QUANTUM

05 December 2021

QUANTUM R81.20

Release Notes

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point Copyright Notice

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.

Feedback

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

Revision History

Date	Description
05 December 2021	First release of this document

Table of Contents

What's New

Introduction

Check Point Quantum R81.20 is packed with new features. that offer elasticity, efficiency, and innovative security enhancements

Quantum IoT Protect offers enterprise IoT device discovery embedded into Quantum Gateways and applies autonomous zero-trust policies that are automatically updated based on device type, risk level, and industry best practice, making it easy to secure IP cams, smart TVs, wi-fi printers and much more.

Zero-Day Phishing Prevention, powered by patented technologies and AI engines, prevents access to the most sophisticated phishing websites, both known and completely unknown, without the need to install and maintain clients on end-user devices.

Continuing to innovate Maestro, several new features improve efficiency, elasticity, and compatibility with public clouds. The new Autoscaling feature in Maestro Hyper-scale lets you automatically allocate resources across security groups (based on your priorities), bringing cloud-like scale and agility to your prem-based security (for example, to accommodate peak traffic hours). To support high-speed, high-volume transaction environments (e.g. digital trading), Maestro now offers accelerated data paths for higher throughput and lower latency based on predefined rules (“Fast Forwarding”).

Enhancing the gold standard in Security Management: Quantum R81.20 lets you leverage the new Management API to integrate security from the ground up and efficiently manage access policies with support for dynamic policy objects taken from external sources. A new workflow now supports policy change management to minimize errors, allowing verification for new policies before they are applied and enforced throughout (“4 Eyes Principle”). And automating VPN connections to public clouds, R81.20 makes it easy to connect your Quantum Gateways with data centers hosted in the public cloud. Offering simplified user authentication with third party SAML Identity Providers, authentication is modernized and improved for administrators log-in to SmartConsole as well as remote users accessing corporate assets. This enables SSO, MFA, and compliance checks, and complements current support for third-party Identity Providers by the Identity Awareness blade.

Quantum Security Gateway and Gaia

Threat Prevention

- Prevent browsing to Zero-Day phishing websites
  - Check Point Quantum Security Gateway enhances its web browsing protection to further prevent users from accessing phishing websites.
  - Powered by patented technologies and AI engines, the Security Gateway now uses Clientless In-Browser protection to prevent access to the most sophisticated phishing websites, both known and completely unknown (zero-day phishing websites).
  - The enhanced solution is available through the Security Gateway network flow, introducing dynamic security components that run within the browser with no need to install any client.
  - Delivered as part of your existing NGTX license.
  - Works out of the box for Security Gateways with Autonomous Threat Prevention enabled.
- Up to 50% performance enhancement to IPS CIFS protections.
- IOC feeds now support a significantly increased capacity in the number of observables for URLs, Domains, IP addresses, and Hashes - 2 million and up to hardware limit.
- Support for inspection of FTPS by Content Awareness, Anti-Virus and Threat Extraction blades.

Maestro Hyperscale

Maestro Fastforward -Significantly Improved throughput and latency for trusted connections. Maestro Fastforward offloads accept or drop policy rules to the Maestro Hyperscale Orchestrator for hardware acceleration.

- Sub microseconds latency.
- Port line-rate throughput for single connection.
- Support for Accelerated policy installation on Maestro Security Gateways. For more information see sk169096 .
- Support gradual upgrade with Multi Version Cluster (MVC)
- Based on the current traffic load, the Security Gateway automatically changes the number of CoreXL SNDs, Firewall instances and the Multi-Queue configuration for zero traffic impact.
- Management Data Plane Separation (MDPS) support for Scalable Platforms.

IoT Protect

Leverage Quantum Security Gateway and Infinity to instantly discover IoT devices and enforce independent Zero-Trust policies.

- Only allow what's needed for the device to operate.
- Automatic grouping based on device type.

IPsec VPN

- Seamless site to site tunnel establishment with AWS native cloud VPN. Setup a route based VPN tunnel with a virtual Gateway with just a few simple steps.
- Major performance and stability improvement for Remote Access and Site to Site VPN that delivers a much higher capacity for VPN tunnels.
- Extended Security Gateway certificate validation capabilities for faster authentication.

Access Control

- Network Feed Object - Use a Network Feed object to get dynamic IPs or domains of a specific external service that is not included in the Updatable Objects options. In addition, the user can create its own service containing a list of IPs or domains and have them in his policy. The object is automatically updated in Security Gateway without the need to install the policy.
- Performance improvements - support for Updatable Objects, Domain objects, and Dynamic objects with the Optimized Drop feature (drop templates).

Advanced Routing

- Support for Intermediate System (IS-IS) routing protocol.
- DHCP Relay Agent Information Option 82 that addresses several scaling and security issues arising in public DHCP use.
- OSPFv3 NSSA support.
- IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.
- Support for Routed control scripts to allow ClusterXL fail-over and tear down of BGP connections.
- Routing Protocol History for BFD to improve troubleshooting capabilities.
- Netflow Live connections and Firewall rule ID UUID.

Gaia Operating System

- Configure a retention policy for Gaia scheduled backups and snapshots.
- Using the CLI, monitor the module temperature, module supply voltage, TX Bais voltage, Rx optical Power, and TX optical power for a single transceiver or all transceivers on an appliance.
- Automatic update to the NIC firmware during the ISO installation process for appliances that have 40GbE, 100/25GbE, and/or SmartNIC acceleration cards.

CoreXL

In UserSpace Firewall (USFW), the number of IPv6 instances can equal the number of IPv4 instances, allowing the configuration of the gateway to process a more significant amount of IPv6 traffic.

Identity Awareness

- The Identity Awareness Gateway automatically identifies and excludes Service Account sessions acquired by the Identity Collector. For more details, see sk174266.
- Improved resiliency, scalability, and stability for PDPs and Identity Brokers. Additional threads handle authentication and authorization flows.
- Automatic tuning of nested LDAP groups - The Identity Awareness Gateway automatically chooses the optimal way to query the LDAP server for users and groups.
- During a PDP failure, a PEP Identity Awareness Gateway can recover its identity database from connected PDP Gateways.
- Identity Collector is now supported with Quantum Spark Appliances.

Mobile Access

Oauth 2.0 support for Capsule Workspace and Office 365.

Quantum Security Management

General

Performance improvements to IPS updates and utilization.

SmartConsole

Administrators can use SAML 2.0 to configure SmartConsole users to authenticate with an Identity Provider.

SmartWorkflow

Send policy and configuration changes for peer review and approval before publishing.

Management REST API

Management API support for:

- Identity Awareness configuration on gateways and clusters.
- HTTPS Inspection outbound certificate configuration.
- Creation of LSM Gateways.
- Creation of LSM Gateways VPN configuration.

Upgrades

- Central Deployment- Use SmartConsole to:
  - Gradually upgrade Quantum Cluster Members.
  - Upgrade Quantum Spark and Quantum Edge Appliances.
- Pre-Upgrade Verifier results are now presented in the upgrade report.
- Significant performance improvement by importing Domain Management Servers concurrently instead of sequentially.

CloudGuard Network Security

- CloudGuard Controller support for:
  - Oracle Cloud Infrastructure (OCI)
  - Nutanix
  - New Azure resources – Application Security Groups, Private Endpoints
  - New AWS resources – Load Balancer tags
- Nutanix Flow support for CloudGuard Network Security Gateways.
- Amazon Web Services (AWS):
  - Security Gateway, Single, High Availability Cluster, Auto Scaling Group (ASG), Gateway Load Balancer Auto Scaling Group (ASG), Transit Gateway with ASG.
  - AWS Gateway Load Balancer support.

Harmony Endpoint

Endpoint Policy Management

Use SSO to connect to the Endpoint Web Management Console.

Remote Access VPN

Authenticate Remote Access VPN users with SAML.

Licensing

For all licenses issues contact *Check Point Account Services*.

Software Changes

This section lists differences in behavior from previous versions.

- Messaging and logging daemon now uses Rsyslog (previously Syslog) for Gaia devices.
- Update to Gaia OS Linux kernel version.
- Isomorphic: Users must use isomorphic build 187 or higher.
- Gaia uses a new installer:
  - You must upgrade to the latest Deployment Agent (DA) before upgrading to R81.20. For More information see sk92449.
  - A new partition layout is introduced to accommodate the new Gaia installer changes.
  - Upgrade from R77.30 to R81.20 can take place only if the Security Gateway work mode is 64 bit. For more information on setting the Kernel edition see sk94627.

Supported Environments

Management Servers boot by default with 64-bit Gaia kernel after a clean install or upgrade to R81.20.

Note - If you revert from the R81.20 upgrade, the appliance will still boot with 64-bit kernel, even if it was originally 32-bit.

Refer to the Product Life Cycle page for more information and announcements about Check Point Appliances.

Management Server Appliances

Product and Supported Appliances

Check Point Product	Smart-1 405, 410, 525, 625, 600-S, 600-M	Smart-1 5050, 5150, 6000-L, 6000-XL
Security Management Server	✓	✓
Log Server	✓	✓
SmartEvent Server	✓	✓
Multi-Domain Security Management Server	–	✓
Multi-Domain Log Server	–	✓

Appliances and Supported Products

Appliance	Management	Management + Log Server	Management + Log Server + SmartEvent
Quantum Smart-1 6000-L/6000-XL	✓	✓	✓
Quantum Smart-1 600-S/Smart-1 600-M	✓	✓	✓
Gen V Smart-1 (405, 410, 525, 625, 5050, 5150)	✓	✓	✓

Standalone (Gateway + Management)

The model numbers in this table are for the series of appliances that support R81.20 Standalone

Appliance Series	Security Gateway	Standalone (Gateway + Management)
3000	✓	✓
5000	✓	✓
6500, **6800**	✓	–
6200 6600, **6400**, **6700**, **6900**	✓	✓
7000	✓	✓
15000	✓	✓(*)
16000, **16200**	✓	✓
16600HS	✓	–
23000	✓	✓(*)
26000, **26000THS**	✓	–
28000, 28600HS, 28800HS, 28800LS	✓	–
Cloud setup, VMware	✓	Using kernel mode only

(*) Standalone is only supported with appliances using HDD for storage (Standalone is NOT supported with appliances using SSD).

Appliance Support for the User Space Firewall (USFW)

Security Gateways on these platforms run in the USFW mode by default:

- 3600, 3600T, 3800, 6200B, 6200P, 6200T, 6400, 6600, 6700, 6900, 7000, 16000, 16000THS, 16200, 16600HS, 23900, 26000, 26000THS, 28000, 28600HS, and 28800HS appliances.
- VMware Virtual Machine.

Note - All other Check Point appliances boot in the kernel mode by default.
Open Server / Cloud setup boots in the USFW mode when using 40 CPU cores or more.

Threat Emulation Appliances

TE100X, TE250X, TE250XN, TE1000X, and TE2000X, TE2000XN are fully supported with R81.20.

Supported Virtualization Platforms

For the most up-to-date information about the supported Linux versions and virtualization platforms, see the **Virtual Machines** section of the *Hardware Compatibility List*.

Cloud Platforms

Supported setups for cloud solutions:

- **Amazon Web Services**:
  - Security Gateway, Single, High Availability Cluster, Auto Scaling Group (ASG), Transit Gateway with ASG.
  - Security Management Server.
  - Standalone.
- **Microsoft Azure**:
  - Security Gateway, Virtual Machine Scale Sets, High Availability.
  - Security Management Server.
  - Standalone.
- **Google Cloud Platform (GCP)**:

- Security Gateway, Managed Instance Group, High Availability.
- Security Management Server.
- Standalone.

Supported Upgrade Paths

Installation Methods

- For Security Management Servers it is recommended to use the CPUSE option available in Gaia Portal. To learn more about CPUSE, see sk92449.
- For Security Gateway upgrade, it is recommended to use the Central Deployment available in SmartConsole.

Upgrade Paths

Upgrade to R81.20 is available only from these versions:

Note - For more information about Security Management Servers and supported managed Security Gateways visit sk113113.

Current Version	Security Gateways and VSX(1)	Management Servers and Multi-Domain Servers	Standalone
R81, **R81.10**	✓	✓	✓
R80.20 kernel 2.6, **R80.20 kernel 3.10**, **R80.30 kernel 2.6**, **R80.30 kernel 3.10**, **R80.40**, **R81.10**	✓	✓	✓
R80.20SP, **R80.30SP**, **R81 for Scalable Platforms**, **R81.10 for Scalable Platforms**	✓**(2)**	Not applicable	Not applicable
R80.20.M1, **R80.20.M2**	Not applicable	✓	Not applicable

Current Version	Security Gateways and VSX(1)	Management Servers and Multi-Domain Servers	Standalone
R80.10	✓	Requires a 2-step upgrade path: 1) R80.10 → R80.40**(3)** 2) R80.40 → R81.20	Requires a 2-step upgrade path: 1) R80.10 → R80.40**(3)** 2) R80.40 → R81.20
R80	Not applicable	Requires a 2-step upgrade path: 1) R80 → R80.40 **(3)** 2) R80.40 → R81.20	Not applicable
R77.30	✓	Requires a 2-step upgrade path: 1) R77.30 → R80.40**(3)** 2) R80.40 → R81.20	Requires a 2-step upgrade path: 1) R77.30 → R80.40**(3)** 2) R80.40 → R81.20

Notes:

1. Starting R81.10, VSLS is the only supported mode for new installations.
   Upgrade of a VSX Cluster in the High Availability mode from R81.10 and earlier versions to R81.20 is supported.
   The VSX Cluster is automatically converted to VSLS.
   Upgrade from R81.10 to R81.20 is supported only in VSLS.
2. Upgrade from these versions to R81.20 is supported only with specific takes of a Jumbo Hotfix Accumulators.
3. To upgrade to R80.40, see the *R80.40 Installation and Upgrade Guide*.
4. To upgrade a Security Gateway or a Management Server that implements Carrier Security, see sk169415.

Upgrade Methods

Use these methods to upgrade your Check Point environment to R81.20:

Check Point Products	Supported Upgrade Methods for These Products
■ Security Gateway ■ VSX	■ Central Deployment of Hotfixes in SmartConsole ■ CPUSE Upgrade ■ CPUSE Clean Install
■ Security Management Server ■ Multi-Domain Server ■ CloudGuard Controller ■ Endpoint Security Management Server	■ CPUSE Upgrade ■ CPUSE Clean Install ■ Advanced Upgrade ■ Upgrade with Migration

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 10 GB of free disk space is required in the `/var/log` partition for a Clean Install or Upgrade to succeed.

Supported Backward Compatibility Gateways

R81.20 Management Servers can manage Security Gateways of these versions:

Gateway Type	Release Version
Security Gateway	R77.30, R80.10, R80.20, R80.30, R80.40, R81, R81.10
VSX	R77.30, R80.10, R80.20, R80.30, R80.40, R81, R81.10
Security Groups on Maestro	R80.20SP, R80.30SP, R81, R81.10
Security Groups on Scalable Chassis	R80.20SP, R81, R81.10

R81.20 Management Servers can manage appliance Security Gateways that run these versions:

Appliance	Release Version
1100 Appliances	R77.20.x
1200R Appliances	R77.20.x
1400 Appliances	R77.20.x
1530, 1550, 1570, 1590 Appliances	R80.20.x
60000 / 40000 Scalable Chassis	R80.20SP, R81, R81.10

Open Server Hardware Requirements

Minimal Hardware Requirements

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

Note - The above numbers do not apply to SmartEvent and SmartLog.

Disk Space Requirements

Disk Space	Security Management	Multi-Domain Server	Security Gateway	VSX	Standalone
Recommended free disk space	1 TB	1 TB	200 GB	200 GB + 1 GB for each Virtual System	1 TB
Minimum free disk space	110 GB	100 GB	110 GB	100 GB + 1 GB for each Virtual System	110 GB

Notes:

- Only one upgrade is allowed.
- Additional backup / snapshot is not supported.
- Logging partition size is just enough for minimal machine operations.
- At least 20 GB of free disk space is required in the `root` partition to start the upgrade process to R81.20.

Maximum Supported Physical Memory

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

Requirements

Threat Extraction Requirements for Web-downloaded documents

- A minimum of 2.3GB free RAM must be available, regardless of the number of cores or connection used by the Security Gateway.
- Supported with 5000 and higher appliances series.

Threat Emulation Requirements

Threat Emulation using ThreatCloud requires Gaia operating system (64 or 32-bit).

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 machine. This is recommended 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 R81.20 can connect to an R81.20 or R81 Log Server.

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

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

SmartConsole Requirements

Hardware Requirements

This table shows the minimum hardware requirements for SmartConsole applications:

Component	Minimal 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

Software Requirements

SmartConsole is supported on:

- Windows 10 (all editions), Windows 8.1 (Pro), and Windows 7 (SP1, Ultimate, Professional, and Enterprise)
- Windows Server 2019, 2016, 2012, 2008 (SP2), and 2008 R2 (SP1)

Gaia Portal Requirements

The Gaia Portal supports these web browsers:

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

Mobile Access Requirements

OS Compatibility

Endpoint 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 Internet Explorer	Microsoft Edge	Google Chrome	Mozilla Firefox	Apple Safari	Opera for Windows
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)	✓	✓	✓	✓	✓	Limited support
Web mail	✓	–	✓	✓	✓	✓

Notes:

1. For a list of the prerequisites required for using 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.
3. Microsoft Internet Explorer is only browser supported inside Secure Workspace.

Identity Awareness Requirements

Identity Agents

See *"Clients and Agents Support by Windows Platform" on page 37* and *"Clients and Agents Support by macOS Platform" on page 38* for:

- Identity Agent (Light and Full)
- Identity Agent for Terminal Servers
- Identity Collector

AD Query and Identity Collector

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

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

- 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.
- R81.20 Endpoint Security Management Server can manage:
  - E81.00 and higher versions of Endpoint Security Clients for Windows
  - E82.00 and higher Client for macOS

Anti-Malware signature updates:

- To allow Endpoint Security clients to get Anti-Malware signatures updates from a cleanly installed R81.20 Primary Endpoint Security Management Server, follow the instructions in the *R81.20 Endpoint Security Server Administration Guide* when you select the Anti-Malware component.
- For cleanly installed R81.20 Endpoint Policy Server, you must follow sk127074. No additional steps are required, if you upgrade the Primary Endpoint Security Management Server to R81.20.
- Endpoint Security Clients can still 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.

For more information, see the *R81.20 Endpoint Security Server Administration Guide*.

Scalable Platform Requirements

You can manage R81.20 Security Groups with an R81.20 Security Management Server or Multi-Domain Server.

For the list of available Maestro Security Appliances, see sk162373.

For the list of compatible transceivers for Check Point Appliances, see sk92755.

For comparison between different software versions for Scalable Platforms (Maestro and Chassis), see sk173183.

Supported Network Cards on Maestro Security Appliances

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

Network Card	Notes

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`

40 GbE Fiber QSFP+
SKU:
CPAC-2-40F-B
 	
100 GbE Fiber QSFP
SKU:
CPAC-2-100/25F-B
	The minimal required card firmware version is 12.22.1002
	To verify, 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`

Supported Hardware and Firmware on 60000 / 40000 Scalable Chassis

All information is documented in sk93332.

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	5
Virtual System Load Sharing	13

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 deployment: ■ Minimum: 1 ■ Maximum: 31 In Dual Site deployment: ■ Minimum: 1 ■ Maximum: 28	In Dual Site deployment: ■ Each Security Group must contain at least one Security Appliance from each site (see MBS-7606 in sk148074). ■ Each Security Group can contain a maximum of 28 Security Appliances - 14 Security Appliances from each site (see MBS-7773 in sk148074).
Number of interfaces configured on top of Uplink ports in one Security Group	In Security Gateway Mode: ■ Minimum: 2 ■ Maximum: 1024 In VSX Mode: ■ Minimum: 2 ■ Maximum: 4096 For every Virtual System: ■ Minimum: 2 ■ Maximum: 250	Includes all interface types (Physical, Bonds, VLAN, Warp).

Check Point Clients and Agents Support

Multiple Login Option Support

This version supports multiple login options per gateway with multi-factor authentication schemes, for users of different clients and the Mobile Access Portal. For example, configure an option to authenticate with Personal Certificate and Password, or Password and DynamicID for SMS or email.

These features are supported when connected to an R81.20 gateway that has IPsec VPN or Mobile Access enabled.

Supported Client or Portal	Lowest Supported Version
Mobile Access Portal	R80.10
Capsule Workspace for iOS	1002.2
Capsule Workspace for Android	7.1
Remote Access clients for Windows - Standalone clients	E80.65
Remote Access VPN Blade of the Endpoint Security Suite for Windows	E80.65

Clients and Agents Support by Windows Platform

Microsoft Windows

In this table, Windows 7 support is true for Ultimate, Professional, and Enterprise editions. Windows 8 support is true for Pro and Enterprise editions. All the marked consoles and clients support Windows 32-bit and 64-bit.

Check Point Product	Windows 7 (+SP1)	Windows 8.1	Windows 10 *
Remote Access clients E80.x	✓	✓ (with 8.1 Update 1)	✓ (E80.62 and higher)
Capsule VPN Plug-in	–	✓	✓
SSL Network Extender	✓	✓	✓
UserCheck Client	✓	✓	✓
Identity Agent (Light and Full)	✓	✓	✓
Identity Agent for Terminal Servers	✓	–	–

* Supported Windows 10 versions: 1703, 1709, 1803 for more information see the **Detailed Client Releases Information** section in sk117536.

Microsoft Windows Server

Check Point Product	Server 2008 R2 (+SP1)	Server 2012	Server 2012 R2 64-bit	Server 2016	Server 2019
UserCheck Client	✓	–	✓	✓	–
Identity Agent for Terminal Servers	✓	✓	✓	✓	✓
Identity Collector	✓	✓	✓	✓	✓

Note - Identity Agent for Terminal Servers is also supported on XenApp 6.

Clients and Agents Support by macOS Platform

All support is for macOS 64-bit.

Check Point Product	OS X 10.11	macOS 10.12	macOS 10.13	macOS 10.14
Identity Agent	✓	✓	✓	✓
SSL Network Extender	✓	✓	✓	✓
Endpoint Security VPN E80.x or higher	✓ (E80.62 and higher)	✓ (E80.64 and higher)	✓	✓

DLP Exchange Agent Support

The R81.20 DLP Exchange Security Agent is supported on:

Windows Server	Exchange Server
2012 R2 64-bit	2010, 2013
2016 64-bit	2016

For earlier server versions, use the R77.30 DLP Exchange Security Agent.