



## Endpoint Security

*Check Point Endpoint Security is total endpoint protection for enterprises.*

# SecureClient Mobile

*Secure, uninterrupted remote access for mobile devices*

## YOUR CHALLENGE

Devices such as Windows Mobile-powered PDAs and smartphones are becoming valuable tools for organizations like yours. With more powerful features and access to multiple cellular and WiFi networks, your mobile workers can access email, essential business applications, and corporate resources from anywhere just as easily as if they were in the office.

As your workers become more mobile, protection from malware and hackers that can compromise devices and confidential data becomes more critical. Reliable and secure remote access presents unique challenges for mobile workers as they try to connect from unknown networks. VPN sessions can easily be interrupted as mobile workers roam across networks and move in and out of connectivity, requiring them to reauthenticate to keep from losing their work.

You need a trusted security solution that will protect your mobile workers and your networks so your business can stay connected and competitive. A solution designed for mobility that can deliver reliable, uninterrupted secure remote access to email, business applications, and critical resources is essential to enabling your users to roam while staying connected and productive, just as if they were in the office.

## OUR SOLUTION

SecureClient™ Mobile delivers secure, uninterrupted remote access to enterprise email, critical business applications, and resources protected by Check Point VPN-1® and Connectra™ gateways.

Combining a personal firewall, which protects your mobile devices and networks from malware and hackers, with an SSL-based VPN client (for easily traversing firewalls, proxies, and NAT devices) enables your mobile workers to securely connect from anywhere. As they roam across cellular and WiFi networks or connections are interrupted, mobility features like session

## PRODUCT DESCRIPTION

SecureClient™ Mobile delivers firewall protection and secure, uninterrupted remote access for mobile devices that connect to VPN-1® and Connectra™ for continuous protection and productivity.

## PRODUCT FEATURES

- VPN client for secure remote access from mobile devices
- Session continuation across interrupted connections
- Personal firewall, interface control, and data protection
- Centralized management through SmartCenter™ and Provider-1®
- Small footprint and intuitive client GUI
- Interoperable with Pointsec® Mobile device encryption

## PRODUCT BENEFITS

- Protects mobile devices from hackers and malware
- Securely connects mobile-device users to critical applications and resources
- Maintains VPN sessions when roaming across networks or connections
- Reduces and simplifies deployment, administration, and costs
- Minimizes effect on device resources and user experience



The NGX platform delivers a unified security architecture for Check Point.

continuation and credential caching eliminate the need to reauthenticate, delivering uninterrupted VPN connectivity transparent to the user. With an intuitive user interface and minimal effect on device resources, SecureClient Mobile delivers secure, uninterrupted remote access to enterprise networks for Windows Mobile devices.

Centralized management and policy control from SmartCenter™ and Provider-1®, the same NGX unified management platform used for perimeter, internal, Web, and endpoint protection, enables you to define and enforce a unified remote access policy that extends to road warriors, remote offices, business partners, and mobile users.

### **Secure, uninterrupted remote access for mobile devices**

SecureClient Mobile delivers secure, uninterrupted remote access to enterprise email, critical business applications, and resources protected by Check Point VPN-1 and Connectra gateways. With centralized management, silent updates, and automatic policy enforcement, SecureClient Mobile protects your mobile workers and networks so your business can stay connected and competitive.

### **Greater protection and security enforcement**

The SecureClient Mobile personal firewall protects your mobile devices from hackers, malware, and other threats and enforces your predefined security policies—automatically. Choose to allow/disallow encrypted data when connected or force all traffic through the gateway for complete control and inspection. You can even control granular device settings like ActiveSync connections to PCs, so devices and data stay confidential and follow corporate guidelines for meeting regulatory compliance.

### **Reliable, secure remote access from anywhere**

Unknown networks, firewalls, proxies, and NAT traversal can all create problems for your mobile workers, preventing them from connecting to critical applications and resources. That is why SecureClient Mobile uses a robust and flexible SSL-based VPN client to more easily traverse firewalls, NAT devices, and proxies, so your mobile workers can reliably connect to email, business applications, and critical resources—regardless of their locations.

### **Transparent, uninterrupted VPN connectivity**

Maintaining continuous VPN sessions can be difficult as your mobile workers roam across multiple cellular and WiFi networks and move in and out of connectivity. Requiring new sessions or authentication every time the connection changes quickly becomes disruptive and unusable, resulting in lost data and productivity. SecureClient Mobile solves these problems by using session continuation and credential caching to preserve the VPN session without reauthenticating—even while roaming across networks or changes in connectivity—to deliver continuous and transparent VPN connectivity to your mobile workers.

### **Reduced administration and simplified deployment**

Centralized management from Check Point SmartCenter or Provider-1 reduces your administration and costs by leveraging the same NGX unified management platform used for perimeter, internal, Web, and endpoint security. Your administrators can create custom MSI or CAB installation packages with preconfigured security settings, simplifying and speeding deployment while immediately enforcing your corporate policies. Once installed, your security policies can be silently updated and broadcast to your mobile devices over the air to ensure automatic protection and enforcement, transparent to your end users.

### **Designed with mobility in mind**

SecureClient Mobile was designed and built from the ground up for the specific needs of mobile devices. Its small footprint preserves valuable device resources while a simple and intuitive GUI minimizes user interruptions, silently protecting and keeping your mobile workers productive. Advanced mobile networking features enable applications to push data directly to mobile devices, such as Microsoft's Direct Push technology, for sending email, calendar, contacts, and tasks as soon as items arrive/change on the server and with the same familiarity as their desktop experience.

### **Open platform for interoperability**

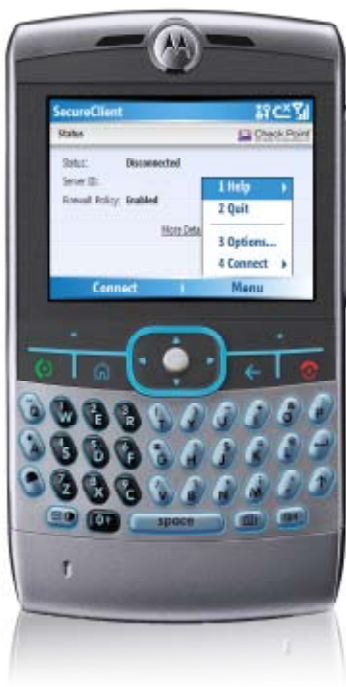
The Check Point open API enables OPSEC™ (Open Platform for Security) partners to easily integrate their solutions with SecureClient Mobile, providing extended security features such as antivirus, device encryption, and more. For a complete list of tested and verified solutions, see the OPSEC Web site at <http://www.opsec.com>.

### **Learn more**

Learn more about SecureClient Mobile and request an evaluation or sales quote from your local Check Point reseller, or visit us on the Web at [http://www.checkpoint.com/products/vpn-1\\_clients/sc\\_mobile.html](http://www.checkpoint.com/products/vpn-1_clients/sc_mobile.html).



SecureClient Mobile protects Windows Mobile devices and enforces corporate security using centralized management and policy control.



Designed specifically for mobile devices, SecureClient Mobile preserves device resources and worker productivity with a configurable GUI that minimizes disruptions.

## TECHNICAL SPECIFICATIONS

### Connectivity

- SSL-based VPN client connects to Check Point VPN-1 and Connectra gateways
  - Office Mode (assign IP address from the gateway)
  - Visitor Mode (tunnel all traffic through SSL Port 443)
  - Hub Mode (route all device traffic through gateway)
- Credential caching
- Multiple and alternate gateway support
- Secure Configuration Verification (SCV) and Endpoint Security On Demand Scanner (ICS)
- Connection status profiles
  - Always connected
  - Automatic disconnect
  - Initiate dialup

### Security

- Firewall protection
- ActiveSync control
- Allow unencrypted traffic when physically connected
- Encryption protocols: SSL 3DES, RC4
- Data integrity protocols: MD5, SHA-1
- Negotiation through SSL PKI server certificates with optional user authentication, including:
  - Client certificates (X.509, SmartCards, PKCS #12, etc.)
  - One-time password (RSA SecurID, SoftID, etc.)
  - User/password combinations and multi-challenge response
  - LDAP, AD RADIUS, TACCAS, and others
- Secure Authentication (SAA) OPSEC interface allows third party-extensions such as three-factor or biometric authentication

### Management

- Centralized management and policy control through SmartCenter or Provider-1
- Customized installation CAB files or MSI packages with preconfigured settings
- Automatic policy update upon connection or schedule
- Version updates broadcast over the air
- Advanced troubleshooting access

### Platform

- Small installation footprint
- Simple and intuitive client GUI
- Configurable startup, user control, and GUI notifications

**Operating systems**

- Windows Mobile 6.0 Pocket PC
- Windows Mobile 6.0 Smartphone
- Windows Mobile 5.0 Pocket PC
- Windows Mobile 5.0 Smartphone
- Windows Mobile 2003, Pocket PC

**Hardware**

- Intel ARMMv4, StrongARM, XScale, PXA Series processor
- Texas Instruments OMAP processor
- 64MB memory

**About Check Point Software**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is the leader in securing the Internet. Check Point offers total security solutions featuring a unified gateway, single endpoint agent, and single management architecture, customized to fit customers' dynamic business needs. We are unique in this offering as a result of our leadership and innovation in the enterprise firewall, personal firewall/endpoint, data security, and VPN markets. The pure focus of Check Point is on information security. Through its NGX platform, Check Point delivers a unified security architecture to protect business communications and resources, including corporate networks and applications, remote employees, branch offices, and partner extranets. The company also offers market-leading endpoint and data security solutions with Check Point Endpoint Security products, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point award-winning ZoneAlarm solutions protect millions of consumer PCs from hackers, spyware, and identity theft. Check Point solutions are sold, integrated, and serviced by a network of Check Point partners around the world, and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.



**CONTACT CHECK POINT**

**Worldwide Headquarters**

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)

**U.S. Headquarters**

800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | [www.checkpoint.com](http://www.checkpoint.com)

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.