NetMotion Wireless Mobility XE™
Award-Winning, Best-in-Class Mobile VPN Solution

Mobility XE is built specifically for highly mobile workers who need secure, reliable wireless access to critical data and applications. Whether they drive to multiple locations in a single day or roam between floors or buildings on a corporate campus, workers remain productive while they access different networks, cross coverage gaps, or suspend and resume their devices.

Security

Protection. The industry's strongest FIPS-validated encryption secures data sessions within the VPN tunnel. Before allowing access, Network Access Control verifies that every device is up-to-date with software and patches, and that security measures are enabled.

Authentication. Support for two-factor, standards-based authentication gives government organizations an affordable way to meet federal security mandates. For commercial enterprises, a two-factor method adds a layer of protection for vulnerable mobile devices. With support for inexpensive smart cards or free or low-cost X.509v3 user certificates, Mobility XE supports most standards-based PKI authentication infrastructures — including the one Microsoft builds into their server operating systems, by interfacing with RADIUS EAP infrastructure.

Productivity

Enforcement. Flexible policies control device and application behavior, restrict application access, and keep bandwidth-intensive processes off slower networks where they can bog down performance.

Convenience. Mobile workers have a convenient, single sign-on experience — no matter how many different networks or access points they use. Mobility XE keeps mobile workers authenticated and their applications reliable during coverage loss.

Roaming. Mobility XE enables seamless roaming in and across any combination of IP networks. Users move freely between docked connections, corporate Wi-Fi networks, third-party hotspots and cellular data networks from multiple carriers — automatically using the fastest available connection.

Performance. Mobility XE improves throughput, application responsiveness and productivity over bandwidth-constrained wireless networks. It reduces protocol overhead and chattiness, and compresses data and web images, dramatically improving throughput.

Reliability. No other mobile VPN matches Mobility XE's ability to keep application sessions alive and stable. In coverage gaps, applications simply pause, then resume sending when a connection returns. Data transfers pick up where they left off, even days later after a device is resumed.

Management

Control. Set-and-forget design requires little management for routine operations. The browser-based administrative console allows all aspects of the system to be centrally configured, managed, and observed — from overall metrics down to the details of a single mobile worker. And the central controls make it easy to quarantine devices that are misused, lost or stolen.

Visibility. Automated notifications promote hands-off management. Sophisticated analytics from a full reporting package deliver insight into mobile worker behavior and application usage.

Compatibility. Any application that works over Ethernet can be transitioned to run reliably over wireless, simply by installing Mobility XE. There's no need to modify applications, do expensive development, or upgrade to special wireless-enabled versions. Mobility XE provides the application compatibility of an IPSec VPN without the application setup hassles of SSL VPNs. It is compatible with any IP network, and with any Windows device.

Cost-efficiency. Installation and setup take only a few hours. The Mobility XE server installs on standard, off-the-shelf hardware, including virtual environments, either behind the corporate firewall or within a DMZ. The client software installs on any Windows device, can be centrally configured, and is transparent to the end user.

Scalability. Mobility XE handles the transition from a small pilot deployment to a large installation. A single server can handle up to 1,500 concurrently connected devices. Servers can be pooled to provide additional capacity as well as load balancing, failover and redundancy for thousands of workers, creating a highly scalable, reliable system with no single point of failure.

NetMotion® WIRELESS

DuraTech USA Inc. 6765 Westminster Ave #314   Westminster, CA 92683
Email: sales@DuraTechUSA.com   www.DuraTechUSA.com
Phone: (714) 898-2171   Fax: 866-704-9132   Toll Free: 866-761-9555

Policy Management Module

Centralized, Flexible Control over Mobile Productivity & Security. The optional Policy Management Module enforces enterprise-specific security policies and selectively grants access by user, device, network or application.

- **Control application and resource access.** Policies provide granular control over which applications are allowed network access, and when.

- **Assign policies.** Enforcement of policies is transparent to the user and can be assigned based on individual, job function, work group or entire organization.

- **Manage traffic with Quality of Service (QoS).** Using traffic classification and traffic-shaping policies, mission-critical applications can be prioritized to ensure their availability regardless of network type.

- **Confine bandwidth-intensive applications to high-capacity connections.** Policies can block bandwidth-intensive applications from slower networks, or proactively launch applications when a high speed network becomes available.

- **Support real-time applications.** In addition to the Quality of Service (QoS) capabilities, Mobility XE includes packet loss recovery capabilities that improve the performance of real-time applications such as VoIP, streaming video, or real-time conferencing that are sensitive to latency and jitter.

- **Use wireless LANs and hotspots securely and effortlessly.** Policies can selectively permit or deny application traffic based on the access point or hotspot provider.

Network Access Control Module

Enforcement of Mobile Device Security and Compliance Policies. The Network Access Control (NAC) module ensures that workers' devices have adequate security measures in place before allowing connectivity and granting access to applications and data.

- **Deploy quickly.** The NAC module wizard makes it easy to configure and deploy security policies in minutes without network infrastructure reconfiguration.

- **Ensure security compliance.** Using NAC, mobile devices are scanned for compliance with required software including antivirus, antispyware, firewall, operating system version, Windows™ update status, registry keys, and other applications.

- **Exert flexible control over non-compliant devices.** Based on severity, administrators may choose from simple warnings, to triggering customizable remediation policies that can limit application access, launch websites, initiate software downloads, or even disconnect or quarantine the device.

- **Automate updates and compliance checks.** Updated rules are automatically pushed down to client devices. Devices are also automatically re-scanned at regular intervals to ensure ongoing compliance even after they connect.

- **Consistent support on multiple platforms.** NAC policies are supported on all Windows-based client devices including laptops, handhelds and smart phones.

Analytics Module

Proactive Management and Visibility into Mobile Deployments. The Analytics Module delivers a level of detail and business insight not available in other VPNs. It provides detailed statistics on performance and usage; insight and intelligence on the networks and applications used by mobile workers; and automated notifications that save administration time and facilitate fine-tuning and capacity planning.

- **See the big picture; drill down to the details.** Go far beyond simple activity logs used by typical VPNs, with graphical reports that show usage trends. Use filters to selectively drill down on populations and time periods to view the data you need.

- **Know how resources are used.** See which applications, devices and users are consuming the most bandwidth. Set policies to improve productivity and comply with carrier service agreements.

- **Spot coverage or connection problems.** See which devices have connection problems, and when, why, and which network is involved.

- **Gain a more efficient help desk.** Empower help desk employees by showing the applications mobile workers are running, including version details and when a battery might be failing. See how frequently applications are run, how much traffic they use, and which other applications cause performance problems.

- **Receive alerts of impending problems.** More than 30 notifications, many with adjustable thresholds, alert via email, SNMP or syslog.

- **Prove performance and plan proactively.** Show that users are using the mobile environment efficiently, and know when more bandwidth or better coverage might be needed.