BACnet/SC

Setup Guide

• Catalog No. 11-808-847-01 • 7/18/2024

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

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

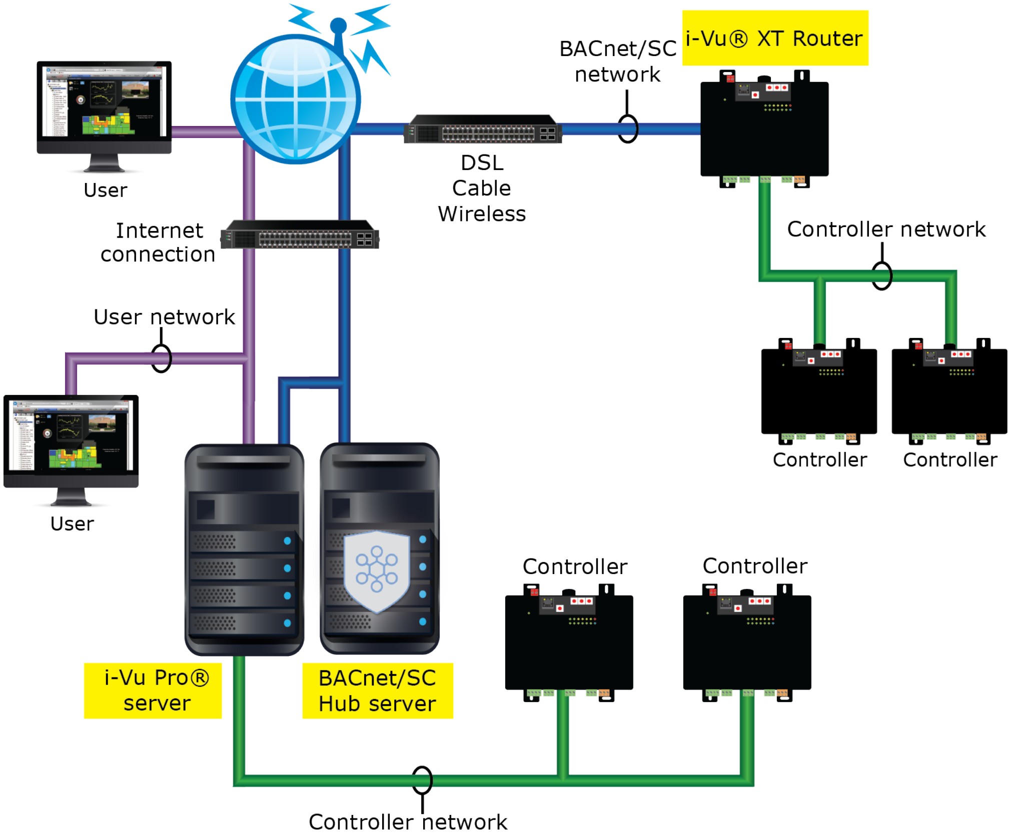
Contents

What is BACnet Secure Connect?

BACnet Secure Connect (BACnet/SC) is a new BACnet data link that addresses many of the security concerns that owners, facility managers, and IT professionals have expressed regarding unsecured BACnet networks. Using a “hub and spoke” topology, BACnet/SC provides the means to secure communications between building automation devices both across the cloud and within facilities. The BACnet/SC standard is described in addendum bj of ASHRAE Standard 135-2016.

NOTE To learn more, see the ASHRAE BACnet Working Group's BACnet/SC white paper, which can be found at www.bacnet.org.

Components of a BACnet/SC network



BACnet/SC Hub

The BACnet/SC Hub is a software service that acts as the central director of traffic between all node devices on a BACnet/SC network. It provides a web-based interface that allows you to configure the BACnet/SC Hub, including the installation of the certificates used to authenticate connected devices.

The BACnet/SC Hosted Hub is included with the i-Vu® Pro Cloud subscription to ensure a secure connection between your cloud-hosted i-Vu® Pro server and your on-site equipment.

You can install the BACnet/SC Virtual Hub on-premises or in the cloud to secure BACnet traffic within your site's network or to secure communication between your on-site equipment and an off-site i-Vu® Pro server. For instructions on how to install the BACnet/SC Virtual Hub, see the *BACnet/SC Virtual Hub Installation and Start-up Guide*.

i-Vu XT™ routers

The following products support routing over BACnet/SC: XT-RB and XT-LB. Throughout this document, these are referred to as "routers".

TruVu™ routers allow communication between your BACnet/SC network and your downstream BACnet/IP, BACnet/MSTP, and BACnet/ARCNET networks.

Before configuring the router to connect to the BACnet/SC network, download the latest Gen5 driver to the TruVu™ router to ensure it is compatible with BACnet/SC communications.

To set up a BACnet/SC connection in the router, see "BACnet/SC Port tab" in the router's *Installation and Start-up Guide*.

TIP Do not download drivers to downstream controllers at the same time as you download your BACnet/SC router. Allow the router to reconnect to the BACnet/SC network before downloading to any downstream controllers.

NOTE The router’s clock may be incorrect after the first startup or after reverting to default settings. It is important to set the clock’s time and time zone correctly before installing your BACnet/SC certificates. You can set the clock in one of two ways:

- Connect the router to the i-Vu® Pro system on a BACnet/IP network and perform a download.
- Synchronize the router's time to your computer:
    1. Install a local copy of the i-Vu® Pro application on your computer and add the router to the database.
    2. Set your computer's IP address to be in the same subnet as the router's Gig-E port IP address.
    3. Connect your computer to the router's Gig-E port.
    4. Log in to the local i-Vu® Pro instance from a browser on your computer.
    5. Navigate to the router's Properties page on the navigation tree.
    6. Click **Time Sync** in the BACnet Device Management section.
    7. Shut down the application, release the static IP on your computer, and move the IP cable to the Service Port to continue configuring the router.

i-Vu® Pro application

The i-Vu® Pro Cloud subscription uses BACnet/SC communications for secure connectivity to site controllers and includes access to the BACnet/SC Hub management user interface.

The i-Vu® Pro v8.0 or later on-premises application includes the capability to connect to a BACnet/SC network.

To set up a BACnet/SC connection in the i-Vu® Pro application, see “Setting up BACnet/SC network communication" in i-Vu® Pro Help.

Configuring the BACnet/SC Hub

When configuring the BACnet/SC Hub, changing certain values will require a restart. A **Restart** button will appear at the top of the screen when needed. You can continue to make changes on all tabs, then restart once to activate all your changes.

Preliminary Steps

- Obtain the URL and administrator password for the BACnet/SC Hub management user interface.
- Log in using the provided password.

Connections tabs

Device tab

The **Connections** > **Device** tab allows you to configure the items described in the table below.

Identification	
Device Instance	BACnet Device ID, must be unique on the BACnet system. **NOTE** Using a Device ID of zero (0) is not recommended.
Device Name	A specific device name that is unique on the BACnet system.
Location	An intuitive location of the BACnet device.
Description	An intuitive description of the BACnet device.
APDU	
APDU Timeout	How many milliseconds the device waits before resending a message if no response is received.
APDU Segment Timeout	How many milliseconds the device waits before resending a message segment if no response is received.
Number of APDU Retries	The number of times the device resends a message.

BACnet/SC Port tab

The **Connections** > **BACnet/SC Port** tab provides hub status information and the ability to configure the items described in the table below.

URIs	List of one or more web addresses that may be used by network devices to connect to the BACnet/SC Hub. These URIs are specified when the BACnet/SC Hub is installed. They are displayed here for information. **NOTE** If you are connecting a client device to the hub on an IPV6 network and your device has multiple Network Interfaces (NICs), then you must add a zone index to the URI.
Address	The Virtual MAC address of the BACnet/SC Hub on the BACnet/SC network. It is the hex representation of the Device ID found on the **Connections** > **Device** tab. **NOTE** If the Device ID of the BACnet/SC Hub is zero (not recommended), a ’01’ will be assigned to the third octet of this address because zero addresses are not valid on a BACnet/SC network.
Connection State	The status of the BACnet/SC Hub’s connection as a client on the BACnet/SC network.
Is Failover Hub?	**No** if using this BACnet/SC Hub as a primary hub. **Yes** if using as a failover hub.
Primary Hub URI	If the BACnet/SC Hub is acting as a failover hub, the URI of the associated primary hub must be entered here. Format options (address can be an IP address or DNS name): • `wss://address` (if using standard port 443) • `wss://address:port`
Primary Hub Status	If the BACnet/SC Hub is acting as a failover hub, this is the status of the associated primary hub.
Advanced	
Minimum Reconnect Time	Initial number of seconds to wait before retrying a connect to a hub. Time between retries increases with each failure.
Maximum Reconnect Time	Maximum number of seconds to wait between connection retries to a hub.
Connection Wait Timeout	Number of seconds to wait for a hub to reply to a connection request.
Disconnect Wait Timeout	Number of seconds to wait for a hub to reply to a disconnect request.
Initiating Heartbeat Interval	Number of seconds to wait to send a heartbeat.
Accepting Heartbeat Interval	Number of seconds to wait to receive a heartbeat.
Certificate Management	
Certificate table	See *To create or replace a BACnet/SC device’s operational certificate* (page 18) for instructions for how to create the BACnet/SC Hub’s operational certificate, signed by the BACnet/SC network’s Certificate Authority.

License Admin tab

When you purchase the BACnet/SC Virtual Hub, you must activate your license in the BACnet/SC Hub management user interface. If you are a Carrier Distributor or Service Office, you will be able to register your license and receive your Activation Key from the i-Vu License Manager (https://accounts.ivusystems.com). Those who do not have access to the i-Vu License Manager, such as Carrier Controls Experts, can get this license emailed to them from their distributor.

NOTES

- Purchase the BACnet/SC Virtual Hub license that coincides with the number of Gen5 routers that you plan to connect to your BACnet/SC network. The license allows for 3 additional connections for the BACnet/SC Hub, your i-Vu® Pro system, or a failover hub, if you have one.
- You do not need to purchase a separate license for the BACnet/SC Hosted Hub. It is included in the i-Vu® Pro Cloud subscription. For a hosted hub, this tab is for your information only.

To register the license and get the Activation Key

1. Log in to the Carrier® Community Portal website.
2. Select **Orders** > **Software Licenses**.
3. Select **BACnet/SC Virtual Hub**, and then select the unregistered license.
4. Fill out the registration form, and then check **I Agree to the terms of use**. The Activation Key appears below the checkbox.
5. Copy the key to a file that you can access while you are logged into the BACnet/SC Hub management user interface.

To activate a license in the BACnet/SC Virtual Hub

Navigate to the **Connections** > **License Admin** tab. The method you use to activate your licenses depends on whether or not the computer running the BACnet/SC Virtual Hub can access the Internet.

If the BACnet/SC Virtual Hub has Internet access

1. Verify that **This product can access the Internet** is checked.
2. Open the file that has the Activation Key, and then copy and paste the key in the **License Activation Key** field.
3. Click **Activate**.

NOTE If it is necessary to use a proxy to reach the license manager server, you can configure your proxy server on the **Advanced** > **Network** tab. See *Network Tab* (page 12).

If the BACnet/SC Virtual Hub does not have Internet access

1. Uncheck **This product can access the Internet**.
2. Click **Offline Activation** to expand the section.
3. Open the file that has the Activation Key, and then copy and paste the key in the **License Activation Key** field.
4. Click **Create Activation Request File** to download the **Activation_Request.bin** file. Save the file to a location or USB thumb drive so it can be accessed by a computer that has Internet access.
5. Retrieve your activation file:
   a) On the computer that can access the Internet, go to the Carrier® Community Portal website and select **Orders** > **Software Licenses.**
   b) Select **BACnet/SC Virtual Hub**, and select the license.
   c) Check **I Agree to the terms of use**.
   d) Under **Offline Activation**, browse to the **Activation_Request.bin** file, and then click **Upload Request File**. An **ActivationResponse-(key).bin** file will download.
   e) Save the response file to a location or USB thumb drive so it can be accessed by the computer running the BACnet/SC Virtual Hub.

6 On the BACnet/SC Virtual Hub **Connections** > **License Admin** tab, under Offline Activation, browse to the **ActivationResponse-(key).bin** file.

7 Click **Activate License**.

To deactivate a license in the BACnet/SC Virtual Hub

You cannot use the BACnet/SC Virtual Hub license on multiple computers simultaneously. If you need to move the BACnet/SC Virtual Hub to a different computer, you must first deactivate the license on the current computer before activating it on the new computer.

NOTE Changing the network interface card used for BACnet communications* on the computer running the BACnet/SC Virtual Hub changes the Host ID, which the license system will interpret as a different computer. To keep your system running, you must deactivate your license before changing the network card and then reactivate it after changing the card.

*This is defined in the Admin Tool under **BACnet Settings** > **Network Interface**.

If the BACnet/SC Virtual Hub has Internet access:

Navigate to the **Connections** > **License Admin** tab and click **Deactivate.**

NOTE If it is necessary to use a proxy to reach the license manager server, you can configure your proxy server on the **Advanced** > **Network** tab. See *Network tab* (page 12).

If the BACnet/SC Virtual Hub does not have Internet access:

Navigate to the **Connections** > **License Admin** tab and perform the following steps:

1 Uncheck **This product can access the Internet**.

2 Click **Offline Deactivation** to expand the section.

3 Click **Create Deactivation Request File** to download the **Deactivation_Request.bin** file. Save the file to a location or USB thumb drive so it can be accessed by a computer that has Internet access.

4 Retrieve your deactivation file:

   a) On the computer that can access the Internet, go to the Carrier® Community Portal website and select **Orders** > **Software Licenses.**

   b) Select **BACnet/SC Virtual Hub**, and select the license. This deactivation process will deactivate all licenses associated with the BACnet/SC Virtual Hub license.

   c) Check **I Agree to the terms of use**.

   d) In the first field under **Offline Deactivation**, browse to the **Deactivation_Request.bin** file, and then click **Upload Request File**. A **DeactivationResponse-(activation key).bin** file will download.

   e) Save the response file to a location or USB thumb drive so it can be accessed by the computer running the BACnet/SC Virtual Hub.

5 On the BACnet/SC Virtual Hub **Connections** > **License Admin** tab, under Offline Deactivation, browse to the **DeactivationResponse-(activation key).bin** file.

6 Click **Deactivate All Licenses Locally**.

7 Click **Create Confirmation File** to create a **Confirmation.bin** file. Put the file in a location that is accessible by another computer that can access the Internet.

8 Confirm deactivation:

a) On the computer that can access the Internet, go to the Carrier® Community Portal website and select **Orders** > **Software Licenses.**

b) Select **BACnet/SC Virtual Hub**, and select the license.

c) Check **I Agree to the terms of use**.

d) In the second field under **Offline Deactivation**, browse to the **Confirmation.bin** file, and then click **Upload Confirmation File**.

Advanced tabs

Alarms tab

The **Advanced** > **Alarms** tab allows you to configure the BACnet/SC Certificate Expiration alarm the hub sends to the i-Vu® Pro system. When this alarm is enabled, an alarm will trigger when a BACnet/SC Hub certificate is within the configured **Warning** or **Critical** thresholds. While in the Warning period, the alarm repeats once per week. In the Critical period, the alarm repeats daily.

NOTE To send this alarm to the i-Vu® Pro system, enter “8:<i-Vu® Pro device ID>” in the **Recipient Device** field for the first listed recipient on the **Advanced** > **Notification Class** tab.

Alarm Active	The current status of the alarm
Enable To Off-Normal Event	Clear this checkbox to disable the **To Off-Normal** alarm messages from the BACnet/SC Hub.
Enable To Normal Event	Clear this checkbox to disable the **To Normal** alarm messages from the BACnet/SC Hub.
Time Delay	Specifies the delay between the onset of the Off-Normal condition and the reporting of the alarm to the i-Vu® Pro system.
Description	Short message shown when this type of alarm is generated.
Notification Class	A BACnet alarm's Notification Class defines: • Alarm priority for Alarm, Fault, and Return to Normal states • Options for BACnet alarm acknowledgment • Where alarms should be sent (recipients)
Object Name	A unique alphanumeric string that defines the BACnet object.
Warning Threshold	If a certificate is within this number of days of expiring, it will appear yellow in the Certificate Management table on the **Connections** > **BACnet/SC Port** tab and in the BACnet/SC Info section of the **Advanced** > **BACnet/SC Clients** tab. A weekly alarm will be triggered in the i-Vu® Pro system when one of the BACnet/SC Hub’s certificates is in this state.

Critical Threshold	If a certificate is within this number of days of expiring, it will appear red in the Certificate Management table on the **Connections** > **BACnet/SC Port** tab and in the BACnet/SC Info section of the **Advanced** > **BACnet/SC Clients tab**. A daily alarm will be triggered in the i-Vu® Pro system when one of the BACnet/SC Hub's certificates is in this state.

Notification Class tab

A BACnet alarm's Notification Class defines:

- Alarm priority for Alarm, Fault, and Return to Normal states
- Options for BACnet alarm acknowledgment
- Where alarms should be sent (recipients)

Notification Class Recipients	The first row in this list is from the i-Vu® Pro application. Do not delete this row. Click **Add** if you want other BACnet devices to receive alarms associated with this Notification Class.
Recipient Type	Select **Recipient Device** for device recipients that support dynamic binding. Complete the **Recipient Device** field if you are using this recipient type. Select **Recipient Address** (static binding) for either of the following: • Third-party BACnet device recipients that do not support dynamic binding • When you want alarms to be broadcast (you must uncheck **Issue Confirmed Notifications**). This use is rare. Complete the **Network Number** and **MAC Address** fields if you are using this recipient type.
Recipient Device	Type the **Device Instance** of the device that is to receive the alarm, whether that is the i-Vu® Pro server or a third party device, in the **#** field following the "8:". **NOTE** To enable the **BACnet/SC Certificate Expiration** alarm, this should be set to the i-Vu® Pro system's device instance.
Network Number	Specify the number of the BACnet network on which to send the notification. **TIP** For the home network, this can be set to 0.
MAC Address	MAC address of the recipient software or device.
Issue Confirmed Notifications	Select to have a device continue sending an alarm message until it receives delivery confirmation from the recipient.

Transitions to Send	Uncheck the types of alarms you do not want the recipient to get.
Off Normal	BACnet priority for Alarms.
Fault	BACnet priority for Fault messages.
Normal	BACnet priority for Return-to-normal messages.

Days and Times to Send	
Monday to Sunday **From Time** **To Time**	Select days and times during which the recipient will receive alarms.
Process Identifier	Change for third-party devices that use a BACnet Process Identifier other than 1. The i-Vu® Pro application processes alarms for any 32-bit Process Identifier.

Acknowledgments Required	
To Fault Ack Required **To Normal Ack Required** **To Off-Normal Ack Required**	Specifies whether alarms associated with this Notification Class require a BACnet Acknowledgment for Off-Normal, Fault, or Normal alarms. **TIP** You can require operator acknowledgment for an Alarm or Return-to-normal message (stored in the i-Vu® Pro database). In the i-Vu® Pro interface on the **Alarm** > **Enable/Disable** tab, change the acknowledgment settings for an alarm source or an alarm category.

Priority	
To Fault Priority	BACnet priority for Fault messages.
To Normal Priority	BACnet priority for Return-to-normal messages.
To Off Normal Priority	BACnet priority for Alarms.

Identification	
Notification Class	A BACnet alarm's Notification Class defines: • Alarm priority for Alarm, Fault, and Return to Normal states • Options for BACnet alarm acknowledgment • Where alarms should be sent (recipients) **NOTE** To enable the **BACnet/SC Certificate Expiration** alarm, this value must match the **Notification Class** value set on the **Advanced** > **Alarms** tab.
Object Instance	The instance number of this BACnet Notification Class object. It must be unique within the BACnet Device that contains it.
Object Name	The alpha-numeric name of this BACnet Notification Class object. It must be unique within the BACnet Device that contains it.
Description	The description of this BACnet Notification Class object.

Controller Clock tab

The **Advanced** > **Controller Clock** tab displays the current system date and time.

BACnet/SC Clients tab

The **Advanced** > **BACnet/SC Clients** tab lists all the devices that have connected to the BACnet/SC Hub since it was last restarted, including the BACnet/SC Hub itself, the BAS, and all connected controllers. Information in the table includes:

Column	Description
Address	Virtual MAC address assigned to the device to uniquely identify it on the BACnet/SC network. The value in parentheses is the decimal equivalent of the last 3 octets of the address. For Carrier® devices, it represents the device's BACnet device ID, unless there is a duplicate, in which case it is a random number. For third party devices, this value is unknown. **NOTE** If the device's Device ID is zero, a '01' will be assigned to the third octet of this address because zero addresses are not valid on a BACnet/SC network.
Certificate Serial Number	Serial number assigned by the certificate issuer.
Certificate Exp Date	Date on which the device's operational certificate will expire. This date will be highlighted if it is within the warning (yellow) or critical (red) threshold defined on the **Connections** > **BACnet/SC Port tab**.
Last Active Timestamp	Time of the device's most recent connection to the BACnet/SC network.
Last Inactive Timestamp	Time of the device's most recent disconnect from the BACnet/SC network. Value will be **N/A** if the device is currently connected.

Diagnostics tab

The **Advanced** > **Diagnostics** tab allows you to capture network communication on a port and then download the capture file for troubleshooting.

Logs	• **Retrieve all** - Downloads all logs in a zip file to your computer • **Specific log** - Allows you to choose to download the application logs (by date) or the system logs • **Delete all** • **Delete captures**
Packet Capture	This allows you to capture network communication on the BACnet/SC ports and then download the capture file for troubleshooting. Click **Start** and **Stop** to initiate and end your capture, then click **Get capture file** to download the file. **NOTE** Capture files have a 1GB limit. If you need a larger capture, contact Carrier Control Systems Support. To dissect BACnet/SC packet captures, place the two Lua scripts provided into the plugins directory of your Wireshark installation. Contact Carrier Control Systems Support for assistance working with BACnet/SC packet captures.

Technical Support Tools	Send the displayed **Challenge** key to the Carrier Control Systems Support representative who will provide an **Activation Key** for you to enter, then click **Enable**. Additional tools will be displayed to help Carrier Control Systems Support troubleshoot issues. Enabling these tools has security implications, therefore they are automatically disabled after 2 hours.

Network tab

The **Advanced** > **Network** tab appears on the BACnet/SC Virtual Hub. It is not applicable on the BACnet/SC Hosted Hub.

Proxy updates made on this tab do not become active until the Hub service has been stopped and restarted.

Device Host Name	Read-only. Assigned from the host server.
Enable Proxy	Enable this checkbox if the BACnet/SC communication interface needs to get through a proxy firewall to communicate out to other networks.
Proxy Server Address	Set the IP address of the proxy host.
Proxy Port	Set the port for communication on the proxy host.
Proxy Username	Set a username if required to authenticate on the proxy server.
Proxy Password	Set a password if required to authenticate on the proxy server.
No Proxy For	Set addresses that do not require passing through the proxy to communicate. These addresses are typically exempt from the proxy requirements.

Connecting the site's equipment to the BACnet/SC network

For the router to communicate on the BACnet/SC network, you must:

1 Download the latest Gen5 driver.

TIP To download the new driver from the i-Vu® Pro interface:

a) Temporarily assign the router to a BACnet/IP network in SiteBuilder.

b) Download the driver (see the router's *Installation and Start-up Guide*).

c) Assign the router to the BACnet/SC network in SiteBuilder.

2 Configure it with information about how to connect to the hub, including installation of an operational certificate signed by the BACnet/SC network's Certificate Authority.

TIP Do not download drivers to downstream controllers at the same time as you download your BACnet/SC router. Allow the router to reconnect to the BACnet/SC network before downloading to any downstream controllers.

See "BACnet/SC Port tab" in the router's *Installation and Start-up Guide* for detailed instructions.

To validate that your connection has been set up successfully, confirm that the router is now listed on the BACnet/SC Hub's **Advanced** > **BACnet/SC Clients** tab.

Connecting the i-Vu® Pro application to the BACnet/SC network

For the i-Vu® Pro application to communicate on the BACnet/SC network, you must create a BACnet/SC network with a corresponding BACnet/SC connection.

In SiteBuilder

1 If NAT is enabled in your existing system, you must create a separate site for the BACnet/SC network that does not have NAT settings enabled. If you are not using NAT in your system, you can put your BACnet/SC network under an existing site. To create a new site:

a) Right-click on the root node of the network tree on the **Network** tab and choose **Add Site**.

b) Set values as applicable, then click **OK**.

2 Create a BACnet/SC network.

a) Right-click on a site on the **Network** tab and choose **Add BACnet Network.**
NOTE The site should not have NAT settings enabled.

b) Set **Media Type** to BACnet/SC.

c) Set other values as applicable, then click **OK.**

3 Add the BACnet/SC Hub to the BACnet/SC network.

NOTE If you have a failover hub, add it to the BACnet/SC network as well.

a) Right-click on the BACnet/SC network and choose **Add BACnet Device.**

b) Set **Controller** to Third Party Controller.

c) Set other values as applicable, then click **OK.**

4 Add each i-Vu® XT router to the BACnet/SC network.

a) Right-click on the BACnet/SC network and choose **Add BACnet Device Router.**

b) Set **Controller** to the router name.

c) Set other values as applicable, then click **OK.**

5 Add the BACnet/SC Hub equipment to the **Geographic** tree. Associate with the **sc-hub-ivu.equipment** file that you downloaded from the Carrier® Community Portal website.

a) Place the **sc-hub-ivu.equipment** file in the <system_name>**\programs** folder.

b) Right-click a location on the **Geographic** tree and choose **Add BACnet Equipment**.

c) Set **Control Program** to **sc-hub-ivu**.

d) Set other values as applicable, then click **OK**.

6 Associate the BACnet/SC Hub equipment with the BACnet/SC Hub in the **Network** tree.

a) Select the BACnet/SC Hub equipment in the **Geographic** tree.

b) Right-click the **BACnet/SC Hub** in the **Network** tree and choose **Assign Equipment**.

7 Enable BACnet/SC Hub failure alerts using Peer Caching.

NOTE When a router is set up as a Peer Caching device, it monitors all of its peer devices in its network, including your primary hub and your failover hub, if you have one. If either of your hubs fails, a Dead Controller Timeout alarm generates and appears in the i-Vu® Pro interface.

a) Double-click the site that contains your BACnet/SC network.

b) Select **Use Peer Caching**.

c) Choose a router from the **Device** dropdown that is in the same network as your BACnet/SC Hub(s).

d) Click **OK**.

In the i-Vu® Pro application

You can set up certificate expiration warning thresholds on the **System Configuration** > **System Settings** > **Scheduled Tasks** tab to trigger alarms when the i-Vu® Pro system's BACnet/SC certificates are nearing expiration. Warning alarms repeat once per week until it reaches the critical threshold, after which alarms repeat every day. See "Scheduled Tasks tab" in i-Vu® Pro Help for more details.

You must configure the BACnet/SC connection in the i-Vu® Pro application. See "Setting up BACnet/SC network communication" in i-Vu® Pro Help to connect to the hub and install an operational certificate signed by the BACnet/SC network's Certificate Authority.

To validate that your connection is set up successfully, confirm that the i-Vu® Pro system is now listed on the BACnet/SC Hub's **Advanced** > **BACnet/SC Clients** tab.

Managing certificates

A BACnet/SC network requires each device connected to the network to have a unique operational certificate signed by a common Certificate Authority (CA). The CA is owned by the site.

Depending on a site's IT policies, the network's CA can be issued by a trusted CA issuer, such as GoDaddy or DigiCert, or it can be "self-signed". This section describes how to create and use self-signed certificates using a no-cost, open source signing tool called Keystore Explorer. Of course, you may use any signing tool of your choice.

NOTE Although both RSA and EC CAs are supported by this product, other vendor's BACnet/SC implementations may support only EC. We recommend that you choose the EC algorithm to ensure interoperability with other vendor's BACnet/SC devices.

Certificate best practices

- The site's BACnet/SC signing CA certificate should always be a non-public CA used exclusively for signing that site's BACnet/SC certificates. It is acceptable to use either a self-signed certificate or an intermediate certificate signed by a trusted certificate authority to sign BACnet/SC operational certificates. The trusted certificate authority may be a public certificate authority or one private to the customer. In either case, the signing certificate should be used exclusively for this purpose.
- The site's CA certificate must be stored securely and should be protected by a password.
- Dispose of devices securely.
  - ○ Use the **Delete Keystore** button on the **Connections** > **BACnet/SC Port** tab to remove certificates when decommissioning the hub server or any connected device.
  - ○ When decommissioning a controller, revert the controller to its default settings. See "To revert to default settings" in the controller's Installation and Start-up Guide.

To download and install Keystore Explorer

NOTE The instructions in the following sections apply to Keystore Explorer 5.5.0 or later.

1. Ensure you have the required version of Java. Java Runtime Environment (JRE) Version 8 or above is required. You may obtain Java from the following sources.
   - ○ https://www.java.com/en/download/ *requires oracle technology network license agreement
   - ○ https://adoptopenjdk.net/releases.html *open source option
2. Download Keystore Explorer from https://keystore-explorer.org.
3. Follow the directions in the Keystore Explorer user manual for installation and use. The user manual can be found on the same site as the download files.

To create a BACnet/SC Certificate Authority using Keystore Explorer

Use Keystore Explorer to create a Certificate Authority (CA) to sign BACnet/SC certificates for the devices on a BACnet/SC network.

NOTE We recommend creating a separate keystore for each network, each with its own password.

1. Create a new keystore by clicking **Create a Keystore** from the Quick Start menu or by clicking the **New** icon in the tool bar.
2. Select keystore type **PKCS#12**.
3. Click **File** > **Save** to save the keystore as a ".pkcs12" file.
4. Click **Tools** > **Generate Key Pair**.
5. Select one of the following algorithms, set the associated fields as indicated below, then click **OK**.

Algorithm	Fields
EC (recommended)	○ **Set**: SEC ○ **Named Curve**: secp256r1
RSA	○ **Key Size**: 2048

6. Set the **Validity Period**, and then click **Apply**. We recommend a minimum of 20 years. See *To replace a BACnet/SC network's Certificate Authority* (page 19).

   TIP Set **Validity Start** to a previous date to avoid potential time zone issues.
7. Click the **Edit** icon beside the **Name** field to complete the Name fields with appropriate values for the site and customer.
8. Click **Add Extensions** > **Use Standard Template**, select **CA**, then click **OK**.
9. Click **OK** on the **Add Certificate Extensions** dialog.
10. Click **OK** on the **Generate Key Pair Certificate** dialog.
11. In **Enter Alias**, enter a meaningful alias that identifies the owner of the signing certificate and how it is to be used, then click **OK**.
12. Set a key pair password. We recommend giving each CA its own unique password.
13. If this new CA will be used to replace an existing CA on a BACnet/SC network, export the new CA's certificate:

    a) Right click on the CA and select **Export** > **Export Certificate Chain**.

    b) On the **Export Certificate Chain** dialog choose:

       1. **Export Length**: Head Only
       2. **Export Format**: X.509
       3. **PEM**: select checkbox
       4. **Filename**: Enter path and filename. File extension should remain .cer

To sign a BACnet/SC certificate signing request using Keystore Explorer

A BACnet/SC network requires each device to have a unique operational certificate signed by a common Certificate Authority (CA). You can use Keystore Explorer to sign an operational certificate using an existing CA.

1. Open the keystore containing the CA you wish to use.
2. Right-click on the CA and select **Sign** > **Sign CSR**.
3. Select the CSR file to sign. For example, "cert.csr".
4. On the **Sign CSR** dialog:
    1. Select the desired **Validity Period** on the **Sign CSR** dialog, and then click **Apply**.

       NOTE When choosing a validity period, consider that this process will have to be repeated whenever certificates expire. See *To create or replace a BACnet/SC device's operational certificate* (page 18) to replace this certificate when it expires.

       TIP Set **Validity Start** to a previous date to avoid potential time zone issues.
    2. Click **Add Extensions**.
    3. Click **Use Standard Template**.
    4. Select **SSL Server**, then click **OK**.
    5. Select the **Extended Key Usage** extension and click ✏ to select **TLS Web Client Authentication**. **TLS Web Server Authentication** should already be selected, do not deselect it. Click **OK**, then click **OK** on the **Add Certificate Extensions** dialog.
    6. On the **Sign CSR** dialog, click **OK**.
    7. On the **Export Certificate Chain** dialog, set the fields as indicated below, then click **Export**.
        - **Export Length**: Select **Entire Chain**
        - **Export Format**: Select **X.509**
        - **Export File**: Set the path and filename where the signed certificate (.cer) file will be created.

To create or replace a BACnet/SC device's operational certificate

Every device on the BACnet/SC network includes a user interface where the operational certificates are managed. The procedure to create or replace a device's operational certificate is outlined below and is the same for all devices.

Device Type	Certificate management tab
BACnet/SC Hub	Connections > BACnet/SC Port
i-Vu® Pro interface	Connections > Configure tab > Manage Certificates
i-Vu® XT router	Connections > BACnet/SC Port

1 **Create Keystore:** If a keystore has not yet been created, update the five Certificate Name fields (Name, Organization, City, State, Country) as desired, then click **Create Keystore**.

2 **Create Certificate Signing Request (CSR):** Update the five certificate Name fields (Name, Organization, City, State, Country) as desired, then click **Download CSR**. A .csr file will be created and downloaded to your PC.

3 **Sign the CSR:** Send the .csr file to be signed by the manager of the BACnet/SC network's signing CA. If you are using self-signed certificates, see *To sign a Certificate Signing Request using Keystore Explorer* (page 18).

4 **Upload the CSR response files:** You will receive either one or two files from your Certificate Authority (CA) manager to upload to your device. If you receive two files, one is the CA certificate, and the other is the operational certificate. If only one file is provided, it contains both the CA and the operational certificate. For each file you receive, click **Upload** and select the file to upload. After uploading, the CA is listed in the certificate table, and the operational certificate details and expiration date are updated accordingly.

To replace a BACnet/SC network's Certificate Authority

If a Certificate Authority (CA) is expiring or has been compromised, every BACnet/SC device on the network must get an updated operational certificate signed by a new CA. To do this without losing connectivity to existing devices, load the new CA onto every device before removing the old CA from any device.

1 Create a new CA. If you are using self-signed certificates, see step **13** in *To create a BACnet/SC Certificate Authority using Keystore Explorer* (page 17).

2 On each device, add the new CA to the device by uploading the .cer file created in step **1**.

IMPORTANT Do not move on to step **3** until this has been done on every device on the network.

3 On each device, update the operational certificate by having it signed by the new CA and uploading the newly signed certificate to the device. You can use the device's original .csr file or create a new one. After uploading the newly signed certificate, check the certificate table to validate that the operational certificate's issuer now matches the description of the new CA that was uploaded in step **2**. See *To create or replace a BACnet/SC device's operational certificate* (page 18).

IMPORTANT Do not move on to step **4** until this has been done on every device on the network.

4 On each device, remove the old CA by clicking **Delete** beside it in the certificate table.

Troubleshooting

To get a Module Status report

A Module Status report provides information about the hub and verifies proper network communications. You can get this report:

- In the i-Vu® Pro application—Right-click the hub on the navigation tree, then select **Module Status**.

  NOTE If a Module Status report is not generated, ensure that the hub's Device ID is correctly configured in the i-Vu® Pro application.

- In the hub's management user interface—Click ⚙ and select **Modstat** from the drop-down list.

See *Appendix – BACnet/SC Hub Module Status field descriptions* (page 22).

No devices can connect to the BACnet/SC Hub

- Make sure that firewall settings on the server on which the hub is running are allowing incoming traffic on the configured port.
- Confirm that the hub's operational certificate and Certificate Authority have not expired**.**

A particular device cannot connect to the BACnet/SC Hub

- Confirm that the device's operational certificate and Certificate Authority have not expired.
- Confirm that the device's operational certificate is signed by the correct Certificate Authority (the same one that was used to sign the hub).
- Download logs from the failing device and review any BACnet/SC detailed messages that may indicate why the SC connection will not connect.

Hub cannot reach the license server to activate or deactivate your license

If you use a proxy to reach the license manager server and your proxy server uses https:

1. Ask your IT representative to obtain the proxy's certificate chain.
2. In Keystore Explorer:
   a) Open the hub's truststore: `C:\Program Files\BACnet SC Hub\jre\lib\security\cacerts`. No password is required.
   b) Select **Tools** > **Import Trusted Certificate** to import into the truststore.

Device not communicating as expected

You can generate a packet capture to capture network communication on the device's BACnet/SC port. You can download the capture and use Wireshark to view it.

- For the hub, see Diagnostics tab.
- For a controller, see "Network Diagnostics - Packet Capture" in the controller's Installation and Start-up Guide.
- For the i-Vu® Pro application, see command "sccap" in *Console Commands*.

Loss of license (BACnet/SC Virtual Hub only)

The Host ID associated with the hub's license, found on the **Connections** > **License Admin** tab, is tied to the BACnet Network Interface card chosen in the **Admin Tool**. If you change the network card while the license is active, Flexera will invalidate your license the next time it checks it because the Host IDs do not match. In this case, contact Carrier Control Systems Support for a new license.

The proper procedure for changing the BACnet Network Interface card is to:

1. Deactivate your BACnet/SC Virtual Hub license. See License Admin tab.
2. Change the network card using the BACnet/SC Virtual Hub Admin Tool. See *BACnet/SC Hub Installation and Start-up Guide*.
3. Reactivate your BACnet/SC Virtual Hub license. See License Admin tab.

Appendix — BACnet/SC Module Status field descriptions

Field	Description
Product Name	Identifies the Product Type
Version	The version of the driver
Date/Time	Date and time the Modstat was run
Product Serial Number	The serial number of the applied license
Operating System Java Version Processor Architecture Memory	Underlying hardware and software architecture of the hub
Device Instance	A unique ID assigned to the hub
Number of BACnet Objects	The number of BACnet objects that were created in the device and the number of those objects that are trends or events.
Model Name	Identifies the Product Type
Reset Counters:	The number of times each of the following events have occurred since the last restart of the hub
Power failures	Interruption of incoming power
Commanded boots	Includes commands issued from the i-Vu® Pro interface such as the zap manual command, plus commands issued during a memory download.
System errors	Error in the hub's firmware or hardware
S/W Watchdog timeouts	Watchdog is firmware that monitors the application firmware for normal operation. If the watchdog firmware detects a problem, it restarts the application firmware.
H/W Watchdog timeouts	H/W Watchdog will restart the controller if it detects a severe problem with the controller's operating system
Data Link Statistics	Shows network communication statistics to assist with troubleshooting.
BACnet/SC Information	BACnet/SC connection state as of when the Modstat was run. Also shows the web address used to access the hub and whether it is acting as a failover hub.
BACnet/SC Certificates	Lists the operational certificate and certificate authorities installed on the hub, with expiration information.
Routing Information	Gives the current status of the hub's networks.
BACnet/SC Hub License Info	Max number of devices allowed to connect to the hub as per the installed license.
System error message history	Shows the 10 most recent high-severity errors. Earlier messages can be found in the logs.
Warning message history	Shows the 10 most recent low-severity errors and warning messages. Earlier messages can be found in the logs.
Information message history	Shows the 10 most recent information-only messages. Earlier messages can be found in the logs.

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*
7/18/24	Hub cannot reach the license server to activate or deactivate your license	New Topic	X-PO-LO-R-LO
	To create or replace a BACnet/SC device's operational certificate	Updated "Upload the CSR response files"	
	BACnet/SC Port tab	Added format options for Primary Hub URI	
	i-Vu® XT routers	Added list of products Added note regarding router clock	
6/12/23	In Sitebuilder	Revised system path name	X-PM-LO-R-LO
5/15/23	In SiteBuilder	Updated system path	X-D
9/22/22	What is BACnet Secure Connect?	Updated BACnet/SC white paper location	X-PM-LO-R-LO
7/18/22	In SiteBuilder	Added note to step 3 Added step 7	X-PM-LO-R
5/17/22	Certificate best practices	Added first bullet Changed site's "Certificate Authority" to "CA certificate"	X-PM-LO-E-LO

* For internal use only

Carrier ©2024 · Catalog No. 11-808-847-01 · 7/18/2024