QUANTUM

29 May 2025

# QUANTUM CYBER SECURITY PLATFORM

## R82

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 R82

For more about this release, see the R82 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 |
|---|---|
| 29 May 2025 | ▪ Updated *"Management Server and Log Server" on page 33*<br>• Added Smart-1 7000-UL, Smart-1 7000-XL, and Smart-1 7000-L<br>• Added Smart-1 700-M and Smart-1 700-S<br>▪ Updated *"Threat Emulation Appliances" on page 41*<br>• Threat Emulation Appliances do not support R82 |
| 21 May 2025 | Updated:<br>▪ *"Standalone and Full High Availability" on page 38* |
| 25 April 2025 | Updated:<br>▪ *"Scalable Platforms Requirements" on page 70*<br>Removed:<br>▪ "Supported Clients and Agents" - this information is documented in the corresponding product documentation |
| 06 January 2025 | Updated:<br>▪ *"Management Server and Security Gateway Versions" on page 58* - notes below the table |
| 29 December 2024 | Updated:<br>▪ *"Supported Upgrade Paths" on page 46* - required Takes of Jumbo Hotfix Accumulators for upgrading Scalable Platforms to R82 |
| 18 December 2024 | Improved formatting |
| 13 November 2024 | Updated:<br>▪ *"Threat Emulation Appliances" on page 41* - TE250XN and TE2000XN do not support R82 |
| 30 October 2024 | Updated:<br>▪ *"What's New" on page 11* - removed the "Threat Prevention Dashboards" section. |

| Date | Description |
|---|---|
| 23 October 2024 | Updated *"Software Changes" on page 25*:<br>- In the section "Quantum Maestro, Scalable Chassis, and ElasticXL", updated the list of deprecated CLI commands.<br>- In the section "Gaia Operating System", added the new default disk space limit for storing core dump files. |
| 21 October 2024 | First release of this document. |

# Table of Contents

# Important Links

For more about R82, see:

- Quantum R82 Home Page
- Quantum R82 Known Limitations
- Quantum R82 Resolved Issues and Enhancements

Visit the *Check Point CheckMates Community* to:

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

Visit *Check Point Infinity Consolidated Security Architecture*.

# What's New

## Introduction

**R82** is Check Point's major software release for Quantum products and CloudGuard Network Security. It introduces 50 innovative capabilities to strengthen threat prevention, greatly streamline operations and provisioning, and troubleshoot network connections with integrated diagnostics tools.

This release provides access to new AI-powered threat prevention engines that strengthen defense against zero-day phishing, brand spoofing, malware, and more. R82 also adds DNS protection against NXNS, offers DNS configuration granularity, and supports DNS-over-HTTPS Inspection.

Check Point offers the industry's first complete protection for HTTP/3 over QUIC. R82 also enables effortless and automated HTTPS Inspection deployment with granular controls and exceptional performance.

Check Point's VSX has a new versatile mode (VSNext) that unifies management features and APIs across Virtual Systems and physical Security Gateways. Furthermore, cluster management is greatly simplified with a new page in Gaia Portal and a new mode (ElasticXL) that enables Security Gateway clustering without the need for physical Orchestrators.

In addition, R82 introduces a new version of Check Point's operating system with superior networking and routing capabilities. For automation, users and DevOps teams can now execute API calls directly to security gateways through a new dynamic policy layer. For future-proofing, R82 enables NIST-approved Kyber (ML-KEM) encryption to protect today’s VPN traffic against future quantum computing-based hacking.

These are just some of the powerful new capabilities in R82.

## Threat Prevention

### AI-based prevention engines

Check Point's new AI security engines represent a shift in how we utilize data, transitioning from mostly a single indicator perspective to a multi-dimensional approach.

- ThreatCloud Graph - Leverages ThreatCloud AI knowledge base to form relationship graph, identifying attacks patterns to prevent zero-day threats.
- **Kronos** - Inspects behavior over time with AI and signal processing algorithms to detect malicious activity, preventing zero-day C2, phishing campaigns and other threats.

- **Deep Brand Clustering** - Prevents zero-day brand phishing campaigns with a patent-pending unsupervised deep learning engine. This engine cluster websites into local and global brands and determine whether it’s an attack.
- **Dynamic classification of uncategorized websites** - An AI-based engine for dynamic classification of websites, accurately categorizing URLs to block previously uncategorized dangerous or inappropriate websites.

## Improved DNS Security Capabilities

This release provides new and enhanced DNS security capabilities with the addition of:

- **Advanced DNS protection against Non-Existent Domain (NXNS) Attack**.
- **Support for DNS over HTTPS (DoH) protocol**.
- **Configuration Granularity** - Advanced DNS Security settings in the Threat Prevention profile.
- **Detailed DNS Security statistics** - Now available in the SmartView Dashboard.

## Automatic Security Services Configuration

Zero Phishing, Anti-Virus, Anti-Bot and IPS Software Blades are now more accessible, providing a simpler and easier user experience.

- Zero Phishing Software Blade - Introducing a new **Automatic mode** that significantly simplifies the configuration process, providing a seamless experience. With the Automatic mode, the Software Blade configuration is now effortless: simply enable the Software Blade and you are ready to go.
- The Anti-Virus and Anti-Bot Software Blades are now activated by default in newly created Security Gateway and Cluster objects.
- It is now possible to automatically load and update SNORT rules file as Custom Intelligence Feed and enforce them as new IPS protections.

## Web Security

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

# HTTPS Inspection

This release sets a new standard with breakthrough performance, unmatched simplicity, and effortless deployment of HTTPS Inspection. Now, you can significantly increase your security without sacrificing speed or user experience. Embrace cutting-edge technology that transforms HTTPS Inspection into a seamless, innovative solution, ensuring your systems stay secure and your users stay satisfied.

- **Enhanced HTTPS Inspection UI** - HTTPS Inspection is fully managed in SmartConsole:
  - **Enhanced HTTPS Inspection policy** - A dedicated policy for inbound inspection, including certificate management views for both inbound and outbound policies and enhanced default outbound policy.
  - **Trusted CA package** - A new view to manage Trusted certificates and see the status of the trusted CA package
  - **HTTPS Inspection Advanced settings** - A new view to configure advanced settings, including R82 new features.
- **Client Side Fail mode** - This new feature automatically detects failures in inspected TLS connections caused by client-side issues, such as certificate-pinned applications. When a failure is detected, the connection is flagged to be bypassed in future attempts, and Artificial intelligence (AI) learns from these failures to identify similar connections.
  - **Endpoint Detection** - Identifies endpoints without deployed outbound CA certificate.
- **Learning mode**:
  - **Gradual & Smart deployment** - Activated during the deployment of HTTPS Inspection, inspecting a minor percentage of traffic over two weeks.
  - **Network Learning** - Gathers insights into network behavior and detects potential connectivity issues for Artificial intelligence consideration.
  - **Performance Prediction** - Estimates the impact on performance when HTTPS Inspection is fully implemented.
- **Bypass Under Load** - Bypasses TLS connections when the Security Gateway experiences high CPU load.
- **HTTPS Inspection monitoring** - Introducing the HTTPS Inspection statistics view in SmartView, including bypass/inspect statistics.

# Quantum Security Gateway

## 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 on the Security Gateway in seconds without involving Security Management or installing Security Policy.

## Identity Awareness

- Quantum Gateways can now use multiple external Identity Providers defined in the Check Point Infinity Portal, providing a cross product unified identity management.

- Improved resiliency in case of connectivity loss to the PDP by adding new Identity Cache Mode for Identity Sharing protocols.

# IPsec VPN

- Added support for ML-KEM (Kyber768) as required by the FIPS 203 standard to address Post-Quantum Cryptography (PQC).
- 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 public IP addresses as tunnel identifiers to establish separate tunnels for each link.
    - 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 (E88.40 and higher).

# 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 *Check Point Management API Reference* > section "*Mobile Access*".

# 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.
- Route age information.
- IPv4 PIM-SSM with non-default prefixes.
- IPv4 PIM with BFD.
- IPv4 PIM neighbor filtering.
- IPv4 PIM RPT to SPT switchover control.
- IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).

Added support for new Dynamic Routing API calls:

- 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 *Check Point Gaia API Reference* v1.8 (and higher) > section "*Networking*".

# Performance and Infrastructure

- HyperFlow acceleration of elephant flows for the SMB/CIFS protocol.
- HyperFlow acceleration of elephant flows for the QUIC protocol.
- Quantum Security Gateway log rate output capacity increased by up to 100% through a new multi-process architecture.

## Quantum Maestro, Scalable Chassis, and ElasticXL

This release features improvements in managing and monitoring Scalable Platform clusters, which include:

- Support for REST API:
  - New API calls on Quantum Maestro Orchestrator to configure and monitor Maestro Security Groups, Gateways, Sites, and Ports.

    See the complete list of available API calls in the *Check Point Gaia API Reference* v1.8 and higher > section "*Maestro*".
  - Support for Gaia REST APIs on Scalable Platform Members.
- Support for Gaia First Time Configuration Wizard on Quantum Maestro Orchestrators with ability to configure the Maestro Site settings.
- Support for authentication to secure the synchronization connections between Quantum Maestro Orchestrators.
- Support for SNMP Queries on each Security Group Member.
- Support for LLDP on Uplink, Sync, and Management ports of Quantum Maestro Orchestrators.
- New page "Ports" in Gaia Portal on Quantum Maestro Orchestrator. This page shows a summary and interactive view of port configuration, runs diagnostics on ports, and blinks a port LED for identification.
- New page "Cluster Management" in Gaia Portal on ElasticXL / Security Group. This page shows the state and performance of Scalable Platform Members.
- "`insights`" - New CLI tool to monitor the entire Scalable Platform cluster in both Expert mode and Gaia gClish.
- New Gaia gClish commands "`show cluster`" and "`set cluster`".
- Improved boot time and decreased number of reboots of Scalable Platform Members when there is a change in the Gaia OS configuration in a Scalable Platform.
- Improved upgrade simplicity:
  - This release introduces automatic updates for the CPUSE Deployment Agent on Scalable Platforms. Manual deployment is no longer required.
  - Upgrade to R82 and higher no longer requires the "`sp_upgrade`" script and can be easily monitored with Scalable Platform monitoring tools.
- Additional snapshot mechanism to take small Gaia OS snapshots (lightshots).

# VSX

Check Point VSX is enhanced with a new mode (**VSNext**), 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.
- Managing different Virtual Gateways with different Security Management Servers, in addition to different Domain Management Servers on the same Multi-Domain Security Management Server.

# Tools and Utilities

- New tool "`connview`" - a new consolidated troubleshooting tool for viewing connections information on the Security Gateway that works in the User Space Firewall (USFW).
- New tool "`fw up_execute`" - performs virtual Access Control / NAT Rule Base execution. Given inputs based on logs or connections, the execution provides detailed information such as matched rules and classification information.

# Gaia Operating System

**Note** - This section applies to Security Gateways, Management Servers, and Log Servers.

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 Link Layer Discovery Protocol (LLDP) in the VSX mode.
  - DHCPv6 server, DHCPv6 client, and DHCPv6 client for prefix-delegation in Gaia Portal and Gaia Clish.
  - 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 OS 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 in Gaia Portal and Gaia Clish.
  - NFSv4 configuration.
  - Keyboard layout.
  - TLS configuration for a remote Syslog server in Gaia Portal and Gaia Clish.
- Support for storing a Gaia OS backup in Amazon S3 and Microsoft Azure and restoring it from there.

# 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 *Check Point Management API Reference* > 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 *Check Point Management API Reference* > section "Data Types".
- Security Gateways can now be managed by a Security Management Server hosted behind a public cloud or third-party NAT device.
- Support to manage up to 500 Security Gateways / Cluster Members, allowing concurrent policy installation on all managed Security Gateways / Cluster Members. See *"Maximum Supported Items" on page 71*.
- Support for SAML login in SmartConsole when Gaia Portal on the Management Server runs on a different port than the default port 443. See sk182032.
- Ability to verify an Access Control policy that contains unpublished changes.
- The "Access Rule Name" and "Access Rule Number" fields will now prioritize information from administrator-defined rules by excluding Accept rules from the pre-defined Playblocks and IoT Access Policy layers.

## SmartConsole

- Added the ability for the system account to install SmartConsole.
- Enhancements in the SmartConsole > "Gateways & Servers" view:
  - You can now see and manage the Recommended Jumbo Hotfix Accumulators and Recommended Software Updates for Security Gateway / Cluster objects and Check Point Host objects.
  - HealthCheck Point (HCP) tests are now integrated. You can see them as part of the Security Gateway's status. The feature is disabled by default.

## Web SmartConsole

- These new Web SmartConsole capabilities are available for this release:
  - Threat Prevention Rule Base
  - HTTPS Inspection Rule Base
  - NAT Rule Base
  - Rule Base search

## 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 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 support for IPv6 configuration (only with Management API "`set mds`") on a Multi-Domain Security Management Server that allows Domains to communicate with the managed Security Gateways over IPv6.
- Automatic refresh of modified Global objects in SmartConsole that is connected to a non-Global Domain when a superuser assigns a Global Policy to a Domain Management Server. See sk182307.
- Ability to select the Access Control, Threat Prevention, or both policies in a Policy Preset object.

## Compliance

- Added Gaia OS Best Practice support for Quantum Maestro- presenting a consolidated Best Practices status for each Security Group Member and Orchestrators.
- Added Gaia OS Best Practice support for Quantum Spark Appliances (only for applicable Gaia OS Best Practices).
- Added Gaia OS Best Practice support for Log Servers.
- Added new regulations:
  - Center for Internet Security Benchmarks
  - Cyber Essentials v3.1
  - Cybersecurity Maturity Model Certification
  - Essential Eight & Strategies to Mitigate Cyber Security Incidents
  - IEC 62443-2-1 201
  - ISO 27001:2022
  - Israeli Cyber Defense Methodology 2.0
  - Network and Information Systems Directive 2
  - PCI DSS 4.0
  - TISAX 5.1

# CloudGuard Network Security

## CloudGuard Controller

- CloudGuard Controller now supports Identity Awareness PDP (Identity Sharing).
- CloudGuard Controller now supports VMware NSX-T Global Manager to allow integration with VMware NSX-T v4.1.
- CloudGuard Controller for VMware NSX-T now uses Policy Mode APIs to import objects from an NSX-T Manager.
- Multi-Domain Security Management Server now supports Data Center objects and Data Center Query objects in the Global Policy.

# Harmony Endpoint Web Management

- Client optimization for Windows servers - Harmony Endpoint now 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 - Using the Push Operation, an administrator can run a diagnostic check on endpoint clients.

  The reports show the total CPU and RAM usage for the last 12 hours, including the CPU usage by processes. Based on the report data, Harmony Endpoint may offer suggested exclusions to optimize the endpoint performance. You can easily add an exclusion as part of "Global Exclusion" or "Exclusion per Rule".
- Exclusions Enhancements:
  - **Exclusion description** - You can now add comments to new or existing exclusions.
  - **Global Exclusion** - You can now easily add global exclusions that apply 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.
- Support for **Harmony Endpoint Management API** on an on-premises Endpoint Security Management Server.

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

# 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.
- The search in SmartConsole Object Explorer and "Objects" sidebar was improved in a specific scenario. The partial search in text fields (name of an object, comment, and so on) does not require entering the wildcard character "*"(asterisk) anymore. See sk182006.

# 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:
    - `$CPDIR/log/cpviewd.elg`
    - `$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.
- Introducing 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.
- More user space log files are now rotated based on the settings in the `/etc/cpshell/log_rotation.conf` configuration file.
- The name template of a Gaia regular backup file changed:

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

  to "`backup_--_<HostName>.<Domain>_<YYYY>_<MM>_<DD>_<HH>_<MM>_<SS>.tgz`"
- The name template of a Gaia scheduled backup file changed:

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

  to "`backup_-<Name_of_Scheduled_Backup>-_<HostName>.<Domain>_<YYYY>_<MM>_<DD>_<HH>_<MM>_<SS>.tgz`"
- User Space Firewall (USFW) is now enabled by default on all environments except Threat Emulation (TE) Appliances and Standalone setup.
- Default disk space limit for storing core dump files was increased:

- Management Server - from 1000 MB to 5000 MB
- Security Gateway in the Kernel Space Firewall (KSFW) mode - from 1000 MB to 5000 MB
- Security Gateway in the User Space Firewall (USFW) mode - from 10000 MB to 15000 MB

# VSX

- In the Traditional 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 System 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.
- Changed the default value of the kernel parameter "`cphwd_medium_path_qid_by_mspi`" from 1 to 0.
- Changed the default value of the kernel parameter "`cphwd_medium_path_qid_by_cpu_id`" from 0 to 1.

# Quantum Maestro, Scalable Chassis, and ElasticXL

- Newly added Scalable Platform Security Group Member always clones the image from the SMO Security Group Member, regardless of the SMO Image Cloning state.
- Outputs of CLI commands were unified to use the same terms on an ElasticXL Cluster, a Maestro Security Group, and a Scalable Chassis:
  - "Site" instead of "Chassis"
  - "Member" instead of "SGM"
  - The hostname shows the letter "`s`" instead of the letters "`ch`" (for example, `SG-s01-01`)
- The feature name changed from "Unique IP Address per Chassis" (UIPC) to "Unique IP Address per Site" (UIPS).
- On the Maestro Orchestrator MHO-175 ports, increased the default MTU size from 9216 to 10240 bytes.
- Automated creation of the management bond interface (MAGG).

  All management interfaces assigned to a Security Group are automatically assigned to this MAGG interface.
- 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.
- When an administrator changes the administrative state of a port on a Maestro Orchestrator, this change now survives an Orchestrator reboot and the restart of the Orchestrator daemon with the "`orchd restart`" command.
- On the Orchestrator, the Gaia Portal > **Network Management** section > **Network Interfaces** page now hides interfaces that are used for internal purposes:
  - `Sync-ext`
  - `Sync-int`
  - `dl<`*`number`*`>`
  - `eth<`*`number`*`>`
  - `eth<`*`number`*`>-CIN<`*`number`*`>`
  - `swid0_eth`

- On the Maestro Orchestrator, it is no longer supported to convert an existing Security Group from the 'Gateway' mode to the 'VSX' mode (by selecting the corresponding checkbox in the Security Group properties).
- The output of the Gaia gClish / Gaia Clish command "`show interfaces`" on Scalable Platforms was aligned with the output of this command on a regular Security Gateway.
- These CLI commands were deprecated and replaced:

| Deprecated Command | Use this Command in the Expert mode | Use this Command in Gaia gClish |
|---|---|---|
| `asg cluster_site_admin` | • `cluster_site_admin -c <Site ID> {down \| up}` | • `set cluster site-id <Site ID> admin-state {up \| down}`<br>• `set cluster sites-admin-state id <Site ID> {down \| up}` |
| `asg conns` | • `insights`<br>• `cluster-cli show connection --help`<br>• `g_connview --help` | • `insights`<br>• `show cluster info connection <parameter>` |
| `asg cores_stat` | • `insights`<br>• `cluster-cli show cpu` | • `insights`<br>• `show cluster info cpu` |
| `asg diag`<br>`asg_diag`<br>`asg6 diag` | • `insights`<br>• `hcp --help` (run the applicable tests) | • `insights` |
| `asg if`<br>`asg_if`<br>`asg6 if` | • `insights`<br>• `hcp --help` (run the applicable tests)<br>• `cluster-cli show interfaces` | • `insights`<br>• `show cluster info interfaces` |

| Deprecated Command | Use this Command in the Expert mode | Use this Command in Gaia gClish |
|---|---|---|
| `asg perf` | • `insights`<br>• `cluster-cli show --help` | • `insights`<br>• `show cluster info <parameter>` |
| `asg resource`<br>`asg6 resource` | • `insights`<br>• `cluster-cli show --help` | • `insights`<br>• `show cluster info <parameter>` |
| `asg search`<br>`asg6 search` | • `insights`<br>• `cluster-cli show connection --help` | • `insights`<br>• `show cluster info connection <parameter>` |
| `asg_bond` | • `hcp --help` (run the "Bond Health" test) | • N / A |
| `asg_chassis_admin` | • `cluster_site_admin -c <Site ID - 1 or 2> {down \| up}` | • N / A |
| `toggle_same_vmac` | • `toggle_same_vmac_os` | • N / A |
| • `show chassis id {1\|2} general unique_ip`<br>• `set chassis id {1\|2} general unique_ip`<br>• `delete chassis id {1\|2} general unique_ip` | • N / A | • `show cluster configuration unique-ip <Site ID> interface <parameters>`<br>• `set cluster configuration unique-ip <Site ID> interface <parameters>`<br>• `delete cluster configuration unique-ip site-id <Site ID> interface <parameters>` |

| Deprecated Command | Use this Command in the Expert mode | Use this Command in Gaia gClish |
|---|---|---|
| • `show chassis high-availability <parameters>`<br>• `set chassis high-availability <parameters>` | • N / A | • `show cluster configuration high-availability <parameters>`<br>• `set cluster configuration high-availability <parameters>` |
| • `show smo`<br>• `set smo`<br>• `delete smo` | • N / A | • `show cluster <parameters>`<br>• `set cluster <parameters>` |
| `asg_collect_vsx_logs` | • `cpinfo -h` (see sk92739) | • `cpinfo -h` (see sk92739) |
| `drop_monitor` | • N / A | • N / A |
| `asg_affinity_enhance` | • N / A | • N / A |

**Notes:**

- In the Expert mode, the command "`cinfo`" is the alias for the command "`cluster-cli show info`".
- For information about the new commands, see the *R82 Scalable Platforms Administration Guide* > Chapter "Working with Command Line".

# 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.
- Improved the output of the `adlogconfig` command. See the *R82 CLI Reference Guide*.
- In the Threat Prevention Engine Settings, the default "Connection Unification" period changed from 600 minutes to 180 minutes (in SmartConsole, click "Manage & Settings" > "Blades" > in the "Threat Prevention" section, click "Advanced Settings" > click the "General" page).

# Mobile Access

- Changed the default value of the "`max_concurrent_vpn_tunnels`" parameter from 200 to 10000 in VSX environments.

# 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
  ```
- The "HTTPS Inspection" tab was removed from the Legacy SmartDashboard.

# Supported Environments

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

**Notes:**

- 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.
- For documentation about Check Point Appliances, see sk96246.
- Refer to the Support Life Cycle Policy page for more information and announcements.

## Management Server and Log Server

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

| Check Point Product | Smart-1 7000-UL,<br>Smart-1 7000-XL,<br>Smart-1 7000-L | Smart-1 700-M,<br>Smart-1 700-S | Smart-1 6000-XL,<br>Smart-1 6000-L,<br>Smart-1 5150,<br>Smart-1 5050 | Smart-1 625,<br>Smart-1 600-M,<br>Smart-1 600-S,<br>Smart-1 410,<br>Smart-1 405 | Open Servers | Virtual Machines |
|---|---|---|---|---|---|---|
| **Security Management Server, Endpoint Security Management Server** | Yes | Yes | Yes | Yes | Yes | Yes |
| **Log Server** | Yes | Yes | Yes | Yes | Yes | Yes |
| **SmartEvent Server** | Yes | Yes | Yes | Yes | Yes | Yes |

| Check Point Product | Smart-1 7000-UL,<br>Smart-1 7000-XL,<br>Smart-1 7000-L | Smart-1 700-M,<br>Smart-1 700-S | Smart-1 6000-XL,<br>Smart-1 6000-L,<br>Smart-1 5150,<br>Smart-1 5050 | Smart-1 625,<br>Smart-1 600-M,<br>Smart-1 600-S,<br>Smart-1 410,<br>Smart-1 405 | Open Servers | Virtual Machines |
|---|---|---|---|---|---|---|
| **Multi-Domain Security Management Server** | Yes | **No** | Yes | **No** | Yes | Yes |
| **Multi-Domain Log Server** | Yes | **No** | Yes | **No** | Yes | Yes |

1. For information about Smart-1 7000-UL, Smart-1 7000-XL, and Smart-1 7000-L, see sk182601.
2. For information about Smart-1 700-M and Smart-1 700-S, see sk182601.
3. For information about Smart-1 6000-L and Smart-1 6000-XL, see sk171903.
4. For information about Smart-1 600-S and Smart-1 600-M, see sk171903.
5. For information about Smart-1 5050 and Smart-1 5150, see sk120453.
6. For information about Smart-1 625, see sk157153.
7. For information about Smart-1 405 and Smart-1 410, see sk117578.
8. "Virtual Machines" apply to Public Cloud and to Private Cloud. See the *Hardware Compatibility List* > Section **Virtual Machines**.
9. 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 R82 in the Security Gateway or Cluster configuration:

| Platforms | SK | Security Gateway, Cluster (3) | ElasticXL Cluster (4,5) |
|---|---|---|---|
| **MLS200, MLS400** | sk176466 | Yes | Yes |
| **QLS250, QLS450, QLS650, QLS800** | sk176466 | Yes | Yes |
| **29100, 29200** | sk180520 | Yes | Yes |
| **28000, 28600HS** | sk152733 | Yes | Yes |
| **26000, 26000T** | sk152733 | Yes | Yes |
| **23500, 23800, 23900** | sk107516 | Yes | Yes |
| **19100, 19200** | sk180520 | Yes | Yes |
| **16000, 16200, 16600HS, 16600T** | sk152733 | Yes | Yes |
| **15400, 15600** | sk107516 | Yes | Yes |
| **9100, 9200, 9300, 9400, 9700, 9800** | sk181698 | Yes | Yes |
| **7000** | sk139932 | Yes | Yes |
| **6200, 6400, 6500, 6600, 6700, 6800, 6900** | sk139932 | Yes | Yes |
| **5100, 5200, 5400, 5600, 5800, 5900**<br>The models 5100, 5200 do not support ElasticXL | sk110053 | Yes | Yes |
| **3100, 3200, 3600, 3800** | sk110052 | Yes | **No** |
| **64000, 44000** (1) | sk65305 | Yes | **No** |
| **Open Servers** | N / A | Yes | **No** |
| **Virtual Machines** (2) | N / A | Yes | **No** |

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. "Cluster" refers to ClusterXL (Active-Active, High Availability, Load Sharing) and VRRP Cluster on Gaia OS.
4. ElasticXL Cluster supports only Check Point appliances that have the dedicated ports called "**Mgmt**" and "**Sync**".
5. ElasticXL Cluster requires the supported Check Point appliance to run SecureXL in the Kernel Mode (KPPAK).

   The Gaia First Time Configuration Wizard changes the SecureXL mode automatically to KPPAK.

# Standalone and Full High Availability

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

| Platforms | SK | Standalone (1),<br>Full HA |
|---|---|---|
| **23500**, **23800**, **23900** | sk107516 | Yes (2) |
| **15400**, **15600** | sk107516 | Yes (2) |
| **9100**, **9200**, **9300**, **9400**, **9700**, **9800**<br>(must change the SecureXL mode from UPPAK to KPPAK) | sk181698 | Yes (1) |
| **7000** | sk139932 | Yes |
| **6200**, **6400**, **6600**, **6700**, **6900**<br>The models 6500, 6800 do not support Standalone | sk139932 | Yes |
| **5900** | sk110053 | Yes |
| **5100**, **5200**, **5400**, **5600**, **5800** | sk110053 | Yes (2) |
| **3100**, **3200**, **3600**, **3800** | sk110052 | Yes |
| **Open Servers** | N / A | Yes |
| **Virtual Machines** (3) | N / A | Yes |

1. Standalone configuration requires SecureXL to run in the Kernel Mode (KPPAK).

   As a result, the Firewall can run only as the Kernel Space Firewall (KSFW).

   To change the SecureXL mode, run the `cpconfig` command > select "`Check Point SecureXL`" > select "`Change SecureXL Mode`" > reboot.

2. These appliance models support Standalone only with the HDD storage.

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

3. Applies to Public Cloud and to Private Cloud. See the *Hardware Compatibility List* >

Section **Virtual Machines**.

4. It is not supported to enable the SmartEvent Software Blade on any Management Server in the Full High Availability Cluster configuration.

# VSNext and Traditional VSX

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

| Platforms | VSNext [1] | Traditional VSX |
|---|---|---|
| **ElasticXL Cluster** [2] | Yes [3] | **No** |
| **Security Group - Maestro** | Yes [4] | Yes [5] |
| **Security Group - Scalable Chassis** | **No** | Yes [6] |
| **Open Servers** | **No** | Yes [6] |
| **Virtual Machines** | **No** | Yes [6] |

1. Support for IPv6 in VSNext configuration is planned for the R82 Jumbo Hotfix Accumulator (PMTR-107345).
2. ElasticXL Cluster requires the supported Check Point appliance to run SecureXL in the Kernel Mode (KPPAK).

   The Gaia First Time Configuration Wizard changes the SecureXL mode automatically to KPPAK.
3. The Security Appliances must be after a clean install, or restored to factory defaults.

   In the First Time Configuration Wizard, you must select **ElasticXL** and **Install as VSNext**.

   Converting to VSNext after the First Time Configuration Wizard is not supported.

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

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

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

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

     For each Virtual Gateway you configure in this Maestro Security Group, in SmartConsole you configure a regular Security Gateway object.

   - Traditional VSX mode in a Maestro Security Group that runs the version R81.20 or lower.

     In SmartConsole, you configure a VSX Gateway object and the required Virtual System / Virtual Switch objects.

5. To configure a Maestro Security Group that runs the R82 version in the Traditional VSX mode:

   a. Create a new Maestro Security Group and in the **First Time Wizard settings** section, do **not** select **Install as VSNext / VSX**.

   b. In SmartConsole, configure a VSX Gateway object and the required Virtual System / Virtual Switch objects.

6. The Gaia Operating System must be after a clean install, or restored to factory defaults.

   In SmartConsole, you configure a VSX Gateway object and the required Virtual System / Virtual Switch objects.

# Threat Emulation Appliances

| Platform | SK | Security Gateway, ClusterXL |
|---|---|---|
| **TE2000XN** | sk173494 | **No** |
| **TE2000X** | sk106210 | **No** |
| **TE1000X** | sk106210 | **No** |
| **TE250XN** | sk173494 | **No** |
| **TE250X** | sk106210 | **No** |
| **TE100X** | sk106210 | **No** |

# Quantum Maestro

Quantum Maestro Orchestrator models MHO-140, MHO-170, and MHO-175 fully support the R82 release. See sk181127.

For the list of supported Maestro Security Group versions, see *"Quantum Maestro Orchestrator and Security Group Versions" on page 59*.

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 (USFW) mode by default (see sk167052):

| Platform | SK | USFW |
|---|---|---|
| **All supported Check Point Appliances** (*) | sk96246 | Yes |
| **Open Servers** | N / A | Yes |
| **Virtual Machines** | N / A | Yes |
| **CloudGuard Network Security for Public Cloud** | N / A | Yes |
| **CloudGuard Network Security for Private Cloud** | N / A | Yes |

**Notes:**

- For the list of the supported appliances, see the section *"Security Gateway or Cluster" on page 36*.
- These appliances do not support USFW:
  - Threat Emulation Appliances
  - Check Point Appliances in the Standalone configuration

# SecureXL User Mode (UPPAK)

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

| Platforms | SK | UPPAK (1) |
|---|---|---|
| **QLS250**, **QLS450**, **QLS650**, **QLS800** (2) | sk176466 | Yes |
| **29100**, **29200** | sk180520 | Yes |
| **19100**, **19200** | sk180520 | Yes |
| **9100**, **9200**, **9300**, **9400**, **9700**, **9800** | sk181698 | Yes |

**Notes:**

1. On the supported Check Point appliances, the default SecureXL mode is the User Mode (UPPAK).
   On all other supported Check Point appliances (see the section *"Security Gateway or Cluster" on page 36*), SecureXL runs only in the Kernel Mode (KPPAK).
2. Support for the SecureXL User Mode (UPPAK) in Maestro configuration is planned for the R82 Jumbo Hotfix Accumulator. See sk179432.
3. 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"
4. 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
  - 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
- **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)
  - Network Security Integration (NSI)
  - 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

## 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 Traditional VSX (1) | Management Servers and Multi-Domain Servers | Standalone |
|---|---|---|---|
| **R81.20**,<br>**R81.10**,<br>**R81**,<br>**R80.40** | Yes | Yes | Yes |
| For Scalable Platforms:<br>**R81.20**,<br>**R81.10** | Requires a Jumbo Hotfix (2) | *Not applicable* | *Not applicable* |
| For Scalable Platforms:<br>**R81,**<br>**R80.30SP**,<br>**R80.20SP** | Requires a 3-step upgrade path (3) | *Not applicable* | *Not applicable* |

| Current Version | Security Gateways and Traditional VSX (1) | Management Servers and Multi-Domain Servers | Standalone |
|---|---|---|---|
| **R80.30 kernel 3.10**,<br>**R80.30 kernel 2.6**,<br>**R80.20 kernel 3.10**,<br>**R80.20 kernel 2.6** | Requires a 2-step upgrade path (4) | Requires a 2-step upgrade path (4) | Requires a 2-step upgrade path (4) |
| **R80.20.M2**,<br>**R80.20.M1** | *Not applicable* | Requires a 2-step upgrade path (4) | *Not applicable* |
| **R80.10** | Requires a 2-step upgrade path (4)(6) | Requires a 2-step upgrade path (4) | Requires a 2-step upgrade path (4)(6) |
| **R80** | *Not applicable* | Requires a 2-step upgrade path (4) | *Not applicable* |
| **R77.30** | Requires a 2-step upgrade path (4)(5)(6) | Requires a 2-step upgrade path (4)(5) | Requires a 2-step upgrade path (4)(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 convert_cluster`" command.
2. To upgrade a Scalable Platform from R81.10, R81.20 to R82, you must install a required Take of a Jumbo Hotfix Accumulator:
   - On R81.20 for Scalable Platforms
     Must install the R81.20 Jumbo Hotfix Accumulator, Take 92 or higher.
   - On R81.10 for Scalable Platforms
     Must install the R81.10 Jumbo Hotfix Accumulator, Take 172 or higher.

   In Maestro environment, it is possible to upgrade Security Groups and Quantum Maestro Orchestrators (if you decide to upgrade, you must upgrade both).
3. To upgrade a Scalable Platform from R81, R80.30SP, R80.20SP to R82, you must follow this 3-step upgrade path:
   a. Upgrade to one of these versions:
      - R81.20 for Scalable Platforms
        See:
        - sk177624 - R81.20 for Scalable Platforms
        - *R81.20 Quantum Maestro Administration Guide*.
        - *R81.20 Quantum Scalable Chassis Administration Guide*.
      - R81.10 for Scalable Platforms
        See:
        - sk173363 - R81.10 for Scalable Platforms
        - *R81.10 Quantum Maestro Administration Guide*.
        - *R81.10 Quantum Scalable Chassis Administration Guide*.

   b. Install the required Jumbo Hotfix Accumulator:
      - On R81.20 for Scalable Platforms
        R81.20 Jumbo Hotfix Accumulator, Take 92 or higher.
      - On R81.10 for Scalable Platforms
        R81.10 Jumbo Hotfix Accumulator, Take 172 or higher.

   c. Upgrade to R82.

4. The required 2-step upgrade path is:
   a. Upgrade to one of these versions:
      - R81.20 (see the *R81.20 Installation and Upgrade Guide*).
      - R81.10 (see the *R81.10 Installation and Upgrade Guide*).
      - R81 (see the *R81 Installation and Upgrade Guide*).
      - R80.40 (see the *R80.40 Installation and Upgrade Guide*).
   b. Upgrade 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 on R77.30 or R80.10, 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:

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

| Check Point Product | Gaia Fast Deployment Clean Install (1) | Gaia Fast Deployment Upgrade (1) | Central Deployment in SmartConsole (2) | CPUSE Clean Install (3) | CPUSE Upgrade (4) | Advanced Upgrade (5) | Upgrade with Migration (6) | Upgrade with CDT (7) |
|---|---|---|---|---|---|---|---|---|
| Security Gateways | Yes | Yes | Yes | Yes | Yes | **No** | **No** | Yes |
| VSX Gateways | **No** | Yes | Yes | Yes | Yes | **No** | **No** | Yes |
| Security Group Members - Maestro | **No** | **No** | **No** | Yes | Yes | **No** | **No** | **No** |
| Security Group Members - Scalable Chassis | **No** | **No** | **No** | Yes | Yes | **No** | **No** | **No** |

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

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

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

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

**Explanations:**

1. Gaia Fast Deployment:
   Performs a multi-step upgrade or clean install with one image.
   This image already contains a specific base version, a designated role (for example, a Security Gateway), and Hotfixes / Jumbo Hotfix Accumulator.
   You can see and install this image with CPUSE in Gaia Portal or Gaia Clish.
   For more information, see sk120193.
2. Central Deployment in SmartConsole:
   - You perform a remote installation of an upgrade package from SmartConsole.
   - You install the package from the local repository on the Management Server or from Check Point Cloud.
   - You can install the package on several targets at the same time.
   - On a ClusterXL and a VSX Cluster in the High Availability mode, the Central Deployment method performs the Multi-Version Cluster (MVC) Upgrade to preserve the current connections:
     a. Upgrades all Cluster Members in the Standby mode.
     b. Enables the MVC mode to allow the synchronization of the current connections between Cluster Members that run different software versions.
     c. Performs a failover from the Cluster Member in the Active state to one of the upgraded Cluster Members.
     d. Upgrades the remaining Cluster Member (formerly in the Active state).
   - For instructions, see the *R82 Security Management Administration Guide*.

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

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

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

| Gateway Type | Mode | Release Version |
|---|---|---|
| Security Gateways,<br>ClusterXL,<br>VRRP Cluster | Gateway | R82,<br>R81.20, R81.10, R81,<br>R80.40, R80.30, R80.20, R80.10 |
| Security Gateways,<br>VSX Cluster | Traditional VSX | R82,<br>R81.20, R81.10, R81,<br>R80.40, R80.30, R80.20, R80.10 |
| ElasticXL Cluster | Gateway | R82 |
| ElasticXL Cluster | VSNext | R82 |
| Security Groups in Maestro | Gateway | R82,<br>R81.20, R81.10, R81,<br>R80.30SP, R80.20SP |
| Security Groups in Maestro | VSNext | R82 |
| Security Groups in Maestro | Traditional VSX | R81.20, R81.10, R81,<br>R80.40, R80.30, R80.20, R80.10 |
| Security Groups on Scalable Chassis | Gateway | R82,<br>R81.20, R81.10, R81,<br>R80.20SP |
| Security Groups on Scalable Chassis | Traditional VSX | R82,<br>R81.20, R81.10, R81,<br>R80.20SP |

| Gateway Type | Mode | Release Version |
|---|---|---|
| Quantum Spark, Quantum Rugged, and SMB Appliances | Gateway | R81.10.X,<br>R80.20.X,<br>R77.20.8X |

**Notes:**

- Management Servers R81.20 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.
- Management Servers R82 support certain Quantum Spark Appliances with an R82.00 image at the Early Availability level.
  For more information, contact a Check Point office in your area.

# Quantum Maestro Orchestrator and Security Group Versions

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

- R82 (see sk181127)
- 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.

# Open Server Hardware Requirements

## Minimum Hardware Requirements

| Check Point Product | Processor | Total CPU cores | Memory |
|---|---|---|---|
| **Security Management Server** | Supported Intel® Core™ i5 or equivalent | 2 | 8 GB |
| **Multi-Domain Server** | Supported Intel® Core™ i5 or equivalent | 8 | 32 GB |
| **Security Gateway** | Supported Intel® Core™ i5 or equivalent | 2 | 8 GB |
| **VSX** | Supported Intel® Core™ i5 or equivalent | 2 | 8 GB |
| **Standalone** | Supported Intel® Core™ i5 or equivalent | 4 | 8 GB |

For the SmartEvent requirements, see *"SmartEvent Requirements" on page 63*.

# Disk Space Requirements

| Check Point Product | Recommended free disk space | Minimum free disk space (3) |
|---|---|---|
| **Security Management Server** (1) | 1 TB | 110 GB |
| **Multi-Domain Server** (2) | 1 TB | For the Multi-Domain Server:<br>100 GB<br>For each additional Domain:<br>110 GB |
| **Security Gateway** | 200 GB | 110 GB |
| **VSX** | For the VSX Gateway:<br>200 GB<br>For each Virtual System:<br>1 GB | For the VSX Gateway:<br>100 GB<br>For each Virtual System:<br>1 GB |
| **Standalone** | 1 TB | 110 GB |

**Notes:**

1. On an Open Server that runs a Management Server / Log Server, only one upgrade is allowed.
   To upgrade again, use an Advanced Upgrade (with Clean Install) or an Upgrade with Migration - see *"Upgrade Methods" on page 50*.
   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, additional backup / snapshot is not supported.
3. 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.
4. On an Open Server, the logging partition size is only large enough for minimum machine operations.

# Maximum Supported Physical Memory

| Check Point Product | Physical RAM Limit |
|---|---|
| **Security Management Server**,<br>or<br>**Multi-Domain Security Management Server** | 512 GB |
| **Security Gateway**,<br>or<br>**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

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

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

## Desktop SmartConsole Software Requirements

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

Desktop SmartConsole is supported on:

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

# Gaia Portal Requirements

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

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

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

## The Gaia Portal requirements on Quantum Maestro Orchestrators

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

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

# Mobile Access Requirements

You must use one of these operating systems:

**OS Compatibility**

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

You must use one of these web browsers:

**Web Browser Compatibility**

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

**Notes:**

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

# Identity Awareness Requirements

## Identity Clients

See sk134312.

## AD Query

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

## Browser-Based Authentication (Captive Portal)

You must use one of these web browsers:

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

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

  Endpoint Security Management Servers do not support Standalone (Security Gateway + Management Server) and Multi-Domain Security Management deployments.
- R82 Endpoint Security Management Server can manage:
  - E81.00 and higher versions of Endpoint Security Clients for Windows OS
  - E82.00 and higher versions of Clients for macOS

  See sk117536.
- 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 Platforms Requirements

## Software Requirements

See *"Supported Security Gateway Versions" on page 58*.

- To manage an R82 Security Group in the ElasticXL configuration, use:
  - R82 Security Management Server or Multi-Domain Server.
- To manage an R82 Security Group in the Maestro configuration, use:
  1. R82 Quantum Maestro Orchestrator.

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

## Supported Network Cards on Maestro Security Appliances

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

- See sk181433 for the list of supported Maestro Security Appliances and Line Cards.
- See sk158652 for the mandatory guidelines.

## 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 | |

<table>
<tr><th>Item</th><th>Maximum Number</th><th>Hard Limit</th><th>Comment</th></tr>
<tr><td>Security Gateway objects in each Domain</td><td>250<br>and<br>500</td><td>No</td><td>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`).<br>The maximum supported number of the managed Security Gateways and Cluster Members depends on the installed RAM and the number of CPU cores on the Management Server:
<table>
<tr><th>Number of available CPU Cores</th><th>Amount of installed RAM</th><th>Maximum supported number of the managed Security Gateways</th></tr>
<tr><td>32</td><td>96 GB</td><td>500</td></tr>
<tr><td>16</td><td>96 GB</td><td>500</td></tr>
<tr><td>6</td><td>32 GB</td><td>350</td></tr>
<tr><td>6</td><td>16 GB</td><td>250</td></tr>
</table></td></tr>
<tr><td>Objects in each Group object</td><td>12,000</td><td>Yes</td><td></td></tr>
<tr><td>Rules in each policy</td><td>28,000</td><td>Yes</td><td>To ensure optimal Security Gateway responsiveness, we recommend configuring a maximum of 20,000 rules in a policy.<br>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.</td></tr>
<tr><td>Changes in one session</td><td>100</td><td>No</td><td>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).</td></tr>
</table>

| Item | Maximum Number | Hard Limit | Comment |
|---|---|---|---|
| Interfaces in each Security Gateway | 200 | No | To ensure optimal SmartConsole responsiveness, we recommend configuring a maximum of 200 interfaces in SmartConsole.<br>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. |
| Layers in Access Control Policy | 251 | Yes | The maximum number of Policy Layers in an Access Control Policy is 251. |

# Sizing Recommendations for Check Point Management Server

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 mode<br>See *"Security Gateway or Cluster" on page 36* |
| Virtual Gateway in the VSNext mode | 1024 | See *"VSNext and Traditional VSX" on page 40* |
| VSX Gateway in the Traditional VSX mode | 4096 | Includes VLANs and Warp Interfaces<br>See *"VSNext and Traditional VSX" on page 40* |
| Virtual System in the Traditional VSX mode | 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<br>(6 in total in Dual Site) |
| Geo Cluster | 2 |
| Virtual System Load Sharing in the Traditional VSX mode | 13 |

# Number of Supported Items in an ElasticXL Cluster

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

# Number of Supported Items in a Maestro Environment

| Item | Number of Supported Items | Notes |
|---|---|---|
| Number of Security Groups configured | ■ Minimum: 1<br>■ Maximum: 8 | None |
| Number of Security Appliances in one Security Group | In Single Site and Dual Site deployment:<br>■ Minimum: 1<br>■ Maximum: 28 | In Dual Site environments:<br>■ Each Security Group must contain a minimum of one Security Appliance from each site (see MBS-7606 in sk181128).<br>■ 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 the Security Gateway Mode and in the VSNext Mode:<br>■ Minimum: 2<br>■ Maximum: 1024<br>In the Traditional VSX Mode:<br>■ Minimum: 2<br>■ Maximum: 4096<br>For each Virtual System in the Traditional VSX Mode:<br>■ Minimum: 2<br>■ Maximum: 250 | Includes all interface types (Physical, Bonds, VLAN, Warp). |

# Build Numbers

| Software Component | Build Number | Verifying Build Number |
|---|---|---|
| Gaia | OS Build 777<br>OS kernel version 4.18.0-372.9.1cpx86_64<br>OS edition 64-bit | Run this command in Gaia Clish:<br>`show version all` |
| Security Gateway | R82 - Build 151 | Run this command in the Expert mode:<br>`fw ver` |
| Security Management Server | R82 - Build 844 | Run this command in the Expert mode:<br>`fwm ver` |
| Multi-Domain Server | R82 - Build 904 | Run this command in the Expert mode:<br>`fwm mds ver` |
| SmartConsole | 82.0.9800.1027 | Click Menu > About Check Point SmartConsole |

# Licensing

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