NetMotion Mobility®

When business runs on mobile, every connection is critical.

NetMotion Mobility is an intelligent solution that not only secures connections and data, but enhances and optimizes network connectivity to ensure business-critical applications are always accessible. It is the component of NetMotion's Mobile Performance Management solution that accelerates, optimizes and secures all mobile device traffic supporting any network, application or operating system.

Transform Mobile Access

NetMotion Mobility transforms mobile access for both mobile users and the IT support team entrusted to manage and support them. Mobility insulates applications from the instabilities in networks enabling them to roam seamlessly between Wi-Fi and mobile operator network without user intervention delivering a resilient, "always-on" connectivity experience.

NetMotion software also adds a layer of intelligence that is situationally-aware of the connections, devices and applications that a worker is using at any moment. It adjusts for the ever-changing network conditions to ensure mobile workers always get the best use experience from their mobile devices and applications.

NetMotion Mobility Features

Most Reliable Connection Resilience	• Persistence through coverage gaps, areas of weak signal strength, or when users suspend their devices; applications pause, then resume when a connection returns. Transparent transitions between cellular, Wi-Fi and wired networks.
Supported Applications	Any application written for a IP network; no modifications required.
Automated Login	• A single login grants seamless access for the entire workday; workers can use any combination of networks, roam freely between them, cross gaps in coverage, and suspend- and-resume their devices without losing sessions, repeating logins or managing their connections. User transparent login and connection • Depending on session parameters, subsequent logins/reconnections are programmatically handled, transparent to the user. • Automatic detection of hotspot login requirements where supported without disabling the VPN.

NetMotion Mobility Features

Performance Optimizations	• Reduces TCP/IP protocol overhead and chattiness over wireless links. • Policies to selectively compress images and optimize voice and video
Policy Enforcement	• Support for more than 30 policy conditions and actions, providing fine-grained control over how workers access networks and resources. • Ability to sense connection changes and dynamically control device and application behavior, such as restrict or prioritize application access; ensure that only business applications access the secure tunnel and corporate resources; keep bandwidth intensive applications off slower networks. • Reduce data-plan usage by blocking traffic, or automatically compressing data to achieve the greatest effective throughput with the least amount of data usage. • Dynamically adjust application traffic priorities according to the network name, type, or interface speed. • Automatically assign policies and settings to new devices based on OS. • Automatically diagnose connections when a problem is detected.
Third-party Integration	• API for real-time access to key console metrics. • Import real-time usage data from the Mobility server into dashboards and network management applications.
Active Directory Support	Update configuration settings and policies based on changes in Active Directory groups and group membership. Active Directory to Mobility group mapping has been extended to support deployments that use RADIUS authentication.
Troubleshooting	Interrogate device, network, corporate servers and resources to determine root causes of connection problems.
Alerts	Alerts based on diagnostic test results, adapter usage/inactivity, status or other thresholds, delivered via email or text messaging, or exported to alerting systems.
Reporting	Detailed analytics on user, device, network, and application activity and performance, including geo-tagged data when available.
Monitoring	Real-time displays and system status reports on application and network usage, compression rates, network errors, and quarantine status of any given device.
Automated Inventory	Regularly updated database record of all mobile devices and configuration details down to device driver level.
Encryption and Certifications	FIPS 140-2 validated encryption, NSA Suite B cryptography, Common Criteria EAL 4+ certified.
Security Enforcement	Allow varying degrees of user control, or lock down the device so that security and VPN cannot be bypassed. For Android devices, Mobility offers native integration with Android for Work and Samsung KNOX allowing administrators to enforce security and mobile policies using MDM systems.
NAC	Verification that third-party security products are updated and enabled before granting connections; support for the market leading anti-malware and firewall products.
Authentication/Login	• Authentication methods configurable per user, device, or group. Administrators use the most appropriate method for their security requirements, workflows, or form factors; designated authentication method transparently presented to the user. • Support for NTLM, RADIUS, PKI x.509 v3 certificates, RSA, and other industry-standard two-factor solutions. • Customized notices at login to remind users of corporate security policies.

NetMotion Mobility Features

Over-the-air Client Updates	• Mobility updates downloaded and installed transparently over the air, without user intervention; fully supports EMM/MDM software deployment solutions. • Ability to specify allowable network connections for downloading, and options for user to defer or postpone reboot.
Console Access	• Access granted to Active Directory users and groups based on defined roles. • Role-based access to status display and statistics, analytic reports, client and server configuration settings, policy management and NAC rules. • Role templates for common scenarios such as client administration and help desk. • Auditable logging of all changes made by Mobility console users.
Limit Access	Ability to limit access to corporate assets on a device-wide, per-network, and per-application basis.

Platform Support & System Requirements

Clients	• iPad and iPhone devices (iOS 7.1 and later), Mac (running OS X El Capitan and later), Android devices (running on Android 4.0 or later), Android for Work, SamsungKNOX, Windows Pro Tablets, laptops and other devices running Windows 7, 8 and 10. • Clients available in English, Japanese, French, Italian, German and Spanish.
Capacity/Scalability	Each server supports a maximum of ten thousand authenticated users.
Server	• Modern server class processor Windows server 2012 R2; minimum 4 GB RAM and 50 GB disk space. • Servers available in English and Japanese.
Solution Components	• Mobility server – Termination point for client VPN connections. • Mobility Warehouse – Stores configuration and management information for a Mobility server or pool of servers. • Analytics module – Reporting server for VPN client usage data. • Diagnostics module – Collects and aggregates end-to-end performance, location, and coverage data from Windows, iOS and Android clients, Mobility servers and for reporting, alerting and troubleshooting. Requires separate server or cloud deployment. • Recommended configuration – Mobility Server, Warehouse, and Analytics Module should be installed on separate platforms for larger installations; evaluations or environments with fewer than 100 clients may be deployed on a single server.