



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

Provider-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=10307).

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 Provider-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
Provider-1	5
SecurePlatform	5
VPN-1 Edge/Embedded	5
Database Revisions	6
Connectra	6
Eventia Analyzer and Reporting Server	6
Supported Versions, Platforms, and Builds	7
Supported Platforms	7
Supported Products	7
Supported Builds	8
Supported Builds History	8
Installation	9
Required Disk Space	9
Installing HFA with Web User Interface on Smart-1	10
Verifying Installation with Web User Interface	10
Installing on SecurePlatform Open Server	10
Installing on Solaris or Linux	11
Updating Customized INSPECT Files	11
Uninstallation	13
Important Notes	13
Uninstalling HFA from MDS	13
Post-Uninstall Notes	13
Resolved Issues in NGX R65 HFA 60	14
Provider-1	14
Anti-virus	15
Firewall	16
Management	17
SSL Network Extender	17
Miscellaneous	18

Introduction

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

- Improved license handling for various issues and platforms.
- Improved maintenance of objects assigned to deleted Customers.
- Improved import of OSE access list.
- Enhanced log forwarding.
- Improved Activate Plug-in operations.
- Resolved memory leak of global policy instance.

Known Limitations

In this Section

Provider-1	5
SecurePlatform	5
VPN-1 Edge/Embedded	5
Database Revisions	6
Connectra	6
Eventia Analyzer and Reporting Server	6

Provider-1

ID	Description
00380298	If NGX R65 HFA 60 experiences difficulties with SSL Network Extender or Endpoint Security Client, refer to sk37382 (http://supportcontent.checkpoint.com/solutions?id=sk37382).
00427880	If this HFA is uninstalled, stored revisions that were made while it was installed cannot be viewed or reloaded.

SecurePlatform

ID	Description
	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. Check Point SecurePlatform NGX (R65) HFA 60 will be displayed after uninstal. Make sure to read the notes about important steps to do after uninstalling (" Post-Uninstall Notes " on page 13).
00466648	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).
	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.

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.

ID	Description
00522831	<p>During HFA installation, all INSPECT files related to the UTM-1 Edge compatibility package (located at /opt/CPEdgecmp-R65/libsw/) are overwritten. Any manual changes made on these files will be lost.</p> <p>For details see: sk43158 https://supportcontent.checkpoint.com/solutions?id=sk43158</p>

Database Revisions

ID	Description
00432491	<p>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.</p>

Connectra

ID	Description
	<p>Installation of Connectra NGX R62 Central Management plug-in is not supported on an NGX R65 MDS with certain other plug-ins. For a list of plug-in compatibility: (http://www.checkpoint.com/nginx/upgrade/plugin/index.html)</p>

Eventia Analyzer and Reporting Server

ID	Description
00467080	<p>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.</p>
00519595	<p>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.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. <code>cpstop</code> 2. <code>execute:</code> <ul style="list-style-type: none"> • Unix: <code>CRegSvr -p \$RTDIR/lib libCPSet2Sql.so</code> • Windows: <code>CRegSvr /p "%RTDIR%\lib" CPSet2Sql.dll</code> 3. <code>cpstart</code>

Supported Versions, Platforms, and Builds

In this Section

Supported Platforms	7
Supported Products	7
Supported Builds	8
Supported Builds History	8

Supported Platforms

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

Platform	Version
Smart-1	Model 50
SecurePlatform	NGX R65 on SecurePlatform 2.4 and 2.6
Solaris	5.8, 5.9, 5.10
Linux	Red Hat Enterprise Linux 3.0 kernel 2.4

Supported Products

This HFA may be installed with various Check Point products.

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

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 Provider-1 NGX R65 HFA 60 consists of the following builds:

Component	Build Number	Verify Command and Output
MDS	620660010	The output of fw mds ver should appear similar to: This is Check Point Provider-1 Server NGX (R65) HFA_60, Hotfix 660 - Build 010
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	
VPN-1 UTM Edge Compatibility	620660005	

Supported Builds History

	MDS	Firewall	SecurePlatform	Edge Compatibility
R65_HFA_50	620650023	620650048	620650021	620650004
R65_HFA_40	620640039	620640091	620640029	620640008
R65_HFA_30	620630014	620630049	620630036	620630018
R65_HFA_02	620602004	620602008	620602004	Windows: 620602005 Solaris: 620602007
R65_HFA_01	620601030	620601019	620601008	620601004

Installation



Important -

Before installing Provider-1 NGX R65 HFA 60, run

- `mdsenv`
- `mdsstop`

If this is not done, the system will experience functionality issues.

It is also recommended to backup the system by executing `mds_backup` command before any installation.

In this Section

Required Disk Space	9
Installing HFA with Web User Interface on Smart-1	10
Installing on SecurePlatform Open Server	10
Installing on Solaris or Linux	11
Updating Customized INSPECT Files	11

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
Smart-1 SecurePlatform	576	/opt = 440 /var = 100 root = 100
Solaris	311	/opt = 530
Linux	576	/opt = 450 /var = 100

Installing HFA with Web User Interface on Smart-1

You can use the Web User Interface to install this HFA on a Smart-1 appliance.

Before installing this HFA on Smart-1, make sure to take a snapshot of the machine.

To install NGX R65 HFA 60 on Smart-1:

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 Web User Interface: **https://<IP>:4434**
3. Open the Upgrade page: **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 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 Web User Interface

To verify NGX R65 HFA 60 installation through the Web User Interface, make sure that **HFA 60** appears in the Build information: **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 or Linux

To install NGX R65 HFA 60 on Solaris or Linux:

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)
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.

Updating Customized INSPECT Files

The MDS 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.

The installation routine automatically updates INSPECT files for all CMAs only if all INSPECT files are unmodified for that CMA.

If all CMAs were updated successfully (none had modified INSPECT files), the following message appears:

```
The updated Inspect files have been installed successfully.
To complete the installation, please re-install the Security Policy on all your
gateway for the CMAs.
```

If any INSPECT files in a CMA were previously modified, no INSPECT files are updated for this CMA. The following message appears:

```
Signature mismatches were found for some CMAs. This indicates that manual change were
made to the Inspect files. These affected CMAs are listed in:
$MSDIR/tmp/manually_modified_cmas.txt
Please note that the specified Inspect files were NOT updated for these CMAs. If you
wish to update them, execute the following command:
hf_propagate o --override_manual
```

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.

The following procedure is done on **ALL** CMAs at once, not just the one you are working on.

To force INSPECT files to be updated:

1. On the MDS, open **\$MSDIR/tmp/manually_modified_cmas.txt** and note the CMAs that have modified INSPECT files.

For each of these CMAs, do the following.

2. Go to the CMA: `mdsenv <CMA_Name>`.
3. On the CMA, open **\$FWDIR/lib/update_inspect_files_60.log** and note the INSPECT files that were modified.

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

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

4. Open the files that are listed in **update_inspect_files_60.log** and note the customized lines.
5. Run: `hf_propagate o --override_manual`

6. Merge the customized content (that you noted in the previous steps) into the new INSPECT file(s).
7. Re-install the Security Policy to enable the new INSPECT files.



Note - Backups of the upgraded files are saved with **_pre_HFA_60** in the filename.

Uninstallation

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 HFA from MDS

Before you begin this procedure, note that the order of uninstallation executes is important. You must follow the instructions in the order provided here; otherwise, the uninstallation could have unwanted results. In addition, uninstallation of individual packages is not supported.

To uninstall NGX R65 HFA 60 from Provider-1 MDS:

1. Execute: `mdsstop`
2. Execute: `/opt/CPUninstall/R65_HFA_60/UnixInstallScript -u`
3. Reboot the machine when uninstallation is complete.



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

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

Provider-1	14
Anti-virus	15
Firewall	16
Management	17
SSL Network Extender	17
Miscellaneous	18

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.

Provider-1

ID	Description	Install On
00465893 00445921 00450283 00465272	When a Customer object is deleted, it no longer deletes the objects to which the Customer was assigned.	MDS
00465306 00464268 00466035	Improved parsing algorithms provide correct import of Cisco routers (OSE) access list in ASCII format.	MDS
00466439 00428467 00436800 00443490 00466039 00466434	Improved Provider-1 licensing fixed an issue with adding licenses to CMAs with SmartUpdate.	MDS

ID	Description	Install On
00413150 00182658 00218123 00334445 00377778 00424151 00425399 00427742 00406648 00416771 00428000 00441325 00449358	The number of allowed users for SSL Network Extender licenses is now calculated correctly according to the number of licenses on each relevant CMA, rather than the number of licenses on the MDS.	MDS
00467051 00440147 00442116 00467052	Enhanced Log Forwarding mechanism to provide greater stability of fwd process.	MDS and Log Server
00447109 00445956	Improved handling of firewall processes provides increased stability of Provider-1 when performing an Activate Plug-in operation.	MDS
00466320 00465700 00466323 00466483 00503214 00497740	Improved processing fixed a memory leak that occurred if a CMA is assigned to a global policy, and rules are added above or below the policy.	MDS

Anti-virus

ID	Description	Install On
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.	MDS

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

Firewall

ID	Description	Install On
00445961 00443248 00467022 00445963 00446664 00493483 00494114 00503420	Enhancements to CPD process fixed memory leak.	MDS and Gateway
00466612 00464197 00466616	Information of logs with filesize larger than 2GB is now correctly displayed from the Get File List command.	MDS

Management

ID	Description	Install On
00495622 00373479 00409480 00422945 00467064 00495623	Enhanced stability for FWM process to handle corruptions in Thresholds table.	MDS
00504024 00499473	SmartUpdate now allows an unlimited number of packages to be installed on a gateway.	MDS
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.	MDS
00465326 00464693 00493501	Improved stability of the cpd process.	MDS and 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 MDS, the total number of allowed users is now calculated correctly.	MDS

Miscellaneous

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.	MDS

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.	MDS