

# Security for Wide Area Wireless Networks

**WHITE PAPER**

## Executive Summary

Security in a wireless deployment is a balancing act between protecting corporate data assets and ensuring that security measures aren't so cumbersome that they impact worker productivity. Wireless security also presents a variety of challenges depending on the access networks used; and when workers connect via different means such as a mixture of wireless LANs and cellular data networks, the challenges compound. The Mobility XE mobile VPN delivers end-to-end security, regardless of the type and number of different networks involved. It handles multiple means of authentication which can be combined, enforcing strong authentication with minimal worker disruption. Industry standard encryption via a single VPN tunnel keeps data secure as it traverses multiple networks. And since mobile devices are widely dispersed assets, Mobility XE supports additional security measures at device endpoints, including Network Access Control for ensuring that device-level security is up-to-date and active, and Policy Management that governs how devices are used. Deployed properly and in conjunction with other prudent measures, Mobility XE is the centerpiece of a solid, secure, and easily managed mobile deployment.

## Security and Productivity: A Balancing Act

A 2008 Forrester survey of IT executives and technology decision makers found that roughly half of enterprises in North America identified mobility initiatives as critical priorities. The reasons? Mobile applications allow enterprises to cut costs, as well as improve employee productivity and efficiency (Forester, 2009). However, since workers and devices are dispersed in the field, and connect over wide-area networks often controlled by third parties, security is a paramount concern. To reduce the risks while reaping the rewards, organizations must carefully balance competing needs for security and productivity:

- Business managers want mobile employees to have the highest level of productivity while in the field
- Mobile workers want remote access to be easy and seamless
- IT professionals must ensure corporate information and assets are secure

The ultimate success of any mobile initiative lies in the hands of the mobile workers. They will not adopt technologies or adhere to security practices that impede them from doing their “real job.” Appropriate security must be implemented without substantially degrading worker productivity and overall usability, or the mobility project will likely fail to meet its business objectives.

## Concerns and Counter-Measures

There are many security issues inherent in moving users to wireless networks, such as:

### **Authentication and authorization**

- Should a connection be allowed to the enterprise network?
- Who is attempting to connect, and with what device? What access permissions should be given?

### Data integrity & security

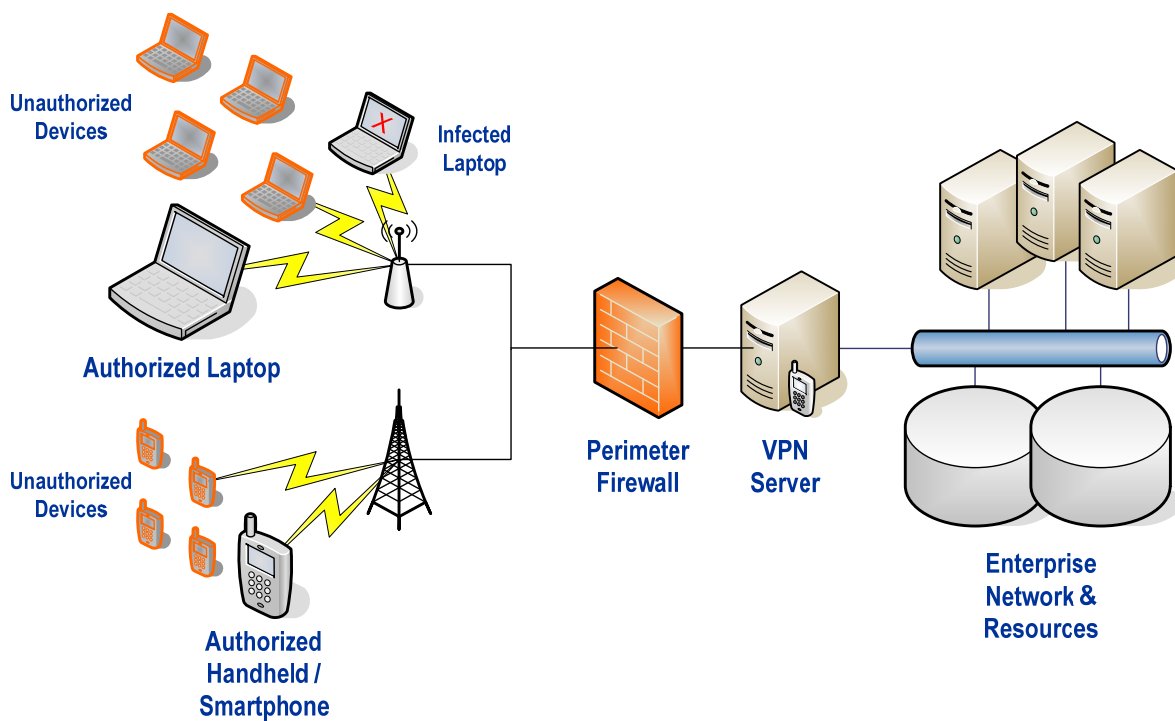
- Is the transmitted data being altered?
- Is someone able to eavesdrop on the data while in transit?

### Network protection, i.e. how can the network be protected against:

- Unauthorized use of corporate networks for personal business?
- Authorized users with untrusted devices?
- Lost, stolen or misplaced devices?
- Worms, viruses, etc.?

### Device protection

- How do you know that the device is still in the hands of an authorized user?
- How do you keep the device up to date with security patches?

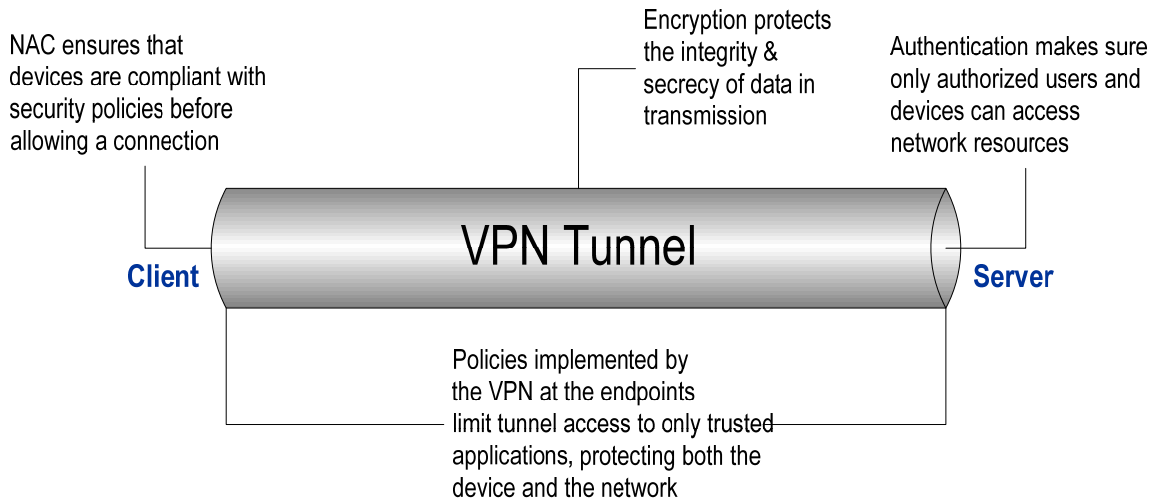


Connections and Threats

The NetMotion Mobility XE mobile VPN is a complete security-enforcement solution for mobile workers. It applies a number of techniques to combat the various security threats:

- **Authentication** provides assurance that the user and device attempting to connect are, in fact, who they claim to be.
- **Encryption** assures that the data in transmission has not been altered and that no one can eavesdrop on the transmission.

- **Network Access Control (NAC)** ensures devices connecting to internal networks are configured correctly and have prescribed security measures installed, enabled, and up-to-date.
- **Policy management** protects both the network and the device, controlling access to each.



### VPN Security Measures

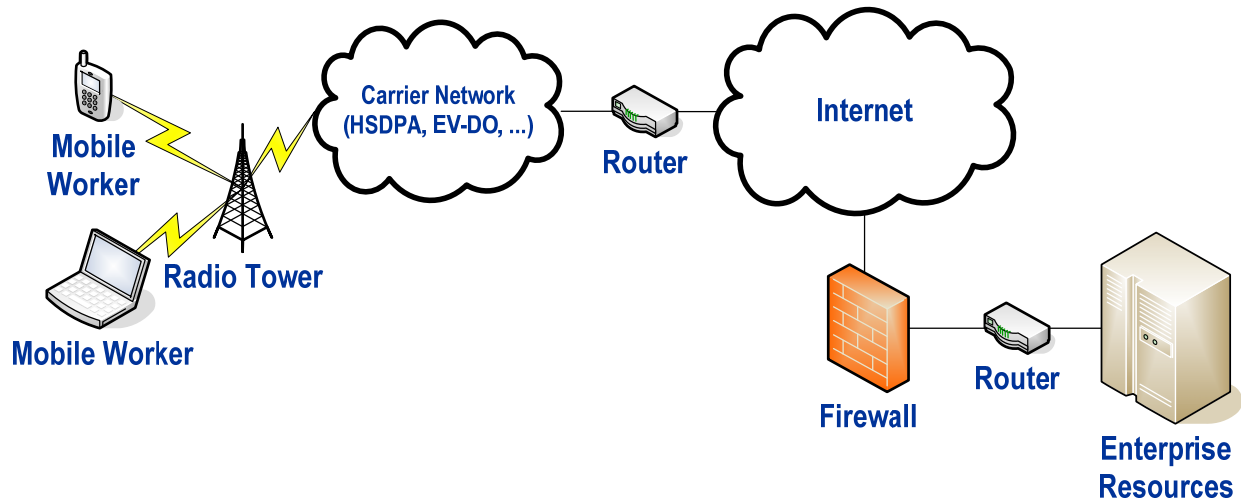
In addition to the above counter-measures, reporting and notifications capabilities give administrators information about security concerns as well as systemic issues, in order to better manage and monitor the security of the deployment.

## Access Methods & Networks

Different wireless access scenarios have their own particular vulnerabilities. The two most common access methods are wireless WANs (WWANs) operated by public cellular data carriers or private owners, and wireless LANs (WLANs) operated by private companies or by publicly accessible hotspot providers. Most legacy private radio networks owned by state and local municipalities are gradually being replaced or augmented by the publicly available WWANs and WLANs.

### WWANs Using Public Backhaul (Internet)

Wireless wide area networks operated by cellular data carriers provide cost-effective solutions for keeping mobile workers in contact with the enterprise. By default, data traffic is routed through the public Internet.

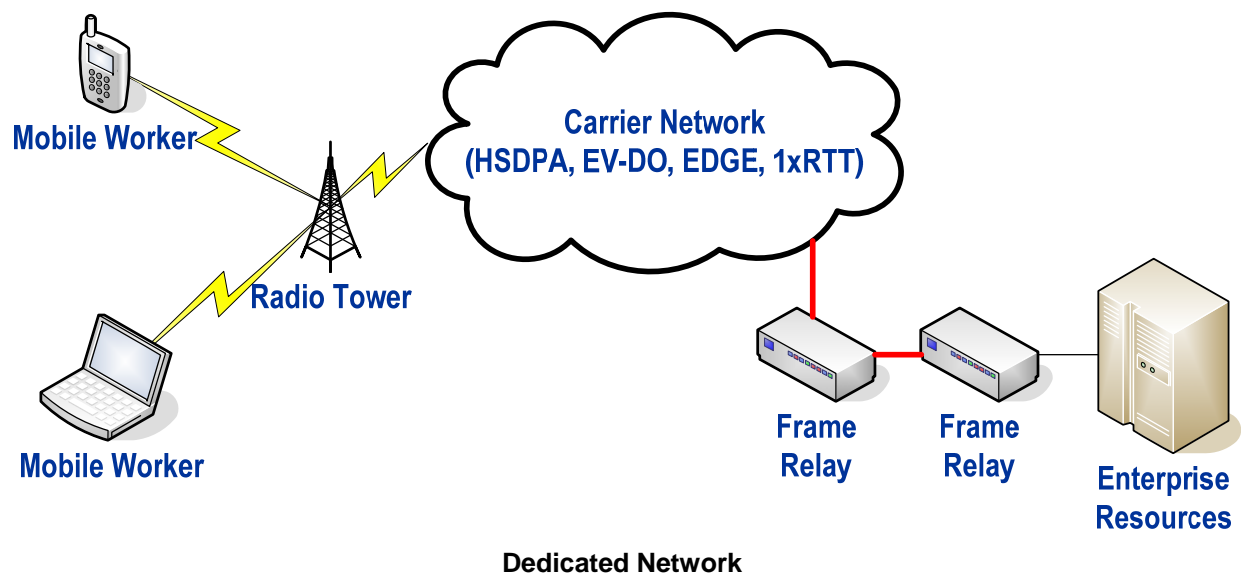


**Wireless WAN with a Public Backhaul**

In this model, the path from the mobile worker to the enterprise is through the carrier network and then via the Internet. Data security over the wireless link depends on the access technology and the wireless carrier, while data security over the Internet portion of the network is entirely the responsibility of the enterprise using it, not the service provider. Regardless of the technology used to secure the wireless link, all information traverses the public Internet unprotected on its way to and from an enterprise data center.

### WWANs Using Private, Dedicated Backhaul

Some WWAN providers provide dedicated routing options through a private data connection, via a dedicated frame relay (or sometimes ATM), from the carrier's network to the enterprise's private network.



**Dedicated Network**

WWANs with a dedicated backhaul connection provide an additional layer of security, but the strength of this additional layer depends on the network technology and the telecommunications carrier. In GSM and derivative networks, SIM (Subscriber Identity Mechanism) cards are used to supply the encryption key for the wireless portion of the network, but still leave the backhaul unencrypted. Several researchers have published weaknesses in the cryptographic algorithms which secure communications in modern GSM networks.

## WLANs

The IEEE 802.11b/g/n standards have made it possible for hardware vendors to create interoperable systems. As a result, WLANs are widely deployed in corporate environments, both inside and outside the trusted network. This success has increased the risk to corporate security.

Security options included with older wireless access points have been repeatedly shown to be insufficient:

- **Wired Equivalent Privacy (WEP)** is easily compromised and its exploits are well documented.
- **Wi-Fi Protected Access (WPA)** improved many of the deficiencies of WEP, but even WPA is susceptible to brute force dictionary attacks (to retrieve pre-shared keys used in authenticating a device to the access point) and Message Integrity Check (MIC) Denial of Service attacks.

Newer standards are far more robust:

- **Wi-Fi Protected Access 2 (WPA2)** has replaced WPA. It uses a new AES-based algorithm called CCMP that uses 128-bit keys. WPA2 is the Wi-Fi Alliance's name for 802.11i certification testing. At time of publication, it is generally accepted as a reasonably secure algorithm although it too has been shown to be susceptible to brute force attacks.
- **802.1x** addresses many of the device-to-access-point authentication issues. Of particular note is how it incorporates RADIUS servers, typically between authenticator and authentication server.

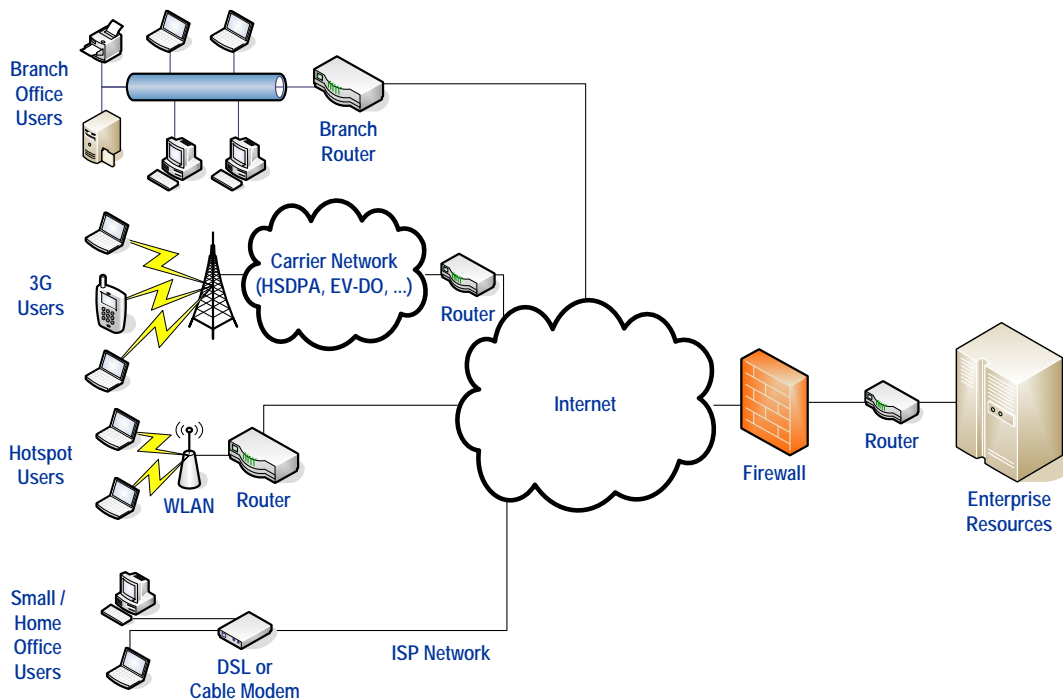
These WLAN security improvements are needed and welcomed. However, many older access points may not support these new standards. Organizations may be forced to either replace their infrastructure or configure their access points and clients for the lowest-common-denominator security protocol.

## WLAN Hotspots

Additional challenges ensue when mobile workers use public Wi-Fi hotspots. Repeated studies have shown that absent strong authentication and encryption, enterprise data is at risk when workers connect via public hotspots available in coffee shops and other public areas. Furthermore, incorrectly configured laptops and handhelds are at greater risk when connecting over hotspots, as they are effectively on a local LAN with all other devices connected to that hotspot. It is possible to "sniff" the contents of e-mails, files and data streams, or for other devices to connect directly.

## Multiple Networks

Many organizations have to rely on a combination of network technologies to get the coverage necessary for their mobile workers. A mobile worker may access enterprise resources after-hours over a home Wi-Fi network connected via DSL or a cable modem; travel to an office and use an Ethernet LAN; visit a customer site and connect via a WLAN for visitors; connect via a public hotspot at a coffee shop; and connect while traveling or out in the field using a carrier's WWAN. Multiple WWANs from different cellular carriers are often needed to cover the entire service area.



### Multiple Networks

Combining multiple networking technologies can be an effective way to effectively expand the footprint of a mobile network deployment, but the security challenges of each component must still be addressed individually. Each segment of the network may or may not have adequate security measures implemented to address its specific weaknesses. Sometimes it is not possible for an organization to physically manage and secure all of the external networks used for remote access. Therefore, it is especially important to have a single, reliable security framework in place that will secure communications both over the air and through the Internet, regardless of the network infrastructure being used.

## Securing Mobile Access: Mobility XE

The Mobility XE mobile VPN enforces security from endpoint to endpoint, regardless of the combination of networks used. It is a standards-based, secure, virtual private network designed specifically for wireless networking in highly mobile environments. Mobility XE is architected with an understanding of disparate network types, providing a seamless solution for users transitioning from home networks to hotspots and to mixed-vendor environments, be they WWANs or WLANs.

Although optimized for wireless networks, it also supports any type of network that uses the IP network protocol including Ethernet, DSL and dial-up.

Mobility XE is a layer 4 VPN. The transport layer (layer 4) implementation allows Mobility XE to manage and protect the data flow between the application (layer 7) and the networks (layer 3) by remotely proxying the mobile devices' application queries on the Mobility XE server. The proxy-based architecture works in conjunction with other technologies to prevent the application crashes that typically plague conventional VPNs in mobile environments. The layer 4 design also allows Mobility XE to offer a secure end-to-end VPN for any application running on the mobile device.

OSI Layer	TCP/IP Internet Protocol	VPN Technology
Application Layer 7		SSL
Presentation Layer 6	Telnet, FTP, SMTP, etc.	
Session Layer 5		Mobility XE
Transport Layer 4	Transmission Control Protocol (TCP) Unacknowledged Datagram Protocol (UDP)	
Network Layer 3	Internet Protocol	IPSec
Data Link Layer 2	Network interface cards: Ethernet, Token-Ring, FDDI, ATM, etc.	
	NIC drivers: Network Independent Interface Specification (NDIS), Open Datalink Interface (ODI)	
Physical Layer 1	Transmission media: Wireless media, fiber optic, coax, twisted pair, etc.	

### VPN Technology Comparison

From a networking security perspective, Mobility XE's location above the network layer allows it to maintain security as it seamlessly roams from one network to another. As a device transitions between networks of various types, the mobile worker, applications and VPN tunnel are automatically shielded from the changes.

The Mobility XE client is a software component that is transparent to the end user and does not require user configuration. The client adds a layer of security to the mobile device and provides local network firewall capabilities, although it does not entirely replace the need for a local firewall. When the Mobility XE client is active, it listens only on the active interface, and the only data path to the device is through the Mobility XE tunnel established between the Mobility client and server. When Mobility XE is connected, the device is hardened against man-in-the-middle attacks, port scans, and other local network attacks.

## Authentication

Before Mobility XE begins transmitting data between the network and Mobility client, it ensures that the end user (and if desired, the device) have successfully authenticated and have the required permissions.

While other VPNs often require multiple, separate authentication steps that get in a user's way, Mobility XE is designed to maximize productivity in the unique environment of a mobile deployment. (Other VPNs may require one interaction to enable network connectivity and a second to authenticate a user and establish the VPN.)

Mobility XE does not require the user to supply credentials other than those required to log in to the Windows domain or other authentication server. Domain policies for that user (for example, limited login times, restricted access to applications, login script requirements) are applied to that user's access to network and domain resources.

### Authentication Methods

Since every mobile deployment is different, Mobility supports multiple authentication methods which may be enforced in combination. The level of defense-in-depth and manageability is configurable by the administrator to fit the needs of the organization.

In addition, device-level authentication makes it possible for administrators to remotely manage a remote device even while users are not logged in. This allows over-the-air device management, just as though the device is physically attached to the network. These options are transparent to the user, boost productivity, and enhance user convenience and security.

### Authentication Protocols

NetMotion Mobility XE supports these protocols for user authentication:

- **NTLM (Windows users and groups, including Active Directory)**  
When a Mobility server is configured to use NTLM (version 2), users' credentials are authenticated against either the Windows domain that the Mobility server is a member of, or against local Windows users defined on the Mobility server itself. Users from other domains are allowed to connect if there is a trust between the domain the user is in and the Mobility server's domain.
- **RADIUS (Remote Authentication Dial-In User Service)**  
When using RADIUS, users' credentials are sent to specified RADIUS servers for authentication. Mobility XE supports RADIUS – LEAP, RADIUS – PEAP (MSCHAP or GTC), and RADIUS – EAP-TLS (smart cards or personal certificates).
- **RSA SecurID**  
Mobility XE supports native SecurID authentication. Mobility servers communicate directly with the RSA Authentication Manager using Authentication Agent software installed on the Mobility server machine.

Authentication Level	Credentials	Protocols	Remarks
Single-Factor	Windows domain credentials – user name/password, or smart card with embedded certificate	Microsoft NTLM with Active Directory or Mobility XE user lists RADIUS – LEAP, RADIUS – PEAP, and RADIUS – EAP-TLS	Simple security, easy to implement
Two-Factor User	Smart card + PIN	RADIUS – EAP protocol as front-end to Microsoft Active Directory	Required by many federal security mandates and standards
	X.509v3 user certificate + password (or biometric device)	RADIUS – EAP protocol as front-end to Microsoft Active Directory	
	RSA security token + PIN	RSA SecurID	
Device	X.509v3 device certificate	RADIUS – EAP-TLS	Allows unattended (no user logged-on) access for remote device management Provides mutual authentication of the device and the server Assures that the device belongs to the enterprise
Multi-Factor	Single-factor or two-factor methods above, combined with device authentication	As above	Ties the device (something you have) with the user's password (something you know) for true, inexpensive two-factor authentication

### Mobility XE Authentication Methods

#### Single-Factor Authentication

A user logs in to the Mobility client using Windows domain credentials – typically user name and password. Using Windows domain credentials allows for a single sign-on process to the device, the domain and the VPN that gives access to domain resources such as file system shares. After a user has been authenticated, Mobility XE establishes the VPN tunnel for securely transmitting application data.

**Integration with Active Directory.** When the Mobility server is configured to use the NTLMv2 authentication protocol (the default), its security is integrated with the security features in Windows, including the Active Directory service. For a Mobility client to connect to a Mobility server and use Mobility XE services, the person using the client must have a user account on the Windows machine running the Mobility server, or in the domain in which the server participates. Users must also be members of either the NetMotion Users group or of a specified domain user group with access to the NetMotion server. The Mobility XE setup program creates the local NetMotion Users group during installation, and allows the administrator to configure a global domain user group that determines which users are allowed to connect to a Mobility server.

#### Two-Factor Authentication

Organizations dealing with sensitive or privileged data often require authentication stronger than traditional user name + password credentials. In some cases, such as in law enforcement, there are

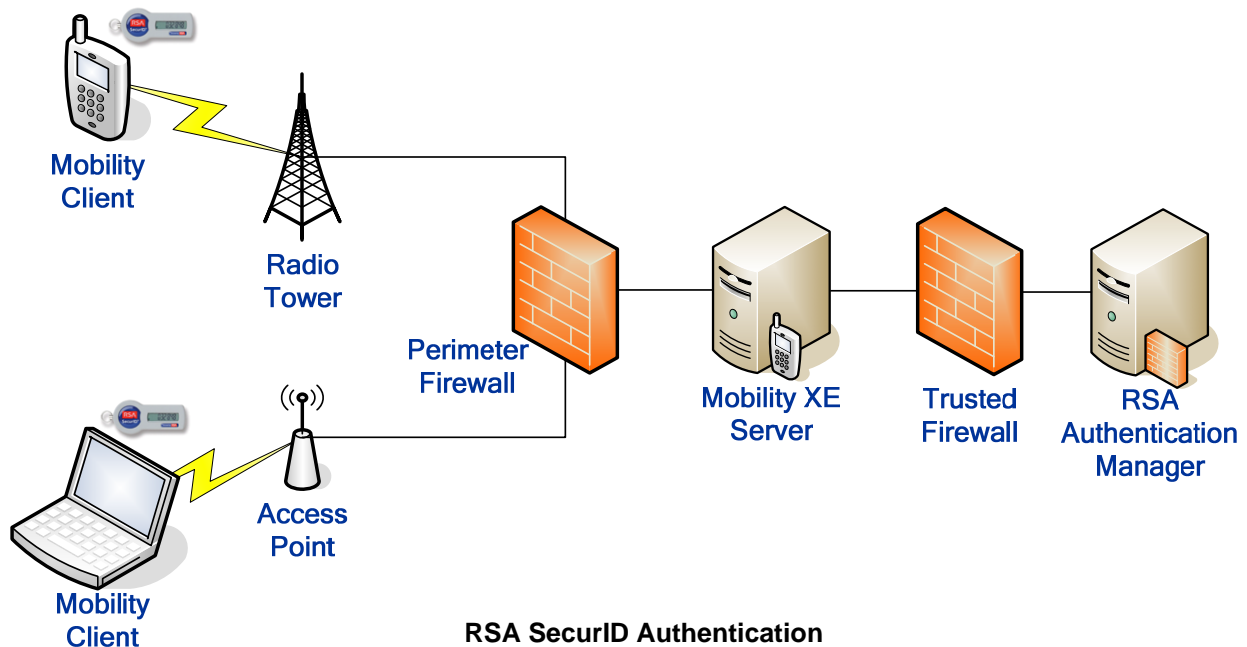
statutory requirements. For example, the federal Criminal Justice Information Services (CJIS) specifies stringent user authentication requirements for municipalities that connect to CJIS via wireless networks, the Internet or dial-up. Other federal regulations call for similar advanced authentication measures.

Mobility XE supports strong user authentication using several different types of credentials, including smart cards, X.509v3 user certificates, or RSA SecurID. These two-factor authentication methods require (1) something the user has (a smart card, device, or token) and (2) something the user knows (a PIN or password). Strong user authentication is important for protecting mobile devices that can be easily lost or stolen.

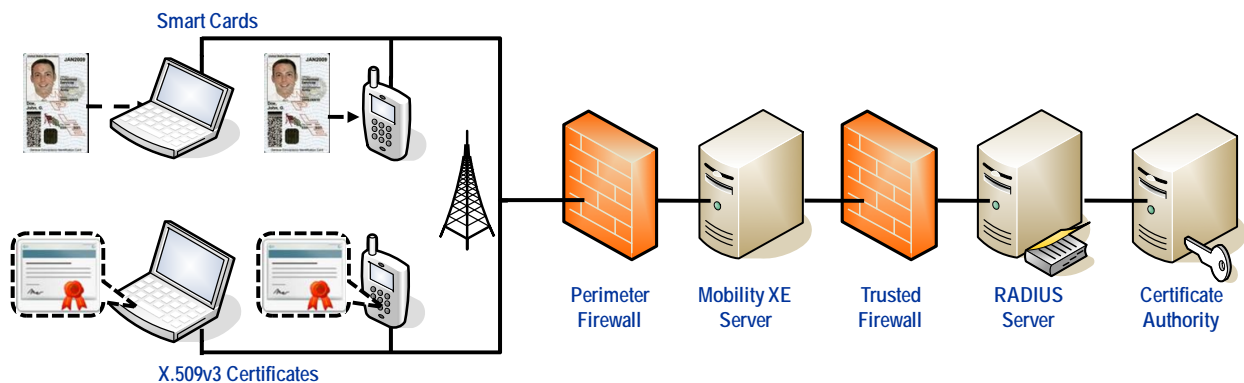
Mobility XE supports the following strong, two-factor user authentication methods:

**RSA SecurID.** RSA SecurID uses key fobs, PIN pads, USB tokens, smart cards and software tokens. The various supported devices all require that the user enter a PIN in order to access the one-time password.

Mobility XE two-factor authentication meets RSA certification criteria, including native authentication via the RSA Authentication Agent and support for New PIN Mode and Next Tokencode Mode. The implementation has been certified as RSA SecurID Ready. For more information about Mobility XE and RSA authentication see Tech Notes 2214 *Enabling Native RSA SecurID Connections for Mobility Clients*, and 2150 *Enabling RSA SecurID Connections for RADIUS* on [www.netmotionwireless.com](http://www.netmotionwireless.com).



**RADIUS/PKI.** RADIUS/PKI two-factor authentication allows organizations to meet federal standards at minimal cost. It uses the RADIUS-EAP protocol as the front-end to Microsoft's Active Directory Authentication and Public-Key Infrastructure (PKI). Because the Microsoft PKI infrastructure is bundled with their server operating systems, and with several free or low-cost RADIUS server options available, this approach is a very low-cost and robust option. It is especially useful for public safety agencies that must comply with the CJIS requirements, but may not have allocated the budget to bring their systems into compliance.



### Two-Factor Authentication via X.509v3 Certificates, Smart Cards, RADIUS and PKI

This RADIUS/PKI approach supports:

- **Smart cards.** Mobility XE supports PKI smart cards from vendors that meet Microsoft's smart card mini-driver requirements, and from vendors that provide a Microsoft Cryptographic Service Provider (CSP). Of particular note, Mobility XE supports smart cards conforming to these requirements: Homeland Security Presidential Directive 12 (HSPD-12); Federal Information Processing Standards Publication 201 (FIPS 201); Personal Identity Verification (PIV) of Federal Employees and Contractors; NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification and CJIS Security Policy 4.5.
- **X.509v3 user certificates.** Certificates are supported when stored on the mobile device in a protected location only accessible to users who successfully complete desktop authentication and who provide the user certificate password. Non-Microsoft PKI solutions are supported if they are compatible with X.509v3 user certificates, standard Microsoft CAPI-enabled access to those certificates, and the RADIUS EAP-TLS or EAP-TLS inside PEAP authentication protocol.
- **Biometric systems.** Mobility XE supports biometric systems where those systems are used in place of a PIN or password to unlock access to X.509v3 certificates. Mobility XE also supports biometric-based user authentication on the Ubtek and Wave biometric systems, which are commonly installed on Lenovo, Itronix, and Dell portable computers.

## Device Authentication

Device authentication enables the device and server to establish a trusted relationship independent of the user login. Device authentication uses the RADIUS EAP-TLS protocol and signed X.509v3 certificates installed on each device to create a mutually-authenticated, encrypted VPN tunnel. Using device authentication, Mobility XE can provide secure access to the mobile device when it is unattended – that is, while the device is powered on but a user is not logged onto the desktop, either in pre-desktop mode before the user logs on or after the user has logged off. (For Windows Mobile devices that do not have a pre-desktop mode, the device is in unattended mode after a user has logged off, and the login dialog box prompts for the next user to log in.)

Device authentication is useful for:

- Allowing over-the-air device management and monitoring, including applying security patches and updates at times when the user is not actively using the device
- Enforcing even stricter security with a third factor, by tying a specific user to a specific device
- Preventing users who have VPN access privileges at the user level from accessing corporate resources from home PCs or other unauthorized and untrusted devices
- Hiding user credentials by establishing a secure tunnel between the device and the server before the user logs in

Support for unattended mode allows enterprises to use their full array of enterprise policy, asset management and control tools to manage their mobile, remote devices while they are still in the field. In fact, they can be managed as easily as devices connected to the local LAN. This can be particularly useful for performing software updates after-hours while the mobile device is not otherwise in use. Unattended access supports Microsoft's Active Directory Group Policies, Microsoft SC-CM, Sybase Afaria and many other policy and remote device-management solutions. Through device authentication, IT is able to extend enterprise management tools to the wireless device population, simplifying device management while lowering total cost of ownership.

## Multi-Factor Authentication

The combination of device and user authentication makes Mobility XE security stronger than that available in other VPNs. It ties the user authentication (something you know) to the device authentication (something you have), much like a PIN is tied to a bankcard, so that only authorized users with sanctioned devices that have been properly provisioned can connect.

Device authentication can be loosely or tightly tied to a user's authentication. Mobility XE can be configured to allow a user to authenticate with any device that has successfully completed device authentication; or to limit the user to logging in with one or a few specifically identified devices.

Alternately, administrators may choose to automatically quarantine new or unknown devices, and specifically authorize them before allowing user access to the network.

Device authentication also hides user authentication credentials and identities by first creating a secure tunnel between the device and the server, through which the user credentials are then passed.

## User Reauthentication

In a mobile environment, devices are prone to being misplaced, lost or stolen. Mobility XE is able to selectively enforce reauthentication at an adjustable interval, or when the device resumes after being suspended. Administrators also have control over the grace period during which the user must respond. This feature works with all of the user authentication methods that Mobility XE supports. A successful response confirms that the user is still in possession of the device. If the user is unable to successfully reauthenticate, Mobility XE disconnects the VPN and records the failure to reauthenticate in the system logs for later review.

Most significantly, Mobility XE is able to enforce this reauthentication and prompt the user without disrupting any application sessions that are open or active. No other VPN is able to reauthenticate users seamlessly without needlessly disrupting application sessions.

## Encryption

### Key Exchange

After successful authentication, the Mobility server sends the Mobility client a data-security-level specification (turning encryption on or off). The server mandates the data security level — it is not negotiated — which prevents possible downgrade attacks.

A signed Diffie-Hellman key exchange (ECDH) occurs between the Mobility client and server that establishes the encryption keys for the session. The key sizes for ECDH are chosen based on the AES key size as recommended by NIST in FIPS PUB 186-2, *Digital Signature Standard*.

For NTMLv2 and LEAP authentication, Mobility protects against man-in-the-middle attacks by signing the Diffie-Hellman parameters in the key exchange. The receiver authenticates the parameters by checking the signature.

Automatic rekeying enhances Mobility VPN security by periodically changing the keys used to encrypt data passing between the Mobility client and server. When rekeying is enabled, the server initiates a key exchange with each client connection at random times within a configurable rekey interval. The exchange produces a new, unique session key for each client connection; it is unrelated to the previous key, so compromising one key does not compromise future communication based on the new key.

### Encryption Methods

NetMotion Mobility offers the following types and levels of encryption:

- **AES.** AES is the Advanced Encryption Standard for the United States. This algorithm is used to encrypt data traffic sent between the Mobility client and the server. Mobility XE's default setting is 128-bit key strength, which is the minimum standard for CJIS security policy compliance. Administrators may also choose 192-bit and 256-bit key strengths.

AES key size	ECDH key size
128	256
192	384
256	521

**Corresponding AES & ECDH Key Sizes**

On the mobile device running the Mobility client, data is processed at the session level. All application data destined for TCP and UDP sessions are secured. (Connection-oriented applications generally use TCP for communications; others such as streaming media use UDP.)

## Device-Level Security

In a mobile deployment, devices are widely dispersed, often hundreds of miles away from the data center and outside of IT's physical reach. Mobility XE offers management capabilities for effective control, ensuring that security measures are in place and users employ devices for authorized uses and in a secure manner.

### Mobile Network Access Control

Mobile devices in the hands of naive and unsuspecting users have emerged as one of the greatest threats to organizational security. These devices can harbor key loggers and other malware, planted via unpatched security holes. Network Access Control (NAC) inspects devices to ensure that they are configured and patched correctly, and that security software (such as antivirus, antispymware and firewall) is up-to-date and running. If mobile devices are not properly configured, Mobility's NAC module warns users, prevents or restricts network access, and facilitates remediation.

The integrated Mobile NAC module gives administrators great control and flexibility over when and how to enforce remediation policies. It monitors the complete security posture of a device and can detect when key security-related components are missing, disabled or out-of-date including:

- Antivirus
- Firewall
- Windows™ Update status
- Line of business applications
- Antispyware
- Operating system version
- Registry keys

Mobile NAC works hand-in-hand with the Mobility XE Policy Management module to push out highly customized warnings and apply remediation policies. Based on severity, user login status and connection speed, administrators can specify simple alert messages or remediation instructions, limit application access, launch websites, initiate software downloads, quarantine the device or disconnect it. For instance:

- If anti-virus signatures are more than seven days old and the device is running in unattended mode, immediately download updated signatures

- If anti-virus signatures are more than seven days old and a user is currently logged in, send a warning message
- If more than 14 days old, send a more strident warning message if on a WWAN connection, and initiate immediate download of the signature file on a fast Wi-Fi connection
- If more than 21 days old, quarantine the device immediately

For a more in-depth discussion of Mobile NAC, read the white paper *Mobile Network Access Control* on [www.netmotionwireless.com](http://www.netmotionwireless.com).

## Policy Management

Mobility Policy Management allows the administrator to centrally define rules and rule sets that can enforce policy on a per-device, device group, user or user group basis from layer 2 through layer 7, dependent on the networks available to the device or user. Rules can be defined using interface name, speed, SSID, BSSID (all layer 2), IP address and port (layer 3), transport (layer 4), session (layer 5), and application (layer 7). In addition, the policies are deployed to each mobile device or user and enforced on the mobile computing device. There is no bandwidth cost in denying access and securing internal networks or resources.

For example, an administrator may wish to prevent bandwidth-heavy applications from passing traffic while on a bandwidth-sensitive WWAN or if the connection speed of that network is below a certain (definable) threshold (i.e., less than 256kbps). In addition, policies can combine multiple layers for more granular control. For instance, a policy can block the functioning of a particular named application, except to a specified address and/or port. This granular approach to policy management allows the administrator to centrally manage and control WWAN costs, bandwidth usage, and user experience while applying a powerful solution that is consistent with the organization’s security policies.

	Mobility XE	IPSec VPN	SSL VPN
<b>Layer(s)</b>	Layer 2 through Layer 7	Layer 3	Layer 7
<b>Created</b>	At the server	At the concentrator	At the server appliance
<b>Enforced</b>	At the client	At the concentrator	At the server appliance
<b>Paradigm</b>	Device/user by interface, network, application	User by network	User by application
<b>Controls access to</b>	Networks, applications & resources	Networks	Applications & resources

### Policy Enforcement Comparison with Other VPN Types

Separate policies may be defined and enforced while a device is running in unattended mode (while a user is not logged in). This allows administrators to dictate when and how authorized management tools may access the network for updating system components and applications, keeping these tasks from impacting worker productivity.

For more about Policy Management, read the white paper *Policy Management Module: Granular Management of Wireless Bandwidth, Security and Mobile Productivity* on [www.netmotionwireless.com](http://www.netmotionwireless.com).

## Visibility and Alerting

When a security issue arises, it's not just corporate data that's at risk. Failed logins could mean that a device has been stolen, or that a device that has been quarantined due to a security concern could seriously hamper the employee's ability to work efficiently. To give administrators the knowledge to deal swiftly with such concerns, the Mobility XE Analytics Module offers notification and reporting capability.

Some of the notifications have immediate security implications, such as repeat login failures (a thief trying to guess passwords) or a device that's outside the standard for NAC compliance. Administrators receive these notifications via e-mail, or through standard network management systems (syslog or SNMP consoles). Immediate notifications allow administrators to investigate and rectify the situation and get the worker back on the job.

The reports capability delivers insight into when and how workers are using networks and applications. This allows administrators to better address the security issues – such as when to remediate devices – while preserving the productivity gains that drive the mobile deployment.

To learn more about the Analytics Module, read the white paper *NetMotion Mobility XE Analytics Module: Bringing Visibility Into Mobile Deployments* on [www.netmotionwireless.com](http://www.netmotionwireless.com).

## Secure Deployment of Mobility XE

For Mobility XE security to be effective, it must be deployed in a secure fashion in concert with other security mechanisms and practices.

### Server Deployment

NetMotion Wireless recommends that organizations follow both Microsoft and U.S. government recommendations regarding hardening Windows servers.

If a Mobility server is going to be accessed by users on public WLANs or WWANs, Mobility servers should be deployed in a firewall DMZ or behind the corporate firewall. Port 5008 (or other port as chosen by the administrator) must be open in the protecting firewall(s) to allow access to the Mobility server.

Specific suggestions for server pool locations and settings can be found in Tech Note 2161 *Where to Deploy Your Mobility Server* on [www.netmotionwireless.com](http://www.netmotionwireless.com).

### Extending the Firewall

The Mobility server acts as a transport-level proxy. Application transactions are forced through controlled software that protects the user's machine from attacks that use malformed packets, buffer overflows, fragmentation errors and port scanning. Because Mobility XE is a transport-level proxy, it provides this protection for a wide range of applications.

## Client Deployment

Depending on security requirements, Mobility XE can be used to strongly tighten security on mobile devices. Administrators can force clients to use the Mobility VPN (preventing network access other than through the VPN tunnel to the Mobility server), put lost or stolen devices in quarantine, and prevent access from new devices.

- **Client lockdown.** When the Mobility client is connected, all IP traffic is tunneled through the Mobility server. In addition, while traffic is tunneled through to the server, an administrator can use the Policy Management module to limit the IP addresses that can be accessed by a Mobility client and the applications that can use the network. Putting lockdown in place substantially enhances security. This is especially valuable when users access the network via public hotspots.
- **Quarantine — lost or stolen devices.** A client in quarantine has no access to network resources. This is useful in case of lost or stolen devices. An administrator can put the device in this state, preventing access to the corporate network, data and applications.
- **Quarantine — preventing access by new devices.** A common use of the Quarantine feature is to put all new client devices in quarantine until manually approved by an administrator. The new device can register, but is then immediately disconnected and placed in quarantine, allowing the administrator to then go back and validate any newly connected devices. This keeps unauthorized devices off the network, even if the user has valid credentials.

## Password Policy

NetMotion Wireless recommends a strong password policy:

- Change passwords frequently.
- Avoid short, common words. Passwords should be more than 8 characters long.
- Use a combination of letters, numbers and other characters.

## Other Security Components & Interoperability

A Mobile VPN is only part of a secure system. Security-conscious enterprises use additional solutions to further secure and protect their mobile devices. NetMotion Mobility XE has been tested with and complements these solutions:

- **Antivirus.** Maintaining and requiring the latest antivirus definition files is crucial. Mobility XE's NAC module interoperates with products from leading antivirus vendors to ensure that protection is enabled and up-to-date.
- **Distributed firewall.** Personal or distributed firewalls have become commonplace. Mobility XE is compatible with many mobile-device firewall solutions commonly used on both the Windows and Windows Mobile platforms. The NAC module can verify that the firewall is enabled before allowing a connection.
- **Local encryption.** Solutions are available that encrypt the data stored locally on mobile devices, and prevent leakage of data via USB drives and other removable media. If a device

is compromised, some include a device-wipe option that destroys the data on the device after a failed login threshold has been reached or in response to a command from a network administrator.

- **Device management.** Patch management and software updates are features common to device management solutions. Device management tasks occur within the secure tunnel provided by Mobility XE. If device authentication is used, the updates can run outside of working hours while the worker is not logged into the system, with full benefit of Mobility XE link optimizations.

## Conclusion

The Mobility XE mobile VPN is an elegant, easily managed solution that handles the myriad challenges involved with enforcing security across a wireless deployment. It not only protects enterprise assets, but also the enterprise investment by minimizing the impact on workers and maximizing the productivity gains.

## For More Information

To learn more about Mobility XE, visit [www.netmotionwireless.com](http://www.netmotionwireless.com).

© 2010 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion Wireless technology is protected by one or more of the following US Patents: 5,717,737; 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; 7,574,208; 7,602,782; 7,644,171; and Canadian Patent 2,303,987. Other US and foreign patents pending.