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

WebCTRL® v6.5 Security

Rev. 5/9/2016

The WebCTRL server 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 server application.

- WebCTRL web server engine:
  - The WebCTRL server 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 server 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. As of v6.0, this includes Write to Database alarm actions.
  - As of v6.0, the WebCTRL server application no longer uses Java® Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers. While the WebCTRL server application no longer uses Applets or Web Start, we do recommend that customers keep their Java Runtime Environment up to date at all times.
  - Any add-on application not provided by Automated Logic® should be carefully reviewed for source and content before using with the WebCTRL server application.

- WebCTRL communications:
  - The WebCTRL server application uses the ports and protocols listed in the following table. In the **Use** column, **Client/Server** is communication between the end user's computer and the WebCTRL server application. **Server/Gateway** is communications between the WebCTRL server application and the Ethernet network interface on an Automated Logic IP controller. If a firewall exists between the Client and Server or the Server and Gateway, you will need to open the following ports to enable communication.

Port	Transfer	Protocol/User	Use
80 (default)	TCP	http (Web server)	Client/Server
443 (default)	TCP	https (Web server)	Client/Server
47806 (default)	TCP	Alarm Notification Client	Client/Server
47808	UDP	BACnet/IP	Server/Gateway
47808	TCP	Diagnostic Telnet *	Client/Server
47806	UDP	Legacy CMnet	Server/Gateway

* This functionality is off by default. You can start it using the `telnetd` console command.

You can edit the default http and https ports in SiteBuilder and the default Alarm Pop-up Client port in the WebCTRL interface (**System Settings** > **General** > **Alarms**).

The WebCTRL server application does not require open ports for standard Telnet, FTP, Windows file sharing, or other applications that can increase the vulnerability of the system. The **Diagnostic Telnet** protocol used on port 47808 is a password-protected plain text only user interface that is limited to WebCTRL server application functions. This functionality is ONLY used for Tech Support purposes and should be firewalled. It is turned off by default. You can start it using the `telnetd` console command.

- Built-in support for Secure Socket Layer (SSL) communications provides 128-bit encryption for all communications to ensure unauthorized 'eavesdroppers' cannot obtain passwords or other sensitive information passed between the web server and server. If needed, you can increase the encryption level to 256-bit. (See "Network Security" in WebCTRL Help for information on configuring SSL.) All network traffic between the WebCTRL server 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 for future WebCTRL installs.
- IPV6 is supported between the WebCTRL server application and browser.
- A WebCTRL server with two NICs can provide additional security and easier system diagnostics. One NIC is dedicated to web page traffic, and the other to unencrypted BACnet® traffic to field controllers. This separation of physical networks is the recommended best practice for building security. In this configuration, it is impossible for BACnet traffic to cross between the two networks.
- The WebCTRL server application is compatible with standard external security provisions such as firewalls and Virtual Private Networks (VPNs). VPNs can limit access to specific computer IDs, provide an additional layer of login/password protection, and offer alternative encryption schemes.
- Remote sites that connect to the WebCTRL server application through modems use an LGR as a BACnet dial-up half-router. These routers are inherently protected by their limited functionality, since they only respond to BACnet commands to local field controllers. They do not provide access to other Ethernet or IP networks within the building, even if they share the same physical wires.

- Sites that have security concerns but cannot physically secure their environment should disable controllers' Local Access ports to prevent non-authenticated access through Field Assistant connected to the Rnet. See "To disable a controller's Local Access" in WebCTRL Help. This setting can also be changed using global modify.
- The 6-02 and later drivers support BACnet whitelist functionality. You can restrict traffic to all private IP adresses and/or a list of specific IP addresses. This can also be used on an isolated network to restrict traffic to only designated BACnet devices and workstation(s) to ensure no other IP devices can tamper with BACnet controllers.

- Operator access to the WebCTRL server 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 server 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.
  - In a 21CFR Part 11 Pharmaceutical/Biotech validated facility, the WebCTRL server application can require an operator to record the reason for a change to operating conditions before accepting the change.
  - As of v6.0, 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.
  - As of v6.0, passwords that the WebCTRL server application uses to access other systems use AES-128 bit encryption. This includes database passwords, hierarchical server passwords, and Email and Write to Database alarm action passwords.

- After installing the WebCTRL software using administrator access, you can minimize risk to the server by running the software using a second non-administrator account. For Windows this non-administrator account must be given "Full Control" to the installation directory so that the software may run properly and apply patches. This account should also be used when run as a service. This can be specified in the "Log On" properties dialog for the WebCTRL service inside the "services" application in the Windows Control Panel. Linux should also be similarly configured to not run as "root". If other accounts are used to run the software (e.g. engineering tools), those accounts must also be granted full permissions to the installation directory.

- Database servers should be configured to allow access only by the WebCTRL server application and tools. This can be done through firewall protection and any other database-specific mechanism that limits access to specific hosts.

- See our *Security Best Practices* document for additional best practices and a security checklist.