i-Vu® Standard/Plus v7.0 Installation and Start-up Guide



CARRIER CORPORATION ©2020 · Catalog No. 11-808-672-01 · 12/1/2020

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

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

CARRIER CORPORATION © 2020. 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.

The contents of this guide and the associated Carrier software are property of Carrier Corporation and its respective licensors, and are protected by copyright. For more information on the software and licensing, see the About section in the software's Help menu.

The content of this guide is furnished for informational use only and is subject to change without notice. Carrier Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide. This document contains no technical data controlled by the EAR or ITAR.

Contents

What is the i-Vu® Standard/Plus application? 1
- i-Vu® Standard and Plus web server specifications 2
- i-Vu® tools 2

What's new in v7.0? 4
- What's new in the i-Vu® Standard/Plus application 4
- What's new in the ViewBuilder application 5

Setting up i-Vu® client devices and web browsers 6
- Setting up and using a computer with the i-Vu® system 7
- Setting up and using a web browser to access the i-Vu® interface 7
  - To set up and use Internet Explorer 7
  - To set up and use Microsoft Edge 8
  - To set up and use Mozilla Firefox 9
  - To set up and use Google Chrome 10
  - To set up and use Safari 11

Before starting the i-Vu® application and your system 13
- Step 1: Install Tools and have documentation ready 13
- Step 2: Install device managers and routers 13
- Step 3: Use Network Service Tool V to ensure hardware is communicating on the CCN network 14
- Step 4: Get your systems ready 15

Starting up an i-Vu® Standard/Plus web server 16
- Optional: Mount the web server to a flat panel display 16
- Connect and power up web server 17
- Access the startup screen 18
- Install the Install self-signed certificates for network security 20
- Configure i-Vu® IP addresses 24
- Configure the i-Vu® system using static IP addresses 24
- Management Tool 25
- Set up login and passwords for an additional user 27
- Operators tab 27

Troubleshooting 32
- If using DHCP and can't access the i-Vu® web server with Internet Explorer, by computer name 32
  - i-Vu® web server connected to computer with a crossover cable 32
  - i-Vu® device plugged into LAN 33
  - Example 1: Determining if a valid Ethernet connection exists 34
  - Example 2: Determining if Internet Explorer is using a proxy server 36
  - Example 3: Pinging by computer name 36
  - Example 4: Adding exceptions to a proxy server in Internet Explorer 37
- Connect a monitor directly to the i-Vu® web server 38

System Management 39
- Backup data from Management Tool 39
- Restore data from backup 40
- Restore factory defaults 40
- Restore i-Vu® system 40
- Update the SAL library 41
- Synchronize to system time 43

Advanced topics 44
- i-Vu® network connection options and requirements 44
- Using a loopback address 47
- If DHCP will not assign two IP addresses 47
- Finding the MAC address of the i-Vu® web server 48

Using TCP/UDP ports 49
Document revision history 50

What is the i-Vu® Standard/Plus application?

An i-Vu® system is a web-based building automation system that can be accessed from anywhere in the world through a web browser, without the need for special software on the workstation. Through the web browser, you can perform building management functions such as:

- adjust setpoints and other control parameters
- set and change schedules
- graphically trend important building conditions
- view and acknowledge alarms
- run preconfigured and custom reports on energy usage, occupant overrides, and much more

	i-Vu® Standard	**i-Vu® Plus**
Part number	CIV-OPN	CIV-OPNPL
Networks supported	BACnet and CCN	BACnet and CCN
Routing devices	• USB-CCN Adapter • USB-MS/TP Adapter • Open/CCN routers • Carrier® ChillerVu™ • i-Vu® XT Router • TruVu™ routers	• USB-CCN Adapter • USB-MS/TP Adapter • Open/CCN Routers • Open/CCN Links • Carrier® ChillerVu™ • i-Vu® XT Router and Link • TruVu™ routers
Maximum controllers supported	750	750
Trend storage	7 days	62 days
Alarms storage	500	500
Audit Log storage	30 days	30 days
Custom Equipment and Trend Reports		✓
Tenant Override Billing Reports		✓
Weather Add-on		✓
Web Services (XML/SOAP) Data Access		✓
BACnet/Modbus®/LonWorks® integration		✓

CARRIER CORPORATION ©2020
All rights reserved

i-Vu® Standard and Plus web server specifications

i-Vu® web server NUC7I3DNHE	
Operating temperature	32°F to 104°F (0°C to 40°C). For indoor use only
Storage temperature	-4°F to 104°F (-20°C to 40°C)
Storage humidity	5% to 90% RH
Weight	2.4 lb (1.09 kg)
Dimensions	4.52 in. (115 mm) deep x 4.37 in. (111 mm) wide x 1.9 in. (48.7 mm) high
USB ports	4 USB 3.0 ports for i-Vu® network connection or for backing up/restoring system data
LAN port	Integrated Intel® 10/100/1000 Mbps port for Ethernet
VESA mounting plate	Attach the web server to the back of a flat monitor
Display Ports	2 HDMI ports to connect to a monitor for troubleshooting
Safety Compliance	IEC, UL, EN, CAN/CSA
Environmental Compliance	RoHS 2011/65/EU, WEEE 2002/96/EC, China RoHS MII Order #39
EMC Compliance	FCC CFR Title 47, Chapter I, Part 15, Subparts A, B

i-Vu® tools

Develop and configure graphics and a system database for your i-Vu® system using the following i-Vu® tools.

NOTE The i-Vu® tools have a built-in license that expires 2 years after the software is released. Contact Carrier Control Systems Support for updates concerning your license.

Use...	To...
ViewBuilder	Create or edit graphics

Tech tools for the Installer only:

Use...	To...
EquipmentBuilder	Build or edit control programs (.equipment files) for programmable controllers. Can also produce graphics, sequence of operation, and screen files
Alarm Notification	Receive a message on any networked computer that is running the i-Vu® Alarm Notification Client application
Virtual BACview®	View and change property values and the controller's real time clock

CARRIER CORPORATION ©2020
All rights reserved

Use...	To...
BBMD Configuration Tool	Configure BACnet/IP Broadcast Management Devices (BBMDs) **NOTE** If your system has multiple routers that reside on different IP subnets, you must set up one router on each IP subnet as a BACnet/IP Broadcast Management Device (BBMD).
MSTP Capture Utility	Capture BACnet traffic on MS/TP. It is intended for situations where Carrier Control Systems Support needs a network capture to troubleshoot communications.
Test & Balance	• Calibrate airflow in a VAV or VVT Zone controller • Calibrate the static pressure in a VVT Bypass controller • Commission air terminals • Override reheat and terminal fans **NOTE** Use Test & Balance to manipulate the controllers associated with an air source, but not the air source itself, or heating and cooling equipment, such as chillers and boilers.
Snap	Build custom control programs using individual blocks of programming code called microblocks
LonWorks Integration Tool	Generate the microblock addresses automatically for third-party LonWorks points
AppLoader	Use to download .clipping files to restore factory defaults and check **Module Status** (Modstat) through the Rnet port
Field Assistant	Service or start up and commission a piece of equipment or a network of controllers.

CARRIER CORPORATION ©2020
All rights reserved

What's new in v7.0?

What's new in the i-Vu® Standard/Plus application

Feature	Improvement
New web server	Model NUC7i3DNHE - New look with same functionality
Management Tool security enhancements	• Management Tool automatically locks out the user for 30 minutes after 5 unsuccessful login attempts. • Management Tool automatically locks out the user after 30 minutes of inactivity. • New option to Redirect HTTP requests to HTTPS.
i-Vu® security enhancement	Security in the Management Tool and the i-Vu® web server increased by the user installing browser self-signed certificates.
v7.0 cumulative update #3	
New fields in System Options	The General tab now shows the System Language and lets you choose the number of levels to show in i-Vu® paths.
v7.0	
Custom reports	i-Vu® Plus only - v7.0 custom reports are managed through the new Report Manager. You can export one or more custom reports to a file so that they can be imported into another system. A custom report can provide data for the following new items on a Graphics page: • Data table • Chart • Color map See *What's new in the ViewBuilder application* (page 5) for more information on the above items. **NOTE** To support upgraded systems, you can still create and access legacy (v6.5 and earlier) custom reports.
Scheduled Reports	i-Vu® Plus only - You can set up a report to run on a recurring basis. The report is saved as a file (PDF, CSV, or XLS), and you can choose to have it automatically emailed to someone.
Email Server Configuration	The Email Server Configuration settings, used by scheduled reports and the Send Email alarm action, are now located on the **System Options** > **General** tab.
Send Email alarm action	This alarm action can use the default Email Server Configuration settings defined in **System Options**, or you can enter settings specific to the alarm action.
New FDD alarm categories	i-Vu® now has two new alarm categories, FDD Comfort and FDD Energy.

CARRIER CORPORATION ©2020
All rights reserved

Feature	Improvement
Add-ons	The i-Vu® Plus application now allows only signed add-ons that are supported by Carrier. The i-Vu® Standard application does not support add-ons.
WAP device support	This has been removed from the i-Vu® application. Smart phone support introduced in v6.5 replaced this functionality.

What's new in the ViewBuilder application

Feature	Improvement
Local Variables	ViewBuilder now preserves local variables through cut/copy and paste, as well as when importing a .viewsymbol.
Layers	• ViewBuilder now preserves layers when importing a .viewsymbol. • If cutting/copying a selection assigned to layers, you must hold Shift while pasting in a new file to preserve layer assignments.

CARRIER CORPORATION ©2020
All rights reserved

Setting up i-Vu® client devices and web browsers

The i-Vu® system can be viewed on the following client devices and web browsers.

Computers

The client computer should have at least:
- Dual core processor
- 1.5 GB RAM
- Communications link of 10 Mbps or higher

The i-Vu® application will work with slower computers and slower links, but the results may not be satisfactory.

A computer with this operating system...	Supports these web browsers...
Windows®	Google™ Chrome™ v66.0 or later [1]
	Internet Explorer® v11 Desktop
	Microsoft® Edge v40 or later
	Mozilla® Firefox® v60.0 or later
Mac® OS X® (Apple® Mac only)	Safari® v11 or later [2]
	Google Chrome v66.0 or later
	Mozilla Firefox v60.0 or later
Linux®	Google Chrome v66.0 or later
	Mozilla Firefox v60.0 or later

1 Best performance

2 Best performance unless browser is running on a Mac® Mini or a MacBook:

WARNING If machine is running Mountain Lion 10.8x with an integrated Intel HD 400 graphics card, it will experience display issues. Use one of these workarounds for better performance:

- If an additional NVIDIA graphics card is available, manually switch the graphic card setting in MAC® OS X® to use that card.
- If not, use Google™ Chrome™ v66.0 or later.

Mobile devices

Device type	Platform support
Smart phone	Android™, iOS
Tablet	Android™, iOS, Surface™

NOTE Some functionality may be limited by the capability of the mobile device and operating system.

CARRIER CORPORATION ©2020
All rights reserved

Setting up and using a computer with the i-Vu® system

- Set the monitor's screen resolution to a minimum of 1920 x 1080 with 32-bit color quality
- You may want to disable the computer's navigation sounds.

Mac only

NOTE The instructions below are for a Mac OS X 10.8. Other versions may vary slightly. See your computer's Help if necessary.

Computer settings	To change setting...
Enable right-clicking to see right-click menus:	
On a Mac	**1** Select **System Preferences** > **Mouse**. **2** Click the drop-down list that points to the mouse's right-click button, then select **Secondary Button**.
On a MacBook	**1** Select **System Preferences** > **Trackpad**. **2** Enable **Secondary click**.

The instructions in Help are for a Windows computer. For instructions that include the **Ctrl** key, replace **Ctrl** with **Command**. For example, replace **Ctrl+click** with **Command+click**.

Setting up and using a web browser to access the i-Vu® interface

After installing and connecting to the i-Vu® application and Management Tool, every computer that will be used to access the application and the Management Tool must install 2 self-signed certificates for your browser. See *Install self-signed certificates for network security* (page 20).

NOTE Thei-Vu® application installer must make sure certificates are installed on the users' computer(s).

To set up and use Internet Explorer

NOTES

- The instructions below are for Internet Explorer® 11. Other versions may vary slightly. See your web browser's Help if necessary.
- If the menu bar is not visible, right-click on the window's header, and then select **Menu bar**.

CARRIER CORPORATION ©2020
All rights reserved

Web browser settings	To set in Internet Explorer...
Accept First-party and Third-party cookies	**Tools** > **Internet Options** > **Privacy** > **Advanced** button
Automatically check for newer versions of stored pages	**Tools** > **Internet Options** > **General** > **Browsing history** > **Settings** button
Load ActiveX Control	**Tools** > **Internet Options** > **Security** > **Custom Level** button. Under **ActiveX controls and plug-ins**, set the following: • **Download signed ActiveX controls** > **Prompt** • **Download unsigned ActiveX controls** > **Disable** • **Run ActiveX controls and plug-ins** > **Enable** • **Script ActiveX controls marked safe for scripting** > **Enable**
Select Play animations in web pages	**Tools** > **Internet Options** > **Advanced** > under **Multimedia**
Disable all the options on the Explorer Bar	**View** > **Explorer Bars**
Disable web browser's pop-up blockers	**Tools** > **Pop-up Blocker** > **Turn Off Pop-Up Blocker**
Disable external toolbar pop-up blockers	Varies
Hide the web browser's toolbars	**View** > **Toolbars**

To...	Do the following...
Maximize the web browser window	Press **F11** to turn full-screen mode on\off, or use the minimize/maximize button in the top right corner of the browser window.
Have 2 different users logged in to the i-Vu® system on the same computer	Start a new web browser session. Select **File** > **New Session**.
Clear browser cache	**1** Select **Tools** > **Internet Options**. **2** Click **Delete**. **3** If you had the i-Vu® system saved as a Favorite, uncheck **Preserve Favorites website data**. **4** Click **Delete** again.

To set up and use Microsoft Edge

The instructions below are for Microsoft® Edge.

Web browser settings	To set in Microsoft Edge...
Do not block cookies	**More Actions** > **Settings** > **View Advanced Settings** > **Cookies**
Disable web browser's pop-up blockers *	**More Actions** > **Settings** > **View Advanced Settings** > **Block pop-ups**

CARRIER CORPORATION ©2020
All rights reserved

To...	Do the following...
Maximize the web browser window *	Use the minimize/maximize button in the top right corner of the browser window.
Have 2 different users logged in to the i-Vu® system on the same computer *	**More Actions** > **New Window**
Clear browser cache	**More Actions** > **Settings** > **Clear browsing data** > **Clear**

* Does not apply to Microsoft Edge on a phone.

To set up and use Mozilla Firefox

NOTES

- The instructions below are for Mozilla® Firefox® v60.0 on a Windows operating system. Other versions may vary slightly. See your web browser's Help if necessary.
- If the menu bar is not visible, right-click on the window's title bar, and then select **Menu bar**.
- If a message appears in the i-Vu® interface that includes the checkbox **Prevent this page from creating additional dialogs**, DO NOT check this box.

Web browser settings	To set in Firefox...
Disable Pop-up blocker	**1** Click **Tools** > **Options** > **Privacy & Security**. **2** Under **Permissions**, click **Exceptions** next to **Block pop-up windows**. **3** Type `http://` (or `https://`) and then the server name or IP address of your system. **4** Click **Allow** and then **Save Changes.**
Enable JavaScript	**1** In the address bar, type `about:config`, and then press **Enter**. **2** Click **I accept the risk**. **3** In the **Search** bar, type `javascript.enabled`. **4** If the value field shows **true**, JavaScript is enabled. If it shows **false**, right-click **javascript:enabled**, and then select **Toggle**.
Add-ons Manager	Select **Tools** > **Add-ons** > **Extensions**. On this page, you can enable/disable installed add-ons such as: • Adobe® Acrobat® Reader (to view PDF's) • QuickTime Plug-in (to play audible alarms) Only installed Firefox add-ons will show up in the list.

CARRIER CORPORATION ©2020
All rights reserved

To...	Do the following...
Maximize the web browser window	Press **F11** to turn full-screen mode on\off.
Clear browser cache	1 Click **Tools** > **Options** > **Privacy & Security**. 2 Under **Cookies and Site Data**, click **Clear Data**. 3 Click **Clear**.
Have 2 different users logged in to the i-Vu® system on the same computer	Start a new web browser session. Select **File** > **New Private Window**.

To set up and use Google Chrome

NOTES

- The instructions below are for Google™ Chrome™ v66.0. Other versions may vary slightly. See your web browser's Help if necessary.
- If a message appears in the i-Vu® interface that includes the checkbox **Prevent this page from creating additional dialogs**, DO NOT check this box.

On a computer

Web browser settings	To set in Chrome...
Enable pop-ups	1 Click on the browser toolbar. 2 Select **Settings**. 3 Click **Advanced** at the bottom of the page. 4 Under **Privacy and security**, click **Content settings**. 5 Under **Pop-ups** > **Allow**, click **ADD**, and then type http:// (or https://) and then the server name or IP address of your system.

To...	Do the following...
Clear browser cache	1 Click on the browser toolbar. 2 Select **More tools** > **Clear browsing data**. 3 Select a time range in the drop-down list. 4 Check the types of information that you want to remove. 5 Click **CLEAR DATA**.
Maximize the web browser window	Press F11 on your keyboard to turn full-screen mode on/off.
Have 2 different users logged in to the i-Vu® system on the same computer	Start a new web browser session. Click , then select **New Incognito window**.

CARRIER CORPORATION ©2020
All rights reserved

On a Google Nexus

Web browser settings	**In the Chrome menu...**
Turn off desktop mode	Uncheck **Request desktop site**
Disable pop-up blocker	**Settings** > **Advanced** > **Content Settings** > uncheck **Block pop-ups**
Enable JavaScript	**Settings** > **Advanced** > **Content Settings** > check **Enable JavaScript**
Enable Cookies	**Settings** > **Advanced** > **Content Settings** > check **Accept Cookies**

To...	**In the Chrome menu...**
Clear browser cache	**Settings** > **Advanced** > **Privacy** > **CLEAR BROWSING DATA**

To set up and use Safari

NOTES

- The instructions below are for Safari® v11. Other versions may vary slightly. See your web browser's Help if necessary.
- We recommend that you do not run Safari in full-screen mode. If you do, i-Vu® pop-ups will open full-screen, covering the main application window.

On an Apple® computer (Mac®)

Web browser settings	**To set in Safari...**
Disable pop-up blocker	**Preferences** > **Security** > uncheck **Block pop-up windows**
Enable JavaScript	**Preferences** > **Security** > check **Enable JavaScript**
Enable Plug-ins	**Preferences** > **Security** > check **Enable plug-ins**
Prevent pop-ups from opening in a new browser tab	**Preferences** > **Tabs** > uncheck **Command-click opens a link in a new tab**
Prevent Safari from automatically opening zip files exported from the i-Vu® application	**Preferences** > **General** > uncheck **Open "safe" files after downloading**

To...	**Do the following...**
Clear browser cache	**History** > **Clear History**
Have 2 different users logged in to the i-Vu® system on the same computer	Start a new web browser session. Select **Safari** > **Private Browsing** > **File** > **New window**

CARRIER CORPORATION ©2020
All rights reserved

On an Apple® iPad

Web browser settings	To set on the iPad...
Disable pop-up blocker	**Settings**> **Safari** > set **Block pop-ups** to **Off**
Enable JavaScript	**Settings** > **Safari** > set **JavaScript** to **On**


TIP Re-enable popup blocking on your device when not using our software.

To...	Do the following...
Clear browser cache	**Settings** > **Safari** > **Clear History**


TIP Re-enable popup blocking on your device when not using our software.

On an Apple® iOS 12.2

Web browser settings	To set on the iPhone...
Enable JavaScript	**Settings** > **Safari** > **Advanced**

CARRIER CORPORATION ©2020
All rights reserved

Before starting the i-Vu® application and your system

NOTE These instructions are typically for a computer with a Microsoft® Windows operating system. If you have a different operating system, some instructions may vary slightly. See your operating system's Help for more information.

You must complete the following steps BEFORE installing i-Vu®.

Step 1: Install Tools and have documentation ready

1. Follow the rest of this document to set up your entire system.
2. Insert the **Tech Tools** USB drive into your computer and wait until the Installation screen appears. If this screen does not appear, open **My Computer** and double-click **Tech Tools**.
3. Click the utilities you wish to install. Depending on how security and permissions are configured on your Windows computer, you may need to right-click the executable file and select **Run as Administrator**. For example, to install Tech Tools, right-click **i-Vu_Tools_v7.0_windows_setup.exe** and select **Run as Administrator**.

   NOTE Documentation and some utilities are not copied to the hard drive. We recommend that you copy the **Tech Tools** USB contents to a folder on your hard drive. This ensures that you have the documentation and utilities when you need them.
4. Print the the *i-Vu® Owner's Guide*.

Step 2: Install device managers and routers

If you haven't already, download the *Installation and Start-up Guides* from the Carrier support website.

Make sure you:

- Mount and wire your CCN device manager(s)*, Open, i-Vu XT, or TruVu router(s).
- Wire the ports for communication and set DIP switches.
- Set up IP addressing, including BACnet/IP Broadcast Management Devices (BBMDs).

  NOTE If your system has multiple routers that reside on different IP subnets, you must set up 1 router on each IP subnet as a BACnet/IP Broadcast Management Device (BBMD's). See the *BBMD Utility User Guide* for details.
- Configure BACnet device instance and network number for Open routers using PuTTY or Hyperterminal connected to the Rnet or S2 port. See Communicating using PuTTY or Communicating using Hyperterminal.
- Configure BACnet device instance and network numbers for i-Vu XT and TruVu routers using an Ethernet cable attached to the router's Service Port. See the individual router's *Installation and Start-up Guide* for details.

*If you have multiple CCN Gateways, you must use the i-Vu® Pro application with the required license.

CARRIER CORPORATION ©2020
All rights reserved

Step 3: Use Network Service Tool V to ensure hardware is communicating on the CCN network

1 Connect the 3-terminal connector of the Network Service Tool's **USB to CCN Converter** to Port **S1** on the i-Vu® device manager.

Carrier USB to CCN converter (top CCN Port)	**i-Vu® device manager** (Port S1)
+	Net+ (Pin 1)
G	Signal Ground (Pin 5)
-	Net- (Pin 2)

2 Launch **Network Service Tool** and connect to the i-Vu® device manager. Each i-Vu® device manager defaults to Gateway functionality and has a CCN address of **0, 1**.

CAUTION Every CCN device must have a unique CCN address on the CCN network! Do not use Bus **0**, Element **238**, as it is automatically assigned to the i-Vu® web server.

3 Find the device manager at 0,1 using **Address Search** and change the device manager's CCN address as desired.

NOTE We do not recommend leaving a device manager's CCN address at 0,1, because this is the address that it defaults to when formatted.

4 Upload the i-Vu® device manager.

5 Access the **Service Configuration Table** IP_CONF to enter the following configuration options:

NOTE A static IP address is required, as DHCP is not supported.

- **Host IP Address** - enter the device manager's IP address, provided by the LAN administrator (allowable entries for xxx.xxx.xxx.xxx: xxx is a decimal number between 0 - 255)
- **Subnet Mask** - enter the device manager's IP address, provided by the LAN administrator (allowable entries for xxx.xxx.xxx.xxx: xxx is a decimal number between 0 - 255)
- **Default Gateway** - enter the IP Gateway's IP address, provided by the LAN administrator (typically a router on the Ethernet LAN).

CCN ENET Configuration

Device Type

- Select **0** if this device manager is the Gateway. (**NOTE** Only 1 Gateway is permitted per system.)
- Select **1** if this device manager is the Bridge.

If using the router as a Bridge, enter **CCN/Ethernet Gateway IP** (the IP address of the i-Vu® device manager that is configured as the Gateway). This is the same address that was entered in the **Host IP address** for the CCN Gateway.

NOTE Record the IP address of the Gateway, because you need it to install your i-Vu® system.

6 Repeat the above steps for every i-Vu® device manager used in the CCN system.

CARRIER CORPORATION ©2020
All rights reserved

Step 4: Get your systems ready

CCN

1. Have the IP address of the external Gateway, if you are not using the USB CCN Adapter.
2. Have a list of all of the devices at your job site, along with the name of each device, the bus and element numbers, and their respective locations.
3. For a retrofit project, which is already using CCN global and network schedules, you must have a list of all existing CCN schedule numbers, systems using global and network schedules, and all global schedule masters.
4. Verify that each device has a unique element number because duplicates will not install correctly.

    **CAUTION** Do not use Bus 0, Element 238. It is automatically assigned to the i-Vu® web server.

BACnet

1. Create a list of all of the i-Vu® Open or XT routers and controllers at your job site, with their BACnet Device ID's, IP addresses (where applicable), BACnet network numbers, and the physical location of all devices.
2. Verify that every router has a unique address because duplicates will not install correctly.

See i-Vu® Help for more information about setting schedules in the i-Vu® interface.

CARRIER CORPORATION ©2020
All rights reserved

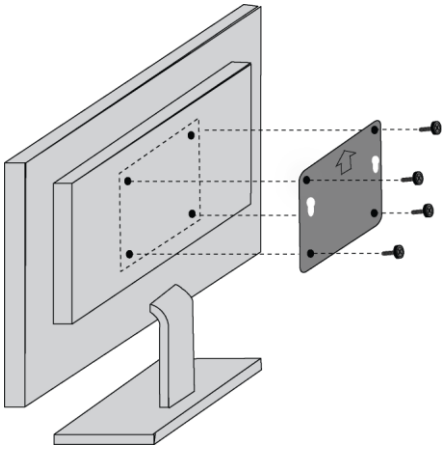
Starting up an i-Vu® Standard/Plus web server

Optional: Mount the web server to a flat panel display

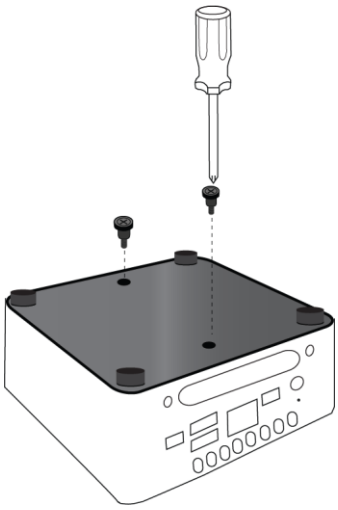
The i-Vu® web server comes with an optional VESA mounting plate and screws. You can mount it directly onto the back of a flat display panel, such as a flat screen TV, monitor, or wall.

1 Screw the mounting plate to the holes on the back of the display panel.

NOTE The arrow on the plate must be pointing straight up.

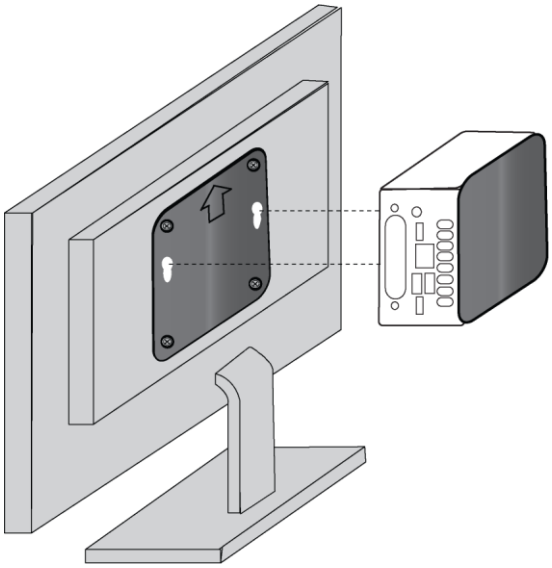


2 Insert the stand-off screws into the bottom of the web server.



CARRIER CORPORATION ©2020
All rights reserved

3 Insert the extruding stand-off screws into the holes on the mounting plate and slide down into place.

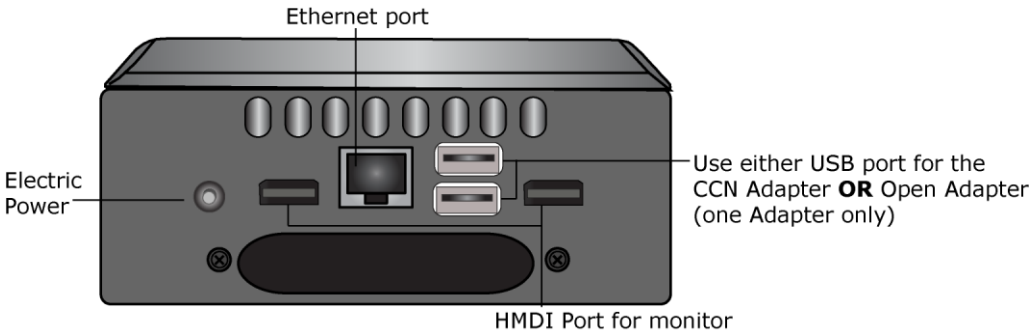


4 Follow the instructions for connecting cables and powering the web server.

Connect and power up web server

WARNINGS!

- Do NOT change the BIOS settings in any way or the software will fail.
- Mount your i-Vu® web server in an air conditioned space to avoid damage.
- Do NOT open the i-Vu® web server! Opening the web server voids your warranty.



CARRIER CORPORATION ©2020
All rights reserved

1 Attach your country's electrical adapter plug onto the power cable.

2 Plug the power cable into the back of the i-Vu® web server and into an electrical outlet.

NOTE We highly recommend using a UL Certified power surge/RFI suppression device.

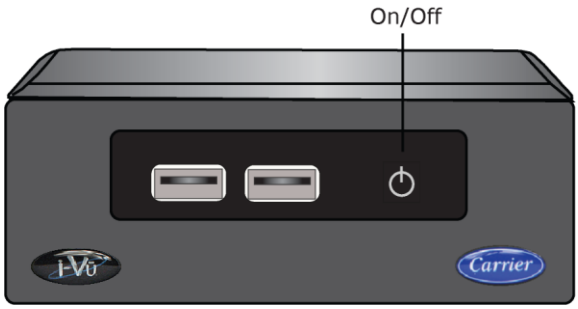
3 Connect an Ethernet cable from the laptop, computer's network port, or the customer's LAN, to the Ethernet jack on the back of the i-Vu® web server.

NOTE Your computer must be configured for DHCP if connecting directly to the i-Vu® web server.

4 If you are using the USB Adapter (CCN or Open) to connect to your network, plug the adapter into any of USB ports and connect to your network. You can only use **one** adapter at a time on the web server.

NOTE The Open Adapter connects to a BACnet over MS/TP network and NOT a BACnet over ARCNET network.

5 Press the **On/Off** Button to turn on the i-Vu® web server.



Access the startup screen

NOTES

- Use only the i-Vu® interface to navigate through the i-Vu® application; do not use the browser's navigation buttons.
- Disable all popup blockers. **Internet Explorer** > **Tools** > **Popup Blocker**, Google, and Yahoo Toolbars, etc.

1 Launch the browser and type **http://ivu** to reach the startup screen. If the i-Vu® startup screen does not appear, see *Troubleshooting* (page 32).

2 Accept the terms of the License Agreement and click **Next**.

3 Fill in all required fields:

Create Installer Account

- **Login Name** - not case sensitive, accepts spaces and special characters
- **Password** - you must enter a password (8 character minimum). You cannot leave it blank.

CARRIER CORPORATION ©2020
All rights reserved

System Settings

Network Name

- Controls the name used to access your system from the Internet or network (LAN)
- Is case sensitive and should not contain special characters or spaces
- If you change the network name from "ivu", make note of the change in the i-Vu® Owner's Guide

System Name

- Enter your organization/building name; this becomes the top level in the navigation tree.
- This can be changed later from the Installer view in the **Arrange User View** window.

USB Network Type

- Enter the type of network connection you are using. If you are using a USB Adapter, make sure that it is plugged into the web server and that you select the CCN or BACnet option.

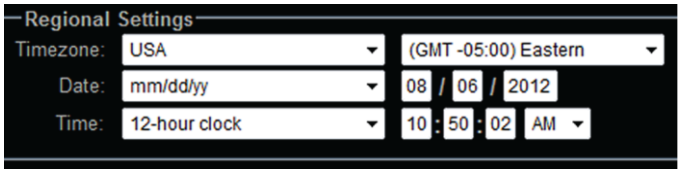
  If you decide to use a USB CCN or BACnet adapter at a later date, after your system is configured without one:

  USB CCN adapter - Requires restoring your system to factory defaults, which results in losing all your system data.

  USB BACnet adapter - Your data is not lost, however, you must restart the web server after the adapter is plugged in. If you have both external Open routers and the USB BACnet adapter, and the USB Network Address is using an internal loopback address of 127.0.0.1, you must assign a new IP address to the USB Network Address in the Management Tool and then restart the web server.

Regional Settings

- **Timezone, Date** - select appropriate options
- **Time** - enter the correct time! The i-Vu® web server will **not** automatically read the time from your computer.



4 Click **Next**.

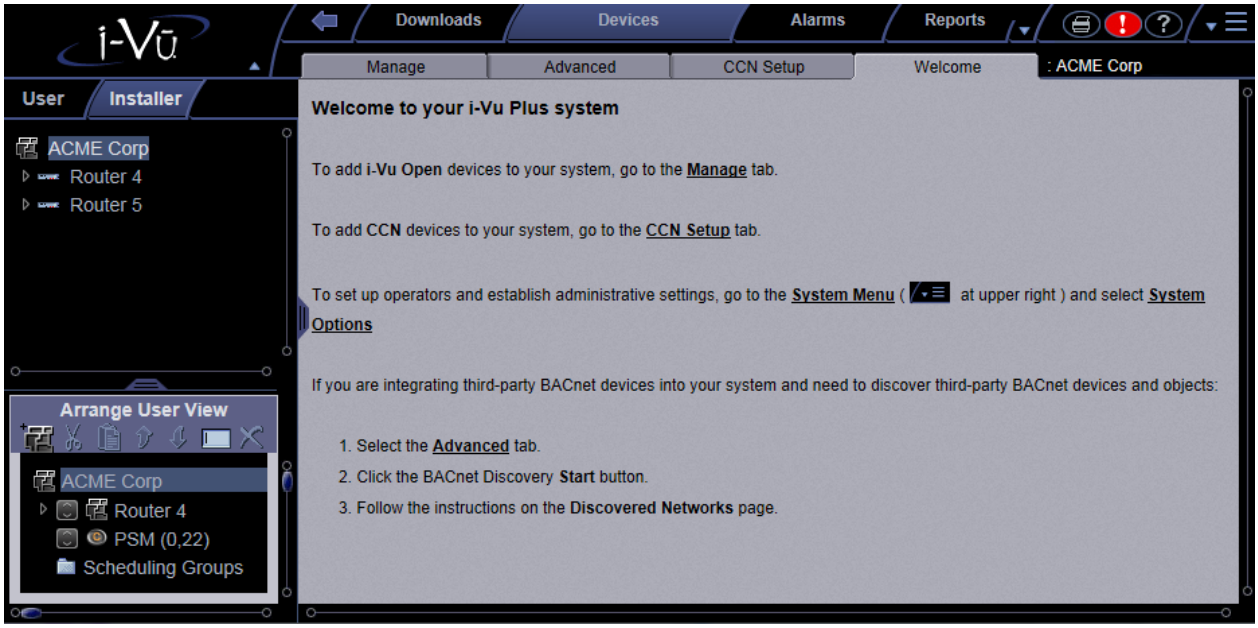
5 Review entries. Click **Submit**. Wait for your system to launch. It will take a minute. If you get an error, type http://<your system name> in your browser and refresh. Click **Next**.

6 Click  and select **Log out**.

IMPORTANT We recommend that you stop setting up your system in the i-Vu® application until you have *installed self-signed certificates* (page 20) to increase the security of your system. After installing the certificates, you should always use `https` instead of `http`.

CARRIER CORPORATION ©2020
All rights reserved

When you launch the i-Vu® application from your browser, using `https`, the **Welcome** page provides basic instructions to get started. Refer to Help in the i-Vu® interface for detailed instructions on navigating, finding your routers and controllers, configuring properties, trends, alarms, reports, and much more.



Install the Install self-signed certificates for network security

For security purposes, you must install a self-signed certificate on every computer used to access the i-Vu® application using "https". A user who has the **Installer Role** and will be accessing the **Management Tool** needs a second certificate.

You will get a browser certificate error when using "https" to access the i-Vu® application and the Management Tool until you install the certificates on your computer.

IMPORTANT We highly recommend that you have the appropriate browser certificates in place **before** finding and uploading your devices and building your system in the i-Vu® application.

CAUTION If you ever change the Network Name, the IP address, or DNS IP address, you must download both certificates again.

CARRIER CORPORATION ©2020
All rights reserved

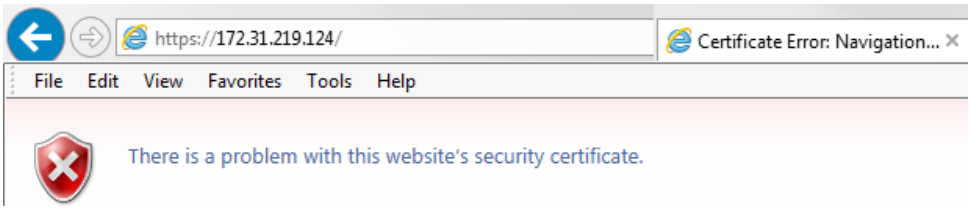
The i-Vu® application

1 After setting up the information on the **Startup** screen, log out.

2 Launch your browser and type https://<your system name> or Server IP address. For ex.: https://ivu/ or https://172.21.319.123.

NOTE Use the TLS indicator `https` instead of `http`.

3 There will be a certificate error in your browser. Follow the steps listed below to install a certificate for the browser you are using to access the i-Vu® application.



The Management Tool

After installing the certificate for browsing to the i-Vu® application, you must install another one for accessing the Management Tool.

1 Log out of the i-Vu® application.

2 Launch your browser and type your system name or Server IP address followed by **:8080.** For ex.: https://ivu:8080/ or https://172.21.319.123:8080

3 You will see a certificate error again. Follow the directions below for the browser you are using.

Instructions to install a self-signed certificate

Internet Explorer®

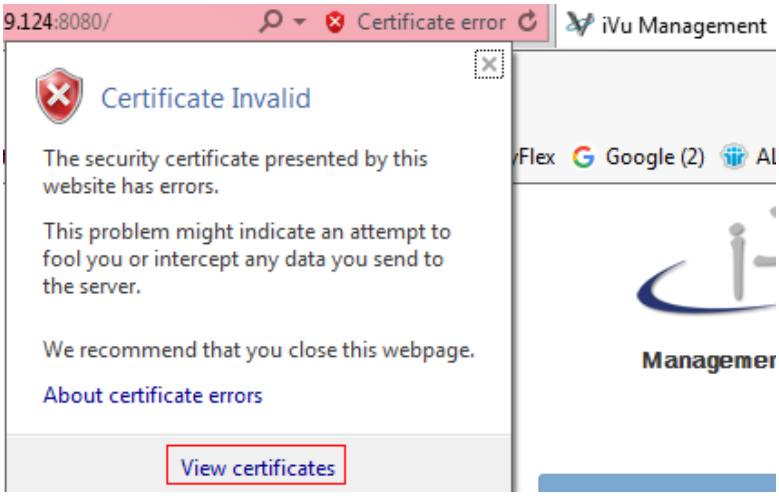
1 If the page displays **There is a problem with this website's security certificate**, click **Continue to this website**.

2 Enter your **Username** and **Login**.

3 In the address bar, click **Certificate Error**.

CARRIER CORPORATION ©2020
All rights reserved

4 Click **View Certificates** to open the Certificate dialog.



5 On the **Details** tab, select **Issuer**, then click **Copy to File**.

6 In the **Certificate Export Wizard**, click **Next** and **Next** again.

7 Browse to the folder on your computer that you want to save the certificate in, enter a name, then click **Next**.

8 Click **Finish**.

9 Click **OK** to close the message **The export was successful**.

10 Click **OK** to close **Certificate** window.

11 To import the certificate, Select **Tools** or > **Internet Options**.

12 On the **Content** tab, click **Certificates**, and then select **Trusted Root Certification Authorities** tab.

13 Click **Import**.

14 Click **Next** in the **Certification Import Wizard**.

15 Browse to the certificate you saved and click **Open**, then **Next**.

16 Select **Place all certificates in the following store**.

17 Click **Browse** and select **Trusted Root Certification Authorities**.

18 Click **Next**.

19 Click **Finish**.

20 Click **Yes** in the **Security Warning** dialog box to install the certificate.

21 Click **OK**.

22 Click **Close** again and then **OK**.

23 Close Internet Explorer, then open it again.

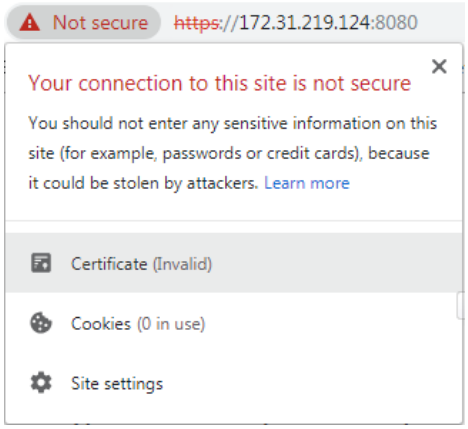
24 Log in to the i-Vu® application.

NOTE Chrome and Windows browsers use the same Certificate store, so it is not necessary to install a certificate obtained through Internet Explorer in a Chrome Browser used on the same computer.

CARRIER CORPORATION ©2020
All rights reserved

Google™ Chrome™

When connecting to the i-Vu® application or Management Tool without a self-signed certificate installed, you will see the following.



1 Export certificate to a known location:

a) In the address bar, click **Not secure**.

b) Click **Certificate (Invalid)** to open the Certificate dialog.

c) On the **Details** tab, select **Issuer**, then click **Copy to File**.

d) In the **Certificate Export Wizard**, click **Next** and **Next** again.

e) Browse to the folder on your computer that you want to save the certificate in, enter a name, click **Save**, then **Next**.

f) Click **Finish**.

g) Click **OK** to close the message **The export was successful**. and click OK again to close the **Certificate** dialog.

2 Import saved certificate:

a) Click on the browser toolbar, then select **Settings**.

b) Click **Advanced**.

c) Scroll down to **Privacy and security**, then click **Manage certificates**.

d) On the **Trusted Root Certification Authorities** tab, click **Import**.

e) In the **Certificate Import Wizard**, click **Next**.

f) Click **Browse**, then select the file you exported in step 2.

g) Click **Open**.

h) Click **Next**, and **Next** again, then **Finish**.

i) Click **Yes** to the Security Warning popup, then **OK** to the **Import was successful** message.

j) Close the **Certificates** window.

k) Close Chrome, then open it again.

NOTE Chrome and Windows browsers use the same Certificate store so it won't be necessary to install this same certificate in a Window Browsers used on the same PC.

CARRIER CORPORATION ©2020
All rights reserved

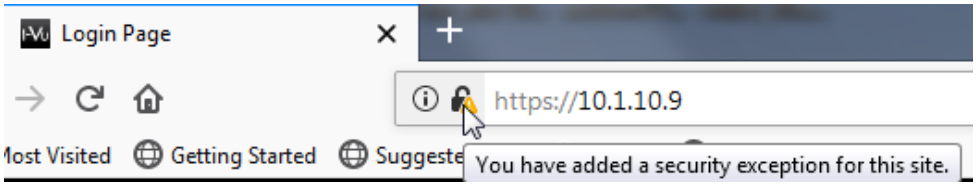
Mozilla® Firefox®

1 Open the i-Vu® application or the Management Tool using Mozilla® Firefox®.

2 Click the **Advanced** button on the page stating **Warning: Potential Security Risk**.

3 Click **Accept the Risk and Continue**.

4 Firefox displays the following icon near the URL window indicating that an exception has been made for this site



Configure i-Vu® IP addresses

The i-Vu® application is set by default to automatically obtain its IP configuration information using DHCP. Once thei-Vu® web server is initially started up, you can connect it to a building LAN that supports DHCP (assuming a DHCP server is available). If the site requires a static IP address for thei-Vu® web server, this information should be provided by the customer and must be assigned to the i-Vu® web server in the Management Tool.

NOTES

- If you need to assign your own IP addresses, see Configure i-Vu® using static IP addresses.
- If you are having problems with a DHCP Server that will not assign two IP addresses to one network card or MAC address, see *If DHCP will not assign two IP addresses* (page 47).
- If using a loopback address, refer to *Using a loopback address* (page 47) for important details.

Configure the i-Vu® system using static IP addresses

NOTE If using a loopback address, refer to *Using a loopback address* (page 47) for important details.

1 In the i-Vu® interface, open the **Management Tool**. Click , then select **System Options** > **General** tab > **Management Tool**, or through your browser by typing your system name or IP address followed by :8080
For ex.: https://ivu:8080, https://<ip address>:8080 https://<networkname>:8080

2 Enter your login and password.

3 Remove the check by **Obtain an IP address automatically** and enter the **I-Vu Address**, **Subnet Mask**, and **Default Gateway**.

4 Enter the **DNS Address**.

CARRIER CORPORATION ©2020
All rights reserved

5 You must enter a fully qualified domain name in the **Domain** field if you want the i-Vu® application to be able to email alarms. Otherwise, you can leave the field blank.

6 Enter a **USB Network Address**.

NOTE You may use an internal loopback address of 127.0.0.1 in this field only if a USB Adapter **or** external routers are used. If you use both the USB Adapter and external routers, the loopback address should not be assigned to the **USB Network Address**. Instead, configure the **USB Network Address** with an appropriate IP address for the subnet that the i-Vu® web server is on.

7 If NTP is enabled, enter NTP server addresses. See Management Tool for detailed instructions.

8 Click **Apply Changes**.

NOTE If the i-Vu® web server was connected directly to a computer when configured, applying changes in the Management Tool will most likely result in the computer being on a different IP subnet than the i-Vu® web server. In this case, the connection to the i-Vu® web server will be lost. To regain communication with the i-Vu® web server, you must configure the IP address of the computer to be on the same subnet.

Management Tool

You can access **Management Tool** by either:

- Clicking  and selecting **System Options** > **General** tab > **Management Tool** button
- Launching your browser and typing your system name followed by **:8080.** For ex.: https://ivu:8080/

You must *install a self-signed certificate* (page 20) to securely access the **Management Tool**. You must install another one for the web server.

NOTES

- The Management Tool is password-protected and can only be accessed by a user with Installer role.
- After 5 invalid login attempts, the user will be locked out for 30 minutes.
- If multiple users are in the Management Tool at the same time, only the first one to access it is able to make changes. Other users see it in View Only mode.
- If you are in the Management Tool and inactive for 30 minutes, you will be logged out. You must refresh the browser and log back in.

System Status	
i-Vu is running at:	This is used to troubleshoot server or LAN communications. Click the **Stop Server** button to stop the i-Vu® web server. When stopped, the button changes to **Start Server.** Do NOT close the Management Tool before restarting the server. Click to restart.
Weekly system logs:	• **System** - used for troubleshooting (same as logs available from **System Options > General** tab). Logs are available for a maximum of 4 weeks. • **Kernel** - operating system logs

CARRIER CORPORATION ©2020
All rights reserved

Addressing	**CAUTION** If you change the name or the IP address of your system, record the numbers in a secure place. • **Name** - Controls the name used to access your system from the Internet. Do not use special characters or spaces. • **Obtain an IP address automatically -** Uncheck this to manually assign addresses for the following: ○ i-Vu Address ○ Subnet Mask ○ Default Gateway ○ DNS Address - IP address of the Domain Name Server ○ Domain - Host name of the domain ○ USB Network Type - Read-only field shows either CCN or BACnet types. ○ USB Network Address - IP address of the internal BACnet router or the internal CCN Gateway
i-Vu Port Configuration	Changing these values forces a web server restart. Default values: **HTTP:** 80 **HTTPS:** 443 **Redirect HTTP requests to HTTPS** - Check this field to have all HTTP requests automatically redirected to the more secure HTTPS.
Operation Status	Message showing progress of background operations, such as backup and restore.
Manage Server Data	• **PC Backup** - Saves the entire database zipped into one file to your computer. • **PC Restore** - Replaces the current server data with a backup from your computer. • **USB Backup** - Saves the entire database zipped into one file onto a USB inserted into the i-Vu® web server. • **USB Restore** - Replaces the current server data with a backup from your USB inserted into the i-Vu® web server. • **Compress System** - Creates more storage space for trend data. • **Factory Defaults** - Deletes all server data and resets the device to the original factory default values. **NOTE** Executing this option does not delete configuration data under the **Addressing** and **i-Vu Port Configuration** sections of the Management Tool.
Machine Maintenance	• **Management Version -** Apply .update file from here. • **Reboot -** System restart

Configuring NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization. You can designate an NTP source that sends the correct time to the i-Vu® web server, ensuring constant accurate time. You can enter 2 static addresses (DNS name or IP) of NTP servers or use the default addresses provided by the i-Vu® application. If you do not enable NTP, the i-Vu® system clock must be monitored and updated regularly in **System Options** > **General** tab.

You can configure DHCP servers to supply IP addresses of NTP servers to the i-Vu® web server. If you have checked **Obtain an IP address automatically** and **Enable Time Synchronization**, the i-Vu® web server tries to obtain an NTP server address from the DHCP server on site. If it cannot find one, the i-Vu® web server uses the User Assigned NTP addresses, if any, in the User Assigned fields.

CAUTION Contact your Network Administrator for guidance in entering these settings.

CARRIER CORPORATION ©2020
All rights reserved

You can access NTP from a local server, a remote server, or a website. To set up NTP:

1 Verify that **Enable time synchronization from an NTP server** is checked.

2 **System Assigned NTP Server Address** - To use this read-only field, make sure you have checked **Obtain an IP address automatically** to allow your system to search for an address for the NTP server and display a primary and alternate address.

3 **User Assigned NTP Server Address** - You can use the default website addresses if your system allows it. Firewalls may prevent successful access to the default websites. Your Network Administrator can provide alternate addresses for a local server, a remote server, or a website.

Set up login and passwords for an additional user

Add new operators and assign an appropriate role to them. You must make a note of this or you could be locked out of your system if no one knows any of the user names and passwords.

We recommend that you

- Assign the **Administrator** role for the main system user.

  NOTE For security purposes, do not use `administrator` as the login name.

- Create a user with the **Installer** role, who will be commissioning the system.

  NOTE For security purposes, do not use `installer` as the login name.

- Use the chart below or the Help to become familiar with the viewing and editing capabilities of each role.
- Be sure to record the user name and password for the first operator in the i-Vu® **Owner's Guide**.
- You cannot leave the password blank for the Tenant Override Billing application. (Available for i-Vu® Plus only.)

Operators tab

Select the necessary settings and assign **Roles** (access rights) to set up operators.

NOTES

- Optimal number of simultaneous users:
  - 2 in the i-Vu® Standard application
  - 10 in the i-Vu® Plus application
- We highly recommended that only 1 user at a time commission the system.

CARRIER CORPORATION ©2020
All rights reserved

To add or edit operators, passwords, and roles

1 Click , then select **System Options**.

2 Select **Operators** tab.

3 Click **Add** to enter a new operator, or, select an operator to edit his settings.

4 Enter information as needed. The required fields are **Name, Login Name,** and **Roles**. See table below.

5 Click **Accept** or **Apply**.

Field	Notes
Login Name	Must be unique within the system.
Force user to change password at login	Forces the operator to change his password immediately after his next login. **NOTE** You can combine the use of this field and the **Change Password** field to create a temporary password that the operator must change after his next login.
Starting Location	Set the starting location for each individual operator by choosing the specific area or controller in the navigation tree and the starting page from the drop-down menu.
Roles	See table below.

This privilege...	allows an operator to...
Installer	• Add, edit, and delete operators, operator groups, and privilege sets. • Update the i-Vu® system with service packs and patches. • Register the i-Vu® software. • Enable and set up the advanced password policy. • Add and remove i-Vu® add-ons.

Access privileges

Guest	Standard User	Power User	Admin	Installer	The following can be accessed but not edited...
☑	☑	☑	☑	☑	User tree
	☑	☑	☑	☑	Control program tables and Properties pages
	☑	☑	☑	☑	Scheduling Groups pages in the User view navigation tree
		☑	☑	☑	System Options Items
☑	☑	☑	☑	☑	Alarms

CARRIER CORPORATION ©2020
All rights reserved

Guest	Standard User	Power User	Admin	Installer	The following can be accessed but not edited...
☑	☑	☑	☑	☑	User tree
				☑	Logic Pages

Functional privileges

Guest	Standard User	Power User	Admin	Installer	The following allows an operator to...
		☑	☑	☑	**Manage Alarm Messages and Actions** - add, edit, and delete alarm messages and actions.
			☑	☑	**Maintain System Parameters** - edit all properties on the System Options pages.
	☑	☑	☑	☑	**Maintain Schedules** - add, edit, delete, and download schedules.
	☑	☑	☑	☑	**Maintain Schedule Group Members** - add, edit, and delete schedule groups.
		☑	☑	☑	**Maintain Categories** - add, edit, and delete categories.
		☑	☑	☑	**Acknowledge Non-Critical Alarms** - acknowledge all non-critical alarms.
		☑	☑	☑	**Acknowledge Critical Alarms** - acknowledge all critical alarms.
		☑	☑	☑	**Force Normal Non-Critical Alarms** - force non-critical alarms to return to normal.
		☑	☑	☑	**Force Normal Critical Alarms** - force critical alarms to return to normal.
		☑	☑	☑	**Delete Non-Critical Alarms** - delete non-critical alarms.
		☑	☑	☑	**Delete Critical Alarms** - delete critical alarms.
			☑	☑	**Execute Audit Log Report** - run the **Location Audit Log** and **System Audit Log** reports.
			☑	☑	**Download Controllers** - mark equipment for download and initiate a download.
			☑	☑	**System Shutdown** - issue the Shutdown manual command that shuts down i-Vu® Server.
				☑	**Access Commissioning Tools**: • Equipment Checkout • Airflow Configuration • Trend, Report, and Graphic categories that require this privilege • Discovery tool (i-Vu® Plus only)
		☑	☑	☑	**Maintain Graphs and Reports** - add, edit, and delete trend graphs and reports.

CARRIER CORPORATION ©2020
All rights reserved

Guest	Standard User	Power User	Admin	Installer	The following allows an operator to...
			☑	☑	**Remote Data Access-SOAP** - retrieve i-Vu® data through an Enterprise Data Exchange (SOAP) application. (i-Vu® Plus only)
			☑	☑	**Manual Commands/Console Operations** - access the manual command dialog box and issue basic manual commands.
				☑	**Manual Commands/File IO** - execute manual commands that access the server's file system.
				☑	**Manual Commands/Adv Network** - execute manual commands that directly access network communications.
	☑	☑	☑	☑	**Change My Settings** - edit preferences on operator's **My Settings** page.

Parameter privileges

Guest	Standard User	Power User	Admin	Installer	The following allows an operator to edit properties such as...
	☑	☑	☑	☑	**Setpoint Parameters** - occupied and unoccupied heating and cooling setpoints
			☑	☑	**Setpoint Tuning Parameters** - demand level setpoint offsets, color band offsets, heating and cooling capacities and design temperatures, color hysteresis, and learning adaptive optimal start capacity adjustment values
		☑	☑	☑	T**uning Parameters** - gains, limits, trip points, hysteresis, color bandwidths, design temperatures, and optimal start/stop.
		☑	☑	☑	**Manual Override Parameters** - locks on input, output, and network point.
		☑	☑	☑	**Point Setup Parameters** - point number, type, range, and network source and destination
		☑	☑	☑	**Restricted Parameters** - properties the installer restricted with this privilege
		☑	☑	☑	**Category Assignments** - Alarm, Graphic, Trend, and Report category assignments
		☑	☑	☑	**History Value Reset** - elapsed active time and history resets, and runtime hours
		☑	☑	☑	**Trend Parameters** - enable trend logging, log intervals, and log start/stop time.
		☑	☑	☑	**Calibration Parameters** - point calibration offsets
		☑	☑	☑	**Hardware Controller Parameters** - module driver properties
					Critical Configuration - critical properties the installer protected with this privilege

CARRIER CORPORATION ©2020
All rights reserved

Guest	Standard User	Power User	Admin	Installer	The following allows an operator to edit properties such as...
		☑	☑	☑	**Area Name** - area display names
		☑	☑	☑	**Control Program Name** - equipment display names
		☑	☑	☑	**Alarm Configuration** - enabling/disabling alarms and editing alarm messages, actions, categories, and templates
		☑	☑	☑	**Status Display Tables** - tables available under Status
		☑	☑	☑	**Maintenance Tables** - tables available under Maintenance
		☑	☑	☑	**User Config Tables** - tables available under User Config
				☑	**Service Config Tables** - tables available under Service Config
	☑	☑	☑	☑	**Setpoint Tables** - tables available under Setpoint
	☑	☑	☑	☑	**Time Schedule data Tables** - tables available under Time Schedule

CARRIER CORPORATION ©2020
All rights reserved

Troubleshooting

WARNINGS!

- Do NOT change the BIOS settings in any way or the software will fail.
- Mount your i-Vu® web server in an air conditioned space to avoid damage.
- Do NOT open the i-Vu® web server! Opening the web server voids your warranty.

If using DHCP and can't access the i-Vu® web server with Internet Explorer, by computer name

Notes about the i-Vu® application and DHCP addressing

The i-Vu® web server is configured to automatically obtain an IP address using DHCP. When the i-Vu® application is turned on, it sends a request out its LAN cable to a DHCP server and asks the server to supply it with its IP configuration.

This IP configuration consists of:

- IP address
- Subnet mask
- Default gateway
- DNS address

If a DHCP server is not available, as in the case of connecting the i-Vu® web server directly to a computer, the i-Vu® web server assigns an internal IP address to its Network Interface Card. The computer that is directly connected to the i-Vu® web server also assigns itself an IP address if it is set up for DHCP. The network portion of each of these IP addresses are identical, 169.254.xxx.xxx. The remaining two octets of each IP address are different. This ensures that communication is possible on the IP network consisting of the i-Vu® web server and the computer.

i-Vu® web server connected to computer with a crossover cable

1. Verify that the i-Vu® web server is on.
2. Check that a valid Ethernet connection exists. (See *Example 1* (page 34).)
3. Click **Start** and type "cmd" in the Search box, 

and click Enter. Type "ping ivu" to ping the i-Vu® application's default name. (See example 3). If you see 4 successful replies, then check Internet Explorer to determine if a proxy server or automatic configuration script is being used and disable them. (See *Example 2* (page 36).)
4. Try accessing the i-Vu® web server again.

CARRIER CORPORATION ©2020
All rights reserved

5 If after performing step 3, the i-Vu® web server still isn't accessible from Internet Explorer, or the Ping command in step 3 failed,

   1. Click **Start** and type "cmd" in the Search box, 

and click Enter.
   2. Type the following commands: "nbtstat –R" and click Enter.
   3. Type in "ipconfig /flushdns" and click Enter.

6 If the i-Vu® web server is still inaccessible from Internet Explorer, try pinging the web server again.

7 If the i-Vu® web server still does not respond to the PING command, try pinging the name of the computer connected to the i-Vu® web server. If this is successful, reboot the i-Vu® web server, and try pinging it.

8 If it still fails the PING test, connect a monitor to the i-Vu® web server and reboot.

At the end of the boot process, the i-Vu® web server displays its IP configuration. If the **i-Vu Address** is something other than 169.254.xxx.xxx, the i-Vu® application is not set to use DHCP and is assigned a static IP address. In this case, to access the i-Vu® application, it is necessary to configure the IP settings of the computer's Network Interface Card (NIC) to be on the same network as the i-Vu® web server. After reconfiguring the NIC, access the i-Vu® application with browser, using the server IP address shown on the monitor.

NOTE If pinging the computer name fails, the network connection on the computer is either disabled, disconnected, or in need of repair. Call Carrier Control Systems Support for assistance.

i-Vu® device plugged into LAN

1 Verify that the i-Vu® web server is on.

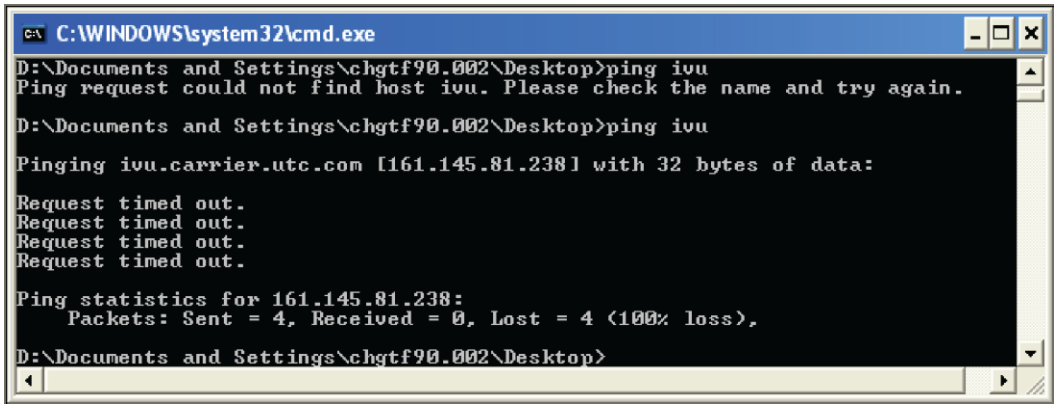
2 Check that a valid Ethernet connection exists. (See Example 1.)

3 Open a Command window (See Example 3.) and ping the i-Vu® web server by its default name (ivu).

- If pinging is successful, then the problem is most likely in the computer's browser settings. Check Internet Explorer to determine if a proxy server or automatic configuration script is being used (See *Example 2* (page 36)).
- If you are using a proxy server, you must add the name of the i-Vu® web server to the exceptions list of the proxy server. (See Example 4)
- If an auto-configuration script is being used, adding the i-Vu® web server to the exceptions list is not possible. Contact your local Information Technology (IT) group for assistance.

CARRIER CORPORATION ©2020
All rights reserved

- If pinging fails, but the i-Vu® name is resolved to an IP address, as shown below, the problem could be that pinging is disabled on the LAN.



- If this is the case, check the proxy server settings in Internet Explorer as in *Example 2* (page 36).
- If the problem isn't with the proxy server settings and pinging is enabled on the LAN, failing to ping successfully could mean that the i-Vu® name is resolving to an incorrect IP address.

Try the following:

1. Open a Command window (See Example 3) and type in the following commands: "nbtstat –R" <enter>.
2. Type in "ipconfig /flushdns" <enter>.
3. Try pinging the i-Vu® web server again by name.

- If successful, try accessing the i-Vu® application with Internet Explorer. If not successful try accessing it in Internet Explorer by IP address, i.e. https://161.145.81.238. If this is not successful, contact your local IT group to resolve this issue.
- If pinging fails with any other error than what is shown in the graphic above, contact your local IT group to assist you. The IT group may want to know what IP address the i-Vu® web server is actually using. To determine this, connect a monitor to the i-Vu® DVI port in the back of the i-Vu® web server and power down. Now power up the i-Vu® web server and the IP configuration information displays at the end of the boot process.

Example 1: Determining if a valid Ethernet connection exists

Ensure there is a proper Ethernet connection, using one of the following methods:

- CLick **Start** and type **ncpa.cpl** in the Search 

box.
- Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Settings**.

  NOTE On the Control Panel screen, verify that **Adjust your computer's settings** is set to **View by**: **Small (or Large) icons**.

CARRIER CORPORATION ©2020
All rights reserved

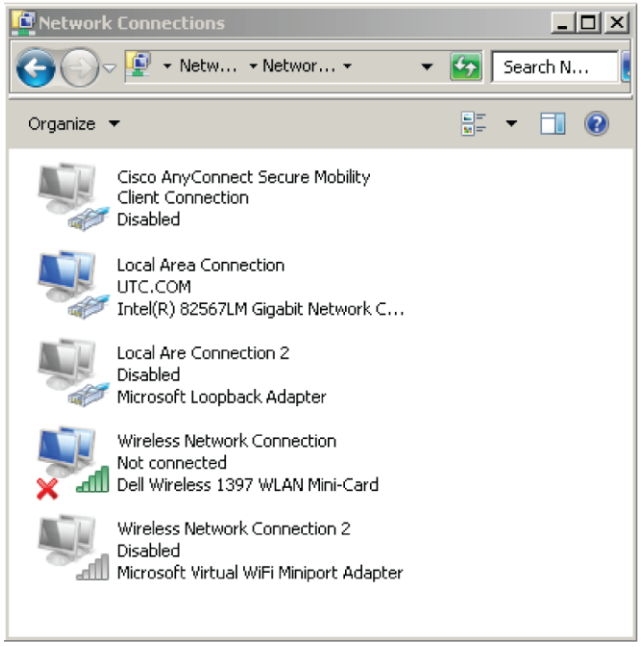
Under LAN or high speed Internet, find your Network Interface Card icon and ensure that a red **X** is not displayed over the icon.

Note that in the following figure:

- The **Local Area Connection** is enabled and connected
- The **Wireless Connection** is enabled, but not connected
- The 2 other connections are disabled

If the connection that is used for the i-Vu® web server shows a red **X**, then check that the Ethernet cable is fully plugged in and that the correct type of Ethernet cable is being used, i.e. crossover or patch cable.

You must have a live Ethernet connection to successfully connect to the i-Vu® web server.

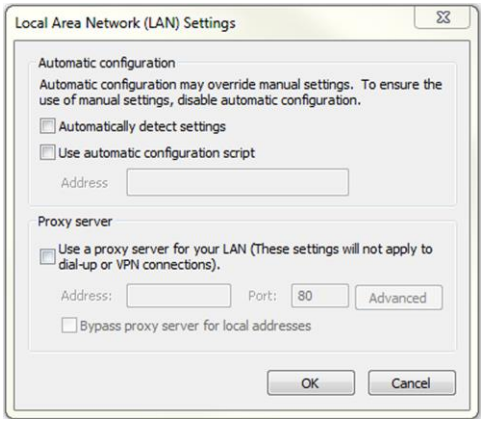


CARRIER CORPORATION ©2020
All rights reserved

Example 2: Determining if Internet Explorer is using a proxy server

1 Launch Internet Explorer and go to **Tools** or click > **Internet Options** > **Connections** and click the **LAN Settings** button.

2 Uncheck every checkbox in this dialog window to disable proxy server usage, as shown below.



3 Click **OK**.

4 Click **OK** again.

5 Close all instances of Internet Explorer.

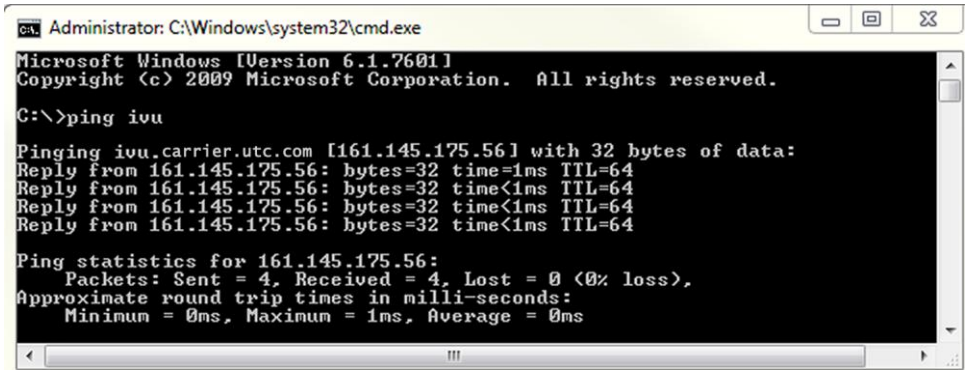
6 Launch Internet Explorer again and access the i-Vu® application.

Example 3: Pinging by computer name

1 Click **Start** and type “cmd” in the Search box 

and click **Enter**.

2 Type “ping ivu” to ping the default name of the i-Vu® web server. If you have a good connection, you should see 4 replies.



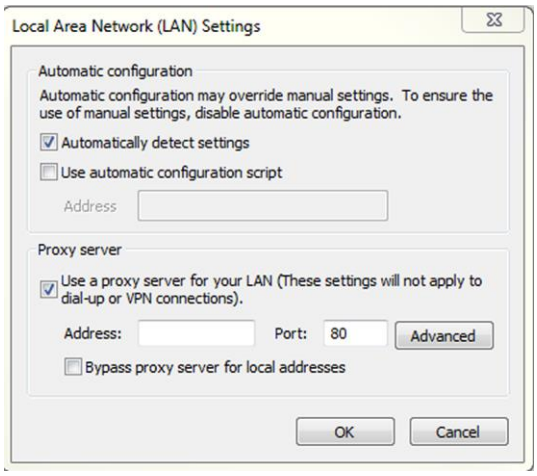
3 Note name and IP address.

CARRIER CORPORATION ©2020
All rights reserved

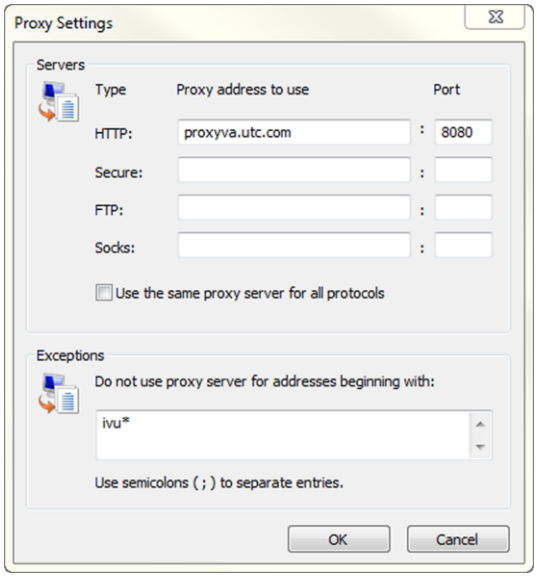
Example 4: Adding exceptions to a proxy server in Internet Explorer

1 Launch Internet Explorer and go to **Tools** or click > **Internet Options** > **Connections** and click the **LAN Settings** button.

2 Verify that the **Proxy Server** checkbox is checked.



3 Click the **Advanced** button and enter the address and port, and the name of the i-Vu® web server followed by an asterisk in the **Exceptions** list.



4 Click **OK** to close each dialog window.

5 Close Internet Explorer and re-open it for the new settings to take effect.

CARRIER CORPORATION ©2020
All rights reserved

Connect a monitor directly to the i-Vu® web server

In the event that you lose your system name and system IP address, you must connect the i-Vu® web server directly to a monitor. Purchase an VGA/DVI/HDMI adapter (VGA/DVI/HDMI - whichever fits your monitor) to connect them.

CAUTION You must turn the i-Vu® web server OFF before plugging the adapter into the port connector or the monitor will not display any information.

1. Turn on the monitor.
2. Turn off the i-Vu® web server.
3. Plug the HDMI adapter into either of the the HDMI connectors on the back of the web server.
4. Plug the adapter into the monitor.
5. Turn on the i-Vu® web server. Your monitor automatically displays the web server's system information.

CARRIER CORPORATION ©2020
All rights reserved

System Management

Although the i-Vu® application is a reliable front-end, you must perform periodic backups of the i-Vu® database to ensure a quick recovery in case of failure. To make sure that your controllers have the latest version of software, you must install periodic library upgrades. The sections below describe how to backup and restore the i-Vu® database and how to install the library updates.

Backup data from Management Tool

Access the **Management Tool** using one of the following methods:

- Click , then select **System Options** > **General** tab > **Management Tool**.
- Launch your browser and type your system name followed by :8080. For ex.: https://ivu:8080/.

Use either of the following methods to backup your data:

Backup data to your computer

1. Click **PC Backup** under **Manage Server Data** to save the entire database zipped into one file to your computer.
2. Click **OK** when you see the message **The system will be stopped and restarted. Do you wish to proceed?** Watch **Operation Status** to see the progress.
3. Click the message **Save/Download Backup File to Your Local Hard drive** when it appears.
4. Click **Save** when asked **Do you want to open or save this file?**
5. Save this system.backup.tgz file to a convenient location on your computer.

   CAUTION! Do not alter the name of this file!
6. Exit from **Management Tool**.

Backup data to a USB drive

1. Plug your own USB drive into any available USB port on your i-Vu® web server.

   CAUTION Do not use the i-Vu® **Restore** USB drive!
2. Click **USB Backup** under **Manage Server Data**.
3. Click **OK** when you see the message **The system will be stopped and restarted. Do you wish to proceed?**
4. When **Operation Status** says **No Background Operations Currently Active**, remove USB drive from the i-Vu® web server.
5. Exit from **Management Tool**.

CARRIER CORPORATION ©2020
All rights reserved

Restore data from backup

1. Click **PC Restore** or **USB Restore** under **Manage Server Data** in the **Management Tool**.
   - **PC Restore** - Browse to your backup file and click **Perform Restore**.
   - **USB Restore** - Place your backup USB drive in any port on thei-Vu® web server. Select the backup file and click **Perform Restore**.
2. Restore is complete when **Operation Status** displays **No Background Operations Currently Active**.
3. If you wish to change the name of your i-Vu® system from the default **ivu**, enter the new name in the **Name** field under **Addressing**. The restore process does not automatically reinstate your previous name.

Restore factory defaults

Restoring factory defaults deletes your existing data and restores your system to factory defaults. This restore process is quicker than using the **Restore** USB drive.

1. Access the **Management Tool** in **System Options** > **General** tab > **Management Tool** or via your browser by typing your system name followed by :8080.

   For ex.: https://ivu:8080.
2. Click **Factory Defaults**. This deletes all server data and resets the device to the original factory default values.
3. **NOTE** Executing this option will not delete configuration data under the **Addressing** and **i-Vu Port Configuration** sections of the Management Tool.
4. Begin setting up your system.

Restore i-Vu® system

⚠ **CAUTION!** Placing the **Restore** USB drive in the i-Vu® web server USB port reformats your system and restores it to factory defaults. Library updates are lost and you must reapply them.

1. Insert the Restore USB drive into any i-Vu® web server USB port.
2. Shut down
   - i-Vu® web server - Shut down the web server by pushing the On/Off button.
   - Older i-Vu® web server - Shut down the web server by holding down the On/Off button for several seconds. Then wait for the blue lights to go out before restarting.
3. Press the On/Off button again to restart. The restore process starts automatically and takes several minutes. The web server shuts off when finished.

   NOTE Do not turn the power off during reformatting!
4. Remove the **Restore** USB drive.
5. Wait another minute or two before accessing the new system using a browser.

CARRIER CORPORATION ©2020
All rights reserved

Update the SAL library

The i-Vu® SAL files update youri-Vu® controllers. The SAL libraries contain control programs, graphics, drivers, screen files, and other important controller data.

Carrier periodically provides updates, which include enhancements and bug fixes.

NOTES

- The library update only changes **default** graphics. If you have edited your graphic in ViewBuilder, it is not updated.
- The last digits in the SAL library name are the release date of the library.
- All of the SAL files will not necessarily have the same <date> revision.
- To ensure that your installation is running the latest software, we recommend that you check *Control Systems Support http://www.hvacpartners.com/*, *https://accounts.ivusystems.com/* for updates. Download the latest SAL files and apply them to all new installations.
- If you are changing to an older SAL file than the current one being used, a warning asks you if you are sure you want to apply an older version.

NOTE Keep copies of the latest libraries in a safe place. In the event of a system restore, the updated .sal file must be reapplied.

To check current SAL library version

1 Login to the i-Vu® application.

2 Click , then select **System Options** > **Update** tab.

3 Click **Current Libraries (.sal)** to view the current SAL libraries and their revision date.

Step 1: Update library

1 Save the updated library (.sal file) to your computer.

2 Click , then select **System Options** > **Update** tab.

NOTE Expand **Current Libraries (.sal)** to see the current SAL libraries and their revision. Compare them to what you downloaded from the Control Systems Support to determine if any of them have been updated.

3 Click 

and browse to the updated .sal file that you have saved on your computer, select the file, and click **Open**.

4 Click **Continue**.

5 When process is complete, the message appears **File added successfully**.

6 Click **Close**.

NOTE These changes are not applied to the controllers until you have updated routers and controllers.

CARRIER CORPORATION ©2020
All rights reserved

Follow these steps to implement the new equipment library:

Step 2: Update the files for the routers

1. Select the router that you wish to update in the navigation tree.
2. Right-click and select **Driver Properties**.
3. Select **Properties** page > **Update** tab.
4. If the database contains two or more routers, you must check **Change for all controllers of this type?** in the **Controller** section.
5. Click **Update**. A message appears **Changes the driver and screen file to use the current library version. Continue?**

   NOTE If more than one router exists, the additional routers are listed below the **Update** button.
6. Click **OK.**
7. Click **Accept.**

Step 3: Update the files for the controllers

1. Double-click the controller in the navigation tree or right-click and select **Configure**.
2. If you have multiple controllers of the same type, enable **Change for all control programs of this type?**.
3. Click **Update** under **Control Program**. A message appears **Changes the control program, view, driver, and screen file to use the current library version. Continue?**
4. Click **OK.** When the message **Updated to the library version xx.** appears, click **Close.**
5. Repeat steps 1 - 4 for any additional types of controllers.
6. Click **Close** again.

Step 4: Update the files for CCN controllers

1. In the navigation tree, select the CCN device manager associated with the controllers that are to be updated.
2. Select **Devices** > **CCN Discovery** and re-scan any controllers that need to be updated by checking **Rescan Controllers Selected Below for Configuration Changes** and clicking **Start Scan**.

Step 5: Apply the update to the routers and controllers

1. Select the **System**  in the navigation tree and then select the **Downloads** page.
2. If you wish to apply the new SAL file to your entire system, you can use this page to compare to your navigation tree and verify that you have selected all of your routers and controllers for download.

   NOTE Only the CCN Gateway and device managers require download, so the CCN controllers/equipment will not be listed.
3. A network's controllers download in the order shown. To change the order, select a controller(s), then drag and drop or click **Move to Top** or **Move to Bottom**.
   EXCEPTION If a controller's router requires a download, it will download first regardless of its position on the Downloads page. Click the **Start** button.

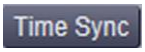
   NOTES

   - Use **Ctrl+click**, **Shift+click**, or the **Select All** checkbox to select multiple controllers.
   - See To download from the Downloads page in Help for more details.

CARRIER CORPORATION ©2020
All rights reserved

Synchronize to system time

To update all routers and controllers to the system time:

1. Click , then select **System Options** > **General** tab.
2. Click 

to immediately synchronize all controllers.
3. To adjust the time when controllers are automatically synchronized each day, click **Enable time synchronization of controllers daily at** and fill in time.

CARRIER CORPORATION ©2020
All rights reserved

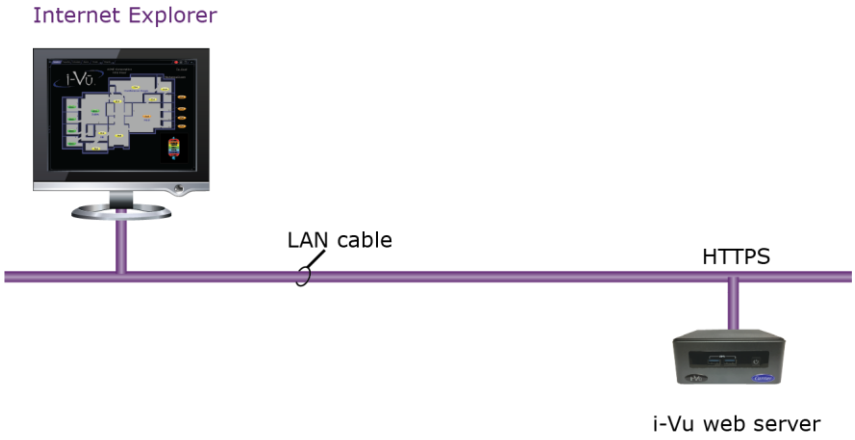
Advanced topics

i-Vu® network connection options and requirements

You can use any of the following common network configurations (see below for details):

- **Option 1** - Connect directly from a computer to the i-Vu® web server
- **Option 2** - Connect to the Intranet for internal network access only
- **Option 3** - Connect to the Internet through the Intranet for both internal and external access
- **Option 4** - Connect to the Internet through a dedicated broadband account

Option 1 - Connect directly from a computer to the i-Vu® web server



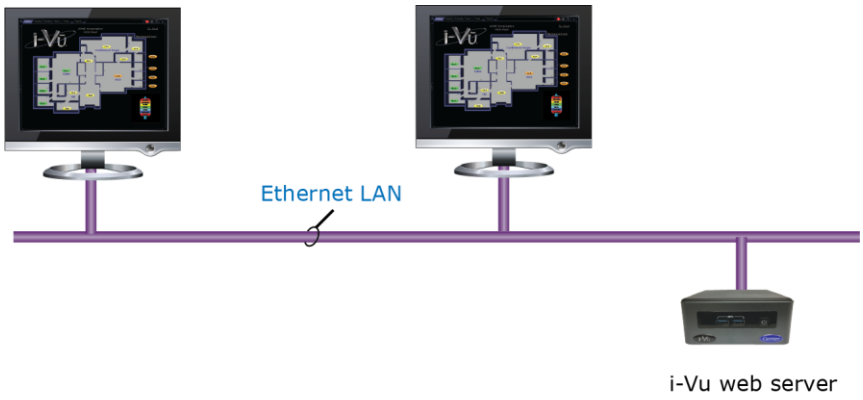
Requirements:

- Windows-based computer with supported web browser and available Ethernet port
- LAN Cable (either straight or crossover)

Email Options - None

CARRIER CORPORATION ©2020
All rights reserved

Option 2 - Connect to a LAN for internal network access only

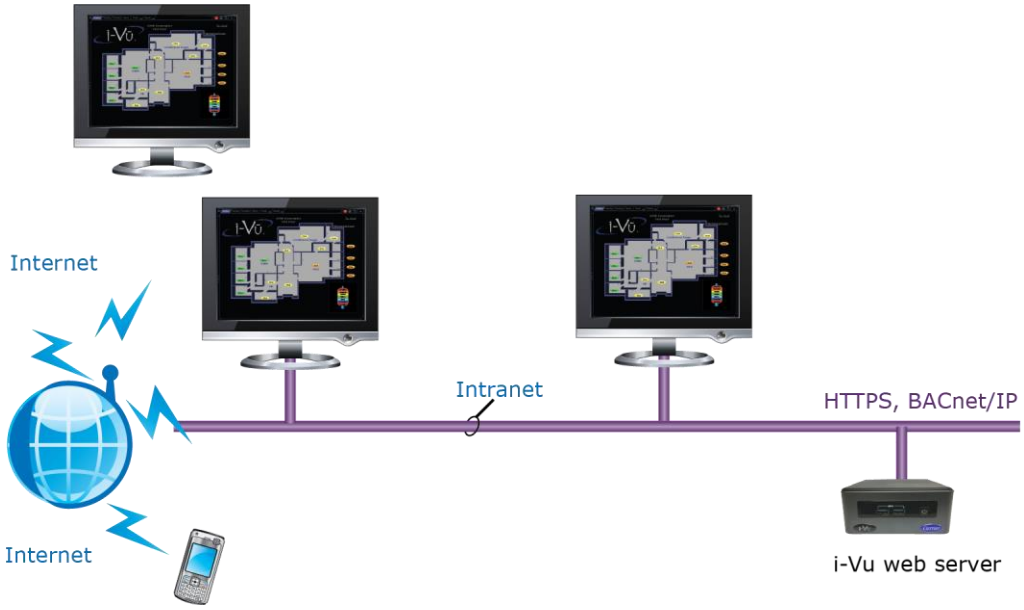


Requirements:

- Windows-based computer with supported web browser and Ethernet port
- Access to Ethernet LAN
- For i-Vu® Standard and Plus systems, you need a (DHCP or static) IP address for each of the following:
  - One IP address for the i-Vu® web server (required)
  - One IP address for the i-Vu® web server's internal router (optional)
  - One IP address for each external i-Vu® router (if applicable)

Email Options - Email can be sent from a local or an Internet mail server if network policies allow this.

Option 3 - Connect to the Internet through an Intranet for both internal and external access



CARRIER CORPORATION ©2020
All rights reserved

Requirements:

- Windows-based computer with supported web browser and Ethernet port
- Access to Ethernet LAN
- For i-Vu® Standard and Plus systems, you need a (DHCP or static) IP address for each of the following:
  - One IP address for the i-Vu® web server (required)
  - One IP address for the i-Vu® web server's internal router (optional)
  - One IP address for each external i-Vu® router (if applicable)
- Internet IP address provided by the site's IT personnel
- Open firewall port for HTTP/HTTPS traffic to the i-Vu® web server's IP address (default is port 80/443 respectively)

Email Options - Email can be sent from both Internet and Intranet mail servers. To send email off of the LAN, the DNS and domain field must be properly configured in the i-Vu® web server.

Option 4 - Connect to the Internet through a dedicated broadband account



- Window-based computer with supported web browser and Ethernet port
- Broadband Internet connection (internet IP address provided by the Internet Service Provider)
- IP router (w/Integrated Switch if computer or external i-Vu® routers will be used)
- For i-Vu® Standard and Plus systems, you need a (DHCP or static) IP address for each of the following:
  - One IP address for the i-Vu® web server (required)
  - One IP address for the i-Vu® web server's internal router (optional)
  - One IP address for each external i-Vu® router (if applicable)
- Open firewall port for HTTP/HTTPS traffic to the i-Vu® web server's IP address (default is port 80/443 respectively)

Email Options - Email can be sent from a local or an Internet mail server if network policies allow this.

CARRIER CORPORATION ©2020
All rights reserved

Using a loopback address

You can successfully use a loopback address for the **USB Network Address** if you are using:

- USB Adapter (CCN or Open)

  OR

- External routers with no USB Adapter connected

CAUTION! Do NOT use a loopback address if you are using both a USB Adapter and external routers and you intend the USB Adapter to communicate with other external devices on the IP network.

Finding devices is affected by plugging or unplugging the USB Adapter when using a loopback address for the USB network. If the USB adapter uses a loopback address, external discovery works as expected and finding devices under the USB Adapter works as expected. However, the USB Adapter and external IP devices will not be able to support features that require them to communicate with each other over IP

You can plug and unplug a CCN or Open USB Adapter into the web server without having to restart the system. However, you must refresh the system tree on the User view to update devices that are connected to the plugged or unplugged adapter.

If DHCP will not assign two IP addresses

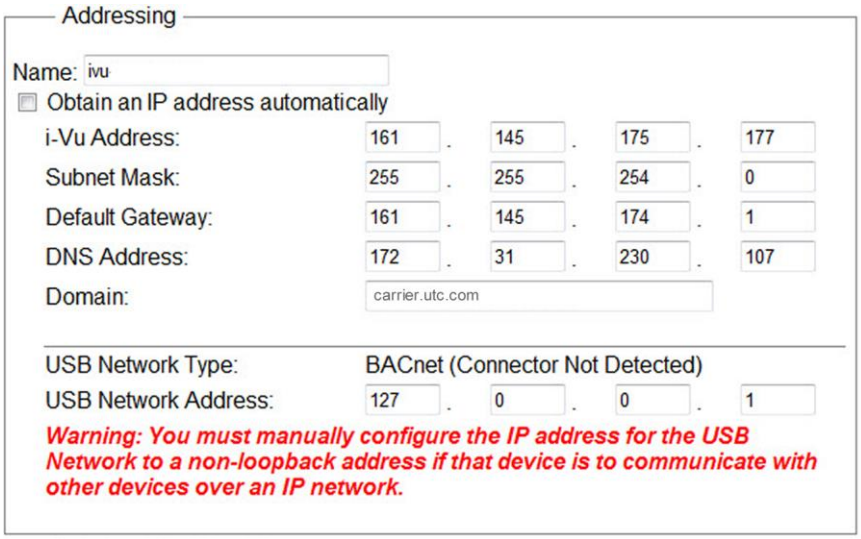
The default IP configuration uses DHCP. the i-Vu® web server attempts to obtain its IP configuration information from a DHCP Server located on the same subnet. Most DHCP Servers will provide all of the information contained in the **Addressing** section of the **Management Tool**, as shown below.

However, there are some DHCP Servers that will not assign2 IP addresses to 1 network card, or more specifically, to 1 MAC address.

As shown below, the i-Vu® web server is set for DHCP and all IP information looks valid except that the **USB Network Address** is configured for 127.0.0.1. This is called a loopback address and this IP address is not visible or accessible from the LAN. The warning in red indicates that you must assign a non-loopback address to the **USB Network Address.**

If using a loopback address, refer to *Using a loopback address* (page 47) for important details.

CARRIER CORPORATION ©2020
All rights reserved



In cases where the DHCP Server will not assign two IP addresses and the i-Vu® system uses both a USB Adapter and external routers, DHCP will not work. You must configure the i-Vu® system with static IP addresses. See Configure the i-Vu® system using a static IP address.

Finding the MAC address of the i-Vu® web server

In some cases, the IT personnel may ask for the Ethernet MAC address of the i-Vu® web server. There are two ways you can obtain this information.

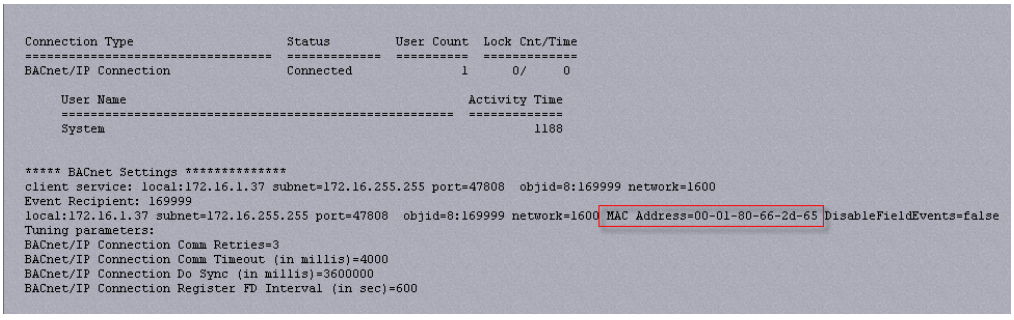
Option 1

1 Login to the i-Vu® application using the Administrator or Installer role.

2 Click **System Menu** and select **Manual Command**.

3 Type **commstat** and click **OK**.

4 The Ethernet MAC address of the web server is listed as shown below.



CARRIER CORPORATION ©2020
All rights reserved

Option 2

1 Carefully follow the instructions in Connect a monitor directly to the i-Vu® web server.

2 Once the server has restarted, the monitor displays the system information and the Ethernet MAC address is on the fourth line.

Using TCP/UDP ports

Server Ports	
Port	**Protocol/User**
tcp*:80	http (Web Server)
tcp *:443	https (Web Server)
tcp *:8080	https (Management Tool)
tcp *:47808	Diagnostic Telnet
udp *:68	DHCP Client daemon
udp *:123	NTP (Network Time Protocol)
udp *:137	nmbd (netbios/tcp requests)
udp *:138	nmbd (netbios/tcp responses)
udp *:47808	Bacnet/IP
udp *:47812	CCN/IP
Udp *:50005 to 50008	Firmware CCN/IP
udp *:47806	Alarm Notification Client

NOTES

- The i-Vu® web server listens through the ports.
- SOAP uses the HTTP port.
- HTTP and HTTPS ports are user-viewable and definable on **System Options** > **General** tab > **Management Tool** or through your browser by typing your system name followed by :8080. For ex.: https://ivu:8080

  NOTE For proper security, you must install two self-signed browser certificates - one for your web server and one for the Management Tool. This enables you to use https without security warnings.
- You enable the Alarm Notification Client on the **System Options** > **General** tab.
- The CCN/IP and BACnet/IP ports have to be exposed if the connection between the i-Vu® web server and the routers contain a firewall.
- All other ports are not configurable.

CARRIER CORPORATION ©2020
All rights reserved

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*
12/1/20	What is the i-Vu® Standard/Plus application?	Added TruVu™ routers to i-Vu® Standard routing devices table	C-TS-OC-E-RD
5/19/20	Cover	Updated logo	C-D
10/2/19	What is the i-Vu® Standard/Plus application?	Deleted location-dependent access - it is not available for i-Vu® Standard or Plus.	C-TS-OC-E-RD
6/6/19		All applicable addresses in this document have been changed to `https`.	C-D
	Access the startup screen	Added instructions to stop and install self-signed certificates before finding and uploading devices.	C-HRDC - BR-O
	Setting up and using a web browser to access the i-Vu® interface > Install self-signed certificates for network security	New Provides detailed instructions to install self-signed certificates for different browsers to securely access the i-Vu® application and the Management Tool.	C-HRDC - BR-O
	Access the startup screen	Added information about needing to install self-signed certificates	C-HRDC - BR-O
	New NUC - model NUC7i3DNHE	updated throughout the document	C-D

* For internal use only

CARRIER CORPORATION ©2020
All rights reserved



CARRIER CORPORATION ©2020 · Catalog No. 11-808-672-01 · 12/1/2020