Quantum
Cyber Security Platform
Titan release

15 February 2026

QUANTUM CYBER SECURITY PLATFORM

R81.20

Titan Release

Release Notes

CHECK POINT™

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.

Check Point Quantum R81.20 Titan Release

For more about this release, see the R81.20 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
18 November 2025	Updated: ■ *"Maximum Supported Items" on page 64*
12 November 2025	Updated: ■ *"Supported Environments" on page 26* - Added a note "VSX mode is not supported in Public Cloud" ■ *"Supported Upgrade Methods" on page 41*
14 September 2025	Updated: ■ *"Hardware Requirements for Open Server / Virtual Machine" on page 50* - Disk Space Requirements ■ *"Maximum Supported Items" on page 64* - added "Change in IPS Protections"
04 July 2025	Updated: ■ *"Maximum Supported Items" on page 64* - added "Rules in each NAT policy"
23 June 2025	Updated: ■ *"Management Server and Log Server" on page 27*
15 August 2024	Added: ■ *"SecureXL User Mode (UPPAK)" on page 36*
04 June 2024	Updated: ■ *"Security Gateway or Cluster" on page 29* ■ *"Desktop SmartConsole Hardware Requirements" on page 54* ■ *"Maximum Supported Items" on page 64*
22 April 2024	Updated: ■ *"Supported Upgrade Paths" on page 38* ■ *"Hardware Requirements for Open Server / Virtual Machine" on page 50*
05 April 2024	Updated: ■ *"Gaia Portal Requirements" on page 55*

Date	Description
28 March 2024	Updated: ■ *"Supported Environments" on page 26* ■ *"Maximum Supported Items" on page 64*
28 February 2024	Updated: ■ *"Supported Environments" on page 26* - added 9000, 19000, 29000 appliance models
01 January 2024	Updated: ■ *"Supported Environments" on page 26* - The TE2000XN model supports R81.20
01 January 2024	Updated: ■ *"Harmony Endpoint Management Server Requirements" on page 59* ■ *"Supported Clients and Agents" on page 70*
24 December 2023	Updated: ■ *"What's New" on page 12*: • In the section "Quantum Security Management", added the new sub-section "Internal Certificate Authority (ICA)"
30 October 2023	Updated: ■ *"Supported Environments" on page 26*
11 September 2023	Updated: ■ *"Upgrade Paths" on page 38*

Date	Description
27 August 2023	Updated: ■ Improved formatting and document layout ■ *"What's New" on page 12*: • In the section "Clustering", added the list of Software Blades that the ClusterXL in the Active-Active mode supports • In the section "CloudGuard Network Security", added New Cisco ACI resources ■ *"Software Changes" on page 23*: • Change in the Gaia backup file names • ClusterXL MVC Upgrade ■ *"Upgrade Paths" on page 38* - To convert the upgraded VSX Cluster to VSLS, use the "`vsx_util to convert`" command ■ *"Maximum Supported Items" on page 64* - Maximum number of Security Appliances in one Maestro Security Group is 28
10 June 2023	Updated: ■ *"Supported Environments" on page 26* > *"Management Server and Log Server" on page 27* > added the "Management High Availability" section ■ *"Scalable Platform Requirements" on page 61* > added the "2-Port Dual-Width 10/25/40/100G QSFP28 Card"
12 February 2023	Updated: ■ *"Supported Environments" on page 26*
09 January 2023	Improved formatting and document layout
02 December 2022	Updated: ■ *"Supported Environments" on page 26*
27 November 2022	Updated: ■ *"What's New" on page 12* - corrected the link to the Administration Guide for the SmartWorkflow feature
22 November 2022	Updated: ■ *"Supported Environments" on page 26* - added the section "Quantum Maestro"
20 November 2022	First release of this document

Table of Contents

Important Links

For more about R81.20, see:

- Quantum R81.20 Home Page
- Quantum R81.20 Known Limitations
- Quantum R81.20 Resolved Issues

For more about R81.20 for Scalable Platforms, see:

- Quantum R81.20 for Scalable Platforms Home Page.
- Known Limitations for Scalable Platforms.
- Scalable Platforms (Maestro and Chassis) comparison between versions.

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 Infinity Consolidated Security Architecture*.

What's New

Introduction

The **Quantum Cyber Security Platform Titan Release R81.20** delivers significant innovations in Advanced Threat Prevention, Security Management, and Security Performance. In addition, Check Point has expanded on-premises and cloud network security through new and upcoming advanced cloud-based Check Point applications and services. By upgrading to R81.20, these new cloud-based applications offer powerful feature upgrades on Check Point Security Gateways, without requiring an upgrade to the next software release.

With R81.20, customers immediately benefit from a wide range of new security capabilities across four major categories:

Deep Learning Threat Prevention

- AI Deep Learning prevents 5x more DNS attacks in real-time. The feature it is part of the NGTX license, and is enabled when the Anti-Bot and Anti-Virus Software Blades are active. For more information see:
  - sk178487 - ThreatCloud DNS tunneling protection.
  - sk175623 - ThreatCloud Domain Generation Algorithm (DGA) protection.
- Firewall-based, Zero-Day phishing prevention blocks 4x more Zero-Day phishing attacks (Check Point patented solution).

Quantum IoT Protect

- Discover IoT assets with Quantum Security Gateways.
- Autonomous Zero Trust Profiles allow only the necessary device communication and prevent threats that target IoT assets.

Network Security Management

- New Infinity Cloud Services page in SmartConsole – Quick and easy integration between your on-premises Security Management Server and Infinity Portal Applications. This includes the ability to share Quantum logs with Infinity Events for a unified view of logs across Quantum, CloudGuard, and Harmony products, and helps accelerate event correlation and Threat Hunting delivered through Check Point Detection & Response solutions.
- Automated policy enforcement & updates using new Network Feed Objects. DevOps and other teams can manage their own access lists without requiring interaction from Security Admin groups.
- SmartWorkflow - streamlined policy change review, ensures accuracy of Security Policies through customizable built-in policy supervision work-flows.

Performance Acceleration for Quantum Security Gateways

- Maestro Auto-Scaling provides dynamic performance scaling for mission critical apps and large workloads. Automatically shifts firewall resources in and out of Security Groups to support critical applications as throughput and compute requirements change.
- Maestro Fastforward provides a 100G cut-through mode for trusted connections - the highest throughput and lowest latency for specific applications.
- Quantum HyperFlow delivers 2.5x times higher throughput for elephant flows (very long, high-bandwidth intensive connections). Security Gateway automatically allocates more CPU cores to process elephant flow connections upon detection.

Quantum Security Gateway and Gaia

Threat Prevention

- Zero Phishing prevents web 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 SandBlast (SNBT) 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 greater number of observables for URLs, Domains, IP addresses, and Hashes - 2 million and more (only on the XFS file system), depending on the Security Gateway's hardware specifications.

  On the EXT3 file system, the IoC feed is limited to a maximum of 250,000 indicators, depending on the Security Gateway's hardware specifications.

  For more information about the file systems, see sk141432.
- ICAP Server now supports secure ICAP communication over TLS.

IoT Protection

Instantly discover and protect your IoT assets with Quantum Security Gateways and Infinity to enforce automated Zero Trust policies:

- Discover IoT devices, routers, and switches connected to your network using your R81.20 Quantum Security Gateways.
- Assign automatically generated restrictive policies to IoT devices based on their Internet access requirement to allow only what is needed for the IoT devices to operate.

Note - IoT General Availability is planned to be part of the R81.20 Jumbo Hotfix Accumulator.

Maestro Hyperscale

- **Maestro Auto-Scaling** - Automatically assigns Security Appliances (scale units) to a Security Group when the configured conditions are met.
- **Maestro Fastforward** - Significantly improved throughput and latency for trusted connections. Maestro Fastforward offloads accept or drop policy rules to the Quantum Maestro Orchestrator for hardware acceleration and provides:
  - Sub-microsecond latency.
  - Port line-rate throughput for a single connection.
- Support for accelerated policy installation on Maestro Security Groups. See sk169096.
- Monitor utilization of NAT resources in CPView and with SNMP.
- Support gradual upgrade in the Multi-Version Cluster (MVC) mode.
- Scalable Platforms now support CoreXL Dynamic Balancing - Based on the current traffic load, the Security Group automatically changes the number of CoreXL SNDs, CoreXL Firewall instances, and the Multi-Queue configuration for zero traffic impact.
- Scalable Platforms now support Management Data Plane Separation (MDPS, sk138672).

VSX

- Support for the DHCP Server configuration in Gaia Clish in the context of each Virtual System.

IPsec VPN

- Scalable VPN performance - 3 times faster to process simultaneous Remote Access and Site to Site VPN connections.
- Major performance and stability improvement for Remote Access VPN and Site to Site VPN that delivers a significantly greater capacity for VPN tunnels.
- Extended Security Gateway certificate validation capabilities for quicker authentication.
- Resilient VPN architecture - multi-process architecture to handle IKE negotiations in dedicated scalable daemons, providing unprecedented resiliency.

Clustering

- Added support for the "Same VMAC" feature. For more information, see the *R81.20 ClusterXL Administration Guide*.
- ClusterXL in the Active-Active mode now supports these Software Blades:
  - Application Control
  - URL Filtering
  - Content Awareness
  - Anti-Spam and Email Security
  - Anti-Bot
  - Anti-Virus

Access Control

- Dynamic Policy - Use a Network Feed object to customize a private web server feed definition for IP addresses or domains. The objects are automatically updated in Security Gateway without the need to install a policy. Updatable Objects uses the Network Feed to strengthen the dynamic configuration ability of the Access Control policy. See the *Administration Guide*.
- 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.
- Support for DHCP Relay Agent Information Option 82 to address several scaling and security issues that arise in public DHCP use.
- Support for OSPFv3 NSSA.
- Support for IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.
- Support for Routing Event Triggers to allow ClusterXL failover, and tearing down of BGP connections through monitored BGP and BFD sessions.
- Routing Protocol History for BFD to improve troubleshooting capabilities.
- NetFlow Live connections and Firewall rule.

Gaia Operating System

- Configure a retention policy for Gaia scheduled backups and snapshots.
- Configure Gaia scheduled jobs to run hourly or at specified minute intervals.
- Configuring a logical next hop gateway in IPv6 static routes to send traffic through a specified interface.
- Configure the minimum number of required interface links for a bonding group in the 802.3AD mode.
- Use Gaia Clish commands to monitor NIC transceivers in appliance - module temperature, supply voltage, TX Bias voltage, Rx optical Power, and TX optical power.
- Automatic update to the NIC firmware during the ISO installation process for appliances that have 40GbE, 100/25GbE, and 2-Port Dual-Width 10/25/40/100G QSFP28 Cards.

CoreXL

- HyperFlow provides automatic system resource allocation by proper prioritization of tasks on highly utilized CPU cores and dynamically balances the tasks. Introducing seamless gateway tuning and optimization and improving single flow performance and spikes handling.
- In User Space Firewall (USFW), the number of IPv6 CoreXL Firewall instances is no longer limited, IPv6 Firewall instances can be increased up to the number of IPv4 Firewall instances.

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 Broker. Additional threads handle authentication and authorization flows.

Mobile Access

- OAuth 2.0 support for Capsule Workspace and Office 365.

Quantum Spark

- Central Deployment - Use SmartConsole to upgrade Quantum Spark and Quantum Edge Appliances. See the *Security Management Administration Guide*.
- Quantum Spark Appliances now support Identity Collector.
- Use SmartUpdate and SmartProvisioning (LSM) to manage Quantum Spark appliances that run R81.10.
- Quantum Spark Appliances now support transit connections to an Active Directory server on an internal network (appliances work as an AD proxy).

Quantum Security Management

Cloud Services Integration

- Integration between your on-premises Security Management Server and Infinity Portal:
  - Run cloud services that are managed in the Infinity Portal on your Security Management Server objects.
  - See a unified log view of all your Check Point products, on-premises and in cloud.
  - Run Management API calls securely on the on-premises Security Management Server from anywhere in the world through Infinity Portal.

  See the *Administration Guide*.

SmartConsole

- SmartConsole can use SAML 2.0 to authenticate administrators with an Identity Provider. See the *Administration Guide*.

SmartWorkflow

- Send policy and configuration changes for a review and approval cycle by another administrator before applying the changes. See the *Administration Guide*.

SmartTasks

- New triggers - before and after working on a session that requires an approval, and for critical CloudGuard Controller events.
- New action - send an email with a detailed change report after publishing a session, after policy installation, and more.

See the *Administration Guide*.

Management REST API

Management API support for:

- Identity Awareness configuration on Security Gateways and Clusters.
- Configuration of HTTPS Inspection outbound certificate.
- Configuration of SmartLSM Gateways.
- Configuration of VPN settings on SmartLSM Gateways.

See the *Check Point Management API Reference* (at the top, select the correct version) .

Upgrades

- Central Deployment of CPUSE packages in SmartConsole:
  - Gradually upgrade Quantum Cluster Members.
  - Upgrade Quantum Spark and Quantum Edge Appliances.

  See the *Administration Guide*.
- Pre-Upgrade Verifier results are now presented in the upgrade report.
- Simpler migration from a Standalone environment to a distributed environment located in Quantum Smart-1 Cloud or on-premises. See sk179444.
- Significant performance improvement of Multi-Domain Server upgrades by importing Domain Management Servers concurrently instead of sequentially.

Internal Certificate Authority (ICA)

- Ability to create certificates with 3072-bit RSA keys - the root ICA certificate and SIC certificates. See sk96591.

CloudGuard Network Security

- CloudGuard Controller support for:
  - Oracle Cloud Infrastructure (OCI). See the *Administration Guide*.
  - Nutanix. See the *Administration Guide*.
  - New Microsoft Azure resources - Application Security Groups, Private Endpoints. See the *Administration Guide*.
  - New Amazon Web Services resources - Load Balancer tags. See the *Administration Guide*.
  - New Cisco ACI resources - End-point Security Group (ESG), Policy tag, Name Alias tag. See the *Administration Guide*.
  - SmartTasks for CloudGuard Controller critical events. See the *Administration Guide*.
- Nutanix Flow support for CloudGuard Network Security Gateways.
- Amazon Web Services (AWS):
  - Cross Availability Zones Cluster (Geo Cluster). See the *Administration Guide*.
  - Use of the Generic Network Virtualization Encapsulation (Geneve) network encapsulation protocol for Gateway Load Balancer (GWLB).

Harmony Endpoint

Endpoint Policy Management

- Use Single Sign-On to connect to the Endpoint Web Management Console.

Harmony Endpoint Web UI

- IoC Management - Users can now add Indicators of Compromise to their Endpoint Policy Management.
- Connection Awareness - Allows administrators to configure their own entity to determine the connectivity of the clients, and change a device's policy type from "Connected" to "Disconnected", and vice-versa accordingly.

Remote Access VPN

- Exclude SaaS applications (such as Office 365) from the Remote Access VPN tunnel.
- Use SAML 2.0 to authenticate Remote Access VPN users with an Identity Provider.

Software Changes

Note - - To see the list of changes starting R80.40, see sk180180.

This section describes behavior changes from previous versions.

- **Gaia**
  - Update to Gaia OS Linux kernel version.
  - New Gaia installer:
    - You must upgrade to the latest Deployment Agent (DA) before upgrading to R81.20. See sk92449.
    - A new partition layout is introduced to accommodate the new Gaia installer changes.
    - Upgrade of a Security Gateway from R77.30 to R81.20 is supported only if the Gaia works with the 64 bit kernel edition.

      For more information on configuring the Kernel edition, see sk94627.
  - ISOmorphic Tool: You must use build 187 or higher. See sk65205.
  - SmartConsole download is no longer available from the Gaia Portal(you are redirected to Support Center).
  - The password for the Gaia GRUB (boot loader - maintenance mode) is a dedicated password (separated from the Expert mode password).

    You can configure the Gaia GRUB password during the Gaia First Time Configuration Wizard, or after the Gaia installation.
  - Messaging and logging daemon now uses Rsyslog (previously Syslog).
  - Changed the date format for the Gaia manual backup file.

    Gaia always uses this template (regardless of the Gaia Display Format for Time and Date):

    ```
    backup_--_<HostName>.<Domain>_<DD>_<MMM>_<YYYY>_<HH>_<MM>_
    <SS>.tgz
    ```

- Changed the date format for the Gaia scheduled backup file.

  Gaia always uses this template (regardless of the Gaia Display Format for Time and Date):

  ```
  backup_-<Name_of_Scheduled_Backup>-_<HostName>.<Domain>_
  <DD>_<MMM>_<YYYY>_<HH>_<MM>_<SS>.tgz
  ```

- **SmartConsole**
  - The IoT Network Protection properties in SmartConsole are **read-only**.

    Manage your IoT policies and objects through the IoT Network Protect application in the Infinity Portal.
  - Certificate status indication:
    - For the Internal CA certificate - SmartConsole shows an alert if the ICA certificate expires in less than one year.
    - For IPsec VPN certificates - SmartConsole > **Gateways & Servers** view shows a warning near the VPN Gateway object about the certificate expiration.
- **VSX**
  - CLI commands for DHCP server configuration on VSX now support the Virtual System context notation (`set virtual-system <ID>`).
- **Maestro**
  - The Enhanced NAT Port Allocation Mechanism (Global NAT, GNAT) is enabled by default on Maestro Security Groups.
- **HTTPS Inspection**
  - In SmartDashboard > HTTPS Inspection, the default value for the "**Automatic Updates**" changed to "**Download and install updates automatically**".

    The change applies to a Management Server upgrade from a lower version.

    For more information, see sk173629 How to update trusted CAs automatically.

    Important - Policy installation is required for the changes to take effect on the Security Gateway.
- **IPS**
  - The download package location of the IPS updates changed

    from `/opt/CPsuite-R81.20/fw1/ips`

    to `/var/log/opt/CPsuite-R81.20/fw1/ips`
- **ClusterXL MVC Upgrade**

- During a cluster MVC upgrade, kernel tables with data about VPN are not synchronized from the cluster members with the current version to the upgraded cluster member:
  - In the case of IKEv2 - cluster members do not synchronize the data about VPN at all.
  - In the case of IKEv1 - cluster members do not synchronize the data about IPSec SAs.
- Delta Sync operates fully only from the upgraded cluster members to the cluster members with the current version.
- A new VPN tunnel is created after failover from the cluster members with the current version to the upgraded cluster member.

Supported Environments

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

Notes:

- If you revert from the R81.20 upgrade, the appliance boots with the 64-bit Gaia kernel, even if it was originally 32-bit.
- For documentation about Check Point Appliances appliances, see sk96246.
- Refer to the Support Life Cycle Policy page for more information and announcements.

Management Server and Log Server

These platforms support R81.20 in the Management Server and Log Server configurations:

Product and Supported Platforms

Check Point Product	Smart-1 6000-XL (1), Smart-1 6000-L (1), Smart-1 5150 (2), Smart-1 5050 (2)	Smart-1 625 (3), Smart-1 600-M (4), Smart-1 600-S (4), Smart-1 525 (5), Smart-1 410 (6), Smart-1 405 (6)	Open Servers (7)	Virtual Machines (8)
Security Management Server **Endpoint Security Management Server**	✓	✓	✓	✓
Log Server	✓	✓	✓	✓
SmartEvent Server	✓	✓	✓	✓
Multi-Domain Security Management Server	✓	–	✓ (9)	✓ (9)
Multi-Domain Log Server	✓	–	✓ (9)	✓ (9)

1. For information about Smart-1 6000-L and Smart-1 6000-XL, see sk171903.
2. For information about Smart-1 5050 and Smart-1 5150, see sk120453.
3. For information about Smart-1 625, see sk157153.
4. For information about Smart-1 600-S and Smart-1 600-M, see sk171903.
5. For information about Smart-1 525, see sk120453.
6. For information about Smart-1 405 and Smart-1 410, see sk117578.

7. For certified Open Servers, see the *Hardware Compatibility List* > Tab *Open Servers*. For known limitations, see sk168335.
8. "Virtual Machines" apply to Public Cloud and to Private Cloud.

   See the *Hardware Compatibility List* > Tab *Virtual Machines*. For known limitations, see sk168335.
9. Requires a license to manage a minimum of 25 Security Gateways.
10. Each of these Smart-1 models and platforms 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 R81.20 in the Security Gateway or Cluster configuration:

Platforms	SK	Security Gateway, Cluster
MLS200, MLS400 (1)	sk176466	✓
QLS250, QLS450, QLS650, QLS800 (1)	sk176466	✓
29100, 29200 (2)	sk180520	✓
28000, 28600HS	sk152733	✓
26000, 26000T	sk152733	✓
23500, 23800, 23900	sk107516	✓
19100, 19200 (2)	sk180520	✓
16000, 16200, 16600HS, 16600T	sk152733	✓
15400, 15600	sk107516	✓
9100, 9200, 9300, 9400, 9700, 9800 (3)	sk181698	✓
7000	sk139932	✓
6200, 6400, 6500, 6600, 6700, 6800, 6900	sk139932	✓
5100, 5200, 5400, 5600, 5800, 5900	sk110053	✓
3100, 3200, 3600, 3800	sk110052	✓
64000, 44000 (4)	sk65305	✓
Open Servers (5)	N / A	✓
Virtual Machines (6)	N / A	✓

1. R81.20 does **not** support the Hardware Acceleration on these appliance models. See sk179432 and sk176466.
2. The 19000 and 29000 appliances require a dedicated R81.20 image.

See the *Downloads* section in sk180520.

3. The 9000 appliances require a dedicated R81.20 image.

   See the *Downloads* section in sk181698.

4. R81.20 supports only **SSM440** and **SGM400** in Scalable Chassis.

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.

   VSX mode is not supported in Public Cloud.

   See the *Hardware Compatibility List* > Tab *Virtual Machines*. For known limitations, see sk168335.

Standalone and Full High Availability

Only these platforms support R81.20 in the Standalone (Gateway + Management Server) configuration or Full High Availability Cluster configuration:

Platforms	SK	Standalone
23500, 23800, 23900	sk107516	✓ (1)
16000, 16200, 16600T The model 16600HS does not support Standalone	sk152733	✓
15400, 15600	sk107516	✓ (1)
9100, 9200, 9300, 9400, 9700, 9800 (2)	sk181698	✓
7000	sk139932	✓
6200, 6400, 6600, 6700, 6900 The models 6500, 6800 do not support Standalone	sk139932	✓
5900	sk110053	✓
5100, 5200, 5400, 5600, 5800	sk110053	✓ (1)
3100, 3200, 3600, 3800	sk110052	✓
Open Servers (3)	N / A	✓
Virtual Machines (4)	N / A	✓

1. 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

   a. Connect to the command line.

   b. Log in to the Expert mode.

   c. 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).

d. 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
```

e. The returned value:

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

2. The 9000 appliances require a dedicated R81.20 image.

   See the *Downloads* section in sk181698.

3. For certified Open Servers, see the *Hardware Compatibility List* > Tab *Open Servers*. For known limitations, see sk168335.

4. "Virtual Machines" apply to Public Cloud and to Private Cloud.

   See the *Hardware Compatibility List* > Tab *Virtual Machines*. For known limitations, see sk168335.

5. It is not supported to enable the SmartEvent Software Blade on any cluster member in Full High Availability Cluster configuration.

Threat Emulation Appliances

Platform	SK	Security Gateway, Cluster
TE2000XN	sk173494	✓
TE2000X	sk106210	✓
TE1000X	sk106210	✓
TE250XN (*)	sk173494	–
TE250X	sk106210	✓
TE100X	sk106210	✓

(*) This appliance model does not support R81.20. See sk173494.

Quantum Maestro

Quantum Maestro Orchestrator models MHO-140, MHO-170, and MHO-175 fully support the R81.20 release. See sk177624.

For the list of supported Security Appliances in a Maestro Security Group, see sk162373.

User Space Firewall (USFW)

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

Platform	SK	USFW
MLS200, MLS400	sk176466	✓
QLS250, QLS450, QLS650, QLS800	sk176466	✓
29100, 29200 (1)	sk180520	✓
28000, 28600HS	sk152733	✓
26000, 26000T	sk152733	✓
23900	sk107516	✓
19100, 19200 (1)	sk180520	✓
16000, 16000T, 16200, 16600HS	sk152733	✓
9100, 9200, 9300, 9400, 9700, 9800 (2)	sk181698	✓
7000	sk139932	✓
6200B, 6200P, 6200T, 6400, 6600, 6700, 6900	sk139932	✓
3600, 3600T, 3800	sk110052	✓
Open Servers (3)(4)	N / A	✓
Virtual Machines (5)(6)	N / A	✓
CloudGuard Network Security for Public Cloud (7)	N / A	✓
CloudGuard Network Security for Private Cloud (7)	N / A	✓

1. The 19000 and 29000 appliances require a dedicated R81.20 image.

   See the *Downloads* section in sk180520.
2. The 9000 appliances require a dedicated R81.20 image.

   See the *Downloads* section in sk181698.

3. For certified Open Servers, see the *Hardware Compatibility List* > Tab *Open Servers*. For known limitations, see sk168335.
4. Open Server must have 40 or more CPU cores.
5. "Virtual Machines" apply to Public Cloud and to Private Cloud.

   See the *Hardware Compatibility List* > Tab *Virtual Machines*. For known limitations, see sk168335.
6. Virtual Machine must have 40 or more virtual CPU cores. Applies to Public Cloud and to Private Cloud.
7. CloudGuard Network Virtual Machines support USFW regardless of the number of available CPU cores.

Notes:

- Security Gateways on all other Check Point appliance models run in the Kernel Space Firewall (KSFW) mode by default.
- 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):
  - 23800
  - 15400, 15600
  - 6500, 6800
  - 5400, 5600, 5800, 5900

SecureXL User Mode (UPPAK)

Only these Check Point appliances support SecureXL in the User Mode (UPPAK):

Platforms	SK	UPPAK
MLS200, MLS400	sk176466	✓
QLS250, QLS450, QLS650, QLS800	sk176466	✓
29100, 29200	sk180520	✓
19100, 19200	sk180520	✓
9100, 9200, 9300, 9400, 9700, 9800	sk181698	✓

- On the supported Check Point appliances, the default SecureXL mode is the User Mode (UPPAK).

  For the required (missing or bad snippet) Take, see sk179432.

- On all other supported Check Point appliances (see the section *"Security Gateway or Cluster" on page 29*), SecureXL runs only in the Kernel Mode (KPPAK).

- For more information about SecureXL modes, see:

  - sk153832 - Chapter "SecureXL Modes - KPPAK and UPPAK"
  - sk179432
  - *LightSpeed 10/25/40/100G QSFP28 Ports Administration Guide*:
    - Chapter "Configuring SecureXL"
    - Chapter "Known Limitations" > Section "SecureXL"

- SecureXL UPPAK Mode is not supported when the Firewall works in the Kernel Mode (KSFW). See sk167052.

Virtualization Platforms

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

Cloud Platforms

Supported setups for cloud solutions:

- **Amazon Web Services**:
  - Security Gateway
  - High Availability Cluster
  - Cross AZ Cluster
  - Security Gateway Auto Scaling Group
  - Security Management Server
  - Multi-Domain Server
  - Standalone
- **Microsoft Azure**:
  - Security Gateway
  - High Availability Cluster
  - Virtual Machine Scale Sets
  - Security Management Server
  - Multi-Domain Server
  - Standalone
- **Google Cloud Platform (GCP)**:
  - Security Gateway
  - High Availability Cluster
  - Managed Instance Group (MIG)
  - Security Management Server
  - Multi-Domain Server
  - 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.
- For Security Gateway upgrade, we recommend that you use the Central Deployment available in SmartConsole. See sk168597.

Upgrade Paths

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

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

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

Current Version	Security Gateways and VSX (1)	Management Servers and Multi-Domain Servers	Standalone
R80.10	✓ (4)	Requires a 2-step upgrade path (3) (4)	Requires a 2-step upgrade path (3)(4)
R80	*Not applicable*	Requires a 2-step upgrade path (3)	*Not applicable*
R77.30	✓ (4)(5)	Requires a 2-step upgrade path (3) (4)(5)	Requires a 2-step upgrade path (3)(4)(5)

Notes:

1. Starting from R81.10, VSLS is the only supported mode for **new** installations of **VSX Clusters**.
   Upgrade of a VSX Cluster in the High Availability mode from R81.10 and earlier versions to R81.20 is supported.
   To convert the upgraded VSX Cluster to VSLS, use the "`vsx_util to convert`" command.
2. Upgrade from these versions to R81.20 is supported only with specific takes of a Jumbo Hotfix Accumulators.
   See sk177624.
   In Maestro environment, it is possible to upgrade Security Groups and Quantum Maestro Orchestrators (if you decide to upgrade, you must upgrade both).
3. The required 2-step upgrade path is:
   a. To R80.40
      See the *R80.40 Installation and Upgrade Guide*.
   b. To R81.20
4. Before you start the upgrade, you must make sure the Gaia OS edition is 64-bit:
   a. Get the current Gaia OS edition with this Gaia Clish command:
      ```
      show version all
      ```
   b. If the Gaia OS edition is "32-bit", run these Gaia Clish commands:
      ```
      set edition 64-bit
      save config
      reboot
      ```
5. To upgrade an R77.30 environment that implements Carrier Security (former Firewall-1 GX), you must follow sk169415:
   a. Upgrade the R77.30 Management Server to the special R80.30-based image.
   b. Upgrade the R80.30 Management Server to R81.
   c. Change the GTP settings.
   d. Upgrade the R77.30 Security Gateway / Cluster to R81.
   e. Upgrade the R81 Management Server to R81.20.
   f. Upgrade the R81 Security Gateway / Cluster to R81.20.

Supported Upgrade Methods

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 20 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.

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

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	✓	✓	✓	✓	✓	–	–	✓
VSX Gateways	–	✓	✓	✓	✓	–	–	✓

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	–	–	–	✓	✓	–	–	–
Security Group Members - Scalable Chassis	–	–	–	✓	✓	–	–	–
ClusterXL Members in the High Availability modes	–	✓	–	✓	✓	–	–	✓
ClusterXL Members in the Load Sharing modes	–	✓	–	✓	✓	–	–	✓
VSX Cluster Members	–	✓	✓	✓	✓	–	–	✓

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)
VRRP Cluster Members	–	✓	–	✓	✓	–	–	✓
Primary Security Management Server	✓	✓	–	✓	✓	✓	✓	–
Secondary Security Management Server	–	–	–	✓	✓	✓	✓	–
Primary Multi-Domain Security Management Server	✓	✓	–	✓	✓	✓	✓	–
Secondary Multi-Domain Security Management Server	✓	✓	–	✓	✓	✓	✓	–

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 Multi-Domain Log Server	✓	✓	–	✓	✓	✓	✓	–
Secondary Multi-Domain Log Server	✓	✓	–	✓	✓	✓	✓	–
Primary CloudGuard Controller	–	–	–	✓	✓	✓	✓	–
Secondary CloudGuard Controller	–	–	–	✓	✓	✓	✓	–
Primary Endpoint Security Management Server	–	–	–	✓	✓	✓	✓	–

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 Endpoint Security Management Server	–	–	–	✓	✓	✓	✓	–
Dedicated Log Server	–	–	–	✓	✓	✓	✓	–
Dedicated SmartEvent Server	–	–	–	✓	✓	✓	✓	–
Full High Availability Cluster Members	–	–	–	✓	✓	✓	✓	–
Standalone Server	–	–	–	✓	✓	✓	✓	–

Notes:

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.
   - For instructions, see the *R81.20 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.
   - For instructions, see the *R81.20 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.
   - For instructions, see the *R81.20 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 *R81.20 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 *R81.20 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 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

Management Server and Security Gateway Versions

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

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

Gateway Type	Release Version
Security Gateway	R81.20, R81.10, R81, R80.40, R80.30, R80.20, R80.10, R77.30
VSX	R81.20, R81.10, R81, R80.40, R80.30, R80.20, R80.10, R77.30
Security Groups on Maestro	R81.20, R81.10, R81, R80.30SP, R80.20SP See *"Quantum Maestro Orchestrator and Security Group Versions" on the next page*.
Security Groups on Scalable Chassis	R81.20, R81.10, R81, R80.20SP
Quantum Spark, Quantum Rugged, and SMB Appliances	R81.10.X, R80.20.X, R77.20.X

Note - To manage R81.20 Security Gateways / Security Groups:

- An R81.10 Management Server requires the R81.10 Jumbo Hotfix Accumulator Take 82 or higher (see PRJ-39424).
- An R81 Management Server requires the R81 Jumbo Hotfix Accumulator Take 79 or higher (see PRJ-39424).

Management Server and Managed Appliances

R81.20 Management Servers can manage these Security Gateway appliances:

Appliance	Release Version
1500 / 1600 / 1800 Quantum Spark Appliances	R81.10.X(*), R80.20.X
1200R SMB Appliances	R77.20.X
700 / 1400 SMB Appliances	R77.20.X
600 / 1100 SMB Appliances	R77.20.X
60000 / 40000 Scalable Chassis	R81.20, R81.10, R81, R80.20SP

Notes:

- The support for the Quantum Spark 1800 / 1600 / 15x0 models is integrated in the R81.20 Management Server (see sk179615).
- To manage the Quantum Spark 15x5 models, an R81.20 Management Server requires the R81.20 Jumbo Hotfix Accumulator Take 26 or higher (see sk179615).

Quantum Maestro Orchestrator and Security Group Versions

R81.20 Quantum Maestro Orchestrator can manage Maestro Security Groups that run these versions:

- R81.20 (see sk177624)
- R81.10 (see sk173363)
- R81 (see sk169954)
- R80.30SP (see sk162552)
- R80.20SP (see sk138233)

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

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	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 *"SmartEvent Requirements" on page 53*.

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
VSX Gateway, **VSX Cluster Member**	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:

1. On an Open Server / Virtual Machine, only one upgrade is allowed.
   To upgrade again:
   - On a Security Gateway:
     a. Export the Gaia OS configuration (`save configuration /var/log/Gaia_Config.txt`).
     b. Copy all other configuration files, in which you made manual changes.
     c. Perform a Clean Install of the required version.
     d. Configure the required settings again based on the exported files.
   - On a Management Server:
     Use an Advanced Upgrade or an Upgrade with Migration - see *"Supported Upgrade Paths" on page 38*.
     a. Export the management database.
     b. Copy all other configuration files, in which you made manual changes.
     c. Perform a Clean Install of the required version.
     d. Import the management database.
     e. Configure the required settings again based on the exported files.
2. On an Open Server / Virtual Machine, additional backup / snapshot is not supported.
3. 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.
4. 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

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

SmartEvent R81.20 can connect to a Log Server that runs the R81 or R81.10 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 run 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:

- 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	Intel Pentium Processor E2140, or 2 GHz 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 4.5.
- Microsoft Visual C++.

SmartConsole is supported on:

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

  Important - Support for Windows Server 2012 and 2012 R2 was removed in the R81.20 Jumbo Hotfix Accumulator, starting from Take 79. See sk181879.

Gaia Portal Requirements

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

To connect to Gaia Portal on R81.20 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	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 in the Gaia Portal are limited to 2 GB)

The Gaia Portal requirements on Quantum Maestro Orchestrators

To connect to Gaia Portal on R81.20 Quantum Maestro Orchestrators, you must use one of these web browsers:

Browser	Supported Versions
Microsoft Edge	40.15063 and higher
Google Chrome	71.0 and higher
Mozilla Firefox	64.0 and higher
Microsoft Internet Explorer	11.0.50 and higher

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)	✓	✓	✓	✓	Limited support	✓
Web mail	–	✓	✓	✓	✓	✓

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.
3. Microsoft Internet Explorer is only browser supported in Secure Workspace.

Identity Awareness Requirements

Identity Clients

See *"Check Point Clients and Agents for Windows OS" on page 71* and *"Check Point Clients and Agents for macOS" on page 73* for:

- Identity Agent for a User Endpoint Computer (Light and Full)
- Identity Agent for a Terminal Server
- 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

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

- 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 are 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 versions of Clients for macOS
- For supported Endpoint Security Clients for each OS version, see the *Harmony Endpoint 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 R81.20 Primary Endpoint Security Management Server, follow the instructions in the *R81.20 Harmony Endpoint Security Server Administration Guide* when you select the Anti-Malware component.
- For a new R81.20 Endpoint Policy Server that was installed from scratch (not upgraded), 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 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 R81.20 Security Groups on Maestro, use:

  1. R81.20 Quantum Maestro Orchestrator.
  2. R81.20 Security Management Server or Multi-Domain Server.

     In addition, see sk113113 > section "Management Servers and Security Gateways they can manage".

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

- To manage R81.20 Security Groups on Scalable Chassis, use:

  - R81.20 Security Management Server or Multi-Domain Server.

    In addition, see sk113113 > section "Management Servers and Security Gateways they can manage".

- 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 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+ (2-Port Dual-Width 10/25/40/100G QSFP28 Card) 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. **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): ▪ 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 • The second port on the card connects to one of the Downlink ports on the second Orchestrator ▪ 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 • The second port on the card connects to another Downlink port on the second Orchestrator

Network Card	Notes

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`

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`

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.

Maximum Supported Items

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	300 and 500	No	To make sure the Management Server is responsive when you manage more than 300 Security Gateways, it is necessary to disable the three LSM Add-ons as described in sk135972 (`LSMServerAddon`, `PAServerAddon`, and `PAHBServerAddon`).
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 smaller the number of rules in the installed policy, the more responsive the Security Gateway is.

Item	Maximum Number	Hard Limit	Comment
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.
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.

Smart-1 6000-L/6000-XL Sizing Recommendations and Limitations

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.
VSX Gateway	4096	Includes physical, VLAN, and Warp Interfaces.
Virtual System on a VSX Gateway	64	Includes physical, VLAN, and Warp Interfaces.
Virtual System 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
Geo Cluster	2
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 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 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 each Virtual System: ■ Minimum: 2 ■ Maximum: 250	Includes all interface types (Physical, Bonds, VLAN, Warp).

Supported Clients and Agents

Check Point Clients and Agents for Windows OS

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 11 (4)	Windows 10 (5)	Windows 8.1 (6)	Windows 7 (+SP1) (7)
Endpoint Security Clients (1)	✓ (E85.40 and higher)	✓	✓ (With 8.1 Update 1)	✓ (3)
Remote Access clients E81 and higher (1)	✓ (E85.40 and higher)	✓	✓ (With 8.1 Update 1)	✓ (3)
Capsule VPN Plug-in	✓	✓	✓	–
UserCheck Client	✓	✓	✓	✓
SSL Network Extender	–	✓	✓	✓
Identity Agent for a User Endpoint Computer (2)	✓	✓	✓	✓
Identity Agent for a Terminal Server (2)	✓	–	–	✓

1. For supported Endpoint Security Clients for each OS version, see the *Harmony Endpoint EPMaaS Administration Guide* > section "*Supported Operating Systems for the Endpoint Client*".
2. For additional information about Identity Clients, see sk134312.
3. For additional information about the Windows 7 support timeline, see sk164006.
4. For additional information about Check Point support for Windows 11, see sk175323.

5. For additional information about Check Point support for Windows 10, see sk107036.
6. Windows 8 support is true for Pro and Enterprise editions.
7. Windows 7 support is true for Ultimate, Professional, and Enterprise editions.

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)	✓ (E85.40 and higher)	✓	✓	✓	✓	✓
UserCheck Client		–	✓	✓	–	✓
Identity Agent for a Terminal Server (2)		✓	✓	✓	✓	✓
Identity Collector (2)		✓	✓	✓	✓	✓

1. For supported Endpoint Security Clients for each OS version, see the *Harmony Endpoint EPMaaS Administration Guide* > section "*Supported Operating Systems for the Endpoint Client*".
2. For additional information about Identity Clients, see sk134312.

Check Point Clients and Agents for macOS

All support is for macOS 64-bit.

Check Point Product	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)	✓ (E86.20 and higher)	✓ (E84.30 and higher)	✓ (E82.50 and higher)	✓	✓	✓	✓
Endpoint Security VPN (2)	✓ (E86.20 and higher)	✓ (E84.30 and higher)	✓ (E82.50 and higher)	✓ (E81 and higher)	✓ (E81 and higher)	✓ (E81 and higher)	✓ (E81 and higher)
SSL Network Extender	–	✓	✓	✓	✓	✓	✓

1. For additional information about Identity Clients, see sk134312.
2. For supported Endpoint Security Clients for each OS version, see the *Harmony Endpoint EPMaaS Administration Guide* > section "*Supported Operating Systems for the Endpoint Client*".

Check Point DLP Exchange Security Agent

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 Windows Server and Exchange Server versions, use the R77.30 DLP Exchange Security Agent.

Build Numbers

Software Component	Build Number	Verifying Build Number
Gaia	OS Build 634 (*) OS kernel version 3.10.0-1160.15.2cpx86_64 OS edition 64-bit	Run this command in Gaia Clish: `show version all`
Security Gateway	R81.20 - Build 703	Run this command in the Expert mode: `fw ver`
Security Management Server	R81.20 - Build 440	Run this command in the Expert mode: `fwm ver`
Multi-Domain Server	R81.20 - Build 413	Run this command in the Expert mode: `fwm mds ver`
SmartConsole	81.20.9700.633	Click Menu > About Check Point SmartConsole

(*) On 3 June 2024, the Build was updated. The new R81.20 image (Take 634) contains Preventative Hotfix for CVE-2024-24919. See sk182336.

Licensing

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

Why Now

As the cybersecurity industry is learning, the high velocity and sophistication of modern cyberattacks makes it impossible for human-managed models to fully protect organizations in real-time. Blocking the most evasive attacks requires AI Deep Learning that predicts malicious behavior without human intervention.

Secondly, the industry has not effectively leveraged the true power of the cloud to enhance and accelerate on-premises security to keep up with the pace of business. Customers now expect their on-premises network security to quickly evolve with new requirements. Check Point made strategic developments to quickly and seamlessly expand on-premises Quantum Security Gateway capabilities through cloud-based services, with this R81.20 release.

Thirdly, there is a huge global shortage of security expertise, and policy creation has become more complex than ever - driving the importance of automation and DevSecOps. Security administrators need automation and greater efficiency to eliminate labor-intensive security administration and management.

Finally, legacy on-premises network security firewalls do not automatically scale-up or prioritize performance (packet processing and network throughput) for peak workloads and mission-critical applications. As a result, traditional network security approaches cannot keep up with the unpredictable network demands and new IT requirements from lines of business. Customers expect their on-premises and cloud security solutions to easily scale, while maintaining the highest levels of resiliency with up to 99.999% SLAs for the most demanding data centers, enterprises, and service providers.

The new R81.20 release provides important solutions and advances for both on-premises and native-cloud environments.