



We Secure the Internet.

Check Point R70

Release Notes

March 11, 2009



Note - The latest available version of this document is at:
http://supportcenter.checkpoint.com/documentation_download?!D=8712

In This Document

Information About This Release	3
New Terms	3
What's New in R70	4
Check Point Software Blades.....	4
IPS.....	5
Provisioning Software Blade	6
CoreXL.....	6
Performance Enhancements.....	6
Provider-1/SiteManager-1	6
Endpoint Connect VPN Client.....	7
SecurePlatform.....	7
Supported Products.....	8
Build Numbers	8
Management Products by Platform	9
Clients and Consoles by Platform.....	10
Platform Provisions and Requirements	10
Upgrade Notes.....	13
HFAs Included in this Release	13
Minimum System Requirements	14
Security Gateway Hardware Requirements	14
Security Management Hardware Requirements	14
SmartConsole and Provider-1 MDG Hardware Requirements.....	14
Provider-1/SiteManager-1 Multi Domain Server Requirements.....	15
VSX Gateway Hardware Requirements	15
Eventia Analyzer Requirements	15
Eventia Reporter Requirements	16
SecureClient Requirements.....	16
Endpoint Security Server Requirements	18
Endpoint Security Client Requirements	18
Known Limitations	20
Documentation Feedback.....	21

Information About This Release

This document contains important information not included in the documentation. Review this information before setting up Check Point R70.

New Terms

The following product and technology names have been changed for this version.

Table 1 Product and Technology Names

Versions NG and NGX Products and Technologies	Version R70 Products and Technologies
Firewall-1	Firewall
Integrity	Endpoint Security
Integrity Clientless Security	Endpoint Security On Demand
ROBO Gateway	Check Point SmartLSM Security Gateway
SmartCenter server	Security Management server
SmartDefense	IPS
SmartDirectory (LDAP)	User Directory
SmartLSM management	SmartProvisioning
SmartPortal	Management Portal
VPN-1 (Power/UTM) Gateway	Check Point Security Gateway
VPN-1 UTM Edge	UTM-1 Edge
Web Filtering	URL Filtering

Table 2 SmartDashboard Tab Titles

Versions NG and NGX SmartDashboard Tabs	Version R70 Products SmartDashboard Tabs
Address Translation	NAT
Connectra	SSL VPN
Content Inspection	Anti-Virus and URL Filtering
Messaging Security	Anti-Spam and Mail
Security	Firewall
SmartDefense	IPS
VPN	IPSec VPN

What's New in R70

Check Point R70 introduces the revolutionary *Software Blades* architecture. The Software Blades architecture provides a complete selection of Software Blades, each delivering a modular security gateway or security management function. Software Blades enable users to efficiently and quickly tailor Security Gateway and Management functionality to specific and changing needs. When running on multi-core platforms and appliances, Check Point CoreXL technology delivers near linear performance scalability for many of the Software Blades.

The release has several highlights:

- New IPS blade which delivers superb IPS capabilities integrated into the Security Gateway:
 - Integrated IPS Engine delivering over 2000 Pre-emptive/Behavioral-based Protections, Signature-based Protections, Client and Server Protections and Application Controls
 - Admin workflow and tools that allow simple management and deployment of IPS capabilities
 - Support for Prevent or Detect Mode per Profile and per Protection
 - Breakthrough performance of up to 10Gbps
 - Ability to limit system resources (CPU and memory) dedicated to IPS
 - Granular Exceptions
 - Easy IPS Protection updates including full coverage for Microsoft Patch Tuesday updates and many others
 - Enhanced log information (including packet capture) and new troubleshooting capabilities
- New Provisioning blade provides centralized administration and provisioning of Check Point security devices through a single management console. The blade provides an intuitive and easy interface to centrally manage both security and device configurations, such as operating system and network settings. Management can be done either device-by-device or using profiles which enable an administrator to manage large scale deployments that benefit from common security policies and device settings.
- CoreXL for multi-core support and other performance enhancements.
- Enhanced SecurePlatform operating system, supporting new hardware platforms and providing better performance.
- Provider-1 Enhancements: New Migration Tool, New High Availability Capabilities, Cross-CMA Search, New IPS Global Policy capabilities and more.

Check Point Software Blades

Check Point Security Gateways are comprehensive security solutions that deliver industry-leading performance, threat coverage, and value on a flexible Check Point Software Blade architecture.

With software blades, Security Gateways can be optimized to provide simple, flexible, extensible, and manageable security for deployments ranging in size from small branch offices to large enterprises to datacenters.

A software blade is a logical security building block that is independent, modular and centrally managed. Software Blades can be quickly enabled and configured into a solution based on specific business needs. And as needs evolve, additional blades can be quickly activated to extend security to an existing configuration within the same hardware foundation.

Check Point Software Blades include Firewall, VPN, IPS, Web Security, Anti-Virus and Anti-Malware, URL Filtering, Messaging Security, Acceleration and Clustering, Advanced Networking, Network Policy Management, End Policy Management, Logging and Status, Monitoring, Management Portal, User Directory, Provisioning, Reporting, Event Correlation.

Software Blades can be deployed on Check Point UTM-1 and Power-1 appliances, partner appliances, open servers and within virtualized environments. New blades can be added by simply enabling their functionality in software; no additional hardware, firmware or drivers are necessary. This enables organizations to deploy security dynamically, as needed, with lower total cost of deployment.

More information about Software Blades can be found at:

<http://www.checkpoint.com/products/softwareblades/architecture/index.html>

IPS

New IPS engine: R70 introduces a new multi-tier inspection engine, delivering:

- Excellent security capabilities for detection and prevention of known and unknown, client and server attacks.
- Application controls for Peer-To-Peer, Instant Messaging and many other applications.
- On-going update services covering Microsoft Patch Tuesday and many other applications.
- Admin workflow and tools that allow simple management and deployment of IPS capabilities.

Blazing Fast Performance: Introducing a completely new IPS enforcement architecture that allows up to 10 Gbps IPS throughput. Even when all protections are activated throughput remains above 2.2 Gbps.

Signature Matching Engine: New signature matching engine provides faster release of new updates, while maintaining excellent performance no matter how many new protections are added.

Bypass Under Load: Maintain high network performance, with the new ability to stop inspection of traffic when the gateway reaches user-defined memory or CPU thresholds. Inspection resumes when the stress decreases.

Automatic Activation of Protections: Automatically manage protections or profiles based on policy decisions, allowing easier creation of new profiles; predictable, consistent maintenance; and update of protections and security policies. All protections received through the protection update service can now be activated, deactivated or put in detect-only mode automatically, according to the same policy decisions defined for the profile. Protections can also be automatically activated based on user-defined criteria such as threat severity, estimated impact on performance, and confidence indexing.

Network Exceptions: Exclude any source, destination, service or gateway from IPS inspection, for any specific protections or from all protections.

Intuitive Information Access Points: Directly access any SmartView Tracker log from the protection that generated it and link back to IPS. Easily create an exception to a specific protection based on a log or set the protection to Detect.

Packet Capture: Added ability to save identified packets for forensics and analysis.

Protections Browser: The Protections Browser provides a central view of all protections and the capability to quickly find, view or modify protection activation settings, globally or per profile. Find any protection by name, CVE number, protocol, severity or any other parameter.

Provisioning Software Blade

Check Point's Provisioning Software Blade provides an intuitive and easy interface to centrally manage device configurations, such as operating system and network settings. Networking configurations include DNS, hosts, domain, routing and interfaces settings.

Each provisioned device can be managed separately or associated with a provisioning profile, and thus inherits all of the profile's settings. Each profile defines the gateway properties per profile object - which represents multiple, unlimited gateways with similar properties and policies - rather than per physical gateway. This means that time invested in each device can be minimized and batch operations performed, thereby reducing administrative overhead.

A provisioning profile can define specific settings for networking, device management, and the operating system. Common device settings include DNS, time zones, domain names and routing data. Provisioning profiles can be applied to UTM-1, Power-1, SecurePlatform or UTM-1 Edge appliances.

All devices managed fetch their assigned profiles from the centralized management server. If the fetched profile differs from the previous profile, the device is updated with the changes. Thus, one profile is able to update potentially hundreds and thousands of devices, each acquiring the new common properties, while maintaining its own local settings.

CoreXL

Multi-Core Performance Acceleration: SecurePlatform, IPSO 6, and Crossbeam support excellent performance scalability across multiprocessing cores using CoreXL.

Performance Enhancements

Anti-Spoofing Enforcement Acceleration: Spoofed traffic is dropped, significantly improving the performance of the gateway when handling spoofed traffic.

Provider-1/SiteManager-1

New Migration Tool: Easily export CMAs from one MDS to another with the new R70 Migration Tool. Enable automatic export and archive of CMAs, Security Management servers, or MGS global database for migration.

High Availability Capabilities: New High Availability features make Load Sharing and Failover deployments even more flexible and reliable.

- **Cross-Platform High Availability:** Add Provider-1 systems of one operating system to an existing HA deployment of another.
- **Multi-CMA High Availability:** Include more than two CMAs per Customer (one primary CMA and multiple secondary CMAs).
- **Failure Recovery in High Availability Deployments:** Recovery in many cases of a failed MDS in a High Availability deployment.

Cross-CMA Search: Search across multiple CMA databases for defined Network objects (including groups, Dynamic objects and Global objects) and for rules (including Global and implied rules) that contain or affect a specified object.

Provider-1 Shell (P1Shell): New command line shell that enables Provider-1 administrators to run commands in both MDS and CMA environments - without root permissions.

IPS in Global Policy: When a Global Policy is assigned, CMAs receive the global IPS profiles contained in the Global Policy. Global profiles can be specifically assigned to individual gateways.

Endpoint Connect VPN Client

R70 supports Endpoint Connect: Check Point's new lightweight remote access client, providing seamless, secure (IPSec) VPN connectivity to corporate resources.

SecurePlatform

R70 includes the latest enhancements to SecurePlatform and SecurePlatform Pro operating systems. This release of SecurePlatform supports a large variety of hardware, including open servers, network cards and RAID controllers. A comprehensive list of certified hardware can be found at:

http://www.checkpoint.com/products/supported_platforms/secureplatform.html

Supported Products

In This Section

[Build Numbers](#)

[page 8](#)

[Management Products by Platform](#)

[page 9](#)

[Clients and Consoles by Platform](#)

[page 10](#)

[Platform Provisions and Requirements](#)

[page 10](#)

[Upgrade Notes](#)

[page 13](#)

[HFAs Included in this Release](#)

[page 13](#)

Build Numbers

The following table lists all R70 software products available, and the build numbers as they are distributed on the product CD. To verify each product's build number, use the given command format or direction within the GUI. All build numbers are subject to change.

Table 3 Product Build Numbers

Software Blade / Product	Build No.	Verifying Build No.
Security Gateway	730121143	fw ver
Security Management	730121040	fwm ver
SmartConsole Applications	730121214	Help > About Check Point <product name>
Provider-1/SiteManager-1 Multi-Domain Server (MDS)	730121061	CPvinfo \$MDSDIR/lib/libmids.so grep "Build Number"
Provider-1/SiteManager-1 Multi-Domain GUI (MDG)	730121050	Help > About Check Point Provider-1/SiteManager-1
SecurePlatform	730121097	ver
Infrastructure (SVN Foundation)	730121153	cpshared_ver
Acceleration (Performance Pack)	730121023	sim ver -k
Advanced Networking (QoS)	730121015	fgate ver
Advanced Networking (Routing)	ngc2.3	gated -ver
Monitoring (SVM Server)	730121010	rtm ver
Management Portal	730121013	cpvinfo /opt/CPportal-R70/portal/bin/smartportalstart
Event Correlation (Eventia Analyzer)	730121011	cpsemd ver
Reporting (Eventia Reporting)	730121025	SVRServer ver
Endpoint Policy Server (SecureClient Policy Server)	007	dtps ver
SecuRemote/SecureClient	019	Help > About
UTM-1 Edge Firmware	8.0.36	Displayed on the default portal page
Endpoint Security Client Flex/Agent	7.0.888.000	Right-click the System Tray icon and select About
Endpoint Security Server	7.20.121.000	System configuration > Version information
Compatibility Packages	CPNGXCMP-R70: 011 VSX NGX R65 (V40): 663 CPvsxngxcmp-R70: 510 UTM-1 Edge: 4.1 CPCON66CMP-R70: 006 CPCON62CMP-R70: 16	/opt/CPNGXCMP-R70/bin/fw_loader ver /opt/CPV40Cmp-R70/bin/fw_loader ver /opt/CPvsxngxcmp-R70/bin/fw_loader ver /opt/CPEdgecmp-R70/bin/fw ver /opt/CPCON66CMP-R70/bin/fw_loader ver /opt/CPCON62CMP-R70/bin/fw_loader ver

Management Products by Platform

Table 4 Management Products and Software Blades by Platform

Software Blade / Product	Platform and Operating System						
	Check Point	Windows		RHEL 5.0	Nokia	Crossbeam	Solaris
	Secure Platform	Server 2003 (SP1-2)	Server 2008	kernel 2.6.18	IPSO 6.0.7	X-Series	Ultra-SPARC 8, 9, 10
Security Gateway	X	X	X		X	X	
Security Management	X	X	X	X	X		X
Provider-1/SiteManager-1 Server (MDS)	X			X			X
Performance Pack	X				X	X	
Advanced Routing	X				X	X	
Management Portal	X	X	X	X			X
Reporting and Event Correlation	X	X	X	X			X
Clustering (ClusterXL)	X	X	X		X	X	
CoreXL	X				X	X	
Provisioning Enabled SmartLSM Gateways	X	X	X		X		
Provisioning Enabled Management	X	X	X	X			X
SSL Network Extender Server	X	X	X		X		
Endpoint Security Server	X	X	X	X			
VSX Security Gateway	X				(IPSO 5)	X	
OSE Supported Routers	Cisco OS Versions: 9.x, 10.x, 11.x, 12.x						

Product and Software Blade Notes

- The maximum number of supported cluster members in ClusterXL mode is five; in third-party mode the maximum is eight.
- Management Portal is supported on the following Web browsers: Internet Explorer 6 and 7, and Mozilla Firefox 1.5 - 3.0.

Clients and Consoles by Platform

Table 5 Client Product by Platform

Check Point Product	Platform and Operating System									
	Windows							Mac	Mac	Linux
	2000 Server / Advanced Server (SP1-4)	2000 Pro (SP1-4)	XP Home & Pro (SP3)	Mobile 2003 2003SE 5.0, 6.0, 6.1	Server 2003 (SP1-2)	Vista (SP1)	Server 2008	OS 10.4	OS 10.5	
SmartConsole			X		X	X	X			
Provider-1/SiteManager-1 MDG			X		X	X	X			
SecuRemote	X	X	X		X					
SecureClient	X	X	X		X	X		X	X	
SecureClient Mobile				X						
SSL Network Extender		X	X			X		X	X	X
Endpoint Security Client		X	X							X
Endpoint Connect Client		X	X			X				

Platform Provisions and Requirements

In This Section

[SecurePlatform](#)

[page 10](#)

[Linux](#)

[page 11](#)

[UTM-1 Edge](#)

[page 11](#)

[IPSO](#)

[page 11](#)

[Microsoft Windows](#)

[page 11](#)

[Solaris](#)

[page 12](#)

SecurePlatform

This release is shipped with the latest SecurePlatform and SecurePlatform Pro operating systems, which support a large variety of concurrent and upcoming hardware – open servers, network cards and RAID controllers. A comprehensive list of certified hardware appears at:

<http://www.checkpoint.com/services/techsupport/hcl/index.html>

Check this list before installing SecurePlatform on the target hardware.

On UTM-1 and Power-1 appliances, to be able to restore images with the boot menu, modify the `/boot/grub/grub.conf` file:

change `configurefile /grub/submenus/snapshots.lst` to
`configurefile /grub/submenus/switch_to_backup.lst`

Linux

This release supports Red Hat Enterprise Linux 5.0 for specific management products only. Before installing a Check Point management product on Red Hat Enterprise Linux 5.0, perform the following steps.

To prepare Red Hat Enterprise Linux 5.0 for Check Point management installation:

1. Install the sharutils-4.6.1-2 package
 - a. Check if 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. Check if 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. Check if 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 machine.

UTM-1 Edge

R70 Security Management can manage UTM-1 Edge devices with firmware 7.5 and up. Earlier firmware is not supported.

IPSO

- Provides Advanced Routing and SecureXL as default.
- Clustering on IPSO supports VRRP and IP Clustering.
- UTM-1 Edge devices cannot be managed from a Security Management running on IPSO.
- The following hardware platforms are supported in all forms (Disk-based, Flash-based, Hybrid):
IP560, IP690, IP1280, IP2450
- This release supports IPSO 6.0.7.

Microsoft Windows

HA Legacy mode is not supported on Windows Server 2003.

Security Management and Gateways are supported on Windows Server 2003 and Windows Server 2008 (see [Table 4](#)). Windows Server 2000 is not supported.

Solaris

Security Management Server and Provider-1 are supported with Solaris running on UltraSPARC 64-bit platforms (see [Table 4](#)). R70 Security Gateways are not supported on Solaris.

Required Packages

- SUNWlibC
- SUNWlibCx (except Solaris 10)
- SUNWter
- SUNWadmC
- SUNWadmfw

Required Patches

The patches listed below are required to run Check Point software on Solaris platforms. They can be downloaded from: <http://sunsolve.sun.com>.

To display your current patch level, use the command: `showrev -p | grep <patch number>`

Table 6 Required Solaris Patches

Platform	Required	Recommended	Notes
Solaris 8	108528-18		If the patches 108528-17 and 113652-01 are installed, remove 113652-01, and then install 108528-18.
	110380-03		
	109147-18		
	109326-07		
	108434-01		Required only for 32 bit systems
	108435-01		Required only for 64 bit systems
			109147-40 or higher
Solaris 9	112233-12		
	112902-07		
	116561-03		Only if dmfe(7D) ethernet driver is defined on the machine
			112963-25 or higher
Solaris 10	117461-08 or higher		When using bge interfaces, operating system updates must be no higher than update 1, and the kernel patch must be no higher than 118822-20. For information regarding installing more recent patches, see Check Point SecureKnowledge sk31772.

Upgrade Notes

- Check Point Suite Products before version NGX R60 cannot be upgraded to R70.
- When upgrading NGX R65, only the following plug-ins may be present: Connectra, SmartProvisioning, VSX, and Messaging Security. The presence of any other plug-in will cause the upgrade process to fail.



Warning - If you upgrade from NGX R65 with plug-ins to R70, and later want to uninstall R70 (rollback to NGX R65), follow the instructions in sk37252 (<http://supportcontent.checkpoint.com/solutions?id=sk37252>) to avoid potential problems.

- When upgrading Eventia from a version prior to R63, after upgrading the distributed Eventia Reporter, run cpstop on the Eventia Reporter machine, and only then perform the add-on upgrade.
- It is recommended to read the list of Known Limitations, published in sk37042 (at: <http://supportcontent.checkpoint.com/solutions?id=sk37042>), prior to any upgrade procedure.

HFAs Included in this Release

This release includes fixes and improvements that were initially distributed as part of NGX R65 Hotfix Accumulator (HFA) R65_HFA_40.

- See VPN-1 NGX R65 HFA 40 Release Notes at:
http://supportcontent.checkpoint.com/documentation_download?ID=8684
- See Provider-1/SiteManager-1 NGX R65 HFA 40 Release Notes at:
http://supportcontent.checkpoint.com/documentation_download?ID=8764

Minimum System Requirements

In This Section

Security Gateway Hardware Requirements	page 14
Security Management Hardware Requirements	page 14
SmartConsole and Provider-1 MDG Hardware Requirements	page 14
Provider-1/SiteManager-1 Multi Domain Server Requirements	page 15
VSX Gateway Hardware Requirements	page 15
Eventia Analyzer Requirements	page 15
Eventia Reporter Requirements	page 16
SecureClient Requirements	page 16
Endpoint Security Server Requirements	page 18
Endpoint Security Client Requirements	page 18

Security Gateway Hardware Requirements

Table 7 Minimum Hardware Requirements of Security Gateway

	Windows	SecurePlatform	Linux
Processor	Intel Pentium IV or 1.5 GHz equivalent	Intel Pentium IV or 2 GHz equivalent	Intel Pentium IV or 2 GHz equivalent
Free Disk Space	1GB	10GB	1.4GB
Memory	500MB	500MB	500MB
CD-ROM Drive	Yes	Yes	Yes
Network Adapter	One or more	One or more supported cards	One or more

Security Management Hardware Requirements

Table 8 Minimum Hardware Requirements of Security Management

	Windows	Linux	SecurePlatform	Solaris
Processor	Intel Pentium IV or 1.5 GHz equivalent	Intel Pentium IV or 2 GHz equivalent	Intel Pentium IV or 2 GHz equivalent	Intel Pentium IV
Free Disk Space	1GB	1.4GB	10GB (installation includes OS)	1GB
Memory	1GB	1GB	1GB	512MB
CD-ROM Drive	Yes	Yes	Yes (bootable)	Yes
Network Adapter	One or more	One or more	One or more	Yes

SmartConsole and Provider-1 MDG Hardware Requirements

The following table shows the minimum hardware requirements for console applications, including: SmartDashboard, SmartView Tracker, SmartView Monitor, Provisioning, Eventia Reporter and Eventia Analyzer, SecureClient Packaging Tool, SmartUpdate, and Provider-1 Multi-Domain GUI (MDG).

Table 9 Minimum Hardware Requirements for Consoles

	Windows
CPU	Intel Pentium IV or 2 GHz equivalent processor
Memory	512MB
Disk Space	500MB
CD-ROM Drive	Yes
Video Adapter	minimum resolution: 1024 x 768

Provider-1/SiteManager-1 Multi Domain Server Requirements

Table 10 Minimum Hardware Requirements of Provider-1 MDS

	Linux	Solaris	SecurePlatform
CPU	Intel Pentium IV or 2 GHz equivalent	UltraSPARC III 900MHz	Intel Pentium IV or 2 GHz equivalent
Memory	4GB	4GB	4GB
Disk Space	2GB	2GB	10GB (install includes OS)
CD-ROM Drive	Yes	Yes	Yes (bootable)

Provider-1 Resource Consumption

Actual disk space consumption depends on the scale of the deployment. The larger the deployment, the more disk space, as well as memory and CPU, is required.

The Provider-1 disk space requirements are as follows:

- For basic MDS installation: 800MB (mostly for /opt directory).
- For each CMA: 100MB (for the CMA directory located in /var/opt)

VSX Gateway Hardware Requirements

Table 11 Minimum Hardware Requirements of VSX Gateway

	SecurePlatform
Processor	Intel Pentium III or 1 GHz or equivalent
Memory	512MB
Disk Space	9GB (Including the operating system)
CD ROM Drive	Yes
Network Interface Cards	3 (4 if you are planning to deploy a VSX cluster)



Note - VSX also supported on Crossbeam X-Series Security Services Switches and IPSO 5.0.

Eventia Analyzer Requirements

Eventia Analyzer is installed on a Log Server; it is not supported for installation on a Security Management server.

Table 12 Minimum Hardware Requirements of Eventia Analyzer

	Windows/Linux/SecurePlatform	Solaris
CPU	Intel Pentium IV 2.8 GHz	v240 1.5 GHz
Memory	2GB	4GB
Disk Space	25GB	25GB

Eventia Reporter Requirements

The hardware requirements presented below are designed for an Eventia Reporter server that will process at least 15GB of logs per day and generate reports according to the performance numbers. For deployments that will generate fewer logs per day, a machine with less CPU or memory can be used, with the caveat that this may cause degradation in the performance numbers.

Table 13 Minimum Hardware Requirements of Eventia Reporter

	Windows & Linux Minimum	Windows & Linux Recommended	Solaris
CPU	Intel Pentium IV 2.0 GHz	Dual CPU 3.0 GHz	UltraSPARC III 900 MHz
Memory	1GB	2GB	1GB
Disk Space		(on 2 physical disks)	
Installation:	80MB	80MB	80MB
Database:	60GB (40GB for database, 20GB temp directory)	100GB (60GB for database, 40GB for temp directory)	60GB (40GB for database, 20GB for temp directory)
CD-ROM Drive	Yes	Yes	Yes

Recommendations to Optimize Eventia Reporter Performance

- Disable DNS resolution - consolidation performance may improve to 32GB of logs/day.
- Configure the network connection between the Eventia Reporter server and the Security Management (or the Log Server), to the optimal speed.
- Use the fastest disk available with the highest RPM (revolutions per minute) and a large buffer size.
- Use the **UpdateMySQLConfig** to tune the database configuration and adjust the consolidation memory buffers to use the additional memory.
- Increase the machine's memory, as it significantly improves performance.
- Install an uninterruptible power supply (UPS) for the Eventia Reporter Server.

SecureClient Requirements

Table 14 Minimum Hardware Requirements for SecureClient

	SecureClient
CPU	133 MHz Pentium-compatible CPU
Memory	128MB
Disk Space	40MB



Note - These requirements are true for Mac OS-X as well.

Supported SecureClient Mobile Hardware

- Intel ARM/StrongARM/XScale/PXA Series Processor family
- Texas Instruments OMAP processor family
- Qualcomm MSM 7200 processor family

Supported SecureClient Mobile Operating Systems

- Windows Mobile 2003/2003 SE or Windows Mobile 5.0 on Pocket PC devices
- Windows Mobile 5.0 on Smartphone devices
- Windows Mobile 6.0 (classic, standard, professional)
- Windows Mobile 6.1

SecureClient Mobile Tested Devices

The following table shows tested devices for installing SecureClient Mobile.

Table 15 Tested Devices for SecureClient Mobile Hardware

Operating System	Tested Devices
PocketPC running Windows Mobile 2003/2003 SE	<ul style="list-style-type: none"> Dell AXIM X50 Pocket PC 2003 HTC Blue Angel (XDA III, MDA III, Qtek 9090, i-Mate 2K, Sprint PPC-660, Verizon XV6600, Cingular SX66) HTC Himalaya (XDA II, MDA II, Qtek 2020, i-Mate, Orange SPV1000) HTC Magician (Dopod 818, i-mate JAM, O2 XDA mini, Qtek 5100, MDA Compact) HP/Compaq iPAQ Pocket PC 2003 - series 4150,4350,3950,5450, 5550, 2210,6340 HP/Compaq iPAQ Pocket PC 2003 SE / Phone Edition - series 4700, hx2x00
PocketPC running Windows Mobile 5.0	<ul style="list-style-type: none"> Dell AXIM X51v ETEN M600 Fujitsu Siemens LOOX T830 HP iPAQ HX2790 HTC Universal (O2 Exec, i-Mate JasJar, Orange M5000, MDA IV) HTC Wizard/Apache (Sprint PPC6700, Orange SPV M3000a, T-Mobile MDA Vario, i-mate K-Jam) HTC TyTN Palm Treo 700w, 700wx, 700v
Windows Mobile 6.0 (Classic/Professional)	<ul style="list-style-type: none"> ETEN Glofiish M700 HTC s710/VOX; HTC s730; HTC PPC6800 HTC Touch; HTC Touch Dual; HTC Touch Cruiser HTC TyTN II HP iPAQ 510 Voice Messenger i-mate SP5m; i-mate Ultimate 8150 Motorola Q9 Toshiba Portégé g900
Windows Mobile 6.1	<ul style="list-style-type: none"> HTC Touch Diamond HTC TyTN II HP iPAQ 914c Business Messenger
Windows Mobile 5.0 Smartphone	<ul style="list-style-type: none"> HP iPAQ 6900 series HTC Advantage X7500/X7501 HTC S620 (Excalibur, t-mobile Dash) HTC StrTrk (i-mate smartflip, qtek 8500, Cingular 3125) HTC Tornado (i-mate sp5/sp5m, qtek 8310) Motorola Q Samsung i320, i600
Hardened PocketPC devices	<ul style="list-style-type: none"> Intermec 700 Motorola HC700 Symbol MC70

Supported SecureClient Mobile Communication Cards

Any communication card that is supported by the supported devices listed above, and provides an IP interface, should be valid.

The following cards have also been tested and proved to work.

- Linksys WCF 12
- SanDisk Connect Wi-Fi SD Card
- Sierra AirCard: 555, 750
- Socket Communications: CF Bluetooth Adapter, CF Wireless LAN Card, Serial Adapter
- Spectec WLAN-11b
- TRENDNet TE-CF100 10/100Mbps CompactFlash Fast Ethernet Adapter

Endpoint Security Server Requirements

Table 16 Minimum Hardware Requirements of Endpoint Security Server

	Number of Users	Endpoint Security server
CPU	2000	Intel Pentium 4 2GHz Intel Dual Xeon 2GHz
Memory	2000	1GB
Disk Space	2000	10GB
CD-ROM Drive	N/A	Yes

Table 17 Bandwidth / Policy Download of Endpoint Security Server

Users	Policy Downloads (Kbps) ¹	Ask Requests (Kbps) ²	Log Uploads (Kbps) ³	Total (Kbps) ⁴
500	513.33	0.66	11.11	645.1
1,000	1026.66	1.33	22.22	1170.21
2,000	2053.33	2.22	40.22	2215.77
5000	5133.33	6.66	111.11	5251.11

1. Policy Downloads - 1 deployment of a Default Policy within the heartbeat time.
2. Ask Requests - 1 Ask Request/hr
3. Log Uploads - 1 Log Upload/hr containing 5 events and 10 program observations
4. Total - 1 Sync/day, 1 Heartbeat/min, 1 Ask Request/hr, 1 Log Upload/hr, 1 Administrator

Table 18 Bandwidth / Administrator of Endpoint Security Server

Administrators (typical)	Kbps
1	120
3	355.55
5	600

Table 19 Supported Gateways and Clients of Endpoint Security Server

Check Point	<ul style="list-style-type: none"> • VPN-1 NGX R60 and later • FireWall-1 NG with Application Intelligence R55W and later • VPN-1 SecureClient with Application Intelligence R56 build 619 and later • Safe@Office 425W 5.0.58x and later
Cisco	<ul style="list-style-type: none"> • VPN 3000 Series Concentrator v. 4.7.1 and later • client 4.6.00.0049-K9 and later • Aironet 1200 Series Wireless Access Point v.12.2 (11)JA1 (Certified version)
Nortel	<ul style="list-style-type: none"> • Contivity 4.8.083 (TunnelGuard TG_1.1.3.0_002)
Enterasys	<ul style="list-style-type: none"> • RoamAbout R2 G060405 and later

Endpoint Security Client Requirements

Table 20 Minimum Hardware Requirements for Endpoint Security Agent and Flex Clients

	Endpoint Security Agent / Flex
CPU	Intel Pentium II 450 MHz
Memory	256MB
Disk Space	30MB



Note - Endpoint Security Clients support Novell Linux Desktop 9.1 SP1 as well as Red Hat Red Hat Linux WS 3.0 (Update 5).

Supported Anti-Virus Solutions

Endpoint Security server supports the latest version of the antivirus solutions listed below within 60 days of their latest release.

The following table lists the minimum supported versions of third-party antivirus solutions.

Table 21 Supported Anti-Virus Solutions for Endpoint Security Server

Computer Associates	<ul style="list-style-type: none"> • Vet v. 10.65.0.10 • eTrust Antivirus (InoculateIT) v. 7.0.139 and 7.1 • eTrust EZ Antivirus (EZ Armor) 2005 (r3.1)
McAfee	<ul style="list-style-type: none"> • VirusScan v. 4.1 • VirusScan Enterprise v. 8.0i • VirusScan Professional v. 9.0 • Internet Security Suite 2004 and 2005
Sophos	<ul style="list-style-type: none"> • Anti-Virus v. 3.81.0, 3.90.0, and 5.0 • Anti-Virus Small Business Edition 1.0.1
Symantec	<ul style="list-style-type: none"> • Norton AntiVirus 2004 and 2005 • Norton AntiVirus Corporate Edition v. 9.0 and 10.0 • Norton Internet Security 2004 and 2005
Trend Micro	<ul style="list-style-type: none"> • PC-cillin Antivirus 2004 • PC-cillin Internet Security 2004 and 2005 • OfficeScan Corporate Edition v. 6.5, 7.0, and 7.5

Supported Instant Messaging Software

- AOL 9, AOL Instant Messenger v. 5.9, AOL Instant Messenger Triton v. 0.1.12 Beta
- MSN v. 7.5, Windows Messenger
- Yahoo Instant Messenger v. 5, 6, and 7
- ICQ v. 5.04, ICQ Pro 2003b
- Trillian v. 2.0.12 (3 protocols), 2.0.13 (4 protocols), 3.0 (4 protocols), and 3.1 (4 protocols)
- GAIM v. 1.0.0, 1.0.2, 1.0.3, 1.1.0, 1.2.1, and 1.5.0
- Miranda v. 0.4rc1

Known Limitations



Note - This document does not include Known Limitations, which are published in [sk37042](https://supportcontent.checkpoint.com/solutions?id=sk37042) at:
<http://supportcontent.checkpoint.com/solutions?id=sk37042>

Documentation Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com

© 2003-2009 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to <http://www.checkpoint.com/copyright.html> for a list of Check Point trademarks

For third party notices, see http://www.checkpoint.com/3rd_party_copyright.html.

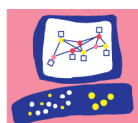
www.checkpoint.com

Worldwide Headquarters

Check Point Software Technologies, Ltd.
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753-4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

Check Point Software Technologies, Inc.
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.