

# CASE STUDY

## Army Medical Department



### Fortress Secures AMEDD Wireless Network

#### Solution Allows Medical Personnel to Access Patient Information Wirelessly

While Field medical units operate under the direction of combat commanders, the Army Medical Department (AMEDD) is responsible for the U.S. Army's medics, evacuation units, surgical teams and field hospitals in the theater of war. AMEDD provides a seamless chain of care stretching back to fixed hospitals in Europe and the United States, where soldiers receive state-of-the-art care. Besides these fixed hospitals, AMEDD also includes preventive health, medical research, development and training facilities located at military bases around the world.

One of the primary challenges for Army medicine includes better integrating the work of field and fixed units. This is an area where wireless networking can provide substantial value. Before deploying any wireless networking technology, AMEDD must ensure that the solution helps meet Army policy, including Department of Defense Directive 8100.2.

AMEDD is able to bring the flexibility of wireless technologies to its workforce and still meet DoD policy by integrating the Fortress FC-X Series of security controllers into their wireless network. The Fortress Security Controller provides the required Layer 2 security and allows medical personnel wireless access to patient information. Now, medical personnel can securely access patient information from a government issued laptop or handheld device.

Fortress has security controllers installed at 12 AMEDD locations, including Walter Reed Army Medical Center, Washington, D.C., Fort Carson, CO, Fort Gordon, GA and Fort Sill, OK. All installations have been fully implemented and tested. The ability to provide military doctors and other medical personnel critical patient information securely and on demand is a top priority for the Army. This secure wireless project is a major step forward in that direction.

#### Bringing Secure Wireless Connectivity to Any Network

Fortress' FC-X Series of security controllers are capable of securing large enterprise Wireless Local Area Networks (WLAN) processing encrypted throughputs up to 1.9 Gigabits per second (Gbps). This enables large-scale organizations or agency-wide deployments to secure communications from thousands of wireless users over high-bandwidth wireless links. Complemented by the industry's broadest range of Federal Information Processing Standard (FIPS) certified clients, the Fortress solution is perfect for diverse environments that leverage various laptops, PDAs and industrial scanners. FC-X Series security controllers work across all wireless transports - including Wi-Fi (802.11), WiMAX (802.16), free space optics (FSO), Military RF and satellite.

Deploying secure wireless technologies enables Army doctors to do their job more efficiently by providing access to real-time information - while at the same time ensures the protection of U.S. Army soldiers' personal health information.

#### Challenges

- Provide strong security that meets DoD policy
- Support high-bandwidth multimedia applications
- Accommodate a mixed multi-vendor environment
- Provide transparent operation for users

#### Solution

- Rugged, Wi-Fi enabled PCs and PDAs
- Commercially available wireless access points
- Fortress Security Controllers
- Fortress Secure Clients

#### Results

- Strong, FIPS 140-2 validated security in place for wireless network
- All applications are supported
- Transparent operation for users
- Solution meets Army and DoD policy



For more information about Fortress:

phone: 813.288.7388 or 1.888.4PRIVACY (477.4822)

visit: [www.fortresstech.com](http://www.fortresstech.com)

email: [fedteam@fortresstech.com](mailto:fedteam@fortresstech.com)

Fortress Technologies, Inc.  
4023 Tampa Road, Suite 2000  
Oldsmar, FL 34677

© 2008 Fortress Technologies Inc. All rights reserved.

FTI Doc#: CS 003 041708 V01