product sheet

MOBILITY XE

Eliminate Dropped Connections with Industry-Leading Mobile VPN

Mobility XE® is mobile Virtual Private Network (VPN) software that maximizes mobile field worker productivity by maintaining and securing their data connections as they move in and out of wireless coverage areas and roam between networks. Designed specifically for wireless environments, Mobility XE provides IT managers with the security and centralized control needed to effectively manage a mobile deployment.

mobility XE®

Overcome Wireless Challenges

Mobility XE helps organizations save time and money overcoming the top challenges to wireless data deployments: ensuring **secure** data transfers, creating persistent connections to keep mobile workers **productive**, and providing the capabilities to **manage** and control your wireless deployments.

Mobility XE Features

Security	
Enhanced Protection	Mobility XE supplies the industry's strongest security with FIPS 140-2 validated encryption. You can verify that every device is up-to-date with software and patches, and that security measures are enabled.
Two-Factor Authentication	Mobility XE supports two-factor authentication, as well as most standards-based PKI authentication infrastructures by leveraging RADIUS and NTLM.
Enforcement	Flexible policies control device and application behavior, restrict application access, and keep bandwidth-intensive processes off slower networks where they can slow down performance.

Productivity	
Ease of Use	Mobile workers don't need to worry about the technology. Mobility XE is a service, providing an always-on VPN connection that automatically connects users at start-up and resume.
Improved Performance	By reducing protocol overhead and transmitting less data, Mobility XE improves application responsiveness and productivity over wireless networks, an important factor as networks get faster.
Always Reliable	Mobility XE keeps applications alive and stable through any disruption. In coverage gaps, or when users suspend and resume their device, applications pause, then resume when a connection returns. Data transfers pick up where they left off, even days after a device is resumed.

Management	
Central Control	Mobility XE's console allows all aspects of the system to be centrally configured, managed, and monitored — from overall metrics like application usage, to the ability to block and prioritize applications, down to the details of a single mobile worker's battery power on their device.
Streamlined Compatibility	Mobility XE allows any application to run reliably over wireless networks. There's no need for modifications. Mobility XE is compatible with Windows™ devices, and any IP network.
Easy to Scale	Mobility XE easily handles the transition from small to large deployments. It can scale up to 1,500 concurrently connected devices when servers are pooled to provide additional capacity and create a highly scalable system with no single point of failure.

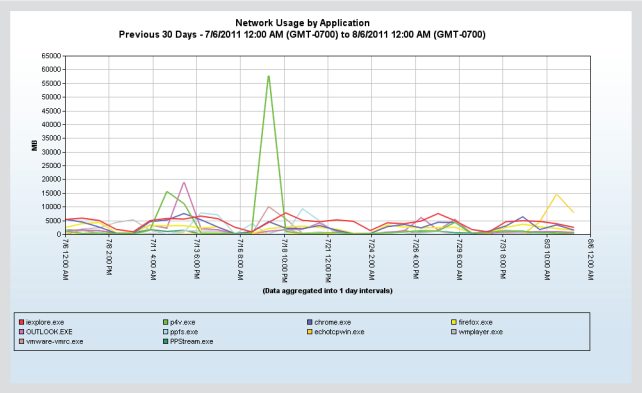
Add-On Modules for Powerful Management and Control

Mobility XE comes equipped with three powerful management modules that provide IT Administrators the capability to run reports, set bandwidth and access policies, and enforce security procedures.

Analytics

Mobility XE is the only VPN to deliver a detailed level of business insight. Through the Analytics module you can get statistics on performance and usage, as well as gather intelligence on networks and applications used by workers. With Analytics, you can:

- **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.
- **Gain a More Efficient Help Desk**. Get a detailed view of mobile worker's activity to help troubleshoot field issues including applications they are running, their device battery power, and which devices have connection problems.



The Analytics Module allows you to see detailed device and application usage

- **Get Intelligence to Plan Proactively.** Show that users are using mobile resources efficiently, and know when more bandwidth or better coverage might be needed.

Policy Management

Policy Management allows you to create and enforce security policies based on business needs. With Policy Management, you can control access by user, device, network or application, and create policies to:

- **Control Applications and Access**. Policies provide control over which applications are allowed network access, and when, as well as selectively permit or deny application traffic based on the access point or hotspot provider.
- **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 selected applications from slower networks, or proactively launch applications when a high speed network becomes available.

Network Access Control (NAC)

Network Access Control ensures that workers' devices have adequate security measures in place before granting access to applications and data. With NAC, you have greater control over access to your network and can:

- **Deploy Quickly**. The NAC module wizard makes it easy to configure and deploy security policies in minutes without network infrastructure reconfiguration.
- **Ensure Security Compliance**. Mobile devices are scanned for compliance for required software including antivirus, antispyware, firewall, operating system version, Windows update status, registry keys, and other applications.
- **Automate Updates and Compliance Checks**. Updated rules are automatically pushed down to client devices. Devices are also automatically rescanned at regular intervals to ensure ongoing compliance even after they connect.

Learn more at: www.NetMotionWireless.com

CONTACT US:
NetMotion Wireless
TEL 866.262.7626
www.NetMotionWireless.com