R75.40VS

Release Notes

16 July 2012

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

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.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=17401

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R75.40VS home page (http://supportcontent.checkpoint.com/solutions?id=sk76540).

Revision History

Date	Description
16 July 2012	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R75.40VS Release Notes).

Contents

Introduction

Thank you for choosing to install Check Point version R75.40VS. Please read this document carefully before installing R75.40VS.

Licensing

Important - Check Point software versions R75.10 or higher must have a valid Software Blades license. Users with NGX licenses cannot install the software. To migrate NGX licenses to Software Blades licenses, see Software Blade Migration (http://www.checkpoint.com/products/promo/software-blades/upgrade/index.html) or contact Account Services.

If you manage GX gateways from a Security Management server, you must regenerate your GX licenses in the User Center to be compliant with Software Blades. This procedure is optional for Multi-Domain Servers and Domain Management Servers.

IPS Software Blade License

Virtual Systems with IPS Software Blades must have a current, valid IPS contract that is renewed annually. To manage your contracts, go to your UserCenter account or contact your reseller.

- IPS service contracts notifications show in these places:
  - SmartDashboard > IPS
  - SmartUpdate
  - Product reports in your Check Point UserCenter account
- If your service contract expired, IPS continues to operate using the R70 (Q1/2009) signature set. Renew your IPS service contract to download and use the current signature set.

For more about IPS contract enforcement, see sk44175 (http://supportcontent.checkpoint.com/solutions?id=sk44175).

What's New

Integrated VSX

- Support of Gaia operating system.
- High performance and capacity, using 64-bit and CoreXL per Virtual System.
- VSX integrated with Software Blades architecture, with flexibility to enable Software Blades per Virtual System.
- Virtualize Security Gateways to VSX Gateways and add more Virtual Systems.
- Convert a VSX Gateway with a singe Virtual System to a physical Security Gateway.
- SNMP monitoring per Virtual System (SNMP v3).
- Optimal Service Upgrade, upgrade between VSX releases with minimal downtime.
- Hit count, and many other Security Gateway features, for VSX Gateways.

New Graphical User Interface

- Simplified toolbars and menus. To use the traditional menus, select **View** > **Menu Bar**.

- New Check Point Gateway and Cluster **Topology** view with filtering capabilities.
- **Firewall**:
  - New **Firewall Overview**
  - NAT policy is in Firewall tab
  - New query capabilities for Firewall rulebase
  - Take a picture of a rule: Right-click rule and select **Copy as Image**
- **IPSec VPN**:
  - New IPSec VPN **Overview**
  - New **VPN Community** view with improved search

VoIP

- Improved interoperability with VoIP servers and VoIP endpoints of leading vendors including NAT support.
- Simplified VoIP configuration in SmartDashboard.
- Highly detailed logs for VoIP events, such as calls and registrations. Tailored to VoIP traffic, these logs enable easy ongoing administration and troubleshooting.
- More than 80 VoIP IPS protections and VoIP settings:
  - Give granular security for maximum flexibility in VoIP deployment and enforcement
  - Include all IPS functionality: Profiles granularity, Packet Capture, Detect mode, Exceptions and Logs with attack data.

TLS Protocol Support

In addition to SSLv3 and TLS 1.0 (RFC 2246), the Security Gateway now supports:

- TLS 1.1 (RFC 4346)
- TLS 1.2 (RFC 5246)

Features that support TLS 1.1 and 1.2:

- HTTPS Inspection
- Mobile Access Network Extender
- Portals:
  - Identity Awareness Portal
  - DLP Portal
  - User Check Portal
  - Mobile Access Web Portal
  - Mobile Access SSL Network Extender Portal
  - Gaia WebUI

Support is enabled by default. You can disable it: **Global Properties** > **SmartDashboard Customization** > **Advanced Configuration** > **Portal Properties**.

IPS

New in the IPS blade: support for import of SNORT-compatible signatures. Import SNORT signatures from other sources, or manually create signatures for immediate IPS protection.

Easier Installation

- One installation for Security Management server and Multi-Domain Security Management
- One installation for SmartConsoles and SmartDomain Manager
- Convert from Security Management server to Multi-Domain Server with minimum downtime on Smart-1 appliances

Build Numbers

This table shows the R75.40VS software products and their build numbers as included on the product DVD. To verify each product build number, use the show command syntax or do the steps in the GUI.

Software Blade / Product	Build Number	Verifying Build Number*
Gaia	OS build 249	`show version all`
SecurePlatform	988000163	`ver`
Security Gateway	988000219	`fw ver`
Security Management	988000037	`fwm ver`
SmartConsole Applications	988000249	Help > About Check Point <*Application name*>
Mobile Access	988000115	`cvpn_ver`
Multi-Domain Server	988000009	`fwm mds ver`
SmartDomain Manager	988000155	Help > About Check Point SmartDomain Manager
Acceleration (Performance Pack)	988000137	`sim ver -k`
Advanced Networking (Routing)	988000014	SecurePlatform: `gated_ver` Gaia: `rpm -qf /bin/routed`
Server Monitoring (SVM Server)	988000022	`rtm ver`
Management Portal	988000014	`cpvinfo /opt/CPportal-R75.40VS/portal/bin/smartportalstart`
SmartReporter	988000155	`SVRServer ver`
Compatibility Packages**		
CPNGXCMP-R75.40VS-00	986000006	`/opt/CPNGXCMP-R75.40VS/bin/fw_loader ver`
CPV40VSCmp-R75.40VS-00	986000005	`cpvinfo /opt/CPV40Cmp-R75.40/bin/fw_loader | grep Build`
CPEdgecmp-R75.40VS-00	988000009	`/opt/CPEdgecmp-R75.40VS/bin/fw ver`

Software Blade / Product	Build Number	Verifying Build Number*
CPR71CMP-R75.40VS-00	988000007	`/opt/CPR71CMP-R75.40VS/bin/fw_loader ver`
CPR75CMP-R75.40VS-00	988000008	`/opt/CPR75CMP-R75.40VS/bin/fw_loader ver`
CPSG80CMP-R75.40VS-00	988000008	`/opt/CPSG80CMP-R75.40VS/bin/fw_loader ver`
CPR7520CMP-R75.40VS-00	988000009	`/opt/CPR7520CMP-R75.40VS/bin/fw_loader ver`
CPCON66CMP-R75.40VS-00	Build 007	`/opt/CPCON66CMP-R75.40/bin/fw_loader ver`

* Some of the commands to see the installed build show only the last three digits of the build number.

** To see build numbers on Windows, look at **C:\Program Files\CheckPoint\R75.40VS** instead of **/opt/../R75.40VS**

System Requirements

Important - Resource consumption is dependent on the scale of your deployment. The larger the deployment, the more disk space, memory, and CPU are required.

Check Point Appliance Naming Conventions

An appliance model name that ends with 00 (two zeros) is the generic name of the model. Any other number shows the number of Software Blades on the appliance. Some model names end with one zero.

This document uses the generic appliance names.

For example:

- Check Point 4800 is the generic name of the model.
- Check Point 4810 is the model with 10 Software Blades.
- Check Point IP2450 is the generic name of the model.
- Check Point IP2457 has 7 Software Blades.

Check Point Appliances

Note - R75.40VS IP Appliances support only Disk-based configurations on Gaia.

Appliance	Security Management	Security Gateway	Standalone Deployment	Full Standalone High Availability Deployment	Multi-Domain Security Management
2200 Appliance		✓	✓	✓	
4000 Appliances		✓	✓	✓	
12000 Appliances		✓	✓	✓	
21400 Appliance		✓	✓	✓	
IP Appliances (IP150, IP280, IP290, IP390, IP560, IP690, IP1280, IP2450)		✓	✓		
Smart-1 5	✓				
Smart-1 25	✓				
Smart-1 50	✓				✓
Smart-1 150					✓
Power-1		✓			
UTM-1		✓	✓	✓	

Check Point Appliances in VSX Mode

These appliances can be converted to VSX mode:

- 21400 Appliance
- 12000 Appliances
- 4000 Appliances
- 2200 Appliances
- Power-1 11000 and 9070
- UTM-1 3070
- IP 2450 and 1280

These appliances can only be used in VSX mode:

- 21400 VSX Appliances
- 12000 VSX Appliances
- VSX-1 11000 series
- VSX-1 9000 series
- VSX-1 3070

Note - You must use a R75.40VS Security Management server with R75.40VS VSX Gateways.

Check Point Operating Systems

	Gaia	SecurePlatform
Security Management	✓	✓
Security Gateway	✓	✓
Multi-Domain Security Management	✓	✓
VSX Gateway	✓	

Note - You must use a R75.40VS Security Management server with R75.40VS VSX Gateways.

Other Platforms and Operating Systems

Software Blade Containers	Microsoft Windows Server 2003, 2008	Microsoft Windows XP, 7	Red Hat Enterprise Linux 5.0, 5.4	Crossbeam X-series
Security Management	✓ & 2008 R2	✓	✓	
Security Gateway	✓			✓
Multi-Domain Security Management			✓	
VSX Gateway				✓

Operating System Versions

These are the supported versions of Microsoft and RedHat operating systems.

For Windows 2003 SP1, you must install the hotifx specified in Microsoft KB 906469 (http://support.microsoft.com/kb/906469).

Windows 2008 Server 64-bit is supported for Security Management only.

Operating System		Editions	Service Pack	32/64-bit
Microsoft	Windows XP	Professional	SP3	32-bit
	Windows 2003 Server	N/A	SP1, SP2	32-bit
	Windows 2008 Server	N/A	SP1, SP2	32-bit, 64-bit
	Windows 7	Professional, Enterprise, Ultimate	N/A	32-bit, 64-bit
RedHat	RHEL 5.0		N/A	32-bit
	RHEL 5.4	kernel 2.6.18	N/A	32-bit

Appliance Hardware Health Monitoring

R75.40VS supports these Hardware Health Monitoring features for Gaia and SecurePlatform:

- **RAID Health:** Use SNMP to monitor the health of the disks in the RAID array, and be notified of the states of the volumes and disks.
- **Hardware Sensors:** Use the WebUI or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Open Servers are only supported when they have an IPMI card installed.

Check Point Appliances

	21000	12000	4000 and 2200	Power-1	UTM-1	Smart-1
Hardware sensors monitoring with SNMP (polling and traps)	✓	✓	✓	✓	✓(1)	✓
Hardware sensors monitoring with the WebUI	✓	✓	✓	✓	✓(1)	✓
RAID monitoring with SNMP	✓	✓		✓(2)		

Notes

1. Hardware sensors monitoring is supported on all UTM-1 models except the xx50 series.
2. RAID Monitoring with SNMP is supported on Power-1 servers with RAID card installed (Power-1 9070 and Power-1 11070).

Open Servers

- **Hardware Sensors Monitoring:** Use SNMP (polling and traps) or the WebUI to monitor hardware on IBM, HP, Dell, and Sun certified servers with an Intelligent Platform Management Interface (IPMI) card installed. The IPMI standard defines a set of common interfaces for a computer system, which system administrators can use to monitor system health.

  Note - IPMI is an open standard, and we cannot guarantee the Hardware Health Monitoring performance on all systems and configurations.

- **RAID Monitoring with SNMP:** Use SNMP to monitor RAID on HP servers with HP Smart Array P400 Controller. Note the HP Smart Array P400i Controller is a different controller, which is not supported for hardware monitoring.

Dedicated Gateways

To install R75.40VS on an R71 DLP-1 appliance or an R71 DLP open server, do a clean installation of R75.40VS.

Note - To upgrade from DLP-1 9571 of version R71.x DLP, you must upgrade the BIOS. Then do a clean installation of R75.40VS. See sk62903 (http://supportcontent.checkpoint.com/solutions?id=sk62903) for details.

You cannot upgrade these dedicated gateways to R75.40VS:

- Open Server - IPS-1 Sensor
- Appliances - Security Gateway 80, UTM-1 Edge, IPS-1 Sensor

Platform Requirements

Gaia Requirements

This release is shipped with the new Gaia operating system, which supports most Check Point appliance platforms, selected open servers, and selected network interface cards.

If your open server has less than 6GB RAM, it can run in 32-bit mode only. You can run 64-bit compatible open servers with 6GB RAM or more in 64-bit mode.

- **Gaia Open Servers** - All open servers in the Hardware Compatibility List are supported (http://www.checkpoint.com/services/techsupport/hcl/all.html).
- **Gaia and Performance Pack** - Performance Pack is supported on all Gaia platforms.

Gaia on Check Point Security Appliances

Appliances	32-bit / 64-bit	Notes
2200	32	
4200	32	
4600	32	
4800	32, 64	64-bit is available with 6GB RAM or more
12200	32, 64	
12400	32, 64	
12600	32, 64	
21400	32, 64	

Gaia on IP Appliances

Important - Gaia is not supported on Flash-Based or Hybrid platforms at this time.

These configurations are supported:

IP Appliance Disk Based Platform	32-bit / 64-bit	
IP150	32	
IP280	32	
IP290	32	
IP390	32	
IP560	32	
IP690	32	
IP1280	32, 64	64-bit is available on appliances with 6GB RAM or more. The basic configuration for IP appliances is **4GB** of RAM.
IP2450	32, 64	

Gaia on Power-1, UTM-1 and Smart-1 Appliances

Platform	32-bit / 64-bit	Notes
Power-1 11000	32, 64	default is 64
Power-1 9070 and 5070	32	
UTM-1 3070, 2070, 1070, 570, 270, 130	32	
Smart-1 150, 50, 25, 5	32	

Gaia WebUI

The Gaia WebUI (also known as the Gaia Portal) is supported on these browsers:

- Internet Explorer 8 or higher
- Firefox 6 or higher
- Chrome 14 or higher
- Safari 5 or higher

Note - Gaia WebUI is not supported for VSX Gateway.

SecurePlatform

This release is shipped with the latest SecurePlatform operating system, which supports a variety of appliances and open servers.

See the list of certified hardware (http://www.checkpoint.com/services/techsupport/hcl/index.html) before installing SecurePlatform on the target hardware.

Linux

Note - Cross-platform High Availability is not supported with a mix of Windows and non-Windows platforms.

Before you install Security Management on Red Hat Enterprise Linux 5:

1. Install the `sharutils-4.6.1-2` package.
   a) Make sure that you have the `sharutils-4.6.1-2` package installed by running:
   ```
   rpm -qa | grep sharutils-4.6.1-2
   ```
   b) If the package is not already installed, install it by running:
   ```
   rpm -i sharutils-4.6.1-2.i386.rpm
   ```
   This package can be found on CD 3 of RHEL 5.
2. Install the `compat-libstdc++-33-3.2.3-61` package.
   a) Make sure that you have the `compat-libstdc++-33-3.2.3-61` package by running:
   ```
   rpm -qa | grep compat-libstdc++-33-3.2.3-61
   ```
   b) If the package is not already installed, install it by running:
   ```
   rpm -i compat-libstdc++-33-3.2.3-61.i386.rpm
   ```
   This package can be found on CD 2 of RHEL 5.
3. Disable **SeLinux**.
   a) Make sure that **SeLinux** is disabled by running: `getenforce`
   b) If **SeLinux** is enabled, disable it by setting `SELINUX=disabled` in the `/etc/selinux/config` file and rebooting the computer.

IPSO

R75.40VS does not currently support IPSO. IP appliances run on Gaia.

Microsoft Windows

Note - Cross-platform High Availability is not supported with a mix of Windows and non-Windows platforms.

High Availability Legacy mode is not supported on Windows.

Maximum Number of Interfaces Supported by Platform

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

Platform	Max Interfaces	Notes
Gaia	1024	
SecurePlatform	1015	255 virtual interfaces per physical interface, or 200 virtual interfaces per physical interface with Dynamic Routing
Windows	32	
Virtual System	64	Includes VLANs and Warp Interfaces
VSX Gateway	4096	Includes VLANs and Warp Interfaces

Security Management Open Server Hardware Requirements

Component	Windows	Linux	SecurePlatform on Open Servers
Processor	Intel Pentium Processor E2140 or 2 GHz equivalent processor	Intel Pentium Processor E2140 or 2 GHz equivalent processor	Intel Pentium Processor E2140 or 2 GHz equivalent processor
Free Disk Space	1GB	1.4GB	10GB (installation includes OS)
Memory	1GB	1GB	1GB
Optical Drive	Yes	Yes	Yes (bootable)
Network Adapter	One or more	One or more	One or more

Multi-Domain Security Management Requirements

The minimum recommended system requirements for Multi-Domain Security Management are:

Component	Linux	SecurePlatform
CPU	Intel Pentium Processor E2140 or 2 GHz equivalent processor	Intel Pentium Processor E2140 or 2 GHz equivalent processor
Memory	4GB	4GB
Disk Space	2GB	10GB (install includes OS)

Component	Linux	SecurePlatform
Optical Drive	Yes	Yes (bootable)

Multi-Domain Security Management Resource Consumption

Resource consumption is dependent on the scale of your deployment. The larger the deployment, the more disk space, memory, and CPU are required.

The Multi-Domain Security Management disk space requirements are:

- For basic Multi-Domain Server installations: 2GB (1GB `/opt`, 1GB `/var/opt`).
- For each Domain Management Server: 400MB (for the Domain Management Server directory located in `/var/opt`)

Security Gateway Open Server Hardware Requirements

Component	Windows	SecurePlatform on Open Servers
Processor	Intel Pentium IV or 1.5 GHz equivalent	Intel Pentium IV or 2 GHz equivalent
Free Disk Space	1GB	10GB
Memory	512MB	512MB
Optical Drive	Yes	Yes
Network Adapter	One or more	One or more supported cards

VSX Gateway Open Server Hardware Requirements

Component	Gaia on Open Servers
Processor	Intel Pentium IV or 2 GHz equivalent
Free Disk Space	12 GB
Memory	2 GB

Mobile Access Blade Requirements

Endpoint OS Compatibility	Windows	Linux	Mac	iOS	Android
Mobile Access Portal	✓	✓	✓	✓	✓
Clientless access to web applications (Link Translation)	✓	✓	✓	✓	✓
Endpoint Security on Demand	✓	✓	✓		
SecureWorkspace	✓				
SSL Network Extender - Network Mode	✓	✓	✓		
SSL Network Extender - Application Mode	✓				

Endpoint OS Compatibility	Windows	Linux	Mac	iOS	Android
Downloaded from Mobile Access applications	✓	✓	✓		
Clientless Citrix	✓				
File Shares - Windows File Explorer viewer (WebDAV)	✓				
File Shares - Web- based file viewer (HTML)	✓	✓	✓	✓	✓
Web mail	✓	✓	✓	✓	✓

Endpoint Browser Compatibility	Internet Explorer	Google Chrome	Mozilla Firefox	Macintosh Safari	Opera for Windows
Mobile Access Portal	✓	✓	✓	✓	✓
Clientless access to web applications (Link Translation)	✓	✓	✓	✓	✓
Endpoint Security on Demand	✓	✓	✓	✓	
SecureWorkspace	✓	✓	✓		
SSL Network Extender - Network Mode	✓	✓	✓	✓	
SSL Network Extender - Application Mode	✓	✓	✓		
Downloaded from Mobile Access applications	✓	✓	✓	✓	
Clientless Citrix	✓		✓		
File Shares - Windows File Explorer viewer (WebDAV)	✓ IE6 only				
File Shares - Web- based file viewer (HTML)	✓	✓	✓	✓	✓
Web mail	✓	✓	✓	✓	✓

SmartEvent Requirements

You can install SmartEvent on a Security Management Server or on a different, dedicated computer.

Component	Windows/Linux/SecurePlatform
CPU	Intel Pentium IV 2.8 GHz
Memory	4GB
Disk Space	25GB

To optimize SmartEvent performance:

- Use a disk available high RPM, and a large buffer size.
- Increase the server memory.

SmartReporter Requirements

These hardware requirements are for a SmartReporter server that monitors at least 15GB of logs each day and generates many reports. For deployments that monitor fewer logs, you can use a computer with less CPU or memory.

SmartReporter can be installed on a Security Management Server or on a dedicated machine.

Component	Windows & Linux Minimum	Windows & Linux Recommended
CPU	Intel Pentium IV 2.0 GHz	Dual CPU 3.0 GHz
Memory	1GB	2GB
Disk Space Installation: Database:	80MB 60GB (40GB for database, 20GB for temp directory)	(on 2 physical disks) 80MB 100GB (60GB for database, 40GB for temp directory)
DVD Drive	Yes	Yes

Optimizing SmartReporter Performance

We recommend these tips to optimize SmartReporter performance:

- Disable DNS resolution. This can increase consolidation performance to as much as 32GB of logs for each day.
- Configure the network connection between the SmartReporter server and the Security Management server to the optimal speed.
- Install a disk with high RPM (revolutions per minute) and a large buffer size.
- Use `UpdateMySQLConfig` to adjust the database configuration and adjust the consolidation memory buffers to use the more memory.
- Increase memory for better performance.

Console Requirements

This table shows the minimum hardware requirements for console applications: SmartDashboard, SmartView Tracker, SmartView Monitor, SmartProvisioning, SmartReporter, and SmartEvent, SecureClient Packaging Tool, SmartUpdate, and SmartDomain Manager.

Component	Windows
CPU	Intel Pentium Processor E2140 or 2 GHz equivalent processor
Memory	1024MB
Available Disk Space	900MB
Video Adapter	Minimum resolution: 1024 x 768

UserCheck Client Requirements

- The UserCheck client can be installed on endpoint computers running Windows.
- UserCheck for DLP client notification are supported on Gaia and SecurePlatform gateways.
- UserCheck for Application and URL Filtering client notifications are supported on SecurePlatform, and Gaia gateways.

- The UserCheck client is not compatible with Check Point GO or Secure Workspace.
  If a UserCheck client is installed on a machine and a violation occurs, the UserCheck client notification shows outside the Check Point GO or Secure Workspace environment. We recommend that you not install the UserCheck client on a machine that usually runs the Check Point GO or Secure Workspace environment.
- The UserCheck client is not supported on clusters in a load sharing environment.

Legacy Hardware Platforms

A legacy platform is a hardware platform unsupported for new installations but still supported for database migration.

Solaris

Although Solaris is a legacy platform, R75.40VS supports migration of the Solaris database to Windows, SecurePlatform, and Gaia. (But only from Check Point versions in the supported upgrade path).

- **Security Management server -** The database migration procedure for Solaris is the same as for SecurePlatform and Gaia as described in the chapter on *Advanced Upgrade and Database Migration* in the *R75.40VS Installation and Upgrade guide*.
- **Multi-Domain Security Management -** To export the Multi-Domain Security Management database from a legacy platform, use the R75.40VS SecurePlatform CD. Only two menu options are available:
  - preupgrade verification
  - mds export

  Note - R75.40VS continues to manage Solaris gateways of version R75.40 and below.

Security Management Software Blades

	Check Point OS		Microsoft Windows		RedHat Linux	
Software Blade	**Gaia**	**Secure Platform**	**Server 2003**	**Server 2008**	**XP, 7**	**RHEL 5.0, 5.4**
Network Policy Management	✓	✓	✓	✓	✓	✓
Logging & Status	✓	✓	✓	✓	✓	✓
Monitoring	✓	✓	✓	✓	✓	✓
SmartProvisioning	✓	✓	✓	✓	✓	✓
Management Portal	✓	✓	✓	✓	✓	✓
User Directory	✓	✓	✓	✓	✓	✓
SmartWorkflow	✓	✓		✓	✓	✓
SmartEvent	✓	✓	✓	✓	✓	✓
SmartReporter	✓	✓	✓	✓	✓	✓

Notes:

Management Portal is supported on: Internet Explorer 7 and Firefox 1.5 - 3.0.

SmartEvent on Windows Server 2008 is supported on 32-bit only.

Security Gateway Software Blades

Software Blade	Check Point Operating System		Microsoft Windows		Crossbeam
	Gaia	SecurePlatform	Server 2003	Server 2008	X-series
	VSX Support				
Firewall	✓	✓	✓	✓	✓
Identity Awareness	✓	✓			✓
IPSec VPN	✓	✓	✓	✓	✓
IPS	✓	✓	✓	✓	✓
URL Filtering	✓	✓	✓	✓	✓
Application Control	✓	✓	✓	✓	✓
Advanced Networking - Dynamic Routing and Multicast Support	✓	✓			
Acceleration & Clustering	✓	✓	✓	✓	✓
Mobile Access	✓	✓			
Anti-Bot	✓	✓	✓	✓	
Anti-Virus	✓	✓			
Web Security	✓	✓	✓	✓	✓
Advanced Networking - QoS	✓	✓	✓	✓	
DLP	✓	✓			
Anti-Spam & Email Security	✓	✓			

Acceleration & Clustering Software Blade

- Clustering is supported on Windows, but Acceleration is not. Only third-party clustering is supported on Crossbeam.

Anti-Bot, Anti-Virus, Application Control, IPS, and URL Filtering Software Blades

- For more about Anti-Bot and Anti-Virus support in VSX mode, go to sk79920 (http://supportcontent.checkpoint.com/solutions?id=sk79920).
- HTTPS Inspection is not supported on Windows.

DLP Software Blade

- DLP supports High-Availability clusters, including Full High Availability, on SecurePlatform and Gaia.
- DLP supports Load Sharing clusters in **Detect** and **Prevent** mode.
- On UTM-1 130/270, you can use DLP with Firewall and other Security Gateway software blades, or with Firewall and Security Management software blades.

- The DLP portal supports Internet Explorer 6, 7, 8, 9; Firefox 3, 4; Chrome 8; and Safari 5.
- DLP does not support VRRP on Gaia.

Advanced Networking - QoS Software Blade

- VSX has native QoS support. It does not use the QoS Software Blade.

Mobile Access Software Blade

Mobile Access support of VSX mode is partial. These are the clients and their support of VSX:

Client	Support in VSX Mode
Endpoint Security Suite	R73, E80.x
Check Point Mobile for Windows	E75 and higher
Endpoint Security VPN for Windows	E75 and higher
Endpoint Security VPN for MacOS	E75 and higher
IPSec VPN SSL Network Extender mode	R75.40VS: Windows, Linux, and Mac
Mobile VPN for iOS	E75 and higher
Check Point GO	R75 and higher
SecureRemote	E75 and higher

These clients are *not* supported in VSX mode:

- Mobile Access Portal
- Check Point Mobile for iOS and Android

Security Gateway Bridge Mode

Bridge mode is supported on these platforms:

- Gaia
- SecurePlatform
- Crossbeam

Clients and Consoles by Windows Platform

Check Point Product	XP Home (SP3) 32-bit	XP Pro (SP3) 32-bit	Server 2003 (SP2) 32-bit	Server 2008 (SP1-2) 32 / 64	Server 2008R2 (+SP1)	Vista (SP2) 32-bit	Vista (SP1) 64-bit	Windows 7 Ult, Pro, Ent (+SP1) 32 / 64
SmartConsole	✓	✓	✓	✓	✓	✓		✓
SmartDomain Manager	✓	✓	✓	✓	✓	✓		✓
SecureClient	✓	✓				✓		✓ (32-bit only)

Check Point Product	XP Home (SP3) 32-bit	XP Pro (SP3) 32-bit	Server 2003 (SP2) 32-bit	Server 2008 (SP1-2) 32 / 64	Server 2008R2 (+SP1)	Vista (SP2) 32-bit	Vista (SP1) 64-bit	Windows 7 Ult, Pro, Ent (+SP1) 32 / 64
Endpoint Security VPN	✓	✓				✓	✓	✓
Remote Access Clients E75.x	✓	✓				✓	✓	✓
SSL Network Extender	✓	✓				✓	✓	✓
DLP UserCheck		✓	✓	✓		✓		✓
DLP Exchange Agent			✓*	✓*				
Identity Agent	✓	✓	✓	✓		✓	✓	✓

* DLP Exchange Agent supports Exchange Server 2007 and Exchange Server 2010 on Windows Server 2003 64-bit (SP1-2) and Windows Server 2008 64-bit (SP1-2). A 32-bit version is available for demo or educational purposes.

Clients and Consoles by Mac Platform

Check Point Product	Mac OS X 10.6	Mac OS X 10.7
Identity Agent	32-bit / 64-bit	32-bit / 64-bit
SecureClient	32-bit	32-bit
Endpoint Security VPN E75 for Mac	32-bit / 64-bit	32-bit / 64-bit

Check Point GO Secure Portable Workspace

R75.40VS Security Gateways only support Check Point GO Secure Portable Workspace R75. Check Point GO R70.1 and R70 (formerly known as Check Point Abra) are not supported.

Upgrade Paths and Interoperability

R75.40VS supports upgrading from lower software versions and management of lower Security Gateway versions.

Upgrading to Gaia

You can upgrade SecurePlatform and IPSO Security Management servers and Security Gateways to Gaia R75.40VS, according to the upgrade paths listed below.

Note: Upgrade is not supported in an ISDN configuration.

Supported Upgrade Paths

You can upgrade these Security Management Server and Security Gateway versions to R75.40VS:

- R75
- R75.10
- R75.20
- R75.30
- R75.40

If you upgrade IP disk-based appliances to R75.40VS, the OS must be Gaia. The IP appliance will work in Gateway Mode only (not VSX mode).

You can upgrade these versions of SecurePlatform VSX gateways to Gaia Security Gateways in VSX mode:

- VSX R65, VSX R65.10, VSX R65.20
- VSX R67, VSX R67.10

See the VSX upgrade instructions in the *R75.40VS Installation and Upgrade Guide*.

Important - To upgrade from R75.40 Gaia to R75.40VS Gaia, there must be at least 4GB free space in `/var/log`.

To upgrade a Security Gateway on a 32-bit appliance to 64-bit Virtual System mode:

1. Upgrade to the Gaia OS.
2. Run: `set edition default 64-bit`
3. Reboot.

To upgrade a Security Management server on a 32-bit appliance to 64-bit Virtual System mode:

1. Install the SecurePlatform OS.
2. Change the configuration in `cpconfig`.
3. Reboot.

Compatibility with Gateways

When this release is installed on the Security Management Server, it can manage gateways of these versions.

Release	Version
Security Gateway	NGX R65, R70, R70.1, R70.20, R70.30, R70.40, R71, R71.10, R71.20, R71.30, R71.40, R71.50 R75, R75.10, R75.20, R75.30, R75.40
Security Gateway 80	R71.45
DLP-1	R71 and higher
IPS-1	R71
VSX	VSX R65, VSX R65.10, VSX R65.20, VSX R67, VSX R67.10
Connectra	Centrally Managed NGX R66
UTM-1 Edge	7.5.x and higher*

Release	Version
GX	4.0, 5.0

***** UTM-1 Edge and Safe@ devices that use locally configured VPN connections with download configuration settings, may experience VPN connectivity failure with R75.40VS Security Gateways. To enable this configuration with R75.40VS, see sk65369 (http://supportcontent.checkpoint.com/solutions?id=sk65369).

Note - You must use a R75.40VS Security Management server with R75.40VS VSX Gateways.

Compatibility with Clients

Gateways of this release can support these endpoint clients.

Endpoint Client	VSX Gateway	Security Gateway
SecureRemote E75	Yes	Yes
Check Point Mobile for Windows E75	Yes	Yes
Endpoint Security VPN E75	Yes	Yes
Endpoint Security VPN for Mac E75	Yes	Yes
Endpoint Security with VPN E75	Yes	Yes
SSL Network Extender	Yes	Yes
Mobile VPN for iOS	Yes	Yes
Check Point GO	Yes	Yes
Mobile Access Web Portal	No	Yes
Check Point Mobile for iOS / Android	No	Yes
Mobile Access SSL Network Extender Portal	No	Yes

Updating IPS Patterns

The IPS pattern granularity (converting patterns into protections) will be installed during the first IPS update procedure (online update, offline update, or scheduled update). Therefore, the first update after installation can take a few minutes longer than usual.

Uninstallation of IPS pattern granularity is not supported. If you uninstall R75.40VS, the patterns remain, converted to protections.

Uninstalling

Important - This does not remove Multi-Domain Security Management products.

You cannot use uninstall on Gaia or SecurePlatform. Use the revert or restore commands. See the *Installation and Upgrade Guide*.

Use these procedures to uninstall R75.40VS on other platforms.

Platform	Procedure
Windows	1. Open **Start > Check Point > Uninstall R75.40VS** 2. At the prompt, enter **Y** to continue.
Linux	1. Change directory to: `/opt/CPUninstall/R75.40VS/` 2. Run: `./UnixUninstallScript`

Example of Uninstall output:

```
 ************************************************************
Welcome to Check Point R75.40VS Uninstall Utility
************************************************************
All R75.40VS packages will be uninstalled.
Uninstallation program is about to stop all Check Point processes.
Do you want to continue (y/n) ? y
Uninstalling Management Portal package...Done!
Uninstalling SmartEvent and SmartReporter Suite package...Done!
Uninstalling R75 Compatibility package...Done!
Uninstalling R75.20 Compatibility package...Done!
Uninstalling R71 Compatibility package...Done!
Uninstalling CPSG 80 Series compatibility package...Done!
Uninstalling Connectra R66 Compatibility package...Done!
Uninstalling NGX Compatibility package...Done!
Uninstalling V40 Compatibility package...Done!
Uninstalling UTM-1 Edge compatibility package...Done!
Uninstalling CPinfo package...Done!
Uninstalling Security Gateway / Security Management package...Done!

************************************************************************
Package Name                                                    Status
------------                                                    ------
Management Portal                                               Succeeded
SmartEvent and SmartReporter Suite                              Succeeded
R75 Compatibility                                               Succeeded
R75.20 Compatibility                                            Succeeded
R71 Compatibility                                               Succeeded
CPSG 80 Series compatibility                                    Succeeded
Connectra R66 Compatibility                                     Succeeded
NGX Compatibility                                               Succeeded
V40 Compatibility                                               Succeeded
UTM-1 Edge compatibility                                        Succeeded
CPinfo                                                          Succeeded
Security Gateway / Security Management                          Succeeded

************************************************************************

Uninstallation program completed successfully.
Do you wish to reboot your machine (y/n) ?
```

If any package fails to uninstall, the script generates a log file and prints its location on the screen.