Product Bulletin

Security advisory for XWEB monitoring systems

Dear Customer, For over 30 years, Copeland Controls has been a trusted leader in Refrigeration and HVAC, delivering reliable, high-quality products that set industry standards. Our legacy is built on a foundation of excellence, powered by rigorous testing and an unwavering commitment to reliability and performance. Copeland Controls' XWEB monitoring units have provided reliable service to customers across essential markets for over two decades. During that time, technology and security requirements have evolved significantly, and we are committed to ensuring that our products meet today's standards. Safeguarding the safety, quality, and security of our products is integral to everything we do. We actively partner with the global cybersecurity community, encouraging external experts to report potential vulnerabilities through our dedicated processes. This fosters transparency, trust, and continuous improvement.
We acknowledge the vulnerability identified in a discontinued, end-of-life generation of XWEB EVO controllers. A comprehensive investigation was launched, and the following provides the necessary recommendations to address the vulnerabilities and ensure our customers' systems remain secure.

Recommendations for the Safe Use of XWEB Supervisors

Summary

Remove all XWEB EVO from the public Internet immediately, then review for suspicious activity from the local network and restore devices if necessary.

This advisory lists additional measures that can be implemented to reduce cybersecurity risk associated with XWEB EVO supervisors and explains how to recover a unit that may have been accessed without authorization.

1. **Remove Internet exposure.** Ensure XWEB EVOs cannot be accessed from outside your local network (see *Immediate risk mitigation measures*).
2. **Check and restore the unit.** Follow the step-by-step procedure, working only from the local network.
3. **Plan your migration.** XWEB EVO has reached End of Service and no longer receives security patches; XWEB PRO is the supported platform. Even with PRO, do not expose to the internet

Immediate risk mitigation measures

Apply these measures to every XWEB EVO, whether or not you suspect unauthorized access.

- **Remove XWEB EVOs from the public Internet.** No port forwarding, no DMZ and no direct public IP address.
- **Restrict physical access** to authorized personnel only (for example, limit who can enter equipment rooms and use keyed entry where possible).
- **Use a VPN service** for remote access, so the XWEB is reached only through a restricted and encrypted tunnel.

Copeland Controls recommendations

Follow all instructions and specifications included in the device manual and apply security best practices, including but not limited to:

- never exposing the control system to the broader Internet;
- configuring your firewall to restrict access to administrative protocols, such as SSH;
- configuring your network to restrict inbound and outbound communications to and from the control system;
- updating default account passwords and ensure passwords align with industry best practices;

Copeland Controls S.r.l. | Z.I. Via dell'Industria, 27
32016 Alpago (BL) ITALY - copeland.com - dixell@copeland.com
To learn more, visit **copeland.com**
©2026 Copeland LP

COPELAND

- configuring and enabling HTTPS for web-based traffic, without exposing the controller's web interface to the broader Internet.

How to check and restore a potentially compromised XWEB EVO

Connect to the XWEB only from the local network and work through the steps below in order.

Before you begin

- **Isolate the unit.** Remove any port forwarding or DMZ rule pointing to the XWEB, or disconnect the router's WAN connection, before you start.
- **Record what you find.** Take screenshots of the user list, profiles and system settings before changing anything. Copeland support may need them, and so will any incident report.

Procedure

1. **Log in with your administrator password.**
    - If the password has been changed and you cannot log in, contact Copeland Technical Support, available 24/7, at ColdChain.TechnicalServices@copeland.com and ask for instructions to obtain a temporary access password.
    - Support will need the current XWEB EVO date and the MAC address shown on the XWEB login page. Press **CTRL+ALT** on the login page to display the MAC address.
2. **Restore your latest backup.** Once logged in, restore the most recent backup, selecting:
    - System
    - Devices, Layout, Tools, Users
    - Make sure the backup was created *before* the suspected unauthorized access.
3. **If you have no backup, check users and profiles.** Confirm that the user list matches what you expect, and remove any user or profile you do not recognize.
4. **Change all user passwords.** Each password must meet these minimum requirements:
    - At least 8 characters
    - At least one digit
    - At least one uppercase letter
    - At least one lowercase letter
    - Must not contain the username
    - Must not contain the hostname or system name
    - Must not consist of a single repeated character (e.g., aaaaaaaa)
    - *Recommended: 12 or more characters, at least one symbol, and a different password for every account.*
5. **Update the software.** XWEB EVOs are no longer supported. It is strongly recommended that all customers upgrade to a supported platforms. Download the latest software version for your XWEB EVO model from the Copeland System Software Update page and install it from **SYSTEM > Update > Updates**.
6. **Review the system configuration.** Check that every service in use is set up correctly, including the network settings (gateway and DNS) and the mail server settings.
7. **Check alarm management.**
    - Alarm categories exist and are assigned to the devices' alarm variables.
    - Where needed, alarm categories are linked to a level that sends email or SMS notifications or triggers alarm relays.
    - Email and SMS notification recipients are present and correct.
    - Trigger a test alarm to confirm that notifications are actually delivered.
8. **Restore device parameters from backup files**, if you have them:

1. Select the device from **DEVICES**.
2. Open the **Parameters** tab.
3. Click **Import** and select the backup file.
4. Once the parameter values are loaded, click **Write**.

9. **If you have no parameter backups,** select each device in turn, run a **Read** of its parameters, and verify that

©2026 Copeland LP

they suit the application (setpoints, alarm thresholds, defrost settings).

10. **Create a new backup.** When checks and any restore are complete, always create a new backup and keep a copy off the unit.

Additional recommendations to secure access

These measures close the most common entry points beyond the basics above.

Remote access

- **Leverage a VPN service.** Consult your IT department to assist implementing your organization's approved VPN service

Network

- Place the XWEB on a dedicated network segment (VLAN), separate from office, point-of-sale and guest Wi-Fi networks.
- Allow only the outbound traffic the XWEB needs (for example, mail server, DNS, NTP and the Copeland update server) and block everything else.
- Verify exposure from outside: from a connection off the site network, such as a phone with Wi-Fi turned off, try the site's public IP address in a browser. The XWEB login page must not appear.

Accounts and passwords

- Each user must have a unique, named account; shared accounts should not be permitted.
- Give each account the most restrictive profile that fits the job, and limit administrator rights to one or two people.
- Disable or delete accounts that are no longer needed, and review the user list at least once a year.
- Change passwords after any outside service visit that used a privileged account.
- Never reuse XWEB passwords elsewhere or base them on the site, store or installer name.

Monitoring and backups

- Back up the system configuration and device parameters on a regular schedule and after every significant change; keep copies off the unit.
- Keep the XWEB clock synchronized (NTP) so records and logs carry accurate timestamps.

If you suspect unauthorized access

- Isolate the unit first, then recover it (see *Before you begin*).
- Check product temperatures directly at the cases: altered setpoints or alarm thresholds can put food safety at risk.
- Notify Copeland Technical Support and your IT or security team and, where required, the competent authority (in the U.S., CISA).

Plan your migration to XWEB PRO

XWEB EVO has reached End of Service and will receive no further software updates or security patches. We strongly recommend migrating to XWEB PRO, the current platform, which is actively maintained and regularly updated.

Technical support

Copeland Technical Support is available 24/7 at ColdChain.TechnicalServices@copeland.com.

Copeland Controls S.r.l. | Z.I. Via dell'Industria, 27
32016 Alpago (BL) ITALY - copeland.com - dixell@copeland.com
To learn more, visit **copeland.com**
©2026 Copeland LP