HARMONY

09 March 2025

REMOTE ACCESS VPN CLIENTS FOR WINDOWS

E88.X

Release Notes

CHECK POINT™

Check Point Copyright Notice

© 2023 - 2025 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

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.

Check Point E88.x Remote Access VPN Clients for Windows Release Notes

For more about this release, see the Endpoint Security home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

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

Table of Contents

Introduction to E88.x Remote Access VPN Clients for Windows

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.

For a detailed feature comparison, see *"Comparison of Remote Access Clients" on page 8*.

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

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

We recommend that you read this document before you install Remote Access clients.

What's New

New Features and Enhancements

E88.63 (Standalone Client only) - Released on 04 March 2025
Remote Access VPN Standalone Client E88.62 was replaced with E88.63 due to an operational issue. Customers running Remote Access VPN Standalone Client E88.62 are advised to upgrade to E88.63.
E88.62 - Released on 10 February 2025
This Hotfix complements the E88.61 release with important fixes. If you installed E88.61, we recommend upgrading to E88.62.
E88.61 - Released on 01 December 2024
This Hotfix complements the E88.60 release with important fixes. If you installed E88.60, we recommend upgrading to E88.61.
E88.32 - Released on 17 July 2024
Enhancement: Added ability to centrally manage the browser for authentication using Identity Provider from the *trac_client_1.ttm* file. Refer to sk75221.
E88.32 - Released on 17 July 2024
This Hotfix complements the E88.31 release with important fixes.
E88.31 - Released on 03 June 2024
This Hotfix complements the E88.30 release with important fixes. If you installed E88.30, we recommend upgrading to E88.31.
E88.00 - Released on 22 January 2024
Enhancement: VPN blade of Endpoint Security now shows Office Mode IP as Client IP address in main client window for clients that support Office Mode.

Release Map

For Download packages, the complete list of New Features, Enhancements, Resolved issues and Known Limitations, see the dedicated SK article.

Version	SK article	Release Date
E88.70	sk182578	09 March 2025
E88.62	sk182996	10 February 2025
E88.61	sk182788	01 December 2024
E88.60	sk182468	03 September 2024
E88.50	sk182372	05 August 2024
E88.41	sk182237	23 June 2024
E88.32	sk182489	17 July 2024
E88.31	sk182277	03 June 2024
E88.30	sk182109	17 April 2024
E88.20	sk182044	13 March 2024
E88.10	sk181927	19 February 2024
E88.00	sk181675	22 January 2024

Comparison of Remote Access Clients

Feature	Endpoint Security VPN for Windows	Check Point Mobile for Windows	SecuRemote	Endpoint Security VPN for Mac	Description
Client Purpose	Secure connectivity with Desktop Firewall & compliance checks	Secure connectivity & compliance checks	Basic secure connectivity	Secure connectivity with Desktop Firewall	
Replaces Client	SecureClient NGX R60 Endpoint Connect R73	Endpoint Connect R73	SecuRemote NGX R60	SecureClient for Mac	
IPsec VPN Tunnel	✓	✓	✓	✓	All traffic travels through a secure VPN tunnel.
Security Compliance Check (SCV)	✓	✓	–	–	Monitor remote computers to confirm that the configuration complies with organization's security policy.
Integrated Desktop Firewall	✓	–	–	✓	Integrated endpoint firewall managed centrally from a Security Management Server
Split Tunneling	✓	✓	✓	✓	Encrypt only traffic targeted to the VPN tunnel.
Hub Mode	✓	✓	–	✓	Pass all connections through the Security Gateway.
Dynamic Optimization of Connection Method	✓	✓	✓	✓	When NAT-T connectivity is not possible, automatically connect over TCP port 443 (HTTPS port).
Multi Entry Point (MEP)	✓	✓	✓	✓ Manual only	Client seamlessly connects to an alternative site when the primary site is not available.

Feature	Endpoint Security VPN for Windows	Check Point Mobile for Windows	SecuRemote	Endpoint Security VPN for Mac	Description
Secondary Connect	✓	✓	✓	–	End-users can connect once and get transparent access to resources, regardless of their location.
Office Mode IP	✓	✓	–	✓	Each VPN client is assigned an IP from the internal office network.
Back Connection Protocols	✓	✓	–	✓	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.
Auto Connect and Location Awareness	✓	✓	–	–	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.
Roaming	✓	✓	–	✓	Tunnel and connections remain active while roaming between networks.
Always Connected	✓	✓	–	✓	VPN connection is established whenever the client exits the internal network.
Exclude Local Network	✓	✓	–	–	Exclude local network traffic when Hub mode (**Route all traffic**) is configured on the Security Gateway.
Secure Domain Logon (SDL)	✓	✓	✓	–	VPN tunnel and domain connectivity is established as part of Windows login allowing GPO and install scripts to execute on remote machines.

Feature	Endpoint Security VPN for Windows	Check Point Mobile for Windows	SecuRemote	Endpoint Security VPN for Mac	Description
Split DNS	✓	✓	✓	✓	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.
Hotspot Detection and Registration	✓	✓	–	✓ 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).
Secure Authentication API (SAA)	✓	✓	✓	–	Allows third party-extensions to the standard authentication schemes. This includes 3-factor and biometrics authentication.
Required Licenses	On Security Gateway: IPsec VPN On Management Server: Endpoint Container & Endpoint VPN for all installed endpoints	IPsec VPN and Mobile Access (based on concurrent connections)	On Security Gateway: IPsec VPN for an unlimited number of connections	On Security Gateway: IPsec VPN On Management Server: Endpoint Container & Endpoint VPN for all installed endpoints	

Remote Access VPN Client Upgrades

Supported Upgrade paths for Remote Access VPN clients

From	To	See
Endpoint Connect E75.x or E80.x Remote Access clients, SmartEndpoint-managed	Latest SmartEndpoint-managed Remote Access VPN	*Upgrading Endpoint Security Clients* in the *Harmony Endpoint Server Administration Guide* for your version
	Latest SmartDashboard-managed Remote Access VPN	See Upgrading SmartDashboard-managed Clients

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

For upgrades from SecureClient, see the *Upgrading from SecureClient to Remote Access VPN Clients Guide*.

Supported Client Operating Systems

Microsoft Windows

Version	Editions	Supported starting from
11 LTSC (version 24H2)	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 24H2	Enterprise Pro	Endpoint Security Client E88.41 VPN Standalone Client E88.40
11 23H2	Enterprise Pro	Endpoint Security Client E87.62 VPN Standalone Client E87.60
11 22H2	Enterprise Pro	Endpoint Security Client E86.70
11 21H2	Enterprise Pro	Endpoint Security Client E85.40
10 22H2	Enterprise Pro	EA support: Endpoint Security Client E86.80 GA support: Endpoint Security Client E87.00
10 LTSC (version 21H2)	Enterprise Pro	Endpoint Security Client E86.00
10 21H2	Enterprise Pro	Endpoint Security Client E86.00
10 21H1 (version 2103)	Enterprise Pro	Endpoint Security Client E85.00
10 20H2 (version 2009)	Enterprise Pro	Endpoint Security Client E85.00
10 20H1 (version 2004)	Enterprise Pro	Endpoint Security Client E85.00
10 19H2 (version 1909)	Enterprise Pro	Endpoint Security Client E85.00
10 19H1 (version 1903)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSC (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1809)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1803)	Enterprise Pro	Endpoint Security Client E85.00
10 (version 1709)	Enterprise Pro	Endpoint Security Client E85.00
10 LTSB (version 1607)	Enterprise Pro	Endpoint Security Client E85.00
8.1 Update 1	Enterprise Pro	Endpoint Security Client E85.00
7 SP1 Microsoft update KB3033929	Enterprise Professional	Endpoint Security Client E85.00

Notes:

- For existing Endpoint Security deployments, before upgrading your OS version, you must first upgrade the Endpoint Security Client to a version that supports the desired OS version based on the table above.
- For additional information on Windows 7 support, refer to sk164006.
- Windows Operating Systems are supported according to Check Point Client Support life cycles, also on Virtual Machines. However, there is no dedicated QA process for all possible variants of Windows. If you encounter a specific issue related to a different edition of a supported Windows OS version, Check Point will provide best-effort support through R&D assistance.

Microsoft Windows Server

Version	Editions	Supported starting from	Supported Features
2025 64-bit	All	E88.61	Anti-Bot and URL Filtering, Anti-Malware, Anti-Ransomware, Behavioral Guard and Forensics, Compliance and Posture, Firewall and Application Control, Media Encryption and Port Protection, Threat Emulation.
2022 64-bit	All	E85.40	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client), Media Encryption and Port Protection.
2019 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client), Media Encryption and Port Protection.
2016 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client).
2012 R2 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)
2012 64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)
2008 R2 32/64-bit	All	E85.00	Compliance, Anti-Malware, Firewall, Application Control, Forensics, Anti-Ransomware, Anti-Bot, Threat Emulation, Capsule Docs (Standalone Client)

Notes:

- To support Endpoint Compliance rules for Windows Server 2016 on versions older than R80.20, see sk122136.
- Windows Server CORE is not supported.
- If you install a client package with features that are not supported on the server, the installation succeeds but only the supported features are installed.
- The Anti-Exploit feature is supported starting from the 2016 64-bit version.

Security Management Server and Security Gateway Requirements

For the most up-to-date list of supported operating systems, Management Server and Security Gateway requirements, see sk67820.

Additional Requirements

You cannot install Remote Access clients on a device that has a 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.

Installation of Remote Access Clients 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 *Remote Access VPN Clients for Windows Administration Guide*.

To install a Remote Access client:

1. Download the `MSI` file from the **In a Nutshell** section of the latest Endpoint Security Clients for Windows release.

   See the *"Release Map" on page 7* section for the list of releases.

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

Supported Upgrades for Remote Access VPN Clients for ATMs

Upgrade of Remote Access VPN Clients for ATMs is available from:

- E80.64 Remote Access VPN Clients for ATMs.
- E75.30 Remote Access VPN Clients for ATMs.

Upgrading SmartDashboard-Managed Clients

Download all files from the Endpoint Security Clients for Windows release. See the *"Release Map" on page 7* section for the list of releases.

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 Security 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 Security 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 Security Gateway.

Unattended (ATM) Clients

You cannot upgrade regular Remote Access clients and unattended (ATM) Endpoint Security VPN clients from the same Security 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 Security 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 Security Gateway. See the *Remote Access VPN Clients for Windows Administration Guide* > Setting Up Remote Access clients > Automatic Upgrade from the Security Gateway > Upgrading with a Customized Package

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*.

To deploy code integrity polices, 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.