Mobility 11.50
Simplifying, Strengthening, and Streamlining Mobile Security

Summary

- Counter evolving threats to your mobile deployment with new dynamic policies
  - Domain Names: Support domain name policy for native cloud applications
  - Active Directory: Seamless integration with Active Directory,
  - iOS application: Expanded application name controls for iOS devices, and
  - Unsecured hotspots: Automatic detection and protection from unsecured hotspots.

- Streamline and boost security on iOS, macOS, and Android devices by controlling VPN access to protected networks using facial recognition and other biometric authentication factors.

- Numerous minor enhancements and fixes.

New Dynamic Policy Controls
Policy by Web Domain or Host Name
New domain-based policy rules offer exceptional control of the cloud applications and systems used by mobile workers. Enforce Mobility policy on named hosts or entire domains. For example, enforce the use of onedrive.com but not dropbox.com, prevent access to YouTube on cellular networks to control costs, or restrict access to ESPN during business hours to promote productivity. Domain policy conditions supports wildcard characters to match all servers in a domain or limit to specific servers.
Policy by Application Name for Apple iOS
For supervised iOS devices, administrators now have the flexibility to enforce policies by application name like they do on Android and Windows. Enforcing policies for applications by name is simple yet powerful and eliminates the need to know IP addresses, ports or protocols.

Policy by Active Directory User Group Membership
For organizations leveraging Microsoft’s Active Directory to manage access, Mobility v11.50 Policy rules are now aware of Active Directory user group membership. Administrators can configure Mobility to automatically apply the correct policy based to members of any group, simplifying ruleset management and eliminating the need for frequent hands-on configuration.

Hotspot Security Policies
Using unsecured hotspots exposes mobile workers to direct attacks. Mobility’s new policy condition detects if the device’s WiFi interface is using an unencrypted access point, giving administrators the ability to automatically increase security or change access rights.

For example, you can create a policy that prevents split tunneling and forces all traffic through the Mobility VPN when the device is connected to an unsecured hotspot and send a notification to the user letting them know.
Biometric authentication support for iOS, macOS, and Android

Mobility v11.50 leverages advanced biometrics, like face recognition or fingerprints, available on iOS, macOS, and Android devices to control access to the Mobility tunnel.

As an additional layer of security, biometric checks take place before establishing the VPN, blocking network traffic until a biometric authentication is successful. When used with x.509 certificates, the user gets hands-free two-factor authentication. Support for facial recognition provides added convenience in real world situations such as eliminating the need to remove gloves, allowing a mobile worker to quickly and securely access mobile applications in dirty or cold environments. With this enhancement, Mobility now supports biometrics on all major platforms.

Minor enhancements and Bug fixes

- Mobility Alerts now support secure SMTP
- Minor updates to the macOS user interface
- Numerous minor improvements and fixes
Mobility v11.x Release History
Rel. v11.4

**Mobility 11.40 delivers ground-breaking security for iOS devices, and meets advanced carrier network requirements for delivering quality of experience (QoE) to business-critical applications.**

- A new setting to block all application traffic from exiting a supervised iOS device if the user turns off the Mobility VPN. Ensure that all application traffic is secured by Mobility on iOS without having to configuring per-app VPN for every application.

- Mobility supports advanced 3GPP standards to ensure application priority on carrier networks like FirstNet, AT&T ADTM, and Verizon Business Services. Without having to upgrade them, legacy applications can take advantage of network prioritization.

- Out-of-the-box, Mobility 11.40 optimizes communications with Skype and other real-time apps to sustain high-quality video and audio, especially on spotty mobile networks.

- Support for Mobile IQ® 2.0 data correlation and optimized publishing

**Ground-breaking Security to Enforce Device-wide VPN Use on iOS Devices**

Enforce deployment-wide VPN usage on supervised iOS devices to prevent users from accidentally or willfully sending unsecured data.

NetMotion is the only VPN vendor that can enforce deployment-wide VPN use. If the VPN is not active, Mobility blocks all application traffic. This new capability is available to Apple iOS DEP-enrolled devices in supervised mode. When enabled, apps cannot access the network if the user knowingly or accidentally disables the VPN. Security-conscious administrators can reclaim control and enforce remote access security without configuring a per-app VPN for every app on the device.

**Quality-of-experience and Network Priority for Advanced Networks**

On every client platform, Mobility supports 3GPP network standards for setting priority, providing transparent and consistent quality of service on advanced carrier networks.

Advanced carrier networks including FirstNet, AT&T ADTM, and Verizon Business Services, use 3GPP standards for packet tagging to prioritize traffic on the network by user and data type so that important data receives priority routing. Most applications need to be re-written to use the standard, unless they’re being secured by Mobility 11.40.

Mobility 11.40 is the only VPN that can set priority by policy so that applications don’t need to be rewritten or upgraded to support priority tagging standards. Mobility also fully supports priority tags set by the operating system and by newer, compatible applications.

**Built-in Skype Optimizations Improve Performance and Reliability**

Ensure high-quality video over low-quality networks. Mobility 11.40 now automatically optimizes Skype for Business and other video conferencing solutions, maintaining clear audio and video even when networks have sub-optimal performance.

Microsoft recommends <1% packet loss and less than .05% out-of-order packets to ensure a quality experience with Skype. Even the best carrier networks can drop packets at a higher rate, and packet loss on public Wi-Fi hotspots regularly runs 25% or more.

Mobility 11.40 automatically optimizes Skype for business over networks with variable performance, providing clear audio and video under worsening network quality. Watch our videos showing how our patented packet loss recovery technology maintains high quality audio and video streams, even with 25% packet loss or more.

**Support for Mobile IQ® 2.0 Data Correlation and Optimized Publishing**

Mobility v11.40 and Diagnostics 4.5 standardize the way in which device and user names are exported to Mobile IQ 2.0. This allows Mobile IQ to correlate the located performance and per-application network traffic data from Mobility and Diagnostics with the users and devices that generate them.

Mobility 11.40 also adds a new data type for Mobile IQ 2.0 that logs application flow destinations periodically, optimizing published network flow data.

**More Flexible Enforcement of FIPS 140-2 Validated Cryptography**

Frequent operating system updates combined with evolving methods from NIST for classifying cryptographic libraries complicate the task of maintaining a list of ‘valid’ libraries for security auditors. Mobility 11.40 makes it easy to preserve those modifications when the server is upgraded by prompting admins to reconcile their modified list of libraries with the list that NetMotion ships with each release.
Changes to Android Permissions
As of Android 8, Google has changed how notifications are displayed and has expanded the number of on-device permissions required for Mobility to function.

- **Notifications**: The default Mobility client behavior remains the same, but there are more granular controls for disabling specific messages like “Authentication Required” or “Disconnected.”

- **Permissions**: Android 8 requires two additional permissions for Mobility to function properly. Users may be prompted (once) for one or both of the following:
  - Read Phone State – Mobility requires this permission to read the hardware identifiers used to create the device Mobility ID number. The message from the operating system reads “Would you like Mobility Client to make phone calls or read your phone messages?” To be clear, Mobility is NOT making phone calls or reading phone messages.
  - Coarse Location – Mobility requires this permission to obtain the Wi-Fi network identifier (SSID) used by the Policy module.

If users decline to grant permission, the Mobility client displays a dialog box explaining why they are needed and ask for the permissions again. If permissions are not granted, the VPN does not start.

Rel. v11.3

Data-driven Insight into the Behavior of Mobile Users, Devices and Applications Operating Outside the Corporate Perimeter.
Mobility 11.30 delivers granular data for visibility into the behavior, performance and security of mobile users, devices, and applications. With advanced data gathering and data publishing features, Mobility 11.30 transforms your mobile devices—Android, MacOS, iOS, and Windows—into active behavioral sensors, revealing...

- Risky user behaviors
- Promiscuous applications
- Security-related threats
- Performance bottlenecks

Detailed Insight Outside the Firewall
Mobility publishes over 85 performance and security-related data elements using the universally accepted syslog interface, as well as interfaces for Splunk and NetMotion Mobile IQ®.

Correlate with NetMotion Diagnostics for a full complement of network performance, troubleshooting, and device data to yield comprehensive behavioral analytics for reporting and policy management.

Get near-real-time, data-driven answers about the security and performance of your mobile workers, devices, and applications, without impeding mobile device performance or reliability.

- What services and sites are iPads and iPhones accessing?
- What are the most (and least) accessed destinations by Android devices?
- Are any of my employees communicating with servers outside the country? If so, where?
- How much data is being sent and received by a specific application?
- Are devices being where they should (or shouldn’t) be?
- Which devices and applications are sending the most and least data?

Act on security and performance issues using Mobility policies.

Enhanced Web Services API Provides Real-time Integration for Dashboards and Systems
Use the web services API to actively update existing management dashboards and systems with client connection data, including:

- Local and remote IP address of the mobile device’s active network interface
• Last connection time and current connection status
• The network type (for example, WWAN, Wi-Fi, or Ethernet) of the mobile device’s active network interface
• The network name the mobile device is currently using
• The mobile device’s active Mobility policy and NAC rule sets
• The current user, user group, and device group of the mobile device
• Improved Android deployment and configuration options
• Support for Samsung Knox with SOTI MobiControl
• Support for multiple VPN profiles on a single client
• Improved certificate management and more certificate import methods
• Import VPN configurations using MDM or email
• Support for multiple user name / password formats during logon
• Enhanced user experience based on the Android Material Design specification

Rel. v11.0

Up to Twice as Fast
Mobility 11 accelerates throughput and greatly enhances scalability. Enterprises can support more mobile workers on the latest 4G and Wi-Fi networks using fewer resources, greatly reducing the cost to administer and manage mobile worker connectivity. Customers can reduce the number of servers they need to support their deployment, or improve per-connection throughput with existing resources.

Unlike other VPNs, Mobility does not require expensive, proprietary hardware or forklift upgrades every few years. Adding capacity and increasing throughput with Mobility is as easy as spinning up another virtual machine or deploying common off-the-shelf server hardware. With Mobility’s pool architecture, managing 10 servers is as easy as managing 1.

Multi-language Deployments
Mobility 11 adds support for global, multi-language deployments with clients for Japanese, French, German, Italian, Spanish and English. The Mobility server now supports native Japanese in addition to English. Organizations around the world can deploy a Mobility client in a language their workers understand, and those workers can now connect and interact in their native language.

Apple OS X
With the addition of OS X support, Mobility now supports all major mobile and desktop platforms in use today. Using Mobility, mobile workers throughout an organization using Apple’s sleek line of MacBook laptops stay connected as reliably as iPhone and iPad users.

Other Key Features
Expanded Android Management Options
For Android devices managed by EMM/MDM systems, Mobility offers native integration with Android for Work and Samsung KNOX. Administrators can enforce security and mobile policies using their existing MDM systems.

Policy Action to run NetMotion Diagnostics
When network problems occur, Mobility automatically launches the advanced troubleshooting available in NetMotion Diagnostics. The new policy action is supported on Android, iOS, and Windows and can be triggered by over 20 different policy conditions.

RADIUS Group Mapping
We have extended Active Directory to Mobility group mapping to support deployments that use RADIUS authentication.

Universal Licensing
We simplified client license management with universal license keys that allow any combination of Android, iOS, and Windows clients to connect. You can change the mix of client platforms in your deployment with complete flexibility as the need arises.

Automatic Warehouse Backups
Mobility v.11 automatically creates a daily backup of the Mobility Warehouse. The backup can be used on upgrades or for disaster recover if you do not run a standby warehouse.
Mobility 11 Details
Performance Improvements
At 2 Gbps, a Mobility 11 server is up to twice as fast as previous releases when run on dedicated hardware while still fully supporting deployment in virtual environments. Each server supports a maximum of ten thousand authenticated users, over six times more than version 10.

The increases in throughput and capacity offer NetMotion Mobility system administrators the following advantages:

- Lower operating costs using off-the-shelf server hardware or virtualization instead of costly, proprietary hardware appliances.
- Servers and pools support significantly greater peak traffic loads than previous versions of Mobility.
- Customers can simplify their deployment by reducing the number of servers needed to support it, or increase the number of servers to improve performance.

Multi-language Deployments
Simple Client Management
Packaged as a single executable, the Mobility client automatically detects the language preference on the device during installation and configures itself to run in one of the six supported languages (English, Japanese, French, Italian, German, and Spanish) covering over 130 countries and spoken by over 2.6 billion people. The multilingual clients can connect to any version 10 or greater Mobility server. If the client detects a language preference other than the supported six, it will default to English.

Fully Localized Japanese Server
In addition to localized Mobility clients, the Mobility v.11 server is available fully localized in Japanese.

The Mobility Japanese server is compatible with all version 9, 10, and 11 Mobility clients, regardless of their language setting.

Apple OS X
The new Mobility client for Apple OS X brings our legendary reliability and performance to Apple MacBook users with a native Mac application.
Administrators can support Mac users with the same ease and reliability they’ve come to rely on for their iOS, Android and Windows users, all from a single console.

The Mac client supports the full range of Mobility’s compression, link optimization, roaming, and persistence technologies, and supports the Policy and Analytics modules.
Expanded Android Management Options

Android for Work

Android for work is the emerging standard for integrating Android clients into an enterprise mobile deployment. With Android for Work and Mobility v.11, administrators can build and push per-application VPN configuration profiles to Android users via their MDM systems. When configured using Android for Work, Mobility v.11 can prevent users from deleting or replacing VPN profiles, avoiding support calls before they happen.

Samsung KNOX

A secure, trusted, hardware-based platform that includes secure boot capabilities, Samsung KNOX is the preferred Android platform for many finance, government, and military organizations. Mobility v.11 now supports KNOX with per-app VPN controls and support for KNOX’s containerization architecture.

When used with KNOX, Mobility can secure all device network traffic by keeping users from disconnecting the VPN, preventing users from changing client configuration, and preventing users from creating an alternative VPN profile. The combination of Mobility and KNOX gives administrators the greatest level of security and control possible over Android clients in a Mobility deployment.

MDM Industry API

In response to customer demand, NetMotion has created a fully functional API for MDM partners to integrate directly with the Mobility client on Android. Vendors interested in access to this interface should contact support@netmotionsoftware.com.

Policy Action to Run NetMotion Diagnostics

When network problems are detected, our new Policy action automatically launches the advanced troubleshooting available in NetMotion Diagnostics. This new Policy action is supported on Android, iOS, and Windows and can be triggered by over 20 different policy conditions.

Diagnostics analyzes mobile connections and proactively alerts network administrators as problems arise. It provides end-to-end performance data extending from the device, across cellular and Wi-Fi networks, to corporate and cloud-based servers. It alleviates much of the back-and-forth troubleshooting between end-user and IT support when connectivity issues occur. NetMotion Diagnostics is available as an add-on module for Mobility.

RADIUS Group Mapping

We have extended Active Directory to Mobility group mapping to support deployments that use RADIUS authentication. Mobility now automatically assigns policies and settings based on a user’s group membership for accounts using RADIUS authentication.

With Mobility v.11, Administrators can now take advantage of this feature to do the following:

• Save time and simplify user management by assigning an Active Directory group instead of individual users to a Mobility group. Users in that AD group automatically receive the correct settings.

• Simplify the on-boarding process by assigning Active Directory groups to Mobility policy rules. New users are automatically assigned the appropriate Mobility policies.

• Combine users from multiple Active Directory Domains into a single mobile deployment.

Figure 1: Easily map Mobility groups to multiple Active Directory domains
Universal Licensing

Universal license keys allow any combination of Android, iOS, and Windows clients to connect to a Mobility server and provide complete flexibility to change the mix of client platforms in your deployment.

Customers upgrading from earlier Mobility versions will have their platform specific licenses converted to universal licenses at no additional charge.

During the upgrade process, the Mobility installer will convert all platform specific licenses to temporary universal licenses. Customers will have 30 days to finish the licensing conversion. After upgrading it is no longer necessary to track licenses by client platforms.

Automatic Warehouse Backups

Mobility v.11 automatically creates a daily backup of the Mobility Warehouse and stores it on the Warehouse server. The backup can be used on upgrades or for disaster recovery if you do not run a standby warehouse. The time and location for the backup file are configurable during Warehouse installation or with the Warehouse management tool.

Platform Requirements and Known Issues

Important:

Windows 7 Service Pack 1 is required to run the Mobility v11.00 client on Windows 7.

Mobility v.11 clients Max OS X can only connect to Mobility 11 servers. Mobility v.11 servers will accept connections from all currently supported Mobility clients.

Supported platforms and hardware requirements for Mobility v.11 are available here:

• http://www.netmotionsoftware.com/support/supported-systems/

A list of known and resolved issues for Mobility 10 can be found here

• Known and Resolved Issues for Mobility 11-
http://help.netmotionsoftware.com/support/docs/mobilityxg/1100/docs/known_issues.htm