

NetMotion Wireless Mobility XE™

Preisgekrönte, branchenführende Mobile-VPN-Lösung

Mobility XE wurde speziell für Mitarbeiter entwickelt, die häufig unterwegs und dabei auf sicheren und zuverlässigen drahtlosen Zugriff auf kritische Daten und Anwendungen angewiesen sind. Mit dieser Lösung bleiben Ihre Mitarbeiter produktiv, unabhängig davon, ob sie täglich an mehreren Standorten zugegen sind oder ständig zwischen verschiedenen Büros und Gebäuden auf dem Unternehmensgelände wechseln. Sie ermöglicht den Zugriff auf unterschiedlichste Netzwerke, das Überwinden von Abdeckungslücken und das wiederholte Deaktivieren und Aktivieren der mobilen Endgeräte.

Sicherheit

Schutz. Die branchenweit stärkste Verschlüsselung mit FIPS-Validierung (Federal Information Processing Standard) sichert den VPN-Tunnel. Vor Erteilung einer Zugriffsgenehmigung überprüft das Netzwerkzugriffskontrollmodul, ob auf jedem Endgerät die neuesten Software- und Patch-Versionen installiert und sämtliche Sicherheitsvorkehrungen aktiviert sind.

Authentifizierung. Durch Unterstützung der standardbasierten Zwei-Faktor-Authentifizierung erhalten Behörden eine bezahlbare Möglichkeit, die Sicherheitsvorschriften zu erfüllen.

Mithilfe preisgünstiger Chipkarten sowie kostenloser bzw. kostengünstiger X.509v3-Benutzerzertifikate unterstützt Mobility XE die meisten standardbasierten Infrastrukturen zur PKI-Authentifizierung über RADIUS EAP.

Die Authentifizierung auf Geräteebene ermöglicht eine Mehrfaktor-Authentifizierung, die die Benutzer eng oder lose an das Gerät bindet. Mit einer regelmäßigen Neuauthentifizierung wird sichergestellt, dass sich die Geräte weiterhin im Besitz der befugten Benutzer befinden.

Durchsetzung. Flexible Richtlinien steuern das Verhalten von Geräten und Anwendungen, schränken den Anwendungszugriff ein und halten bandbreitenhungrige Prozesse von langsameren Netzwerken fern, um eine Leistungsbeeinträchtigung zu verhindern.

Produktivität

Nutzungskomfort. Mobile Mitarbeiter können sich mittels SSO (Single Sign-on) einmalig authentifizieren und damit sämtliche Netze und Zugangspunkte nutzen. Mit Mobility XE ist auch bei Unterbrechung des Funkkontakts für eine weiterbestehende Authentifizierung und ein zuverlässiges Funktionieren der Anwendungen gesorgt.

Roaming. Mobility XE ermöglicht nahtloses Roaming in beliebigen IP-Netzen

und über eine beliebige Kombination von IP-Netzen hinweg. Benutzer können sich frei zwischen Dockingstations, Unternehmens-WLANs, externen WiFi-Hotspots und Mobilfunknetzen verschiedener Anbieter bewegen und dabei automatisch die schnellste verfügbare Verbindung nutzen.

Performance. Mobility XE verbessert den Durchsatz, die Antwortzeiten von Anwendungen und die Produktivität bei Drahtlosnetzen mit eingeschränkter Bandbreite. Protokoll-Overhead und Chattyess („Geschwätzigkeit“) werden verringert, Daten und Web-Bilder werden komprimiert, so dass der Durchsatz drastisch erhöht wird.

Zuverlässigkeit. Wenn es darum geht, Anwendungssitzungen aktiv und stabil zu halten, kann es kein anderes mobiles VPN mit Mobility XE aufnehmen. Bei Abdeckungslücken werden Anwendungen ganz einfach pausiert. Der Sendevorgang wird fortgesetzt, wenn wieder eine Verbindung vorhanden ist. Die Datenübertragung wird dort wieder aufgenommen, wo sie unterbrochen wurde – auch wenn das Gerät erst Tage später reaktiviert wird.

Management

Steuerung. Mobility XE ist so konzipiert, dass Einstellungen nur einmal vorgenommen werden müssen und kaum Managementaufgaben für Routineprozesse anfallen. Die browserbasierte Administrator-Konsole ermöglicht die zentrale Konfiguration, Verwaltung und Überwachung sämtlicher Systemaspekte – von den allgemeinen Systemparametern bis hin zu den genauen Daten einzelner mobiler Benutzer.

Durch zentrale Steuerung können unberechtigt genutzte, verlorene oder entwendete Geräte gesperrt werden. Die Geräteauthentifizierung unterstützt das drahtlose Geräte-Management mithilfe von Management-Suites von Drittanbietern.

Transparenz. Automatisierte Benachrichtigungen ermöglichen ein nahezu vollautomatisches Management.

Mittels ausgefeilter Analysefunktionen erhalten Sie dabei genaue Einblicke in das Verhalten und die Anwendungsnutzung mobiler Mitarbeiter.

Kompatibilität. Jede netzwerk-basierte Anwendung lässt sich ganz einfach durch Installation von Mobility XE auf eine zuverlässige Ausführung in Drahtlosnetzwerken umstellen. Dabei ist es nicht erforderlich, Anwendungen zu verändern, teure Entwicklungsarbeiten durchzuführen oder ein Upgrade auf spezielle Wireless-Versionen vorzunehmen. Mobility XE ist mit Windows™-Geräten und jedem IP-Netz kompatibel.

Kosteneffizienz. Installation und Einrichtung nehmen nur wenige Stunden in Anspruch.

Der Mobility XE-Server lässt sich hinter der Unternehmens-Firewall oder innerhalb der DMZ auf standardmäßiger, handelsüblicher Hardware – einschließlich virtuellen Umgebungen – installieren.

Die Clientsoftware kann auf Windows-Geräten installiert und zentral konfiguriert werden und ist für den Endbenutzer transparent.

Skalierbarkeit. Mobility XE ermöglicht den Übergang vom kleinen Pilotprojekt zu groß angelegten Installationen. Dabei kann ein Server bis zu 1.500 gleichzeitig laufende Geräteverbindungen bewältigen. Server lassen sich zusammenschließen, um neben einer Kapazitätserweiterung auch Lastausgleich, Failover und Redundanz für Tausende von Mitarbeitern bereitzustellen. Dies ermöglicht ein hochgradig skalierbares und zuverlässiges System ohne alleinige Fehlerstellen.

Richtlinienverwaltungsmodul

Zentrale, flexible Steuerung mobiler Produktivität und Sicherheit.

Das optionale Richtlinienverwaltungsmodul setzt unternehmensspezifische Sicherheitsrichtlinien durch und gewährt selektiven Zugriff nach Benutzer, Gerät, Netz oder Anwendung.

- **Kontrolle über den Zugriff auf Anwendungen und Ressourcen.**

- Richtlinien bieten präzise Kontrolle darüber, welche Anwendungen wann Zugriff das Netzwerk erhalten.
- **Richtlinienzuweisung.** Die Richtliniendurchsetzung erfolgt für den Benutzer transparent und kann auf Grundlage von Personen, Funktionen, Arbeitsgruppen oder ganzen Organisationsgruppen zugewiesen werden.
 - **Datenverkehrsmanagement mit Quality of Service (QoS).** Mittels Datenverkehrsklassifizierung und Steuerungsrichtlinien können aufgabenkritischen Anwendungen Prioritäten zugewiesen werden, um deren Verfügbarkeit unabhängig vom Netztyp zu gewährleisten.
 - **Beschränkung bandbreitenintensiver Anwendungen auf Verbindungen mit hoher Übertragungskapazität.** Mithilfe von Richtlinien können Sie verhindern, dass bandbreitenintensive Anwendungen langsamere Netze verwenden, oder dafür sorgen, dass Anwendungen gestartet werden, sobald ein Hochgeschwindigkeitsnetzwerk verfügbar wird.
 - **Unterstützung von Echtzeitanwendungen.** Neben den QoS-Funktionen (Quality of Service) beinhaltet Mobility XE Funktionen zur Wiederherstellung verlorener Pakete, die eine bessere Performance bei Echtzeitanwendungen wie VoIP, Video-Streaming und Echtzeit-Videokonferenzen ermöglichen, die anfällig für Latenzzeiten und Jittering sind.
 - **Sichere und einfache Nutzung von WLANs und Hotspots.** Richtliniengesteuertes, selektives Zulassen oder Ablehnen von Datenverkehr je nach Zugangsknoten oder Hotspot-Anbieter.
 - **Schnelle Einsatzbereitschaft.** Der NAC-Modulassistent macht die Konfiguration und Umsetzung von Sicherheitsrichtlinien ohne Neukonfiguration der Netzwerkinfrastruktur zur einfachen, minutenschnellen Aufgabe.
 - **Durchsetzen der Sicherheitskonformität.** Mittels NAC werden mobile Endgeräte auf die Einhaltung von Software-Anforderungen überprüft, u. a. auf Antiviren-, Anti-Spyware- und Firewall-Software, Betriebssystemversion, Windows™-Aktualisierungsstatus, Registrierungsschlüssel und andere Anwendungen.
 - **Flexible Kontrolle über nicht konforme Geräte.** Je nach Schweregrad haben Administratoren die Wahl zwischen Maßnahmen von einfachen Warnungen bis hin zum Auslösen genau definierbarer Problembhebungsprozesse, die den Anwendungszugriff einschränken, Websites aufrufen, Software-Downloads starten oder das Gerät sogar vom Netz trennen und isolieren können.
 - **Automatische Aktualisierung und Konformitätsprüfung.** Aktualisierte Regeln werden automatisch an Client-Geräte übertragen. Darüber hinaus werden Geräte automatisch und in regelmäßigen Abständen gescannt, um auch nach dem Aufbau der Verbindung die Einhaltung der Sicherheitsvorgaben zu gewährleisten.
 - **Durchgängige Unterstützung auf mehreren Plattformen.** NAC-Richtlinien werden auf sämtlichen Windows-basierten Client-Geräten unterstützt, u. a. Notebooks, Handheld-Geräten und Smartphones.

Analytics Module

Proaktives Management und transparente Nutzung mobiler Endgeräte. Das Analytics Module stellt Nutzungsdetails und geschäftliche Einblicke zur Verfügung, die Sie in anderen VPNs nicht finden werden. Es bietet statistische Daten über Leistung und Nutzung sowie Informationen über die Anwendungen und Netze, die von den Mitarbeitern genutzt werden. Automatisierte

Benachrichtigungen reduzieren den Verwaltungsaufwand und erleichtern die bedarfsgerechte Anpassung und Kapazitätsplanung.

- **Vom Überblick zu den Details.** Grafische Berichte mit Nutzungstrends gehen weit über einfache Aktivitätsprotokolle hinaus, wie sie von normalen VPNs verwendet werden. Mithilfe von Filtern können Sie genaue Daten über bestimmte Benutzerpopulationen und Zeiträume anzeigen.
- **Details zur Ressourcennutzung.** Informieren Sie sich darüber, welche Anwendungen, Geräte und Benutzer die größte Bandbreitennutzung aufweisen. Nutzen Sie Richtlinien zur Verbesserung der Produktivität und Einhaltung von Netzbetreiber-Servicevereinbarungen.
- **Abdeckungs- und Verbindungsprobleme erkennen.** Informieren Sie sich, bei welchen Geräten und Netzwerken wann und weshalb Verbindungsprobleme auftreten.
- **Effizienterer Helpdesk.** Geben Sie den Helpdesk-Mitarbeitern mehr Möglichkeiten an die Hand, z. B. Informationen über die Anwendung, die mobile Benutzer verwenden, und deren Versionsstand sowie über einen möglichen Akkuausfall. So können Sie sehen, wie häufig Anwendungen ausgeführt werden, welche Übertragungsbandbreite sie nutzen und welche Anwendungen Leistungsprobleme verursachen können.
- **Warnmeldungen bei drohenden Problemen.** Nutzen Sie mehr als 30 Benachrichtigungsoptionen, oft mit anpassbaren Schwellenwerten, per E-Mail, SNMP oder syslog.
- **Performance-Nachweis und proaktive Planung.** Vergewissern Sie sich, dass Benutzer die mobilen Ressourcen sinnvoll nutzen, und informieren Sie sich, ob mehr Bandbreite oder eine bessere Netzabdeckung erforderlich sind.

Weitere Informationen:

www.netmotionwireless.com

Netzwerkzugangskontrolle

Durchsetzung von Richtlinien für mobile Gerätesicherheit und Compliance. Das Netzwerkzugangskontrollmodul (NAC) für die Steuerung des Netzwerkzugriffs gewährleistet, dass die Geräte von Mitarbeitern mit adäquaten Sicherheitsvorkehrungen ausgestattet sind, bevor der Verbindungsaufbau sowie der Zugriff auf Anwendungen und Daten gestattet wird.