



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

# **R70.30**

## **Release Notes**

## More Information

The latest version of this document is at:

[http://supportcontent.checkpoint.com/documentation\\_download?ID=10694](http://supportcontent.checkpoint.com/documentation_download?ID=10694)

For additional technical information about Check Point visit Check Point Support Center

(<http://supportcenter.checkpoint.com>).

## Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to us ([mailto:cp\\_techpub\\_feedback@checkpoint.com?subject=Feedback on R70.30 Release Notes](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R70.30 Release Notes)).

### © 2010 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:

Please refer to our Copyright page (<http://www.checkpoint.com/copyright.html>) for a list of our trademarks.

Please refer to our Third Party copyright notices ([http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html)) for a list of relevant copyrights.

# Contents

---

<b>Introduction</b> .....	<b>4</b>
<b>What's New in R70.30</b> .....	<b>4</b>
<b>Platform Provisions and Requirements</b> .....	<b>5</b>
Build Numbers.....	5
Supported Security Products by Platform .....	6
Supported Management Clients by Platform.....	7
Supported Appliances .....	7
Minimum System Requirements .....	9
Supported Upgrade Paths .....	9
Previous Releases Included in R70.30 .....	9
Required Disk Space.....	9
<b>Known Limitations and Resolved Issues</b> .....	<b>10</b>
Resolved Issues .....	10

# Introduction

Thank you for updating to R70.30. This release is a recommended update that contains new features and resolves various issues for the Check Point Suite.

Please read this document carefully before installing R70.30.

For installation instructions, see the *R70.30 Installation and Upgrade Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10658](http://supportcontent.checkpoint.com/documentation_download?ID=10658))

## What's New in R70.30

The following features have been added or enhanced in R70.30:

- Non-English regional formats are now supported in the map visualization features of SmartDashboard, IPS Event Analysis and Eventia Analyzer.
- SmartWorkflow reports can now be viewed in Windows 7.
- It is now possible to use the SSL Network Extender client to access internal resources behind the Security Gateway, using a client digital certificate that is signed by a subordinate CA. The certificate need not be directly signed by a trusted CA. For example, the certificate can be signed by a CA that belongs to the organization itself, which is in turn signed by a trusted root CA.

# Platform Provisions and Requirements

In This Section

<a href="#">Build Numbers</a>	5
<a href="#">Supported Security Products by Platform</a>	6
<a href="#">Supported Management Clients by Platform</a>	7
<a href="#">Supported Appliances</a>	7
<a href="#">Minimum System Requirements</a>	9
<a href="#">Supported Upgrade Paths</a>	9
<a href="#">Previous Releases Included in R70.30</a>	9
<a href="#">Required Disk Space</a>	9

## Build Numbers

The following table lists the R70.30 software products available in this release, and their build numbers. To verify each product's build number, use the given command format or direction within the GUI.

Take 40 of R70.30 consists of the following builds:

Software Blade / Product	Build No.	Verifying Build No.
Security Gateway	730630008	fw ver This is Check Point VPN-1(TM) & FireWall-1(R) R70.30 - Build 008
Security Management	730625002	fwm ver This is Check Point Security Management Server R70.30 - Build 002  Installed Plug-ins: Workflow Blade, IPS Event Analysis Blade
SmartConsole Applications	730630016	Help > About Check Point <Product> R70.30 (Build 730630016)
Provider-1 Multi-Domain Server (MDS)	730630006	fwm mds ver This is Check Point Provider-1 Server R70.30 - Build 006
Provider-1 Multi-Domain GUI (MDG)	730630004	Help > About Check Point Provider-1 R70.30 (Build 730630004)
SecurePlatform	730630004	splat_ver 730630004

# Supported Security Products by Platform

## Supported Security Gateway and Security Management Software Blades

Software Blade	Platform and Operating System							
	Check Point			Windows		Linux	Crossbeam	Solaris
	Secure Platform	IPSO 6.2 Disk-based	IPSO 6.2 Flash-based	Server 2003 (SP1-2) 32bit	Server 2008 (SP1-2) 32bit	RHEL 5.0 kernel 2.6.18	X-series	Ultra-SPARC 8, 9, 10
<b>Security Gateway Software Blades</b>								
Firewall	+	+	+	+	+		+	
IPSec VPN	+	+	+	+	+		+	
IPS	+	+	+	+	+		+	
Anti-Virus & Anti-Malware	+	+	+	+	+		+	
URL Filtering	+							
Anti-Spam & Email Security	+							
Web Security	+	+	+	+	+		+	
Advanced Networking	+	+	+					
Acceleration & Clustering (1)	+	+	+				+ (2)	
<b>Security Management Software Blades</b>								
Network Policy Management	+	+		+	+	+		+
Endpoint Policy Management	+			+	+	+		
Logging & Status	+	+		+	+	+		+
Monitoring	+	+		+	+	+		+
SmartProvisioning	+	+		+	+	+		+
Management Portal	+			+	+	+		+
User Directory	+	+		+	+	+		+
SmartWorkflow	+			+	+	+		+
SmartEvent	+			+	+	+		+

**Note -**

(1) The maximum number of supported cluster members in ClusterXL mode is five; in third-party mode the maximum is eight.

(2) Only third-party clustering

**Provider-1 Support**

Product	Platform and Operating System							
	Check Point			Windows		Linux	Crossbeam	Solaris
	Secure Platform	IPSO 6.2 Disk-based	IPSO 6.2 Flash-based	Server 2003 (SP1-2) 32bit	Server 2008 (SP1-2) 32bit	RHEL 5.0 kernel 2.6.18	X-series	Ultra-SPARC 8, 9, 10
Provider-1 Server (MDS)	+					+		+

# Supported Management Clients by Platform

Check Point Product	Microsoft Windows				
	XP Home & Pro (SP3)	Server 2003 (SP1-2)	Vista (SP1) 32-bit	Server 2008 (SP1)	Windows 7 Ultimate & Enterprise 32-bit
SmartConsole	+	+	+	+	+ (except Eventia Analyzer, Eventia Reporter, and IPS Event Analysis)
Provider-1 MDG	+	+	+	+	+

# Supported Appliances

Appliance Name	Security Management Server	Provider-1 MDS	Security Gateway
Smart-1	+ (Only models 5, 25, 50)	+ (Only models 50, 150)	
Power-1			+
UTM-1	+ *		+ *
IP Series Disk-based	+		+
IP Series Flash-Based			+



**Note** -Event Correlation and IPS Event Analysis Software Blades are supported on UTM-130 and UTM-270, however, they require a different installation package. See sk44125 (<http://supportcontent.checkpoint.com/solutions?id=sk44125>) for details.

# Minimum System Requirements

The system requirements for R70.30 are the same as for R70. See the R70 Release Notes ([http://supportcontent.checkpoint.com/documentation\\_download?ID=8712](http://supportcontent.checkpoint.com/documentation_download?ID=8712)) for more information.

## Supported Upgrade Paths

R70.30 can be installed **only** on top of R70, R70.1 or R70.20 Security Gateways, Security Management servers, and Provider-1 MDSs. You must upgrade to R70, R70.1 or R70.20 before using this release.

Customers with R70.30 EA can also upgrade to R70.30.



**Note** - R70.30 gateways can be managed **only** by R70.20 (or higher) Management Servers.

## Previous Releases Included in R70.30

This release include all features and fixes that were included in R70.20, R70.1 and R65 HFA 60. For more information, see:

- R70.20 Home Page sk43168 (<http://supportcontent.checkpoint.com/solutions?id=sk43168>)
- R70.1 Home Page sk41810 (<http://supportcontent.checkpoint.com/solutions?id=sk41810>)
- VPN-1 NGX R65 HFA 60 Release Notes ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10306](http://supportcontent.checkpoint.com/documentation_download?ID=10306))
- Provider-1 NGX R65 HFA 60 Release Notes ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10307](http://supportcontent.checkpoint.com/documentation_download?ID=10307))

## Required Disk Space



**Note** - It is safe to delete the downloaded .tgz file after it is extracted in order to allow more disk space for installation.

### Required Disk Space for Installation on a Security Management Server or MDS

Operating System	Packed and Extracted .tgz File	Installation Size	Total Space Required
SecurePlatform	/var - 900 MB	root - 200 MB /opt - 600 MB /var - 400 MB	root - 200 MB /opt - 600 MB /var - 1300 MB
IPSO	/opt - 400 MB	/opt - 200 MB	/opt - 600 MB
Linux	800 MB	1000 MB	1800 MB
Windows	500 MB	900 MB	1400 MB
Solaris	700 MB	400 MB	1100 MB

## Required Disk Space for Installation on a Security Gateway

Operating System	Packed and Extracted .tgz File	Installation Size	Total Space Required
SecurePlatform	/var - 800 MB	root - 150 MB /opt - 400 MB /var - 200 MB	root - 200 MB /opt - 400 MB /var - 1000 MB
IPSO	/var - 400 MB	/opt - 200 MB /var - 100 MB	/opt - 200 MB /var - 500 MB
IPSO Diskless	/var - 300 MB	/opt - 300 MB /preserve - 300 MB	/var - 300 MB /opt - 300 MB /preserve - 300 MB
Windows	500MB	400 MB	800 MB

# Known Limitations and Resolved Issues

Known Limitations for R70.20 (<http://supportcontent.checkpoint.com/solutions?id=sk43166>) also apply to R70.30.

## Resolved Issues

Issues resolved in this release are as follows:

ID	symptoms	Install On
<b>IPS</b>		
00532753, 00532685, 00532802	The Security Gateway correctly handles CIFS traffic when CIFS IPS protections are enabled.	Gateway
<b>SmartConsole Applications</b>		
00533995	The map visualization features in SmartDashboard, IPS Event Analysis and Eventia Analyzer now correctly handle non-English regional formats.	SmartConsole client
00530309, 00530285, 00530311	SmartWorkflow reports can now be viewed in Windows 7	SmartConsole client
<b>Authentication</b>		
00533840, 00502016	It is now possible to authenticate with SSL Network Extender to a Security Gateway, using a digital certificate which is not directly signed by a trusted CA.	Gateway

ID	symptoms	Install On
<b>SmartWorkflow</b>		
00536155 00534033	SmartWorkflow reports now correctly identify two connections as belonging to the same SmartWorkflow session even if the first session used the IP address and the second used the DNS address.	SmartConsole client
<b>SIC</b>		
00531275, 00496700, 00530812, 00531120, 00531121, 00531183	<p>The automatic SIC (Secure Internal Communication) renewal mechanism does not function correctly in R70 releases prior to R70.30. One of the symptoms of this issue is that SIC communication between Security Management server and Security Gateway fails. The earliest possible date this issue can arise is 15 months after installation of R70/R70.1/R70.20 - no earlier than May 2010.</p> <p>For upgraded environment this problem can happen only when both of the following conditions are met:</p> <ul style="list-style-type: none"> <li>• Five years passed from the initial installation of NGX R60-R65 on the Security Gateway.</li> </ul> <p>AND</p> <ul style="list-style-type: none"> <li>• The Security Gateway was upgraded by way of an in-place upgrade of R70/R70.1/R70.20.</li> </ul> <p>For new R70/R70.1/R70.20 installation this problem can happen in 5 years.</p> <p>To find if this issue is relevant for you, check the expiration date of your SIC certificates by using the procedure in SecureKnowledge solution sk43744 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk43744">http://supportcontent.checkpoint.com/solutions?id=sk43744</a>)</p> <p>The solution to this problem is to renew all certificates that are within a year of expiration. Do this by installing R70.30. For other solutions, and for more information, see SecureKnowledge solution sk43744.</p>	Security management and Gateway
<b>VoIP</b>		
00531217, 00531197, 00537915	A memory leak that intermittently prevented customers seeing streaming media via iNATed RTSP traffic has been resolved.	Gateway
<b>Traffic Monitoring</b>		
00535515, 00378428, 00519047, 00374261, 00534790, 00534791, 00535501, 00537852, 00345084, 00345243, 00406751, 00422613, 00184399	The Security Gateway now correctly handles very high traffic loads for SmartView Monitor.	Gateway
<b>Clustering</b>		
00529913, 00529256, 00529915	Pinging the cluster virtual IP address (VIP) from a cluster member in standby state now results in a response.	Gateway

