Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point E80.89
For more about this release, see the E80.89 home page http://supportcontent.checkpoint.com/solutions?id=sk131152.

More Information

Latest Version of this Document
Open the latest version of this document in a Web browser.

Download the latest version of this document in PDF format http://supportcontent.checkpoint.com/documentation_download?ID=76005.
To learn more, visit the Check Point Support Center https://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security VPN for Mac E80.89 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 December 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
## Contents

- Important Information ................................................................................................... 3
- Introduction ................................................................................................................... 5
- What’s New ................................................................................................................... 5
- Upgrading Your Mac OS ................................................................................................. 5
- Migrating from SecureClient .......................................................................................... 5
- Remote Access Clients Comparison ............................................................................. 6
- Supported Upgrade Paths to E80.89 Mac ..................................................................... 8
- Client Requirements ..................................................................................................... 9
- VPN Server and Gateway Requirements ....................................................................... 9
- Installation and Configuration ....................................................................................... 9
- Installing the Client .................................................................................................... 9
- Uninstalling the Client .................................................................................................. 10
- Automatic Upgrade from the Gateway .......................................................................... 10
Introduction

Check Point offers multiple enterprise-grade VPN clients to fit a wide variety of organizational needs. The Remote Access VPN stand-alone clients provide a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel, and are managed in SmartDashboard.

See Remote Access Clients Comparison (on page 6) for a detailed feature comparison of different E80.89 clients.

What's New

This release includes stability and quality fixes. It supports all the features of previous releases.

New Features

- Support for the Endpoint Security VPN Client on macOS Mojave (10.14).
- Full support for macOS 64-bit.

Enhancement

- Opens the default browser of the machine to register to hotspot.

Upgrading Your Mac OS

macOS 10.14 (Mojave) can only work with E80.89 clients. Therefore you must upgrade the Endpoint Security VPN client to this version before you can upgrade the operating system.

To upgrade an Endpoint Security VPN client computer:
1. Upgrade the Endpoint Security VPN client to E80.89.
2. Upgrade the operating system to macOS 10.14 (Mojave).

Migrating from SecureClient

Endpoint Security VPN for Mac is not compatible with SecureClient for Mac. You must uninstall SecureClient before you install Endpoint Security VPN.
## Remote Access Clients Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Endpoint Security VPN for Windows</th>
<th>Check Point Mobile for Windows</th>
<th>Secu-Remote</th>
<th>Endpoint Security VPN for Mac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Purpose</td>
<td>Secure connectivity with desktop firewall &amp; compliance checks</td>
<td>Secure connectivity &amp; compliance checks</td>
<td>Basic secure connectivity</td>
<td>Secure connectivity with desktop firewall</td>
<td></td>
</tr>
<tr>
<td>Replaces Client</td>
<td>Secure-Client NGX R60 Endpoint Connect R73</td>
<td>Endpoint Connect R73</td>
<td>SecuRemote NGX R60</td>
<td>Secure-Client for Mac</td>
<td></td>
</tr>
<tr>
<td>IPSEC VPN Tunnel</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>All traffic travels through a secure VPN tunnel.</td>
</tr>
<tr>
<td>Security Compliance Check (SCV)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Monitor remote computers to confirm that the configuration complies with organization’s security policy.</td>
</tr>
<tr>
<td>Integrated Desktop Firewall</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Integrated endpoint firewall centrally managed from a Security Management Server</td>
</tr>
<tr>
<td>Split Tunneling</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Encrypt only traffic targeted to the VPN tunnel.</td>
</tr>
<tr>
<td>Hub Mode</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Pass all connections through the gateway.</td>
</tr>
<tr>
<td>Dynamic Optimization of Connection Method</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>When NAT-T connectivity is not possible, automatically connect over TCP port 443 (HTTPS port).</td>
</tr>
<tr>
<td>Multi Entry Point (MEP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Manual only: Client seamlessly connects to an alternative site when the primary site is not available.</td>
</tr>
<tr>
<td>Feature</td>
<td>Endpoint Security VPN for Windows</td>
<td>Check Point Mobile for Windows</td>
<td>Secu-Remote</td>
<td>Endpoint Security VPN for Mac</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------</td>
<td>-------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secondary Connect</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>End-users can connect once and get transparent access to resources, regardless of their location.</td>
</tr>
<tr>
<td>Office Mode IP</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>Each VPN client is assigned an IP from the internal office network.</td>
</tr>
<tr>
<td>Back Connection Protocols</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>Support protocols where the client sends its IP to the server and the server initiates a connection back to the client using the IP it receives. These protocols include: Active FTP, X11, some VoIP protocols.</td>
</tr>
<tr>
<td>Auto Connect and Location Awareness</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>Intelligently detect if the user is outside the internal office network, and automatically connect as required. If the client senses that it is inside the internal network, the VPN connection is terminated.</td>
</tr>
<tr>
<td>Roaming</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>Tunnel and connections remain active while roaming between networks.</td>
</tr>
<tr>
<td>Always Connected</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>VPN connection is established whenever the client exits the internal network.</td>
</tr>
<tr>
<td>Exclude Local Network</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>Exclude local network traffic when Hub mode (Route all traffic) is configured.</td>
</tr>
<tr>
<td>Secure Domain Logon (SDL)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>VPN tunnel and domain connectivity is established as part of Windows login allowing GPO and install scripts to execute on remote machines.</td>
</tr>
<tr>
<td>Feature</td>
<td>Endpoint Security VPN for Windows</td>
<td>Check Point Mobile for Windows</td>
<td>Secu-Remote</td>
<td>Endpoint Security VPN for Mac</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>-------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Split DNS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>Support for multiple DNS servers - a regular DNS server for resolving the external resources; an internal company DNS server assigned by the Office Mode for resolving the internal company resources.</td>
</tr>
<tr>
<td>Hotspot Detection and Registration</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>Detection only</td>
<td>Makes it easier for users to find and register with hot spots to connect to the VPN through local portals (such as in hotels or airports).</td>
</tr>
<tr>
<td>Secure Authentication API (SAA)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Allows third party extensions to the standard authentication schemes. This includes 3 factor and biometrics authentication.</td>
</tr>
<tr>
<td>Required Licenses</td>
<td>On Gateway: IPsec VPN On Management: Endpoint Container &amp; Endpoint VPN for all installed endpoints</td>
<td>IPsec VPN and Mobile Access (based on concurrent connections)</td>
<td>On Gateway: IPsec VPN for an unlimited number of connections</td>
<td>On Gateway: IPsec VPN On Management: Endpoint Container &amp; Endpoint VPN for all installed endpoints</td>
<td></td>
</tr>
</tbody>
</table>

**Supported Upgrade Paths to E80.89 Mac**

- E80.64
- E80.71
Client Requirements

E80.89 Endpoint Security Mac clients are compatible with these Mac platforms:

- macOS Mojave (10.14)
- macOS High Sierra (10.13)

Supported OS upgrades to Endpoint Security VPN from:

- macOS High Sierra (10.13)
- macOS Sierra (10.12)

VPN Server and Gateway Requirements

<table>
<thead>
<tr>
<th>E80.89 Client Type</th>
<th>Supported Security Management Server</th>
<th>Supported VPN Gateway</th>
</tr>
</thead>
</table>
| Endpoint Security Suite with Remote Access VPN Blade | R77.30.03  
R77.20 EP6.0 | R80 and higher  
R77 and higher |
| Standalone Endpoint Security VPN for OS X | R80 and higher  
R77 and higher | |

For the most up-to-date list of supported operating systems, server and gateway requirements, see: sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820.

Installation and Configuration

Before you install this release, make sure that you have supported gateways.

If Visitor mode is configured on port 443 and WebUI is enabled on the Security Gateway, the WebUI must listen on a port other than 443. Otherwise, Endpoint Security VPN cannot connect.

Installing the Client

Install the client on a supported Mac platform booted in 64-bit mode.

To install Endpoint Security VPN for Mac on a client computer:

1. Download the **Endpoint Security VPN for Mac E80.89 - Disc Image** file to the client computer.
2. Double-click the file.
   After the disk image mounts to the file system, a **Finder** window opens with the contents of the package.
3. Double-click the **Endpoint_Security_VPN.dmg** file to start the installation.
4. Follow the on-screen instructions.
Uninstalling the Client

If necessary, you can uninstall the Endpoint Security VPN client.

To install Endpoint Security VPN for Mac from a client computer:

1. Double-click the **Endpoint_Security_VPN.dmg** file.
   After the disk image mounts to the file system, a **Finder** window opens with the contents of the package.
2. Double-click the **Uninstaller** to start the uninstall process.
3. Do the on-screen instructions.

Automatic Upgrade from the Gateway

You can configure your Security Gateway to automatically upgrade Remote Access VPN clients the next time that they connect. When this occurs, the Security Gateway downloads the applicable package to the client. Endpoint users must have administrator permissions to install an upgrade.

You can have packages for different versions of the VPN client for Windows and Mac OS X on your Security Gateway at the same time. For example, you can have E80.60 for Mac and E80.62 for Windows at the same time.

To set up a gateway to automatically install client upgrades:

1. Download **Endpoint Security VPN for Mac E80.89 Signature for Automatic Upgrade**.
2. Rename the **Endpoint_Security_VPN.pkg**, **Endpoint_Security_VPN.pkg.signature** and **ver.ini** files to **TRAC.pkg**, **TRAC.pkg.signature** and **trac_ver_osx.txt** respectively.
3. Upload these files to this directory on the gateway:
   `$FWDIR/conf/extender/CSHELL`
   - For version R71.x only, copy the **TRAC.pkg** and **TRAC.pkg.signature** files also to:
     `$CVPNDIR/htdocs/SNX/CSHELL`.
4. On a non-Windows gateway, run:
   - `chmod 750 TRAC.pkg`
   - `chmod 750 TRAC.pkg.signature`
   - `chmod 750 trac_ver_osx.txt`
5. In SmartDashboard, go to **Policy > Global Properties > Remote Access > Endpoint Connect**.
6. Select one of these **Client upgrade mode** options:
   - **Do not upgrade** - This option disables automatic upgrades from the gateway. Automatic upgrades are not available for endpoint users.
   - **Ask user** - The user receives a prompt and can install immediately or at a later time.
     If the user does not install the upgrade immediately, the prompt will show again in one week.
   - **Always upgrade** - The new package installs silently without user intervention. The user receives a notification once the upgrade completes successfully.
7. Install the policy.