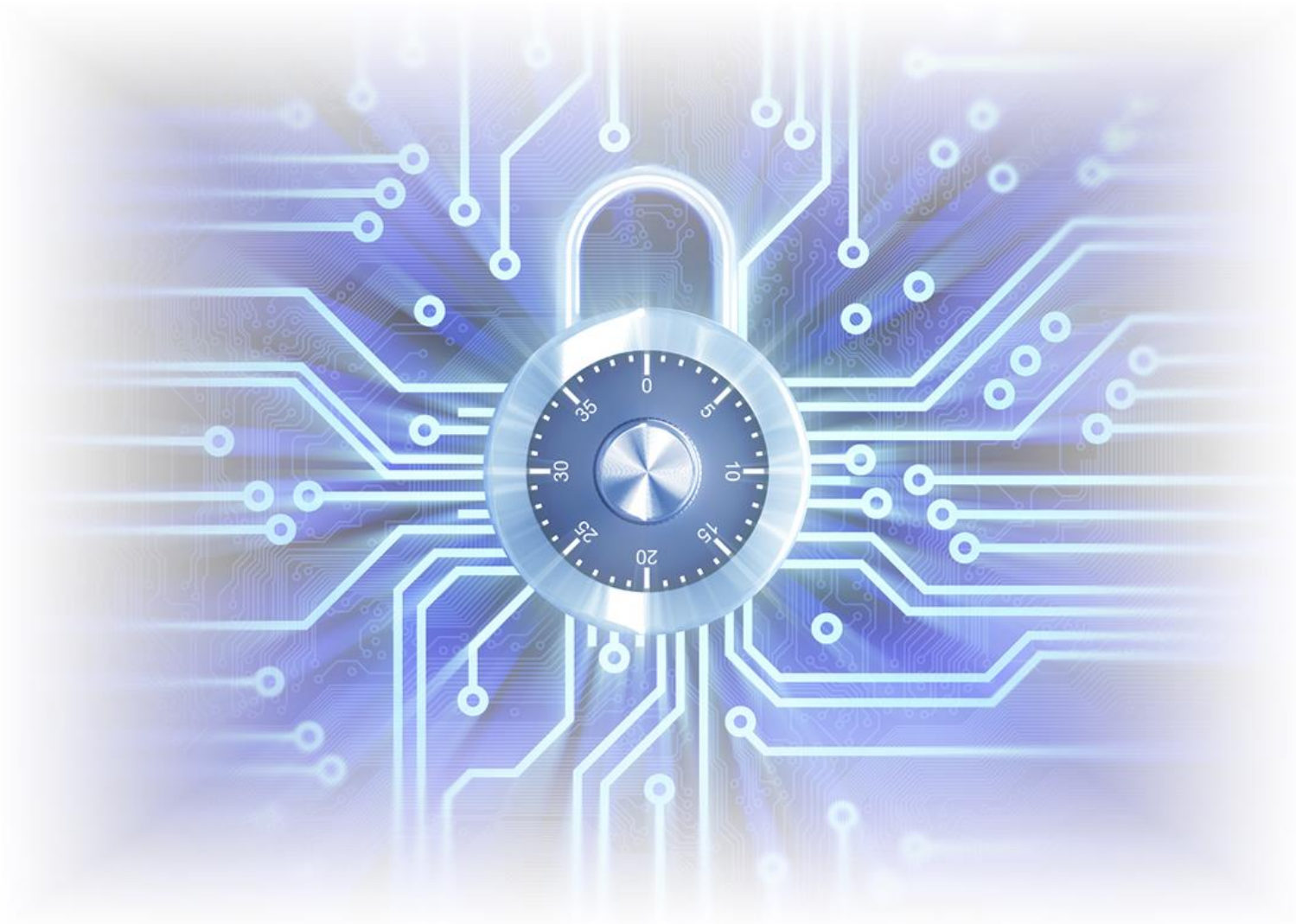




United Technologies
turn to the experts 

Security Best Practices for an i-Vu® Pro v6.0 system





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

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

CARRIER CORPORATION ©2017. All rights reserved throughout the world. i-Vu is a registered trademark of Carrier Corporation. All other trademarks are the property of their respective owners.

Contents

Security best practices	1
Network separation	1
Internet connectivity scenarios.....	2
Firewall configuration	5
BACnet firewall.....	5
Users	12
i-Vu Pro server	12
Database server.....	13
Appendix A: Glossary	14
Appendix B: Security checklist	15
Document revision history	17

Security best practices

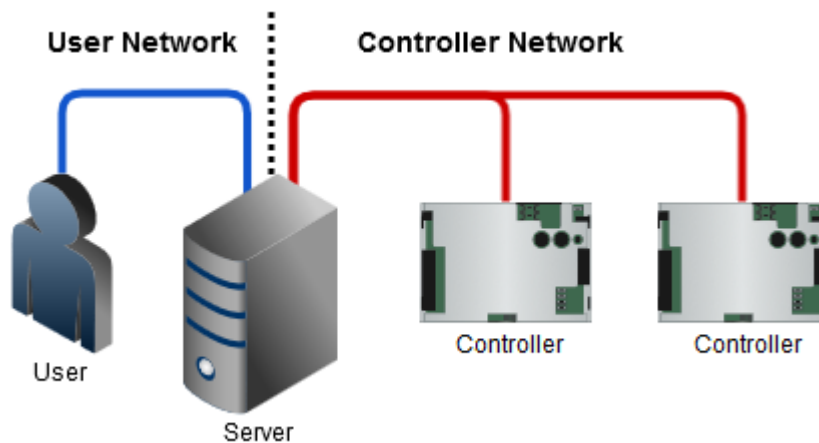
Carrier takes the security of our systems very seriously and you play the biggest part in this by installing and configuring systems in a secure manner. We encourage you to establish security policies for your own company networks and all the systems you install and service.

Follow the best practices in this document when deploying i-Vu® Pro building automation systems.

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

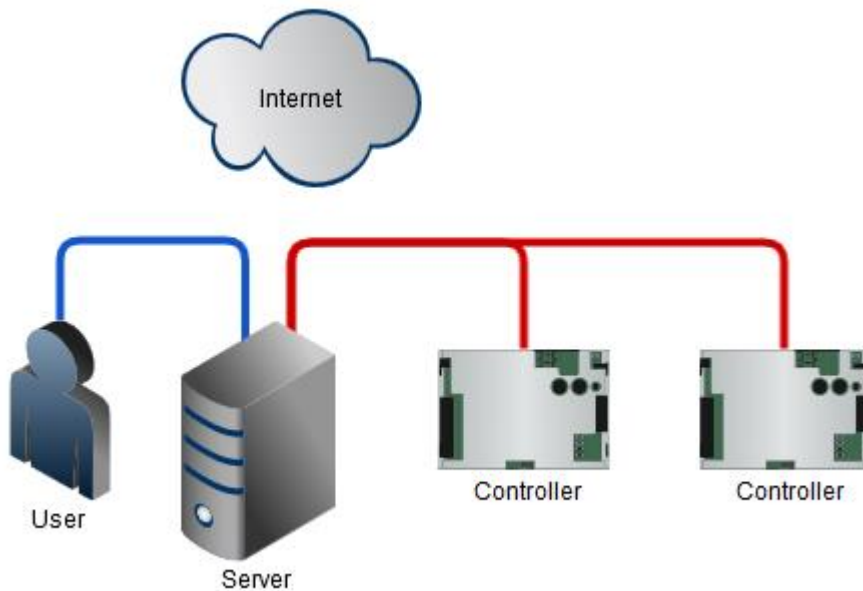
If you have dual NICs (Network Interface Cards), the i-Vu Pro server must have a different IP address for each network:

- 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 i-Vu Pro interface on the **Connections** page > **Configure** tab.

Internet connectivity scenarios

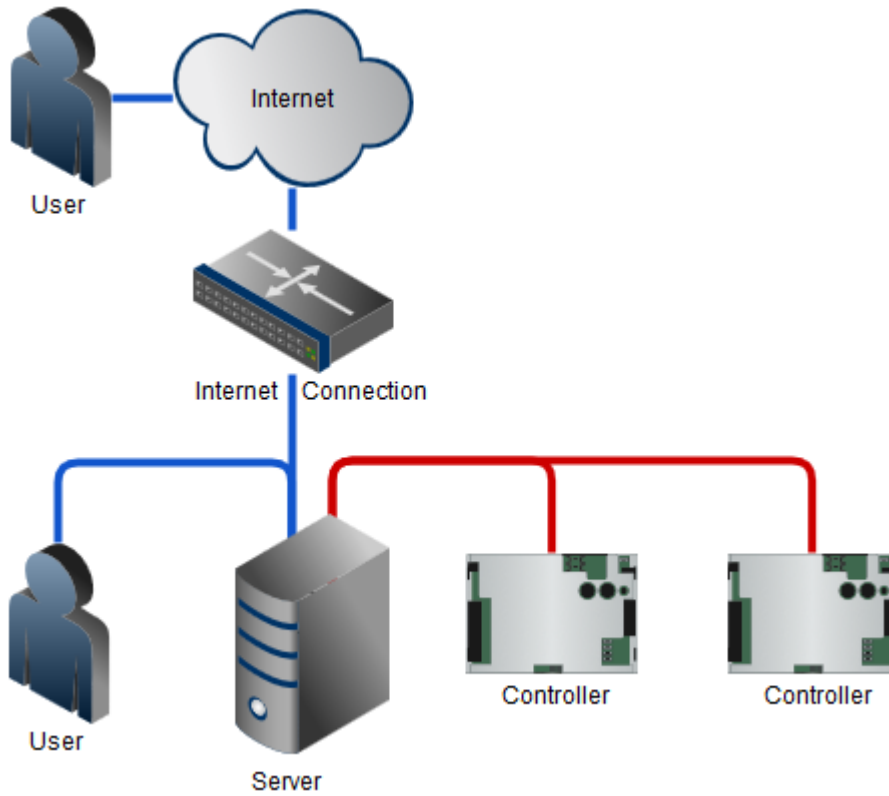
The i-Vu Pro system's connection to the Internet may vary greatly based on the client's needs and IT capabilities. The following possible network scenarios are listed in order of DECREASING security.

Scenario A: Isolated Network - Low risk



Do not permanently expose the i-Vu Pro server or the BACnet network to the Internet. You can, however, allow users to access the i-Vu Pro 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 Pro server or any controllers.

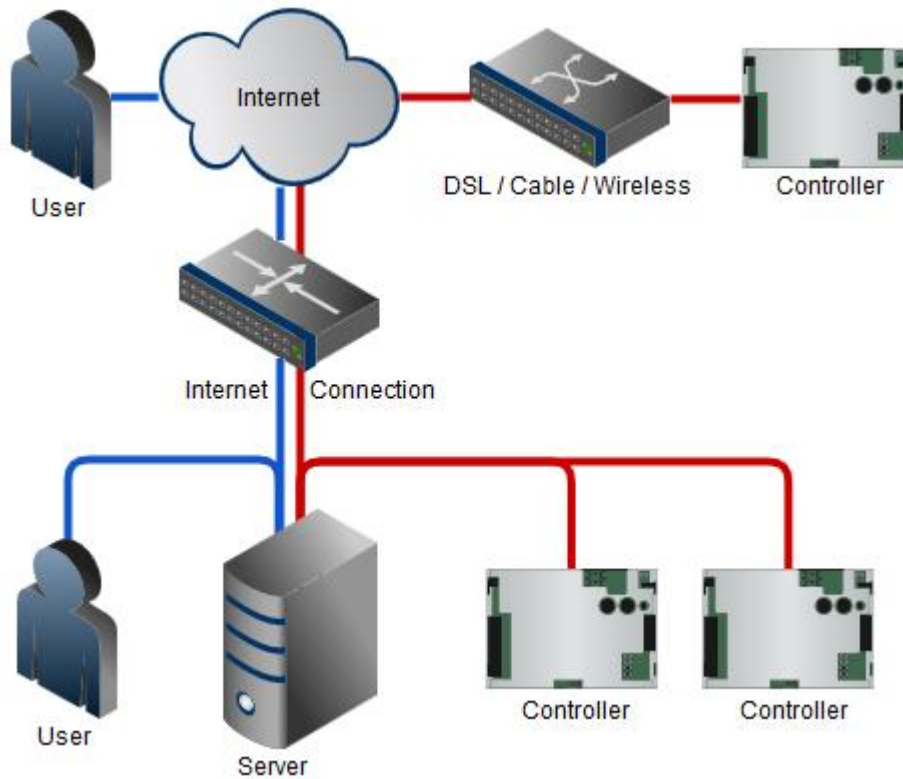
Scenario B: Public Users - Medium risk



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

- The BACnet network is not exposed.
- The NAT/Firewall device exposing the i-Vu Pro system exposes only TCP ports 80 and 443 on the i-Vu Pro 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 Pro 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, 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® Pro 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 Pro server. The i-Vu Pro 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.

Firewall configuration

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

Port	Use
TCP 80	HTTP
TCP 443	HTTPS
UDP 47808	BACnet/IP
TCP 47806	Alarm Notification Client
TCP 47808	Telnet

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.

Use the following for CCN:

Port	Use
UDP 47812	Server CCN/IP
UDP 50005	Controller CCN/IP

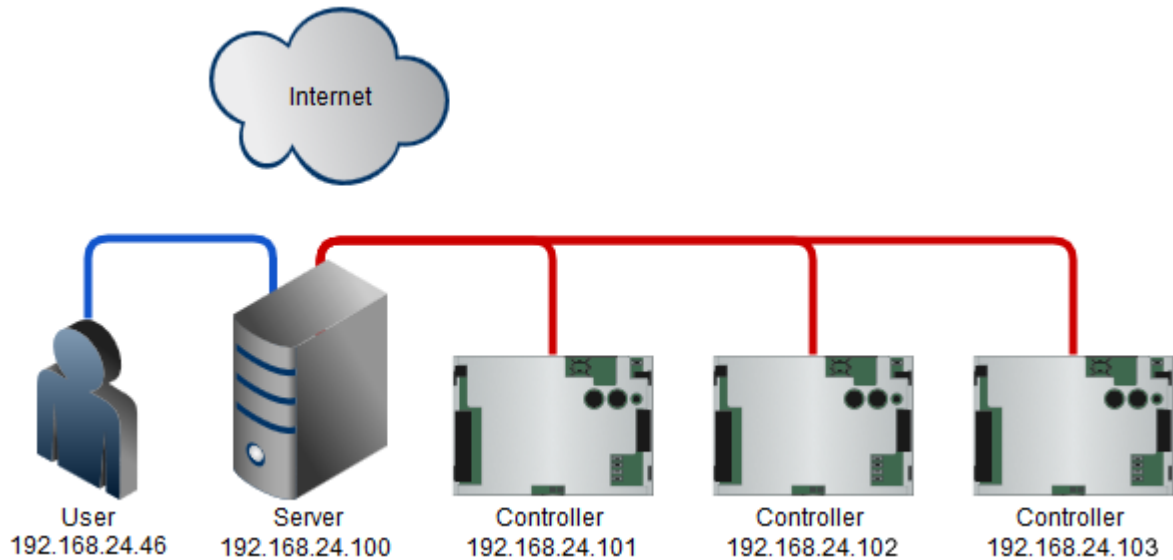
BACnet firewall

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.



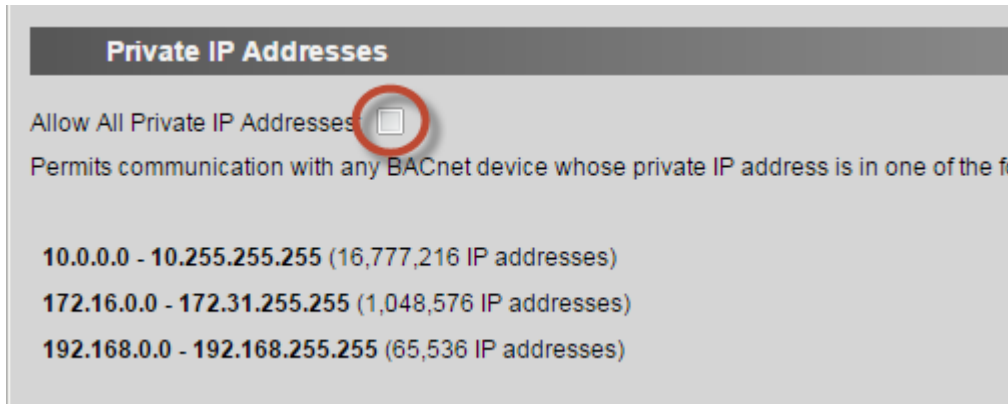
In this example, each controller's BACnet firewall should allow BACnet communication from the i-Vu® Pro server's IP address and the controller's IP addresses. The user at 192.168.24.46 should not be allowed BACnet communication with the controllers.

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.

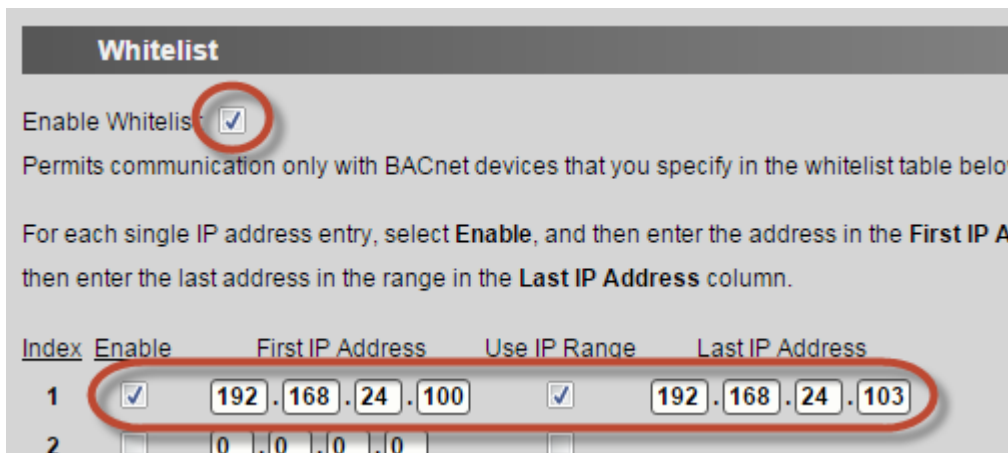
To set up the BACnet firewall:

- 1 In the i-Vu® Pro interface, right-click each controller and select **Driver Properties**.
- 2 Select **BACnet Firewall > Properties** tab.
- 3 Check **Enable BACnet firewall**.

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



- Check **Enable Whitelist**.
- 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.

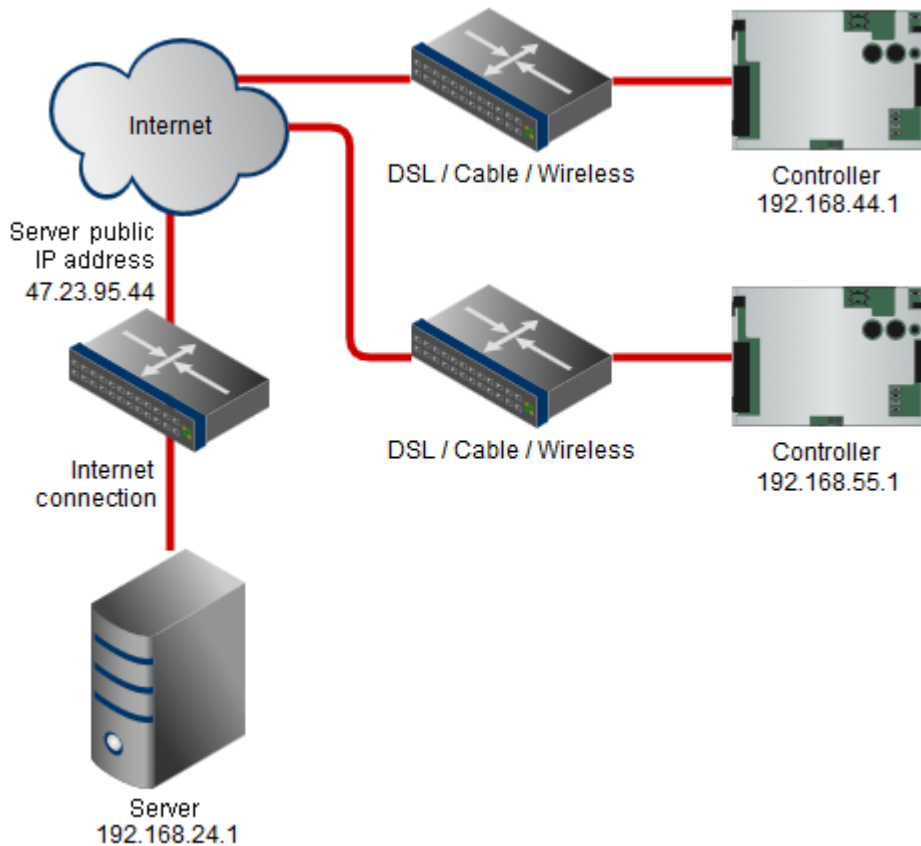


- Click **Accept**.
- Wait for the page to update, and then check **Confirm firewall settings**.

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.

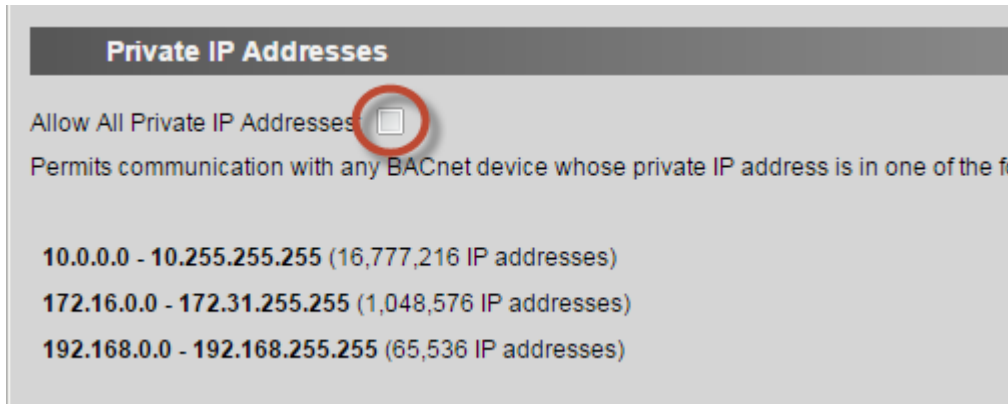


In this example, each controller needs to communicate with only the i-Vu® Pro server so their BACnet firewall's whitelist should have only the server's public IP address. The controllers do not need to communicate with each other.

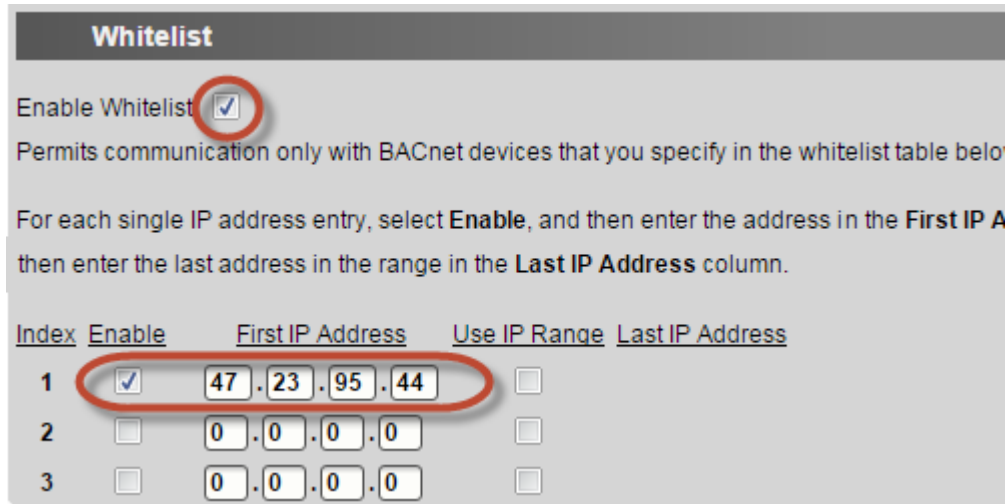
To set up the BACnet firewall:

- 1 In the i-Vu® Pro interface, right-click each controller and select **Driver Properties**.
- 2 Select **BACnet Firewall > Properties** tab.
- 3 Check **Enable BACnet firewall**.

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



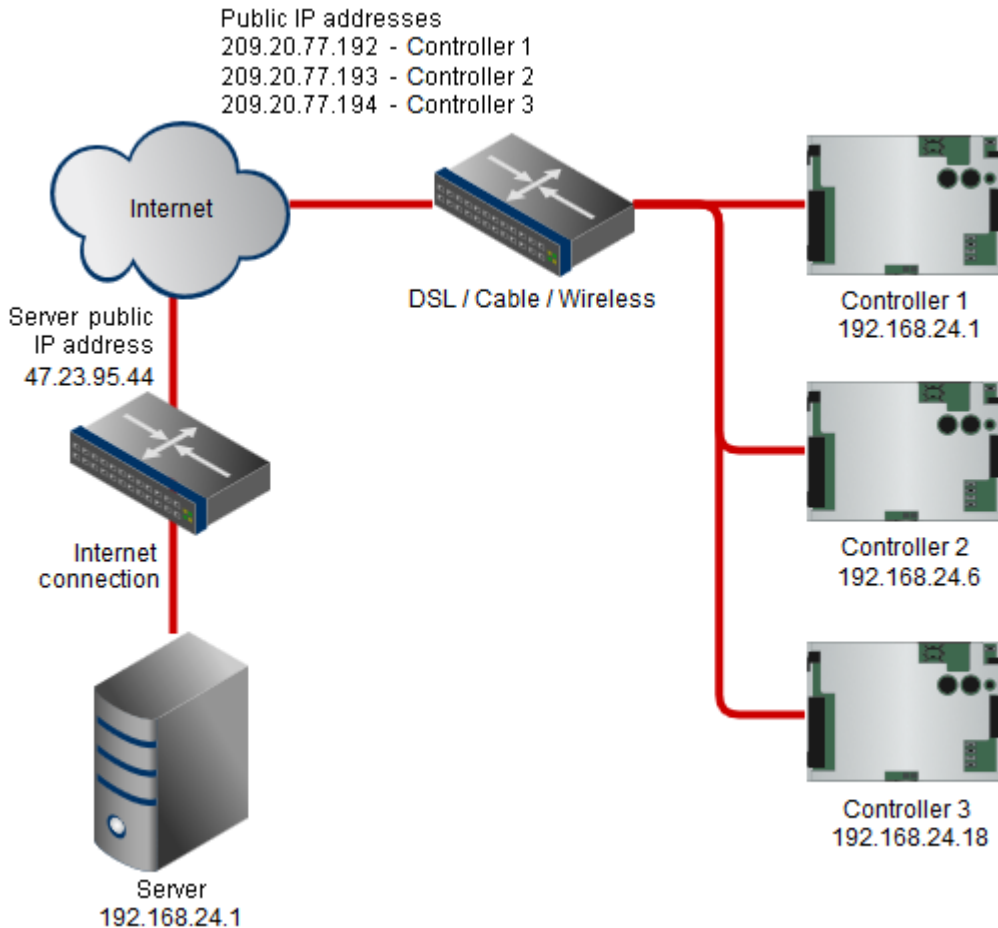
- Check **Enable Whitelist**.
- On the first row, check **Enable**, and then enter the address 47.23.95.44.



- Click **Accept**.
- 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® Pro 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® Pro 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® Pro 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. 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.

- **Administrator account**—A system has a default Administrator user. Change its login name and add a password. DO NOT leave the password blank. DO NOT use the same password for multiple systems.
- **Anonymous account**—A system has a default Anonymous user that requires no user name or password. Delete this user.
- **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 Pro 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.

i-Vu Pro server

Follow the guidelines below to protect the i-Vu Pro server.

- **Patches**—Keep the i-Vu Pro system and the operating system up-to-date with the latest patches.
- **Anti-virus protection**—Keep the i-Vu Pro server's anti-virus software and definitions up-to-date.
- **Single-use server**—i-Vu Pro software should be the only application running on the server. DO NOT put other applications on the same server.
- **HTTPS**—Use https:// with a root certificate 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.

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 i-Vu Pro system. Most database servers have a whitelist mechanism to facilitate this.

Appendix A: Glossary

BAS—A Building Automation System is a collection of BACnet and/or CCN devices, the i-Vu Pro 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* (page 2).

Installing

If you have dual NICs:

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

If using Internet connectivity scenario A:

- Verify that IP addresses for the i-Vu Pro 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 Pro server only exposes TCP ports 80 and 443.

If using Internet connectivity scenario C:

- Verify that the NAT router or firewall exposing the i-Vu Pro server only exposes
 - BACnet: TCP ports 80 and 443 and UDP port 47808
 - CCN: UDP ports 48712 and 50005
- 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.
- Test the whitelist protection from the Internet. Use a separate i-Vu Pro 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.
- Remove the Anonymous user account.
- Verify that the i-Vu Pro 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 i-Vu Pro application using a whitelist.

After Commissioning

- 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

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*
10/3/17	Appendix B: Security checklist	Added System Maintenance at end of checklist	X-TS-RD-E
1/27/17	BACnet firewall	New topic	C-D
7/20/16	Database server	Added paragraph on following database server vendor's best practices for a secure installation.	X-O-DD-E
4/7/16	Users	Removed reference to LDAP add-on. It is not available yet.	C-TS-RR-E-RD

* For internal use only



CARRIER CORPORATION ©2017

A member of the United Technologies Corporation family · Stock symbol UTX · Catalog No. 11-808-560-01 · 10/3/2017