

Endpoint Security

Release Notes
Version R72



Check Point
SOFTWARE TECHNOLOGIES LTD.

July 28, 2009

Contents

- About This Release 1
 - Components of This Release 1
 - Build Numbers 2
- What's New 2
 - WebCheck Introduced in Endpoint Security 2
 - Endpoint Connect VPN Introduced in Endpoint Security 2
 - Support for Windows Vista 64-Bit 3
 - Federated Servers Improve Scalability and Failover 3
 - Secure Single Authentication to Endpoint Security Functions - OneCheck Logon 3
 - MFAE and Language Files in Full Disk Encryption Profiles 3
 - Support for Spanish and Russian Languages 3
 - HTTPS File Shares Enhance Manageability 4
- Installation and Upgrade 4
- System Requirements for Servers 4
 - Supported Operating Systems for Servers 4
 - Endpoint Security Server 4
 - Application Server Hardware 4
 - Admin Application Server / Connection Points 5
 - Total Bandwidth* 5
 - Policy Download* 6
 - Operating Systems 7
 - Browsers (Administrator Console) 7
 - Supported Gateways and Clients 7
 - Supported Antivirus Solutions (pre-configured) 7
- Endpoint Security MI Framework 3.3 HFA 2 13
 - Endpoint Security MI Database (MIDB) 13
 - Endpoint Security MI Connection Point (CP) 14
 - Endpoint Security MI Directory Scanner (DS) 14
 - Endpoint Security MI Management Console (MIMC) 15
 - Endpoint Security MI Device Agent 16
- Endpoint Security webRH 2.4 HFA 2 16
- Endpoint Security Media Encryption 18
 - Disk and Memory Space 18
- Endpoint Security License Server and Reporting Tool 19
- System Requirements for Clients 19
 - Supported Operating Systems for Clients 19
 - Memory (RAM) and Disk Space Requirements per Client 20
 - Endpoint Security VPN (Endpoint Connect) 20
 - Endpoint Security VPN Legacy (SecureClient) 20
 - Endpoint Security Firewall 20
 - Endpoint Security Full Disk Encryption for Windows 20
 - Endpoint Security Full Disk Encryption for Mac 22
 - Endpoint Security Media Encryption 22
- Upgrading to Endpoint Security R72 23
- Installing Endpoint Security Server and webRH on Same Machine 23

Resolved Issues	24
Known Limitations	24

About This Release

Note - The latest version of this document is available at:

http://supportcontent.checkpoint.com/documentation_download?ID=10169

Check Point Endpoint Security unifies the highest-rated firewall, antivirus, anti-spyware, endpoint encryption, network access control (NAC), and remote access VPN in a single, centrally managed client and console. The unification of these components eliminates the need to deploy and manage multiple endpoint security agents. This not only mitigates the broadest possible range of endpoint threats, including confidential data theft, viruses, and host-based intrusions, but also reduces total cost of ownership through lower administrative overhead and increased operational efficiencies unlike any other endpoint solution.

Components of This Release

The components of Endpoint Security are:

- **Endpoint Connect VPN:** Virtual Private Network for secured private communication over public networks
- **Anti-Virus and Anti-Spyware:** Prevention and treatment of virus, worm, trojan horse, keylogging software, and malware.
- **WebCheck:** protection against Web-based threats, for example, phishing.
- **Firewall:** Defense against Internet threats with definable zones and security levels.
- **Program Control:** Ensures that only legitimate and approved programs are allowed to run on PCs. Enables automation of most application policy decisions.
- **Full Disk Encryption:** Data security through pre-boot authentication and full disk encryption.
- **Media Encryption:** Data security through encryption of removable media.

To enable correct and easy installation, the following components are also added:

- **Deployment Utility:** System administrator utility to create installation packages for all components.
- **License Server and Reporting Tool:** System administrator utility to easily activate licenses for required environment.

Build Numbers

The relevant build numbers at the time of this release are as follows:

Table 2-1 Build numbers

Component	Build number
Secure Access	7.5.225
WebCheck	1.4.338.0
Media Encryption	4.95.0.329
Full Disk Encryption	7.3.1522

What's New

WebCheck Introduced in Endpoint Security

The WebCheck feature was created from the ground up to protect users from the Web-based threats that exist today. At its core is a powerful yet lightweight virtualization engine that surrounds the user from all sides in a “bubble of security” as they surf the Web. WebCheck also contains advanced anti-phishing and data protection functionality.

Endpoint Connect VPN Introduced in Endpoint Security

Endpoint Connect revolutionizes Remote Access. It provides intelligent auto-connection, so that the end user only has to press the Connect button regardless of the network connection. It is no longer necessary to select different connectivity modes depending on the network topology (for example, NAT Traversal, UDP encapsulation, Visitor Mode). Endpoint Connect also maintains VPN connections when the underlying network is intermittent (for example, wireless on the go) or the end user changes network by moving between different networks (for example, EDGE, LAN to wireless).

The customer can now choose the VPN client in the Endpoint Security client. It can be based on either the SecureClient code base or the Endpoint Connect code base.

Support for Windows Vista 64-Bit

The Check Point Endpoint Security client now runs on 64-bit Windows Vista operating system.

Federated Servers Improve Scalability and Failover

Endpoint Security now supports federated servers. With a federated architecture, clients will connect to one of several Connection Points (sub-servers). If the main server becomes unreachable, the clients will randomly pick another Connection Point in their list and connect to that server. The Connection Points connect back to the primary server to upload the logs, download policy, and DAT files. This provides high availability/scale beyond the single server model. The Connection Point can be geographically distributed and will connect back to the primary server whenever a connection is available.

Secure Single Authentication to Endpoint Security Functions - OneCheck Logon

Currently, once an end user logs on to preboot authentication, he or she can be automatically logged onto Windows with the Single Sign-On feature. But the end user still has to log in to VPN and to the encrypted USB sticks for USB sticks that are created to be read also on machines that do not have an EPS client. OneCheck Logon provides single sign-on functionality to Check Point's Endpoint Connect VPN, Media Encryption, and to Windows.

MFAE and Language Files in Full Disk Encryption Profiles

In past releases, customers wanting to make changes to MFAE (Multi Factor Authentication Engine) or localized languages had to run a script after installation. Changes to MFAE drivers and localized language files can now be specified in the same profile as all the other FDE settings.

Support for Spanish and Russian Languages

In addition to English, French, Italian, German, and Japanese, the Endpoint Security client now supports Spanish and Russian.

HTTPS File Shares Enhance Manageability

FDE logs and policy can now be transferred over HTTPS in addition to the existing UNC file share method. This is useful because firewalls are often configured to block UNC file share traffic, which can prevent an EPS client using the FDE feature in EW mode from reaching the file share used by the FDE server. HTTPS ports are more likely to be kept open. Transferring over HTTPS is also better for MSPs that manage endpoints that are permanently outside the firewall.

Installation and Upgrade

To install Endpoint Security Client, use the R72 Client, which you can download from http://supportcontent.checkpoint.com/file_download?id=10249, or use the client package on CD1 of the Endpoint Security R72 package.



Note - An evaluation licence is available from the **Check Point User Center**. Go to **Products > Quick Evaluation**.

System Requirements for Servers

Supported Operating Systems for Servers

Endpoint Security Servers are supported on the following operating systems:

- Windows 2003
- Check Point Secure Platform (SPLAT) v. R65

Endpoint Security Server

Application Server Hardware

- Intel Pentium Intel Core 2
- Intel Dual Xeon 2GHz

Admin Application Server / Connection Points

Table 2-2 Admin Application Server / Connection Points

Users	RAM	Disk Space
up to 500	1 GB	5 GB
up to 1,000	1 GB	10 GB
up to 2,000	1 GB	12 GB
up to 5,000	1 GB	15 GB
up to 20,000	3 GB	53 GB
up to 60,000 ¹	3 GB	53 GB

1. With 3 Connection Points running 20,000 users each and 1 server aggregating them.

Total Bandwidth*

Table 2-3 Total bandwidth

Users	Kbps
up to 500	469
up to 1,000	916
up to 2,000	1,809
up to 5,000	4,488
up to 20,000	17,882

*Assumes 1 sync per day, 1 heartbeat per minute, 1 ask per hour, 1 log upload per hour and 1 Administrator.

Policy Download*

Table 2-4 Policy downloads

Users	Kbps
up to 500	1
up to 1,000	2
up to 2,000	4
up to 5,000	11
up to 20,000	43

*Assumes one deployment for all users and policies of certain sizes.

Ask Bandwidth*

Table 2-5 Ask bandwidth

Users	Kbps
up to 500	.8
up to 1,000	1
up to 2,000	3
up to 5,000	8
up to 20,000	35

*Assumes one ask per hour.

LogUpload Bandwidth*

Table 2-6 LogUpload bandwidth

Users	Kbps
up to 500	11
up to 1,000	22
up to 2000	44
up to 5,000	111
up to 20,000	444

*Assumes one logupload per day.

Operating Systems

- Red Hat Enterprise Linux ES v. 3.0 (Update 5)
- Windows 2000 Server (SP4) and Advanced Server (SP4)
- Windows Server 2003 (SP1 and SP2)
- Windows Server 2003 R2 (SP2)
- Check Point Secure Platform (SPLAT) v. R65

Browsers (Administrator Console)

- Internet Explorer v. 6 (SP2), v. 7, and v. 8
- Google Chrome
- Mozilla Firefox 1.5, 2.0, 3.0 and 3.5

Supported Gateways and Clients

- Check Point VPN-1 NGX 157 or later
- Check Point VPN-1 Power
- Check Point VPN-1 UTM
- Check Point VPN-1@ SecureClient™ with Application Intelligence R56 build 619 or later (recommended)
- Check Point Safe@Office 425W 5.0.58x or later
- Cisco VPN Concentrator v. 4.7.1 or later
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco client 4.6.00.0049-K9 or later
- Cisco Aironet 1100 Series Wireless Access Point v.12.2 (11)JA1 (Certified version)
- Nortel Contivity 4.8.083 (Tunnelguard TG_1.1.3.0_002)
- Enterasys RoamAbout R2 G060405 or later

Supported Antivirus Solutions (pre-configured)

This section lists the minimum supported versions of third-party antivirus solutions. Generally, Endpoint Security supports the latest version within 60 days of its release.

McAfee

- On Windows XP:
 - McAfee Internet Security Suite 2005 and 9.0 (VS 11.0)
 - McAfee Total Protection 2008 (VS 12.1)
 - McAfee VirusScan Plus 2007 11.2 and 2008 12.1
 - McAfee VirusScan 2009 13.0 and 13.3
 - McAfee VirusScan Enterprise 7.0, 8.5 and 8.7
- On Windows Vista:
 - McAfee Internet Security Suite 2007 (PFW 9.1), 9.0 (PFW 8.0) and PFW 10.0
 - McAfee VirusScan Plus 2007 (PFW 8.0)

Computer Associates

On Windows XP:

- CA Anti-Virus, the following versions:
 - 8.3.0.1 (CA ISS 2007)
 - 8.3.0.3 (CA ISS 2007)
 - 10.0.0.163 (CA AV 2009)
- CA eTrust Threat Management Agent, the following versions:
 - 8.1.655.0
 - 8.0.403.0
- CA eTrust azAntivirus 7.0.8.1

Symantec

- On Windows XP:
 - Norton Internet Security, the following versions:
 - 2005, 2006, 2007, 2008
 - 2009, the following versions:
 - » 16.0.0.103
 - » 16.1.0.33
 - » 16.2.0.7
 - » 16.5.0.135
 - Symantec Endpoint Protection, the following versions:
 - » 11.0.4000.2295
 - » 11.0.3001.2224
 - Symantec Endpoint Protection Small Business Edition 12.0.122.192
 - Norton 360, the following versions:
 - » 1.3
 - » 2.0
 - » 2.5
 - » 3.0
 - Symantec AntiVirus Corporate Edition 10.1
- On Windows Vista:
 - Norton Internet Security, the following versions:
 - » 2007 and 2008
 - » 2009 16.0.0.103, 16.2.0.7 and 16.5
 - Symantec Endpoint Protection 11.0.4000.2295 and 11.0.3001.224
 - Norton 360 1.3

Sophos

- On Windows XP:
 - Antivirus 6.5
 - Antivirus 7.3
 - Antivirus 7.6.4
 - Antivirus 7.6.6
- On Windows Vista
 - Antivirus 7.3

Trend Micro

- On Windows XP:
 - Internet Security 2008 and 2009
 - Antivirus 2007
 - PC-cillin 2006 and 2007
 - OfficeScan 7.0, 7.3 and 8.0
 - OfficeScan 10 conventional mode and smart mode
 - Virus Buster 2008 and 2009
- On Windows Vista:
 - Internet Security 2009

Panda Software

On Windows XP:

- Panda Antivirus 2009 and 2010

ALWIL Software

On Windows XP:

- avast! Antivirus, the following versions:
 - 4.8.1296
 - 4.8.1229
 - 4.8.1201
 - 4.7.1098
 - 4.7.1098
 - 4.6.763
 - 4.6.603
 - 4.8.1335

ESET

- On Windows XP:
 - NOD32 Antivirus, the following versions:
 - » 3.0.621.0
 - » 3.0.669.0
 - » 4.0.314.0
- On Windows Vista:
 - NOD32 Antivirus 4.0.314.0

AVG

- On Windows XP:
 - Antivirus, the following versions:
 - » 8.0.233
 - » 8.0.176
 - » 8.0.173
 - » 8.0.156

- » 8.5.278
- » 8.5.323
- » 8.5.339
- On Windows Vista:
 - Antivirus, the following versions:
 - » 7.0
 - » 7.5
 - » 8.5.278

Kaspersky

- On Windows XP:
 - Internet Security 6, 7, 8 and 9
- On Windows Vista:
 - Internet Security 7, 8 and 9

Microsoft

- On Windows XP:
 - Windows Live OneCare 2.5.2900.15
 - Forefront MSFCS 1.5.1937.0
- On Windows Vista:
 - Windows Live OneCare 2.5
- On Windows 2003:
 - Forefront MSFCS 1.5.1937.0

Endpoint Security MI Framework 3.3 HFA 2

This section describes the requirements for the Endpoint Security MI components.

Endpoint Security MI Database (MIDB)

This table describes the system requirements for the Endpoint Security MI database:

Table 2-7 Endpoint Security MI Database Requirements

Item	Requirement
Operating System	Microsoft Windows 2000 Server (Standard, Enterprise, and Web Edition) – minimum Service Pack 4 Microsoft Windows Server 2003, minimum Service Pack 2
Databases	Microsoft SQL Server 2000 (Standard and Enterprise) minimum Service Pack 2 (Service Pack 3 for Microsoft Windows Server 2003) or Microsoft SQL Server 2005 (Standard and Enterprise)
Disk Space (initial)	35 MB available
Memory	256 MB
Network Connectivity	TCP/IP networking Stored Procedure Call access from other Endpoint Security components

Endpoint Security MI Connection Point (CP)



Note - We strongly recommend that you use a dedicated IIS server for Endpoint Security MI. The reason for this is that the IIS server needs to be restarted during installation and upgrade of the connection point component, and during upgrade of the 'Connection Point – Device Agent' component.

This table describes the system requirements for the Endpoint Security MI connection point:

Table 2-8 Endpoint Security MI Connection Point Requirements

Item	Requirement
Operating System	Microsoft Windows 2000 Server (Standard, Enterprise, and Web Edition) – minimum Service Pack 4 Microsoft Windows Server 2003, minimum Service Pack 2
Web Servers	Microsoft Internet Information Server (IIS) IIS 5.0 (MS Windows 2000) IIS 6.0 (MS Windows Server 2003, all variants)
Disk Space (initial)	15 MB
Memory (initial)	512 MB
Network Connectivity	TCP/IP networking Stored Procedure Call access to MIDB HTTP and HTTPS access from MI enabled clients SSL Certificate – Optional
Application	Microsoft .NET 2.0

Endpoint Security MI Directory Scanner (DS)

This table describes the system requirements for the Endpoint Security MI directory scanner:

Table 2-9 Endpoint Security MI Directory Scanner Requirements

Item	Requirement
Operating System	Microsoft Windows 2000 Server (Standard, Enterprise, and Web Edition) – minimum Service Pack 4 Microsoft Windows Server 2003, minimum Service Pack 2
Directory Services	Microsoft Windows 2000 AD, Microsoft Windows Server 2003 AD, 2003 R2 AD, and 2008 AD

Table 2-9 Endpoint Security MI Directory Scanner Requirements

Item	Requirement
Disk Space (initial)	15 MB
Memory (initial)	256 MB
Network Connectivity	TCP/IP networking Stored Procedure Call access to MIDB Access to Directory Service host system (LDAP)

Endpoint Security MI Management Console (MIMC)

This table describes the system requirements for the Endpoint Security MI management console:

Table 2-10 Endpoint Security MI Management Console Requirements

Item	Requirement
Operating System	Microsoft Windows Vista Enterprise Edition Microsoft Windows XP Professional SP 2 or higher Microsoft Windows 2000 Server, minimum Service Pack 4 Microsoft Windows Server 2003, minimum Service Pack 2
Disk Space (initial)	15 MB
Memory (initial)	128 MB
Network Connectivity	TCP/IP networking Stored Procedure Call access to MIDB
Terminal Server	MIMC can be used over Terminal Services. Only one instance at the same time can run if the logged in Windows user has permission view/list running processes in the system. If the user does not have this permission, several instances can be run. Hence several users can use the MIMC on one Terminal Server.
Application	Microsoft .NET 2.0

Endpoint Security MI Device Agent

This table describes the system requirements for installing the Endpoint Security MI Device Agents on clients:

Table 2-11 Endpoint Security MI Device Agent Requirements

Item	Requirement
Operating System	Microsoft Windows 2000 Professional SP 4 or later, or Microsoft Windows XP Professional, SP 2, or Microsoft Windows XP Tablet PC Edition, or Microsoft Windows 2000 Server, or Windows 2003 Server, minimum Service Pack 2, or Microsoft Windows Vista Enterprise (32-bit and 64-bit)

Endpoint Security webRH 2.4 HFA 2

The following sections document the server and system administrator requirements and recommendations for installing Endpoint Security webRH.

Rights Required to Install Endpoint Security webRH

The user account used to install the Endpoint Security webRH SQL database must be member of a group with the right to create a database. By default the local system administrator account has this right.

The user account used to install Endpoint Security webRH on the web server should have local administrative rights in order to access the database, install files, modify the registry and assign rights locally. A domain account for the ComPlus application must be dedicated to Endpoint Security webRH.

msvcr71.dll File Required in System32 Folder

The Microsoft file `msvcr71.dll` must be present in the System32 folder on the machine where Endpoint Security webRH is to be installed. If it is not, find the `msvcr71.dll` file on the machine and copy it to the System32 folder.

Server Requirements

These are the server requirements for Endpoint Security webRH R72:

The IIS Server:

- Microsoft Windows 2000 Server with service pack 4 together with Internet Information Server (IIS) 5 and the latest IIS security hot fixes installed or
- Microsoft Windows 2003 Web Edition with service pack 1 together with IIS 6 and the latest IIS security hot fixes installed.



Note - We recommend that you remove as many server headers as possible from the IIS server configuration.

- An SSL certificate for IIS. For security reasons, we strongly recommend that you run SSL 3.0 on the IIS server.

The SQL Database Server:

- The following versions of Microsoft SQL Server:
 - MS SQL 2000 Standard SP3+
 - MS SQL 2000 Enterprise SP3+



Note - For SQL Server 2000, you must use Auto Identity range management of SQL Server 2000 or use GUIDs as identifiers in a replicated SQL Server environment. However, if SQL Servers are used as master and slave setup, this is not relevant.

- MS SQL 2005 Standard
- MS SQL 2005 Enterprise
- MS SQL 2005 Express
- We do not currently support Desktop, MSDE, or Developer editions.
- 20 MB of free disk space on the server
- See also Microsoft TechNet at <http://www.microsoft.com/technet>.



Note - You may also want to check your product documentation for dependency requirements depending on your SQL server version.

Database Replication

If the webRH database is going to be used for replication, please read this information.

This information is relevant only if the databases set up for synchronization are going to be merged at each synchronization event. It is not relevant if the databases are going to be set up as master and slave and all changes are being made at master.

When setting up database replication for Endpoint Security webRH, the master database must distribute identity ranges to the other databases to avoid collisions of identity values.

The reason for this is that Endpoint Security webRH utilizes identity columns as primary keys on some tables in the database.

When setting up identity ranges and scheduling database merges make sure that the ranges are large enough so that there is no chance that one database will run out of identity values between two merges with the master database.

Administrator and Helpdesk Staff Requirements

These are the requirements for Endpoint Security webRH users:

- Microsoft Internet Explorer 4.01 and higher or Mozilla Firefox 2.0 or higher
- Dynamic tokens or fixed passwords for login authentication.

Virtual Systems

Endpoint Security webRH is supported on VMware.

Endpoint Security Media Encryption

Disk and Memory Space

This table presents the minimum hardware requirements for the Media Encryption Server.

Table 2-12 Media Encryption Server system requirements

Item	Description
Disk and memory space	30 MB+

Endpoint Security License Server and Reporting Tool

This table presents the minimum hardware requirements for the License Server.

Table 2-13 License Server system requirements

Item	Description
CPU	Pentium III 450 MHz
Disk Space	300 MB
RAM	512 MB
Network Interface	1

System Requirements for Clients

Besides being available on the Check Point Download Center, the client is also on CD1.

Required Software

- Check Point License for version to install
- Microsoft Installer support

For all the Endpoint Security products:

Required Minimum Hardware

- 512 MB RAM (depending on the scanning load)
- 1 GB Disk Space

Supported Operating Systems for Clients

The Client is supported on:

- Microsoft Windows Vista 32-bit (Enterprise/Business SP1 and later)
- Microsoft Windows Vista 64-bit
- Microsoft Windows XP SP2 and later
- VMware ESX 3.5

Memory (RAM) and Disk Space Requirements per Client

Endpoint Security VPN (Endpoint Connect)

Table 2-14 Memory and Disk Space Requirements for Endpoint Security VPN (Current)

RAM	Disk Space
256 MB	40 MB

Endpoint Security VPN Legacy (SecureClient)

Table 2-15 Memory and Disk Space Requirements for Endpoint Security VPN (Legacy)

RAM	Disk Space
256 MB	40 MB

Endpoint Security Firewall

The Endpoint Security Firewall component includes the following:

- **Anti-virus/spyware**
- **WebCheck**
- **Program Control**
- **E-mail Protection**
- **Policies**
- **Alerts & Logs**

Table 2-16 Memory and Disk Space Requirements for Endpoint Security Firewall

RAM	Disk Space
500MB	500MB

Endpoint Security Full Disk Encryption for Windows

Table 2-17 Hardware, Memory, and Disk Space Requirements for Endpoint Security Full Disk Encryption for Windows

Hardware	RAM	Disk Space
Pentium III 450 MHz	500 MB	300 MB

Additional Operating Systems Supported

Note that, besides the operating systems listed above for all clients, Full Disk Encryption for Windows also supports Microsoft Windows XP Tablet PC Edition SP2, SP3 (SP3 recommended).

Other Systems Required

Microsoft .NET Framework 2.0 or later is required to use the Full Disk Encryption Management Console (FDEMC). If, however, the PCMC will not be used on a machine, you do not need to install .NET on that machine.

Tablet PCs That Support Touch-Pen Logon in Preboot:

Full Disk Encryption supports preboot authentication with touch pens on the following tablet PCs:

- HP TC1100
- HP TC4200
- IBM X41
- Toshiba Portégé M200
- Toshiba Portégé M400
- Motion Computing LS800
- Motion Computing LS1600
- Motion Computing LS1700
- Motion Computing C5
- AMTek Smart Caddie SCA0

Endpoint Security Full Disk Encryption for Mac

Table 2-18 Hardware, Memory, and Disk Space Requirements for Endpoint Security Full Disk Encryption for Mac

Hardware	RAM	Disk Space
Intel-based Macintosh computers	512 MB	50 MB inside file system, where Full Disk Encryption for Mac is installed. Note: <ul style="list-style-type: none"> • The disk encryption process does not require extra space on the hard disk. • A file share for central management repository (used for central storage of profiles and recovery files) is required. • A new partition (32MB) is created automatically in an existing area specified by Apple for preboot purposes.

Supported Operating Systems

- Mac OS 10.4.5 - 10.4.11, 10.5.x

Account Requirements

To install or uninstall Full Disk Encryption for Mac, you will be prompted for your password. This is because the user account executing the action must be authorized to perform certain steps of the installation. In cases in which a separate administrator account has been created, you will be asked for the password for that account.

Endpoint Security Media Encryption

Table 2-19 Memory and Disk Space Requirements for Endpoint Security Media Encryption

RAM	Disk Space
500 MB	300 MB

Upgrading to Endpoint Security R72

The Deployment Utility automatically upgrades previously installed versions of the Endpoint Security components of the versions listed in this section.

Supported Versions for Upgrade:

- Endpoint Security R70 and R71
- Integrity Client 6 and 6.5, Secure Access 7.0 and 7.2 (includes all HFAs of each version)
- Pointsec for PC 4.1 (sr 2.14 and later), 4.2 (sr 1.4 and later), 4.3, 5.x, 6.x, Full Disk Encryption 7.0
- Pointsec Protector version 4.51 and higher
- MI version prior to MI 3.2.1 HFA3



Note - Upgrade directly from Full Disk Encryption 6.0 (Pointsec for PC 6.0.0) is not supported. See the *Full Disk Encryption Administrator's Guide* for details.

Installing Endpoint Security Server and webRH on Same Machine

To install Endpoint Security server and Endpoint Security webRH on the same machine, the following procedure is necessary for correct functionality.

1. Install Endpoint Security server.
2. Install Endpoint Security webRH.
3. Stop CP Apache service.
4. Stop IIS service, HTTPS, and World Wide Web.
5. Log onto IIS and under Default Site (or the site WEbRH is installed on), right-click and choose Properties. Change the HTTP and SSL ports to be other than default.
Do **NOT** start the IIS service yet.
6. Start CP Apache service. Verify you have access to Endpoint Security server.
7. Start IIS service.

To access webRH, use one of the following:

- <https://<servername>:<SSL IPaddress>/webrh/logon.asp>
- <http://<servername>:<HTTP IPaddress>/webrh/logon.asp>

Resolved Issues



Note - The R72 Resolved Issues can be found in [sk41771](http://supportcontent.checkpoint.com/solutions?id=sk41771) at:
<http://supportcontent.checkpoint.com/solutions?id=sk41771>

Known Limitations



Note - The R72 Known Limitations can be found in [sk37659](http://supportcontent.checkpoint.com/solutions?id=sk37659) at:
<http://supportcontent.checkpoint.com/solutions?id=sk37659>

www.checkpoint.com

Worldwide Headquarters

Check Point Software Technologies, Ltd.
5 Ha'Soleim 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.