product sheet

WHAT'S NEW IN MOBILITY XE

mobility XE®

Improved Mobile VPN Software Creates Compliance for Future

Mobility XE 9.5® contains a number of improvements and feature upgrades, and is built with the future in mind: supporting next generation networks and security standards.

New Features for 9.5

IPv6 support – Transparent, Seamless Roaming Between IPv4 and IPv6 Networks

Mobility XE v9.5 now supports transparent, seamless roaming between networks using the IPv4 and IPv6 protocols. Enterprises can confidently adopt new carrier network technologies without concern for which IP protocols their carriers are using.

A Mobility client running on Windows 7 can now use either IPv4 or IPv6 to establish the VPN tunnel back to a Mobility server running on Microsoft Windows Server 2008 R2. Mobility XE v9.5 clients and servers will automatically detect and configure support for both IPv4 and IPv6 networks. IPv6 protocol support extends to networks used by mobile devices to connect to the Mobility server but not to applications or servers behind the corporate firewall. IPv6 is not supported on Mobility servers running Microsoft Windows Server 2003.

NSA Suite-B – The Only Mobile VPN that Supports NSA Suite B Cryptography

Mobility XE v9.50 uses FIPS 140-2 validated cryptographic modules that use NSA Suite B compliant algorithms. These algorithms are supported on Mobility server and client systems running Windows Server 2008 R2 and Windows 7.

NSA Suite B is the United States government's standard for securing data classified up to 'Secret.' Using Suite B cryptography is mandatory for all federal networks handling data up to 'Secret,' and is best practice for other industries.

By default, Mobility XE v9.5 servers running on Windows 2008 R2 connected to clients running on Windows 7 use the Suite B cryptographic algorithms. The Mobility server and client will use the other algorithms if they are running on other supported operating systems or are connected to prior Mobility XE versions (v8.x through v9.23).

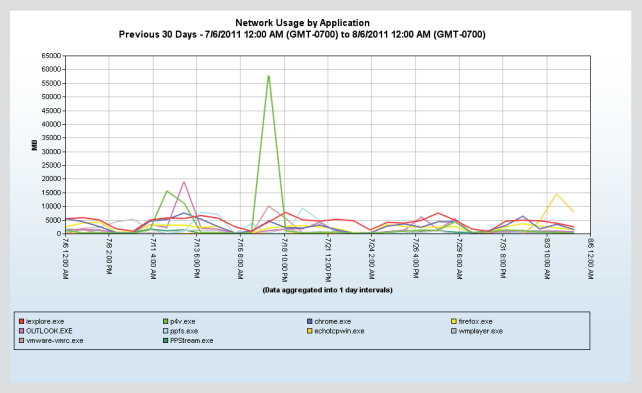
Mobility XE 9.5 supports Suite B, a set of cryptograhic algorithms that is the federal standard for securing data up to "Secret"

Improvements for 9.5

Analytics Module

The Analytics module in Mobility XE version 9.5 is easier to manage without database expertise:

- It installs on a single system and is completely self-contained.
- It is no longer necessary to purchase or manage a Microsoft SQL Server license.
- The upgraded Analytics Module will hold up to a year of data for any supported pool size.
- All maintenance, reporting, and management tasks are accessible from the Mobility XE management console.



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

- Reports run faster - particularly reports that aggregate large amounts of data.
- VMware and Microsoft Hyper-V virtualization environments are fully supported.

The upgrade process automatically migrates data without risking data loss. The new Analytics Module requires that all servers in the pool be upgraded to Mobility XE v9.5. Hardware requirements are listed in *Appendix A* of this document, the server help system, and in the *System Administrator Guide*. For details on the upgrade process, review the product documentation.

Improved Support for Multi-Homed Servers Running on Windows Server 2008 R2

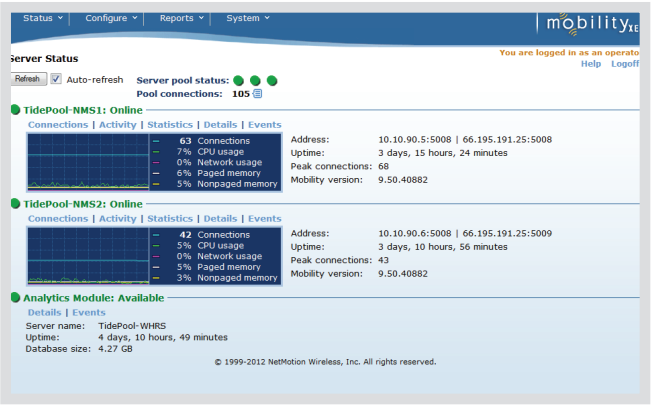
Enterprises running Mobility XE v9.5 on Windows Server 2008R2 with two or more network interface cards now specify which interface is on the trusted internal network.

- Virtual IP address pools (VIP pools) can now be assigned on any network routable from the specified internal interface. This makes it easier to install and configure the Mobility server and to integrate it with enterprise networks.
- Unencrypted traffic is only allowed on the internal interface, improving security and compliance with best network security and routing practices.

Enhanced Mobility Console Usability and Flexibility

The Mobility console is easier to navigate with similar functions grouped together. The settings associated with the Analytics Module, for example, are now consolidated on their own page, instead of being intermingled with other settings.

- Administrators can configure a console logon message, making it easier to comply with regulations that require warnings or disclosures when administering critical infrastructure.
- The Mobility console timeout is configurable, allowing administrators to balance productivity and risk.
- The Mobility console is more responsive – in particular, the status pages display faster.



Mobility XE 9.5 ships with an updated interface that is easier to navigate and configure

Network Performance Optimizations

Mobility XE v9.5 has significant network performance improvements:

- Mobility XE v9.5 automatically recalculates the maximum packet size (MTU) to reduce packet fragmentation and improve performance when devices roam between networks.
- Faster transitions roaming between WiFi access points.
- Improved Dynamic DNS support. Clients are reachable by name at either their virtual IP address (VIP) or point-of-presence (POP) address.
- Virtual environments use less CPU processing the same amount of traffic.
- VoIP and other real-time applications may experience lower jitter and latency.
- Users will see faster downloads where the underlying network is not the limiting factor. For example when connected via Ethernet, as opposed to 3G.

Enhanced client API

The Mobility Client API (nmclapi) now supports native application calls from the C# programming language in addition to C, C++, and Visual Basic. API documentation is now available in online help, making it easier to develop custom applications to query and control Mobility clients.

Warehouse Changes

Mobility XE version 9.5 installs an updated warehouse based on Oracle's Directory Server Enterprise Edition v11. The updated warehouse contains the most current security and stability improvements. This upgrade is only supported by Mobility XE v9.2 or later.

Mobility XE v9.5 also supports selective warehouse backup / restore making it easier much easier to migrate devices, users, and policies from one pool to another.

Other Improvements and Changes

Mobility XE version 9.5 includes numerous bug fixes and stability improvements. For details refer to *Known and Resolved Issues* on the software download page.

Most Current Versions

Mobility XE v9.5 replaces all previous version 9 releases for Windows desktop and server platforms, with the following exceptions:

- Version 9.23 remains the most current version for Windows Vista.
- Version 9.21 remains the most current version of Mobility XE for Windows CE and Windows Mobile.

Restricted Upgrade Path

Upgrades to Mobility XE v9.5 are only supported from pools running Mobility XE v9.2 or later with a v7.x warehouse. For assistance in upgrading, **contact the Technical Support Team**:

Telephone: **888.723.2662**

Email: **support@netmotionwireless.com**

Web: **http://www.netmotionwireless.com/support-request-form.aspx**

Integrating Mobility XE v9.5 and NetMotion Wireless Locality

The Mobility XE v9.5 Analytics Module is incompatible with versions of Locality prior to v1.20. When upgrading to Mobility XE v9.5, customers running Locality must also upgrade to Locality v1.20 to allow data collection from Mobility.

Development of Mobility XE for Windows Server 2003 Ending

Mobility XE v9.5 is the last feature release for Windows Server 2003. Technical support for Mobility XE v9.5 running on Server 2003 will be available to customers under maintenance agreements until end-of-life (typically three years after the release date).

Supported Platforms

Current information on the Mobility XE product lifecycle and supported operating systems is available on our web site.

For More Information

To learn more about Mobility XE, visit **www.NetMotionWireless.com**.

APPENDIX A

Mobility XE v9.5 Analytics Module Platform Requirements

Appendix A:

Mobility XE v9.5 Analytics Module Platform Requirements

The Mobility XE 9.5 Analytics Module uses embedded database technology licensed from Oracle. In a small deployment (up to 100 clients), the Analytics Module can be installed on either Windows Server 2003 R2 or Windows Server 2008 R2. For all other deployment sizes the Analytics Module must be installed on a computer running Windows Server 2008 R2.

The Analytics Module requires the following:

- The computer or virtual machine on which the Analytics Module is installed must meet the requirements listed in the hardware requirements table (below).
- In a deployment that has multiple server pools, each pool must have its own Analytics Module; it cannot be shared between pools.

Mobility XE v9.5 Analytics Module Hardware Requirements

Clients	CPU	Memory	Disk
Up to 100	• 2 GHz • 2 cores	4 GB (minimum)	SATA HD **Free disk space:** • 10 GB
Up to 1,000	**Minimum:** • 2GHz • 2 cores **Recommended:** • 2.8 GHz • 4 cores	**Minimum:** • 8 GB **Recommended:** • 16 GB	**Minimum:** • SATA HD **Recommended:** • RAID 10 array **Free Disk Space:** • 25 GB
Up to 6,000	• 3.06 GHz • 6 cores	• Hyper Threading • 64 GB	RAID 10 SAS array; hardware RAID should be used (do not use software RAID) **Free Disk Space:** • 400 GB • Write-back cache must not be used in the disk controllers for the drives on which the Analytics Module data files are stored
Up to 15,000	• 3.06 GHz • 6 cores	• Hyper Threading • 64 GB	RAID 10 SAS array; hardware RAID should be used (do not use software RAID) **Free Disk Space:** • 700 GB • Write-back cache must not be used in the disk controllers for the drives on which the Analytics Module data files are stored

APPENDIX B

Previous “What’s New” Releases

What's New in Mobility XE 9.23

Overview

Mobility XE version 9.23 is a maintenance release containing bug fixes and stability improvements. For details refer to Known and Resolved Issues on the downloads page.

Version 9.23 replaces all previous version 9 releases for Windows desktop and server platforms. Version 9.21 remains the most current version of Mobility XE for Windows CE and Windows Mobile

Issues addressed in 9.23

Servers

- The encryption library used in Microsoft Server 2008 R2 SP1 and Windows 7 SP1 (CNG.sys version 6.1.7601.17514), was added to the list of FIPS validated modules.
- The Mobility console interface for adding and removing licenses has been modified to support our new software download and licensing process. See "Adding and Removing Licenses" on page 338 for more information.
- We disabled the optional TCP offloading engine in Windows Server 2008 R2. If called by another application or piece of hardware, it could keep Mobility XE from passing traffic.

Clients

- Stability improvements for users with Windows 7 clients using non-default window sizes.
- Improved the change password experience for customers using token-based authentication solutions

What's New in Mobility XE 9.22

Overview

Mobility XE version 9.22 is a maintenance release containing bug fixes and stability improvements for issues reported in previous versions of Mobility XE. For details on these issues, refer to Known and Resolved Issues on the downloads page.

- Version 9.22 replaces all previous version 9 releases for Windows desktop and server platforms. Version 9.21 is the most current version of Mobility XE for Windows CE and Windows Mobile

Issues addressed in 9.22

Servers

- Intermittent stability issues with the Mobility reporting server.
- Routing inconsistencies when a single Mobility server had more than one interface with a valid route to a destination.
- Incompatibilities between Mobility XE clients and some third-party applications on Windows XP that rely on ping when connecting to Windows Server 2008R2 servers.

Clients

- Incomplete processing of some login scripts on Windows XP.
- Incompatabilities between Mobility XE clients and Trend Micro Office Scan v10.5.
- Incompatibilities between Mobility XE and Microsoft's Remote Assistance and Remote Desktop Protocols.

What's New in Mobility XE 9.21

Overview

- Mobility XE 9.21 is a maintenance release containing fixes, stability improvements, and minor enhancements.
- Version 9.21 replaces all previous version 9 releases for all platforms.

Major Features and Changes

Server Platform

- Service Pack 1 for Microsoft Server 2008 R2 has been tested and is fully supported in this release.
- The server setting (Security – FIPS required) that strictly enforces the use of FIPS 140-2 validated cryptography is now turned Off by default on new installations to create less disruption when Microsoft updates the cryptographic libraries in Microsoft Server 2008 R2 and Windows 7. All customers should review Known and Resolved Issues on the downloads page for details.
- Mobility XE 9.21 offers full support of real-time traffic optimizations for all Mobility clients and servers when operated in "FIPS Required" mode. For more details please review Known and Resolved Issues on the product download page.
- Network settings have been adjusted to optimize performance over 4G networks.

Client Platform

- Service Pack 1 for Microsoft Windows 7 has been tested and is fully supported in this release.
- The list of tested products for the NAC module was expanded– Detailed information is available in the System Administrator Guide under "Client Security Software and Mobility Client Compatibility" in the Network Access Control section.

Other changes

Mobility XE 9.21 fixes several customer-reported issues found in previous releases:

- File locking (mutex) errors in the warehouse
- Routing problems when a single adapter had multiple IP addresses on Windows Server 2008 R2.
- Incompatibilities with Entrust IdentityGuard 9.3 server.

For details on these and the other issues addressed in version 9.21, refer to Known and Resolved Issues on the downloads page.

What's New in Mobility XE 9.2

Overview

- Mobility XE™ 9.2 is a platform release supporting Windows Server® 2008 R2 and 64-bit versions of Windows 7. Included in the release are FIPS 140-2 validated cryptographic libraries for both Windows Server 2008 R2 and Windows 7 64-bit, support forMicrosoft Server 2008 R2 Hyper-V, and a new Mobility warehouse which will run on either Windows Server 2008 R2 or Windows Server 2003. Mobility XE 9.2 is functionally equivalent to version 9.1.

Features and Changes

Server platform support

- Mobility XE version 9.2 supports Windows Server 2008 R2 Standard and Enterprise editions. Guidance on configuring Mobility XE 9.2 servers is available in the product documentation. Late-breaking information on platform support, compatibility with third-party components, and legacy technologies is available in Known and Resolved Issues on the product download page.

Client platform support

- Mobility XE 9.2 adds support for Windows 7 64-bit clients and updates the currently shipping Windows 7 32-bit clients. The Windows 7 clients are compatible with all currently supported Mobility XE servers. For important information on platform support, compatibility with third-party components and legacy technologies, please review the Known and Resolved Issues file on the product download page and the system administrators guide.

New warehouse version

- Mobility XE version 9.2 incorporates Sun Java System Directory Server version 7.0 in the Mobility warehouse. This version of the warehouse can be installed on either Windows Server 2008 R2 or Windows Server 2003. The version 9.2 warehouse supports only Mobility XE version 9.1 and 9.2 server pools. For important details on configuration and compatibility of the Sun Java System Directory Server version 7.0, see the Mobility XE System Administrator Guide before installing the warehouse included with version 9.2.

Other improvements

Support for Microsoft Server 2008 R2 Hyper-V. Mobility XE now supports Microsoft's most current server virtualization platform. For more details, please review Known and Resolved Issues on the product download page.

Support for Intel's AES-NI (Advanced Encryption Standard - New Instructions) for on –CPU acceleration of AES encryption and decryption operations.

Improved warehouse management tools. It is much easiser to move the warehouse from one machine to another or recover from a catastrophic hardware failure.

Note:

- When operated in "FIPS Required" mode, Mobility XE 9.2 offers limited support of real-time traffic optimizations for older Mobility clients. For more details please review Known and Resolved Issues on the product download page.

What's New in Mobility XE 9.1

Overview

- Mobility XE 9.1 is a maintenance release containing fixes, stability improvements, and minor enhancements to Mobility XE 9.0.

Features and Changes

Client platform support

- The version 9.1 Mobility client for Windows XP, Vista, and Windows 7 fixes a handful of routing, authentication, and stability issues reported since the release of version 9.0.

New warehouse version

- In version 9.0, NetMotion Wireless installed an updated version of the Mobility warehouse (version 6.3.1). In version 9.1, automated migration of data from a pre-version-6.3.1 warehouse to the new warehouse is supported.
- The new warehouse is easier to install and includes a new Warehouse Management Tool for easier warehouse administration. The managment tool is available from the Start menu in the NetMotion program group.
- If you are upgrading from an earlier version of Mobility XE, the Sun ONE Java System Directory Server version 5.2 is detected and you are prompted to install the 6.3.1 warehouse. If you opt to install the new warehouse your existing database is automatically migrated.
- While NetMotion Wireless supports both old and new warehouses, we recommend customers migrate to the newer warehouse. Sun Microsystems has ended support for version 5.2 of their LDAP directory server. NetMotion Wireless will continue to support customers running a warehouse that shipped with Mobility XE versions prior to 9.0 as follows:
- Assistance with configuration, management, operation, or migration of the warehouse continues to be available through all the current NetMotion Wireless support channels: telephone, web and email.
- For defects in the warehouse that are either known to be fixed in a later release of Mobility XE or that would require escalation to Sun, the only remediation is to upgrade to the most-recently released version of Mobility XE – both the server and warehouse.

Other improvements

- Removed the Disconnect button from the logon dialog.
- Fixed a conflict between RSA SecurID tokens and user reauthentication.
- Improved client stability for Windows XP and Windows Vista when both encryption and compression are disabled.
- Fixed bugs related to the Properties dialog on the Windows CE client.
- Corrected the list of Windows 7 patch levels in the NAC wizard.
- Enhanced compatibility with enterprise network management suites such as HP Network Node Manager. The Mobility client now polls only for NAC status when a NAC policy requires it.

What's New in Mobility XE 9.01

Client platform support

- Version 9.01 supports Windows 7 Professional, Ultimate and Enterprise, and is fully compatible with all currently supported versions of the Mobility server. Organizations evaluating or migrating to Windows 7 can combine the improved performance and security of Microsoft's newest operating system with the productivity enhancements of Mobility XE 9.0. The latest information on platform support, compatibility with third-party components, and legacy technologies is available in the Readme and Known Issues for Mobility XE 9.0.

What's New in Mobility XE 9.0

Overview of New Functionality

User reauthentication

- For organizations concerned about the consequences of device theft or that are subject to regulatory requirements such as CJIS, SOX, or HIPAA, the new user reauthentication capability added in version 9.0 helps protect your network resources. Unlike competing solutions, which disconnect users from networks and applications during the reauthentication process, Mobility XE version 9.0 provides a seamless reauthentication experience to mobile workers without needlessly disrupting their application sessions. Since workers can re-enter their credentials without shutting down and restarting their applications, workers stay productive and your network stays secure.

Unattended device access

- Keeping mobile devices in the field and up-to-date with the latest patches and applications becomes easier with the unattended device access in Mobility XE version 9.0. This new feature extends the reach of your current device- and patch-management tools to your mobile platforms with true "over the air" management access. By using certificates to authenticate the device at boot time, Mobility XE provides a secure wireless connection that's just as full-featured as your internal wired network. The unattended device access in Mobility XE version 9.0 supports device-management technologies such as Active Directory Domain scripting and software update policies, as well as other popular device-management suites. With unattended device access, your users stay in the field and your remote devices stay up to date – all without new investment in wireless-specific management tools.

Certificate-based device authentication

- For organizations with security policies or regulatory environments that restrict corporate network access to approved company devices, Mobility offers certificate-based device authentication, which binds a certificate to a specific mobile device, providing an extra level of trust. By leveraging industry-standard PKI technology, the device authentication capabilities in Mobility XE version 9.0 prevent foreign devices from attaching to your network. The device certificate is validated before the user is prompted for authentication credentials. If the device's certificate isn't valid or recognized, no access is granted, even if the proper credentials are used. With certificate-based device authentication, organizations can exercise fine-grained control over network access and meet their regulatory burdens – without burdensome new access control solutions that hamper user productivity.

Strong multi-factor authentication

- For customers who need strong authentication but worry about the impact that stronger authentication protocols will have on their capital and operational expenses, as well as their workers' productivity, Mobility XE 9.0 has the solution. Its multi-factor authentication capabilities tie hardware platforms and authentication protocols to a strong, two- or three-factor, standards-based authentication solution that does not require the purchase of expensive new hardware. Administrators get inexpensive but strong authentication, and mobile workers stay focused on their jobs rather than the technology that enables it.

Major Features and Changes

User reauthentication

- With Mobility XE version 9.0, you can require users to re-enter their credentials periodically or when a device reconnects or resumes. This helps protect your network resources from unauthorized use in the event that a device is

left unattended or is stolen. If the user does not successfully reauthenticate, he or she is disconnected from the VPN and appropriate system events and notifications are generated.

- Reauthentication options are controlled by three new client settings in the Mobility console:

Logon – Reauthentication Interval

- Specifies how often (in days, hours and minutes) a user is prompted to reauthenticate. If a device is out of range at the end of that interval, the user is prompted when the device comes back in range.

Logon – Reauthentication Grace Period

- When a user is prompted to reauthenticate, he or she has a certain amount of time in which to provide valid credentials. This setting specifies the number of minutes in this grace period.

Logon – Reauthenticate when resuming

- You can require users to re-enter their credentials when a device has been inactive (sleep, suspend, or hibernate). Network data traffic is automatically blocked on the resumed device until the user reauthenticates.

Device authentication

- Device authentication enables you to establish a mutually authenticated, encrypted VPN tunnel between client devices and the Mobility server without user intervention. Device authentication uses the RADIUS EAP-TLS protocol and signed X.509v3 certificates installed on the client. The addition of device authentication brings the following new capabilities:

Strong two- and multi-factor authentication

- Device-based, multi-factor authentication can be loosely or tightly tied to user authentication. For example, Mobility XE can be configured to allow a user to authenticate with any device that successfully authenticates. Alternatively, a user can be limited to logging on to just specific devices. Both factors – device authentication (something the user has) and user authentication (something the user knows) – must succeed before the user is allowed VPN access to network resources.

Secure access to unattended devices

- With the unattended mode feature in version 9.0, administrators have secure access to mobile devices when users are logged off. This means they can securely manage the device, apply security patches and updates, and monitor status when the mobile device is not in use (during off-hours, for example). In previous versions of Mobility XE, network traffic was blocked when the user was not logged on.

- Unattended mode supports Microsoft's Active Directory Group Policies, Microsoft SC-CM, Sybase Afaria, and many other policy and remote-device management solutions.

User credential protection/hiding

- Device authentication extends "credential hiding" capabilities — previously available only to customers using PEAP and RADIUS — to all supported authentication types, including SecurID. Credential hiding protects user authentication credentials and identities with an encrypted tunnel to prevent eavesdropping or the hijacking of user-authentication credentials.

Mutual authentication

- When using EAP-TLS authentication with X.509v3 certificates, device authentication provides mutual authentication of the client and the server, ensuring the identity of both the Mobility server pool and client.

New server setting: Authentication:device – Require Device Authentication

- When this new global setting is set to True, all devices attempting to connect to the Mobility XE 9.0 or later server pool must successfully complete device authentication before they are allowed to connect. Any device that fails device authentication is automatically disconnected.

New server settings: Authentication:device – RADIUS <settings>

- These settings mirror the user-authentication RADIUS settings that were available in previous versions and apply only to device authentication.

New client setting: Authentication – Mode

- This client setting can be set globally, for device classes, or for individual devices. Four different authentication modes are provided with Mobility XE version 9.0:
- **User authentication only**: The system performs only user authentication. Device authentication is not attempted, even if there is a valid device certificate installed. This is the default authentication mode and causes the Mobility XE system to behave as in previous releases.
- **Multi-factor**: When Mobility XE is configured to perform device authentication, true two-factor authentication is performed when user authentication is configured to require a user name and password (or another single-factor means of user authentication). When device authentication is paired with a two-factor user authentication scheme, Mobility XE performs three- or multi-factor authentication. With multi-factor authentication, the system performs both device authentication and user authentication before a VPN connection is established.
- **Unattended**: The system establishes a VPN tunnel after successfully authenticating the device, before user desktop authentication. Use this setting if devices need to be managed when a user is not logged on. When set to Unattended, user authentication is required for the VPN to remain connected when a user accesses the desktop.
- **User required / Device optional**: If the device is configured for device authentication, the system authenticates the device. However, if the device is not configured for it, the system skips device authentication and moves on to user authentication. The Device optional setting is intended to help administrators during the transition from User only to either Unattended or Multi-factor. Using this mode, an administrator can quickly see which devices are properly configured for device authentication and which are not.

New client setting: Security - Approved Devices

- You can restrict users to one or more devices during their Mobility VPN sessions by adding particular devices to the Approved Devices list. By default, all devices are approved and users can authenticate from any device.

Linking a device to its device authentication identity

- Whenever a client device successfully connects with any type of device authentication, Mobility XE records the device's authentication identity. Administrators can specify how lenient or restrictive Mobility XE is using the following settings:

New client setting: Authentication – Device Certificate Name

- The Mobility server records the Common Name contained in the certificate the Mobility client uses for device authentication. Once a given device's authentication identity has been recorded, the device is disconnected if the reported authentication identity is different than what is recorded. A blank identity can always be overridden with a new identity.

New client setting: Authentication: Device Certificate Name Cannot Change

- By default, a Mobility client device that has successfully authenticated must always use the same certificate for subsequent device authentications. When this setting is disabled, the device can authenticate using any valid device certificate, even if it previously authenticated successfully using a different certificate.

New client setting: Authentication – Device Certificate Names Must Be Unique

- When this setting is enabled (the default), a device's identity can be updated only if there are no other devices using the same identity. If the current identity is a duplicate of one already registered, the device's session is disconnected.

New client setting: Authentication – Unattended Mode Refresh Settings on Logoff

- This setting applies only to devices configured for unattended access. By default, when a user logs off, the VPN session remains active and drops back to unattended mode without disrupting the VPN tunnel. When this setting is enabled, the device's VPN sessions are temporarily disconnected after the user logs off, and device authentication is performed again, thus ensuring that device settings are updated after every logoff.

Mobility Console Changes

Client settings

- Several client settings are either new or have been revised:

"Logon – Wait Time" changed to "Logon - Connecting Dialog Duration"

- Specifies the amount of time the client waits for all authentication steps to be completed before displaying the desktop; the default is 60 seconds.

"Delay – Connecting Dialog" changed to "Logon - Connecting Dialog Delay"

- Specifies the amount of time the client waits before displaying the Connecting dialog box; the default is 15 seconds.

"Logon – Hide Connecting Dialog" changed to "Logon - Connecting Dialog Hidden"

- Specifies whether the Connecting dialog box is displayed after the amount of time specified with Logon – Connecting Dialog Delay; the dialog box is not displayed by default. This has been changed to an advanced setting.

New "Logon – Prompt for user credentials at every reconnect" setting

- When this setting is enabled, users must re-enter their credentials when reconnecting after bypassing or disconnecting (cached user credentials).

New "Logon – Try Windows Credentials" setting

- When this setting is enabled, Mobility XE automatically tries to complete the logon process with a user's Windows logon credentials. When you disable this setting, you disable this single sign-on functionality: users are always prompted to re-enter their credentials, even if the desktop and Mobility logons are the same.

Connection list changes

User Name handling updated

- In the connection list, authenticated devices that do not yet have an authenticated user display none in the User Name column. The User name filter on this page has been updated to allow none.

New Device Certificate Name column

- The Device Certificate Name column is available to display in the Current Connection list. The column shows the device identity that was established during device authentication.

New Authentication Mode column

- The Authentication Mode column in the Connection List shows what mode is currently in use by each device: User only, Multi-factor, Unattended, or Device optional.

New Authentication Mode filter

- A new filter on the Connection List enables you to search or filter by a device's authentication mode: User only, Multi-factor, Unattended, or Device optional.

New Reauthentication column

- The Reauthentication column in the Connections list displays the status and reauthentication time for each device. If the device authentication is successful, the status is success with a time stamp for the last reauthentication. If the device is waiting on reauthentication, the status shows as blocked with a timestamp.

Session Details changes

- The Session Details page now shows the authentication mode for a given session: User only, Multi-factor, Unattended, or User required / Device optional; it also displays the encryption type, reauthentication status, policy, and key strength.

Analytics Changes

New "Show Unattended data only" option

- You can configure reports to include devices that were connected in unattended mode. The filter is available for the following Analytics reports:
  - Application Launch Count
  - Application Version Usage Detail
  - Network Usage by Device

Updated Connection Status report

- The Connection Status Report now differentiates between attended and unattended modes when devices are connected and unreachable. The report shows the following states:
  - Connected (attended)
  - Connected (unattended)
  - Disconnected
  - Unreachable (attended)
  - Unreachable (unattended)
  - Unknown

General report changes

- Reports that display a "last logged on user" show the most recent attended logon; an unattended device session is not shown because there was no associated user.

New notification based on Disconnect Reason

- There is a new notification available in the Analytics Module that allows you to select from the many Mobility XE disconnect reasons, so that when they occur, an administrator can be notified.

New NAC failure notification in Analytics Module

- When a client fails to comply with a NAC (network access control) rule, the administrator can configure the severity level at which Analytics Module notifications are sent.

Policy Management Module Enhancements

New condition: Unattended

- There is a new condition in the Policy Management module that evaluates whether a device is attended (user logged on) or unattended (device authentication only). You can create, for example, a customized policy specifying that only specific device-management applications are allowed to run on a client device when a user is not logged on.

New action: Mobility Bypass mode

- You can now force Mobility in and out of bypass mode using a client policy. Mobility Bypass mode does not allow any traffic to be sent over Mobility XE, but it differs from normal bypass (the Bypass NetMotion Mobility menu item available from the Mobility XE system tray icon) and passthrough as follows:
- The client remains connected to the Mobility XE server when using the policy action. The client is able to receive policies and NAC rule sets, and it sends its status to the server. Policies sent from the server are evaluated. Only Block/Allow policy actions are ignored.
- With the Mobility Bypass mode action, in contrast to passthrough, the Mobility XE client VNIC is disconnected, allowing the operating system to disregard the virtual DNS and WINS addresses and to read the interface and routing tables correctly.

New condition: Connected

- There is a new Connected condition that evaluates to TRUE after a device or user has authenticated and the VPN session is established. This is different from the already-available Reachable condition. Connected is TRUE whenever there is an active VPN session, even when the device is out of range or otherwise unable to contact the Mobility XE server.

Improved comparison capabilities added to some conditions

- It is now possible to do an expanded set of string comparisons of conditions that include an interface name, DNS suffix, connection name, or access point SSID. The ability to do "equals/not-equal to" was added to the local address (POP), WINS server address, and DNS server address conditions.

Policy interface comparisons now allow "Any Interface"

- The Interface-based conditions (such as local address) have been enhanced to allow the option of specifying "Any Interface." This allows conditions to be checked for all active interfaces, not just the one currently in use by Mobility XE.

New condition: Battery Power

- You can create a client policy rule that takes an action, such as closing an application, based on what percentage of a device's battery is available.

New condition: Mobility server address

- There is a new option in the Address group of conditions that returns TRUE if the Mobility client is directly connected to one of the Mobility server addresses you specify. This means you can apply policies based on whether a mobile worker is inside or outside the company's premises. For example, when the Mobility client is connected through an internal interface, some customers want to operate in passthrough mode, or bypass all traffic.

Policy versioning

- Beginning in v8.0, the Mobility console identifies the release in which policy features were added. You can use the setting Policy - Disconnect if Client Incompatible to specify what to do in the event of a version mismatch: either disconnect clients that are subscribed to a rule set that uses conditions and actions added in later releases, or allow them to connect and ignore the policy.

Debug events configurable in Mobility console

- There is a setting in the Mobility console (for both client and server) called Events – Debug. When this new setting is enabled, the selected server(s) or Mobility client device(s) automatically begin collecting debug event details that are helpful for troubleshooting. On the client, this setting makes it easier for an administrator to collect troubleshooting information from a device without having to coach a mobile worker through a configuration change.

Event log archiving configurable in Mobility console

- To troubleshoot problems that occur infrequently, or that require a log of Mobility events over an extended period of time, you can configure the Mobility server or Mobility client to archive the event log to a text file at regular intervals using Event Log Archive <settings>. This may help identify problems when the maximum event log size is too small to catch the error. The settings are available for both clients and servers.

Simplified method for gathering Mobility server diagnostics

- There is a new icon in the Program Group on the Mobility server. Click Mobility Server Diagnostics to run a process that automatically collects and saves server diagnostic information, such as memory statistics and warehouse logs. This saves you time if you are working with NetMotion Wireless technical support on an issue and you need to gather information about a Mobility client system.

Client Interface Changes

Desktop authentication prompts

In the Windows logon dialog box, the new Skip button functions differently, depending on whether you have enabled bypass mode. If it's enabled, a user who clicks Skip will have network communication (assuming his or her credentials are valid), but no mobile VPN. If it's disabled, clicking Skip means the user is disconnected and must reauthenticate to the Mobility server before network communication is established.

"Connected" and "Authentication Mode" shown in client UI

- There are changes to two tabs in the Client Properties dialog:
  - The Status tab now displays "Connected".
  - The Details tab now shows the authentication mode currently configured for the device: User authentication only, Multi-factor, Unattended, or User required / Device optional.

New user authentication functions added to Mobility client API

- A new function call to the Mobility client API can help you automate Mobility XE logons by allowing the user name, password, and domain to be passed as arguments for Windows authentication. If RSA SecurID authentication is configured, the API supports passing the token string and PIN code. These additions make it possible for other programs to pass user authentication credentials.

Warehouse Changes

- Mobility XE version 9.0 installs the Sun ONE Java System Directory Server version 6.3.1. There were a number of security defects associated with Sun ONE Java System Directory Server version 5.2, which are resolved in version 6.3.1.
- The new warehouse is easier to install and includes a new Warehouse Management Tool for easier warehouse administration. It is available from the Start menu in the NetMotion program group.

Supported Platforms

- Current information on the Mobility XE product lifecycle and supported operating systems is available on our web site.
- The Mobility XE releases covered in this document are supported on the following platforms:

Server platforms

- Windows Server 2003 SP2 Standard, and Enterprise (32-bit Editions)
- Windows Server 2003 R2 SP2 Standard and Enterprise (32-bit Editions)
- Windows Server 2008 R2 Standard and Enterprise (64-bit only)

Client platforms

- Windows 7 (Professional, Enterprise or Ultimate)
- Windows Vista® 32-bit (Business, Enterprise, or Ultimate Edition) with Service Pack 1 or higher
- Windows Vista Tablet PC Edition with Service Pack 1 or higher, Windows XP® with Service Pack 3, or Windows XP Tablet PC Edition® with Service Pack 3
- Windows Mobile® 6.0, 6.1, and 6.5 (Professional, Standard, or Classic)
- Windows Mobile 5.x for Smartphone or Pocket PC® Phone Edition
- Windows® CE version 5.0 with ARM processor including CE Emulator or SH4 processor, or Windows CE version 6.0 and 5.0 with Windows Mobile networking

Reporting database platform support

- When you install the Analytics module, Microsoft SQL Server® 2005 SP2 Express Edition is automatically installed.

Microsoft Active Directory support

- Windows 2000 native and mixed domains
- Windows 2003 native and mixed domains
- Windows 2008 native and mixed domains

RADIUS servers

- Windows Server 2003 IAS
- Windows Server 2008 IAS
- Cisco ACS v4.0 and v4.2
- Juniper Steel Belted Radius v6.1
- Free Radius version v1.1.7

Supported authentication protocols

- NTLM
- RSA SecurID
- LEAP
- EAP/TLS
- PEAP-EAP/TLS
- PEAP-GTC
- PEAP-MSCHAP v2

Supported RSA SecurID products

- RSA Authentication Server 7.1
- RSA ACE/Agent 6.1.2
- RSA Soft token API for XP and Vista v4.0
- RSA Soft token API for CE 2.3

For More Information

To learn more about Mobility XE, visit **www.NetMotionWireless.com**

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