

ON THE MOVE

With Orlando Public Safety

“Before we had NetMotion Wireless’ Policy Management module we had to come up with some pretty creative programming to keep officers in the field from logging on to the Internet.”

*Mark Crain, Sr. Manager for Systems & Networks
and Dave Kaicke, Microcomputer Engineer, City of Orlando, Florida*

Crain and Kaicke: With slow data speeds on CDPD we had to somehow limit patrol officers to logging in and using the Internet only when they were in the station. Before we started using GPRS and NetMotion Wireless’ Policy Management module, we used local accounts with Internet settings in the local profile, so they couldn’t get to the Internet when mobile, and a default account that let them in only when plugged into the network at headquarters. That was hard to manage, subject to hacking, and prone to mistakes. NetMotion Policy Management allows us to do it reliably and a lot more easily.

“We bought the Policy Management program when it first came out. The documentation and the application were easy to understand.”



Crain and Kaicke: We didn’t have any problems. I initially had some questions about policies, since I wasn’t quite sure what I could block and not block without killing our system. But NetMotion Wireless includes many sample policies in the Policy Management module. We use our main policy to manage Internet Explorer. We also use a policy for new devices coming on the network. We had been quarantining them, but that was too restrictive. Now I just allow them to authenticate, but block their access to critical resources and information. It makes it a lot simpler to do mass migrations. The technicians had to reboot to recover from the quarantine and it was just taking too long. Now we have the best of both worlds—the devices are secure, but our technicians can do what they need to do.

Mobility’s Policy Management module provides centralized, flexible tools IT managers can use to control bandwidth usage and costs by preventing mobile workers from using certain applications or downloading large files based on:

- ▶ The network to which a user is connected
- ▶ The type or speed of a network interface
- ▶ Detailed rules that block or allow data traffic based on application name, port or IP address

MEET THE MOVERS

Located in the heart of the Florida high technology corridor, metropolitan Orlando is rich with technology education programs, leading-edge research initiatives and vocational training efforts. In this environment Orlando Public Safety is charged with the protection and security of some 185,000 citizens and the countless tourists who flock to the area’s year-round attractions. They have the equipment and support to meet the demands of their mission. And they take every advantage of Orlando’s reservoir of technological savvy, including the City of Orlando’s IT specialists, who ensure communications and integrity for the city’s 900 police and 400 fire personnel.

The City of Orlando’s Technology Management Division continuously seeks out and evaluates the best hardware, software and technology available to ensure state-of-the-art performance for systems and the people who use them. Their long-term goals are ambitious, but they continually move closer to them as they create a seamless, easily managed system that allows anywhere, anytime communication and the most efficient use of resources and funding.