Carrier®

Turn to the Experts.℠

September 24, 2008

Dear i-Vu CCN 4.2 Standard/PLUS Owner:

Given the heightened security awareness in all aspects of our society, it is not surprising that customers are concerned about whether or not i-Vu CCN poses a security risk to their building network. While there is no such thing as a system that is absolutely invulnerable to hackers, the inherent design and security aspects of i-Vu CCN make it extremely unlikely that anyone could gain unauthorized access to the building network through the i-Vu CCN web server. There are several key reasons why i-Vu CCN does not pose a security risk:

- i-Vu CCN uses its own, built-in web server engine (Tomcat). It does not utilize the Microsoft IIS web server, which is a favorite and well-known target for hackers. This web server is only used by the i-Vu CCN system and is not shared by any other system on the network.
- The i-Vu CCN web server runs a custom, streamlined version of the Linux operating system. The i-Vu CCN database is restricted to internal connections only and cannot be accessed externally.
- The HTTP, HTTPS, and Alarm Pop-up Utility ports are the only user-configurable ports in the system. They can be viewed and/or modified using the i-Vu CCN Management Tool. All other ports are NOT configurable.
- The i-Vu CCN Management Tool uses the Ruby WEBrick 1.3.1 server on port 8080. The i-Vu CCN server does not open ports for traditional Telnet, FTP, Windows file sharing, or other applications that increase the vulnerability of the system.
- The i-Vu CCN web server is “locked down” and will only render i-Vu CCN pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.
- i-Vu CCN offers an extremely “fine grained” password security control, allowing operator privileges to be custom tailored for each operator, providing no more access than is required.
- i-Vu CCN offers built-in support for Secure Socket Layer (SSL) communications, providing 128-bit encryption for all communications to ensure that unauthorized “eavesdroppers” cannot obtain passwords.

In addition to the inherent protection listed above, i-Vu CCN is compatible with external security provisions such as firewalls and Virtual Private Networks (VPNs) that the customer’s IT staff may wish to use. These systems can limit access to specific computer IDs and provide an additional layer of login/password protection, as well as offering alternative encryption schemes.

For a detailed list of ports and protocols that are used by i-Vu CCN, or if you have additional questions, please feel free to contact your local Carrier office.

Sincerely,

Carrier Systems Support