Remote Access Clients for Windows

E80.65

Release Notes
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.

**Check Point E80.65**
For more about this release, see the home page

**Latest Version of this Document**
Download the latest version of this document
To learn more, visit the Check Point Support Center

**Feedback**
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 February 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
Introduction ................................................................................................................... 5
What’s New ................................................................................................................... 5
Remote Access Clients Comparison ............................................................................. 6
Remote Access Client Upgrades ................................................................................... 9
Build Number ................................................................................................................ 9
Client Requirements ..................................................................................................... 9
Security Management Server and Security Gateway Requirements ........................... 10
Additional Requirements ............................................................................................ 10
Remote Access Client Installation for Windows .......................................................... 10
Upgrading SmartDashboard-Managed Clients .............................................................. 11
Known Limitations ....................................................................................................... 12
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 all SmartDashboard-managed.

These are the stand-alone clients offered in this release:

- **Endpoint Security VPN** - Incorporates Remote Access VPN with Desktop Security in a single client. It is recommended for managed endpoints that require a simple and transparent remote access experience together with desktop firewall rules.

- **Check Point Mobile for Windows** - An easy to use IPsec VPN client to connect securely to corporate resources. Together with the Capsule Workspace clients for iPhone and Android, and the Check Point SSL VPN portal, this client offers a simple experience that is primarily targeted for non-managed machines.

- **SecuRemote** - A secure, yet limited-function IPsec VPN client, primarily targeted for small organizations that require very few remote access clients.


We recommend that you read this document before installing E80.65 Remote Access clients.

What's New

New in this release:

- Multiple Login Options support
- Dynamic ID support

E80.65 Remote Access VPN clients have the ability to connect to an IPsec VPN gateway that is configured with Multiple Login Options.

One of the authentication factors can be **Dynamic ID** - Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a Dynamic ID One Time Password (OTP). The OTP is sent by text message or email.

The new support requires an R80.10 or higher IPsec VPN gateway.
## 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</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>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>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>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>
</tbody>
</table>
### 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>Secure Domain Logon (SDL)</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</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>Split DNS</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>Resolves internal names with the SecuRemote DNS Server configuration.</td>
</tr>
<tr>
<td>Hotspot Detection and Registration</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>Detection only 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>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
<td>Allows third party-extensions to the standard authentication schemes. This includes 3-factor and biometrics authentication.</td>
</tr>
</tbody>
</table>

### Required Licenses

- **On Gateway:** IPsec VPN Blade
- **On Management:** Endpoint Container & Endpoint VPN Blade for all installed endpoints

- **IPsec VPN Blade and Mobile Access Blade (based on concurrent connections)**

- **On Gateway:** IPsec VPN Blade for an unlimited number of connections

- **On Gateway:** IPsec VPN Blade
- **On Management:** Endpoint Container & Endpoint VPN Blade for all installed endpoints
Remote Access Client Upgrades

These upgrade paths are available for Remote Access VPN clients:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Connect E75.x or E80.x Remote Access Clients, SmartDashboard-managed clients</td>
<td>E80.65 SmartDashboard-managed Remote Access VPN</td>
<td>See Upgrading SmartDashboard-Managed Clients (on page 11)</td>
</tr>
</tbody>
</table>

- SmartEndpoint-managed Remote Access VPN clients are part of the Endpoint Security Suite.
- SmartDashboard-managed Remote Access VPN clients are standalone, without the Endpoint Security Suite.


Build Number

The build number for this release is: **986000810**

Client Requirements

Remote Access Clients E80.65 can be installed on these Windows platforms:

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 1511) 10 (version 1607)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>8.1</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>Update 1</td>
<td>All</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise Professional</td>
<td>32/64-bit</td>
<td>SP1 Microsoft update KB3033929</td>
<td>All</td>
</tr>
</tbody>
</table>
Security Management Server and Security Gateway Requirements

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

Additional Requirements

- To enable Secondary Connect, see the requirements in sk65312 http://supportcontent.checkpoint.com/solutions?id=sk65312.
- The Security Management Server and Security Gateway can be installed on open servers or appliances. On UTM-1 appliances, you cannot use the WebUI to install Remote Access Clients.
- Remote Access Clients cannot be installed on the same device as Check Point Endpoint Security R73 or R80. If ZoneAlarm is installed on a device, you can install Check Point Mobile for Windows and SecuRemote but not Endpoint Security VPN.

Remote Access Client Installation for Windows

You can create packages of the Remote Access Clients with pre-defined settings, such as which client to install, a VPN site and authentication methods. When you deploy the package to users, it is easier for them to connect quickly.

See the Remote Access Clients E80.60 Administration Guide for how to create deployment packages.

To install a Remote Access client:

2. Double-click the MSI and follow the on-screen instructions.
Upgrading SmartDashboard-Managed Clients

Get all files from the Endpoint Security Client E80.65 homepage [http://supportcontent.checkpoint.com/solutions?id=sk115512].

To automatically update clients to this release of Remote Access Clients or a future release, upgrade the client package on the gateway. Then all clients receive the new package when they next connect.

If you have a gateway version that requires the Remote Access Clients Hotfix, make sure that the Hotfix is installed before you put an upgraded package on the gateway.

There are two packages: one for ATM installation and one for non-ATM installation.

Each package has:
- TRAC_ATM.cab or TRAC.cab
- ver.ini
- CheckPointEndpointSecurityForATM.msi (packaged in the cab file)
- CheckPointVPN.msi

If you have R71.x with SSL VPN enabled, put the TRAC.cab file in a different directory, as shown in the instructions.

Users must have administrator privileges to install an upgrade with an MSI package. Administrative privileges are not required for automatic upgrades from the gateway.

Unattended (ATM) Clients

You cannot upgrade regular Remote Access Clients and unattended (ATM) Endpoint Security VPN clients from the same gateway.

**Important** - If you download the Automatic Upgrade for ATM file, you get a file called TRAC_ATM.cab. You must rename it to TRAC.cab before you put it on the gateway.

To distribute the Remote Access Clients from the gateway:

1. On the gateway, in the $FWDIR/conf/extender/CSHELL directory, back up the TRAC.cab and trac_ver.txt files.
   For R71.x, back up the TRAC.cab file in: $CVPNDIR/htdocs/SNX/CSHELL
2. Download the Remote Access Clients E80.65 Automatic Upgrade file from the sk homepage.
3. Put the new TRAC.cab and ver.ini files in the same directory on the gateway:
   $FWDIR/conf/extender/CSHELL
   For R71.x, put the TRAC.cab file also in: $CVPNDIR/htdocs/SNX/CSHELL
4. On a non-Windows gateway, run: chmod 750 TRAC.cab
5. Edit the trac_ver.txt file in the directory and change the version number to the number in the new ver.ini.
6. Make sure the client upgrade mode is set:
   a) Open the SmartDashboard.
   c) Set the Client upgrade mode to Ask user (to let user confirm upgrade) or Always upgrade (automatic upgrade).
   d) Click OK.

7. Install the policy.

When the client connects to the gateway, the user is prompted for an automatic upgrade of the newer version.
   - If users had Endpoint Security VPN R75, it keeps the existing settings.
   - If users had Endpoint Connect R73, it automatically upgrades to Endpoint Security VPN.

8. When the ATM client is installed with No Office Mode, those attributes will not change during upgrade. If the client is automatically upgraded, it is an ATM client with No Office Mode.

In this release you can distribute a customized package from the gateway. See Upgrading with a Customized Package in the Remote Access Clients Administration Guide.

Known Limitations

See sk115513 http://supportcontent.checkpoint.com/solutions?id=sk115513 for known limitations that apply to this release.