



Hybrid Mesh Network Security

03 September 2026

CYBER SECURITY PLATFORM

R82.10

Release Notes



Check Point Copyright Notice

© 2025 - 2026 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 R82.10

For more about this release, see the R82.10 [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](#).

Revision History

Date	Description
03 September 2026	Updated: ▪ "SmartEvent Requirements" on page 50
17 August 2026	Updated: ▪ "Desktop SmartConsole Software Requirements" on page 51
18 January 2026	Updated: ▪ "Threat Emulation Appliances" on page 27 ▪ "Disk Space Requirements for Open Server / Virtual Machine" on page 47
13 January 2026	Updated: ▪ "Maximum Supported Items in R82.10" on page 59
11 January 2026	Updated: ▪ "Upgrade Paths for Scalable Platforms" on page 32
08 January 2026	Updated: ▪ "Upgrade Paths for Scalable Platforms" on page 32
07 January 2026	Updated: ▪ "Security Gateway or Cluster" on page 24
29 December 2025	First release of this document

Table of Contents

Important Links	8
What's New in R82.10	9
Introduction	9
Threat Prevention	11
Threat Prevention Insights	11
Zero Phishing	11
ThreatCloud AI Engines	11
DNS Security	12
HTTPS Inspection	12
IPS	12
Security Gateway	13
Identity Awareness	13
URL Filtering	13
Site to Site VPN	13
SD-WAN	13
Security Gateway Enhancement	14
Dynamic Routing	14
Cluster and Scalability	14
Internal CA	14
Gaia OS Security	15
Security Management	16
Logging and Monitoring	16
Compliance	16
Cloud Firewall Security	16
CloudGuard Controller	16
Software Changes in R82.10	17
Gaia Operating System	17

Security Gateway	18
Scalable Platforms	20
Threat Prevention	20
Management Server	21
Supported Environments in R82.10	22
Management Server and Log Server	22
Security Gateway or Cluster	24
Standalone and Full High Availability	25
VSNext and Traditional VSX	26
Threat Emulation Appliances	27
Maestro	28
Virtualization Platforms	28
Cloud Platforms	29
Supported Upgrade Paths in R82.10	31
Upgrade Paths for Security Gateways, Management Servers, Log Servers, SmartEvent Servers, Standalone Servers	31
Upgrade Paths for Scalable Platforms	32
Supported Upgrade Methods in R82.10	34
Supported Security Gateway Versions in R82.10	43
Management Server and Security Gateway Versions	43
Maestro Orchestrator and Security Group Versions	44
Hardware Requirements for Open Server / Virtual Machine in R82.10	45
Minimum CPU and RAM Requirements for Open Server / Virtual Machine	46
Disk Space Requirements for Open Server / Virtual Machine	47
Maximum Supported Physical Memory on Open Server / Virtual Machine	48
Requirements in R82.10	49
Threat Extraction Requirements for Web-downloaded Documents	49
Logging Requirements	49
SmartEvent Requirements	50
SmartConsole Requirements	51

Desktop SmartConsole Hardware Requirements	51
Desktop SmartConsole Software Requirements	51
Gaia Portal Requirements	52
The Gaia Portal requirements on Security Gateways, Cluster Members, Management Servers, and Log Servers	52
The Gaia Portal requirements on Maestro Orchestrators	52
Mobile Access Requirements	53
Identity Awareness Requirements	55
Identity Clients	55
AD Query	55
Browser-Based Authentication (Captive Portal)	55
Endpoint Security Management Server Requirements	56
Hardware Requirements	56
Software Requirements	56
Anti-Malware Signature Updates	57
Scalable Platforms Requirements	58
Software Requirements	58
Supported Network Cards on Maestro Security Appliances	58
Maximum Supported Items in R82.10	59
Management Server	59
Sizing Recommendations for Check Point Management Server	63
Maximum Supported Number of Interfaces on Security Gateway	64
Maximum Supported Number of Cluster Members	65
Number of Supported Items in an ElasticXL Cluster	66
Number of Supported Items in a Maestro Environment	67
Build Numbers in R82.10	68
Licensing	69

Important Links

For more about R82.10, see:

- [Check Point R82.10 Home Page](#)
- [Check Point R82.10 Known Limitations](#)
- [Check Point R82.10 Resolved Issues and Enhancements](#)

Visit the [Check Point CheckMates Community](#) to:

- Start discussions
- Get answers from experts
- Join the API community to get code samples and share yours

Visit [Check Point Cyber Security Platform Architecture](#).

What's New in R82.10

Introduction

Enterprises are rapidly adopting AI to achieve impressive productivity gains. However, AI systems also introduce unprecedented new security challenges. Traditional detection and response frameworks are no longer enough to protect today's distributed, hybrid mesh networks. It is imperative that enterprises shift left to prevention-first security. R82.10 enables security for the **AI transformation, Hybrid Mesh Network, and advanced threats**.

R82.10 delivers stronger threat prevention, higher scalability & performance, and greater operational simplicity.

Architectural Updates: R82.10 features an upgraded OS based on Linux kernel 5.14 versus 4.xx in previous releases. This release runs exclusively in UPPAK mode (User Space Performance Pack).

Stronger Threat Prevention

- **Threat Prevention Insights:** Provides administrators with clear insights into the effectiveness and coverage of Threat Prevention and IPS, featuring visualizations, metrics, and recommendations to refine rules and profiles.
- **Advanced Zero Phishing:** Zero Phishing Software Blade now protects encrypted traffic from phishing attacks at the domain level - enabling domain analysis by ThreatCloud AI without requiring SSL Inspection or decryption.
- **Protection from HTML Smuggling:** Zero Phishing Software Blade introduces a powerful new capability to detect and block HTML smuggling, an advanced cyberattack technique that avoids firewall detection by building malware locally within a target's web browser.
- **Expanded DNS Protection:** Introduces DNS-over-TLS threat prevention to block malicious DNS activity over encrypted channels.
- **Hardened Encryption:** HTTPS Inspection now supports Hardware Security Module (HSM) for TLS 1.3, making it considerably harder for attackers to compromise encrypted traffic.
- **MCP Detection and Visibility:** Introduces MCP (Model Context Protocol) detection and visibility to ensure that only authorized MCP communications are allowed across the network.
- **Enhanced Drop Templates:** New drop templates improve resilience by reducing CPU usage to enable blocking a much higher volume of denial of service (DoS) attacks while maintaining maximum throughput for permitted traffic.

- **4 New ThreatCloud AI Engines:** PDF security with advanced image and text analysis, malicious GitHub-hosted account and repository detection, automatic creation of file and IPS protection rules, and a new web security model with enhanced decision-making capabilities.
- **Adaptive IPS:** A new optimized IPS defense profile is tailored to fit an organization's exact requirements. This enables IPS to be turned on with minimal CPU performance impact, for improved resiliency and threat detection.

Scalability & Performance

- **Scalable Identity Management:** Improved identity awareness across the enterprise for unified policy enforcement and scalable identity sharing.
 - Each Policy Decision Point (PDP) can now manage up to 1M identities, reducing the number of required PDPs by up to 5X.
 - A single PDP can share identities with up to 300 Policy Enforcement Point (PEP) gateways, even across multiple domains.
 - Direct PDP to PEP sharing works across Multi-Domain Security Management without an Identity Broker, simplifying configuration.
- **Support for SD-WAN in Maestro Security Groups:** Enables higher scalability in branch office networks while providing the highest system reliability and redundancy.
- **Security Management Scalability:** Increases the maximum number of managed Security Gateways to 1,500 per management domain. Users can further scale to 10,000 gateways in a Multi-Domain Security Management Server configuration.

Operational Simplicity

- **Centralized Identity Management:** Identity and Trust is a cloud service that integrates with on-premises network security, provides the option of integrating with multiple identity providers, and eliminates the need for separate management portals. It integrates endpoint device and device security posture data from Microsoft Intune, Microsoft Defender, CrowdStrike Falcon, Endpoint Security, and more for consistent and unified zero-trust access control.
- **New Access Policy Log Generation Modes:** New logging mode enables streamlined control over daily log output, with improved granularity into log levels and analytics on high-volume rules. The Aggregated mode greatly reduces daily log volume by **up to 70%**, reducing storage needs accordingly.
- **Simplified Route-Based VPN:** Automatically configures Site to Site VPN based on network topology, enabling one-click setup and dynamic routing with BGP.
- **Enhanced Web-based UI:** New web-based UI allows users to manage common security use cases from the web for more flexibility.

Threat Prevention

Threat Prevention Insights

- Provides clear insight into Threat Prevention and IPS effectiveness and coverage, with visualizations, metrics, and recommendations to refine policy and profiles. A tuned policy enhances coverage, reduces noise, and maintains Security Gateway performance predictable and manageable.

Key Features:

- **Misconfigurations & Optimizations:**
 - Detects misconfigured IPS profile for example, disabled protections, conflicting exceptions, and outdated profiles).
 - Surfaces overly permissive settings and hitless items, with guidance to remediate safely.
 - Prioritizes changes by security impact and performance benefit.
- **IPS Profile Tuning:**
 - Highlights noisy signatures, false-positive candidates, and protections generating excessive logs.
 - Suggests severity-aware tuning (move to Detect/Prevent, adjust performance impact, add targeted exceptions) to cut noise while preserving critical coverage.

Zero Phishing

- Zero Phishing Software Blade provides prevention for customers without HTTPS Inspection, utilizing [Server Name Indication \(SNI\)](#) in TLS handshake.
- Zero Phishing Software Blade introduces a powerful new capability to detect and block [HTML Smuggling](#), a technique used by threat actors to bypass traditional Network Threat Prevention systems.

ThreatCloud AI Engines

- **Threat Emulation PDF Engine**

The updated PDF engines combine advanced image and text analysis.

- **Image analysis:** QR code extraction, page-layout parsing, brand misuse detection resilient to adversarial obfuscation, and adult-content heuristics.

- **Text analysis:** an SLM (Small Language Model) flags social-engineering patterns in forms, lures, and conversational tone.
- **Brand detection:** adversarial image obfuscation techniques.
- **GitHub Abuse Engine** - Designed to detect malicious GitHub-hosted accounts and repositories used for credential theft and drive-by malware downloads. The engine uses advanced algorithms and AI to analyze user behavior, repository structure, key files, and JavaScript content through deep code inspection.
- **AI Web Security (New model)** - The latest version of the AI web security engine features enhanced decision-making capabilities across web traffic by combining DNS metadata, certificate attributes, and behavioral signals.
- **Generative AI Protections Engine** - Automates the creation of File and IPS protection rules by processing open-source intelligence and ThreatCloud traffic. It generates protection rules automatically, eliminating manual effort and accelerating the protection delivery. By reducing analysis time from days to hours, it enhances threat response and expands coverage with minimal human intervention.

DNS Security

- Introducing [DoT \(DNS over TLS\)](#) - Threat Prevention capabilities for malicious DNS activity over the TLS protocol.

HTTPS Inspection

- Added support for the hybrid PQC-safe key exchange group "X25519MLKEM768" (combining X25519 and ML-KEM768 algorithms) within HTTPS Inspection.
- HTTPS Inspection now supports [Hardware Security Module](#) (HSM) integration for TLS 1.3, ensuring secure storage and management of private keys during encrypted traffic inspection.
- [Rule Base Hit Count](#) is now available for HTTPS Inspection policies, improving visibility and administrative control.

IPS

- [New capability](#) that automatically detects and remediates CPU-intensive IPS protections with a dedicated SmartView dashboard displaying IPS bypass statistics and CPU-intensive protection insights.

Security Gateway

Identity Awareness

- Introducing [Scalable Identity Sharing](#) that allows more flexible and efficient identity distribution with two major enhancements:
 - **Scalable Identity management:** A single Policy Decision Point (PDP) gateway can now distribute identities to up to 300 Policy Enforcement Point (PEP) gateways, significantly improving scalability and performance.
 - **Cross-Management Domain Support:** Identities can now be seamlessly shared across multiple Domain Management Servers (CMAs), enabling unified and consistent identity-based policy enforcement throughout large and distributed environments.
- [Improved PDP Performance](#) - Policy Decision Point (PDP) gateways can now handle up to 1 million identities each, leveraging a new multi-process architecture that optimizes hardware utilization and boosts overall performance.
- Security Gateway integration with [Identity and Trust](#) - Seamless integration with Identity and Trust, delivering centralized and unified Identity Awareness policy enforcement throughout the entire network infrastructure, and supports new identity integrations such as Microsoft Intune, Microsoft Defender, and Endpoint Security.

URL Filtering

- The URL Filtering Software Blade now supports automatic categorization of websites listed in the "Terrorism" category of the CTIRU (Counter-Terrorism Internet Referral Unit) list.

Site to Site VPN

- Added support for standard ML-KEM as required by the FIPS 203 standard to address Post-Quantum Cryptography (PQC). See [sk184080 - Post-Quantum Cryptography \(PQC\) algorithms in R82.10 and higher](#).
- [Simplified Route-based VPN](#) - Automatically configures route-based VPNs on Check Point Security Gateways based on network topology, providing easy, one-click setup and saving configuration time. It also includes support for dynamic routing using BGP.

SD-WAN

- Added support for SD-WAN in Maestro Security Groups. See [sk180605 - Check Point SD-WAN](#).

Security Gateway Enhancement

- New [MCP Detection and Visibility feature](#) designed to monitor and manage Model Context Protocol (MCP) traffic within your network. You can now instantly access detailed information about MCP traffic, including server names, versions, and tools in use. In addition to enhanced visibility, this feature empowers you to accept or drop MCP connections based on your organization's security policies. This gives you greater control over your network traffic and helps ensure only authorized MCP communications are allowed.
- Redesigned the Drop Optimization feature in Access Control policy. The new design supports more acceleration use cases, such as rules with Dynamic Objects and future offloads the traffic to ASIC-powered network cards. See [sk184356 - Firewall Drop Optimization in R82.10 and higher](#).

Dynamic Routing

- Added support for these [Dynamic Routing features](#):
 - Support for up to 256 PIM interfaces, which allows greater flexibility and scalability in network configurations.
 - Support for up to 500 BGP peers, ensuring robust and efficient routing capabilities.
 - Support for BGP Large Communities, which provides enhanced control and management of routing policies across multiple networks.

Cluster and Scalability

- The ElasticXL clustering and Maestro Security Group now support SecureXL in the User Mode (UPPAK).

Internal CA

- Increased RSA Key Size for Internal CA - The default RSA key size for the Root CA has been increased from 2048 bits to 3072 bits, enhancing cryptographic security for Internal CA, SIC, Site to Site VPN, Remote Access VPN clients, user certificates, and Multi-Portal certificates.
 - In the clean installation, this is the default.
 - In the upgraded installation, this is the new default if you remove the current Internal CA and create the new Internal CA.

Gaia OS Security

- In Gaia Clish, you can configure the number of [hashing rounds](#) for new passwords.

Hashing rounds determine the number of iterations a hashing algorithm performs on a password before storing it. This process is used to enhance security by making it more computationally expensive for attackers to crack passwords through brute force attacks.

- Added the Bcrypt hash for [password encryption](#) of local users in the Gaia OS.
- External RADIUS authentication servers can now be configured to use CHAP (Challenge-Handshake Authentication Protocol) or PAP (Password Authentication Protocol).

Security Management

Logging and Monitoring

- [New Access Policy Log Generation Modes](#): Standard and Aggregated. The Aggregated mode significantly reduces the daily log volume.
- The **Log Forwarding** feature is now easier to use. It now forwards locally stored logs to the primary Log Server without requiring a specific Log Server to be selected. The feature is enabled by default for new Gateways, making sure that locally stored logs will automatically upload to the Log Server.
- Additional logging enhancements in SmartConsole:
 - View the rules log level by hovering over the **Track** column in the Access Control rule.
 - Added the ability to customize the default **Track** value for new Access Control rules.
 - Enhanced the session log content with additional fields, including NAT details.
 - Introducing the per-session log level control for Implied Rules.

Compliance

- Added support for new regulations:
 - CSA CCoP 2.0
 - DORA 2023
 - ISO 27002 2022
 - NIST800-82r3
- Added new Management API commands for initiating new scans, showing Best Practices data, Compliance settings, and more.
- Update existing Best Practices for Firewall, IPS, Anti-Bot, and VPN Software Blades.

Cloud Firewall Security

CloudGuard Controller

- New CloudGuard Controller scanner [for Proxmox Virtual Environment](#) data center.

Software Changes in R82.10



Note - To see the list of changes starting from R80.40, see [sk180180](#).

This section describes behavior changes in R82.10 comparing to the previous version R82.

Gaia Operating System

- Updated the Gaia OS Linux kernel version to "5.14".
- Updated the OpenSSL version to "3.5.0".
- Updated the OpenSSH version to "8.6".
- Updated the network interface driver "mlx" version to "24.10-0.7.0".
- Updated the Data Plane Development Kit (DPDK) version to "22.11".
- Removed the user shell `/usr/bin/scponly`.
- Disabled these in the default SSH configuration (only in a Clean Install):
 - Weak Message Authentication Codes (MACs) in SSH:
 - `hmac-sha1:`
 - `hmac-sha1-etm@openssh.com`
 - `umac-64-etm@openssh.com`
 - `umac-64@openssh.com`
 - Weak Public-Keys:
 - `ssh-rsa`
 - `ssh-rsa-cert-v01@openssh.com`
- These Check Point Appliance models do not support R82.10:
 - 23500, 23800, 23900
 - 15400, 15600
 - 6500, 6800
 - 5100, 5200, 5400, 5600, 5800, 5900

- 3100, 3200
- Smart-1 5150, Smart-1 5050, Smart-1 625, Smart-1 405, Smart-1 410
- Scalable Chassis 44000 / 64000

Security Gateway

- On Check Point Appliances, Virtual Machines, and Open Servers:
 - Firewall runs only in the User Space Firewall mode (USFW).
The Kernel Space Firewall mode (KSFw) does not exist anymore.
See [sk167052](#).
 - SecureXL runs only in the User Mode (UPPAK).
The Kernel Mode (KPPAK) does not exist anymore.
See the [R82.10 Performance Tuning Administration Guide](#).
- Updated the Data Plane Development Kit (DPDK) version to 22.11.
- Added support for SecureXL in the User Mode (UPPAK) in Cloud Firewall Security Gateways in all cloud environments.
- Log Forwarding is now enabled by default in new Security Gateway / Cluster objects. At midnight, locally stored logs are sent to the primary Log Server.

In the new Security Gateway / Cluster object, navigate to **Logs > Additional Logging** and refer to the section **Log Forwarding Settings**.
- By default, the Security Gateway's Multi-Portal (Web Portals for various Software Blades) is configured to use only recommended and secure TLS cipher suites.

Weak cipher suites are now disabled by default. To re-enable the necessary weak ciphers, use the `cipher_util` tool.

 **Important:** Remote Access VPN connections and Multi-Portal use the same infrastructure on a Security Gateway.

An R82.10 Security Gateway will fail Remote Access VPN connections from operating systems that:

- Do not support TLS 1.3 connections.
and
- Do not support these TLS 1.2 ciphers:
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38

To support Remote Access VPN connections from such operating systems, you must use the `cipher_util` tool on the Security Gateway / each Cluster Member / Security Group and enable the cipher suite `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`.

If the operating system of a Remote Access client supports either TLS 1.3 or these TLS 1.2 ciphers, then no need to change the configuration.

- Mobile Access support for Citrix is deprecated (see ["Mobile Access Requirements" on page 53](#)).
- Support for Hardware Security Module (HSM) from the FutureX vendor is deprecated.
- These features are deprecated in VPN Communities:

Deprecated Feature	How to Get There in SmartConsole R82 and lower	Next Step
IKEv1	VPN Community properties > page Encryption > section Encryption Settings > field Encryption Method	Use IKEv2
Wire Mode	VPN Community properties > page Wire Mode	Disable
IP Compression	VPN Community properties > page Advanced > section Properties	Disable
Aggressive Mode	VPN Community properties > page Advanced > section Properties	Disable

**Important:**

- VPN Communities continue to work as configured before an upgrade to R82.10.
- R82.10 SmartConsole:
 - Does not support the configuration of these deprecated features.
 - Shows the applicable message and the next supported step.

Scalable Platforms

The CLI syntax to configure weights for Security Group Members changed:

Syntax in R82	Syntax in R82.10
<code>set smo security-group sgm-weight member-id <SGM IDs> weight {default <0-512>}</code>	<code>set cluster configuration member-weight member-id <SGM IDs> weight {default <0-512>}</code>
<code>set smo security-group sgm-weight apply</code>	<code>set cluster configuration member-weight apply</code>
<code>show smo security-group sgm-weight all</code>	<code>show cluster configuration member-weight all</code>
<code>show smo security-group sgm-weight current</code>	<code>show cluster configuration member-weight distribution</code>
<code>show smo security-group sgm-weight <SGM ID></code>	<code>show cluster configuration member-weight <SGM ID></code>

Threat Prevention

- The Zero Phishing Software Blade and the Threat Emulation Software Blade are now activated by default in newly created Security Gateway and Cluster objects.

This feature requires a valid license be installed on a Security Gateway and Cluster Members.

This feature helps to enhance our security measures and protect your systems from potential phishing attacks and malware attacks.

See the [R82.10 Threat Prevention Administration Guide](#).

Management Server

- Updated the PostgreSQL version to 16.4.
- In the Compliance Software Blade, removed these Best Practices:
 - FW202, FW203, FW204
 - IPS110, IPS111, IPS117, IPS122, IPS123, IPS124, IPS125, IPS132
 - MOB131
 - TP106
 - VPN112, VPN113, VPN120, VPN121, VPN127

Supported Environments in R82.10

Management Servers / Log Servers boot by default with the 64-bit Gaia kernel after a clean installation or upgrade to R82.10.

Notes:

- If after the upgrade to R82.10 you revert to the previous version, then Gaia OS boots with the 64-bit Gaia kernel, even if in the previous version the Gaia kernel was 32-bit.
- For documentation about Check Point Appliances, see [sk96246](#).
- Refer to the [Support Life Cycle Policy](#) page for more information and announcements.

Management Server and Log Server

Only these platforms support R82.10 in the Management Server and Log Server configurations:

Check Point Product	Smart-1 7000-UL ⁽¹⁾ , Smart-1 7000-XL ⁽¹⁾ , Smart-1 7000-L ⁽¹⁾ , Smart-1 6000-XL ⁽²⁾ , Smart-1 6000-L ⁽²⁾	Smart-1 700-M ⁽³⁾ , Smart-1 700-S ⁽³⁾ , Smart-1 600-M ⁽⁴⁾ , Smart-1 600-S ⁽⁴⁾	Open Servers ⁽⁵⁾	Virtual Machines ⁽⁶⁾
Security Management Server, Endpoint Security Management Server	Yes	Yes	Yes	Yes
Log Server	Yes	Yes	Yes	Yes
SmartEvent Server	Yes	Yes	Yes	Yes
Multi-Domain Security Management Server	Yes	No	Yes ⁽⁷⁾	Yes ⁽⁷⁾
Multi-Domain Log Server	Yes	No	Yes ⁽⁷⁾	Yes ⁽⁷⁾

1. For information about Smart-1 7000-UL, Smart-1 7000-XL, and Smart-1 7000-L, see [sk182601](#).
2. For information about Smart-1 6000-L and Smart-1 6000-XL, see [sk171903](#).
3. For information about Smart-1 700-M and Smart-1 700-S, see [sk182601](#).
4. For information about Smart-1 600-S and Smart-1 600-M, see [sk171903](#).
5. For certified Open Servers, see the [Hardware Compatibility List](#) > Tab [Open Servers](#). For known limitations, see [sk168335](#).
6. "Virtual Machines" apply to Public Cloud and to Private Cloud.
See the [Hardware Compatibility List](#) > Tab [Virtual Machines](#). For known limitations, see [sk168335](#).
7. Requires a license to manage a minimum of 25 Security Gateways.
8. Each of these Smart-1 appliance models, Open Servers, and Virtual Machines can run any combination of these products:
 - Management Server and Log Server on the same server.
 - Management Server and SmartEvent Server on the same server.
 - Log Server and SmartEvent Server on the same server.
 - Management Server and Log Server and SmartEvent Server on the same server.

Management High Availability:

You can configure Check Point Management High Availability between on-premises Management Servers and Management Servers in a cloud.

You must make sure the required Check Point traffic can flow between the on-premises servers and the servers in the cloud.

For Management High Availability restrictions, see [sk39345](#).

Security Gateway or Cluster

Only these platforms support R82.10 in the Security Gateway, Cluster, or ElasticXL configuration:

Platforms	SK	Security Gateway, Cluster ⁽³⁾	ElasticXL Cluster ⁽⁴⁾
MLS200, MLS400	sk176466	Yes	Yes
QLS250, QLS450, QLS650, QLS800	sk176466	Yes	Yes
29100, 29200	sk180520	Yes	Yes
28000, 28600HS	sk152733	Yes	Yes
26000, 26000T	sk152733	Yes	Yes
19100, 19200	sk180520	Yes	Yes
16000, 16200, 16600HS, 16600T	sk152733	Yes	Yes
9100, 9200, 9300, 9400, 9700, 9800	sk181698	Yes	Yes
7000	sk139932	Yes	Yes
6200, 6400, 6600, 6700, 6900	sk139932	Yes	Yes
3920, 3950, 3970, 3980	sk183199	Yes	Yes
3600, 3800	sk110052	Yes	No
Open Servers ⁽¹⁾	N / A	Yes	No
Virtual Machines ⁽²⁾	N / A	Yes	Yes

1. For certified Open Servers, see the [Hardware Compatibility List](#) > Tab [Open Servers](#). For known limitations, see [sk168335](#).
2. "Virtual Machines" apply to Public Cloud and to Private Cloud.

See the [Hardware Compatibility List](#) > Tab [Virtual Machines](#). For known limitations, see [sk168335](#).

- "Cluster" refers to ClusterXL (Active-Active, High Availability, Load Sharing) and VRRP Cluster on Gaia OS.
- For ElasticXL requirements, see [sk183513](#).

Standalone and Full High Availability

Only these platforms support R82.10 in the Standalone (Gateway + Management Server) configuration or in the Full High Availability Cluster configuration:

Platforms	SK	Standalone, Full HA
9100, 9200, 9300, 9400, 9700, 9800	sk181698	Yes
7000	sk139932	Yes
6200, 6400, 6600, 6700, 6900	sk139932	Yes
3600, 3800	sk110052	Yes
Open Servers ⁽¹⁾	N / A	Yes
Virtual Machines ⁽²⁾	N / A	Yes

- For certified Open Servers, see the [Hardware Compatibility List](#) > Tab [Open Servers](#). For known limitations, see [sk168335](#).
- "Virtual Machines" apply to Public Cloud and to Private Cloud.
See the [Hardware Compatibility List](#) > Tab [Virtual Machines](#). For known limitations, see [sk168335](#).
- It is not supported to enable the SmartEvent Software Blade on any Management Server in the Full High Availability Cluster configuration.

VSNext and Traditional VSX

This table shows the support for VSNext and Traditional VSX in R82.10:

Platforms	VSNext	Traditional VSX
ElasticXL Cluster	Yes ⁽³⁾	No
Security Group - Maestro	Yes ⁽⁴⁾	Yes ⁽⁵⁾
Open Servers ⁽¹⁾	No	Yes
Virtual Machines ⁽²⁾	Yes ⁽³⁾⁽⁶⁾⁽⁷⁾	Yes ⁽⁷⁾

1. For certified Open Servers, see the [Hardware Compatibility List](#) > Tab [Open Servers](#). For known limitations, see [sk168335](#).
2. "Virtual Machines" apply to Private Cloud and Public Cloud.
See the [Hardware Compatibility List](#) > Tab [Virtual Machines](#). For known limitations, see [sk168335](#).
3. The Gaia Operating System must be after a clean install, or restored to factory defaults.
In the First Time Configuration Wizard, you must select **ElasticXL** and **Install as VSNext**.
Converting to VSNext after the First Time Configuration Wizard is not supported.

4. Create a new Maestro Security Group and in the **First Time Wizard settings** section, select **Install as VSNext / VSX**.

Converting an existing Maestro Security Group to VSNext is not supported.

Maestro Orchestrator that runs the R82.10 version, automatically configures these modes:

- VSNext mode in a Maestro Security Group that runs the R82.10 version.

For each Virtual Gateway you configure in this Maestro Security Group:

- a. In SmartConsole click  **(New)** > **VSX** > **Gateway** > select **VSNext mode on Scalable Platform cluster (ElasticXL or Maestro) on R82 and higher** > click **Next**.
 - b. Configure the Security Gateway object.
 - Traditional VSX mode in a Maestro Security Group that runs the version R81.20 or lower.
 - a. In SmartConsole, click  **(New)** > **VSX** > **Gateway** > select **Legacy VSX mode** > click **Next** > configure the Security Gateway object.
 - b. To configure the required Virtual System and Virtual Switch objects, in SmartConsole click  **(New)** > **VSX** > **Virtual System** and **Virtual Switch**.
5. To configure a Maestro Security Group that runs the R82.10 version in the Traditional VSX mode:
 - a. Create a new Maestro Security Group and in the **First Time Wizard settings** section, do **not** select **Install as VSNext / VSX**.
 - b. In SmartConsole, click  **(New)** > **VSX** > **Gateway** > select **Legacy VSX mode** > click **Next** > configure the Security Gateway object..
 - c. To configure the required Virtual System and Virtual Switch objects, in SmartConsole click  **(New)** > **VSX** > **Virtual System** and **Virtual Switch**.
 6. To install ElasticXL Cluster on Virtual Machines, see the requirements in [sk183513](#).
 7. VSNext and Traditional VSX modes are not supported in Public Cloud.

Threat Emulation Appliances

R82.10 does **not** support Threat Emulation Appliances.

Maestro

Maestro Orchestrator models MHO-140, MHO-170, and MHO-175 fully support the R82.10 release. See [sk183506](#).

For the list of supported Maestro Security Group versions, see *"Maestro Orchestrator and Security Group Versions" on page 44*.

For the list of supported Security Appliances in a Maestro Security Group, see [sk162373](#).

Virtualization Platforms

For the most up-to-date information about the supported Linux versions and virtualization platforms, see the [Hardware Compatibility List](#) > Tab [Virtual Machines](#).

Cloud Platforms

Supported setups for cloud solutions:

- **Amazon Web Services:**

- Security Gateway
- Single Zone High Availability Cluster
- Cross Availability Zone Cluster (Cross AZ Cluster)
- Security Gateway Auto Scaling Group
- Gateway Load Balancer Virtual Machine Scale Sets
- Security Management Server
- Multi-Domain Security Management Server
- Standalone

- **Microsoft Azure:**

- Security Gateway
- High Availability Cluster
- Virtual Machine Scale Sets
- Security Management Server
- Multi-Domain Security Management Server
- Standalone
- Virtual WAN

- **Google Cloud Platform (GCP):**

- Security Gateway
- High Availability Cluster
- Managed Instance Group (MIG)
- Network Security Integration (NSI)
- Security Management Server
- Multi-Domain Security Management Server
- Standalone

■ Oracle Cloud Infrastructure (OCI):

- Security Gateway
- High Availability Cluster
- Security Management Server
- Multi-Domain Security Management Server
- Standalone

■ Huawei Cloud:

- Security Gateway
- High Availability Cluster
- Security Management Server
- Standalone

■ Tencent Cloud:

- Security Gateway
- High Availability Cluster
- Security Management Server
- Standalone

Supported Upgrade Paths in R82.10

Notes:

- For information about Security Management Servers and supported managed Security Gateways see:
 - ["Supported Security Gateway Versions in R82.10" on page 43](#)
 - [sk113113](#)
- CPUSE does not support a Clean Install of the versions R81.20 or lower, while the version R82.10 is installed.
To perform a Clean Install of the versions R81.20 or lower, you must follow [sk65205](#) and use a bootable USB device.

Upgrade Paths for Security Gateways, Management Servers, Log Servers, SmartEvent Servers, Standalone Servers

Upgrade to R82.10 is available only from these versions for Security Gateways, Management Servers, Log Servers, SmartEvent Servers, and Standalone Servers:

Current Version	Security Gateways, Cluster Members, Traditional VSX ⁽¹⁾	Management Servers, Multi-Domain Servers, Log Servers, SmartEvent Servers	Standalone Servers
R82, R81.20, R81.10, R81	Yes	Yes	Yes
R80.40, R80.30 kernel 3.10, R80.30 kernel 2.6	Requires a 2-step upgrade path ⁽²⁾	Yes	Requires a 2-step upgrade path ⁽²⁾

**Notes:**

1. Starting from R81.10, in the Traditional VSX mode, VSLS mode is the only supported mode for **new** installations of **VSX Clusters**.
Upgrade of a Traditional VSX Cluster in the High Availability mode from R81.10 and earlier versions to R82.10 is supported.
To convert the upgraded Traditional VSX Cluster to VSLS, use the "vsx_util convert_cluster" command.
2. The required 2-step upgrade path is:
 - a. Upgrade to one of these versions:
 - R81.20 (see the [R81.20 Installation and Upgrade Guide](#)).
 - R81.10 (see the [R81.10 Installation and Upgrade Guide](#)).
 - R81 (see the [R81 Installation and Upgrade Guide](#)).
 - b. Upgrade to R82.10.

Upgrade Paths for Scalable Platforms

Upgrade to R82.10 on Scalable Platforms (Maestro and ElasticXL) is available only from these versions:

Current Version for Scalable Platforms	Mode	Upgrade Path
R82	Security Gateway, ElasticXL, VSNext, Traditional VSX	Requires a 3- step upgrade path ⁽¹⁾
R81.20, R81.10	Security Gateway, Traditional VSX	Requires a 3- step upgrade path ⁽¹⁾
R81, R80.30SP, R80.20SP	Security Gateway, Traditional VSX	Requires a 4- step upgrade path ⁽²⁾

Notes for Scalable Platforms:

1. To upgrade a Security Group from R81.10, R81.20, R82 to R82.10, you must follow this 3-step upgrade path (for the required packages, see [sk183506](#) > section "Downloads and Installation" > section "ElasticXL and Quantum Maestro"):
 - a. Install the required Jumbo Hotfix Accumulator on the current version ([R82](#), [R81.20](#), [R81.10](#)).
 - b. Install the required CPUSE Deployment Agent on the current version.
 - c. Upgrade to R82.10.
2. To upgrade a Security Group from R80.20SP, R80.30SP, R81 to R82.10, you must follow this 4-step upgrade path (for the required packages, see [sk183506](#) > section "Downloads and Installation" > section "ElasticXL and Quantum Maestro"):
 - a. Upgrade to **one** of these versions:
 - R81.20 for Scalable Platforms.
See:
 - [sk177624 - R81.20 for Scalable Platforms](#)
 - [R81.20 Maestro Administration Guide](#).
 - R81.10 for Scalable Platforms.
See:
 - [sk173363 - R81.10 for Scalable Platforms](#)
 - [R81.10 Maestro Administration Guide](#).
 - b. Install the required Jumbo Hotfix Accumulator on R81.10 / R81.20 for Scalable Platforms.
 - c. Install the required CPUSE Deployment Agent on R81.10 / R81.20 for Scalable Platforms.
 - d. Upgrade to R82.10.
3. In a Maestro environment, you must follow this upgrade order:
 - a. Upgrade the Management Server that manages the Maestro Security Group.
 - b. Upgrade the Maestro Orchestrators on each Maestro Site.
See *"[Maestro Orchestrator and Security Group Versions](#)" on page 44*.
 - c. Upgrade the Maestro Security Groups on each Maestro Site.
4. To upgrade a Security Group, it must contain a minimum of two configured and working Security Group Members.

Supported Upgrade Methods in R82.10

Use the methods below to upgrade your Check Point environment to R82.10.

 **Best Practice** - If several methods are supported for your product, we recommend Central Deployment in SmartConsole.

 **Important:**

- To start an upgrade with a CPUSE package on a Check Point appliance, Open Server, or Virtual Machine:
 - The `/var/log/` partition must have 30 GB of free space (to import and extract the package).
 - The `root` partition must have at least 20 GB of free space.
- To start an upgrade with a Gaia Fast Deployment image on a Check Point appliance:
 1. The `/var/log/` partition must have free space that is at least twice the size of the image.
 2. The `root` partition must have free space that is at least twice the size of the image.

Check Point Product	Gaia Fast Deployment Clean Install (1)	Gaia Fast Deployment Upgrade (1)	Central Deployment in SmartConsole (2)	CPUSE Clean Install (3)	CPUSE Upgrade (4)	Advanced Upgrade (5)	Upgrade with Migration (6)	Upgrade with CDT (7)
Security Gateways	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Traditional VSX Gateway	No	Yes	Yes	Yes	Yes	No	No	Yes

Check Point Product	Gaia Fast Deployment Clean Install (1)	Gaia Fast Deployment Upgrade (1)	Central Deployment in SmartConsole (2)	CPUSE Clean Install (3)	CPUSE Upgrade (4)	Advanced Upgrade (5)	Upgrade with Migration (6)	Upgrade with CDT (7)
Security Group Members - Maestro (including these modes: Gateway, VSNext, Traditional VSX)	No	No	No	Yes	Yes	No	No	No
ElasticXL Cluster Members (including these modes: Gateway, VSNext)	No	No	No	Yes	Yes	No	No	No
ClusterXL Members in the High Availability modes	No	Yes	Yes	Yes	Yes	No	No	Yes

Check Point Product	Gaia Fast Deployment Clean Install ⁽¹⁾	Gaia Fast Deployment Upgrade ⁽¹⁾	Central Deployment in SmartConsole ⁽²⁾	CPUSE Clean Install ⁽³⁾	CPUSE Upgrade ⁽⁴⁾	Advanced Upgrade ⁽⁵⁾	Upgrade with Migration ⁽⁶⁾	Upgrade with CDT ⁽⁷⁾
ClusterXL Members in the Load Sharing modes	No	Yes	No	Yes	Yes	No	No	Yes
Traditional VSX Cluster Members in the High Availability mode	No	Yes	Yes	Yes	Yes	No	No	Yes
Traditional VSX Cluster Members in the VSLS mode	No	Yes	No	Yes	Yes	No	No	Yes
VRRP Cluster Members	No	Yes	No	Yes	Yes	No	No	Yes

Check Point Product	Gaia Fast Deployment Clean Install (1)	Gaia Fast Deployment Upgrade (1)	Central Deployment in SmartConsole (2)	CPUSE Clean Install (3)	CPUSE Upgrade (4)	Advanced Upgrade (5)	Upgrade with Migration (6)	Upgrade with CDT (7)
Primary Security Management Server	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Secondary Security Management Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Primary Multi-Domain Security Management Server	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Secondary Multi-Domain Security Management Server	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Primary Multi-Domain Log Server	Yes	Yes	No	Yes	Yes	Yes	Yes	No

Check Point Product	Gaia Fast Deployment Clean Install ⁽¹⁾	Gaia Fast Deployment Upgrade ⁽¹⁾	Central Deployment in SmartConsole ⁽²⁾	CPUSE Clean Install ⁽³⁾	CPUSE Upgrade ⁽⁴⁾	Advanced Upgrade ⁽⁵⁾	Upgrade with Migration ⁽⁶⁾	Upgrade with CDT ⁽⁷⁾
Secondary Multi-Domain Log Server	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Primary CloudGuard Controller	No	No	No	Yes	Yes	Yes	Yes	No
Secondary CloudGuard Controller	No	No	Yes	Yes	Yes	Yes	Yes	No
Primary Endpoint Security Management Server	No	No	No	Yes	Yes	Yes	Yes	No
Secondary Endpoint Security Management Server	No	No	Yes	Yes	Yes	Yes	Yes	No

Check Point Product	Gaia Fast Deployment Clean Install ⁽¹⁾	Gaia Fast Deployment Upgrade ⁽¹⁾	Central Deployment in SmartConsole ⁽²⁾	CPUSE Clean Install ⁽³⁾	CPUSE Upgrade ⁽⁴⁾	Advanced Upgrade ⁽⁵⁾	Upgrade with Migration ⁽⁶⁾	Upgrade with CDT ⁽⁷⁾
Dedicated Log Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Dedicated SmartEvent Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Full High Availability Cluster Members	No	No	No	Yes	Yes	Yes	Yes	No
Standalone Server	No	No	No	Yes	Yes	Yes	Yes	No

 Explanations:

1. Gaia Fast Deployment:

Performs a multi-step upgrade or clean install with one image.

This image already contains a specific base version, a designated role (for example, a Security Gateway), and Hotfixes / Jumbo Hotfix Accumulator.

You can see and install this image with CPUSE in Gaia Portal or Gaia Clish.

For more information, see [sk120193](#).

2. Central Deployment in SmartConsole:

- You perform a remote installation of an upgrade package from SmartConsole.
- You install the package from the local repository on the Management Server or from Check Point Cloud.
- You can install the package on several targets at the same time.
- On a ClusterXL and a Traditional VSX Cluster in the High Availability mode, the Central Deployment method performs the Multi-Version Cluster (MVC) Upgrade to preserve the current connections:
 - a. Upgrades all Cluster Members in the Standby mode.
 - b. Enables the MVC mode to allow the synchronization of the current connections between Cluster Members that run different software versions.
 - c. Performs a failover from the Cluster Member in the Active state to one of the upgraded Cluster Members.
 - d. Upgrades the remaining Cluster Member (formerly in the Active state).
- For instructions, see the [R82.10 Security Management Administration Guide](#).

3. CPUSE Clean Install:

- You perform a local installation of the higher version from scratch in Gaia Portal or Gaia Clish.
- You install the package from the local repository in Gaia OS or from Check Point Cloud.
- Requires these steps to preserve the configuration and database:
 - a. Export the data before the installation.
 - b. Import the data after the installation.
- On a ClusterXL and a Traditional VSX Cluster, there are different ways to perform a local upgrade on the Cluster Members based on how you need to preserve the current connections:
 - Multi-Version Cluster (MVC) Upgrade
 - Minimum Effort Upgrade
 - Minimum Downtime Upgrade
- For instructions, see the [R82.10 Installation and Upgrade Guide](#).

4. CPUSE Upgrade (In-place Upgrade):

- You perform a local installation of an upgrade package in Gaia Portal or Gaia Clish.
- You install the package from the local repository in Gaia OS or from Check Point Cloud.
- Keeps the current configuration and database.
- On a ClusterXL and a Traditional VSX Cluster, there are different ways to perform a local upgrade on the Cluster Members based on how you need to preserve the current connections:
 - Multi-Version Cluster (MVC) Upgrade
 - Minimum Effort Upgrade
 - Minimum Downtime Upgrade
- For instructions, see the [R82.10 Installation and Upgrade Guide](#).

5. Advanced Upgrade:

- Intended for Management Servers only.
- You perform a local installation of an upgrade package in Gaia Portal or Gaia Clish.
- You install the package from the local repository in Gaia OS or from Check Point Cloud.
- Requires these steps:
 - a. Export of the current management database from the server.
 - b. Upgrade of the server with CPUSE (In-place Upgrade or Clean Install).
 - c. Import of the exported management database.
- For instructions, see the [R82.10 Installation and Upgrade Guide](#).

6. Upgrade with Migration:

- Intended for Management Servers only.
- Requires these steps:
 - a. Export of the current management database from the server.
 - b. Installation of a different server with a higher version (Clean Install).
 - c. Import of the exported management database.
- For instructions, see the [R82.10 Installation and Upgrade Guide](#).

7. Upgrade with CDT (Central Deployment Tool):

- Intended for Security Gateways and Cluster Members only.
- You perform a remote installation of an upgrade package from the Management Server.
- You install the package from the local repository on the Management Server.
- You can install the package on several targets at the same time.
- For more information, see [sk111158](#).

8. The minimum required unpartitioned disk space is the highest value of one of these:

- Size of the current root partition.
- The used space in the current root partition plus 3 GB.
- If the used space is more than 90% of the root partition, then 110% of the size of the current root partition.

**Important:**

- At least 20 GB of free disk space is required in the `root` partition for an Upgrade to succeed.
- At least 30 GB of free disk space is required in the `/var/log` partition for a Clean Install or Upgrade to succeed.

Supported Security Gateway Versions in R82.10

Management Server and Security Gateway Versions

 **Note** - For more information about Security Management Servers and supported managed Security Gateways see [sk113113](#).

R82.10 Management Servers can manage Security Gateways that run only these versions and modes:

Gateway Type	Mode	Release Version
Security Gateways, ClusterXL, VRRP Cluster	Gateway	R82.10, R82, R81.20, R81.10, R81, R80.40, R80.30, R80.20, R80.10
Security Gateways, Traditional VSX Cluster	Traditional VSX	R82.10, R82, R81.20, R81.10, R81, R80.40, R80.30, R80.20, R80.10
ElasticXL Cluster	Gateway	R82.10, R82
ElasticXL Cluster	VSNext	R82.10, R82
Security Groups in Maestro	Gateway	R82.10, R82, R81.20, R81.10, R81, R80.30SP, R80.20SP See <i>"Maestro Orchestrator and Security Group Versions" on the next page.</i>
Security Groups in Maestro	VSNext	R82.10, R82 See <i>"Maestro Orchestrator and Security Group Versions" on the next page.</i>
Security Groups in Maestro	Traditional VSX	R82.10, R82, R81.20, R81.10, R81, R80.30SP, R80.20SP See <i>"Maestro Orchestrator and Security Group Versions" on the next page.</i>

Gateway Type	Mode	Release Version
Security Groups on Scalable Chassis 44000 / 64000	Gateway	R82, R81.20, R81.10, R81, R80.20SP
Security Groups on Scalable Chassis 44000 / 64000	Traditional VSX	R82, R81.20, R81.10, R81, R80.20SP
Spark Firewall, Rugged Firewall	Gateway	R82.00.X, R81.10.X

Notes:

- To manage R82.10 Security Gateways / Security Groups, an R82 Management Server requires:
 1. The [R82 Jumbo Hotfix Accumulator](#), Take 19 or higher (see PRJ-61143).
 2. The [R82 SmartConsole Releases](#), Build 1053 or higher.
- Management Servers R82.10 do **not** support:
 - Security Gateways and VSX Gateways R77.30 or lower.
 - Rugged Firewall 1200R Appliances.
- Management Servers R81.20 and lower **cannot** manage R82.10 Security Gateways / Security Groups / Clusters.

Maestro Orchestrator and Security Group Versions

R82.10 Maestro Orchestrator can manage Maestro Security Groups that run these versions:

- R82.10 (see [sk183506](#))
- R82 (see [sk181127](#))
- R81.20 (see [sk177624](#))
- R81.10 (see [sk173363](#))

 **Important** - The major software version on the Orchestrator must be equal to or higher than the major software version on the managed Security Group.

Hardware Requirements for Open Server / Virtual Machine in R82.10

See [sk168335 - Known Limitations for Open Servers and Virtual Machines](#).

Minimum CPU and RAM Requirements for Open Server / Virtual Machine

Check Point Product	Processor	Total CPU cores	Memory
Security Management Server, Dedicated Log Server	Supported Intel® Core™ i5 or equivalent	2	8 GB
Multi-Domain Security Management Server, Multi-Domain Log Server	Supported Intel® Core™ i5 or equivalent	8	32 GB
Security Gateway	Supported Intel® Core™ i5 or equivalent	2	8 GB
ClusterXL Cluster Member, VRRP Cluster Member	Supported Intel® Core™ i5 or equivalent	2	8 GB
Traditional VSX Gateway, Traditional VSX Cluster Member	Supported Intel® Core™ i5 or equivalent	2	8 GB
Standalone	Supported Intel® Core™ i5 or equivalent	4	8 GB



For the SmartEvent requirements, see ["SmartEvent Requirements" on page 50](#).

Disk Space Requirements for Open Server / Virtual Machine

These are the requirements for the entire disk device to perform a Clean Install:

Check Point Product ⁽⁴⁾	Recommended free disk space	Minimum free disk space ⁽³⁾
Security Management Server ⁽¹⁾ , Dedicated Log Server ⁽¹⁾	1 TB	110 GB
Multi-Domain Security Management Server ⁽²⁾ , Multi-Domain Log Server ⁽²⁾	1 TB	For the Multi-Domain Server: 100 GB For each additional Domain: 110 GB
Security Gateway	200 GB	110 GB
ClusterXL Cluster Member, VRRP Cluster Member	200 GB	110 GB
Traditional VSX Gateway, Traditional VSX Cluster Member	For the Traditional VSX Gateway / Cluster Member: 200 GB For each Traditional VSX Virtual System: 1 GB	For the Traditional VSX Gateway / Cluster Member: 100 GB For each Traditional VSX Virtual System: 1 GB
Standalone	1 TB	110 GB

Notes:

1. On an Open Server / Virtual Machine, additional backup / snapshot is not supported.
2. On an Open Server / Virtual Machine, at least 20 GB of free disk space is required in the `root` partition for an Upgrade to succeed.
3. On an Open Server / Virtual Machine, at least 10 GB of free disk space is required in the `/var/log` partition for a Clean Install or Upgrade to succeed. On an Open Server / Virtual Machine, the logging partition size is only large enough for minimum server operations.

Maximum Supported Physical Memory on Open Server / Virtual Machine

Check Point Product	Physical RAM Limit
Security Management Server, or Multi-Domain Security Management Server	512 GB
Security Gateway, or Cluster Member	256 GB

Requirements in R82.10

Threat Extraction Requirements for Web-downloaded Documents

- Supported with appliance series 5000, 6000, 7000, and higher.

Logging Requirements

Logs can be stored on:

- A Management Server that collects logs from the Security Gateways. This is the default.
- A Log Server on a dedicated server. This is the recommendation for environments that generate many logs.

A dedicated Log Server has greater capacity and performance than a Management Server with the activated Logging & Status Software Blade.

The dedicated Log Server must run the same version as the Management Server.

SmartEvent Requirements

Software Requirements

1. To deploy SmartEvent and to generate reports, a valid license or contract is required.
2. The dedicated SmartEvent Server must run the same version as the Management Server or the dedicated Log Server.
3. If a dedicated SmartEvent Server gets logs from a dedicated Log Server, then the two servers must have these Takes of the [R82.10 Jumbo Hotfix Accumulator](#) installed:
 - Both servers must have Take 36 or higher (in such a case, different Takes are supported on each server).
 - Both servers must have Take 24 or lower (in such a case, different Takes are supported on each server).
4. If you install a dedicated SmartEvent Server and a dedicated SmartEvent Correlation Unit (for example, to balance the load in large logging environments), then these two servers must run the same version.

Hardware Requirements

For an average rate of 500 logs per second:

- Total CPU Cores: 4
- RAM: 16GB

SmartConsole Requirements

Desktop SmartConsole Hardware Requirements

This table shows the minimum hardware requirements for the Desktop SmartConsole applications:

Component	Minimum Requirement
CPU	Supported Intel® Core™ i3 or equivalent processor
Memory	4 GB
Available Disk Space	2 GB
Video Adapter	Minimum resolution: 1024 x 768
Disk Partition	NTFS

Desktop SmartConsole Software Requirements

- Microsoft .NET framework 4.8.
- Microsoft Visual C++ Redistributable 2019.

Desktop SmartConsole is supported on:

- Windows 11, Windows 10 (all editions).
- Windows Server 2025, 2022, 2019.

(*) On Windows Server 2025, SmartProvisioning is not supported - managing with SmartLSM Profiles and Provisioning Profiles (Limitation PMTR-124448).

Gaia Portal Requirements

The Gaia Portal requirements on Security Gateways, Cluster Members, Management Servers, and Log Servers

To connect to Gaia Portal on R82.10 Security Gateways, Cluster Members, Scalable Platform Security Groups, Security Management Servers, Log Servers, SmartEvent Servers, Multi-Domain Security Management Servers, Multi-Domain Log Servers, Endpoint Security Management Servers, and Endpoint Policy Servers, you must use one of these web browsers:

Browser	Supported Versions
Microsoft Edge	All versions
Google Chrome	14 and higher
Mozilla Firefox	6 and higher
Apple Safari	5 and higher

The Gaia Portal requirements on Maestro Orchestrators

To connect to Gaia Portal on R82.10 Maestro Orchestrators, you must use one of these web browsers:

Browser	Supported Versions
Microsoft Edge	85.0 and higher
Google Chrome	85.0 and higher
Mozilla Firefox	79.0 and higher

Mobile Access Requirements

You must use one of these operating systems:

OS Compatibility

Endpoint Computer OS Compatibility	Windows	Linux	macOS	iOS	Android
Mobile Access Portal	Yes	Yes	Yes	Yes	Yes
Clientless access to web applications (Link Translation)	Yes	Yes	Yes	Yes	Yes
Compliance Scanner	Yes	Yes	Yes	No	No
Secure Workspace	Yes	No	No	No	No
SSL Network Extender - Network Mode	Yes	Yes	Yes	No	No
SSL Network Extender - Application Mode	Yes	No	No	No	No
Downloaded from Mobile Access applications	Yes	Yes	Yes	No	No
Citrix	No	No	No	No	No
File Shares - Web-based file viewer (HTML)	Yes	Yes	Yes	Yes	Yes
Web mail	Yes	Yes	Yes	Yes	Yes

You must use one of these web browsers:

Web Browser Compatibility

Endpoint Web Browser Compatibility	Microsoft Edge	Google Chrome	Mozilla Firefox	Apple Safari	Opera for Windows
Mobile Access Portal	Yes	Yes	Yes	Yes	Yes
Clientless access to web applications (Link Translation)	No	Yes	Yes	Yes	Yes
Compliance Scanner	Yes	Yes	Yes	Yes	No
Secure Workspace ⁽²⁾	Yes	Yes	Yes	No	No
SSL Network Extender - Network Mode	No	Yes	Yes	Yes	No
SSL Network Extender - Application Mode ⁽²⁾	Yes	Yes	Yes	No	No
Downloaded from Mobile Access applications	No	Yes	Yes	Yes	No
Citrix	No	No	No	No	No
File Shares - Web-based file viewer (HTML)	Yes	Yes	Yes	Yes	Limited support
Web mail	No	Yes	Yes	Yes	Yes



Notes:

1. For a list of the prerequisites necessary to use the Mobile Access Portal on-demand clients, such as SSL Network Extender Network mode, SSL Network Extender Application Mode, Secure Workspace and Compliance Scanner, refer to [sk113410](#).
2. Secure Workspace and SSL Network Extender Application Mode are available for Windows platforms only.

Identity Awareness Requirements

Identity Clients

See [sk134312](#).

AD Query

Supported Active Directory versions:

- Microsoft Windows Server 2022.
- Microsoft Windows Server 2019.
- Microsoft Windows Server 2016.
- Microsoft Windows Server 2012 R2.
- Microsoft Windows Server 2012.
- Microsoft Windows Server 2008 R2.

Browser-Based Authentication (Captive Portal)

You must use one of these web browsers:

- Microsoft Edge
- Google Chrome
- Apple Safari
- Mozilla Firefox
- Opera for Windows

Endpoint Security Management Server Requirements

Hardware Requirements

These are the minimum requirements to enable Endpoint Security management on a Security Management Server:

Component	Requirement
Number of CPU cores	4
Memory	16 GB
Disk Space	845 GB

The requirements for dedicated Endpoint Security Management Servers are similar.

Resource consumption is based on the size of your environment. For larger environments, more disk space, memory, and CPU are required.

Software Requirements

For more information, see the [R82.10 Endpoint Web Management Administration Guide](#).

- Endpoint Security Management Servers (the "Network Policy Management" Software Blade) are supported on the Check Point Management-only appliances or on Open Servers.

Endpoint Security Management Servers do not support Standalone (Security Gateway + Management Server) and Multi-Domain Security Management deployments.

- For information about the versions of Endpoint Security Clients that the R82.10 Endpoint Security Management Server can manage, see [sk117536](#).
- For supported Endpoint Security Clients for each OS version, see the [Endpoint Security EPMaaS Administration Guide](#) > section "Supported Operating Systems for the Endpoint Client".

Anti-Malware Signature Updates

- To allow Endpoint Security clients to get Anti-Malware signature updates from a cleanly installed R82.10 Primary Endpoint Security Management Server, follow the instructions in the [R82.10 Endpoint Web Management Administration Guide](#) when you select the Anti-Malware component.
- Endpoint Security Clients can continue to acquire their Anti-Malware signature updates directly from an external Check Point signature server or other external Anti-Malware signature resources, if your organization's Endpoint Anti-Malware policy allows it.

Scalable Platforms Requirements

Software Requirements

See *"Supported Security Gateway Versions in R82.10" on page 43*.

- To manage an R82.10 Security Group in the ElasticXL configuration, use:
 - R82.10 Security Management Server or Multi-Domain Server.
- To manage an R82.10 Security Group in the Maestro configuration, use:
 1. R82.10 Maestro Orchestrator.
For the list of supported Maestro Security Appliances, see [sk181433](#).
 2. R82.10 Security Management Server or Multi-Domain Server.
- To manage an R82.10 Virtual Gateway in the VSNext configuration (supported in Maestro or ElasticXL), use:
 - R82.10 Security Management Server or Multi-Domain Server.
- For the list of compatible transceivers for Check Point Appliances, see [sk92755](#).

Supported Network Cards on Maestro Security Appliances

To connect a Maestro Security Appliance to Maestro Orchestrators with **DAC cables**, you must install one of the supported Line Cards in the Maestro Security Appliance.

- See [sk181433](#) for the list of supported Maestro Security Appliances and Line Cards.
- See [sk158652](#) for the mandatory guidelines.

Maximum Supported Items in R82.10

This section provides the maximum supported numbers for various hardware and software items.

Management Server

Item	Maximum Number	Hard Limit	Comment															
Network objects in all Domains	1,000,000	Yes	This applies to objects of these types - Security Gateway, Cluster, Network, Host, Group, Network Feed, Address Range, Dynamic Object, Wildcard Object, Security Zone, LSV Profile, Domain, Interoperable Device, VoIP Domain, Logical Server, OSE Device, Access Point Name.															
Network objects in each Domain	100,000	No																
Security Gateway objects in each Domain	1500	No	The maximum supported number of the managed Security Gateways and Cluster Members depends on the installed RAM and the number of CPU cores on the Management Server: <table><tr><th>Number of available CPU Cores</th><th>Amount of installed RAM</th><th>Maximum supported number of the managed Security Gateways</th></tr><tr><td>32</td><td>96 GB</td><td>1500</td></tr><tr><td>16</td><td>96 GB</td><td>1500</td></tr><tr><td>6</td><td>32 GB</td><td>1500</td></tr><tr><td>6</td><td>16 GB</td><td>250</td></tr></table>	Number of available CPU Cores	Amount of installed RAM	Maximum supported number of the managed Security Gateways	32	96 GB	1500	16	96 GB	1500	6	32 GB	1500	6	16 GB	250
Number of available CPU Cores	Amount of installed RAM	Maximum supported number of the managed Security Gateways																
32	96 GB	1500																
16	96 GB	1500																
6	32 GB	1500																
6	16 GB	250																

Item	Maximum Number	Hard Limit	Comment
Objects in each Group object	12,000	Yes	
Rules in each Access Control policy	28,000	Yes	To ensure optimal Security Gateway responsiveness, we recommend configuring a maximum of 20,000 rules in a policy. While the Security Gateway can support more rules than 20,000 rules, the smaller the number of rules in the installed policy, the more responsive the Security Gateway is.
Rules in each NAT policy	16,384	Yes	The maximum number of NAT rules in a policy is 16,384. For optimal performance, keep the number of rules in the installed policy as low as possible. A large number of rules can affect Security Gateway responsiveness. Remove unused or disabled rules to stay within the supported limit.
Changes in one session	100	No	To ensure optimal Management Server responsiveness, we recommend making 100 or fewer changes in each session (although the Management Server can support more than 500 changes at a time).
Interfaces in each Security Gateway	200	No	To ensure optimal SmartConsole responsiveness, we recommend configuring a maximum of 200 interfaces in SmartConsole. If the Security Gateway object contains more interfaces, use the applicable Management API to configure interfaces. See the Check Point Management API Reference (at the top, select the correct version) . To ensure optimal API responsiveness, we recommend configuring a maximum of 600 interfaces with API.
Layers in Access Control Policy	251	Yes	The maximum number of Policy Layers in an Access Control Policy is 251.

Item	Maximum Number	Hard Limit	Comment
Change in IPS Protections	200	Yes	In SmartConsole > Security Policies view > Threat Prevention section > Custom Policy Tools panel > IPS Protections page, an operation performed on more than 200 protections is not supported.
Secondary Management Servers	None	No	The number of Secondary Management Servers is not limited by the code. The more Secondary Management Servers you install, the more resources the primary Management Server spends on the synchronization. This also applies to CloudGuard Controllers.

Item	Maximum Number	Hard Limit	Comment
Simultaneous administrator sessions	32,000 and 100	Yes	■ Limit for simultaneous connections per Domain: The theoretical maximum number of simultaneous unique administrator sessions per Domain is 32,000. This limit applies to the read-write sessions with SmartConsole and with Management API (in the local CLI and from a remote API client). Because of various components that handle all administrator sessions, the practical limit for simultaneous connections (read-write and read-only) to the management database is no more than several hundred. ■ Limit for simultaneous connections per administrator per Domain: The number of active read-write sessions is restricted to 100 sessions per administrator per Domain - see sk113955. An active session is a session that was not published and was not discarded. Because of various components that handle all administrator sessions, the practical limit for simultaneous read-only connections to the management database per administrator is no more than several hundred.

Item	Maximum Number	Hard Limit	Comment
			 Note - Follow these steps in SmartConsole to allow the same administrator to open and manage multiple sessions to the Management Server at the same time: 1. From the left navigation panel, click Manage & Settings. 2. Expand Sessions. 3. Click Advanced. 4. In the Session management section, select Each administrator can manage multiple SmartConsole sessions at the same time. 5. Publish the session.

Sizing Recommendations for Check Point Management Server

See [sk178325](#).

Maximum Supported Number of Interfaces on Security Gateway

This table shows the maximum supported number of interfaces (physical and virtual).

Note - This table applies to all hardware platforms - physical and virtual.

Mode	Max # of Interfaces	Notes
Security Gateway	1024	Non-VSX mode. See "Security Gateway or Cluster" on page 24 .
ElasticXL Cluster in the VSNext mode, Maestro Security Group in the VSNext mode	4096	See "VSNext and Traditional VSX" on page 26 .
Virtual Gateway in the VSNext mode	4096	Includes physical, VLAN, and Warp Interfaces. See "VSNext and Traditional VSX" on page 26 .
VSX Gateway in the Traditional VSX mode	4096	Includes physical, VLAN, and Warp Interfaces. See "VSNext and Traditional VSX" on page 26 .
Virtual System in the Traditional VSX mode on a VSX Gateway	64	Includes physical, VLAN, and Warp Interfaces.
Virtual System in the Traditional VSX mode on a VSX Cluster	256	Includes physical, VLAN, and Warp Interfaces. In a VSX Cluster, the default maximum is 64 interfaces. To increase it, see sk99121 .

Maximum Supported Number of Cluster Members

Cluster Type	Maximum Supported Number of Cluster Members
ClusterXL High Availability or Load Sharing	5
ClusterXL Active-Active	4
ElasticXL	3 on each Site (6 in total in Dual Site)
Geo Cluster	2
Virtual System Load Sharing in the Traditional VSX mode	13

Number of Supported Items in an ElasticXL Cluster

Item	Number of Supported Items	Notes
Number of Security Appliances in one ElasticXL Cluster	In Single Site and Dual Site deployment: ■ Minimum: 1 on each Site ■ Maximum: 3 on each Site	In a Dual Site deployment, an ElasticXL Cluster must contain a minimum of one Security Appliance from each site.
Number of interfaces configured in one ElasticXL Cluster	In the Security Gateway Mode: ■ Minimum: 2 ■ Maximum: 1024 For each Virtual Gateway in the VSNext Mode: ■ Minimum: 2 ■ Maximum: 1024	Includes all interface types (Physical, Bonds, VLAN, Warp).

Number of Supported Items in a Maestro Environment

Item	Number of Supported Items	Notes
Number of Security Groups configured	- Minimum: 1 - Maximum: 8	None
Number of Security Appliances in one Security Group	In Single Site and Dual Site deployment: - Minimum: 1 - Maximum: 28	In Dual Site environments: - Each Security Group must contain a minimum of one Security Appliance from each site (see MBS-7606 in sk183507). - Each Security Group can contain a maximum of 28 Security Appliances - 14 Security Appliances from each site (see MBS-7773 in sk183507).
Number of interfaces configured on top of Uplink ports in one Security Group	In the Security Gateway Mode and in the VSNext Mode: - Minimum: 2 - Maximum: 1024 In the Traditional VSX Mode: - Minimum: 2 - Maximum: 4096 For each Virtual System in the Traditional VSX Mode: - Minimum: 2 - Maximum: 250	Includes all interface types (Physical, Bonds, VLAN, Warp).

Build Numbers in R82.10

Software Component	Build Number	Verifying Build Number
Gaia	OS Build 464 OS kernel version 5.14.0-427.13.1cpx86_64 OS edition 64-bit	Run this command in Gaia Clish: <code>show version all</code>
Security Gateway	R82.10 - Build 767	Run this command in the Expert mode: <code>fw ver</code>
Security Management Server	R82.10 - Build 317	Run this command in the Expert mode: <code>fwm ver</code>
Multi-Domain Server	R82.10 - Build 432	Run this command in the Expert mode: <code>fwm mds ver</code>
SmartConsole	82.10.9900.408	Click Menu > About Check Point SmartConsole

Licensing

For all licenses issues contact [Check Point Account Services](#).