27 September 2018

REMOTE ACCESS CLIENTS FOR WINDOWS E80.87

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 E80.87
For more about this release, see the E80.87 home page

Latest Version of this Document
Download the latest version of this document
http://supportcontent.checkpoint.com/documentation_download?ID=73163
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 E80.87 Release Notes

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 September 2018</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
Supported Client Operating Systems ............................................................................ 9
Security Management Server and Security Gateway Requirements ......................... 10
Additional Requirements ............................................................................................ 10
Remote Access Client Installation for Windows .......................................................... 10
Supported Upgrades for Remote Access client VPN Client for ATMs ......................... 10
Upgrading SmartDashboard-Managed Clients ............................................................... 11
Installing and Upgrading the VPN client on a Computer with Device Guard Enabled . 12
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.

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.

**Note** - Starting E80.8x, the Remote Access VPN client is not supported on a computer with the end-of-life Full Disk Encryption stand-alone client (R7.x or FDE 7.x). Installing or upgrading the Remote Access VPN client on a computer with the Full Disk Encryption stand-alone client may cause the computer to become non-functional.

We recommend that you read this document before installing E80.87 Remote Access clients.

What's New

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

**Enhancements**

- Resolves a Remote Access issue in a customized package of Endpoint Security Client full suite created with the VPN Configuration Utility. In previous releases, the original trac.defaults remains instead of the customized file.

- Resolves a possible issue when a “no network” message may occur when the client tries to connect to the VPN Security Gateway when there is connectivity.
## 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>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</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</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>IP</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>Back Connection Protocols</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>Auto Connect and Location</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>Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tunnel and connections remain active while roaming between networks.</td>
</tr>
<tr>
<td>Roaming</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>Always Connected</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>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>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>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>
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></td>
<td>E80.87 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.


Supported Client Operating Systems

<table>
<thead>
<tr>
<th>Version</th>
<th>Editions</th>
<th>Arch.</th>
<th>SPs or Updates</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (version 1803) 10 (version 1709) 10 (version 1703) 10 LTSB (version 1607)</td>
<td>Enterprise Pro</td>
<td>32/64-bit</td>
<td>All</td>
<td></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

Remote Access Clients cannot be installed on the same device as Check Point Endpoint Security R73 or E80. 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.

To learn how to create deployment packages, see the E80.72 Remote Access Clients Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=60345.

To install a Remote Access client:

2. Double-click the MSI and follow the on-screen instructions.

Supported Upgrades for Remote Access client VPN Client for ATMs

Upgrade to E80.87 Remote Access client VPN client for ATMs is available from:

- E80.64 Remote Access VPN client for ATMs
- E75.30 Remote Access VPN client for ATMs
Upgrading SmartDashboard-Managed Clients

Get all files from the Endpoint Security Client E80.87 homepage

You can distribute an upgrade of the Remote Access Clients from the Security Gateway, while the
user is connected to it, using the TRAC.cab file.

The installation is downloaded automatically from the gateway, and it installs automatically.

This is only for users who are upgrading from a previous version. You cannot edit the file before
you distribute it.

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.

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

Each package has these files:

- TRAC_ATM.cab or TRAC.cab
- ver.ini
- CheckPointEndpointSecurityForATM.msi [packaged in the cab file]
- CheckPointVPN.msi

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.

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**.

You can distribute a customized package from the gateway. See **Upgrading with a Customized
Package** in the *E80.72 and higher Remote Access clients Administration Guide*

For E80.86 and higher client there is an unattended client package for Endpoint Security clients.
To learn how to install and upgrade unattended Endpoint Security clients, see the *E80.86 and
higher Endpoint Security Client for ATMs Deployment Guide*
Installing and Upgrading the VPN client on a Computer with Device Guard Enabled

The Remote Access VPN client cannot be installed when Device Guard User Mode Code Integrity (also known as UMCI) is enabled.

To install, upgrade or uninstall the Remote Access client on a computer on which UMCI is Enforced:

1. Disable Device Guard user mode Code Integrity.
2. Install the client
3. Enable Device Guard user mode Code Integrity.

To learn how to disable and enable Device Guard user mode Code Integrity, see the Microsoft instructions https://docs.microsoft.com/en-us/windows/device-security/device-guard/deploy-code-integrity-policies-policy-rules-and-file-rules#code-integrity-policy-rules.

To deploy code integrity policies https://docs.microsoft.com/en-us/windows/device-security/device-guard/deploy-code-integrity-policies-steps, follow the steps that Microsoft provides. After changing the policy xml file, initiate a new bin file. There is no need to re-scan the system, so skip step 2. Use New-CIPolicy to create a new code integrity policy by scanning the system for installed applications. This is because the scan runs when Device Guard is deployed, so there is no need to scan again when you disable or enable UMCI.

Known Limitations

See the E80.87 home page http://supportcontent.checkpoint.com/solutions?id=sk135432 for known limitations that apply to this release.