

Case Study: International Airline

Major airline takes service to new heights with Mobility XE. At its key international hub, one of the world's largest airlines operates in a facility that is colossal in scope. There are more than 2500 departures and arrivals daily, with passengers passing through 200 gates attached to six separate concourses. In order to more efficiently maintain its aircraft across the huge airport and conveniently serve passengers at the gates, the airline relies on mobile technology. Mobility XE assures that the devices maintain reliable connections — so the passengers can keep theirs.

About the Deployment

More than 100 separate Wi-Fi access points throughout the vast facility give airline employees access to corporate servers and data. There are two groups of workers for whom Mobility XE from NetMotion Wireless is critical: maintenance personnel and customer service reps

Maintenance personnel carry Panasonic Toughbooks to consult aircraft service manuals, check parts inventory and update maintenance logs. Every part on the airliners is serial-numbered, and all service activity has to be meticulously tracked and recorded. The workers move in and out of aircraft throughout their shifts, and the aircraft frames are heavily shielded against wireless signals. Before installing Mobility XE, entering the fuselage caused loss of signal, severed connections and dropped application sessions. Now, Mobility XE persists the network connections so workers have continuous access to critical data. While inside the aircraft, they can access measurement and parts information from their local database and enter any new data. When they exit the aircraft and re-enter coverage areas, the local database automatically resynchronizes with the corporate data.

Before installing Mobility XE, entering the aircraft frame caused loss of signal and dropped application sessions. Now, Mobility XE persists the network connections. While inside the aircraft, workers can access measurement and parts information from their local database and enter any new data. When they exit the aircraft and re-enter coverage, the local database automatically resynchronizes with the corporate data.

A second, passenger-facing deployment assists customers who need to adjust their itineraries due to flight delays. Customer-service representatives roam between gates with a cart that carries a Motorola handheld device and a printer. When a late-arriving flight causes a missed connection, the roving representative meets the passenger at the gate and retickets, so the passenger doesn't have to return to the terminal building or go through security a second time. Without Mobility XE, transitioning between access points triggered dropped connections and crashed the ticketing application; with Mobility XE, the problem was solved.

Organization

Major international airline

Industry

Transportation

Objectives

- Eliminate dropped connections for maintenance personnel and customer service reps
- Use multiple access points seamlessly
- Implement airtight security

Solution

- Mobility XE Mobile VPN
- Panasonic Toughbooks and Motorola handhelds
- Aircraft maintenance and ticketing applications
- Mix of internal and third-party Wi-Fi access points

Results

- Continuous connections to applications
- Data security over public access points in busy international airport
- Devices locked down for security
- Transparent user experience

NetMotion Wireless

701 N 34th Street, Suite 250
Seattle, WA 98103 USA

TEL 206.691.5555

FAX 206.691.5501

www.netmotionwireless.com

Multiple Challenges, Single Solution

Initially, the airline had tried to use a conventional SSL-VPN for the aircraft maintenance deployment but ran into compound issues. Not only was the connection being dropped while inside the aircraft, the devices were also going into suspend mode to conserve battery power. That was shutting off the Wi-Fi, also causing disconnects.

While piloting the roving gate-agent deployment, they discovered that even though there was ubiquitous Wi-Fi coverage blanketing the concourses, the coverage wasn't seamless. Moving out of range of one internal access point and connecting to another caused a connection loss. To further complicate matters, some access points are owned by the airline while others are public Wi-Fi provided by various telecommunications carriers. The airline needed to use both types of access points, and they use varying schemes for assigning IP addresses.

Installing Mobility XE provided a straightforward solution to all of these challenges. It handles the underlying complexities and maintains the connections wherever the users roam, making the user experience like one continuous, available-everywhere network.

Airtight Security at a Bustling Airport

With a quarter-million passengers from all over the world passing through the airport every day and able to access the public hotspots, security is a paramount concern for the airline. The VPN encryption protects the data going over the air. The Mobility XE clients are locked down so the VPN is always enabled and cannot be bypassed. And through the Mobility XE Policy Management module, only applications that are specific to the user's task are able to run over the network, preventing unauthorized access.

The devices used by the roaming gate agents are locked down so only the one ticketing application is allowed to run, with no desktop access allowed and the operating system hardened against the user installing additional software or changing the configuration. The Policy Management module also prevents any external communication with access points and external networks that have not been specifically allowed.

Through the Mobility XE Policy Management module, only applications that are specific to the user's task are able to run over the network, preventing unauthorized access. The module also prevents any external communication with access points and external networks that have not been specifically allowed.

Additionally, the airline quarantines all new devices that attempt to connect until the administrator specifically authorizes them. That guards against a worker – or anyone else – from introducing a new device that can connect with the corporate network.

One Administrator for the Whole Deployment

While the deployment includes more than 1000 licensed devices spanning two distinct user groups, one part-time administrator is able to handle it all. In a vital deployment at one of the world's largest airlines and busiest air terminals, Mobility XE maintains reliable connections and critical security – with zero turbulence.

©2010 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion Wireless technology is protected by one or more of the following US Patents: 5,717,737; 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; 7,574,208; 7,602,782; 7,644,171; 7,778,260 and Canadian Patent 2,303,987. Other US and foreign patents pending.