DOME™ Building Automation Starter Kit

Testing and Troubleshooting Guide

P/N DD-0015 | Rev 1.1 | October 2022

Proprietary Notices

1. Legal Disclaimer

The use of DOME is subject to Veridify's standard license terms and conditions as set forth in the DOME Building Automation Starter Kit - Proprietary Notices; License Terms and Conditions ("Standard Terms"), as well as the Software-as-a-Service Agreement. This documentation does not expand or otherwise modify Veridify's Standard Terms or mutually, in writing, agreed upon terms, including, but not limited to, the disclaimers and warranties expressed therein.

2. Copyright Notice

Third Party notices, terms, and conditions pertaining to third-party software and hardware can be found at:

https://www.veridify.com/terms-of-use/

3. Trademark Notice

Device Ownership and Management Enrollment, and DOME are trademarks or service marks (individually and collectively, "Marks") of Veridify Security Inc. ("Veridify"). The Marks displayed in this documentation or on any hardware or in any software represent some of the proprietary rights currently owned or controlled by Veridify and are not intended to be a comprehensive compilation of all Veridify's worldwide proprietary ownership rights. See, https://www.veridify.com/terms-of-use/ for representations of additional Marks owned or controlled by Veridify and additional guidance with respect to Veridify Marks All other trademarks and service marks, which may be registered in certain jurisdictions, belong to the holder or holders of such marks.

4. Patent Notice

DOME is protected by certain patents. In accordance with the virtual marking provisions of the American Invents Act, 335 U.S.C. 287(a), See, https://www.veridify.com/terms-of-use/, which enumerates the list of products and components that may be protected by one or more patents, or patents pending in the U.S. and elsewhere. Certain third-party components embedded in DOME may be protected by certain patents of such third-party; reference should be made to the third-party documentation.

DOME™ Building Automation Starter Kit — Testing and Troubleshooting Guide

Table of Contents

1. Functional Testing

By now you should have a DOME installation that resembles the starter kit architecture given in the installation guide and repeated in Fig. 1.

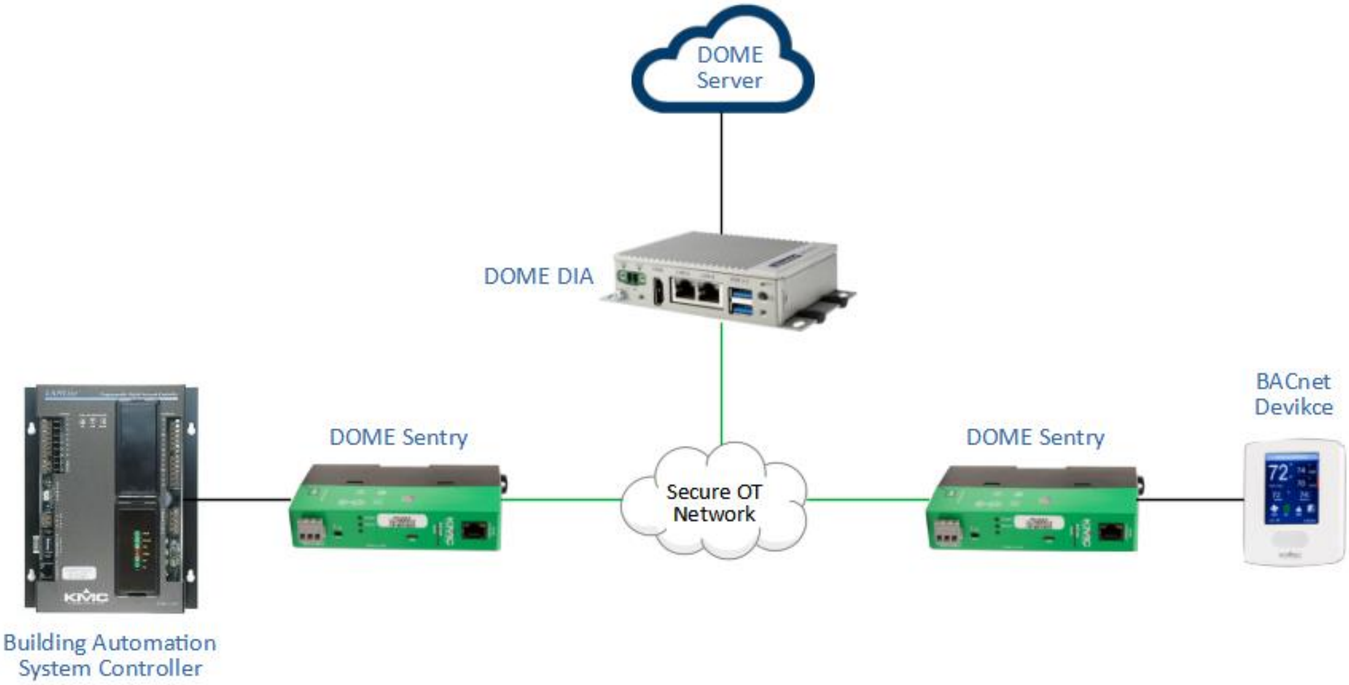


Fig. 1. DOME Starter Kit architecture

1.1. Initial verification

The simplest and fastest way to test your overall installation is to ensure that your BAS Controller can communicate with your BACnet/IP endpoint device. Because each building installation is different, it is not possible to provide a step-by-step functional test procedure, but if your endpoint devices can communicate with each other, you have successfully installed and configured the components. You should also ensure that unicast messages as well as broadcast messages are able to pass. If one of your endpoint devices is a BACnet/IP to MS/TP router, you should check to make sure that the other endpoint device (assuming it is some type of BAS controller) can see all the MS/TP devices behind the router.

1.2. Viewing secure BACnet packets

The best way to view the operation of DOME Sentry™ devices from a security perspective is to capture BACnet packets with Wireshark or other packet capture tool. Fig. 2. shows the typical setup. What follows is just a guideline—you may need to adapt the specific steps to your own installation environment and preferred BACnet tools.

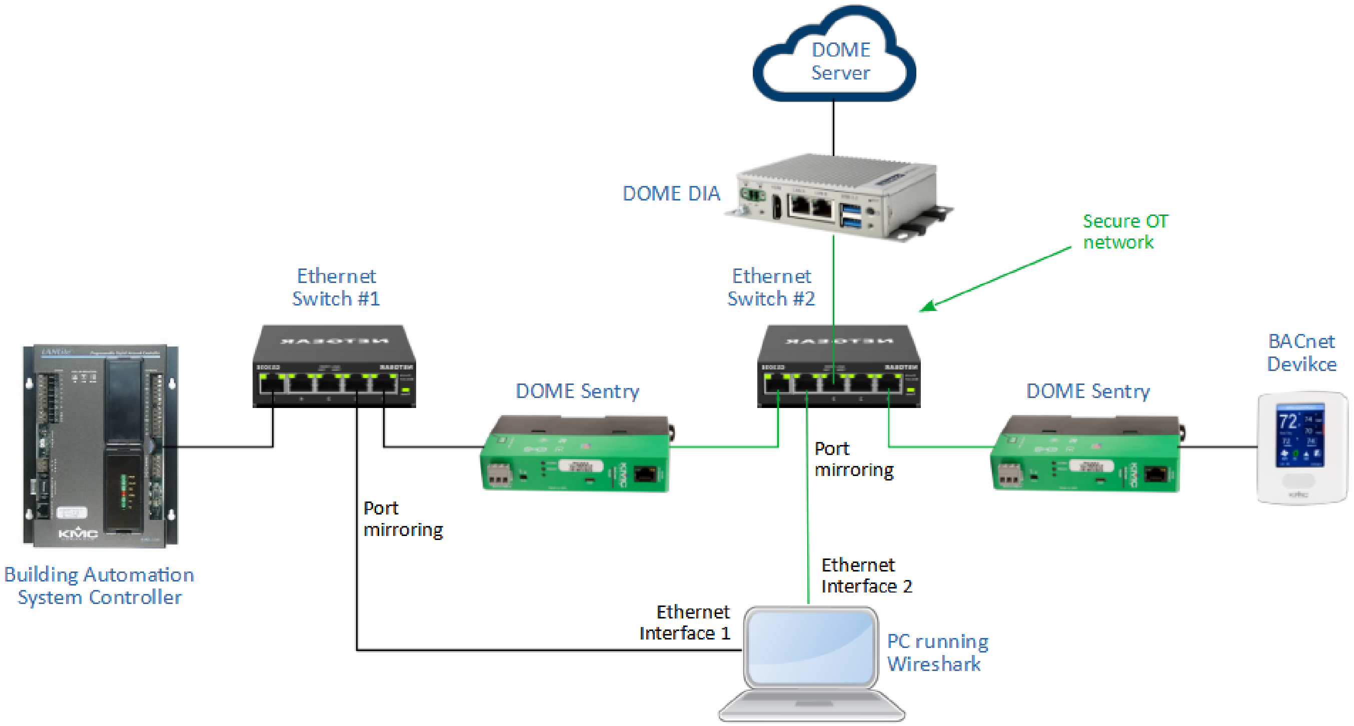
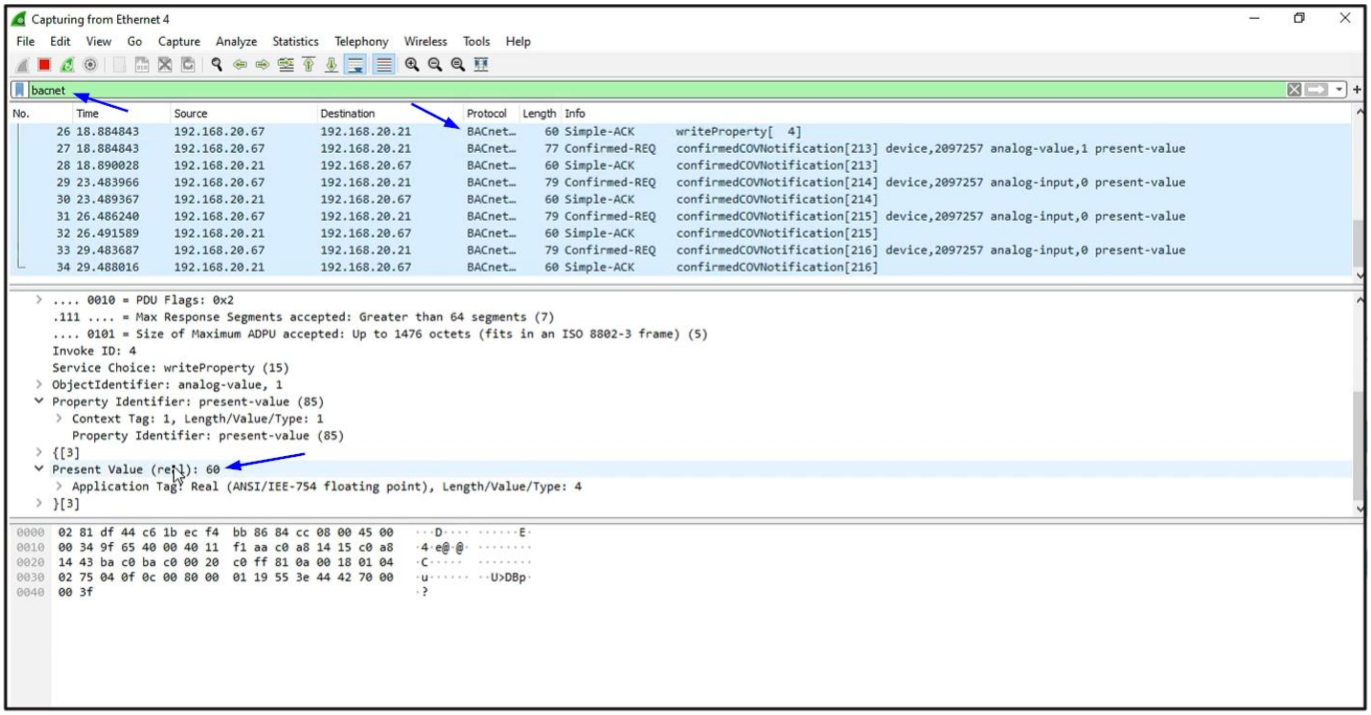


Fig. 2. Example DOME Starter Kit with packet capture

The idea is to capture packets on the protected side of the DOME Sentry and compare them with the packets on the secure OT side. In the example shown in Fig. 2., Ethernet switch #1 is configured to mirror the traffic between the BAS and the first DOME Sentry. Those packets appear in port 4 of the switch and may be captured on a PC running Wireshark. Similarly, Ethernet switch #2 mirrors the secure BACnet packets on the OT network and makes them available to the PC via port 2. You can use a PC with two Ethernet ports, a PC with two USB-to-Ethernet adapters, or two separate PCs.

Fig. 3. shows an example of BACnet messages captured outside of the secure OT network. This capture uses Wireshark's "bacnet" display filter. Note that the nature of each message is easily discernable in the "Info" column of the capture screen. If you select a single message, you can also read the critical values, such as "60" in the example.


Capturing from Ethernet 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bacnet

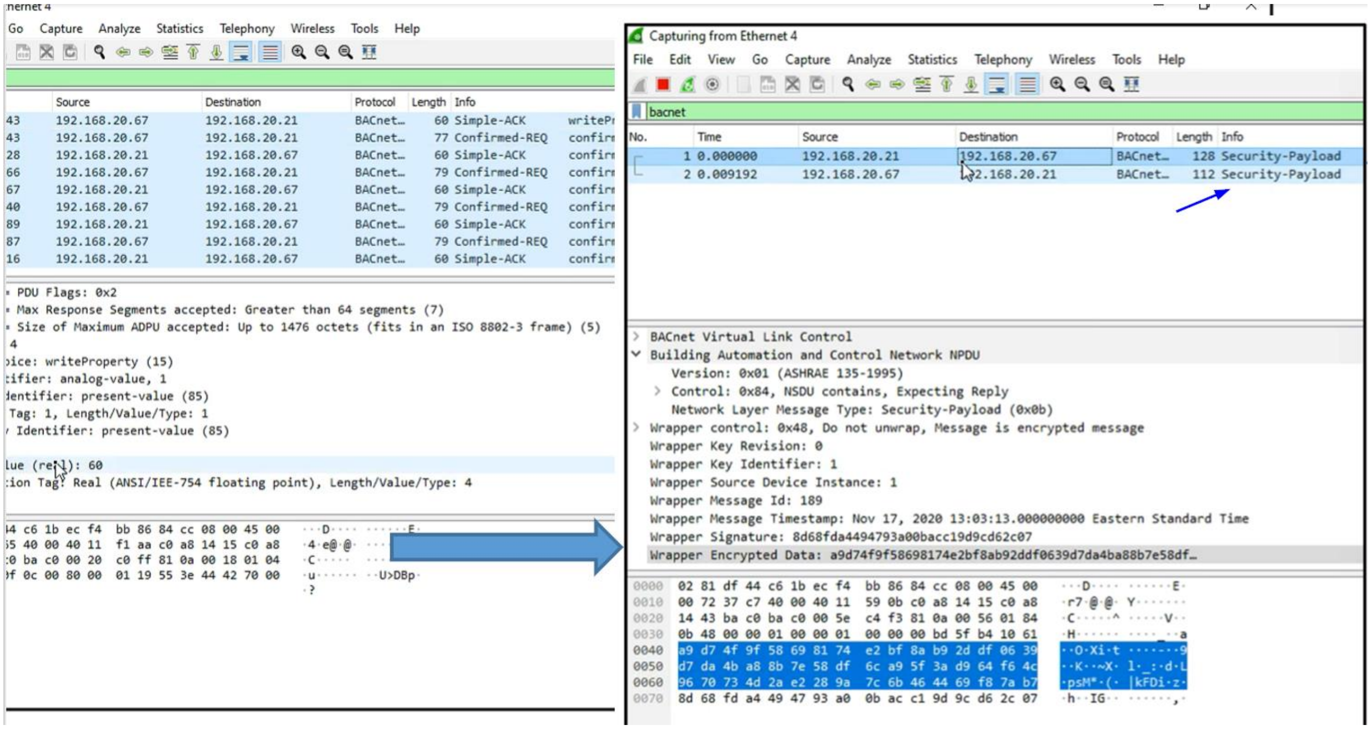
```
No.  Time          Source          Destination     Protocol  Length Info
  26 18.884843     192.168.20.67   192.168.20.21   BACnet…   60 Simple-ACK     writeProperty[  4]
  27 18.884843     192.168.20.67   192.168.20.21   BACnet…   77 Confirmed-REQ  confirmedCOVNotification[213] device,2097257 analog-value,1 present-value
  28 18.890028     192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirmedCOVNotification[213]
  29 23.483966     192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirmedCOVNotification[214] device,2097257 analog-input,0 present-value
  30 23.489367     192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirmedCOVNotification[214]
  31 26.486240     192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirmedCOVNotification[215] device,2097257 analog-input,0 present-value
  32 26.491589     192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirmedCOVNotification[215]
  33 29.483687     192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirmedCOVNotification[216] device,2097257 analog-input,0 present-value
  34 29.488016     192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirmedCOVNotification[216]
```

```
 > .... 0010 = PDU Flags: 0x2
   .111 .... = Max Response Segments accepted: Greater than 64 segments (7)
   .... 0101 = Size of Maximum ADPU accepted: Up to 1476 octets (fits in an ISO 8802-3 frame) (5)
   Invoke ID: 4
   Service Choice: writeProperty (15)
 > ObjectIdentifier: analog-value, 1
 v Property Identifier: present-value (85)
   > Context Tag: 1, Length/Value/Type: 1
     Property Identifier: present-value (85)
 > {[3]
 v Present Value (real): 60
   > Application Tag: Real (ANSI/IEE-754 floating point), Length/Value/Type: 4
 > }[3]
```

```
0000  02 81 df 44 c6 1b ec f4  bb 86 84 cc 08 00 45 00   ···D····  ······E·
0010  00 34 9f 65 40 00 40 11  f1 aa c0 a8 14 15 c0 a8   ·4·e@·@·  ········
0020  14 43 ba c0 ba c0 00 20  c0 ff 81 0a 00 18 01 04   ·C·····   ········
0030  02 75 04 0f 0c 00 80 00  01 19 55 3e 44 42 70 00   ·u······  ··U>DBp·
0040  00 3f                                              ·?
```

Fig. 3. Wireshark capture of plaintext BACnet messages

In contrast, Fig. 4. shows an example of BACnet messages on the secure OT network. These messages are classified as “Security-Payload” messages by Wireshark, and the message content is now encrypted. Note that even though the payload is now encrypted, Wireshark still considers them to be BACnet packets.


nernet 4
Go Capture Analyze Statistics Telephony Wireless Tools Help
Capturing from Ethernet 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bacnet

```
     Source          Destination     Protocol  Length Info
43   192.168.20.67   192.168.20.21   BACnet…   60 Simple-ACK     writePr
43   192.168.20.67   192.168.20.21   BACnet…   77 Confirmed-REQ  confirm
28   192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirm
66   192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirm
67   192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirm
40   192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirm
89   192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirm
87   192.168.20.67   192.168.20.21   BACnet…   79 Confirmed-REQ  confirm
16   192.168.20.21   192.168.20.67   BACnet…   60 Simple-ACK     confirm
```

```
= PDU Flags: 0x2
= Max Response Segments accepted: Greater than 64 segments (7)
= Size of Maximum ADPU accepted: Up to 1476 octets (fits in an ISO 8802-3 frame) (5)
 4
oice: writeProperty (15)
tifier: analog-value, 1
dentifier: present-value (85)
 Tag: 1, Length/Value/Type: 1
/ Identifier: present-value (85)

lue (real): 60
:ion Tag: Real (ANSI/IEE-754 floating point), Length/Value/Type: 4
```

```
4 c6 1b ec f4  bb 86 84 cc 08 00 45 00   ···D····  ······E·
5 40 00 40 11  f1 aa c0 a8 14 15 c0 a8   ·4·e@·@·  ···
0 ba c0 00 20  c0 ff 81 0a 00 18 01 04   ·C·····   ···
f 0c 00 80 00  01 19 55 3e 44 42 70 00   ·u······  ··U>DBp·
                                         ·?
```

```
No.  Time          Source          Destination     Protocol  Length Info
   1 0.000000      192.168.20.21   192.168.20.67   BACnet…   128 Security-Payload
   2 0.009192      192.168.20.67   192.168.20.21   BACnet…   112 Security-Payload
```

```
 > BACnet Virtual Link Control
 v Building Automation and Control Network NPDU
      Version: 0x01 (ASHRAE 135-1995)
    > Control: 0x84, NSDU contains, Expecting Reply
      Network Layer Message Type: Security-Payload (0x0b)
 > Wrapper control: 0x48, Do not unwrap, Message is encrypted message
   Wrapper Key Revision: 0
   Wrapper Key Identifier: 1
   Wrapper Source Device Instance: 1
   Wrapper Message Id: 189
   Wrapper Message Timestamp: Nov 17, 2020 13:03:13.000000000 Eastern Standard Time
   Wrapper Signature: 8d68fda4494793a00bacc19d9cd62c07
   Wrapper Encrypted Data: a9d74f9f58698174e2bf8ab92ddf0639d7da4ba88b7e58df…
```

```
0000  02 81 df 44 c6 1b ec f4  bb 86 84 cc 08 00 45 00   ···D····  ······E·
0010  00 72 37 c7 40 00 40 11  59 0b c0 a8 14 15 c0 a8   ·r7·@·@·  Y·······
0020  14 43 ba c0 ba c0 00 5e  c4 f3 81 0a 00 56 01 84   ·C·····^  ·····V··
0030  0b 48 00 00 01 00 00 01  00 00 00 bd 5f b4 10 61   ·H······  ····_··a
0040  a9 d7 4f 9f 58 69 81 74  e2 bf 8a b9 2d df 06 39   ··O·Xi·t  ····-··9
0050  d7 da 4b a8 8b 7e 58 df  6c a9 5f 3a d9 64 f6 4c   ··K··~X·  l·_:·d·L
0060  96 70 73 4d 2a e2 28 9a  7c 6b 46 44 69 f8 7a b7   ·psM*·(·  |kFDi·z·
0070  8d 68 fd a4 49 47 93 a0  0b ac c1 9d 9c d6 2c 07   ·h··IG··  ······,·
```

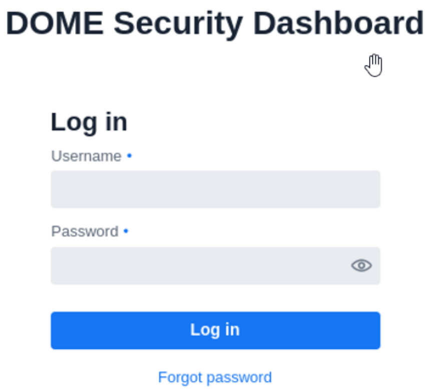
Fig. 4. Wireshark capture of secure BACnet messages

1.3. Viewing DOME Security Dashboard

Because DOME Sentries sit between the secure and insecure OT network, they are in a unique position to record building automation traffic that can detect security breaches, anomalies, and other significant events. Such occurrences are likely to go unnoticed by building management systems, so the detection of these incidences provides valuable intelligence to building owners that they cannot otherwise get.

Veridify has created a web-based dashboard that receives a synopsis of all building automation traffic that passes through every Sentry installed in a building. That information is filtered and processed to provide a summary of the security health of a building. Additionally, the dashboard displays trends and potential security alerts, and it enables users to drill down to time-stamped log messages from each and every DOME Sentry.

To view the dashboard, point your browser to dome.veridify.com and provide your login credentials:



2. Security Testing

The main feature of the DOME Sentry is that, in addition to reporting potential anomalies and important events, it blocks all cyberattacks. One way to test that is to connect a BACnet/IP device to the secure OT network and command it to send a message. An easy way to do that, referring to Fig. 2 above, is to disconnect the Building Automation System Controller from Ethernet Switch #1 and plug it into Switch #2. If you generate a BACnet message from the BAS as if it were an attacker that gained access to the secure OT network, it will be rejected by both DOME Sentries—the message will never make it to the other BACnet endpoint device. If you perform this test and are logged into your security dashboard, you will see a corresponding alert notification.

Another potential attack would be to disconnect one or more DOME Sentry devices that protect a building automation system. Try unplugging one of the Ethernet cables from either DOME Sentry. If you disconnected the Sentry from the network, then after 60 seconds, the device will be marked off-line in the dashboard. After five minutes remaining offline, the system will raise an alert. If you disconnected the protected device behind the Sentry, an alert will be raised immediately.

3. Troubleshooting

If you are unable to pass BACnet traffic through the secure OT network, these are the most likely reasons:

3.1. One or more of the DOME Sentries do not have power.
Refer to section 4.1 "DOME Sentry Installation Procedure" in the DOME Starter Kit Installation Guide.

3.2. Ethernet cable connecting to the DOME Sentries are in the wrong port.
Refer to section 4.1 "DOME Sentry Installation Procedure" in the DOME Starter Kit Installation Guide.

3.3. The Network list in the DIA is misconfigured.
Refer to section 3.5 "OT Network Configuration" in the DOME Starter Kit Installation Guide.

3.4. You have inserted an Ethernet switch in between a DOME Sentry and the device it protects before the Sentry has been configured.
Temporarily remove the switch until the Sentry has been configured.

3.5. One of your BACnet devices does not respond to the BACnet "whois" message or was not online when the Sentry configured itself.
Try the installation with BACnet devices that are known to respond to the standard whois message, and ensure all devices are online when the Sentry powers on to configure itself. If you know the list of devices, you can verify what the Sentry found by using the Sentry "showconfig" user.

4. Technical Support

Please direct all technical support inquiries to: suport@veridify.com or by phone 203-227-3151 (Option 6)