



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

VPN-1

NGX R65 HFA 60

Release Notes

More Information

To view the latest version of this document, see the User Center (http://supportcontent.checkpoint.com/documentation_download?ID=10306).

For additional technical information about Check Point visit Check Point Support Center (<http://support.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 VPN-1 NGX R65 HFA 60 Release Notes).

© 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:

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) for a list of relevant copyrights.

Contents

Introduction	4
What's New	4
Known Limitations	5
SecurePlatform	5
SecurePlatform Web User Interface	6
IPSO	6
Windows	6
VPN-1 Edge/Embedded	6
Database Revisions	7
Endpoint Connect	7
Connectra	7
Eventia Analyzer and Reporting Server	7
ClusterXL	8
Supported Versions, Platforms, and Builds	9
Supported Platforms	9
Supported Products	10
Supported Builds	10
Supported Builds History	11
Installation	12
Required Disk Space	12
Installing with SecurePlatform WebUI - Appliance and Open Server	13
Verifying Installation with SecurePlatform Web User Interface	13
Installing on SecurePlatform Open Server	13
Installing on Solaris, Linux, and IPSO Disk-Based	14
Installing on IPSO Flash-Based	14
Installing on Windows	15
Installing with SmartUpdate	15
Updating Customized INSPECT Files	15
Installing HFA on Clusters	16
Uninstallation	17
Important Notes	17
Uninstalling with SecurePlatform Web User Interface	17
Uninstalling with Command Line	18
Uninstalling with SmartUpdate	18
Uninstalling from Windows	18
Post-Uninstall Notes	18
Resolved Issues in NGX R65 HFA 60	19
Anti-virus	19
Eventia Reporter/Analyzer	20
Firewall	20
Management	24
Performance Pack	25
SmartDefense	25
SSL Network Extender	26
VoIP	26
VPN	26
Platform Specific	27
Miscellaneous	28

Introduction

Thank you for updating your Check Point products with VPN-1 NGX R65 HFA 60 (Hotfix Accumulator). This HFA is a recommended update that resolves various issues and contains improvements for VPN-1 and other Check Point products on a variety of platforms.

Please read this document carefully prior to installing this HFA. We also recommend that you refer to the appropriate Check Point user documentation and release notes, which contain hardware requirements, software requirements, and version recommendations.

What's New

Highlights of NGX R65 HFA 60 include the following.

- New support for an unlimited number of packages to be installed using SmartUpdate.
- New comprehensive protection against the sockstress vulnerability.
- Improved license handling for various issues and platforms.
- Improved ftp command parsing.
- Eventia Reporter has enhanced support for log servers with long names.
- Enhanced firewall control of large SCCP packets and large Connections tables.
- Improved certificate handling with NAT.
- Improved Anti-virus for web page loading.

Known Limitations

In this Section

SecurePlatform	5
SecurePlatform Web User Interface	6
IPSO	6
Windows	6
VPN-1 Edge/Embedded	6
Database Revisions	7
Endpoint Connect	7
Connectra	7
Eventia Analyzer and Reporting Server	7
ClusterXL	8

SecurePlatform

ID	Description
	<p>After installing Check_Point_NGX_R65_HFA_60.linux.tgz (http://supportcontent.checkpoint.com/file_download?id=10349) that contains a number of packages on a SecurePlatform, the HFA package named SecurePlatform (for the Operating System) cannot be uninstalled.</p> <p>Check Point SecurePlatform NGX (R65) HFA 60 will be displayed after uninstal.</p> <p>Make sure to read the notes about important steps to do after uninstalling ("Post-Uninstall Notes" on page 18).</p>
00466648	<p>Uninstalling NGX R65 HFA 60 from SecurePlatform 2.6 is not supported as it may cause system instability. Before installing NGX R65 HFA 60 on SecurePlatform 2.6, make sure to take a snapshot of the entire system to enable reverting to the previous state if needed. For details refer to sk42329 (http://supportcontent.checkpoint.com/solutions?id=sk42329).</p>
	<p>SecurePlatform 2.6: Check Point NGX R65.4 is not supported for installation on top of NGX R65 HFA 60 running on SecurePlatform 2.6.</p>
	<p>SecurePlatform 2.4: On SecurePlatform Pro 2.4, stand-alone architecture (with the SmartCenter server and Gateway installed on the same machine), with Advanced Routing, the installation of NGX R65.4 on top of NGX R65 HFA 60 overwrites the Advanced Routing installation to build 62064001 (included in HFA_40).</p> <p>To complete installation of NGX R65.4 on top of NGX R65 HFA 60:</p> <ul style="list-style-type: none"> Download and unpack HFA 60: <code>tar zxvf Check_Point_NGX_R65_HFA_60.linux.tgz</code> Go to the Advanced Routing directory: <code>cd hotfixes/dr_splat/</code> Unpack the dr_splat package: <code>tar zxvf dr_splat_R65_HFA.tgz</code> Install the package: <code>./dr_splat_HOTFIX_R65_60_620660005_1 -FORCED</code> Follow the installation instructions.

SecurePlatform Web User Interface

ID	Description
00435874	When using SecurePlatform Web User Interface to restore a machine from a snapshot with a path name that has spaces, the restore will fail on error: "Filename must not contain spaces." Workaround: Restore the machine from a path name that has no spaces.
00520229	When upgrading with the Web User Interface, if snapshot is enabled, you must close all GUI applications before the snapshot can start.

IPSO

ID	Description
	Installation of this HFA by Voyager is not supported.
	After installing this HFA on IPSO Flash-based platforms, the installation log files are automatically deleted after reboot.
	Installing and uninstalling this HFA from IPSO gateways using SmartUpdate, or from IPSO Flash-based platforms, is not supported.
	IPSO version 6 is not supported.

Windows

ID	Description
00194720	Using SmartUpdate to uninstall this HFA from Windows gateways requires a manual reboot of the gateway.
	To install this HFA on Windows gateways using SmartUpdate, a previous HFA must have been installed on the gateway via CLI.
00520349 00520346	R65.4 installation on top of HFA 50 or above is blocked. For a workaround, see sk42965 (sk42965 - http://supportcontent.checkpoint.com/solutions?id=sk42965). Uninstallation of both R65.4 and this HFA is not supported.

VPN-1 Edge/Embedded

ID	Description
00437851	Installing a policy on a large number of VPN-1 UTM Edge devices managed from SmartDashboard may not succeed. Workaround: Install the policy on Edge devices in several batches.
00522831	During HFA installation, all INSPECT files related to the UTM-1 Edge compatibility package (located at <code>/opt/CPEdgecmp-R65/libsw/</code>) are overwritten. Any manual changes made on these files will be lost. For details see: sk43158 https://supportcontent.checkpoint.com/solutions?id=sk43158

Database Revisions

ID	Description
00432491	A database version created with the Policy Revision Control cannot be viewed or restored if the list of currently installed plug-ins is different from when the Revision Control version was created.

Endpoint Connect

ID	Description
00416341	When using Smart Card certificate authentication, renewal of certificates that were enrolled to the Smart Card is not supported. Note: Renewal from the local (CAPI) store is supported.
00434786	Endpoint Connect requires MSXML3.dll on Windows 2000 SP4. This dll can be obtained from Windows Update (Microsoft site). Place it in C:\WINDOWS\System32 .
00426700	If the trac_client_1.ttm file should be edited on a Windows platform, it must be done in Notepad; Wordpad will corrupt the file.
00434083	Connecting from two different machines to the same gateway with the same username is not supported, because they may both get the same Office Mode IP, which would disconnect the first session.

Connectra

ID	Description
	Installation of Connectra NGX R62 Central Management plug-in is not supported on an NGX R65 SmartCenter server with certain other plug-ins. For a list of plug-in compatibility, see (http://www.checkpoint.com/ngx/upgrade/plugin/index.html).

Eventia Analyzer and Reporting Server

ID	Description
00467080	When changing the Database Maintenance configuration from a very large size (20 GB) to a smaller size (2 GB) the cleaning process takes a very long time. Workaround: In Database Maintenance, reduce the DB size gradually from 20 GB to 15 GB, then to 10 GB, and so on.
00519595	After uninstalling this HFA from a machine with Eventia Reporting Server, on which R65 HFA 25 was previously installed, the cpsemd process will not be able to start. Workaround: <ol style="list-style-type: none">1. <code>cpstop</code>2. <code>execute:</code><ul style="list-style-type: none">• Unix: <code>CPRegSvr -p \$RTDIR/lib libCPSet2Sql.so</code>• Windows: <code>CPRegSvr /p "%RTDIR%\lib" CPSet2Sql.dll</code>3. <code>cpstart</code>

ClusterXL

ID	Description
00501854	All interfaces that are not part of the ClusterXL topology should be defined in: \$FWDIR/conf/discntd.if

Supported Versions, Platforms, and Builds

In this Section

Supported Platforms	9
Supported Products	10
Supported Builds	10
Supported Builds History	11

Supported Platforms

The following platforms are supported for VPN-1 NGX R65 HFA 60.

Platform	Version
Power-1	NGX R65 on Power-1 5070 and 9070
UTM-1	NGX R65 on UTM-1 450, 1050, 2050, 130, 270, 570, 1070, 2070, 3070
Smart-1	Models 5, 25 and 50
SecurePlatform	NGX R65 on SecurePlatform 2.4 and 2.6
IPSO 4.2 Platforms	IP150, IP260, IP290, IP350/IP355, IP380/IP385, IP390, IP560, IP690, IP710, IP740, IP1220, IP1260, IP1280, IP2250/2255, IP2450
Windows	2000 Server SP4, 2003 Server, 2003 Server SP1, SP2
Solaris	5.8, 5.9, 5.10
NEC UNIVERGE UnifiedWall	NGX R65 on NEC UNIVERGE UnifiedWall 1000, 2000, 4000
Linux	Red Hat Enterprise Linux 3.0 kernel 2.4



Note - On the IPSO Disk and IPSO Flash-based platforms, IPSO version 6 is not supported.

Supported Products

This HFA may be installed with various Check Point products, but is not supported with CoreXL or IPSO 6.

Check Point NGX R65 Product	Supports R65_HFA_60 Installation?
Check Point NGX R65 GA	YES
HFA 01	YES
HFA 02	YES
HFA 30	YES
HFA 40	YES
HFA 50	YES
Check Point NGX R65.4	YES
with Messaging Security (HFA 25)	YES
with R65 VSX Management Update (and revision 2)	YES
on Power-1/UTM-1 appliances with Messaging Security	YES
with CoreXL	NO
IPSO 6	NO



Note - Before upgrading or uninstalling HFAs on SecurePlatform operating systems, it is highly recommended that you take a snapshot of the machine. For details refer to sk42329 (<http://supportcontent.checkpoint.com/solutions?id=sk42329>).

On Power-1 and UTM-1 appliances, the snapshot file is stored in:

`/var/log/CPsnapshot/snapshots/NGX_R65_/`

On open-servers, the snapshot files is stored in: **`/var/CPsnapshot/snapshots`**

Supported Builds

To verify you have the HFA described in this document: extract the contents of the tgz package you downloaded and open the **take_number.conf** file using a text editor. Verify that it contains: **take_51**.

Take 51 of NGX R65 HFA 60 consists of the following builds:

Component	Build Number	Verify Command and Output
Firewall	620660039	The output of fw ver -k should be similar to: This is Check Point VPN-1(TM) & Firewall(R) NGX (R65) HFA_60, Hotfix 660 - Build 039
SecurePlatform	620660021	

Component	Build Number	Verify Command and Output
Performance Pack	620660007	The output of sim ver -k should be similar to: This is Check Point Performance Pack version: NGX (R65) HFA_60, Hotfix 660 - Build 007
VPN-1 UTM Edge Compatibility	620660006	
Eventia	620660007	The output of SVRServer ver should be similar to: This is Check Point Eventia Reporter Server (TM) NGX (R65) HFA_60, Hotfix 660 - Build 007
Advanced Dynamic Routing for SecurePlatform	620660005	The output of gated_ver is a list of information including: 005

Supported Builds History

	Firewall	Secure-Platform	Performance Pack	Edge Compatibility	Eventia	Advanced Dynamic Routing for Secure-Platform
R65_HFA_50	620650048	620650021	620650016 Solaris: 015	620650004	620650010	620650004
R65_HFA_40	620640091	620640029	620640003	620640008	620640008	620640001
R65_HFA_30	620630049	620630036	620630003	620630018	620630007	
R65_HFA_02	620602008	620602004	620601006	Windows: 620602005 Solaris: 620602007	620601012	
R65_HFA_01	620601019	620601008	620601006	620601004	620601012	

Installation

In this Section

Required Disk Space	12
Installing with SecurePlatform WebUI - Appliance and Open Server	13
Installing on SecurePlatform Open Server	13
Installing on Solaris, Linux, and IPSO Disk-Based	14
Installing on IPSO Flash-Based	14
Installing on Windows	15
Installing with SmartUpdate	15
Updating Customized INSPECT Files	15
Installing HFA on Clusters	16



Note - To install the HFA on Power-1 and UTM-1 appliances, you may use SmartUpdate or the SecurePlatform Web User Interface.

Required Disk Space

The table below shows the amount of free disk space in MB required to download, extract, and install NGX R65 HFA 60.

Platform	To download and extract	To Install
Power-1 UTM-1 Smart-1 SecurePlatform NEC UNIVERGE UnifiedWall	576	/opt = 440 /var = 100 root = 100
IPSO Disk-based	235	/opt = 350 /var = 450
IPSO Flash-based		1000 Refer to: Installing on IPSO Diskless (see " Installing on IPSO Flash-Based " on page 14)
Windows	145	500
Solaris	311	/opt = 530
Linux	576	/opt = 450 /var = 100

Installing with SecurePlatform WebUI - Appliance and Open Server

Use the Web User Interface to install this HFA on Check Point Power-1, UTM-1, Smart-1 appliances, or on open servers running SecurePlatform.

Before installing this HFA on SecurePlatform with Web User Interface, make sure to take a snapshot of the machine.

To install NGX R65 HFA 60 with SecurePlatform Web User Interface:

1. Download the HFA file: Check_Point_NGX_R65_HFA_60.linux.tgz (http://supportcontent.checkpoint.com/file_download?id=10349).
2. Connect to the SecurePlatform Web User Interface:
 - Open server: **https://<IP>**
 - Appliance: **https://<IP>:4434**
3. Open the Upgrade page:
 - Open server: **Device > Upgrade**
 - Appliance: **Appliance > Upgrade**
4. In the **Upgrade Steps** pane, browse to the downloaded HFA.
5. Click the **Upload package** button.
6. In the **Safe Upgrade** step, make sure the **Save a snapshot of the current system** check box is selected.



Important - Be sure that all GUI applications are closed and then to select the option that takes a snapshot of the machine, before installing an HFA.

7. Click **Start Upgrade**.
At the end of the installation, the device automatically reboots.
8. Re-login to the machine.



Important - After upgrading, move the snapshot file from the Desktop to a pathname without spaces. This must be done before attempting to restore the machine.

Verifying Installation with SecurePlatform Web User Interface

To verify NGX R65 HFA 60 installation through the SecurePlatform Web User Interface, make sure that **HFA 60** appears in the Build information, according to the platform type:

- Open server: **Status > Version and Build**
- Power-1 and UTM-1: **Information > Appliance Status > Version and Build**

Installing on SecurePlatform Open Server



Important - The default idle timeout on SecurePlatform is ten minutes. After this time, the user is logged out. To ensure that installation is not interrupted by this timeout, before entering **expert** mode, type: `idle 60` in the command line.

To install this HFA on SecurePlatform open server with CLI:

1. Create a snapshot. Run `snapshot` and go through the options of the CLI snapshot wizard.
2. Create a temporary directory on `/var`: `mkdir /var/hfa`

3. Verify that there is enough free disk space for the installation of the HFA packages.
4. Navigate to the new directory: `cd /var/hfa`
5. Download `Check_Point_NGX_R65_HFA_60.linux.tgz` (http://supportcontent.checkpoint.com/file_download?id=10349) to `/var/hfa`.
6. Extract the packages.
7. Execute: `./UnixInstallScript` and follow the instructions.
8. Reboot the machine after the installation is done.

Installing on Solaris, Linux, and IPSO Disk-Based

To install NGX R65 HFA 60 on Solaris, Linux, or Disk-based IPSO:

1. Create a temporary directory on `/opt`: `mkdir /opt/hfa`
2. Navigate to the new directory: `cd /opt/hfa`
3. Verify that there is enough free disk space for the installation of the HFA packages.
4. Download the HFA file to `/opt/hfa`.
 - Solaris: `Check_Point_NGX_R65_HFA_60.solaris2.tgz` (http://supportcontent.checkpoint.com/file_download?id=10347)
 - Linux: `Check_Point_NGX_R65_HFA_60.linux.tgz` (http://supportcontent.checkpoint.com/file_download?id=10349)
 - IPSO: `Check_Point_NGX_R65_HFA_60.ipso.tgz` (http://supportcontent.checkpoint.com/file_download?id=10346)
5. Extract the contents.
6. Delete the `*.tgz` file to save disk space.
7. Execute: `./UnixInstallScript` and follow on-screen instructions.
8. Reboot the machine.

Installing on IPSO Flash-Based

To install this HFA on IPSO Flash-based platforms, you must follow the steps precisely to avoid installation problems.

To install NGX R65 HFA 60 on IPSO Flash-based:

1. If using 1GB RAM systems, run the following command to extend the `/opt` RAM disk partition:


```
/sbin/mount -u -o extend_partition /dev/null /opt
```

 To verify that the `/opt` partition was extended to at least 500000 KB, run the `df` command.
2. Verify that there is enough free disk space for the installation of the HFA packages:
 - For `/preserve`, you need at least 455000 KB free.

(To find absolute free space: run the `df -k /preserve` command and subtract the 3rd column **Used** from the 2nd column **1K-blocks**).
 - For `/opt` and `/var`, you need at least 382000 KB free.
3. Create a temporary directory on `/opt`: `mkdir /opt/hfa`
4. Navigate to the new directory: `cd /opt/hfa`
5. Download `Check_Point_NGX_R65_HFA_60.ipso.tgz` (http://supportcontent.checkpoint.com/file_download?id=10349) to `/opt/hfa` and extract the contents.
6. Delete the `*.tgz` file to save disk space.
7. Execute: `./UnixInstallScript`
8. Reboot the machine.

Installing on Windows

To install NGX R65 HFA 60 on Windows NGX R65:

1. Verify that there is enough free disk space for the installation of the HFA packages.
2. Download the HFA (http://supportcontent.checkpoint.com/file_download?id=10348).
3. Extract the packages.
4. Run **Setup.bat**
5. Reboot the machine.

Installing with SmartUpdate

You can use SmartUpdate to remotely install this HFA on SecurePlatform (open server or appliance), Solaris, Linux, Windows, and IPSO gateways.

To install with SmartUpdate:

1. Install this HFA on the SmartCenter server, using the Command Line or SecurePlatform Web User Interface.
2. Open SmartUpdate and close SmartDashboard.
3. Click **Packages > Get Data from All**.
When the **Operation Status** of the known gateways is **Done**, the installed packages and their versions are listed.
4. Open the Package Repository: **Packages > View Repository**.
5. Add the HFA file (*.tgz) of each required gateway platform to the Package Repository (**Packages > Add**; or drag-and-drop).

Wait until the **Operation Status** of adding the package is **Done**. The HFA package appears in the Package Repository: **Check Point Suite VPN-1**.

6. Right-click the package and choose **Distribute**.
The Distribute Package window opens.
7. Select the gateways on which you want to install the HFA.
8. Click **Distribute**.

The HFA is distributed to and installed on the selected gateways. The gateways are rebooted automatically; except for Windows gateways, which must be rebooted manually.

Notice in SmartUpdate, the **Minor Version** of the upgraded packages is **R65_60**.



Note - If after installing this HFA on a Windows machine, the gateway does not accept traffic, re-install the policy.

Updating Customized INSPECT Files

The SmartCenter server contains several INSPECT (*.def) files, typically located in the **\$FWDIR/lib** directory. This HFA may include one or more updated INSPECT files, which replace the files currently in use.

For environments using only original Check Point INSPECT files, the updated INSPECT files are installed automatically: the previous *.def files are replaced with the new ones.

If even one INSPECT file was manually customized, none of the new INSPECT files replace the previous ones. The following message appears:

```
The updated inspect files were NOT installed due to signature mismatches or errors.  
To complete the installation replace the inspect files.
```

```
Inspect files that were not replaced may lead to unexpected behavior!
```

```
To force update of the inspect files run: update_inspect_files -f
```

If the files were not replaced (signature mismatch message displayed), you must force the INSPECT files to be updated.



Important - You must replace the previous files. If you do not, unexpected behavior may result.

To force INSPECT files to be updated:

1. Make note of the customized INSPECT files.

To see which INSPECT files were not replaced, see the log:

- Unix - **/opt/CPInstLog/update_inspect_files_60.log**
- Windows - **C:\Program Files\Checkpoint\CPInstLog\update_inspect_files_60.log**

If the files were not replaced because of customizations, the log shows:

<filename>.def was changed by user, signature didn't match!

2. Open the files that are listed in update_inspect_files_60.log and note the customized lines.
3. Run: update_inspect_files -f
The log will show: <filename>.def was replaced.
4. Merge the customized content (that you noted in the previous steps) into the new INSPECT file(s).
5. Re-install the Security Policy to enable the new INSPECT files.

Installing HFA on Clusters

When upgrading from the NGX R65 general release, the following upgrade options are available and explained in the NGX R65 Upgrade Guide

(http://supportcontent.checkpoint.com/documentation_download?ID=7259):

- **Minimal Effort Upgrade** - For more information, refer to the *Minimal Effort Upgrade on a ClusterXL* chapter in the *Upgrade* guide.
- **Zero Down Time Upgrade** - For more information, refer to the *Zero Down Time Upgrade on a ClusterXL Cluster* chapter in the *Upgrade* guide.
- **Full Connectivity Upgrade** – For more information, refer to the *Full Connectivity Upgrade on a ClusterXL Cluster* chapter in the *Upgrade* guide.

Notes:

- When performing a Full Connectivity Upgrade, follow all steps described in the *Full Connectivity Upgrade on a ClusterXL Cluster* chapter in the *Upgrade* guide. This includes running the **fw fcu** command and understanding the relevance of the **Ready** state as described in step 7 of the *Zero Down Time Upgrade on a ClusterXL Cluster* section in the *Upgrade* guide.
- The Full Connectivity Upgrade is not supported when upgrading a cluster from any version prior to NGX. Only Minimal Effort or Zero Down-Time upgrades can be done in this circumstance.
- The maximum number of cluster members that is supported in ClusterXL mode is five; in third-party mode the maximum is eight.

Uninstallation

In this Section

Important Notes	17
Uninstalling with SecurePlatform Web User Interface	17
Uninstalling with Command Line	18
Uninstalling with SmartUpdate	18
Uninstalling from Windows	18
Post-Uninstall Notes	18

Important Notes



After uninstallation, make sure the machine reboots before attempting to run uninstall again. A second uninstall command may cause unexpected behavior.



If uninstalling this HFA from a machine that has the VSX NGX compatibility package, complete uninstallation by running:
`/opt/CPvsxngxcmp-R65/uninstall_den_cmp_HOTFIX_R65_60`

Uninstalling with SecurePlatform Web User Interface

If you are using SecurePlatform Web User Interface only, you may restore the SecurePlatform (open server or appliance), to its state before the HFA installation.



Important - Any database change or configuration definitions will not be preserved. It is recommended that if possible you use the uninstall executable from the command line.

To restore SecurePlatform, UTM-1, or Power-1 to pre-HFA state:

1. Connect to the SecurePlatform Web User Interface:
 - Open server: `https://<IP>`
 - Power-1 and UTM-1: `https://<IP>:4434`
2. Open the Image Management page:
 - Open server: **Device > Image Management**
 - Power-1 and UTM-1: **Appliance > Image Management**
3. In the **Available Images** pane, find the relevant image.
4. Click **Revert** and then **Apply**.
5. In the message, click **Yes**.
The device automatically reboots.
6. Reconnect.

Uninstalling with Command Line

This procedure should be used for uninstalling the HFA from IPSO, Solaris, Linux, or SecurePlatform open servers (not including appliances and SecurePlatform 2.6).

To uninstall this HFA with command line:

1. Navigate to `/opt/CPUninstall/R65_HFA_60/`
2. Execute `UnixInstallScript -u`
3. Reboot the machine.



Note - On SecurePlatform, if you reboot the machine from `/opt/CPUninstall/R65_HFA_60` an error message appears that can be ignored.

Uninstalling with SmartUpdate

You can use SmartUpdate to remotely uninstall this HFA on gateways of all platforms, except IPSO.

To uninstall with SmartUpdate:

1. Make sure SmartDashboard is closed.
2. Open SmartUpdate.
3. From the **Packages** menu choose **Get Data From All**.
4. Right-click each package with **Minor_Version** value of **R65_60** and choose **Uninstall** in the following order:
 - **VPN-1 Power/UTM**
 - **Performance Pack** (for SecurePlatform and Solaris gateways, if installed)



Note - All packages must be uninstalled except for the SecurePlatform package that cannot be uninstalled from SecurePlatform gateways.

5. On Windows platforms, reboot manually.

Uninstalling from Windows

To uninstall NGX R65 HFA 60 from Windows:

1. Go to: `C:\Program Files\CheckPoint\CPUninstall\R65_HFA_60`
2. Run: `Setup.bat -u`
3. Reboot the machine.

Post-Uninstall Notes

After uninstalling this HFA from a management server machine which had plug-ins installed, you may find that policy installation is not functioning correctly. To fix this issue, execute: `plugin_reset`

After uninstalling this HFA from a SecurePlatform machine, the login prompt may still display `Check Point SecurePlatform NGX (R65) HFA 60` as the installed version, because the SecurePlatform package was not uninstalled. Use the `fw ver` command to see the current version.

Resolved Issues in NGX R65 HFA 60

In this Section

Anti-virus	19
Eventia Reporter/Analyzer	20
Firewall	20
Management	24
Performance Pack	25
SmartDefense	25
SSL Network Extender	26
VoIP	26
VPN	26
Platform Specific	27
Miscellaneous	28

Installing this HFA provides performance enhancements and functionality fixes to Check Point Suite NGX R65. It includes fixes of previous NGX R65 HFAs. A complete list of resolved issues in NGX R65 and previous HFA versions is in sk42318 (<http://supportcontent.checkpoint.com/solutions?id=sk42318>).



Note - The number associated with each issue is the tracking number in Check Point's internal database. Reference this number if you contact Check Point about an item.

If you have previously installed a hotfix provided by Check Point, search for the tracking number of the hotfix (not to be confused with the build number) in this document. If your hotfix is not included in this HFA (or if you do not have the number of the hotfix), contact Check Point before installing this HFA - if your hotfix is not included in the HFA, installing the HFA may overwrite the hotfix.

Anti-virus

ID	Description	Install On
00445265 00444823 00466238 00466240	Anti-virus, with HTML file type set to Pass, has been improved to ensure that sites using http 1.1 (chunked headers) function properly.	Gateway
00442634 00442431 00495461 00502525 00503182 00467069	Improved license handling, to resolve an issue that occurred with multiple licenses, when one enabled Anti-virus and another did not.	SmartCenter server

Eventia Reporter/Analyzer

ID	Description	Install On
00495737 00494981 00495741	Eventia Analyzer. Improved object attribute handling fixes an error that caused the "syslog -r" command to fail on certain objects.	Eventia Log server
00496458 00426047 00495927 00496459	Eventia Reporter. Improved file handling enables large tables (greater than 2.5GB) to be re-imported.	Eventia Reporter
00495785 00494733 00495788 00504736	Eventia Reporter. Improved handling of MIME connections enables reports to be emailed with IronMail.	Eventia Reporter server
00495468 00494814	Eventia Reporter. Added support for long (more than 22 characters) name for log servers, resolving an issue that blocked the cpWatchDog process from starting.	Gateway

Firewall

ID	Description	Install On
00445961 00443248 00467022 00445963 00446664 00493483 00494114 00503420	Enhancements to CPD process fixed memory leak.	SmartCenter server and Gateway
00450170 00449637 00496799	Gateways now correctly pass SIP packets that contain a tag string within the URI (for example: sip:datagateway.com;tag=193442)	Gateway
00463395 00447015 00496407	The Log Forwarding Mechanism has been improved, fixing a memory leak in the FWD process.	Gateway

ID	Description	Install On
00443980 00114058 00201616 00202511 00213339 00213308 00424180 00445418	When using HTTP Security server, while the firewall is the proxy server, the DNS timeout cache is now correctly set to five minutes. Refer to sk22953 (http://supportcontent.checkpoint.com/solutions?id=sk22953).	Gateway
00466875 00463844 00466878	Improved ftp command parsing. Refer to sk36267 (http://supportcontent.checkpoint.com/solutions?id=sk36267)	Gateway
00374058 00372921 00374056 00374057 00374059 00376382 00420715 00442128 00449393	New kernel parameters for enhanced control of SCCP packets. This fixes an error that was seen when SCCP packets of larger than 1000 bytes were sent: "Malformed SCCP packet - message length exceeds the limit of 1KByte". To change the limit of the packet size, set the sk_len_limit kernel parameter to the relevant value.	Gateway
00438719 00438125 00466062 00467056 00499646	With an FTP Security server (when a rule uses ftp resource, or Anti-virus for ftp), the firewall consistently opens the data connection to the FTP client on port 20.	Gateway
00448962 00447240	H.323 traffic is now passed correctly; fixed "Malformed H.225 message" error.	Gateway
00442822 00441870 00496981	UDP packets with IP option of type NOP or EOL are dropped by firewall, by design. (Drop error: "options not approved"). This HFA provides a new kernel parameter, allowing you to change the behavior of the firewall, to pass these packets. To enable UDP packets with NOP and EOL IP options to pass, change the value of the asm_allow_ipopt_on_udp kernel parameter to 1.	Gateway
00496465 00172047 00179881 00214588 00376982 00433918 00496466	Improved performance of firewall on Crossbeam by enabling logs to be held locally, rather than transferred to a flash filesystem that is not always accessible.	Gateway

ID	Description	Install On
00495714 00345195 00348690 00350188 00350355 00428682 00431338 00495776 00445402	Improved clustering with Clientless VPN to provide proper functionality for environments that upgrade to NGX R65.	Gateway
00494698 00493702 00494701 00494699 00494700 00494703	Improved handling of server list, to ensure that new Log Servers can be added without adversely affecting the fwd process.	Gateway
00450113 00449986 00493494	Retrieving interface information through cpstat now provides the MAC address.	Gateway
00415147 00412518 00415145 00420694 00423641 00423378 00426633 00426672	Japanese character URIs (containing shift_jis encoding) are now correctly recognized; they are no longer falsely detected as command injections.	Gateway
00416546 00416191 00434917 00435662 00416547 00416548 00421889 00497908 00503998	The Firewall has been improved to handle large connections tables.	Gateway

ID	Description	Install On
00376299 00347784 00376296 00376297 00376298 00445756 00495071	SNMP handling improved to properly accept Check Point SNMP Pull requests.	Gateway
00496093 00217318 00351548 00406381 00496093 00501616 00496094	Gateways can now successfully open SSL VPN connections, even if clustering is not enabled.	Gateway
00466612 00464197 00466616	Information of logs with filesize larger than 2GB is now correctly displayed from the Get File List command.	SmartCenter server
00495637 00444032 00463576 00495638	Improved firewall process handling fixed error (see /var/log/messages): "Failed to init ctipd's iprep object".	Gateway
00495632 00421360 00495633	Improved SMTP resource with MX-resolving to fix a memory leak.	Gateway
00435013 00434854 00435011	Improved SIP connectivity with Hidden NAT.	Gateway
00495666 00137684 00179812 00448482 00495667 00185059	Improved Clientless VPN for correct translation of the location HTTP header from http to https.	Gateway
00495004 00466145 00494415 00495005	Improved sam_alert configured on IPSO stand-alone environments, fixing handling conditions that were causing sam_alert to not be executed.	Gateway

ID	Description	Install On
00494698 00441036 00439548 00467061	VPN debug mode has been improved for stability when working with NAT traversal tunneling (UDP encapsulation).	Gateway
00496601 00341170 00403922 00417598	SIP packet handling has been improved to fix the "Attack Info - BYE message is out of state" error.	Gateway
00512176 00511326 00512178 00517764 00519229	Enhancements to Web Filtering are implemented in SmartView Monitor.	SmartCenter server Gateway
00446671 00443585 00446870 00503511 00508639 00504798 00510866 00517061 00508196 00508962 00510318 00511879 00517405 00517716 00521505	Improved stability of FWD process while handling logs.	Gateway

Management

ID	Description	Install On
00495622 00373479 00409480 00422945 00467064 00495623	Enhanced stability for FWM process to handle corruptions in Thresholds table.	SmartCenter server

ID	Description	Install On
00504024 00499473	SmartUpdate now allows an unlimited number of packages to be installed on a gateway.	SmartCenter server
00443001 00442874 00442996 00443471	SmartView Monitor provides improved gateway status information, fixing scenarios where the information could not be retrieved, due to enhanced communications between server and gateway.	SmartCenter server
00465326 00464693 00493501	Improved stability of the cpd process.	SmartCenter server and Gateway

Performance Pack

ID	Description	Install On
00443702 00443074 00466281 00466507	Improved the "fwaccel stat" command output for accurate display of accelerated connection information.	Gateway

SmartDefense

ID	Description	Install On
00501588 00415867 00416559 00422066 00424727 00428683 00430198 00431184 00463232 00501045	String search of SmartDefense packets in SmartView Tracker now correctly handles issues that would return an Internal Handling error if the packet was too small to hold the string.	Gateway

ID	Description	Install On
00427013 00426431 00427359 00433544	(Web Intelligence)Anti-virus improved for web page loading; previously certain pages were not refreshed well.	Gateway

SSL Network Extender

ID	Description	Install On
00450332 00445014 00450334 00464487 00467062	With multiple SSL Network Extender licenses for five users installed on one SmartCenter server, the total number of allowed users is now calculated correctly.	SmartCenter server and Gateway
00496949 00448958 00496973 00497118	If Office Mode assignment on the gateway depends on a RADIUS group, SSL Network Extender is now correctly authenticated.	Gateway

VoIP

ID	Description	Install On
00447938 00445389 00445541 00446481	Improvements to packet handling fix a "Malformed SCCP packet - Invalid Reserved field" error and correctly pass SCCP packets.	Gateway

VPN

ID	Description	Install On
00496029 00410051 00417632 00450301	Improved NAT-T connections between SecureClient and ClusterXL in Legacy mode, to correctly recognize the cluster interface for Main Mode packet 4 with NAT-D payload. This fixes the issue that resulted in a "Payload Malformed" error.	Gateway

ID	Description	Install On
00415860 00414578 00415499 00498285 00430640 00439726 00444898	Fixed certificate enrollment when management is behind NAT	Gateway
00444892 00427454 00427592 00499156 00429669 00433580 00444412	Improved IKE to IP address mapping to provide a relevant IPsec SA to packets after the mapping has been changed.	Gateway
00496911 00436874 00496976	When a route-based VPN community is defined between a gateway and an Edge appliance, the VPN tunnel persistence is maintained after restarting the firewall (cpstop and cpstart).	Gateway
00415544 00415371 00496978	In an environment with multiple tunnels between two gateways, and multiple IKE SAs for each gateway, the "vpn tu" command now correctly displays the relation between the IPSEC SAs and the IKE SAs when printing IPSEC SAs list.	Gateway

Platform Specific

SecurePlatform

ID	Description	Install On
00464335 00464252	Enhanced password handling fixes truncated passwords, which happened when using SCP or FTP backup.	Gateway
00494933 00467170	Improved SecurePlatform SSH commands for correctly persistent IP address changes.	Gateway
00462732 00450357 00502325 00503381	When creating a backup file, if the command includes a -path flag but not a filename, the default filename is appended, ensuring that the backup file is created.	Gateway
00435672 00435536	SCP backup passwords may now contain a zero (0) character in any place.	Gateway

IPSO

ID	Description	Install On
00495973 00192811 00362754 00420292	Increased outgoing buffer size for UDP sockets (to 64K) fixes errors with IKE on MM packet 5 and 6.	Gateway

Miscellaneous

SMTP Security Server

ID	Description	Install On
00496720 00494943 00496722	Firewall now passes the Temporary SMTP error code 402 which is used by greylisting. This allows users to send mail to a site whose mail server uses greylisting for Anti-spam.	Gateway

Policy Server

ID	Description	Install On
00374568 00368079	When a SecureClient for Mac OSX connects to a Policy Server that does not have a "SecureClient for Macosx" license, the SmartView Tracker will now log the "Mac license is limited to 0 users" error only once per Mac OS user connection, rather than every ten minutes.	SmartCenter server

SecureXL

ID	Description	Install On
00467162 00465493	Resolved connectivity issue with Performance Pack and interfaces with non equal MTU size.	Gateway

Authentication

00374443 00369981 00374435 00374441 00383500	When using partially automatic client authentication and when the Primary ISP link is down, the client can still get authenticated. Previously, the client received a "The page cannot be displayed" message in the browser when attempting authentication.	Gateway
--	---	---------

ClusterXL

ID	Description	Install On
00496596 00418374 00419982	ClusterXL, configured in Load Sharing mode with Performance Pack turned on, now handles the load for policy installation properly; previously both members were processing same traffic.	Gateway

SmartProvisioning

ID	Description	Install On
00449966 00449183 00449969 00463798 00501246	Gateway status on SmartProvisioning is now correct, fixing an error that may appear after installing HFA_30, that displayed "Needs Attention" for gateway status when it should have displayed "OK".	SmartCenter server

QoS

ID	Description	Install On
00448638 00448553 00448637 00498469	When verifying Traditional QoS policy which includes DiffServ rule and there is an Edge object with QoS enabled, the following error was displayed: "Traditional QoS policy cannot contain VPN-1 UTM Edge/Embedded Gateways. Instead please use Express QoS policy." This was a false error and is now no longer shown.	SmartCenter server

Gateway Protection

ID	Description	Install On
00509491	In response to the Sockstress TCP DoS vulnerability, this HFA provides a comprehensive protection for Check Point Security Gateways and the resources behind them. See sk42723 https://supportcontent.checkpoint.com/solutions?id=sk42723	SmartCenter server