AutomatedLogic
1150 Roberts Boulevard
Kennesaw, Georgia 30144
770/429-3000
Fax 770/429-3001
www.automatedlogic.com

WebCTRL® Cloud Security Policy

Rev. 4/25/2022

Overview

At Carrier, system and operational security is integral. To ensure the security posture of products and offerings manufactured at Carrier, research and development teams leverage the domain expertise of our own world class secure architecture domain experts to design for security and continuously analyze, identify, and improve our offerings. Carrier's processes and standards ensure the appropriate methods and controls are proactively applied through all phases of the development and product support lifecycle. Rigorous testing and analysis capabilities are continuously implemented to ensure our products meet and exceed international standards of cybersecurity assurance, and Carrier's own demanding requirement for customer mission success. The Carrier Way also ensures that customers and end users are responsibly supported for cybersecurity assurance throughout the life of our offerings.

Security Team

Our team is comprised of highly experienced and credentialed veterans; diverse and dynamic cybersecurity domain experts who've maintained prominent roles and responsibilities in designing, building, and operating highly secure complex systems at companies ranging from startups to large public companies.

Cybersecurity Principles

Carrier endeavors to adhere to the following security principles in every product, offering or service development, deployment, support and/or maintenance activity:

- Application and implementation of the appropriate proactive and reactive security controls is a necessity throughout all phases of the Secure Product Development and Support Lifecycle, in accordance with industry standards and best practices for cybersecurity, and in a manner that ensures Carrier and customer mission success.
- Processes and support services shall align with and, where possible, exceed appropriate industry best practices, codes, and standards, in a manner that transcends fundamental security maturity norms in a manner that ensures Carrier and customer mission success.

- Security requires teamwork, situational awareness, domain expertise, context, collaboration, transparency and continual analysis, improvement, and vigilance.
- Comprehensive identification and proactive management of all cybersecurity risk in a repeatable and consistent manner is foundational to support the Carrier standard for security maturity.
- World class capabilities, practices and activities shall be maintained in the cybersecurity domain areas of secure deployment, threat intelligence, monitoring, and cybersecurity incident response, to consistently provide responsible and effective cybersecurity channel support and transparency.

Technical Security Standards

The WebCTRL Cloud application provides a very high level of security to protect against unauthorized access. This memorandum briefly outlines design, security, configuration, and implementation aspects of your WebCTRL Building Automation System Cloud application.

- WebCTRL source code is subjected to source code analysis and independent third-party penetration testing as part of our software development lifecycle process.
- All third-party libraries are scanned for known vulnerabilities.
- WebCTRL web server engine:
    - The WebCTRL Cloud application uses its own built-in web server engine based on a locked-down version of Apache Tomcat. This greatly reduces the chance of an undiscovered Apache Tomcat vulnerability.
    - The WebCTRL Cloud application does NOT use Microsoft's IIS web server.
    - The web server renders only WebCTRL pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.
    - All database queries use a single internal interface that protects against common SQL injection attacks.
    - The WebCTRL Cloud application does not use Java® Applets or Java Web Start.
    - The WebCTRL Cloud application allows only add-on applications provided and signed by Automated Logic®.
- WebCTRL Cloud communication:
    - **Client/Server** is communication between the end user's computer and the WebCTRL Cloud application.
    - **Server/Gateway** is communication between the WebCTRL Cloud application and the BACnet/SC connection on an Automated Logic® IP controller

- The WebCTRL Cloud application uses the ports and protocols listed in the following table:

Port	Transfer	Protocol/User	Use
443 (default)	TCP	HTTPS (Web server)	Client/Server
4443 (default)	TCP	WSS (secure WebSocket for BACnet/SC)	Server/Gateway
1500 (temporary)	TCP	AWS Migration Tool	Migration of existing server into the AWS environment

- The WebCTRL Cloud application does not require open ports for standard Telnet, FTP, Windows file sharing, or other applications that can increase the vulnerability of the system.
- Built-in support for Transport Layer Security (TLS 1.2+) communication provides state of the art encryption for all communication to ensure unauthorized 'eavesdroppers' cannot obtain passwords or other sensitive information passed between the web server and client. All network traffic between the WebCTRL Cloud application and the browser can be encrypted using a locally created certificate. The WebCTRL software suite offers tools to recreate these self-signed certificates at any time, export to a third-party Certificate Authority (CA) and re-import the signed certificate. After you receive and install a signed certificate, be sure to back up the certificate and keystore.
- IPv6 is supported between the WebCTRL Cloud application and browser.
- The WebCTRL Cloud application securely connects to remote sites using the BACnet Secure Connect (BACnet/SC) protocol. This protocol uses secure WebSocket connections and Transport Layer Security (TLS 1.3) with mutual authentication to ensure the confidentiality, integrity, and authenticity of all messages transmitted across the connections. Support for PKI and X.509 certificates enable strong security for communication within the BACnet/SC network.
- The WebCTRL Cloud application provides the additional security features of Amazon Web Services (AWS) Guard Duty—threat detection that monitors for malicious activity and unauthorized behavior.
- Operator access to the WebCTRL Cloud application:
    - WebCTRL password security allows operator access based on privileges set by the administrator. The advanced security policy provides further security through password character/expiration requirements and user lockouts.
    - Access to the WebCTRL Cloud application can be restricted based on geographic assignment of operator privileges. For example, this allows persons with the same operator privileges access to different geographic areas of the system (i.e. two different rooms, floors, or buildings).
    - The WebCTRL audit log provides a detailed list of all operator actions and can be searched by operator name, date, and geography.
    - The WebCTRL Cloud application can require an operator to record the reason for a change to operating conditions before accepting the change.

    - WebCTRL Cloud operator passwords are "salted" and "hashed" using SHA512 and therefore cannot be reversed-engineered and are not exposed if the WebCTRL database is compromised. This also means that Automated Logic® cannot help recover lost passwords.
    - Passwords that the WebCTRL Cloud application uses to access other systems use AES-128-bit encryption. This includes database passwords and Email and Write to Database alarm action passwords.

- All patches to the WebCTRL software are signed for authentication and to prevent tampering.
- Database servers are configured to allow access only by the WebCTRL Cloud application and tools.

- See our *Security Best Practices* document for a security checklist.