Check Point
SOFTWARE TECHNOLOGIES LTD.

28 January 2020

R80.40

Release Notes

[Classification: Protected]

STEP UP TO
5TH GENERATION
CYBER SECURITY

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 R80.40

For more about this release, see the R80.40 home page.

Latest Version of this Document

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
28 January 2020	First release of this document

Table of Contents

Important Links

For more about R80.40, see:

- R80.40 Home Page
- R80.40 Known Limitations
- R80.40 Resolved Issues

Visit the Check Point CheckMates Community to:

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

To learn more about R80.40, visit http://www.checkpoint.com/architecture/infinity/.

What's New

Introduction

As our networks continue to increase and the threat landscape continues to evolve, customers need security solutions that allow endless scalability and simple operations. With over 100 new features, R80.40, is imperative for putting our network security on the fast track. Providing unified management for both physical and virtual networks, on premise, and cloud enforcement points. By consolidating all aspects of your security environment seamlessly, it allows you to deploy protections across your organization without impeding business innovation. It also allows full visibility into security across your network in a customizable visual dashboard, helping you monitor and focus on what matters to you. With its scalable, extensible architecture, you can manage the most complex environments easily and efficiently.

This release contains innovations and significant improvements such as:

- **SmartTasks** automates daily work with pre-defined or customizable actions.
- **Dedicated HTTPS policy layer** preventing encrypted traffic from Gen V attacks.
- **Zero-touch deployment** – from hours to minutes for installing new gateways.
- **IoT Security Manager** Identify IoT devices and seamlessly turn their attributes into an IoT security policy.

New in this release

IoT Security

A new IoT security controller to:

- Collect IoT devices and traffic attributes from certified IoT discovery engines (currently supports Medigate, CyberMDX, Cynerio, Claroty, Indegy, SAM and Armis).
- Configure a new IoT dedicated Policy Layer in policy management.
- Configure and manage security rules that are based on the IoT devices attributes.

HTTPS Inspection

HTTP/2

HTTP/2 is an update to the HTTP protocol. The update provides improvements to speed, efficiency and security and results with a better user experience.

- Check Point's Security Gateway now supports HTTP/2 and benefits better speed and efficiency while getting full security, with all Threat Prevention and Access Control blades, as well as new protections for the HTTP/2 protocol.

- Support is for both clear and SSL encrypted traffic and is fully integrated with HTTPS Inspection capabilities.

HTTPS Inspection Layer

Provides these new capabilities:

- A new Policy Layer in SmartConsole dedicated to HTTPS Inspection.
- Different HTTPS Inspection layers can be used in different policy packages.
- Sharing of a HTTPS Inspection layer across multiple policy packages.
- API for HTTPS Inspection operations.

Threat Prevention

Optimized Security and Productivity for the Different Modes – Threat Extraction works with Threat Emulation to provide users with more productivity without compromising security.

- *Background Mode* is now called *Rapid Delivery* to prevent many more malicious files within the emulation window of 3 seconds.
- *Hold Mode* is now called *Maximum Prevention* and provides improved productivity to ensure that all Threat Extraction cleaned documents deliver quickly to end users. Maximum Security minimizes the time users wait without a compromise on security.

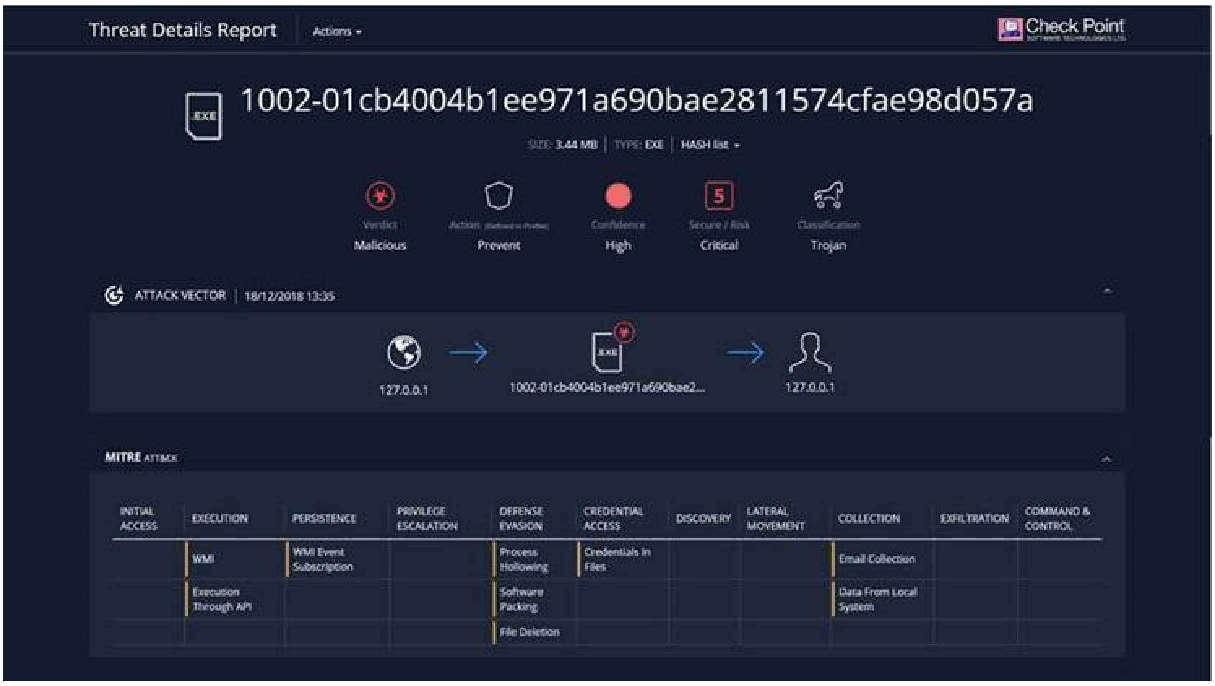
Threat Extraction

Automatic Engine Updates – Like the automatic updates to the Threat Emulation engines, you can now receive Threat Extraction updates automatically on your gateways. There is no need to update to a hotfix or a major version. Security improvements, new features and more do not require intervention.

To learn more, refer to the Advanced Threat Emulation Settings Chapter in the *R80.40 Threat Prevention Administration Guide*.

Anti-Virus and SandBlast Threat Emulation

MITRE ATT&CK™ Reporting – Threat Emulation Forensics Reports now include a detailed MITRE ATT&CK Matrix with the detected adversary tactics and techniques for every malicious executable file.



1002-01cb4004b1ee971a690bae2811574cfae98d057a

SIZE: 3.44 MB | TYPE: EXE | HASH list

Verdict	Action	Confidence	Secure / Risk	Classification
Malicious	Prevent	High	Critical	Trojan

ATTACK VECTOR | 18/12/2018 13:35

127.0.0.1 → 1002-01cb4004b1ee971a690bae2... → 127.0.0.1

MITRE ATT&CK

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL
	WMI	WMI Event Subscription		Process Hollowing	Credentials In Files			Email Collection		
	Execution Through API			Software Packing				Data From Local System		
				File Deletion						

Enhanced Support for Archive Files – includes significant improvements in handling archive files:

- Support for password protection for all supported file types, including .7z and .rar. For more details, please refer to sk112821.
- An improved mechanism to "guess" passwords automatically when it opens password-protected archives for emulation.
- Added support for password-protected archives when the password includes Unicode characters.
- Stability improvements.

Faster delivery of an emulation verdict for documents with embedded files.

Enhanced Support for Password-Protected Documents:

- Admins can now configure a default action for password-protected documents. If such a file is emulated, the file is allowed or blocked by default. To configure a default action, follow the instructions in sk132492.

New File Types and Protocols:

- Attachments from Nested MSG Files - Threat Emulation now supports emulation for files that attach to MSG files that attach to other MSG files.
- Support for new Archive Formats - WIM, CHM, CramFS, DMG, EXT, FAT, GPT, HFS, IHEX, MBR, MSI, NSIS, NTFS, QCOW2, RPM, SquashFS, UDF, UEFI, VDI, VHD, VMDK, LZH, ARJ, CPIO, AR.
- SCP and SFTP file transfers can be scanned using SSH Deep Packet Inspection.

- SMBV3 Multi-Channel Connections – Multi-channel file transfer is on by default on all Windows operating systems. The Check Point Gateway is now the only one in the market that inspects large file transfers through SMBv3 (3.0, 3.0.2, 3.1.1) over multi-channel connections.

Enhanced Logging for Emulated Archive Files:

- The archive file log includes the names of all the files inside.
- A new log generates for every extracted file from the archive with its emulation results. This log contains the name of the archive file. Logs correlate easily between the archive file and those of the files it contains.

Importing SHA-256 IOCs - Anti-Virus now supports SHA-256 hashes as Indicators of Compromise (IOCs). Administrators can import SHA-256 IOCs manually or connect the gateway to a live feed of SHA-256 IOCs. For more information, refer to sk132193.

Replacing the Threat Emulation API Certificate – Administrators can now upload their own certificate to use for Threat Emulation API calls to their Threat Emulation appliance. For more information, refer to sk160693.

Email Security

- Enhanced Support for POP3 and IMAP protocols - Anti-Virus and SandBlast Threat Emulation now support inspection of e-mail over the POP3 protocol and improve inspection of e-mail over the IMAP protocol.
- Enhanced Protection against BaseStriker - MTA Gateways now protect against malicious emails with URLs that use the BaseStriker technique.
- Bounce Messages Behavior Change - Modifies the configuration of the MTA so that it tries to send bounce messages only once whether it reaches its destination or not.
- Enhanced Threat Emulationinspection for files behind shortened links - The body of an email sometimes includes customized *Bitly* links that point to files. With this release, Threat Emulation scans the files behind these links to detect zero-day attacks. This capability requires Threat Emulation and Anti-Virus to be enabled and MTA must be configure for the Security Gateway.

[*Early Availability*] Click-Time URL Protection – The MTA gateway can now re-write links in incoming emails. When users click on them, the resources (web sites or files) behind the links have inspections again. This prevents delayed attacks where attackers replace the resource behind the link after the email delivery.

[*Early Availability*] Anti-Phishing Engine – The MTA gateway introduces a new State of the Art Anti-Phishing engine. This design alerts against and prevents sophisticated phishing, spear phishing, and targeted phishing attacks.

Want to join the program and hear more? Contact us at email_security@checkpoint.com.

Other Enhancements

Dynamic, Domain and Updatable Objects can be used in Threat Prevention and HTTPS Inspection Policies.

Access Control

Identity Awareness

- Support for Captive Portal integration with SAML 2.0 and third party Identity Providers.
- Support for Identity Broker for scalable and granular sharing of identity information between PDPs, as well as cross-domain sharing.
- Enhancements to Terminal Servers Agent for better scaling and compatibility.

IPsec VPN

- Configure different VPN encryption domains on a Security Gateway that is a member of multiple VPN communities. This provides:
  - Improved privacy - Internal networks are not disclosed in IKE protocol negotiations.
  - Improved security and granularity - Specify which networks are accessible in a specified VPN community.
  - Improved interoperability - Simplified route-based VPN definitions (recommended when you work with an empty VPN encryption domain).
- Large Scale VPN (LSV) environment. - using LSV profiles provides the ability to connect Externally Managed and Third Party VPN peers seamlessly by simply providing them with the same CA certificate used by central Security Gateway.

URL Filtering

- Improved scalability and resilience.
- Extended troubleshooting capabilities.

Application Control

Improved performance, diagnostics and monitoring tools.

NAT

- Enhanced NAT port allocation mechanism - on Security Gateways with 6 or more CoreXL Firewall instances, all instances use the same pool of NAT ports, which optimizes the port utilization and reuse.
- NAT port utilization monitoring in CPView and with SNMP.

Voice over IP (VoIP)

Multiple CoreXL Firewall instances handle the SIP protocol to enhance performance.

Remote Access VPN

Machine Certificate Authentication - use machine certificate to distinguish between corporate and non-corporate assets adding the ability to restrict access to corporate assets only. Enforcement can be pre-logon (device authentication only) or post-logon (device and user authentication).

Mobile Access Portal Agent

Enhanced Endpoint Security on Demand within the Mobile Access Portal Agent to support all major web browsers. For more information, see sk113410.

Mobile Access

SMB v2/3 mount support in Mobile Access blade.

Security Gateway and Gaia

CoreXL and Multi-Queue

- Security Gateway automatically changes the number of CoreXL SNDs and Firewall instances and the Multi-Queue configuration based on the current traffic load. To learn more visit the *R80.40 Performance Tuning Administration Guide*
- Priority Queues are enabled by default. For more information see sk105762.

Clustering

- Multi-Version Clustering (MVC) – ClusterXL acts like a standard cluster running cluster members with different software versions during upgrade scenarios supporting redundancy between members and state synchronization.
- New ClusterXL mode: Active-Active ,supports running several cluster members in ACTIVE state, each member is a part of a separated routing domain and handles its own traffic, redundancy is kept during failover.
- Geo-Clustering in Active-Active mode – Supports the configuration of the cluster Sync interface on different subnets while allowing L3 communication between the members on the sync interface. making the requirement for L2 connectivity and a trusted network between the cluster members (while working in Active-Active mode) obsolete.
- Support for Cluster Control Protocol (CCP) in Unicast mode for any number of cluster members eliminating the need for CCP Broadcast, Multicast or Automatic modes.
- Configuring VMAC does not require changing the NIC to promiscuous mode.
- Eliminated the need for MAC Magic configuration when several clusters are connected to the same subnet.
- Cluster Control Protocol encryption is now enabled by default.

VSX

- Support for VSX upgrade with CPUSE in Gaia Portal.
- Support for Active Up mode in VSLS.
- Support for CPView statistical reports for each Virtual System

Zero Touch

A simple Plug & Play setup process for installing an appliance - eliminating the need for technical expertise and having to connect to the appliance for initial configuration.

Gaia REST API

Gaia REST API provides a new way to read and send information to servers that run Gaia Operating System. See sk143612.

CloudGuard IaaS

AWS Data Center enhancements:

- Load Balancer (ALB and NLB) objects are supported.
- Security Groups support the use of tags.
- Subnet objects include IP addresses from all associated Network Interfaces.

Azure Data Center improvements:

- Load Balancer (Public and Internal) objects are supported.
- Load Balancers, Virtual Networks, and Network Security Groups support the use of tags.
- Subnet objects include Front end IP addresses of the Internal Load Balancers.

Advanced Routing

- Enhancements to OSPF and BGP allow to reset and restart OSPF neighbor adjacency per OSPF instance and BGP peering per peer.
- Enhancing route refresh for improved handling of BGP routing inconsistencies.

New kernel capabilities

- Upgraded Linux kernel
- New partitioning system (gpt):
  - Supports more than 2TB physical/logical drives
- Faster file system (xfs)
- Supporting larger system storage (up to 48TB tested)
- I/O related performance improvements
- Multi-Queue - Full Gaia Clish support for Multi-Queue commands
- Added NFSv4 (client) support (NFS v4.2 is the default NFS version used)
- Support of new system tools for debugging, monitoring and configuring the system

Security Management

Revert to Revision

The Security Management Server architecture supports built-in revisions, Each publish operation saves a new revision that contains only the delta from the previous revision allowing:

- Safe recovery from a crisis, restore a Domain or a Management Server to a good known revision.
- Improved policy verification process based on the difference between the current policy and the one contained in the revision database.

Multi-Domain Server

- Backup and restore an individual Domain Management Server on a Multi-Domain Server.
- Migrate a Multi-Domain Security Management from one Multi-Domain Server to a different Multi-Domain Server.
- Migrate a Security Management Server to become a Multi-Domain Security Management on a Multi-Domain Server.
- Migrate a Domain Management Server to become a Security Management Server.

SmartTasks and API

- DevOps teams can automate their security and transform it into DevSecOps workflows using Ansible and Terraform. Automate security responses to threats, provision both physical and virtualized next-generation firewalls and automate routine configuration tasks, saving time and reducing configuration errors.
  - For more information about Check Point Ansible module see Check Point Ansible security modules
  - For more information about Check Point Terraform provider see Check Point Terraform Provider.
- New Management API authentication method that uses an auto-generated API Key.
- New Management API commands to create cluster objects.
- SmartTasks - Configure automatic scripts or HTTPS requests triggered by administrator tasks, such as publishing a session or installing a policy.
- Significant increase of performance for multiple set/edit/delete object commands with Batch API.

CloudGuard Controller

- Generate Events and Automatic Reactions based on CloudGuard Controller logs and events.
- Performance enhancements for connections to external Data Centers.
- Integration with VMware NSX-T.
- Support for additional API commands to create and edit Data Center Server objects.

SmartConsole

- Central Deployment of Jumbo Hotfix Accumulator and Hotfixes from SmartConsole or via API allowing multiple Security Gateways and Cluster installations in parallel.
- Object search - support for partial word search using a wildcard, for example: a match is returned for searching *oba for an existing Host named: USGlobalHost.

SmartEvent

Share SmartView views and reports with other administrators.

Log Exporter

- Export logs filtered according to field values.
- Generate SIEM compatible Threat Emulation and Forensics reports.

Endpoint Security

- Collect Logs push operations - upload logs and debug information automatically to an FTP server.
- Support for BitLocker encryption with Full Disk Encryption.
- Support for external Certificate Authority certificates for Endpoint Security client authentication and communication with the Endpoint Security Management Server.
- Support for dynamic size of Endpoint Security Client packages based on the selected features for deployment.
- Policy can now control the level of notifications to end users.
- Randomize the Malware scan time to make sure that not all computers do a scan at the same time. This makes sure that network performance is not affected by many simultaneous scans.
- Uninstall Endpoint Security clients using a Challenge-Response process
- Gaia Backup includes Endpoint Management components.
- All client-server communication use HTTPS.
- Endpoint Security Clients can connect to the Endpoint Security Management Server using FQDN in addition to the IP Address.

Licensing

For all licenses issues contact Check Point Account Services.

Software Changes

1. R80.40 supports the 3.10 kernel only for all Security Gateways and Appliances.
   - Security Gateway upgrade from 2.6.18 kernel to 3.10 kernel is supported.
   - Starting R80.20 Security Management Server supports the 3.10 kernel.
2. These appliances are no longer supported starting R80.40:
   - 21600
   - Smart-1 25B, Smart-1 50, Smart-1 150.
3. UTM-1 Edge Security Gateways cannot be managed with R80.40. These gateways should be removed or replaced before upgrading the Security Management Server to R80.40.
4. In-place upgrade from R75.4x to R80.40 is not supported. The recommended upgrade path is:
   a. Upgrade to R77.30.
   b. Upgrade from R77.30 to R80.40.
5. By default, Policy Verification now only warns about conflicting rules, in previous versions the verification process warned for rules configured with the same action. For more information see sk161574.
6. After a CloudGuard Controller upgrade to R80.40, the Subnet and Security Group objects may include more IP addresses which will be enforced by the security policy.

Supported Environments

Check Point Appliances

Management Servers boot by default with 64-bit Gaia kernel after a clean install or upgrade to R80.40.

Note - If you revert from the R80.40 upgrade, the appliance will still boot with 64-bit Gaia kernel, even if it was originally 32-bit.

Check Point Product	Smart-1 205, 210, 225, 405, 410, 525, 625	Smart-1 3050, 3150, 5050, 5150
Security Management Server	✓	✓
Log Server	✓	✓
SmartEvent Server	✓	✓
Multi-Domain Security Management Server		✓
Multi-Domain Log Server		✓

Appliance	Management	Management + Log Server	Management + Log Server + SmartEvent
Gen V Smart-1 (405, 410, 525, 625, 5050, 5150)	✓	✓	✓
Smart-1 225, 3050, 3150	✓	✓	✓
Smart-1 210 (16GB RAM)**	✓	✓	✓
Smart-1 210 (8GB RAM)	✓	✓	
Smart-1 205 (16GB RAM)**	✓	✓	✓
Smart-1 205 (4GB RAM)*	✓		

* Smart-1 205 and 210 appliances with default memory can run Security Management Server *OR* Log Server *OR* SmartEvent.

** We recommend that you upgrade the memory of Smart-1 205 to 16GB as part of the upgrade to R80.40.

Security Gateway and Standalone (Gateway + Management)

The model numbers in this table are for the series of appliances that support R80.40.

Appliance Series	Security Gateway	Standalone (Gateway + Management)
2200	✓	
3000	✓	✓
4000	✓	*, **
5000 excluding 5900	✓	✓***
5900		✓
6500, 6800	✓	
6200, 6600, 6900	✓	✓
12000	✓	**
13000	✓	✓
15000	✓	✓***
16000/16000T	✓	
21000	✓	✓
23000	✓	✓***
26000/26000T	✓	
Open Server/Cloud setup, VMware,	✓	Using kernel mode only

* The 4200 appliance does not support a Standalone deployment.

** These appliance models do not support a Standalone deployment with their default RAM (4GB): 4400, 4600, 4800, 12200, and 12400. Upgrade these models to at least 8 GB RAM to support a Standalone deployment.

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

Appliance support for User Space Firewall (USFW)

The following appliances run in USFW mode by default:

26000T, 26000, 23900 and 16000T.

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

Supported Platforms

Check Point Product	Red Hat Enterprise Linux	VMware ESXi	Microsoft Hyper-V*
Security Management Server	7.3 or higher	5.x, 6.x	Windows 2012 R2, 2016 (64-bit only)*
Multi-Domain Security Management Server	7.3 or higher	5.x, 6.x	Windows 2012 R2, 2016 (64-bit only)*
Security Gateway	Not Supported	5.x, 6.x	Windows 2016 (64 bit only)

* For the most up-to-date information about Microsoft Hyper-V, see the *Virtual Machines* section of the Hardware Compatibility List.

Cloud Platforms

Supported setups for cloud solutions:

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

Supported Upgrade Paths

CPUSE is the recommended installation and upgrade method supported for this release. To learn more about CPUSE, see sk92449.

R80.40 Security Management Server and Multi-Domain Server supports Linux 3.10 kernel and the `xfs` file system providing support for improved system capabilities and performance, such as an enlarged system storage, improved I/O operations, better debugging tools and more.

When you perform a Clean Install, or Advanced Upgrade to R80.40 from versions prior to R80.20, it uses the `xfs` file system.

After an in-place upgrade (using CPUSE), the file system remains `ext3` except for Smart-1 525, 5050, 5150 appliances, which use the `xfs` file system.

Use the below methods to upgrade your Check Point environment to R80.40.

Upgrade to R80.40 is available from the following versions: R76, R77.x, EP6.0/EP6.1/EP6.2, R77.30.01, R77.30.02, R77.30.03, R77.30 EP6.5, R80, R80.10, R80.20.M1, R80.20, R80.20.M2, R80.20 3.10, R80.30, and R80.30 3.10

Note - To upgrade from R75.x versions to R80.40 first upgrade to R77.30

Check Point Product	Supported Methods
Security Gateway VSX Security Management Server Multi-Domain Server CloudGuard Controller Endpoint Security	CPUSE Upgrade CPUSE Clean Install Advanced Upgrade (Security Management Server only)

Important - At least 10 GB of free disk space is required in the /var/log/ partition for a Clean Install or Upgrade to succeed

Build Numbers

Software Component	Build Number	Verifying Build Number
Gaia	OS build 294	`show version all`
Security Gateway	This is Check Point's software version R80.40 - Build 685	`fw ver`
Security Management Server	This is Check Point Security Management Server R80.40 Build 150	`fwm ver`
Multi-Domain Server	This is Check Point Multi-Domain Server R80.40 Build 176	`fwm mds ver`
SmartConsole	Version: R80.40 Build: SmartConsole 994000394	Menu > About Check Point SmartConsole

Supported Backward Compatibility Gateways

R80.40 Management Servers can manage Security Gateways of these versions:

Gateway Type	Release Version
Security Gateway	R75.20, R75.30, R75.40, R75.45, R75.46, R75.47, R76, R77, R77.10, R77.20, R77.30, R80.10, R80.20, R80.30
VSX	R76, R77, R77.10, R77.20, R77.30, R80.10, R80.20, R80.30
Maestro Security Groups	R80.20SP

R80.40 Management Servers can manage appliance Security Gateways that run these versions *****:

Appliance	Release Version
1100 Appliances	R77.20.x
1200R Appliances	R77.20.x
1400 Appliances	R77.20.x
1550, 1590 Appliances	R80.20.x
60000/40000 Scalable Platforms	R76SP, R76SP.10, R76SP.20, R76SP.30, R76SP.40, R76SP.50, R80.20SP

***** UTM-1 Edge devices cannot be managed with R80.40.

Maximum Supported Number of Interfaces on Security Gateway

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

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

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

Maximum Supported Number of Cluster Members

Cluster Type	Maximum Supported Number of Cluster Members
ClusterXL	5
Virtual System Load Sharing	13

Open Server Hardware Requirements

Important - R80.40 for Open Servers is supported only for Security Management Servers .
Security Gateways and Standalone configurations for Open Servers is expected with R80.40 Jumbo Hotfix Accumulator.

Component	Security Gateway	VSX	Security Management Server/ Standalone	Multi-Domain Server
Processor	Intel Pentium IV,2 GHz or equivalent	Intel Pentium IV, 2 GHz or equivalent	Intel Pentium IV, 2.6 GHz or equivalent	Intel Pentium IV,2.6 GHz or equivalent
Total CPU cores	2	2	2	8
Memory	4 GB RAM	4 GB RAM	6 GB RAM	32 GB RAM

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

Disk Space Requirement

Setup/Disk Space	Security Management	Security Gateway	Standalone	VSX	Multi-Domain
Recommended free disk space	1 TB	200 GB	1 TB	200 GB + 1 GB per VS	1 TB
Minimum free disk space*	110 GB	110 GB	110 GB	100 GB + 1 GB per VS	100 GB

*** Notes** - Only one upgrade is allowed, additional backup/snapshot is not supported. Logging partition is just enough for minimal machine operations.

Maximum Supported Physical Memory

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

Hardware Health Monitoring

R80.40 supports these Hardware Health Monitoring features for Gaia Check Point appliances:

- **RAID Health:** Use SNMP to monitor the health of the disks in the RAID array, and be notified of volume and disk states.
- **Hardware Sensors:** Use the Gaia Portal or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Some open servers are supported with an IPMI interface card that requires an IPMI card.

Check Point Appliances	Smart-1
SNMP Hardware sensor monitoring (polling and traps)	✓
Gaia Portal hardware sensor monitoring	✓
RAID monitoring with SNMP	✓

Requirements

Threat Extraction Requirements for Web-downloaded documents

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

Threat Emulation Requirements

The Threat Emulation requirements are different based on the emulation location:

- ThreatCloud - Gaia operating system (64 or 32-bit)
- Local or Remote emulation - Threat Emulation Private Cloud Appliance on the Gaia operating system (64-bit only)

Logging Requirements

Logs can be stored on:

- A Security Management Server that collects logs from the Security Gateways. This is the default.
- A Log Server on a dedicated machine. This is recommended for organizations that generate many logs.

A dedicated Log Server has greater capacity and performance than a Security 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

You can enable the SmartEvent Blade on a Security Management Server, or install a dedicated SmartEvent Server. SmartEvent R80.40 can connect to a different version of Log Server - R77.xx or lower.

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

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

SmartConsole Requirements

Hardware Requirements

This table shows the minimum hardware requirements for SmartConsole applications:

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

Software Requirements

SmartConsole is supported on:

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

Gaia Portal Requirements

The Gaia Portal supports these web browsers:

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

Mobile Access Requirements

OS Compatibility

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

Browser Compatibility

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

Notes:

1. For a list of the prerequisites required for using Mobile Access Portal on-demand clients such as SSL Network Extender Network mode, SSL Network Extender Application Mode, Secure Workspace and Compliance Scanner refer to sk113410.
2. Secure Workspace and SSL Network Extender Application Mode are available for Windows platforms only.
3. Microsoft Internet Explorer is only browser supported inside Secure Workspace.

Identity Awareness Requirements

Identity Agents

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

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

AD Query and Identity Collector

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

Endpoint Security Requirements

Endpoint Security Server Hardware Requirements

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

Component	All Supported Operating Systems
Number of cores	4
Memory	16 GB
Disk Space	845 GB

The requirements for External Endpoint Policy Servers are similar.

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

Endpoint Security Software Requirements

- Endpoint Security Management Servers are supported on Management-only appliances or open servers. Endpoint Security Management Servers do not support Standalone (Security Gateway + Management Server) and Multi-Domain Security Management deployments.
- Endpoint Security Management Servers is not supported on Red Hat Enterprise Linux releases.
- R80.40 Endpoint Security Management Server can manage:
    - E80.64 and higher versions of Endpoint Security Clients for Windows
    - E80.64 and higher Client for macOS

Anti-Malware signature updates:

- To allow Endpoint Security clients to get Anti-Malware signatures updates from a cleanly installed R80.40 Primary Endpoint Security Management Server follow the instructions in the *R80.40 Endpoint Security Server Administration Guide* when selecting the Anti-Malware component.
- For cleanly installed R80.40 Endpoint Policy Server, you must follow sk127074. No additional steps are required, if you upgrade the Primary Endpoint Security Management Server to R80.40.
- Endpoint Security Clients can still acquire their Anti-Malware signature updates directly from an external Check Point signature server or other external Anti-Malware signature resources, if your organization's Endpoint Anti-Malware policy allows it.

For more information, see the *R80.40 Endpoint Security Server Administration Guide*.

Check Point Clients and Agents Support

Multiple Login Option Support

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

These features are supported when connected to an R80.40 gateway that has IPsec VPN or Mobile Access enabled.

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

See the *R80.40 Mobile Access Administration Guide* or the *R80.10 and Higher Remote Access VPN Administration Guide* for details.

Clients and Agents Support by Windows Platform

Microsoft Windows

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

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

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

Microsoft Windows Server

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

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

Clients and Agents Support by Mac Platform

All support is for Macintosh OS 64-bit.

Check Point Product	OS X 10.11	OS X10.12	OS X 10.13	OS X 10.14
Identity Agent	✓	✓	✓	✓
SSL Network Extender	✓	✓	✓	✓
Endpoint Security VPN E80.x or higher	✓ (E80.62 and higher)	✓ (E80.64 and higher)	✓	✓

DLP Exchange Agent Support

The R80.40 DLP Exchange Agent is supported on:

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

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