Cybersecurity | Security Bulletin

Hardening Bulletin: Securing BACnet BBMDs and Foreign Device Access

DELTA IBT POLICY: KEEP BACNET BBMDS AND FOREIGN DEVICES OFF THE PUBLIC INTERNET

Summary

The exposure of BACnet controllers to the public internet is a widespread cybersecurity concern across the building automation industry. These exposures can leave building automation systems vulnerable to unauthorized access and operational disruption. This is a network configuration and security issue, rather than a specific product vulnerability, and affects equipment from multiple manufacturers, including Delta Intelligent Building Technologies Canada Inc, (Delta IBT).

Recent cybersecurity incidents involving internet-exposed control systems reinforce the importance of protecting building automation networks against unauthorized access. Delta IBT has consistently emphasized secure network practices through partner training and its Hardening Guides. This bulletin reinforces these expectations and highlights the importance of adopting secure communication technologies.

Delta IBT requires the use of BACnet Secure Connect (BACnet/SC) for all remote BACnet communications. BACnet/SC provides encrypted, authenticated communications designed to protect building automation networks against unauthorized access.

BACnet Broadcast Management Devices (BBMDs) and foreign device registration serve legitimate functions within BACnet networks but do not provide secure remote access. **BBMDs and foreign device registration must not be used as a means of remote access.** All customers and sites are expected to review their existing installations, ensure compliance with Delta IBT's Remote Access Policy outlined below, and transition remote BACnet connectivity to BACnet/SC. Where BACnet/SC is not yet possible, every BBMD must be isolated from direct public access. Any site without the ability to use BACnet/SC should remain behind a firewall and should only be remotely accessed using an appropriate VPN. BBMD and foreign device connections are not an approved method of remote access from external locations. DELTA IBT's Remote Access Policy, set out below, defines the only approved method.

DELTA IBT Remote Access Policy

Effective immediately, the following policy applies to all DELTA IBT BACnet installations:

1. **Remote access through a BBMD is not supported.** Remote access to a building network from the public internet through a BBMD, whether by foreign device registration or any other method, is unsupported and not approved by Delta IBT.
2. **BACnet/SC is the only approved method.** BACnet Secure Connect (BACnet/SC) is the only Delta IBT-approved method for connecting to a building network from the public internet.
3. **Building networks must be private.** All building networks must be secured within a private network. BACnet devices must not be connected directly to the internet.

***Note:** BACnet/SC uses outgoing TCP connections and does not require port forwarding for access. Therefore, BACnet/SC devices are not technically connected directly to the internet via incoming public internet connection.

Sites that do not meet this policy should follow the steps in How to Harden a Site.

Configurations to Review

Category	Configuration
Open BBMDs	BBMDs reachable from the internet that accept foreign device registrations without a password
Exposed BACnet/IP	Any site where UDP is port-forwarded or otherwise reachable from the public internet
Remote access via BBMD	Any site that relies on a foreign device connection to provide remote access, even with passwords enforced
Network not isolated	Any site where BACnet devices are not behind a VLAN or other private network, or are connected directly to the internet

Why This Matters

An exposed, unauthenticated BBMD gives an outsider the same level of BACnet access as a device installed on site. The consequences include:

Threat	Impact
Unauthorized changes to setpoints, schedules and outputs	Values controlling heating, cooling, ventilation and lighting can be written remotely, with direct effect on occupants and equipment.
Device-level commands	Commands that reinitialize controllers or disable their communications can take a building system offline.
Reconnaissance of the building network	Device, object and network details can be read freely, giving an attacker a map of the site.
Abuse of BBMD broadcast forwarding	Exposed BBMDs can be used to flood the site BACnet network or to generate traffic against third parties.
Liability and reputational exposure	An incident traced to an unprotected BBMD reflects on the installing partner, the building owner and the product vendor.

Required Configuration for Remote Access

Delta IBT requires all sites to use BACnet/SC for remote access.

Configuration	Description	Status
BACnet Secure Connect (BACnet/SC)	BACnet/SC	**Recommended standard. Encrypted, certificate-authenticated connections. Expected for all new installations and the target state for every existing site.**

Non-Approved Configurations for Remote Access

A BBMD that accepts unauthenticated foreign device registrations from the internet leaves the site open to anyone who finds it.

Configuration	Description	Status
BBMD with password checks	Foreign device password checks enforced on every BBMD	**Suitable only for use within a private building network that is not accessable from inbound internet connections. Not approved for access from the public internet. Use strong, unique passwords per site**
Open BBMD	BBMD accepting unauthenticated foreign device registrations	**Not supported or approved. An open BBMD is a misconfiguration, not a remote access design. Harden as a priority using the steps below.**
Internet-exposed BACnet/IP	Port-forwarding UDP 47808 or any other BACnet/IP port from the internet	**Not supported or approved. Under DELTA IBT policy, BACnet devices must never be connected directly to the internet, with or without a BBMD.**
BBMD for remote access	Foreign device registration used as a remote access method	**Not supported or approved. Remote access to a building network through a BBMD from the public internet is not approved, even with passwords enforced.**

Remote Access

BBMD and foreign device registration were designed to pass BACnet broadcasts between IP subnets. They were not designed as a remote access mechanism and must not be used as one. Under DELTA IBT's Remote Access Policy:

- BACnet/SC is the only approved method for connecting to a building network from the public internet. Its connections are encrypted and authenticated by certificate.
- The building network must sit behind a firewall, agreed with the building owner's IT team, with no BACnet devices connected directly to the internet.

How to Harden a Site

Work through the following steps for each site you install or maintain. Schedule changes in a planned maintenance window and agree them with the building owner so the site stays operational:

Step	Action	Owner
1	Inventory every site. Identify every BBMD and every device configured for foreign device registration, and back up controller databases before making changes.	Partner/Customer
2	Confirm the building network sits within a private network that is blocked from incoming public IP traffic. Test from outside the site that UDP 47808 or any other custom BACnet/IP port are not reachable from the internet.	Partner/Customer
3	If the site needs remote access, put BACnet/SC in place first, then remove any firewall or router port forward that exposes BACnet/IP.	Partner/Customer/Site IT
4	Migrate the site to BACnet/SC.	Partner/Customer
6	Confirm with the building owner that the site is operating normally and document the agreed remote access method.	Partner/Customer
7	If you need assistance with any of these steps, contact DELTA IBT technical support.	Partner/Customer

Next Steps

Partners/Customers/Sites who install and maintain BACnet systems are responsible for ensuring those systems are configured securely. DELTA IBT will continue to monitor public internet exposure and may reach out to offer help with sites that remain exposed. Password enforcement reduces exposure but is not a substitute for BACnet/SC. DELTA IBT asks all partners to review their installations and take the actions above. For support, including help configuring BBMD passwords or moving a site to BACnet/SC, contact DELTA IBT technical support.

Real-World Incidents

Attacks on internet-exposed control systems are no longer theoretical. Two recent, publicly reported campaigns show what happens when controllers are left reachable from the internet:

Incident	What happened	Relevance to BACnet sites
Danfoss refrigeration controllers Europe, October 2026	On the night of October 11–12, attackers remotely took over Danfoss refrigeration management systems at hundreds of supermarkets, mainly in France. They forced fridges and freezers into continuous defrost with setpoints as high as 50°C (122°F) and changed alarm thresholds, so in some stores temperatures climbed for hours before staff noticed. Stock losses run into the millions of euros. Danfoss said most affected units were older models it no longer updates. The attack has not been publicly attributed.	The same pattern as an open BBMD: a supervisory controller reachable from the internet, with setpoints and alarm limits that can be written remotely. An open BBMD exposes the same kinds of values on a BACnet site.
Iranian-affiliated PLC targeting U.S. critical infrastructure, 2026	A joint advisory from CISA, the FBI and partner agencies (AA26-097A, published April 7, 2026 and updated July 22, 2026) reports Iranian-affiliated actors targeting internet-connected PLCs from Rockwell Automation/Allen-Bradley, Schneider Electric and Siemens across sectors including energy and water. The actors altered PLC project files and manipulated HMI and SCADA displays, causing operational disruption and financial loss.	State-affiliated actors are actively searching for and exploiting internet-exposed control devices across multiple vendors. The advisory's first recommended action is to remove these devices from direct internet exposure, the same action this bulletin asks of every BACnet site.

In both cases, the attackers did not need sophisticated techniques. They started from the same place: control devices reachable directly from the internet, with weak or no authentication. An open BBMD offers the same starting point.

Sources: CISA et al., Joint Cybersecurity Advisory AA26-097A; public reporting by SecurityWeek, The Hacker News and Sekoia, October–November 2026.