



Niagara 4.11 Feature Sneak Peak

Introducing BACnet Secure Connect

September 23, 2021

Q&A

1. **Do you think that BACnet/SC is going to be too complicated for customers and vendors to get the proper ECC communications certificates for the BACnet/SC devices?**

This potential problem is solved with education. We're likely overdue for a good video showing off all the cert tools available in Niagara to make this workflow easier. We also are considering an additional tool to add and will provide a nice overview of all tools at that time.

2. **Do you see a time where customers will demand that BACnet/IP will not be allowed to run on their job sites?**

We have already seen sites where BACnet/IP has been removed from the site specifications, but that does not mean all customers will follow suit. Like all good engineering, it is about applying the correct technology to meet the requirements of the customers.

3. **If there are mixed devices BACnet/IP (old style comm) and newly added BACnet/SC devices. Are both handled by the new driver in 4.11?**

Yes, the BACnet/IP link layer is still included with Niagara's BACnet driver and messages can be routed between the IP and SC link layers.

4. **Do you have a list of BACnet IP SC devices from other manufacturers you have tested the JACEs with these devices?**

We participated in BACnet International's BRITE program and connected Niagara as a Secure Connect node to a node by Shenzhen MEK Intellisys. We have also tested our Secure Connect implementation with BACnet's reference implementation.

5. **Are BACnet SC devices going to be able to be turned off their "SC-ness" in the chance that someone sells an SC device for perhaps an RTU and the school just has a Jace-8000 for a couple VAV's, no supervisor on-site? The picture of the hub/spoke design shows the workstation talking to the SC "because they are node->node communication" but nothing about the Jace-8000 and SC device talk??**

It's likely that would depend on the SC device manufacturer. That said, if a SC device was present it would need a hub and the JACE 8000 can be enabled as a hub.

6. Curious about file transfer to controllers in Niagara. I'm guessing most controllers need their native software to receive the files (because in my case I'm thinking sending DDC). How do you do file transfer to controllers and will the BACnet S/C disallow that since it is a new comm protocol?

There is a BACnet packet type called AtomicFileWrite. Some companies have BACnet devices that get their controller program from the application and send it this way. SC will allow that.

7. Can a JACE be a hub?

Yes, a JACE can be a hub.

8. How will Tridium address SC certificates in the 3rd party controls OEM IP controllers the "JACE" supervises? I assume it will be specific for each particular controls Vendor?

Until addendum CC is integrated with the BACnet standard and Niagara's BACnet reaches that protocol revision, there will not be a BACnet interoperable way to exchange certificate signing requests and signed certificates; proprietary methods will be required to perform these operations.

9. Is the BACnet/SC license included with the standard license or do you have to buy a feature add just to get BACnet/SC?

A station with the regular BACnet license feature can connect to a hub; no additional license features would be required for that functionality. Additional license features will be required to allow stations to host a hub function and initiate/accept SC direct connections. These license features will be standard on Supervisors, Jace8000s, and made available to NPSDK offerings for their consideration.

10. The network drawing shows the N4 supervisor as a HUB, does that mean 2 supervisors would be required - one as primary HUB and one as failover HUB?

Each Secure Connect node must be able to connect to both a primary and failover hub but the presence of a failover hub in the network is optional. If a failover hub is desired, then it may need to be hosted on a separate supervisor or JACE.

11. Am I seeing that devices will require a hub in order to exchange data, so we will no longer be able to push/pull data directly to/from BACnet devices? How will this be handled, in summary, by each manufacturer?

Each Secure Connect node must initiate and maintain an outbound connection to a primary hub in the network. The hub will direct unicast messages between nodes and distribute broadcast messages to all nodes connected to the hub. A connection to the hub is required to receive broadcast messages. In addition to the connection to the hub, it is possible to create direct connections between nodes to exchange unicast messages directly between BACnet devices.

12. Are there traffic considerations to be taken using a single point for the hub? For example, if the site uses a 10Gb fibre backbone etc.?

Sizing the correct hardware always needs to be considered. Choosing to run Niagara on PC where hardware can be adjusted could be a more viable option than squeezing everything through an embedded device.



13. Can Tridium provide a step-by-step best practice and recommended tool(s) with examples for CA and certificate management for Tridium devices and now, BACnet SC?

We have an additional tool in the works to improve certificate workflow and are thinking once released (or near release) a large overview of all cert offerings in Niagara is long overdue.

14. Is the UUID persistent with the Station running on the device, or with the host itself? If I would choose to run two or more Stations simultaneously, would each Station have a unique UUID?

The UUID is persisted with the station. Each station running on a single host would have its own unique UUID.

15. What TCP port is BACnet/SC traffic using? Typical TLS (443)? Or a different port? Are there any issues with the WebService using the same port as BACnet/SC?

BACnet/SC traffic will use the port configured in the Web Service, so port 443 by default. One of the issues that can come up is that you want your BACnet/SC certificate signed by an internal CA, but for most web traffic (e.g. connecting to the station via the browser), you want a cert signed with a public CA. We've addressed this by allowing you to add additional certificate to the Web Service for each purpose, or to add multiple Web Services.

16. Is there support for IPV6?

Yes. Any datalink technology possible that supports IPv4 or IPv6 can be used for a BACnet/SC link layer: Ethernet, WLAN, 4G/5G. Niagara has not yet implemented the IPv6 BACnet link layer.

17. Is Wiretap function working for SC port type?

The Wiretap function will work for the SC port type.

18. Can we have demo for revoked certificate management?

There is support for certificate revocation lists in Niagara's BACnet/SC link layer. A demonstration of this would be helpful in a separate session. BACnet/SC addendum CC includes procedures for excluding devices from a Secure Connect network. Once that addendum is accepted and the Niagara driver advances to that protocol revision, these procedures could be made available and demonstrated.

19. Will this be incorporated into the Tridium Certification or Advanced Certification curriculum? Will there be supplemental training from Tridium for BACnet SC engineering?

We'll communicate the interest to the training department. It's not likely to be covered in the TCP course as there is already much to learn and this is likely an advanced topic.

20. Are there any plans to add multi factor authentication in the future?

Niagara currently supports the Google Authenticator.

21. How BACnet IPv4 device shall work with BACnet/SC device?

A BACnet/IP only device would need to connect to BACnet devices capable of both IP (on a private ethernet bus, for example) and SC so messages can be routed between the IP and SC networks.

22. Can you load balance over multiple hubs?

No. Failover mechanism only (at least at this time per the BACnet spec).

23. You mentioned that large systems will impose a significant processing burden on the designated "hub" device. Will you be offering some sort of estimating algorithm to help folks choose PCs with appropriate resources (or, for that matter, to configure VMs with appropriate resources)?

Do you think a single hub will be able to handle connections from 1000 devices?

In our testing, we supported at least 1,000 connections in a Niagara 4.11 supervisor station running on a PC with Windows 10 version 1909, an Intel i7-7820HQ (2.90 GHz), and 32 GB RAM.

24. How many nodes can be supported in one BACnet/SC network?

The number of node connections that can be supported by the hub(s) in the SC network is most likely the limiting factor on the number of nodes that can be supported.

25. Is the intention of BACnet SC for the JACE(s) to communicate with the Supervisor via BACnet SC vs. FoxS? If so, does supervisor device licensing need to be added vs. Niagara nodes?

Secure Connect allows BACnet devices to communicate securely with each other. SC requires at least one device to host a hub that directs messages between the other nodes. Those other nodes can send messages to the node that is hosting the hub but that node is not necessarily supervising the other nodes. Whether that node is also a Niagara supervisor would be a separate decision.

26. Should we expect slower communications in general compared to BACnet/IP?

The overhead of encrypting the messages and routing them through a hub will most likely cause communication over an SC network to be somewhat slower than over an IP network. That trade-off will hopefully be acceptable given that the communications are now secure.

27. Is there any range for using websocket ports in websocket URIs?

Any valid port number can be used in the web socket URIs. There may, however, be port ranges that are restricted by the operating system of certain devices.

28. Will a mixed BACnet/IP and BACnet/SC network be secure?

Communications within an SC network or routed between SC networks only are secure. If messages are routed between SC and IP networks, then those communications may not be secure depending on how well the IP network infrastructure is protected. There is a Secure Path data option that can be used to detect whether a message has remained within SC networks between the source and destination devices.



29. Can a 4.11 Jace handle an external 3rd party CA (=get its certificates from it)?

Certificate signing requests generated by a JACE can be processed by an external 3rd party CA and the resulting signed certificate can be imported back into the JACE. The signed certificate must contain the entire certificate chain in order to be re-imported. Note: certificates used in an SC network should be directly signed by a CA controlled by the site; they should not be directly signed by a public CA.

30. Are user actions tracked in any way in BACnet/SC so we could track overrides on points who & when did last action?

There is no additional audit logging with SC beyond what is already available in Niagara.