DATA SHEETS

CHECK POINT
YOU DESERVE THE BEST SECURITY

CHECK POINT MOBILE ACCESS

Remote work is the new norm. Efforts to slow the spread of COVID-19 accelerated the transition of employees working from home and accessing corporate resources securely through various VPN (Virtual Private Network) technologies. In a recent Gartner CFO survey [1], 74% of companies said they intend to shift employees to work from home permanently.

Check Point Mobile Access is the safe and easy solution to securely connect to corporate applications over the Internet with your Smartphone, tablet or personal computer (PC). Mobile Access allows remote and mobile workers to simply and securely connect to email, calendar, contacts and corporate applications. Because it's fully integrated into the Check Point network security suite, administrators can easily set policy and monitor remote user's use of corporate assets.

Simple and Secure Corporate Access from Mobile Devices

FLEXIBLE

Easy access for mobile workers – secure connectivity for smartphones, tablets, PCs and laptops

SECURE

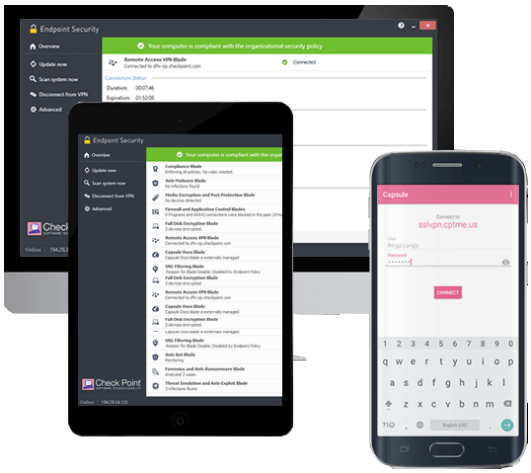
Communicate securely with proven encryption technology, and multi-factor authentication

UNIFIED

Deploy and manage on your existing security gateways from one unified console

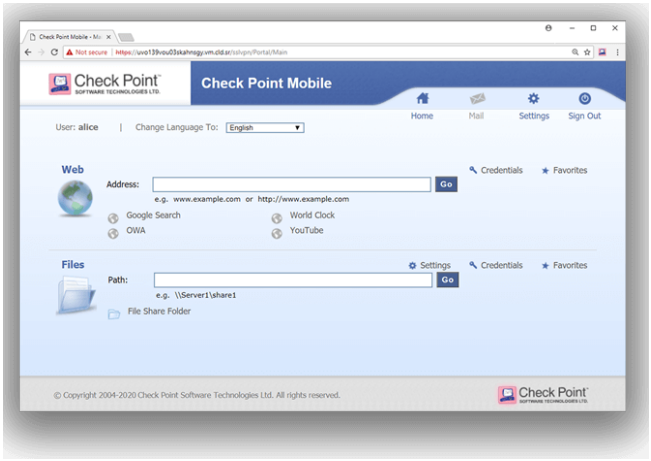
Full Layer-3 VPN Technology using a Client

IPsec VPNs authenticate and encrypt every communication session. Layer-3 VPN technology is highly scalable and allows flexible any-to-any connectivity.



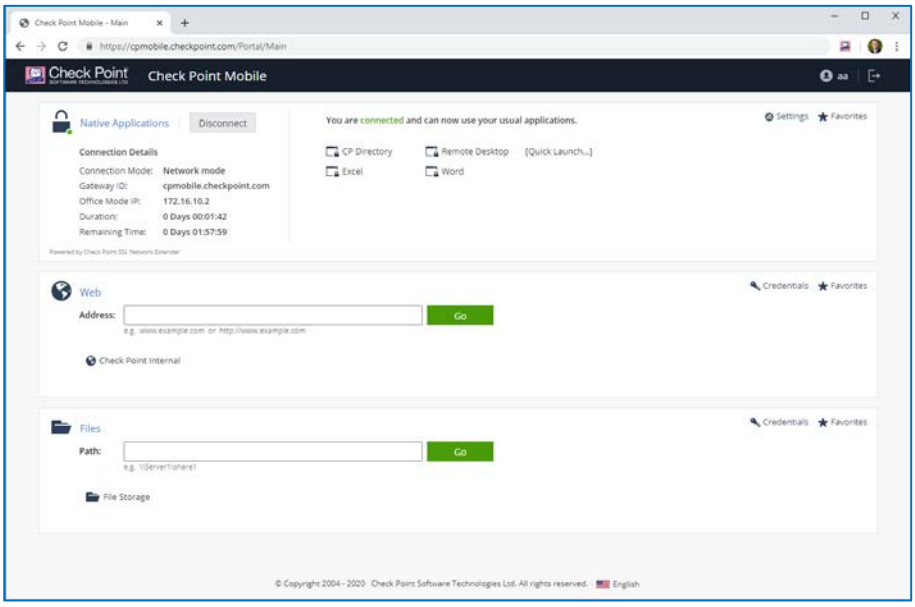
Encrypted SSL/TLS VPN using a Browser

Encrypt communications from unmanaged mobile devices. Both web-based and network-level access through SSL/TLS encryption is delivered through a browser.



SPOTLIGHT ON THE WEB PORTAL

The Web Portal is best for connecting securely to corporate resources from a web browser. Through an integrated web portal, users can access native corporate applications including web-based resources, shared file and email. Administrators can customize the design of the web portal to match their corporate brand identity. Mobile Access offers secure SSL/TLS VPN transport, strong multi-factor authentication and Role-based Access Control (RBAC).



Connect from Everywhere - Web, Mobile and Desktop

DynamicID™ Direct SMS Authentication
Mobile Access can be configured to send a One-Time Password (OTP) to an end-user 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.

Compliance Scanner
An endpoint compliance scanner ensures that connecting endpoints are compliant with corporate policy. Out-of-compliance users are offered links to self-remediation resources. Enforce your corporate compliance policy for Windows, macOS and Linux endpoints.

SSL Network Extender (SNX, an 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. 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. SNX delivers full network connectivity for IP-based applications including a 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. SNX Application Mode works without requiring administrative privileges and establishes a VPN tunnel for the specified applications.

Secure Workspace
End-users can utilize the Check Point 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 and creates a secure virtual environment insulated from the host. Browser and application caches, files, etc. are encrypted and then deleted when session ends.

CHECK POINT
YOU DESERVE THE BEST SECURITY

SPOTLIGHT ON CLIENTS

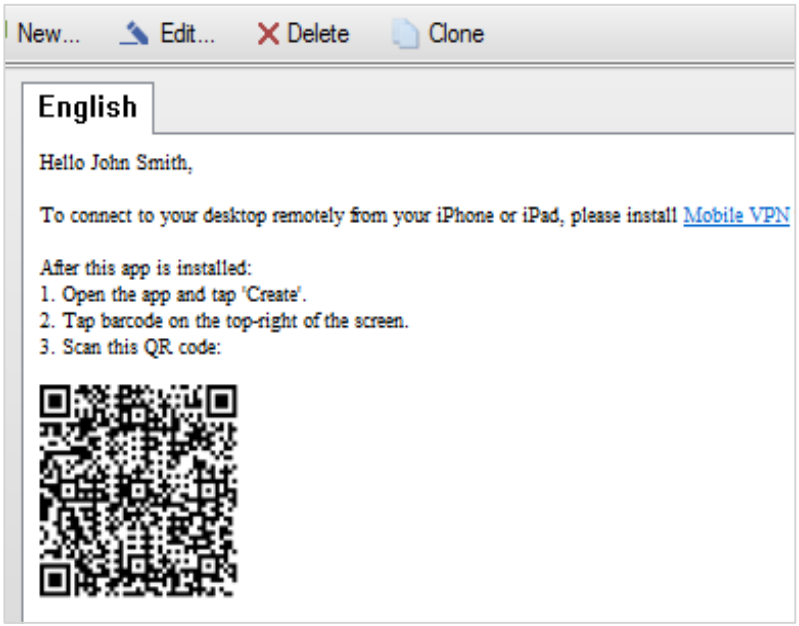
Check Point Capsule VPN (for Windows 10, 8.1)
Securely Access all your corporate resources from your device through a Virtual Private Network (VPN) tunnel. As you launch business applications such as RDP, VoIP or any other app on your mobile device, all transmitted data to corporate is encrypted, without any additional actions required by you.

Check Point Capsule Connect and Capsule VPN (for iOS and Android)
Check Point Connect for iOS and Capsule VPN for Android are simple client-to-site VPN clients available on mobile devices. Simply set up the site and connections to assets protected by the site gateway are secured by an IPsec or SSL VPN.

Check Point Capsule Workspace (for iOS and Android)
Check Point Capsule Workspace is a mobile security container on iOS and Android devices that creates an isolated corporate workspace on personal devices, making it simple to secure corporate data and assets both inside and outside the corporate network. Check Point Capsule Workspace protects and manages enterprise apps and data without needing to manage Mobile Device Management (MDM) profiles. So no matter which team is responsible for supporting smartphones and tablets, they'll value how Capsule Workspace secures mobile environments with ease – including BYOD.

Capsule Workspace is easy to deploy and manage, helping to reduce the time, effort, and cost of keeping mobile devices and data secure. Once deployed, it creates an AES256-bit encrypted container for enterprise apps and data that puts you in control of the sensitive enterprise information you need to protect. It never touches the personal apps, media, or content, on a device which helps improve end user adoption, even on personally-owned devices. Users will also appreciate the native experience and one-touch access Capsule Workspace provides to the critical enterprise apps they need to stay in touch on the go. It supports Microsoft Exchange Server and Office 365 email, calendar, and contacts, and includes secure enterprise instant messaging and document access.

Rapid and Flexible Deployment
With SmartConsole, companies can email users at their leisure with information on how to download the Mobile client directly to users' smartphones. Multiple ways to distribute notice of a Mobile client are available as well as choosing what Mobile client will be available for users using customized emails.



Endpoint VPN Clients (for Windows and macOS)
Mobile Access is part of our larger remote access solution. For additional endpoint protection, install our endpoint VPN client with or without the full Endpoint Security suite. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data. The VPN client has the ability to transparently establish a VPN tunnel upon demand when accessing corporate resources. The connection is re-established when roaming between networks and automatically tears down the VPN tunnel when the device is connected to the local corporate network.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com