QUANTUM

16 January 2024

QUANTUM CYBER SECURITY PLATFORM

R82

Early Availability

Release Notes

CHECK POINT™

Check Point Copyright Notice

Table of Contents

What's New

Introduction

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

Quantum Security Gateway

Web Security

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

HTTPS Inspection

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

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

Automatic Zero Phishing Configuration

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

Improved Threat Prevention Capabilities

- Added configuration granularity for advanced DNS protections in Threat Prevention.
- Added Advanced DNS protection against NXNS Attack.
- Added support for DNS over HTTPS Inspection.
- New Zero-Day prevention engine integrated into the Anti-Bot Blade. This engine detects and blocks advanced malware Zero-Day variants by automatically analyzing and identifying communication patterns.
- Added Advanced DNS capability to block DNS queries to newly created domains.
- DNS Security statistics are now available in the SmartView Dashboard.
- It is now possible to load SNORT rules file as Custom Intelligence Feed automatically with 5-minute intervals to enforce them as IPS protections.

New Clustering Technology

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

Dynamic Policy Layer

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

Unified Configuration

- Kernel parameters configuration is now performed in centralized database with Gaia Clish commands and Gaia REST API calls instead of `fwkern.conf` and `simkern.conf` files. See:
  - The Local Gaia API Reference at "`https://<IP Address of Gaia Management Interface>/gaia_docs/#introduction`" > section "*Global Parameters*".

Identity Awareness

- Quantum Gateways can now use Identity Providers defined in the Check Point Infinity Portal, allowing customers to centrally manage identities across multiple Check Point products.
- Introducing a new mode for Identity Awareness Blade - "PDP-Only", where the Security Gateway acts only as Policy Decision Point (PDP) for identity acquisition and distribution and does not enforce the identity-based policy. The new mode improves scalability for PDPs and Identity Broker. To enable the "PDP-Only" mode, see sk181605.
- Introduced Identity Sharing cache mode to improve resiliency in case of connectivity loss with the PDP.

IPsec VPN

- Automatically detect configuration changes in AWS, Azure, and GCP public clouds and adjust the VPN settings ensuring connection stability.
- Introducing the Advanced VPN Monitoring tool that shows information on each VPN Tunnel and tracks its health and performance.
- Enhanced Link Selection:
  - Interoperability:
    - Uses the endpoint IP addresses of the VPN tunnel to improve interoperability with other software vendors.
    - Uses Dead Peer Detection (DPD) as the link probing protocol instead of the proprietary "Reliable Data Protocol" (RDP).
  - Redundancy:
    - Allows redundancy of VPN tunnels including third-party and native cloud VPN peers.
  - Granularity:
    - Ability to configure the Security Gateway to use different VPN interfaces in different VPN communities.

Remote Access VPN

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

Mobile Access

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

  See the Local Management API Reference at "`https://<IP Address of Gaia Management Interface on Management Server>/api_docs/`" > section "*Mobile Access*".

Gaia Operating System

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

The new capabilities are:

- Enhance Gaia OS with:
  - Support for VSX mode in Gaia Link Layer Discovery Protocol (LLDP).
  - DHCPv6 server, DHCPv6 client, and DHCPv6 client for prefix-delegation.
  - Ability to configure the order of the "AAA" authentication (TACACS, RADIUS, Local authentication) in Gaia Portal and Gaia Clish.
  - DNS Proxy forwarding domains, which allows configuring specific DNS servers per DNS suffix.
- New Gaia Clish and Gaia Portal configuration items:
  - Two-Factor Authentication for Gaia OS login using time-based authenticator apps (Google Authenticator and Microsoft Authenticator).
  - NTP pools and a larger number of NTP servers.
  - NFSv4 configuration.
  - Keyboard layout.
- Support for storing a Gaia OS backup in and restoring it from Amazon S3 and Microsoft Azure.

Dynamic Routing

Added support for new Dynamic Routing capabilities:

- BGP Extended Communities (RFC 4360).
- BGP Conditional Route Advertisement and Injection.
- Routing Table Monitor for Event Triggers.
- IPv4 and IPv6 Router Discovery on cluster members.
- Router Preference and Route Information option.
- IPv4 PIM-SSM with non-default prefixes.
- IPv4 PIM with BFD.
- IPv4 PIM neighbor filtering.
- IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).
- REST API calls for BGP, PIM, Multicast Listener Discovery (MLD).
- REST API calls for Route Redistribution, Inbound Route Filters, and NAT Pools.
- REST API calls for IGMP.

See the Local Gaia API Reference at "`https://<IP Address of Gaia Management Interface>/gaia_docs/#introduction`" > section "*Networking*".

Performance and Infrastructure

- HyperFlow acceleration of elephant flows for the SMB/CIFS service.
- Quantum Security Gateway multi-core utilization for sending inspection logs, improving log output capacity by up to 100%.
- SecureXL acceleration of traffic over VxLAN and GRE tunnels.

Maestro Hyperscale

This release features improvements in managing and monitoring Maestro Hyperscale clusters, which include:

- Support for SNMP Queries on each Security Group Member..
- REST API on Quantum Maestro Orchestrator and ElasticXL Cluster Members:
  - New Quantum Maestro Orchestrator API calls for configuration and monitoring of Security Groups, Gateways, Sites, and Ports.
  - Support Gaia REST APIs for Quantum Maestro Security Group Members and ElasticXL Cluster Members.

  See the Local Gaia API Reference at "`https://<IP Address of Gaia Management Interface>/gaia_docs/#introduction`" > section "*Maestro*".

VSX

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

The benefits of the new VSX mode are:

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

Tools and Utilities

- ConnView - a new consolidated troubleshooting tool for viewing connections information on the Security Gateway that works in the User Space Firewall (USFW).

  See the Local Gaia API Reference at "`https://<IP Address of Gaia Management Interface>/gaia_docs/#introduction`" > section "Diagnostics" > section"Connections" > command "`show-connections`".

  In the Expert mode, run the "`connview`" command.

- New policy advisory tool "`up_execute`" (in the Expert mode), which performs virtual Access / NAT Rule Base execution. Given inputs based on logs or connections, the execution provides detailed information such as matched rules and classification information.

Quantum Security Management

Security Management Server Enhancements

- The LDAP Account Unit object now uses the LDAP server name and CA certificate for LDAP trust. The trust is automatically renewed if an administrator renews or replaces the LDAP server certificate. As a result, Check Point servers keep their connectivity to the LDAP server.
- Support for Management API to run the "`vsx_provisioning_tool`" operations to configure VSX Gateway and VSX Cluster objects.

  See the Local Management API Reference at "`https://<IP Address of Gaia Management Interface on Management Server>/api_docs/`" > section "VSX" > command "`vsx-provisioning-tool`".
- Support for Management API to configure the "Data Type" objects for the Data Loss Prevention and Content Awareness Software Blades.

  See the Local Management API Reference at "`https://<IP Address of Gaia Management Interface on Management Server>/api_docs/`" > section "Data Types".
- Security Gateways can now be managed by a Security Management Server hosted behind a public cloud or third-party NAT device.

Central Deployment of Hotfixes and Version Upgrades in SmartConsole

Central Software Deployment through SmartConsole was enhanced and now supports:

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

SmartProvisioning

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

Multi-Domain Security Management Server

- Ability to clone an existing Domain on the same Multi-Domain Security Management Server. See sk180631.
- Improved upgrade time of large Multi-Domain Security Management Server environments by up to 50%.
- New Management API for setting IPv6 address of Multi-Domain Security Management Server.

Compliance

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

CloudGuard Network Security

CloudGuard Controller

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

CloudGuard Network

- New Management API for CloudGuard Central License utility.

Harmony Endpoint

Harmony Endpoint Web Management enhancements:

- **Client optimization for Windows servers** - Harmony Endpoint allows you to easily optimize the Endpoint Security clients for Windows servers, such as Exchange servers, Active Directory servers, Database servers, and so on, by manually assigning Windows server roles.
- **Run Diagnostics**:
  - Runs performance checks on endpoint clients using Push Operation.
  - The performance report presents each client's CPU and RAM utilization, including the editable threshold.
  - Harmony Endpoint presents suggested exclusion for performance improvements.
  - You can easily add an exclusion as part of "Global Exclusion" or "Exclusion per Rule":
    - **Exclusion description** - You can now add comments for new or existing exclusions.
    - **Global Exclusion** - You can now easily add global exclusion that applies to all rules.
- Application Control for macOS - Control which applications can run or use networking.
- New Asset Management view:
  - **Filters** - A brand new look and functionality for filters that enhances operation and productivity, while using the Asset Management view.
  - **Asset Management Table** - Bigger asset management table to see all relevant data easily.
  - **Columns reorder** - New Column reorder option to customize the asset management table based on their specific needs by changing columns location.
- **Linux Offline Package** - Supports upload and export package for Linux OS clients.
- Added Harmony Endpoint Management API to support on-premises Endpoint Security Management Server.

  The API is disabled by default for on-premises deployments. See the Harmony Endpoint Management API article.

Software Changes

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

This section describes behavior changes from the previous version.

Management Server

- Security Gateways R77.30 are not supported.

Gaia Operating System

- Updated the Gaia OS Linux kernel version to 4.18.
- CPView Utility saves its log messages in these files:
  - On a Management Server / Log Server / Security Gateway:R81.20_Scalable_Platforms.flprj
    - `$CPDIR/log/cpviewd.elg`
    - `$CPDIR/log/cpview_api_service.elg`
  - On a VSX Gateway:
    - `$CPDIR/log/cpviewd.elg.vs<VSID>`
    - `$CPDIR/log/cpview_api_service.elg.vs<VSID>`
- Added the Python v3.11 package.
- There is a dedicated messaging daemon `MSGD`..
- You can use the Gaia Clish command "`set dns timeout <value>`" to control how long Gaia OS waits for a response from a DNS server before it sends the DNS request to the next configured DNS server.
- The log files in the `$RTDIR/laas/adjuster_service/log/` directory moved from the root partition "`/`" to the `/var/log/` partition.
- The log file `$FWDIR/log/avi_del_tmp_files.elg` is now rotated based on the settings in the `/etc/cpshell/log_rotation.conf` configuration file.

VSX

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

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

VPN

- When a Check Point Management Server creates an IKE certificate, by default this certificate contains the "`Server Authentication`" attribute within the "`Extended Key Usage`" field.
- Changed the default value of "`Maximum concurrent IKE negotiations`" from 1,000 to 10,000 in the Security Gateway / ClusterXL object > the "`Optimization`" page.

Scalable Platforms

- On the Maestro Orchestrator MHO-175 ports, increased the default MTU size from 9216 to 10240 bytes.
- On a Maestro Security Group, in the output of the "`asg if`" command, the column header changed from "`Link State (ch1)/(ch2)`" to "`Link State (site1)/(site2)`".
- If an administrator stops a Maestro Orchestrator with the "`orchd stop`" command (or reboots it), and the Orchestrator detects that other Orchestrators on the Maestro Site are not operational, then before stopping (or rebooting) the Orchestrator shows a warning and a prompt to the administrator.

Security Gateway

- In the feature "Hide NAT behind IP Address Range", it is now possible to configure the Security Gateway to select the Hide NAT IP address based on the combination of the source IP address and the source port. See sk105302.

QoS

- QoS policy now supports different Service objects with the same Destination Port and different Source Ports.

SmartConsole

- Upgraded the SmartConsole .NET Framework from 4.5 to 4.8.
- Upgraded the SmartConsole Visual C++ Redistributable from 2012 to 2019.
- Hovering over the SmartConsole icon on the Windows OS taskbar now shows the SmartConsole version in the tooltip in this format:

  <IP_Address>-<Version>-SmartConsole

Supported Environments

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

Note - If after the upgrade to R82 you revert to the previous version, then Gaia OS boots with the 64-bit Gaia kernel, even if in the previous version the Gaia kernel was 32-bit.

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

Management Server and Log Server

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

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

(*) Applies to Public Cloud and to Private Cloud. See the *Hardware Compatibility List* > Section **Virtual Machines.**

Management High Availability:

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

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

Security Gateway or Cluster

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

Platforms	Security Gateway, Cluster	ElasticXL Cluster [3]
MLS200, MLS400	✓	✓
QLS250, QLS450, QLS650, QLS800	✓	✓
28600HS	✓	✓
26000, 26000T	✓	✓
23500, 23800, 23900	✓	✓
16000, 16200, 16600HS, 16600T	✓	✓
15400, 15600	✓	✓
7000	✓	✓
6200, 6400, 6500, 6600, 6700, 6800, 6900	✓	✓
5100, 5200, 5400, 5600, 5800, 5900	✓	✓ 5400 and stronger
3100, 3200, 3600, 3800	✓	–
64000, 44000 [1]	✓	–
Open Servers	✓	–
Virtual Machines [2]	✓	–

1. R82 supports only **SSM440** and **SGM400** in Scalable Chassis.
2. Applies to Public Cloud and to Private Cloud. See the *Hardware Compatibility List* > Section **Virtual Machines**.
3. ElasticXL Cluster supports only Check Point appliances that have the dedicated ports "Mgmt" and "Sync".

Standalone (Gateway + Management Server)

Only these platforms support R82 in the Standalone configuration:

Platforms	Standalone
16000, **16200**, **16600T** The model 16600HS does not support Standalone	✓
7000	✓
6200, **6400**, **6600**, **6700**, **6900** The models 6500, 6800 do not support Standalone	✓
3600, **3800** The models 3100, 3200 do not support Standalone	✓
Open Servers	✓
Virtual Machines (*)	✓

(*) Applies to Public Cloud and to Private Cloud. See the *Hardware Compatibility List* > Section **Virtual Machines.**

Threat Emulation Appliances

Platform	Security Gateway, Cluster
TE2000XN	✓
TE2000X	✓
TE1000X	✓
TE250XN	✓
TE250X	✓
TE100X	✓

Quantum Maestro

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

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

User Space Firewall (USFW)

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

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

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

   Applies to Private Cloud when you use only the Gaia ISO image.
3. CloudGuard Network Virtual Machines support USFW regardless of the number of available CPU cores.

   Applies to Public Cloud and to Private Cloud when you use only the native cloud image (`ova`, `qcow2`, and so on).

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

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
  - Single Zone High Availability Cluster
  - Cross Availability Zone Cluster (Cross AZ Cluster)
  - Security Gateway Auto Scaling Group
  - Gateway Load Balancer Virtual Machine Scale Sets
  - Security Management Server
  - Multi-Domain Server
  - Standalone
  - VPC Endpoint objects
- **Microsoft Azure**:
  - Security Gateway
  - High Availability Cluster
  - Virtual Machine Scale Sets
  - Gateway Load Balancer Virtual Machine Scale Sets
  - Security Management Server
  - Multi-Domain Server
  - Standalone
  - Virtual WAN

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

Supported Upgrade Paths

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 R82 is available only from these versions:

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

Current Version	Security Gateways and VSX [(1)]	Management Servers and Multi-Domain Servers	Standalone
R80.20.M2, **R80.20.M1**	*Not applicable*	Requires a 2-step upgrade path [(3)]	*Not applicable*
R80.10	Requires a 2-step upgrade path [(3)(6)]	Requires a 2-step upgrade path [(3)]	Requires a 2-step upgrade path [(3)(6)]
R80	*Not applicable*	Requires a 2-step upgrade path [(3)]	*Not applicable*
R77.30	Requires a 2-step upgrade path [(3)(5)(6)]	Requires a 2-step upgrade path [(3)(5)]	Requires a 2-step upgrade path [(3)(5)(6)]

Notes:

1. Starting from R81.10, VSLS is the only supported mode for **new** installations of **VSX Clusters** (does not apply to the VSNext mode).
   Upgrade of a VSX Cluster in the High Availability mode from R81.10 and earlier versions to R82 is supported.
   To convert the upgraded VSX Cluster to VSLS, use the "`vsx_util to convert`" command.
2. Upgrade from these versions to R82 is supported only with specific takes of a Jumbo Hotfix Accumulators.
   In Maestro environment, it is possible to upgrade Security Groups and Quantum Maestro Orchestrators (if you decide to upgrade, you must upgrade both).
3. The required 2-step upgrade path is:
   a. To R80.40, R81, R81.10, or R81.20
      See the applicable guide:
      - *R80.40 Installation and Upgrade Guide*.
      - *R81 Installation and Upgrade Guide*.
      - *R81.10 Installation and Upgrade Guide*.
      - *R81.20 Installation and Upgrade Guide*.

   b. To R82
4. The required 2-step upgrade path is:
   a. To R81.10 or R81.20 for Scalable Platforms
      See the applicable article:
      - sk173363 - R81.10 for Scalable Platforms
      - sk177624 - R81.20 for Scalable Platforms

   b. To R82
5. To upgrade an R77.30 environment that implements Carrier Security (former Firewall-1 GX), you must follow sk169415.
6. 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
      ```

Upgrade Methods

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

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

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

Check Point Product	Central Deployment in SmartConsole (1)	CPUSE Upgrade (2)	CPUSE Clean Install (3)	Advanced Upgrade (4)	Upgrade with Migration (5)	Upgrade with CDT (6)
Primary Endpoint Security Management Server	–	✓	✓	✓	✓	–
Secondary Endpoint Security Management Server	✓	✓	✓	✓	✓	–
Dedicated Log Server	✓	✓	✓	✓	✓	–
Dedicated SmartEvent Server	✓	✓	✓	✓	✓	–
Full High Availability Cluster Members	–	✓	✓	✓	✓	–
Standalone Server	–	✓	✓	✓	✓	–

Notes:

1. Central Deployment in SmartConsole:
   - You perform a remote installation of an upgrade package from SmartConsole.
   - You install the package from the local repository on the Management Server or from Check Point Cloud.
   - You can install the package on several targets at the same time.
   - For instructions, see the *R82 Security Management Administration Guide*.
2. CPUSE Upgrade (In-place Upgrade):
   - You perform a local installation of an upgrade package in Gaia Portal or Gaia Clish.
   - You install the package from the local repository in Gaia OS or from Check Point Cloud.
   - Keeps the current configuration and database.
   - For instructions, see the *R82 Installation and Upgrade 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 *R82 Installation and Upgrade Guide*.
4. Advanced Upgrade:
   - Intended for Management Servers only.
   - You perform a local installation of an upgrade package in Gaia Portal or Gaia Clish.
   - You install the package from the local repository in Gaia OS or from Check Point Cloud.
   - Requires these steps:
     a. Export of the current management database from the server.
     b. Upgrade of the server with CPUSE (In-place Upgrade or Clean Install).
     c. Import of the exported management database.
   - For instructions, see the *R82 Installation and Upgrade Guide*.
5. Upgrade with Migration:
   a. Intended for Management Servers only.
   b. You export of the current management database from the server.
   c. You install a different server with a higher version (Clean Install).
   d. You import of the exported management database.
   e. For instructions, see the *R82 Installation and Upgrade Guide*.

6. 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.
7. The minimum required unpartitioned disk space is the highest value of one of these:
   - Size of the current root partition.
   - The used space in the current root partition plus 3 GB.
   - If the used space is more than 90% of the root partition, then 110% of the size of the current root partition.

   Important:
   - 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.

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

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

Notes:

- Management Servers version R81.10 and lower **cannot** manage R82 Security Gateways / Security Groups / Clusters.
- Management Servers R82 do **not** support Security Gateways and VSX Gateways R77.30 or lower.

Quantum Maestro Orchestrator and Security Group Versions

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

- R82
- R81.20 (see sk177624)
- R81.10 (see sk173363)
- R81 (see sk169954)
- R80.30SP (see sk162552)
- R80.20SP (see sk138233)

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

Open Server Hardware Requirements

Minimum Hardware Requirements

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

ℹ For the SmartEvent requirements, see *"SmartEvent Requirements" on page 42*.

Disk Space Requirements

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

Notes:

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

Maximum Supported Physical Memory

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

Requirements

Threat Extraction Requirements for 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 an activated logging service. On dedicated Log Servers, the Log Server must be the same version as the Management Server.

SmartEvent Requirements

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

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

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

Hardware Requirements

For an average rate of 500 logs per second:

- Total CPU Cores: 4
- RAM: 16GB

SmartConsole Requirements

SmartConsole Hardware Requirements

This table shows the minimum hardware requirements for SmartConsole applications:

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

SmartConsole Software Requirements

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

SmartConsole is supported on:

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

Gaia Portal Requirements

The Gaia Portal supports these web browsers:

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

Mobile Access Requirements

OS Compatibility

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

Browser Compatibility

Endpoint Browser Compatibility	Microsoft Edge	Google Chrome	Mozilla Firefox	Apple Safari	Opera for Windows	Microsoft Internet Explorer
Mobile Access Portal	✓	✓	✓	✓	✓	✓
Clientless access to web applications (Link Translation)	–	✓	✓	✓	✓	✓
Compliance Scanner	✓	✓	✓	✓	–	✓
Secure Workspace (2), (3)	✓	✓	✓	–	–	✓
SSL Network Extender - Network Mode	–	✓	✓	✓	–	✓
SSL Network Extender - Application Mode (2)	✓	✓	✓	–	–	✓
Downloaded from Mobile Access applications	–	✓	✓	✓	–	✓
Citrix	–	✓	✓	–	–	✓
File Shares - Web-based file viewer (HTML)	✓	✓	✓	✓	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 sk134312.

AD Query

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

Harmony Endpoint Management Server Requirements

Hardware Requirements

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

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

The requirements for dedicated Endpoint Security Management Servers are similar.

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

Software Requirements

For more information, see the *R82 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.
- R82 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 R82 Primary Endpoint Security Management Server, follow the instructions in the *R82 Harmony Endpoint Security Server Administration Guide* when you select the Anti-Malware component.
- For a new R82 Endpoint Policy Server that was installed from scratch (not upgraded), you must follow sk127074.

  No additional steps are required, if you upgrade the Primary Endpoint Security Management Server to R82.
- Endpoint Security Clients can continue to acquire their Anti-Malware signature updates directly from an external Check Point signature server or other external Anti-Malware signature resources, if your organization's Endpoint Anti-Malware policy allows it.

Scalable Platform Requirements

- To manage R82 Security Groups on Maestro, use:

  1. R82 Quantum Maestro Orchestrator.
  2. R82 Security Management Server or Multi-Domain Server.

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

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

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

  - R82 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`
	You cannot use this network card with a splitter cable to split a port on an appliance.

40 GbE Fiber QSFP+
SKU:
CPAC-2-40F-B
	The minimal required card firmware version is 12.22.1002
	To make sure the version is correct, run this single long command in the Expert mode on the Security Appliance:
	`for NIC in $(ifconfig | grep ethsBP | awk '{print $1}') ; do echo $NIC: ; ethtool -i $NIC | grep firmware ; done`
	Example output:
	`ethsBP4-01:`
	`firmware-version: 12.22.1002`
	`ethsBP4-02:`
	`firmware-version: 12.22.1002`
	You cannot use this network card with a splitter cable to split a port on an appliance.

10 GbE Fiber SFP+
SKUs:
CPAC-4-10F-B
CPAC-4-10F-6500/6800-C
	Output of the "`lspci -v`" command must show:
	`Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection`
	To verify, run this command in the Expert mode on the Security Appliance:
	`lspci -v | grep 'Ethernet controller' | grep Intel`

Supported Hardware and Firmware on 60000 / 40000 Scalable Chassis

All information is documented in sk93332.

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	
Objects in each Group object	12,000	Yes	
Rules in each 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.
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*. To ensure optimal API responsiveness, we recommend configuring a maximum of 600 interfaces with API.

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

See sk178325.

Maximum Supported Number of Interfaces on Security Gateway

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

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

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

Maximum Supported Number of Cluster Members

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

Number of Supported Items in an ElasticXL Cluster

Item	Number of Supported Items	Notes
Number of Security Appliances in one ElasticXL Cluster	In Single Site and Dual Site deployment: ▪ Minimum: 1 on each Site ▪ Maximum: 3 on each Site	In a Dual Site deployment, an ElasticXL Cluster must contain a minimum of one Security Appliance from each site.
Number of interfaces configured in one ElasticXL Cluster	In 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).

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 sk181128). ▪ Each Security Group can contain a maximum of 28 Security Appliances - 14 Security Appliances from each site (see MBS-7773 in sk181128).
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

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

Check Point Product	Windows 11 [4]	Windows 10 [5]	Windows 8.1 [6]	Windows 7 (+SP1) [7]
Endpoint Security Clients [1]	✓	✓	✓ (with 8.1 Update 1)	✓ [3]
Remote Access clients [1]	✓	✓	✓ (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)	✓	✓	✓	✓	✓	✓
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 13	macOS 12	macOS 11	macOS 10.15	macOS 10.14	macOS 10.13	macOS 10.12	OS X 10.11
Identity Agent for a User Endpoint Computer [1]	✓	✓	✓	✓	✓	✓	✓	✓
Endpoint Security Clients [2]	✓	✓	✓	✓	–	–	–	–
Endpoint Security VPN [2]	✓	✓	✓	✓	–	–	–	–
SSL Network Extender	–	–	✓	✓	✓	✓	✓	✓

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 R82 DLP Exchange Security Agent is supported on:

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

Licensing

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