



Simple and Secure
Corporate Access
from **MOBILE
DEVICES**

PRODUCT DESCRIPTION

Check Point Mobile Access Software Blade is the safe and easy solution to connect to corporate applications over the internet with your Smartphone or PC. The solution provides enterprise-grade remote access via SSL VPN, allowing you simple, safe and secure connectivity to your email, calendar, contacts and corporate applications.

Mobile Access Software Blade

YOUR CHALLENGE

Mobile devices are becoming an essential and standard business tool that can be owned by corporations or by employees. With the rise of IT consumerization, employees are increasingly using personal devices, primarily smart phones, laptops and tablets, to access corporate resources. The need for secure remote connectivity to corporate resources to maximize employee productivity while mitigating security risks is a major concern of Security Administrators.

OUR SOLUTION

Check Point Mobile Access Software Blade provides the most comprehensive solution to securely connect road warriors, teleworkers, contractors, and extranet partners to information they need, with the security and ease of management that Administrators demand. The solution offers multiple connectivity options for the remote worker while easing the pain of management for the Security Administrator.

Remote Access with Encrypted SSL VPN Technology

SSL VPN technology is used for secure encrypted communication from unmanaged mobile devices and PCs to your corporate IT infrastructure. Both web-based and network-level access through the SSL encryption can be delivered through most internet browsers.

Multiple end-user connection options include:

Check Point Mobile Client

Best for simple and secure connectivity to corporate resources from smartphones and PCs.

- One-touch access to your business web applications
- Secure sync of your e-mail, calendar and contacts
- Easy setup with downloadable app
- Secure business portal customized for each user ensuring access to only authorized corporate resources
- Single-sign-on reduces login errors into corporate web applications

PRODUCT FEATURES

Mobile Access Software Blade offers:

- Secure SSL VPN access
- Two-factor authentication
- Device/end-user pairing
- Mobile business Portal
- Works cooperatively with additional Gateway Software Blades including IPS, Anti-malware and Firewall

Multiple end-user connection options include:

- Check Point Mobile app
- SSL VPN Portal through a browser
- SSL Network Extender (SNX) with light-weight, dissolvable client

PRODUCT BENEFITS

Simply connect from mobile devices

- Secure connectivity for smartphones, tablets, PCs and laptops
- Provides client-based and web-based VPN connectivity
- Easy access for mobile workers using managed or unmanaged devices

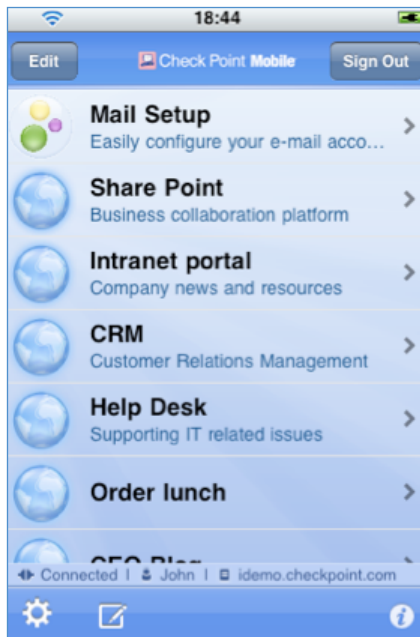
Keeps your data secure

- Communicate securely with proven encryption technology
- Verify authorized users with two-factor authentication
- Protect data on lost or stolen devices with device-lock and remote-wipe

Unified management for simple deployment and administration

- Fully integrated with Check Point Security Policy Manager
- Activate user-certificates with one click
- Deploy and configure the Mobile Access Software Blade on your existing Security Gateway





Check Point Mobile Client: One-tap secure access to corporate resources

SSL VPN Portal

Best for connecting securely to corporate resources through a portal from a web browser.

- **Secure Web-Based Connectivity**
Through an integrated web portal, users can access web applications, web-based resources, shared files, and email. Administrators can customize the design of the web portal, including support for multiple languages.
- **Endpoint Security On Demand** — optional endpoint compliance and malware scanner
 - Ensures that connecting endpoints are compliant with corporate policy
 - Detects keyloggers, trojans and other malware
 - Out-of-compliance users are offered links to self-remediation resources
- **Secure Workspace** — End-users can utilize Check Point's virtual desktop that enables data protection during user sessions, and enables cache wiping, after the sessions have ended. Secure Workspace protects all session-specific data accumulated on the client side
 - Creates a secure virtual environment, insulated from the host
 - Encrypts and deletes browser and application caches, files etc. when session ends

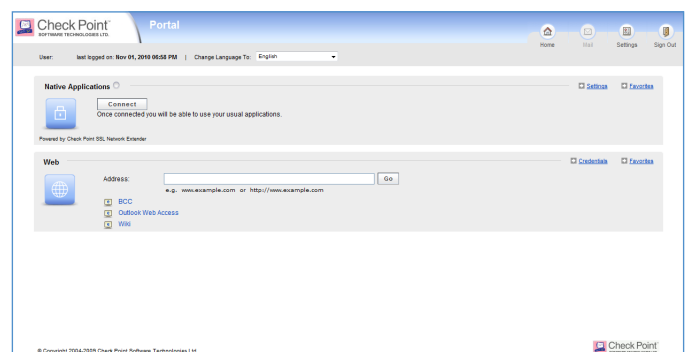
- **DynamicID™ Direct SMS Authentication**
The Mobile Access Software Blade can be configured to send a one-time password (OTP) to an end-user communication device (such as a mobile phone) via an SMS message. SMS two-factor authentication provides an extra level of security while eliminating the difficulties associated with managing hardware tokens.
- **Integrated Intrusion Prevention**
 - Provides protection against malicious code transferred in Web-related applications
 - Blocks worms, various attacks such as buffer overflows, SQL and command injections, cross-site scripting, customizable HTTP worm catcher, directory traversal, header rejection, malicious HTTP code

SSL Network Extender (On-demand Client)

Best for secure connectivity to corporate resources using non-web-based applications via an on-demand, dissolvable client.

The SSL Network Extender (SNX) is used for remote users who need access to network (non-web-based) applications. The SSL Network Extender offers a browser plug-in that provides remote access, while delivering full network connectivity for IP-based applications. It enables an on-demand SSL VPN Layer-3 tunnel to connect to your corporate resources. It supports IP-based applications, including ICMP, TCP, and UDP, without requiring complex configuration to support each application. SSL Network Extender works on remote PCs without requiring administrator privileges.

SSL Network Extender is downloaded automatically from the SSL VPN portal to the endpoint machines, so that client software does not have to be pre-installed and configured on users' PCs and laptops. SSL Network Extender tunnels application traffic using a secure, encrypted and authenticated SSL tunnel to the SSL VPN gateway.



SSL VPN Portal: Customizable browser portal securely accesses corporate web and non-web based applications



CHECK POINT MOBILE CLIENT SPECIFICATIONS

Device	Operating System
iPhone 3G, 3GS	3.1.3 and above
iPhone 4	4/4.01 and above
iPad	3.2.2 and above
Android	2.1 and up
Windows	XP, Vista, Windows 7 - Coming soon
Symbian	Available through SecureClient Mobile
Windows Mobile	Available through SecureClient Mobile

SSL VPN PORTAL SPECIFICATIONS

Browser	Version
Internet Explorer	5.5 and above
Firefox	1.0.3 and above
Safari	All

SSL NETWORK EXTENDER (ON-DEMAND CLIENT - SNX) SPECIFICATIONS

Client Device	Operating System	Browser
PC	Windows 7 32/64-bit, Vista 32/64-bit, XP 32-bit	Internet Explorer 5.5 and above, Firefox 1.0.3 and above
Mac	Mac 10.4 and above	Safari
Linux	Fedora 8, Ubuntu 7, RHEL 3.0, Suse 9 & above, Red Hat 7.3	Firefox 1.0.3 and above

GATEWAY SPECIFICATIONS

Hardware	Suitable for R71.10 such as UTM-1, Power-1 and IAS
Operating System	SecurePlatform
Version	R71.10+iPhone HFA

MANAGEMENT PLATFORM SPECIFICATIONS

(Security Management Server R71.10 required)

Platform	Operating System
Check Point	Secure Platform
Check Point	IPSO 6.2 Disk-Based
Windows	Server 2003/2008- 32-bit
Linux	RHEL 5.0/5.4 32-bit
Sun/Oracle (SPARC)	Solaris 8, 9, 10

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

U.S. Headquarters

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