NetMotion Wireless

NetMotion Wireless Mobility XE™

Award-winning, Best-in-Class Mobile VPN Solution

Mobility XE is the mobile VPN built specifically for highly-mobile workers who need reliable wireless access to mission-critical data and applications. Whether driving to multiple sales or service locations in a single day, or walking between rooms, floors, or buildings on a corporate campus; Mobility XE secures data while providing uninterrupted remote access to all the applications and data resources essential to your mobile work force.

Security

Mobility XE's VPN encryption uses the industry's highest security standards. User authentication integrates seamlessly with your enterprise. The client software on each mobile device automatically keeps users authenticated and application data secure without disruption as users roam between networks and coverage areas.

Roaming

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

Cost-efficiency

Installation and setup of Mobility XE usually takes only a couple of hours. The Mobility XE server installs on standard, off-the-shelf hardware behind the corporate firewall or within the DMZ. The client software installs on any Windows device, can be centrally configured, and is transparent to the end user.

Performance

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

Compatibility

Any application that works over Ethernet runs 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 compatibility of IPSec without the setup hassle of SSL. It works on any IP network and with any Windows-powered device.

Reliability

No other mobile VPN matches Mobility XE's ability to keep application sessions alive. In coverage gaps, applications simply pause, then resume sending data when a connection returns. With Mobility XE, users do not have to log in each time they suspend and resume their devices. Data transfers pick up where they left off, even days later after a suspended device is resumed.

Management

Mobility XE's set-and-forget design requires little management for routine operations. Its robust administrative console allows all aspects of the system to be centrally configured, observed and managed. The browser-based interface gives a complete system-wide view, from overall metrics down to the details of a single mobile worker, including applications in use and the amount of data transferred – regardless of the device or network. And the central controls make it easy to quarantine devices that are misused, lost or stolen.

Scalability

Mobility XE handles the transition from a pilot deployment with a few mobile workers to a production installation supporting thousands with ease. A single server can handle up to 1,500 concurrently connected devices. Servers can be pooled to provide load balancing, failover and redundancy for thousands of workers, creating a highly scalable, reliable system with no single point of failure.

Policy

The optional Policy Management Module provides the ability to customize and enforce changing security and access needs while keeping workers productive. Policy Management features Quality of Service (QoS) capabilities that allow you to prioritize network traffic for any IP-based application, including those sensitive to latency and jitter such as VoIP, video or real-time conferencing applications. Data from business-critical applications or from specific groups of users can take precedence, providing the fastest possible transmission.

Network Access Control

Integrating with Policy Management, the Network Access Control (NAC) module gives administrators full mobile device control. Remote devices can be checked for required software and applications. Based on severity, devices can receive simple warnings or customizable remediation requirement policies to ensure compliance is maintained.

Policy Management Module
Centralized, Flexible Control over Mobile Productivity & Security

Accessible from the Mobility console, the Policy Management Module lets administrators create rules, with conditions and the actions to take when the conditions are met. Rules are combined into policies, to which users are subscribed. The policies are pushed out to mobile devices where the rules are enforced automatically and transparently for each mobile worker, at the right times and situations.

- **Control resource access over any IP network.** Policies provide granular control over which applications are allowed network access, and when.
- **Assign policies by role.** Policy enforcement 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 for real-time applications.** Policy Management optimizes VoIP, video and other real-time applications by reducing data packet loss to enhance both quality and performance.
- **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 (NAC) Module
Enforcing Security and Compliance Policies for Mobile Devices

Mobility XE's Mobile NAC Module gives administrators greater control and flexibility over how and when devices can connect to their enterprise network. Using NAC, mobile workers' devices must comply with specified security policies or face remediation as determined by the network administrator.

- **Simple deployment.** The NAC module wizard makes it easy to configure and deploy security policies in minutes without network infrastructure reconfiguration.
- **Ensures security compliancy.** Using NAC, mobile workers' devices are scanned for compliance to required software including antivirus, antispyware, firewall, operating system version, Windows™ update status, registry keys, and other applications.
- **Flexibility and 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.
- **Automatic updates and compliance.** Updated rules are automatically pushed down to client devices. Devices are also automatically rescanned at regular intervals to ensure ongoing compliance.
- **Multiple platform support.** NAC policies are supported on all Windows-based client devices: laptops, handhelds, and smart phones.