Remote Access Clients for Windows

E80.61

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 E80.61**
For more about this release, see the E80.61 home page (http://supportcontent.checkpoint.com/solutions?id=sk105123).

**Latest Version of this Document**
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=40524.
To learn more, visit the Check Point Support Center http://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 Remote Access Clients for Windows E80.61 Release Notes).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 July 2015</td>
<td>Updated build number for the release (&quot;Build Numbers&quot; on page 9)</td>
</tr>
<tr>
<td>31 March 2015</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 .......................................................................................................................... 8
Build Numbers ...................................................................................................................................................... 9
Remote Access VPN Requirements ...................................................................................................................... 9
  Security Management Server and Security Gateway Requirements ................................................................. 9
  Client Requirements ......................................................................................................................................... 9
  ATM Client Hardware Requirements .................................................................................................................. 10
Additional Requirements ...................................................................................................................................... 10
Configuring Password Complexity Requirements .............................................................................................. 10
Remote Access Client Installation for Windows .................................................................................................. 11
Upgrading SmartDashboard-Managed Clients ..................................................................................................... 11
Installing the Remote Access Clients Hotfix ...................................................................................................... 13
  Uninstalling this Hotfix .................................................................................................................................... 14
Known Limitations and Resolved Issues .............................................................................................................. 14
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.

See Remote Access Clients Comparison (on page 6) for a detailed feature comparison.

Endpoint Security VPN is also the Remote Access VPN client in the Endpoint Security Suite.

We recommend that you read this document before installing E80.61 Remote Access clients.

What's New

New in this release:

- Improved stability, and bug fixes.
- Configure password complexity requirements in the VPN Configuration Utility
## 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>SecuRemote</th>
<th>Endpoint Security VPN for Mac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Purpose</strong></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><strong>Replaces Client</strong></td>
<td>SecureClient NGX R60 Endpoint Connect R73</td>
<td>Endpoint Connect R73</td>
<td>SecuRemote NGX R60</td>
<td>SecureClient for Mac</td>
<td></td>
</tr>
<tr>
<td><strong>IPSEC VPN Tunnel</strong></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>All traffic travels through a secure VPN tunnel.</td>
</tr>
<tr>
<td><strong>Security Compliance Check (SCV)</strong></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><strong>Split Tunneling</strong></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>Encrypt only traffic targeted to the VPN tunnel.</td>
</tr>
<tr>
<td><strong>Hub Mode</strong></td>
<td>![ ]</td>
<td>![ ]</td>
<td></td>
<td>![ ]</td>
<td>Pass all connections through the gateway.</td>
</tr>
<tr>
<td><strong>Multi Entry Point (MEP)</strong></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>SecuRemote</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>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>Split DNS</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td>Resolves internal names with the SecuRemote DNS Server configuration.</td>
</tr>
<tr>
<td>Hotspot Detection and Registration</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></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>
</tbody>
</table>
## 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 R73.x, E75.x, or E80.x Remote Access Clients, SmartDashboard-managed</td>
<td>E80.61 SmartEndpoint-managed Remote Access VPN</td>
<td>Upgrading Endpoint Security Clients in Endpoint Security E80.61 Administration Guide (<a href="http://supportcontent.checkpoint.com/solutions?id=sk105123">http://supportcontent.checkpoint.com/solutions?id=sk105123</a>)</td>
</tr>
<tr>
<td>Endpoint Connect R73.x, E75.x, or E80.x Remote Access Clients, SmartDashboard-managed clients</td>
<td>E80.61 SmartDashboard-managed Remote Access VPN</td>
<td>See Upgrading SmartDashboard-Managed Clients (on page 11)</td>
</tr>
<tr>
<td>E80.4x or higher Endpoint Security suite with or without Remote Access VPN</td>
<td>E80.61 SmartEndpoint-managed Remote Access VPN</td>
<td>Upgrading Endpoint Security Clients in Endpoint Security E80.61 Administration Guide (<a href="http://supportcontent.checkpoint.com/solutions?id=sk105123">http://supportcontent.checkpoint.com/solutions?id=sk105123</a>)</td>
</tr>
</tbody>
</table>

- SmartEndpoint-managed Remote Access VPN clients are part of the Endpoint Security Suite.

### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Endpoint Security VPN for Windows</th>
<th>Check Point Mobile for Windows</th>
<th>SecuRemote</th>
<th>Endpoint Security VPN for Mac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### Required Licenses

|-------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|---|

Remote Access Client Upgrades
Build Numbers

The build number for this release is: **986000320**

Remote Access VPN Requirements

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](http://supportcontent.checkpoint.com/solutions?id=sk67820).

Remote Access VPN requires a supported gateway version. If you use Automatic MEP, the Security Management Server or Multi-Domain Server must also be supported, with the required hotfixes.

For Security Management Servers and gateways of versions earlier than R70.50, R71.50, or R75.40, you must install the Remote Access Hotfix.

Client Requirements

Remote Access Clients E80.61 can be installed on these Windows platforms:

<table>
<thead>
<tr>
<th>Windows Version</th>
<th>Editions</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 with or without Update 1</td>
<td>Enterprise, Pro</td>
<td>32/64 bit BIOS/UEFI</td>
</tr>
<tr>
<td>8</td>
<td>Enterprise, Pro</td>
<td>32/64 bit BIOS/UEFI</td>
</tr>
<tr>
<td>7</td>
<td>Enterprise, Professional, Ultimate, with or without SP1</td>
<td>32/64 bit</td>
</tr>
<tr>
<td>Vista</td>
<td>Enterprise, Professional, SP1 or higher</td>
<td>32/64 bit</td>
</tr>
<tr>
<td>XP</td>
<td>Professional, SP3</td>
<td>32-bit</td>
</tr>
</tbody>
</table>
ATM Client Hardware Requirements

These are the minimum hardware requirements for client computers that run the SmartDashboard-based Endpoint Security VPN ATM package.

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>256 MB RAM</td>
</tr>
<tr>
<td>Free disk space</td>
<td>500 MB</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel® Pentium® 4 CPU 3.20 GHz or equivalent</td>
</tr>
</tbody>
</table>

Additional Requirements

- To enable Secondary Connect, see the requirements in sk65312 http://supportcontent.checkpoint.com/solutions?id=sk65312.
- To enable automatic, implicit MEP (Multiple Entry Points), you must install the Remote Access Clients Hotfix on the Security Management Server and on all Security Gateways. This procedure is not necessary for manual MEP.
- 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.
- All Security Gateways used as primary MEP connections must support this release, with the Remote Access Clients Hotfix installed. NGX R65.70 Security Gateways must be managed by NGX R65.70 Security Management Servers. The servers must also have the Remote Access Clients Hotfix installed.

Configuring Password Complexity Requirements

Configure password complexity requirements in the trac.defaults file and add it to a package with the VPN Configuration Utility.

The parameters below are in the trac.defaults file. To require one or more of the parameters, change the value from 0 to the number of instances required in the password.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_P12_password_lower_case</td>
<td>Minimum number of lower case letters in the password</td>
</tr>
<tr>
<td>min_P12_password_upper_case</td>
<td>Minimum number of upper case letters in the password</td>
</tr>
<tr>
<td>min_P12_password_numbers</td>
<td>Minimum number of digits in the password</td>
</tr>
</tbody>
</table>
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 E80.61 homepage (http://supportcontent.checkpoint.com/solutions?id=sk105123).

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_P12_password_special_characters</td>
<td>Minimum number of special characters in the password. Characters can be: !, $, &amp;,, #, +, -, /, :, ;, &lt;, =, &gt;, ?, @, [, ], ^, _, ` {,</td>
</tr>
</tbody>
</table>

See the E80.60 Remote Access Clients Administration Guide for more information on the VPN Configuration Utility.
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 E80.61 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.
   b) Open **Policy > Global Properties > Remote Access > Endpoint Connect**.
   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 E80.61 *Remote Access Clients Administration Guide*. 
Installing the Remote Access Clients Hotfix

If you have R71.30 and higher or R75 and higher installed on a gateway, Security Management Server, or Multi-Domain Server, it can support Remote Access Clients. It is not necessary to install a Hotfix. See the System Requirements section of the Release Notes for exact details.

For earlier supported gateway versions, install the Hotfix http://supportcontent.checkpoint.com/solutions?id=sk67820.

Install the Remote Access Clients E80.61 Hotfix on gateways or standalone, self-managed gateway deployments. In a Multi-Domain Security Management environment install the Hotfix on the Multi-Domain Server.

Before you install the Hotfix:
This Hotfix has possible conflicts with other installed Hotfixes. If you can, it is safest to uninstall all Hotfixes installed on the Security Management Server or gateways. See Uninstalling a Hotfix ("Uninstalling this Hotfix" on page 14). If you cannot uninstall a Hotfix, contact Check Point Technical Support.

To install the Hotfix on a Security Gateway or Security Management Server:
1. Download the Hotfix.
3. Run the Hotfix:
   On SecurePlatform, Disk-based IPSO, and Solaris:
   a) tar -zxvf <name_of_file>.tgz
   b) ./UnixInstallScript
   On Windows platforms: double-click the installation file and follow the instructions.

To install the Hotfix on a Multi-Domain Server:
2. Download the Remote Access Clients Hotfix to the Multi-Domain Server.
3. Run the Hotfix on SecurePlatform and Solaris:
   a) tar -zxvf <name_of_file>.tgz
   b) ./UnixInstallScript
4. Follow the on-screen instructions.
5. Reboot the Multi-Domain Server.
Uninstalling this Hotfix

If you need to uninstall a Hotfix, use this procedure.

**To uninstall a Hotfix from a gateway:**

1. Go to the installation directory: `cd /opt/CPsuite-\*version*/`
   For example, the installation directory on an R70.40 gateway is: `/opt/CPsuite-R70/`
2. Run: `./uninstall_<name_of_original_Hotfix_file>`
   The name of the Hotfix is different for gateway version and for Hotfix functionality.
3. Enter `y` at the prompt.
4. Reboot the Security Gateway.

Known Limitations and Resolved Issues

For known limitations that apply to this release, see sk105124

For issues resolved in this release, see sk105125