

04

October

2023

**QUANTUM**

**CYBER**

**SECURITY**

**PLATFORM**

**R82**

Early

Availability

Release

Notes

# Check Point Copyright Notice

© 2023 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](https://www.checkpoint.com/copyright/) [page](https://www.checkpoint.com/copyright/) for a list of our trademarks.

Refer to the [Third](https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/) [Party](https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/) [copyright](https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/) [notices](https://www.checkpoint.com/about-us/third-party-trademarks-and-copyrights/) for a list of relevant copyrights and third-party licenses.

# Table of Contents

What's New 6

Introduction 6

Threat Prevention 6

Web Security 6

Automatic

Zero

Phishing

Configuration

6

Improved

Threat

Prevention

Capabilities

6

HTTPS

Inspection

7

Quantum Security Gateway 8

|  |  |
| --- | --- |
|  |  |
| New Clustering Technology | 8 |
| Dynamic Policy Layer | 8 |

Central Unified Configuration 8

Identity Awareness8

|  |  |
| --- | --- |
| IPsec VPN | 8 |
| Remote Access VPN | 9 |
| Mobile Access | 9 |

|  |  |
| --- | --- |
| Gaia Operating System | 9 |
| Dynamic Routing | 10 |

Performance and Infrastructure 10

|  |  |
| --- | --- |
| VSX | 11 |
| Tools and Utilities | 11 |

Maestro Hyperscale 10

Quantum

Security

Management

12

Security

Management

Server

Enhancements

12

Central

Deployment

of

Hotfixes

and

Version

Upgrades

in

SmartConsole

12

SmartProvisioning

12

Multi-

Domain

Security

Management

Server

12

Compliance

13

CloudGuard Network Security 13

CloudGuard Controller 13

CloudGuard Network 13

Harmony Endpoint 14

Software Changes 15

Gaia Operating System 15

VSX 15

VPN 15

Management Server 15

|  |  |
| --- | --- |
|  |  |
| Scalable Platforms | 15 |
| Supported Environments | 16 |

16

Management

Server

and

Log

Server

Security

Gateway

or

Cluster

Standalone

(

Gateway

+

Management

Server)

Threat

Emulation

Appliances

17

18

19

|  |  |
| --- | --- |
| Quantum Maestro | 19 |
| User Space Firewall (USFW) | 20 |
| Virtualization Platforms | 21 |

Cloud Platforms 22

Supported Upgrade Paths 24 Installation Methods 24

Upgrade Paths 24

Upgrade Methods 27

Supported

Security

Gateway

Versions

32

Management

Server

and

Security

Gateway

Versions

32

Quantum

Maestro

Orchestrator

and

Security

Group

Versions

33

Open

Server

Hardware

Requirements

34

Minimum

Hardware

Requirements

34

Disk

Space

Requirements

35

Maximum

Supported

Physical

Memory

35

Requirements

36

Threat

Extraction

Requirements

for

Web-

downloaded

Documents

36

Logging

Requirements

36

|  |  |
| --- | --- |
| SmartEvent Requirements | 36 |
| SmartConsole Requirements | 37 |
| Hardware Requirements | 37 |

SmartConsole Software Requirements 37

Gaia Portal Requirements37

Mobile Access Requirements 38

Identity Awareness Requirements 40

Identity Clients40

AD Query 40

40

Hardware Requirements 40

Harmony

Endpoint

Management

Server

Requirements

Software Requirements 40

Anti-

Malware

Signature

Updates

41

Scalable

Platform

Requirements

42

Supported

Network

Cards

on

Maestro

Security

Appliances

43

Supported

Hardware

and

Firmware

on

60000

/

40000

Scalable

Chassis

44

Maximum

Supported

Items

45

Maximum

Supported

Number

of

Interfaces

on

Security

Gateway

45

Maximum

Supported

Number

of

Cluster

Members

45

Number

of

Supported

Items

in

a

Maestro

Environment

46

Supported

Clients

and

Agents

47

Check

Point

Clients

and

Agents

for

Windows

OS

47

Check

Point

Clients

and

Agents

for

macOS

48

Check

Point

DLP

Exchange

Security

Agent

49

Licensing

50

# What's New

## Introduction

Introducing Check Point Software Technologies' groundbreaking release, R82 “Aurora”. This cutting-edge software marks a pivotal moment in cybersecurity with many innovative features. R82 ushers in a new era of web security, offering complete protection for HTTP/3 over QUIC, setting an industry precedent. Moreover, it presents the world's first firewall tailored for effortless HTTPS Inspection deployment while maintaining exceptional performance. Not stopping there, R82 delivers an enhanced operational experience with simplified cluster deployment through ElasticXL and a versatile new VSX mode. The software, in addition, boasts a new version of the operating system with superior networking and routing capabilities. Additionally, R82 takes automation to new heights, allowing full dynamic policy layer configuration through API calls directly to the Security Gateway.

Stay ahead of the curve with R82 "Aurora" and experience the future of cybersecurity management and protection.

## Threat Prevention

### Web Security

n Added support of HTTP/3 protocol over QUIC transport (UDP) for Network Security, Threat Prevention and Sandboxing.

### Automatic Zero Phishing Configuration

n Introducing a new addition to the Zero Phishing Software Blade - the Automatic mode. The Automatic mode significantly simplifies the configuration process, providing a seamless experience. With the Automatic mode, the blade configuration is now effortless: simply enable the Software Blade, and you are ready to go.

### Improved Threat Prevention Capabilities

* Added configuration granularity for advanced DNS protections in Threat Prevention. n Added Advanced DNS protection against NXNS Attack.
* New Anti-Bot engine that prevents zero-day attacks based on the destination IP address and Port number.
* Added Advanced DNS capability to block DNS queries to newly created domains. n DNS Security statistics are now available in the SmartView Dashboard.
* It is now possible to load SNORT rules file as Custom Intelligence Feed automatically with 5-minute intervals to enforce them as IPS protections.

### HTTPS Inspection

This release brings a significant milestone in performance, simplicity, and deployment of HTTPS Inspection. These capabilities allow customers to implement HTTPS Inspection without compromising performance and user experience.

* Full Fail-open mode - A new capability that automatically detects a failure in the HTTPS Inspection process because of client-side issues such as pinned certificates. When detected, the connection is automatically added to an exception list, ensuring zero connectivity issues for end-users.
* Deployment assessment - Allows customers to gradually deploy HTTPS to a portion of the traffic (up to 30%), predicts the performance, and automatically detects and resolves connectivity issues. n Bypass under load - Optionally bypass HTTPS Inspection in case of high CPU load.
* HTTPS Inspection monitoring - Inspection status overview and detailed advanced HTTPS

Inspection statistics.

* Enhanced HTTPS Inspection policy - An improved HTTPS policy with a default recommended inspection policy, separate inbound and outbound rules, and multiple outbound certificate support.

## Quantum Security Gateway

### New Clustering Technology

n ElasticXL - a new clustering technology delivering simplified operations with a Single Management Object and automatic sync of configuration and software between all cluster members.

### Dynamic Policy Layer

n Fully automated, API-controlled policy layer that allows dynamic policy changes to be implemented directly to the Security Gateway in seconds without involving Security Management.

### Central Unified Configuration

n Kernel parameters configuration is now performed in centralized database with Gaia Clish commands and Gaia REST API calls instead of fwkern.conf and simkern.conf files. See the

local Gaia API Reference at https://<IP Address of Gaia Management Interface>/gaia\_docs/#introduction.

### Identity Awareness

* Quantum Gateways can now use Identity Providers defined in the Check Point Infinity Portal, allowing customers to centrally manage identities across multiple Check Point products.
* Introducing a new mode for Identity Awareness Blade - "PDP-Only", where the Security Gateway acts only as Policy Decision Point (PDP) for identity acquisition and distribution and does not enforce the identity-based policy. The new mode improves scalability for PDPs and Identity Broker.
* Introduced Identity Sharing cache mode to improve resiliency in case of connectivity loss with the PDP.

### IPsec VPN

* Automatically detect configuration changes in AWS, Azure, and GCP public clouds and adjust the VPN settings ensuring connection stability.
* Introducing the Advanced VPN Monitoring tool that shows information on each VPN Tunnel and tracks its health and performance.
* Enhanced Tunneling:
  + Added support for Dead Peer Detection (DPD) with Link Selection.
  + Support for Tunnel IP address that is different from the Gateway Main IP, for enhanced interoperability with third-party vendors.
  + Introducing the capability to configure distinct external interfaces for different communities, enabling greater granularity.
  + Allow ISP links redundancy with third-party and cloud vendors VPN peers.

### Remote Access VPN

n Security Gateway now supports the IKEv2 protocol for connections from Remote Access VPN Clients (E87.70 and higher for Windows OS and E87.80 and higher for macOS).

### Mobile Access

* Mobile Access Policy and Capsule Workspace configurations are now available in SmartConsole.
* SAML authentication support for Mobile Access clients that allows seamless integration with thirdpartyIdentity Providers.
* New Management API calls for Capsule Workspace configuration.

### Gaia Operating System

This release boosts Gaia OS with a new OS kernel and multiple new configuration options for better security, enhanced networking, and a simpler experience.

The new capabilities are:

* Support for VSX mode in Gaia Link Layer Discovery Protocol (LLDP). n Support for DHCPv6 server, DHCPv6 client and DHCPv6 client for prefix-delegation.
* Support for DNS Proxy forwarding domains, which allows configuring specific DNS servers per DNS suffix. n Ability to configure the keyboard layout in Gaia Clish and Gaia Portal. n Ability to configure NTP pools and a greater number of NTP servers. n Support for NFSv4 configuration in Gaia Portal, Gaia Clish, and Gaia REST API calls. n Support for storing a Gaia OS backup to and restoring it from Amazon S3 and Microsoft Azure.
* Ability to configure the order of the "AAA" authentication (TACACS, RADIUS, Local authentication) in Gaia Portal and Gaia Clish.
* Added a Gaia Clish command "set dns timeout <value>" to control how long Gaia OS waits for a response from a DNS server before it sends the DNS request to the next configured DNS server.

### Dynamic Routing

Added support for new Dynamic Routing capabilities: n BGP Extended Communities (RFC 4360).

* BGP Conditional Route Advertisement and Injection.
* Routing Table Monitor for Event Triggers. n IPv4 and IPv6 Router Discovery on cluster members. n Router Preference and Route Information option. n IPv4 PIM-SSM with non-default prefixes. n IPv4 PIM with BFD. n IPv4 PIM neighbor filtering. n IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).
* REST API calls for BGP, PIM, Multicast Listener Discovery (MLD).
* REST API calls for Route Redistribution, Inbound Route Filters, and NAT Pools.
* REST API calls for IGMP.

See the [Gaia](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html) [API](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html) [Reference.](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html)

### Performance and Infrastructure

n Quantum Security Gateway multi-core utilization for log sending, improving log output capacity by up to 100%.

### Maestro Hyperscale

This release features improvements in managing and monitoring Maestro Hyperscale clusters, which include: n Support for SNMP Query on each Security Group Member..

n REST API on Quantum Maestro Orchestrator and ElasticXL Cluster Members:

* New Quantum Maestro Orchestrator API calls for configuration and monitoring of Security Groups, Gateways, Sites, and Ports.
* Support per member Gaia REST APIs for Quantum Maestro and ElasticXL Cluster Members.

See the complete list of available API calls in the [Gaia](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html) [API](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html) [Reference](https://sc1.checkpoint.com/documents/latest/GaiaAPIs/index.html).

### VSX

Check Point VSX is enhanced with a new mode, allowing simpler configuration, easier provisioning, and a similar experience to a physical Security Gateway.

The benefits of the new VSX mode are:

* Unified management experience between Check Point physical Security Gateways and Virtual Gateways, including the capability to manage each Virtual Gateway from a different Management Server.
* Improves VSX provisioning performance and provisioning experience - creating, modifying, and deleting Virtual Gateways and Virtual Switches in Gaia Portal, Gaia Clish, or with Gaia REST API.
* Management feature and API parity between Virtual Gateways (VGW) and physical Security Gateways.

### Tools and Utilities

* ConnView - a new consolidated troubleshooting tool for viewing connections information on the Security Gateway.
* New policy advisory tool up\_execute, which performs virtual Access / NAT Rule Base execution. Given inputs based on logs or connections, the execution provides detailed information such as matched rules and classification information.

## Quantum Security Management

### Security Management Server Enhancements

* The LDAP Account Unit object now uses the LDAP server name and CA certificate for LDAP trust.

The trust is automatically renewed if an administrator renews or replaces the LDAP server certificate. As a result, Check Point servers keep their connectivity to the LDAP server.

* Support for Management API to run the "vsx\_provisioning\_tool" operations to configure VSX Gateway and VSX Cluster objects. See the[CheckPointManagementAPIReference.](https://sc1.checkpoint.com/documents/latest/APIs/index.html)
* Upgraded the SmartConsole.NET framework from 4.5 to 4.8.

### Central Deployment of Hotfixes and Version Upgrades in SmartConsole

Central Software Deployment through SmartConsole was enhanced and now supports:

* Uninstall of Jumbo Hotfix Accumulators.
* Installation of packages on ClusterXL High Availability mode in the "Switch to higher priority Cluster Member" configuration ("Primary Up"). n Installation of packages on Secondary Management Servers.
* Installation of packages on Dedicated Log Servers. n Installation of packages on Dedicated SmartEvent Servers. n Installation of packages on Clusters of Quantum Spark and Quantum Rugged Appliances. n Installation of packages from Standalone Servers.
* Package Repository per Domain on a Multi-Domain Security Management Server.

### SmartProvisioning

n Star VPN Community now supports Quantum Maestro Security Groups, VSX Gateways, and VSX Clusters as Center Gateways (Corporate Office Gateway).

### Multi-Domain Security Management Server

* Ability to clone an existing Domain on the same Multi-Domain Security Management Server. See [sk180631](https://support.checkpoint.com/results/sk/sk180631).
* Improved upgrade time of large Multi-Domain Security Management Server environments by up to 50%.

### Compliance

* Added support for Quantum Maestro and Quantum Spark Appliances:
  + Gaia OS Best Practice support for Maestro Security Groups by checking each Security Group Member individually and presenting a consolidated Best Practices status. l Applying relevantGaia OS Best Practices on Quantum Spark Appliances.
* Added Gaia OS Best Practice support for Log Servers.
* Added new regulations:
  + Cyber Essentials v3.1 regulation l Israeli Cyber Defense Methodology 2.0

## CloudGuard Network Security

### CloudGuard Controller

* CloudGuard Controller support for Identity Awareness PDP (Identity Sharing).
* CloudGuard Controller for VMware NSX-T now uses Policy Mode APIs to import objects from an NSX-T Manager.
* CloudGuard Controller for VMware NSX-T can import Virtual Machines and Tags from an NSX-T Manager.
* Multi-Domain Security Management Server now supports Data Center objects and Data Center Query objects in the Global Policy.

CloudGuard Network

* New Management API calls for CloudGuard Central License utility.

## Harmony Endpoint

Harmony Endpoint Web Management enhancements:

* Client optimization for Windows servers - Harmony Endpoint allows you to easily optimize the Endpoint Security clients for Windows servers, such as Exchange servers, Active Directory servers, Database servers, and so on, by manually assigning Windows server roles.
* Run Diagnostics:
  + Runs performance checks on endpoint clients using Push Operation.
  + The performance report presents each client's CPU and RAM utilization, including the editable threshold. l Harmony Endpoint presents suggested exclusion for performance improvements.
  + You can easily add an exclusion as part of "Global Exclusion" or "Exclusion per Rule": o Exclusion description - You can now add comments for new or existing exclusions.

o Global Exclusion - You can now easily add global exclusion that applies to all rules.

* Application Control for macOS - Control which applications can run or use networking.
* New Asset Management view:
  + Filters - A brand new look and functionality for filters that enhances operation and productivity, while using the Asset Management view. l Asset Management Table - Bigger asset management table to see all relevant data easily.
  + Columns reorder - New Column reorder option to customize the asset management table based on their specific needs by changing columns location.
* Linux Offline Package - Supports upload and export package for Linux OS clients.
* Added Harmony Endpoint Management API to support on-premises Endpoint Security Management Server.

The API is disabled by default for on-premises deployments. See the [Harmony](https://app.swaggerhub.com/apis/Check-Point/web-mgmt-external-api-production) [Endpoint Management](https://app.swaggerhub.com/apis/Check-Point/web-mgmt-external-api-production) [API](https://app.swaggerhub.com/apis/Check-Point/web-mgmt-external-api-production) [article](https://app.swaggerhub.com/apis/Check-Point/web-mgmt-external-api-production).

Software Changes

# Software Changes

 Note - To see the list of changes starting R80.40, see [sk180180](https://support.checkpoint.com/results/sk/sk180180).

This section describes behavior changes from the previous version.

Gaia Operating System

n Updated the Gaia OS Linux kernel version to 4.18.

## VSX

* The default value for concurrent connections in the Virtual System object was increased from 15,000 to 50,000 (Optimizationssection >CapacityOptimizationpage).
* In the VSNext mode, the Expert mode command "clish -c" now supports the context of a Virtual Gateway / Virtual Switch with this syntax:

clish -v <*Virtual Device ID*> -c "<*Gaia Clish Command*>"

## VPN

n When a Check Point Management Server creates an IKE certificate, by default this certificate contains the "Server Authentication" attribute within the "Extended Key Usage" field.

## Management Server

n The default minimum TLS version was changed from TLS1.0 to TLS1.2 in the following Check Point communication types:

* SIC communication between a Management Server and all managed servers and gateways.
* SSL communication to the TCP port 18265 on a Management Server (the ICA Management

Tool).

* SSL communication to the TCP port 18194 on a Security Gateway configured for Local Threat Emulation.

## Scalable Platforms

* On the Maestro Orchestrator MHO-175 ports, increased the default MTU size from 9216 to 10240 bytes.
* On a Maestro Security Group, in the output of the "asg if" command, the column header changed from "Link State (ch1)/(ch2)" to "Link State (site1)/(site2)".

# Supported Environments

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

 Note - If after the upgrade to R82 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.

Refer to the [Support](https://www.checkpoint.com/support-services/support-life-cycle-policy/) [Life](https://www.checkpoint.com/support-services/support-life-cycle-policy/) [Cycle](https://www.checkpoint.com/support-services/support-life-cycle-policy/) [Policy](https://www.checkpoint.com/support-services/support-life-cycle-policy/) page for more information and announcements about Check Point Appliances.

## Management Server and Log Server

These platforms support R82 in the Management Server and Log Server configurations:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Check Point Product | Smart-1 5050,  5150,  6000-L, 6000XL | Smart-1 405,  410, 525,  625, 600-S, 600-  M | Open  Servers | Virtual  Machines (\*) |
| Security  Management  Server  Log  Server  SmartEvent  Server  Multi-  Domain  Security  Management  Server  Multi-  Domain  Log  Server |  |  |  |  |

(\*) Applies to Public Cloud and to Private Cloud. See the[HardwareCompatibilityList](https://www.checkpoint.com/support-services/hcl/)> Section Virtual Machines.

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.

## Security Gateway or Cluster

Only these platforms support R82 in the Security Gateway or Cluster configuration:

|  |  |
| --- | --- |
| Platforms | Security Gateway,  Cluster |
| MLS200  ,  MLS400  QLS250  ,  QLS450  ,  QLS650  ,  QLS800  28600  HS  26000  ,  26000  T  23500  ,  23800  ,  23900  16000  ,  16200  ,  16600  HS  ,  16600  T  15400  ,  15600  7000  6200  ,  6400  ,  6500  ,  6600  ,  6700  ,  6800  ,  6900  5100  ,  5200  ,  5400  ,  5600  ,  5800  ,  5900  3100  ,  3200  ,  3600  ,  3800  64000  ,  44000  (1)  Open  Servers  Virtual  Machines  (2) |  |

1. R82 supports only SSM440 and SGM400 in Scalable Chassis.
2. Applies to Public Cloud and to Private Cloud. See the[HardwareCompatibilityList](https://www.checkpoint.com/support-services/hcl/)> Section Virtual Machines.

## Standalone (Gateway + Management Server)

Only these platforms support R82 in the Standalone configuration:

|  |  |
| --- | --- |
| Platforms | Standalone |
| 23500, 23800, 23900 | (2) |
| 16000, 16200, 16600T  The model 16600HS does not support Standalone  15400  ,  15600 | (2) |
| 7000  6200  ,  6400  ,  6600  ,  6700  ,  6900  The  models  6500  ,  6800  do  not  support  Standalone  5900  5100  ,  5200  ,  5400  ,  5600  ,  5800  3100  ,  3200  ,  3600  ,  3800  Open  Servers  Virtual  Machines  (1) | (2) |

1. Applies to Public Cloud and to Private Cloud. See the[HardwareCompatibilityList](https://www.checkpoint.com/support-services/hcl/)> Section Virtual Machines.
2. These appliance models support Standalone only with the HDD storage.

These appliance models do not support Standalone with the SSD storage.

To see the disk type

* 1. Connect to the command line.
  2. Log in to the Expert mode.
  3. Get the list of disk device names: fdisk -l | grep '/dev/'

In the output, refer to the name of the disk device (sda, sdb, and so on).

* 1. Run this command for your disk device (sda, sdb, and so on):

cat /sys/block/<*DISK\_DEVICE\_NAME*>/queue/rotational Example:

cat /sys/block/sda/queue/rotational

* 1. The returned value:

n 1 - means this disk is HDD n 0 - means this disk is SSD

## Threat Emulation Appliances

|  |  |
| --- | --- |
| Platform | Security Gateway,  Cluster |
| TE2000XN  TE2000X  TE1000X  TE250XN  TE250X  TE100X |  |

## Quantum Maestro

Quantum Maestro Orchestrator models MHO-140, MHO-170, and MHO-175 fully support the R82 release.

For the list of supported Security Appliances in a Maestro Security Group, see [sk162373.](https://support.checkpoint.com/results/sk/sk162373)

## User Space Firewall (USFW)

Security Gateways on these platforms run in the User Space Firewall mode by default:

|  |  |
| --- | --- |
| Platform | USFW |
| MLS200  ,  MLS400  QLS250  ,  QLS450  ,  QLS650  ,  QLS800  28000  ,  28600  HS  26000  ,  26000  T  23900  16000  ,  16000  T  ,  16200  ,  16600  HS  7000  6200  B  ,  6200  P  ,  6200  T  ,  6400  ,  6600  ,  6700  ,  6900  3600  ,  3600  T  ,  3800  Open  Servers  (1)  Virtual  Machines  (2)  CloudGuard  Network  Security  for  Public  Cloud  (3)  CloudGuard  Network  Security  for  Private  Cloud  (3) |  |

1. Open Server must have 40 or more CPU cores.
2. Virtual Machine must have 40 or more virtual CPU cores.

Applies to Public Cloud and to Private Cloud.

1. CloudGuard Network Virtual Machines support USFW regardless of the number of available CPU cores.

 Notes:

n Security Gateways on all other Check Point appliance models run in the Kernel Space Firewall (KSFW) mode by default. n You can change the configuration from the Kernel Space Firewall (KSFW) mode to the User Space Firewall mode on these Check Point appliance models (see [sk167052](https://support.checkpoint.com/results/sk/sk167052)):

l 23800 l 15400, 15600 l 6500, 6800 l 5400, 5600, 5800, 5900

## Virtualization Platforms

For the most up-to-date information about the supported Linux versions and virtualization platforms, see the [HardwareCompatibilityList](https://www.checkpoint.com/support-services/hcl/)> Section Virtual Machines.

## Cloud Platforms

Supported setups for cloud solutions: n Amazon Web Services: l Security Gateway l Single Zone High Availability Cluster l Cross Availability Zone Cluster (Cross AZ Cluster) l Security Gateway Auto Scaling Group l Gateway Load Balancer Virtual Machine Scale Sets l Security Management Server l Multi-Domain Server l Standalone l VPC Endpoint objects. n Microsoft Azure: l Security Gateway l High Availability Cluster l Virtual Machine Scale Sets l Gateway Load Balancer Virtual Machine Scale Sets l Security Management Server l Multi-Domain Server l Standalone l Virtual WAN

* Google Cloud Platform (GCP): l Security Gateway l High Availability Cluster l Managed Instance Group (MIG) l Security Management Server l Multi-Domain Server l Standalone
* Oracle Cloud Infrastructure (OCI): l Security Gateway l High Availability Cluster l Security Management Server l Multi-Domain Server l Standalone
* Huawei Cloud: l Security Gateway l High Availability Cluster l Security Management Server l Standalone
* Tencent Cloud: l Security Gateway l High Availability Cluster l Security Management Server l Standalone

# Supported Upgrade Paths

## Installation Methods

* For Security Management Servers we recommend that you use the CPUSE option available in Gaia Portal. To learn more about CPUSE, see [sk92449](https://support.checkpoint.com/results/sk/sk92449).
* For Security Gateway upgrade, we recommend that you use the Central Deployment available in SmartConsole. See [sk168597](https://support.checkpoint.com/results/sk/sk168597).

## Upgrade Paths

* Note - For more information about Security Management Servers and supported managed Security Gateways see [sk113113.](https://support.checkpoint.com/results/sk/sk113113)

Upgrade to R82 is available only from these versions:

|  |  |  |  |
| --- | --- | --- | --- |
| Current Version | Security  Gateways and  VSX (1) | Management  Servers and  Multi-Domain Servers | Standalone |
| R81.20  ,  R81.10  ,  R81  ,  R80.40  For  Scalable  Platforms  :  R81.20  ,  R81.10  ,  R81 | (2) | Not  applicable | Not  applicable |
| For Scalable Platforms:  R80.30SP,  R80.20SP | Requires a 2step  upgrade path  (4) | Notapplicable | Notapplicable |
| R80.30 kernel 3.10,  R80.30 kernel 2.6,  R80.20 kernel 3.10,  R80.20 kernel 2.6 | Requires a 2step  upgrade path  (3) | Requires a 2step  upgrade path (3) | Requires a 2step  upgrade path  (3) |
| R80.20.M2, R80.20.M1 | Not  applicable | Requires a 2step  upgrade path (3) | Notapplicable |

|  |  |  |  |
| --- | --- | --- | --- |
| Current Version | Security  Gateways and  VSX (1) | Management  Servers and  Multi-Domain Servers | Standalone |
| R80.10 | Requires a 2step  upgrade path  (3)(6) | Requires a 2step  upgrade path (3) | Requires a 2step  upgrade path  (3)(6) |
| R80 | Not  applicable | Requires a 2step  upgrade path (3) | Notapplicable |
| R77.30 | Requires a 2step  upgrade path  (3)(5)(6) | Requires a 2step  upgrade path (3)  (5) | Requires a 2step  upgrade path  (3)(5)(6) |

* Notes:

1. Starting from R81.10, VSLS is the only supported mode for new installations of VSX Clusters (does not apply to the VSNext mode).

Upgrade of a VSX Cluster in the High Availability mode from R81.10 and earlier versions to R82 is supported.

To convert the upgraded VSX Cluster to VSLS, use the "vsx\_util to convert" command.

1. Upgrade from these versions to R82 is supported only with specific takes of a Jumbo Hotfix Accumulators.

In Maestro environment, it is possible to upgrade Security Groups and Quantum Maestro Orchestrators (if you decide to upgrade, you must upgrade both).

1. The required 2-step upgrade path is:
   1. To R80.40, R81, R81.10, or R81.20 See the applicable guide:
      * [R80.40InstallationandUpgradeGuide](https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Installation_and_Upgrade_Guide/Default.htm). n [R81InstallationandUpgradeGuide.](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Default.htm) n [R81.10InstallationandUpgradeGuide](https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_Installation_and_Upgrade_Guide/Default.htm).
      * [R81.20InstallationandUpgradeGuide](https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Installation_and_Upgrade_Guide/Default.htm).
   2. To R82
2. The required 2-step upgrade path is:
   1. To R81.10 or R81.20 for Scalable Platforms See the applicable article:
      * [sk173363](https://support.checkpoint.com/results/sk/sk173363) [-](https://support.checkpoint.com/results/sk/sk173363) [R81.10](https://support.checkpoint.com/results/sk/sk173363) [for](https://support.checkpoint.com/results/sk/sk173363) [Scalable](https://support.checkpoint.com/results/sk/sk173363) [Platforms](https://support.checkpoint.com/results/sk/sk173363) n [sk177624](https://support.checkpoint.com/results/sk/sk177624) [-](https://support.checkpoint.com/results/sk/sk177624) [R81.20](https://support.checkpoint.com/results/sk/sk177624) [for](https://support.checkpoint.com/results/sk/sk177624) [Scalable](https://support.checkpoint.com/results/sk/sk177624) [Platforms](https://support.checkpoint.com/results/sk/sk177624)
   2. To R82
3. To upgrade an R77.30 environment that implements Carrier Security (former Firewall-1 GX), you must follow [sk169415.](https://support.checkpoint.com/results/sk/sk169415)
4. Before you start the upgrade, you must make sure the Gaia OS edition is 64-bit:
   1. Get the current Gaia OS edition with this Gaia Clish command: show version all
   2. If the Gaia OS edition is "32-bit", run these Gaia Clish commands: set edition 64-bit save config reboot

## Upgrade Methods

Use these methods to upgrade your Check Point environment to R82:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Check Point Product | Central  Deployment  in  SmartConsole  (1) | CPUSE  Upgrade  (2) | CPUSE  Clean  Install (3) | Advanced Upgrade (4) | Upgrade with  Migration  (5) | Upgrade with CDT  (6) |
| Security  Gateways  VSX  Gateways  Security  Group  Members Maestro  Security  Group  Members -  Scalable Chassis  ClusterXL Members in the High  Availability  modes  ClusterXL Members in the Load Sharing modes  VSX Cluster Members  VRRP Cluster Members  Primary  Security  Management  Server |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Check Point Product | Central  Deployment  in  SmartConsole  (1) | CPUSE  Upgrade  (2) | CPUSE  Clean  Install (3) | Advanced Upgrade (4) | Upgrade with  Migration  (5) | Upgrade with CDT  (6) |
| Secondary  Security  Management  Server  Primary MultiDomain  Security  Management  Server  Secondary  Multi-Domain  Security  Management  Server  Primary MultiDomain Log  Server  Secondary  Multi-Domain Log Server  Primary  CloudGuard  Controller  Secondary  CloudGuard  Controller  Primary  Endpoint  Security  Management  Server  Secondary  Endpoint  Security  Management  Server  Dedicated Log  Server |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Check Point Product | Central  Deployment  in  SmartConsole  (1) | CPUSE  Upgrade  (2) | CPUSE  Clean  Install (3) | Advanced Upgrade (4) | Upgrade with  Migration  (5) | Upgrade with CDT  (6) |
| Dedicated  SmartEvent Server  Full High  Availability  Cluster  Members  Standalone  Server |  |  |  |  |  |  |

 Notes:

1. 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.
   * For instructions, see the[R82SecurityManagementAdministrationGuide](https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Default.htm).
2. 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.
   * For instructions, see the[R82InstallationandUpgradeGuide.](https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Installation_and_Upgrade_Guide/Default.htm)
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:
     1. Export the data before the installation.
     2. Import the data after the installation.
   * For instructions, see the[R82InstallationandUpgradeGuide.](https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Installation_and_Upgrade_Guide/Default.htm)
4. Advanced Upgrade:
   * Intended for Management Servers only. n 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:
     1. Export of the current management database from the server.
     2. Upgrade of the server with CPUSE (In-place Upgrade or Clean Install).
     3. Import of the exported management database.
   * For instructions, see the[R82InstallationandUpgradeGuide.](https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Installation_and_Upgrade_Guide/Default.htm)
5. Upgrade with Migration:
   1. Intended for Management Servers only.
   2. You export of the current management database from the server.
   3. You install a different server with a higher version (Clean Install).
   4. You import of the exported management database.
   5. For instructions, see the[R82InstallationandUpgradeGuide.](https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_Installation_and_Upgrade_Guide/Default.htm)
6. Upgrade with CDT (Central Deployment Tool):
   * Intended for Security Gateways and Cluster Members only. n 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. n You can install the package on several targets at the same time. n For more information, see [sk111158.](https://support.checkpoint.com/results/sk/sk111158)

7. 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:

n At least 20 GB of free disk space is required in the root partition for an Upgrade to succeed. n At least 10 GB of free disk space is required in the /var/log partition for a Clean Install or Upgrade to succeed.

Supported Security Gateway Versions

# Supported Security Gateway Versions

## Management Server and Security Gateway Versions

* Note - For more information about Security Management Servers and supported managed Security Gateways see [sk113113.](https://support.checkpoint.com/results/sk/sk113113)

R82 Management Servers can manage Security Gateways that run these versions:

|  |  |
| --- | --- |
| Gateway Type | Release Version |
| Security Gateway and VSX | R82, R81.20, R81.10, R81,  R80.40, R80.30, R80.20, R80.10 |
| Security Groups on Maestro | R82, R81.20, R81.10, R81, R80.30SP, R80.20SP |
| Security Groups on Scalable Chassis | R82, R81.20, R81.10, R81, R80.20SP |
| Quantum Spark, Quantum Rugged, and SMB Appliances | R81.10.x,  R80.20.x,  R77.20.8x |

* Note - Management Servers version R81.10 and lower cannot manage R82 Security Gateways / Security Groups / Clusters.

Supported Security Gateway Versions

## Quantum Maestro Orchestrator and Security Group Versions

R82 Quantum Maestro Orchestrator can manage Maestro Security Groups that run these versions: n R82

n R81.20 (see [sk177624](https://support.checkpoint.com/results/sk/sk177624)) n R81.10 (see [sk173363](https://support.checkpoint.com/results/sk/sk173363)) n R81 (see [sk169954](https://support.checkpoint.com/results/sk/sk169954)) n R80.30SP (see [sk162552](https://support.checkpoint.com/results/sk/sk162552)) n R80.20SP (see [sk138233](https://support.checkpoint.com/results/sk/sk138233))

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

Open Server Hardware

# Open Server Hardware Requirements

## Minimum Hardware Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Check Point Product | Processor | Total CPU cores | Memory |
| Security Management Server | Intel Pentium IV, 2 GHz or equivalent | 2 | 8 GB |
| Multi-Domain Server | Intel Pentium IV, 2.6 GHz or equivalent | 8 | 32 GB |
| Security Gateway | Intel Pentium IV, 2 GHz or equivalent | 2 | 4 GB |
| VSX | Intel Pentium IV, 2 GHz or equivalent | 2 | 4 GB |
| Standalone | Intel Pentium IV, 2.6 GHz or equivalent | 4 | 8 GB |



For the SmartEvent requirements, see"SmartEventRequirements"onpage 36.

Open Server Hardware

## Disk Space Requirements

|  |  |  |
| --- | --- | --- |
| Check Point Product | Recommended free disk space | Minimum free disk space (\*) |
| Security Management Server | 1 TB | 110 GB |
| Multi-Domain Server | 1 TB | For the Multi-Domain Server:  100 GB  For each additional Domain: 110 GB |
| Security Gateway | 200 GB | 110 GB |
| VSX | For the VSX Gateway:  200 GB  For each Virtual System:  1 GB | For the VSX Gateway:  100 GB  For each Virtual System:  1 GB |
| Standalone | 1 TB | 110 GB |

 Notes:

* On an Open Server, only one upgrade is allowed. n On an Open Server, additional backup / snapshot is not supported. n On an Open Server, the logging partition size is only large enough for minimal machine operations.
* (\*) On an Open Server, at least 20 GB of free disk space is required in the root partition to start the upgrade process to R82.‎

## Maximum Supported Physical Memory

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

Threat Extraction Requirements for Webdownloaded Documents

n 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 an activated logging service. On dedicated Log Servers, the Log Server must be the same version as the Management Server.

## SmartEvent Requirements

SmartEvent R82 can connect to a Log Server that runs the R81, R81.10, or R81.20 version.

SmartEvent and a SmartEvent Correlation Unit are usually installed on the same server. You can also install them on different servers, for example, to balance the load in large logging environments. The SmartEvent Correlation Unit must be the same version as the SmartEvent Server.

To deploy SmartEvent and to generate reports, a valid license or contract is required.

Hardware Requirements

For an average rate of 500 logs per second:

n Total CPU Cores: 4 n RAM: 16GB

## SmartConsole Requirements

Hardware Requirements

This table shows the minimum hardware requirements for SmartConsole applications:

|  |  |
| --- | --- |
| Component | Minimum Requirement |
| CPU | Intel Pentium Processor E2140, or 2 GHz equivalent processor |
| Memory | 4 GB |
| Available Disk Space | 2 GB |
| Video Adapter | Minimum resolution: 1024 x 768 |

SmartConsole Software Requirements

* Microsoft .NET framework 4.8.
* Microsoft Visual C++.

SmartConsole is supported on:

* Windows 11, Windows 10 (all editions). n Windows Server 2022, 2019, 2016, 2012, 2012 R2.

## Gaia Portal Requirements

The Gaia Portal supports these web browsers:

|  |  |
| --- | --- |
| Browser | Supported Versions |
| Microsoft Edge | Any |
| Google Chrome | 14 and higher |
| Mozilla Firefox | 6 and higher |
| Apple Safari | 5 and higher |
| Microsoft Internet Explorer | 8 and higher  (If you use Internet Explorer 8, file uploads through the Gaia Portal are limited to 2 GB) |

## Mobile Access Requirements

OS Compatibility

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Endpoint Computer OS  Compatibility | Windows | Linux | macOS | iOS | Android |
| Mobile  Access  Portal  Clientless  access  to  web  applications  (  Link  Translation)  Compliance  Scanner  Secure  Workspace  SSL  Network  Extender  -  Network  Mode  SSL  Network  Extender  -  Application  Mode  Downloaded  from  Mobile  Access  applications  Citrix  File  Shares  -  Web-  based  file  viewer  (  HTML  )  Web  mail |  |  |  |  |  |

Browser Compatibility

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Endpoint  Browser  Compatibility | Microsoft Edge | Google Chrome | Mozilla Firefox | Apple  Safari | Opera for Windows | Microsoft  Internet  Explorer |
| Mobile Access  Portal  Clientless  access to web  applications (Link  Translation)  Compliance Scanner  Secure  Workspace (2),  (3)  SSL Network  Extender -  Network Mode  SSL Network  Extender Application Mode  (2)  Downloaded from Mobile Access  applications  Citrix  File Shares Web-based file viewer (HTML)  Web mail |  |  |  |  | Limited  support |  |

 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.](https://support.checkpoint.com/results/sk/sk113410)
2. Secure Workspace and SSL Network Extender Application Mode are available for Windows platforms only.
3. Microsoft Internet Explorer is only browser supported in Secure Workspace.

## Identity Awareness Requirements

Identity Clients

See [sk134312](https://support.checkpoint.com/results/sk/sk134312).

AD Query

Supported Active Directory versions: Microsoft Windows Server 2019, 2016, 2012 R2, 2012, and 2008 R2.

## Harmony Endpoint 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[R82HarmonyEndpointSecurityServerAdministrationGuide](https://sc1.checkpoint.com/documents/R82/SmartEndpoint_OLH/EN/Default.htm).

For additional information about support of Endpoint Security Clients for each OS version, see [sk178408](https://support.checkpoint.com/results/sk/sk178408).

* Endpoint Security Management Servers are supported on Management-only appliances or Open Servers.

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

* Endpoint Security Management Servers is not supported on Red Hat Enterprise Linux releases.
* R82 Endpoint Security Management Server can manage: l E81.00 and higher versions of Endpoint Security Clients for Windows l E82.00 and higher versions of Clients for macOS

Anti-Malware Signature Updates

* To allow Endpoint Security clients to get Anti-Malware signature updates from a cleanly installed R82 Primary Endpoint Security Management Server, follow the instructions in the[R82HarmonyEndpoint SecurityServerAdministrationGuide](https://sc1.checkpoint.com/documents/R82/SmartEndpoint_OLH/EN/Default.htm)when you select the Anti-Malware component.
* For a new R82 Endpoint Policy Server that was installed from scratch (not upgraded), you must follow [sk127074](https://support.checkpoint.com/results/sk/sk127074).

No additional steps are required, if you upgrade the Primary Endpoint Security Management Server to R82.

* 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 Platform Requirements

* To manage R82 Security Groups on Maestro, use:
  1. R82 Quantum Maestro Orchestrator.
  2. R82 Security Management Server or Multi-Domain Server.

In addition, see [sk113113](https://support.checkpoint.com/results/sk/sk113113) > section "Management Servers and Security Gateways they can manage".

For the list of available Maestro Security Appliances, see [sk162373](https://support.checkpoint.com/results/sk/sk162373).

* To manage R82 Security Groups on Scalable Chassis, use:

l R82 Security Management Server or Multi-Domain Server.

In addition, see [sk113113](https://support.checkpoint.com/results/sk/sk113113) > section "Management Servers and Security Gateways they can manage".

* For the list of compatible transceivers for Check Point Appliances, see [sk92755](https://support.checkpoint.com/results/sk/sk92755).
* For comparison between different software versions for Scalable Platforms (Maestro and Chassis), see [sk173183](https://support.checkpoint.com/results/sk/sk173183).

Supported Network Cards on Maestro Security Appliances

To connect a Maestro Security Appliance to Quantum Maestro Orchestrators with DAC cables, one of these Check Point cards has to be installed in the Maestro Security Appliance:

|  |  |
| --- | --- |
| Network Card | Notes |
| 10/25/40/100G Fiber QSFP28+  ([[[Undefined variable Vars\_HW.tp\_  100G\_QSFP\_card\_full]]]) SKU:  CPAC-2-40/100F-C | Important - For the minimum software requirements, see the home page article for your appliance model. You can find the corresponding links in [sk96246.](https://support.checkpoint.com/results/sk/sk96246)  Important - To connect to Quantum Maestro Orchestrators, you must use only the 10/25/40/100G ports. It is not supported to connect other ports to Orchestrators.  Note - You can connect all available 10/25/40/100G ports on a Security Appliance to Quantum Maestro Orchestrators on the Maestro Site.  Example for QLS450 (that has two 10/25/40/100G cards):  n The first 10/25/40/100G card connects to each Orchestrator on the Site:   * The first port on the card connects to one of the   Downlink ports on the first Orchestrator l The second port on the card connects to one of the Downlink ports on the second Orchestrator n The second 10/25/40/100G card connects to each Orchestrator on the Site:   * The first port on the card connects to another   Downlink port on the first Orchestrator l The second port on the card connects to another Downlink port on the second  Orchestrator |
| 100/25 GbE Fiber QSFP+ SKU:  CPAC-2-100/25F-B | The minimal required card firmware version is 12.22.1002 To make sure the version is correct, run this single long command in the Expert mode on the Security Appliance:   |  | | --- | | for NIC in $(ifconfig | grep ethsBP | awk '{print $1}') ; do echo $NIC: ; ethtool -i $NIC | grep firmware ; done |   Example output:   |  | | --- | | ethsBP4-01:  firmware-version: 12.22.1002 ethsBP4-02: firmware-version: 12.22.1002 |   You cannot use this network card with a splitter cable to split a port on an appliance. |
| Network Card | Notes |
| 40 GbE Fiber QSFP+ SKU:  CPAC-2-40F-B | The minimal required card firmware version is 12.22.1002 To make sure the version is correct, run this single long command in the Expert mode on the Security Appliance:   |  | | --- | | for NIC in $(ifconfig | grep ethsBP | awk '{print $1}') ; do echo $NIC: ; ethtool -i $NIC | grep firmware ; done |   Example output:   |  | | --- | | ethsBP4-01:  firmware-version: 12.22.1002 ethsBP4-02: firmware-version: 12.22.1002 |   You cannot use this network card with a splitter cable to split a port on an appliance. |
| 10 GbE Fiber SFP+ SKUs:  CPAC-4-10F-B  CPAC-4-10F-6500/6800-C | Output of the "lspci -v" command must show:  Intel Corporation 82599ES 10-Gigabit SFI/SFP+  Network Connection  To verify, run this command in the Expert mode on the Security Appliance:   |  | | --- | | lspci -v | grep 'Ethernet controller' | grep Intel | |

Supported Hardware and Firmware on 60000 / 40000 Scalable Chassis

All information is documented in [sk93332](https://support.checkpoint.com/results/sk/sk93332).

Maximum Supported Items

# Maximum Supported Items

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

## Maximum Supported Number of Interfaces on Security Gateway

The maximum number of interfaces supported (physical and virtual) is shown in this table.

|  |  |  |
| --- | --- | --- |
| Mode | Max # of Interfaces | Notes |
| Security Gateway | 1024 | Non-VSX |
| VSX Gateway | 4096 | Includes VLANs and Warp Interfaces |
| Virtual System | 250 |  |

Note - This table applies to Check Point Appliances and Open Servers.

## 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 |
| Geo Cluster | 2 |
| Virtual System Load Sharing | 13 |

Maximum Supported Items

## Number of Supported Items in a Maestro Environment

|  |  |  |
| --- | --- | --- |
| Item | Number of Supported Items | Notes |
| Number of Security Groups configured | n Minimum: 1 n Maximum: 8 | None |
| Number of Security  Appliances in one Security  Group | In Single Site and Dual Site deployment:  n Minimum: 1 n Maximum: 28 | In Dual Site environments:  n Each Security Group must contain a minimum of one Security Appliance from each site (see MBS-7606 in [sk181128](https://support.checkpoint.com/results/sk/sk181128)). n Each Security Group can contain a maximum of 28 Security Appliances - 14 Security Appliances from each site (see MBS-7773 in [sk181128](https://support.checkpoint.com/results/sk/sk181128)). |
| Number of interfaces configured on top of Uplink ports in one Security Group | In Security  Gateway Mode:   * Minimum: 2 n Maximum:   1024  In VSX Mode:   * Minimum: 2 n Maximum:   4096  For each Virtual System:   * Minimum: 2 n Maximum: 250 | Includes all interface types  (Physical, Bonds, VLAN, Warp). |

# Supported Clients and Agents

## Check Point Clients and Agents for Windows OS

Microsoft Windows

All the marked consoles and clients support Windows 32-bit and 64-bit.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Check Point Product | Windows 11 (4) | Windows 10 (5) | Windows  8.1 (6) | Windows 7 (+SP1) (7) |
| Endpoint Security Clients (1) |  |  | (with 8.1 Update 1) | (3) |
| Remote  Access  clients  (1)  Capsule  VPN  Plug-  in  UserCheck  Client  SSL  Network  Extender  Identity  Agent  for  a  User  Endpoint  Computer  (2)  Identity  Agent  for  a  Terminal  Server  (2) |  |  | (  with  8.1  Update  1) | (3) |

1. For additional information about support of Endpoint Security Clients for each OS version, see [sk178408](https://support.checkpoint.com/results/sk/sk178408).
2. For additional information about Identity Clients, see [sk134312](https://support.checkpoint.com/results/sk/sk134312).
3. For additional information about the Windows 7 support timeline, see [sk164006](https://support.checkpoint.com/results/sk/sk164006).
4. For additional information about Check Point support for Windows 11, see [sk175323.](https://support.checkpoint.com/results/sk/sk175323)
5. For additional information about Check Point support for Windows 10, see [sk107036.](https://support.checkpoint.com/results/sk/sk107036)
6. Windows 8 support is true for Pro and Enterprise editions.
7. Windows 7 support is true for Ultimate, Professional, and Enterprise editions.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Check  Point  Product | macOS 13 | macOS 12 | macOS 11 | macOS  10.15 | macOS  10.14 | macOS  10.13 | macOS  10.12 | OS X  10.11 |
| Identity Agent for a User  Endpoint  Computer  (1)  Endpoint  Security  Clients (2)  Endpoint  Security VPN (2)  SSL  Network  Extender |  |  |  |  |  |  |  |  |

Microsoft Windows Server

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Check Point Product | Server  2022 | Server  2019 | Server  2016 | Server  2012  R2 64-bit | Server  2012 | Server 2008 R2  (+SP1) |
| Endpoint  Security  Clients  (1)  UserCheck  Client  Identity  Agent  for  a  Terminal  Server  (2)  Identity  Collector  (2) |  |  |  |  |  |  |

1. For additional information on Endpoint Security Client support for each OS version, refer to [sk178408](https://support.checkpoint.com/results/sk/sk178408).
2. For additional information about Identity Clients, see [sk134312](https://support.checkpoint.com/results/sk/sk134312).

## Check Point Clients and Agents for macOS

All support is for macOS 64-bit.

1. For additional information about Identity Clients, see [sk134312](https://support.checkpoint.com/results/sk/sk134312).
2. For additional information on Endpoint Security Client support for each OS version, refer to [sk178408](https://support.checkpoint.com/results/sk/sk178408).

## Check Point DLP Exchange Security Agent

The R82 DLP Exchange Security Agent is supported on:

|  |  |
| --- | --- |
| Windows Server | Exchange Server |
| 2019 64-bit | 2019 |
| 2016 64-bit | 2016 |

Licensing

# Licensing

For all licenses issues contact[CheckPointAccountServices.](https://help.checkpoint.com/)