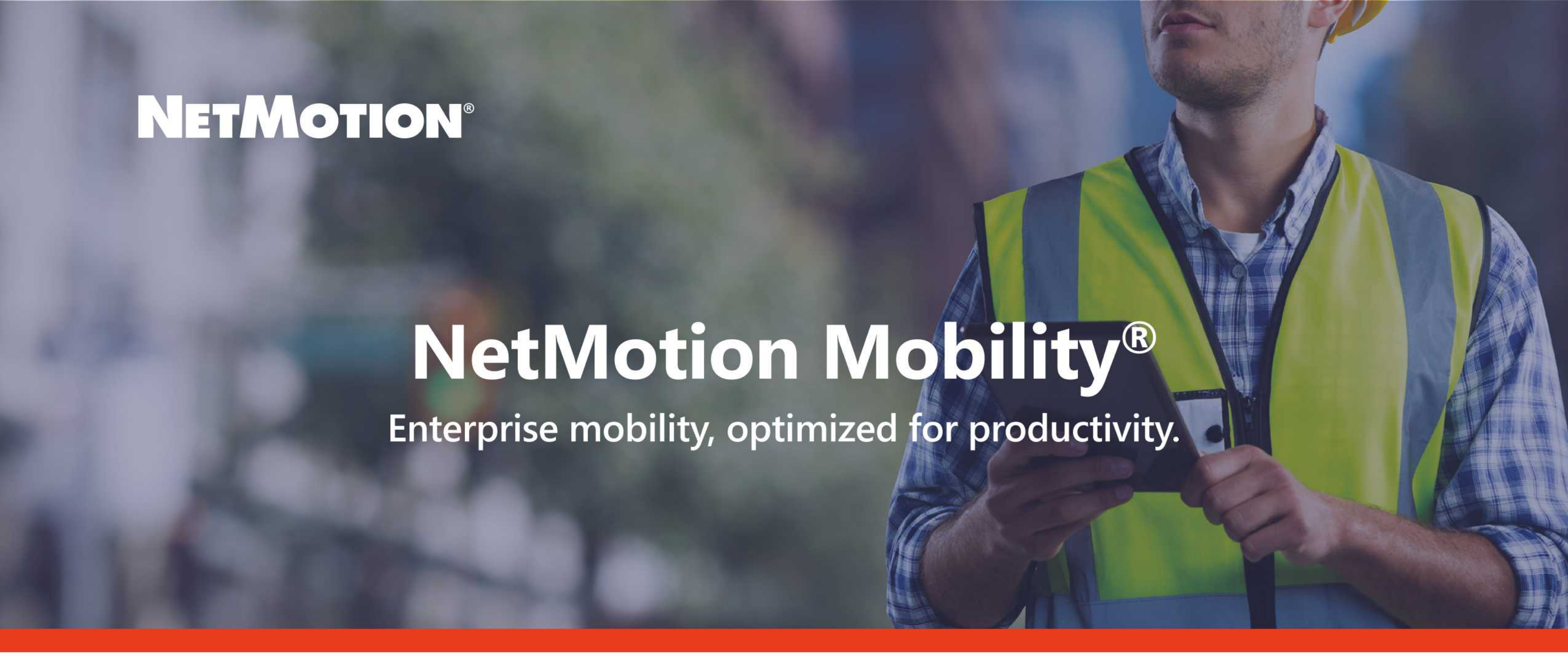

NETMOTION®

NetMotion Mobility®

Enterprise mobility, optimized for productivity.

NetMotion Mobility is an intelligent software solution that secures and optimizes network connections to ensure business-critical applications are always accessible. NetMotion's software is situationally aware of the connections, devices and applications that a worker is using at any moment. It adjusts performance to the ever-changing network conditions to ensure mobile workers always get the best user experience from their devices and applications – and ultimately deliver better interactions to the customers they serve.

Security without Sacrificing Productivity

Where other security products slow productivity and frustrate workers, Mobility enhances and optimizes the end-user experience. Built to the highest cryptographic standards, it provides military-grade encryption and control while also delivering a user experience designed for productivity.

Always Connected. Always Reliable

From start-up, Mobility ensures always-on access to applications. When networks are intermittent or bandwidth slows, Mobility stabilizes applications keeping them accessible even through the toughest conditions. And when a faster network with better bandwidth is available, Mobility seamlessly roams the user to it.

Complete Control, Inside and Outside the Firewall

From the mobile device to the server it securely connects to, Mobility's architecture gives IT complete control over the entire connection regardless of the networks used. That means unprecedented visibility and management – even over networks your organization doesn't own.

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 an IP network. Ensure application priority on carrier networks supporting 3GPP QoS standards like FirstNet, AT&T ADTM, and Verizon Business Services; without re-writing applications to use those advanced features.

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.
- 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.

Performance Optimizations

- Packet coalescence, data compression, and link-layer optimizations reduce protocol overhead and accelerate traffic over wireless links.
- Optimize communications with real-time apps (e.g., Skype) to sustain high quality video and audio, especially on lower quality mobile networks.
- Policies can also be used to selectively compress images and optimize voice and video.

Policy Enforcement

- Supports more than 30 policy conditions and actions, providing fine-grained control over how workers access networks and resources.
- Senses connection changes and dynamically controls device and application behavior, such as restricting or prioritizing application access; ensuring that only business applications access the secure tunnel and corporate resources; keeping 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.
- Stream real-time usage data from the Mobility server into NetMotion Mobile IQ® v2.0 dashboards and other network management applications (e.g., Splunk).

Active Directory Support

Update configuration settings and policies based on changes in Active Directory groups and group membership.

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), can be streamed directly into the NetMotion Mobile IQ v2.0 Mobile Operational Intelligence platform.

Monitoring

Real-time displays and system status reports on application and network usage, compression rates, network errors, and quarantine status of any given device. This data can also be streamed directly into NetMotion Mobile IQ v2 dashboards.

Encryption and Certifications

FIPS 140-2 validated encryption, NSA Suite B cryptography, Common Criteria EAL 4+ certified. Mobility enforces the use of strong encryption and makes it easy to demonstrate compliance with regulatory and organizational security mandates such as CJIS, HIPPA / HITECH, NERC-CIP, and PCI.

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.
- On Apple iOS DEP-enrolled devices in supervised mode, apps cannot access the network if the user knowingly or accidentally disables the VPN. Full management over application access with dynamic policy control.

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.

Console Access

- Role-based access controls based on Active Directory user and group membership
- 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, Samsung KNOX, 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.