COPYRIGHT
©2007 Nokia. All rights reserved.
Rights reserved under the copyright laws of the United States.

RESTRICTED RIGHTS LEGEND
Use, duplication, or disclosure by the United States 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.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

IMPORTANT NOTE TO USERS
This software and hardware is provided by Nokia Inc. as is and any express or implied warranties, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Nokia, or its affiliates, subsidiaries or suppliers be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Nokia reserves the right to make changes without further notice to any products herein.

TRADEMARKS
Nokia is a registered trademark of Nokia Corporation. Other products mentioned in this document are trademarks or registered trademarks of their respective holders.
### Nokia Contact Information

#### Corporate Headquarters

<table>
<thead>
<tr>
<th>Web Site</th>
<th><a href="http://www.nokia.com">http://www.nokia.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>1-888-477-4566 or 1-650-625-2000</td>
</tr>
<tr>
<td>Fax</td>
<td>1-650-691-2170</td>
</tr>
<tr>
<td>Mail Address</td>
<td>Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA</td>
</tr>
</tbody>
</table>

#### Regional Contact Information

<table>
<thead>
<tr>
<th>Region</th>
<th>Address</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>Nokia Inc. 313 Fairchild Drive</td>
<td>Tel: 1-877-997-9199</td>
</tr>
<tr>
<td></td>
<td>Mountain View, CA 94043-2215 USA</td>
<td>Outside USA and Canada: +1 512-437-7089</td>
</tr>
<tr>
<td></td>
<td></td>
<td>email: <a href="mailto:info.ipnetworking_americas@nokia.com">info.ipnetworking_americas@nokia.com</a></td>
</tr>
<tr>
<td>Europe, Middle East, and Africa</td>
<td>Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK</td>
<td>Tel: UK: +44 161 601 8908</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tel: France: +33 170 708 166</td>
</tr>
<tr>
<td></td>
<td></td>
<td>email: <a href="mailto:info.ipnetworking_emea@nokia.com">info.ipnetworking_emea@nokia.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968</td>
<td>Tel: +65 6588 3364</td>
</tr>
<tr>
<td></td>
<td></td>
<td>email: <a href="mailto:info.ipnetworking_apac@nokia.com">info.ipnetworking_apac@nokia.com</a></td>
</tr>
</tbody>
</table>

### Nokia Customer Support

<table>
<thead>
<tr>
<th>Region</th>
<th>Web Site: <a href="https://support.nokia.com/">https://support.nokia.com/</a></th>
<th>Email: <a href="mailto:tac.support@nokia.com">tac.support@nokia.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>Voice: 1-888-361-5030 or 1-613-271-6721</td>
<td>+44 (0) 125-286-8900</td>
</tr>
<tr>
<td></td>
<td>Fax: 1-613-271-8782</td>
<td>+44 (0) 125-286-5666</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Voice: +65-67232999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fax: +65-67232897</td>
<td></td>
</tr>
</tbody>
</table>
Contents

About This Guide ............................................................... 7
In This Guide .................................................................. 7
Conventions This Guide Uses ........................................ 8
Notices ............................................................................ 8
Text Conventions ............................................................. 8
Related Documentation .................................................. 9

1 Preparing for Installation and Configuration .................. 11
Basic VPN-1 Power and Check Point UTM Components ........ 11
Using Nokia Horizon Manager ........................................... 12
Installation and Configuration Overview .......................... 12
Basic Steps for Installing and Configuring ...................... 13
Determining Nokia IPSO and Check Point Software Versions .................................................. 15
  Checking the Nokia IPSO Version .................................. 15
  Checking the Installed Check Point Packages .................. 15
Preparing the Nokia IP Security Platform ......................... 15
Preparing an IP265 Security Platform .............................. 16
Preparing the Network ..................................................... 17
Obtaining Check Point Licensing ...................................... 17

2 Installing Check Point NGX R62 ................................. 19
Before You Start ............................................................. 19
Downloading NGX R62 Software ...................................... 19
Installing the NGX R62 Software ..................................... 20
Installing HotFix Accumulators on Flash-based Platforms .... 24

3 Performing the Initial Configuration ............................ 25
Using Nokia Horizon Manager ......................................... 25
Using the Check Point Configuration Tool ....................... 25
  About the Initial Firewall Policy .................................... 26
  Before You Start .......................................................... 27
Configuring a Standalone Deployment ............................. 27
Configuring a Distributed Deployment ............................. 29
Enabling SecureXL ......................................................... 32
4 Installing SmartConsole NGX R62 .................................................. 33

5 Upgrading to Check Point NGX R62 ........................................... 37
  Overview of the Upgrade Process ............................................. 37
  Obtaining the Software ....................................................... 38
  Preparing an IP265 Platform ................................................. 39
  Upgrading Security Platforms .............................................. 39
  Installing HotFix Accumulators on Flash-based Platforms .... 42
  Reverting to Previous Check Point Versions ......................... 42
About This Guide

This guide describes how to install, initially configure, and upgrade to Check Point NGX R62 on a Nokia IP security platform. This guide is not intended to be a complete guide to configuring or managing Check Point services. For information about these subjects, see the Check Point Getting Started Guide and additional documentation available from the Check Point Web site.

This preface provides the following information:

- In This Guide
- Conventions This Guide Uses
- Related Documentation

In This Guide

This guide is organized into the following chapters:

- Chapter 1, “Preparing for Installation and Configuration,” provides an overview of the installation process and describes how to prepare to install and configure NGX R62.
- Chapter 2, “Installing Check Point NGX R62,” describes how to use Nokia Network Voyager or the newpkg IPSO command to install the Check Point applications on your platform.
- Chapter 3, “Performing the Initial Configuration,” describes how to use the cpconfig utility to perform the initial configuration.
- Chapter 4, “Installing SmartConsole NGX R62,” describes how to install the Check Point SmartConsole, the SmartCenter GUI clients, on a Microsoft Windows system.
- Chapter 5, “Upgrading to Check Point NGX R62,” describes how to upgrade to Check Point NGX R60.

To perform a new installation and configuration of NGX R62 on a Nokia platform, read all of the chapters in this guide except Chapter 5. If your Nokia platform comes with NGX R62 installed, you can skip Chapter 2. If you are upgrading to NGX R62 from an earlier version of the Check Point software, you can skip directly to Chapter 5.

Note

If you do not know which version of Check Point software is installed on your platform, see “Determining Nokia IPSO and Check Point Software Versions” on page 15.
Conventions This Guide Uses

The following sections describe the conventions this guide uses, including notices, text conventions, and command-line conventions.

Notices

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes provide information of special interest or recommendations.</td>
</tr>
</tbody>
</table>

Text Conventions

The following table describes the text conventions this guide uses.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monospace font</td>
<td>Indicates command syntax, or represents computer or screen output, for example:</td>
</tr>
<tr>
<td></td>
<td>Log error 12453</td>
</tr>
<tr>
<td>bold monospace font</td>
<td>Indicates text you enter or type, for example:</td>
</tr>
<tr>
<td></td>
<td># cpconfig</td>
</tr>
<tr>
<td>Key names</td>
<td>Keys that you press simultaneously are linked by a plus sign (+):</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl + Alt + Del.</td>
</tr>
<tr>
<td>Menu commands</td>
<td>Menu commands are separated by a greater than sign (&gt;):</td>
</tr>
<tr>
<td></td>
<td>Choose File &gt; Open.</td>
</tr>
<tr>
<td>The words enter and type</td>
<td>Enter indicates you type something and then press the Return or Enter key.</td>
</tr>
<tr>
<td></td>
<td>Do not press the Return or Enter key when an instruction says type.</td>
</tr>
<tr>
<td>Italics</td>
<td>• Emphasizes a point or denotes new terms at the place where they are defined in the text.</td>
</tr>
<tr>
<td></td>
<td>• Indicates an external book title reference.</td>
</tr>
<tr>
<td></td>
<td>• Indicates a variable in a command:</td>
</tr>
<tr>
<td></td>
<td>newpkg file_name.tgz</td>
</tr>
</tbody>
</table>
Related Documentation

For more information about Check Point NGX R62, see the appropriate guides available at the Check Point Product Documentation Web site at http://www.checkpoint.com.

For more information about how to configure and manage a Nokia IP security platform, see:

- The *IPxxx Series Installation Guide* for your security platform.
- The *Getting Started Guide and Release Notes* for your IPSO version.
- The *CLI Reference Guide* for your IPSO version.

These documents are available at the Nokia Support site at http://support.nokia.com.
Preparing for Installation and Configuration

This chapter describes how to prepare for first-time installation and configuration of Check Point NGX R62 on a Nokia IP security platform.

This chapter contains the following topics:

- Basic VPN-1 Power and Check Point UTM Components
- Using Nokia Horizon Manager
- Installation and Configuration Overview
- Basic Steps for Installing and Configuring
- Determining Nokia IPSO and Check Point Software Versions
- Preparing the Nokia IP Security Platform
- Preparing an IP265 Security Platform
- Preparing the Network
- Obtaining Check Point Licensing

Basic VPN-1 Power and Check Point UTM Components

The Check Point NGX R62 applications include management products, gateway products, and client software. This guide focuses on the Check Point Power and Check Point UTM products, which consist of three main components:

- ** Enforcement module**—the VPN-1 Power gateway or VPN-1 UTM gateway module that enforces the Check Point security policy.
- ** Management server**—the SmartCenter server that maintains the databases of network object definitions, user definitions, policies, and log files for any number of enforcement modules.

**Note**
You can manage VPN-1 gateways using either SmartCenter or Provider-1/SiteManager-1. This guide focuses on SmartCenter, which can be installed on a Nokia IP security platform. For information on installing and configuring Provider-1/SiteManager-1, see the Check Point documentation.
SmartConsole—contains GUI applications that manage different aspects of the security policy. SmartConsole includes the SmartDashboard, which provides a GUI interface for the administrator to define network objects, users, and policies.

VPN-1 Power and Check Point UTM were formerly known as VPN-1/FireWall-1. VPN-1 Power is for companies with more than 500 employees. Check Point UTM is for businesses with up to 500 employees and multiple sites. When you perform the initial configuration, you choose whether to install VPN-1 Power or Check Point UTM.

This document describes how to install and initially configure the enforcement module, the SmartCenter server, or both on a Nokia platform. It also describes how to install the SmartConsole on a Microsoft Windows system.

Using Nokia Horizon Manager

Nokia Horizon Manager is a secure GUI-based software-image management application. With Horizon Manager, you can securely install and upgrade the Nokia IPSO operating system and Check Point packages. Nokia Horizon Manager can perform installations and upgrades on up to 2,500 Nokia IP security platforms, offering administrators the most rapid and dependable upgrade to Check Point NGX R62.

If you plan to use Nokia Horizon Manager to install or upgrade and configure NGX R62, see the Nokia Horizon Manager documentation on the Nokia Support site: http://support.nokia.com.

For information about how to obtain Nokia Horizon Manager, see the “Nokia Contact Information” on page 3.

Installation and Configuration Overview

The order in which you install and configure components depends on whether you choose a distributed or a standalone deployment of the components:

- In a distributed deployment, the SmartCenter server and the enforcement modules are on separate nodes.
- In a standalone deployment, the SmartCenter server and the enforcement module are on a single node.

Note
You must use a distributed deployment for Nokia platforms that are members of an IP cluster or VRRP virtual router. Only enforcement modules should be installed on these platforms.

Install and configure the components in the following order.
Distributed Deployment:
1. Install and configure the SmartCenter server.
2. Install SmartConsole on the Microsoft Windows hosts.
3. Install and configure the enforcement module or modules.

Standalone Deployment:
1. Install and configure the SmartCenter server and enforcement module on the same platform.
2. Install the SmartConsole on the Microsoft Windows hosts.

The SmartCenter component and the VPN-1 Power/UTM enforcement component are installed using the same software package. If NGX R62 is already installed on your Nokia IP security platform, you do not need to install this package, but you do need to enable the package and perform the initial configuration. During the initial configuration, you specify which component is deployed on the platform.

These high-level steps are described in more detail in the rest of this guide.

Basic Steps for Installing and Configuring

Figure 1 shows the main steps you take to install VPN-1 Power or Check Point UTM on your Nokia platform.
After you finish the installation and configuration, you can use the SmartDashboard application to define the network objects, users, and Security Policy. For more information, see the Check Point documentation.
Determining Nokia IPSO and Check Point Software Versions

To run NGX R62, you must have Nokia IPSO 3.9, 4.1 or 4.2 on your Nokia platform. For current information on which IPSO versions are supported, see the Nokia support Web site. It is important to verify that you have a supported IPSO version before you perform the installation and configuration.

Your platform might have NGX R62, an earlier version of Check Point software, or no Check Point applications installed. The software on your platform determines whether you need to skip the NGX R62 installation steps or perform a new installation.

Note
If you are using IPSO 4.1 and you rollback from R62 to R60, use the following procedure:

1. Go to Install Packages and select R60.
2. Go to Manage Images and select IPSO 4.1.
3. Go to Reboot, Shut Down System and click Reboot.

Checking the Nokia IPSO Version

To determine the IPSO version on your platform, log in to the platform by using Nokia Network Voyager. The Software Release field in the summary table on the home Network Voyager page shows the IPSO version your platform is running.

If your platform is not running IPSO 3.9 or later, upgrade the operating system or perform a fresh installation. For instructions on how to do so, see the Getting Started Guide and Release Notes for your IPSO version. The release notes are available on the Nokia Support site: http://support.nokia.com.

Checking the Installed Check Point Packages

To determine what Check Point applications are installed on your platform, log in to the platform by using Network Voyager. Navigate to the Manage Packages page:

IPSO 3.9: System Configuration > Manage Installed Packages
IPSO 4.1 or later: Configuration > System Configuration > Packages > Manage Packages.

The Manage Packages page lists the installed packages and the version of each package. If no Check Point applications are listed, no Check Point products are installed on your platform.

Preparing the Nokia IP Security Platform

To prepare your Nokia IP security platform for Check Point NGX R62:
If you did not already, configure the platform initial interface and the network interfaces. For more information, see the *IPxxx Series Installation Guide* for your IP security platform.

Make sure you can access the security platform by using Network Voyager and by using a console or terminal connection.

If your security policy will block HTTP access while permitting HTTPS access, enable HTTPS access on the security platform. See the *Nokia Network Voyager Reference Guide* for information on how to do so and how to replace the default SSL certificate.

If you need to install NGX R62, ensure that you have at least 300 MB of free disk space in the /opt directory for disk-based platforms and 100 MB of free disk space in the /opt directory for flash-based platforms.

Confirm that you have a static host name associated with the external IP address of the security platform.

You cannot install a Check Point Power or Check Point UTM license unless the external interface has a static host name associated with it.

**To add a static host name**

1. Connect to the security platform by using Network Voyager.
2. Navigate to the Host Address Assignment page:
   - IPSO 3.9: System Configuration > Host Address Assignment
   - IPSO 4.1 or later: Configuration > System Configuration > Host Address
     
     By default, an entry for localhost exists. If it is the only entry, you need to add a host name for the platform.
3. To add a new entry, type the desired name and click Apply.
4. Select on or off as desired; however, do *not* turn off localhost.
5. Specify the host IP address (for example, 192.169.11.45).
6. Click Apply, then click Save to make the changes permanent.

![Figure 2 Example Host Address Assignment](image)

**Preparing an IP265 Security Platform**

Nokia recommends that you use the external flash-memory PC card supplied with your IP265 to store the Check Point packages. Doing so frees up internal memory for firewall use.
To enable the IP265 to use the external flash card for the packages

1. Install your flash-memory PC card into PC-card slot 2. Make sure the card is fully inserted by pressing gently on it.
2. In Network Voyager, select the Optional Disk Configuration page (Configuration > System Configuration > Optional Disk).
3. Click the radio button under Packages; then click Apply and Save.
4. Wait until you see a message telling you that you should reboot the system and then reboot the system.

Note
If Check Point packages are installed, the reboot immediately following enabling/disabling the Packages option will take a long time to complete, as much as 10 minutes. This is normal: do not reboot your platform again until the first reboot completes successfully.

Preparing the Network

Ensure your network is properly configured, with special emphasis on routing:

- Ensure that each of the internal networks and the gateway can see each other.
- Log on to each of the hosts and ping the other hosts in the internal networks.
- If you plan to install the management server and enforcement module on separate platforms, ensure that the management server host can ping the external IP address of the enforcement module host, and the reverse.

For gateways that are members of a VRRP virtual router or an IP cluster, please see the Nokia Network Voyager Reference Guide for Check Point considerations when setting up virtual routers or IP clusters.

Obtaining Check Point Licensing

Obtain the appropriate Check Point Power or Check Point UTM license from Check Point or your vendor. Start this process several days before the anticipated installation or upgrade. If you did not purchase the Check Point software, the software will work for 15 days. You must use the Check Point User Center to register your software.
This chapter describes how to install Check Point NGX R62 on a Nokia IP security platform.

- If you already have NGX R62 installed, skip this chapter and proceed to Chapter 3, “Performing the Initial Configuration.”
- If you have a previous version of Check Point NG or NGX installed and configured and want to perform an upgrade, skip this chapter and proceed to Chapter 5, “Upgrading to Check Point NGX R62.”

**Before You Start**

Before you start the installation, make sure that:

- The Nokia IPSO version on the platform is IPSO 3.9 or a later supported version. If it is not, upgrade the operating system image as described in the *Getting Started Guide and Release Notes* for your IPSO version.
- You have prepared your platform and network as described in “Preparing the Nokia IP Security Platform” on page 15 and “Preparing the Network” on page 17.

**Downloading NGX R62 Software**

Download the NGX R62 software from the Check Point Downloads Web site to an FTP server on your network.

Information on NGX R62 for Nokia and a link to the Check Point Downloads Web site are available in Download 1610455 at the Nokia support Web site.

Which installation packages you should download depends on your type of platform:

- **All platforms except the IP265**—download the following:
  - Comprehensive R62 wrapper for Nokia IPSO (IPSO_wrapper_R62.tgz)
    Use the comprehensive wrapper to install an enforcement module or a SmartCenter server (or both) on a disk-based platform.
  - SmartConsole R62 (SmartConsole_R62_xxxxxxxxx_x_Win.zip)
Use this package to install the SmartConsole GUIs on Microsoft Windows hosts. The package is available under the Windows OS in the Check Point Download selector for NGX R62.

- **IP265 platforms**—download the following:
  - **VPN-1 Power/UTM NGX R62 for flash-based platforms** (fw1_R62_xxxxxxxx_x_IPSO.tgz)
    Use this package to install an enforcement module on a flash-based platforms. You cannot install a SmartCenter server on a flash-based platform.
  - **CPinfo Tool NGX R62 for IPSO platforms** (cpinfo_R62_xxxxxxxx_x_IPSO.tgz)
  - **SmartConsole R62** (SmartConsole_R62_xxxxxxxx_x_Win.zip)
    Use this package to install the SmartConsole GUIs on Microsoft Windows hosts. The package is available under the Windows OS in the Check Point Download selector for NGX R62.

### Installing the NGX R62 Software

On disk-based platforms, all of the Check Point packages required for enforcement modules and management server modules are contained within the comprehensive wrapper and are automatically installed when you install the comprehensive wrapper. Table 1 summarizes the packages installed by the wrapper.

<table>
<thead>
<tr>
<th>Package</th>
<th>Status After Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point VPN-1 Power/UTM NGX R62</td>
<td>Active</td>
</tr>
<tr>
<td>Check Point R55W Compatibility Package for NGX</td>
<td>Not active</td>
</tr>
<tr>
<td>Check Point CPinfo</td>
<td>Active</td>
</tr>
<tr>
<td>R55 Compatibility Package for NGX</td>
<td>Not active</td>
</tr>
<tr>
<td>Check Point Eventia Reporter NGX R62</td>
<td>Not active</td>
</tr>
<tr>
<td>Check Point UserAuthority Server NGX R62</td>
<td>Not active</td>
</tr>
<tr>
<td>Check Point VSX NGX Compatibility Package for VSX NGX</td>
<td>Not active</td>
</tr>
</tbody>
</table>

Since flash-based platforms host enforcement modules only, install the following individual packages in the following order:

1. The VPN-1 Power/UTM package for flash-based platforms
2. The CPinfo package
You can use the newpkg command, the Nokia CLI, or Nokia Network Voyager to install the Check Point packages. The steps for doing so are the same for any IPSO package. You can also use Nokia Horizon Manager to automate the installation process.

This section contains detailed procedures for installing Check Point packages using either the newpkg command or Network Voyager. For information on using the Nokia CLI, see the CLI Reference Guide. For information on using Nokia Horizon Manager, see the Nokia Horizon Manager documentation.

**To install using the newpkg command**

**Note**

On flash-based platforms:

If you plan to install from the local filesystem (that is, download the package to the platform first and then install from that directory), use /var/tmp or a directory you create in /var as your installation directory. The installation files will be automatically deleted when you reboot the system, freeing up space in flash memory.

If you plan to install from an FTP server, delete the contents of /preserve/opt/tmp before and after you perform the installation. newpkg uses this directory to store packages while installing them. Use the following command to delete the directory contents:

```bash rm -R /preserve/opt/tmp```

1. Log in to the platform with a console connection.
2. Enter `newpkg` to start the package installation script.
   The following options appear:
   1. Install from CD-ROM.
   2. Install from anonymous FTP server.
   3. Install from FTP server with user and password.
   4. Install from local filesystem.
   5. Exit new package installation.
3. Enter the number (1 through 4) next to the installation method to use, or enter 5 to exit.
   If you are installing from your current working directory in the local filesystem, you can enter a period (.) when asked for the pathname to the packages.
4. The installation script guides you through the rest of the installation process.
5. On flash-based platforms, repeat steps 2 through 4 to install CPinfo after you have installed VPN-1 Power/UTM.
6. Log off the platform and then log back in.
   When newpkg installs and enables packages, it sets new shell environmental variables that are necessary for executing firewall commands. However, they do not take effect until the next time you log on. For this reason, you need to log off and then log back in again before you can run cpconfig as described in the next chapter.
7. To make sure the NGX R62 packages are installed correctly, see “To confirm the installation” on page 23.

To install using Nokia Network Voyager

1. In the Network Voyager navigation tree, navigate as follows:
   - IPSO 3.9: System Configuration > Manage Installed Packages > FTP and Install Packages
   - IPSO 4.1 or later: Configuration > System Configuration > Packages > Install Package

2. Enter the host name or IP address of the FTP site where you downloaded the wrapper.
3. Enter the directory name where the files reside on the FTP site.
4. Enter the user account and password to use when you connect to the FTP site.
   If you leave these fields empty, the anonymous account is used.

   **Note**
   If you specify a user account and password, you must re-enter the password whenever you change the FTP site, FTP directory, or FTP user on future requests.

5. Click Apply.
   A list of files from the specified FTP directory appears in the Site Listing field.

6. Select the package from Site Listing, then click Apply.
   After the download completes, the package appears in the Select a Package to Unpack box.

7. Select the package, then click Apply.
   The package is unpacked into the local file system.

8. Click the link: Click here to install/upgrade /opt/packages/packagename.

9. Click Yes next to Install and click Apply.
   Wait until Network Voyager refreshes this page with a link to the Manage Installed Packages screen.

10. Click the link to return to the Manage Packages screen.
    The installation of the applications within the comprehensive wrapper can take several minutes to complete: as long as 10 to 20 minutes on some platforms.
    During the initial installation phase, the wrapper appears under the Security Applications heading. If you wait several minutes and click Apply, a warning message appears telling you that the installation is still in progress. The wrapper continues to unpack and install the Check Point applications in the package.
    You can click Apply to refresh the page and monitor the installation process. When the installation is complete, the warning message disappears and the Check Point NGX R62 application packages appear in the installed packages section.
    If you are installing individual packages on a flash-based platform, repeat steps 1 through 9 to install CPinfo after you install VPN-1 Power/UTM.
11. Confirm that the installation was successful, following the steps in “To confirm the installation” on page 23.

The following figure shows an example of the Manage Packages page after a new installation of NGX R62 wrapper on a disk-based platform running IPSO 4.1 or later.

### To confirm the installation

1. On the Manage Packages page in Network Voyager, confirm that the Check Point VPN-1 Power/UTM NGX R62 package appears under Security Applications and is enabled.
2. If the package is not enabled, click On, and then click Apply and then Save.
3. Enable any of the other Check Point packages you want to have enabled and click Apply and then Save.
4. If you enabled packages and are logged onto the platform with an IPSO shell session, log off and then log on again to set the environmental variables.

**Note**

Although you have enabled the Check Point VPN-1 Power/UTM package, firewall services do not start until you have run `cpconfig`, as described in the next chapter, and rebooted the platform.

After you run `cpconfig` and reboot, enabling/disabling the Check Point VPN-1 Power/UTM package on the Manage Packages page starts and stops the firewall services.

You are now ready to configure Check Point Power or Check Point UTM.
Installing HotFix Accumulators on Flash-based Platforms

Nokia recommends you follow these guidelines when installing HFAs on flash-based platforms:

- Do not download the HFAs to your home directory. Files in user home directories are preserved after reboots and consume valuable space in flash memory. Instead, download to /var/tmp or create a directory in /var and install the HFA from there. The installation files will be automatically deleted when you reboot after installing the HFA.

- After you extract the HFA files from the archive.tgz file, delete the archive file and then install the HFA as described in the HFA release notes.

- The IP265 platform must be configured with an external flash (optional disk) for type “Packages” for HFA installation.
Performing the Initial Configuration

You must perform an initial configuration of Check Point NGX R62 before Check Point VPN-1 services are available. During this initial configuration, you:
- Specify whether this is a Check Point Power or Check Point UTM installation
- Specify which components to deploy on the platform you are configuring and provide some administrative information about the components you have selected
- Provide information used to enable secure internal communication (SIC) between components

You can use Nokia Horizon Manager or the Check Point configuration tool, cpconfig, to perform the initial configuration.

This chapter describes:
- Using Nokia Horizon Manager
- Using the Check Point Configuration Tool
- Enabling SecureXL

Using Nokia Horizon Manager

Nokia Horizon Manager can perform the initial configuration of Check Point NGX R62 applications on multiple Nokia IP security platforms simultaneously. Nokia Horizon Manager also exchanges information with Check Point SmartCenter server to keep the Check Point database current with information about the newly added platforms.

If you are using Nokia Horizon Manager to perform the initial configuration, see the Nokia Horizon Manager and Check Point Guide available on the Nokia Support Web site for more information.

Using the Check Point Configuration Tool

This section describes how to use the Check Point configuration tool, cpconfig, to perform the initial configuration. It provides detailed steps for configuring both standalone and distributed deployments.
About the Initial Firewall Policy

After you use cpconfig to configure a VPN-1 Power or VPN-1 UTM enforcement module and reboot the platform, an initial firewall policy is loaded. This policy is based on a default filter that blocks all inbound access to the platform. While this policy is in force, you cannot access the platform remotely through a terminal connection or Nokia Network Voyager. Only SmartConsole clients are permitted access to the platform through the management server.

You can use one of the following ways to regain remote terminal or web access to the platform:

- Use SmartDashboard to create and install a policy that permits the desired remote connections to the platform.

**Note**
Make sure that the desired access methods have also been enabled on the platform. HTTPS, for example, is disabled by default.

- From a console connection, enter the cpstop command. This stops firewall services, allowing you access to the platform with Network Voyager. When you have finished your administrative tasks, start the firewall services again with the cpstart command.

- Before you run cpconfig, change the default filter on which the initial policy is based to one that permits SSH or HTTPS connections or both. Table 2 shows the available default filters.

<table>
<thead>
<tr>
<th>Filter File</th>
<th>Filter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultfilter.boot</td>
<td>Allows outbound traffic (originating from the firewall) and broadcast traffic only. This is the filter used by the default initial policy.</td>
</tr>
<tr>
<td>defaultfilter.dag</td>
<td>Allows outbound traffic, broadcast traffic, and DHCP</td>
</tr>
<tr>
<td>defaultfilter.drop</td>
<td>Drops all traffic in and out of the gateway</td>
</tr>
<tr>
<td>defaultfilter.ipso</td>
<td>Allows inbound SSH, HTTPS, and ICMP (PING) traffic and all outbound traffic</td>
</tr>
<tr>
<td>defaultfilter.ipso_ssl</td>
<td>Allows inbound SSH and ICMP traffic and all outbound traffic</td>
</tr>
<tr>
<td>defaultfilter.ipso_ssl</td>
<td>Allows inbound HTTPS and ICMP traffic and all outbound traffic</td>
</tr>
</tbody>
</table>
To change the default filter used by the initial policy

Enter the following sequence of commands at a console or remote terminal connection. If you want to use a default filter other than defaultfilter.ipso, then replace defaultfilter.ipso in the first command with the name of the filter you want to use.

\[ \text{cp $FWDIR/lib/defaultfilter.ipso $FWDIR/conf/defaultfilter.pf} \]
\[ \text{fw defaultgen} \]
\[ \text{cp $FWDIR/state/default.bin $FWDIR/boot} \]

If you use defaultfilter.ipso or defaultfilter.ipso_ssl, make sure that HTTPS has been enabled on the platform.

Before You Start

Before you start the initial configuration:

- Make sure the Check Point VPN-1 Power/UTM NGX R62 package is enabled.
  If it is not, enable it. For details, see “To confirm the installation” on page 23. If you have an active command line session, log off after you enable the package.

- If you want to install and manage the Check Point license locally, have the license information available. If you plan to use SmartUpdate to manage your licenses centrally, as recommended by Check Point, you do not need the information now.

- If you are configuring a SmartCenter server, be ready to supply:
  - An initial administrator username and password.
  - The IP address or name of at least one SmartDashboard host.

Configuring a Standalone Deployment

In a standalone deployment, a SmartCenter management server and a VPN-1 Power/UTM enforcement module are deployed on the same security platform.

---

**Note**
A gateway that is a member of a VRRP virtual router or an IP cluster cannot be configured as a standalone deployment. It must have an enforcement module only installed on it. See “To install a VPN-1 Power/UTM enforcement module” on page 31.

---

**Note**
Standalone deployments are not supported on flash-based (diskless) platforms.

---

**To configure a standalone deployment**

1. Log in to the host from a console or remote terminal connection.
2. At the command prompt, enter `cpconfig`.
The following text appears:

Welcome to Check Point Configuration Program

Please read the following license agreement.
Hit 'ENTER' to continue...

Note
If the text does not appear when you enter cpconfig, you might need to log out of the command-line session and then log back in to set the environmental variables.

3. Press Enter to read the license agreement, and then enter y to accept it.

4. Specify which product you are installing: Check Point Power or Check Point UTM.

5. Enter the appropriate number to select a standalone installation: 1 for Check Point Power installations or 2 for Check Point UTM installations.

6. Enter y to add a license and fill in the license information, or enter n to complete the license information later.

7. Define an initial administrator name and password.

   The initial administrator name and password you enter here allows you to log in to the SmartCenter server from the SmartDashboard. This administrator has full read/write permissions, allowing you to further add or modify administrators using the SmartDashboard.

   Administrators you define with the SmartDashboard can be issued a certificate for authentication, which provides a more secure means of authentication than the simple username used for the initial administrator. Check Point recommends that once you log on to the SmartDashboard, you create a new administrator with full read/write permissions, generate a certificate for the new administrator, and delete the initial administrator created by cpconfig.

8. Identify the SmartConsole hosts that can access the SmartCenter server.

   You can have as many SmartConsole clients on as many desktops as you desire. However, you need to provide the IP address or name of each client host to cpconfig before the clients can access the SmartCenter server.

   Specify at least one SmartConsole host. You can rerun cpconfig at any time to add additional client hosts.

9. Specify the name of a group for which you want to grant permissions. Enter return to specify no group.

10. As part of configuring the internal certificate authority, type random text at a random pace until you hear a beep.

    The timing latency between your keystrokes is used to generate cryptographic data. The VPN-1 Power and VPN-1 UTM gateways use certificates for secure internal communication (SIC) between the SmartCenter server and the enforcement modules.

11. Choose whether to save the fingerprint of the SmartCenter server to a file.
To save the fingerprint, type y and provide the name of the file.

The SmartCenter server fingerprint will be displayed the first time a user logs into the SmartCenter server from a particular SmartDashboard host. By comparing the fingerprint displayed with the fingerprint you saved at this step, the user can authenticate the identity of the SmartCenter server.

12. When cpconfig asks if you want to reboot the system, enter y.

After the system reboots, an initial firewall policy is installed. Unless you previously modified the initial policy, all remote access to the platform is blocked, except for Check Point SmartConsole clients. For information on how to regain remote terminal access or Network Voyager access, see “About the Initial Firewall Policy” on page 26.

Configuring a Distributed Deployment

In a distributed deployment, the SmartCenter server and the VPN-1 Power/UTM enforcement modules are installed on separate platforms.

To install a Smart Center server

Note
You cannot deploy a SmartCenter server on a flash-based (diskless) platform.

1. Log in to the host from a console or remote terminal connection.

2. At the command prompt, enter cpconfig.

The following text appears:

Welcome to Check Point Configuration Program
==============================================
Please read the following license agreement.
Hit 'ENTER' to continue...

Note
If the text does not appear when you enter cpconfig, you might need to log out of the command-line session and then log back in to set the environmental variables.

3. Press Enter to read the license agreement, and then enter y to accept it.

4. Specify which product you are installing: Check Point Power or Check Point UTM.

5. Enter the appropriate number to select a management-server installation:
   For Check Point UTM, enter 2 to select SmartCenter UTM.
   For Check Point Power, enter 2 to select the distributed option.

6. (Power installations only) Enter 2 to select SmartCenter.
7. (Power installations only) Specify whether this management server will be the primary or secondary server.

Enter 1 for primary if you:
- Are not using the Check Point Management High Availability feature.
- Are using the Check Point Management High Availability feature and this is the first SmartCenter server you are installing.

Enter 2 for secondary if you are using Check Point Management High Availability feature and this is the second SmartCenter server you are installing. This server will take over from the primary server should the primary server fail.

8. Enter y to add a license and fill in the license information, or enter n to complete the license information later.

9. Define an initial administrator name and password.

The initial administrator name and password you enter here allows you to log in to the SmartCenter server from the SmartDashboard. This administrator has full read/write permissions, allowing you to further add or modify administrators using the SmartDashboard.

Administrators you define with the SmartDashboard can be issued a certificate for authentication, which provides a more secure means of authentication than the simple username used for the initial administrator. Check Point recommends that once you log on to the SmartDashboard, you create a new administrator with full read/write permissions, generate a certificate for the new administrator, and delete the initial administrator created by cpconfig.

10. Identify the SmartConsole hosts that can access the SmartCenter server.

You can have as many SmartConsole clients on as many desktops as you desire. However, you need to provide the IP address or name of each client host to cpconfig before the clients can access the SmartCenter server.

Specify at least one SmartConsole host. You can rerun cpconfig at any time to add additional client hosts.

11. Specify the name of a group for which you want to grant permissions. Enter return to specify no group.

12. As part of configuring the internal certificate authority, type random text at a random pace until you hear a beep.

The timing latency between your keystrokes is used to generate cryptographic data. The VPN-1 Power and VPN-1 UTM gateways use certificates for secure internal communication (SIC) between the SmartCenter server and the enforcement modules.

13. Choose whether to save the fingerprint of the SmartCenter server to a file.

To save the fingerprint, type y and provide the name of the file.

The SmartCenter server fingerprint will be displayed the first time a user logs into the SmartCenter server from a particular SmartDashboard host. By comparing the fingerprint
displayed with the fingerprint you saved at this step, the user can authenticate the identity of the SmartCenter server.

14. When cpconfig asks if you want to start the installed products, enter y.

The SmartCenter server will be started, along with the other Check Point applications you enabled in Network Voyager. No initial firewall policy is installed.

To install a VPN-1 Power/UTM enforcement module

1. Log in to the host from a console or remote terminal connection.
2. At the command prompt, enter cpconfig.

The following text appears:

Welcome to Check Point Configuration Program
=============================================
Please read the following license agreement.
Hit 'ENTER' to continue...

Note
If the text does not appear when you enter cpconfig, you might need to log out of the command-line session and then log back in to set the environmental variables.

3. Press Enter to read the license agreement, and then enter y to accept it.

If you are installing the enforcement module on a flash-based platform, skip to step 7.
4. Specify which product you are installing: Check Point Power or Check Point UTM.
5. Enter the appropriate number to select a enforcement module installation:
   For Check Point UTM, enter 1 to select VPN-1 UTM Gateway.
   For Check Point Power, enter 2 to select the distributed option.
6. (Power installations only) Enter 1 to select VPN-1 Power Gateway or 5 to select VPN-1 Power Gateway and Log Server.
7. Enter y or n to the prompt:
   Is this a Dynamically Assigned IP Address gateway installation ? (y/n) [n] ?
8. If the gateway is a VRRP virtual router member or IP cluster member, enter y in response to the following prompt:
   Would you like to install a Check Point clustering product (CPHA, CPLS or State Synchronization)? (y/n) [n] ?
9. Enter y to add a license and fill in the license information, or enter n to complete the license information later.
10. Specify the name of a group for which you want to grant permissions. Enter return to specify no group.
11. As part of configuring the certificate authority, type random text at a random pace until you hear a beep. The timing latency between your keystrokes is used to generate cryptographic data. The VPN-1 Power and VPN-1 UTM gateways use certificates for secure internal communication (SIC) between the management server and the enforcement modules.

12. Enter an activation key of your own choosing that will be used to establish secure internal communication between the management server and this enforcement module. The activation key must be longer than four characters. When you use the SmartDashboard to initialize secure internal communications between the management server and this enforcement module, you will be asked to provide this activation key.

13. When cpconfig asks if you want to reboot the system, enter y. After the system reboots, an initial firewall policy is installed. Unless you previously modified the initial policy, all remote access to the platform is blocked, except for Check Point SmartConsole clients. For information on how to regain remote terminal access or Network Voyager access, see “About the Initial Firewall Policy” on page 26.

**Note**
On an IP265 configured to use the external flash for storing Check Point packages, the first reboot after the packages are installed can take as long as 10 minutes. This is normal: do not reboot your platform again until the first reboot completes successfully.

### Enabling SecureXL

**Note**
Starting with IPSO 4.2 and above, SecureXL is enabled by default on all platforms. If you upgrade to IPSO 4.2, SecureXL is either enabled or disabled by default depending on the state of SecureXL in your previous version of IPSO.

For all Nokia IP security platforms except the IP2250, SecureXL is disabled by default. Rerun the cpconfig utility to enable SecureXL.

**To enable SecureXL**

1. Log in to the host from a remote terminal or console connection.
2. At the command prompt, enter `cpconfig`.
3. Enter the number next to Enable Check Point SecureXL.
4. Enter y to enable SecureXL.
4 Installing SmartConsole NGX R62

This chapter describes how to install Check Point SmartConsole NGX R62 (the SmartCenter GUI) on a Microsoft Windows system. You can install SmartConsole on as many systems as you desire.

SmartConsole is a collection of clients. The clients include:

- **SmartDashboard**—used by the system administrator to define and manage the security policy. From this SmartConsole you can access many Check Point features and add-ons.
- **SmartView Tracker**—used for managing and tracking logs and alerts throughout the system.
- **SmartView Monitor**—used to monitor and generate reports on traffic on interfaces, VPN-1 Power and QoS modules, as well as on other Check Point system counters.
- **SmartUpdate**—used to manage and maintain a license repository.
- **SecureClient Packaging Tool**—used to define user profiles for SecuRemote/SecureClient clients.
- **Eventia Reporter**—used to generate reports for different aspects of network activity.
- **SmartLSM**—used for managing large numbers of ROBO Gateways using SmartCenter server.

**To install SmartConsole NGX R62 on a Windows platform**

1. Close any Check Point applications running on the Windows platform.

2. Download the SmartConsole NGX R62 software into a temporary folder on the Windows computer.
   
   The SmartConsole software is available at the Check Point Downloads Web site at http://www.checkpoint.com. Select VPN-1 Power/UTM and NGX R62 in the Download Selector. Then select Windows OS.

3. Unzip the file, and double-click setup.exe.
   
   The Installation Wizard opens. Click Next on each screen to accept the default values.

After you install SmartConsole, make sure that the SmartDashboard can connect to the SmartCenter server.
To test the connection

1. Double click on the SmartDashboard R62 icon.

   The following login window appears:

2. Enter the administrator username and password you specified when you configured the SmartCenter server with cpconfig.

3. In the SmartCenter server field, enter the IP address of the SmartCenter server.

   Select the Read Only option if you want to allow others access to the SmartCenter server while you view information.

4. Click OK.

   SmartDashboard connects to the SmartCenter server. Because this is the first time SmartDashboard has connected from this Windows host, it displays a Fingerprint Verification window:
5. Compare the fingerprint shown with the fingerprint created by cpconfig during the initial configuration of the SmartCenter server.

6. Click Approve if the fingerprints match.

Refer to the SmartCenter manual, available at the Check Point Documentation Downloads site at www.checkpoint.com, for more information on how to use SmartDashboard for creating managed objects, such as gateways, networks, and services, for creating policies, and for installing policies on VPN-1 Power or Check Point UTM gateways.
This section describes how to upgrade a Nokia IP security platform to Check Point NGX R62. For information on supported upgrade paths and on the interoperability of NGX R62 management with gateways running previous versions of Check Point software, see The Upgrade Guide for NGX R62 from Check Point.

**Note**
To upgrade to Check Point NGX R62, you must upgrade Check Point licenses for product versions that are earlier than NGX R60. Check Point recommends that you upgrade your licenses before you upgrade the software. See The Upgrade Guide for NGX R62 from Check Point for more information on how to upgrade your licenses.

You do not need to upgrade your licenses for product versions NGX R60 or later.

This section covers:
- Overview of the Upgrade Process
- Obtaining the Software
- Preparing an IP265 Platform
- Upgrading Security Platforms
- Installing HotFix Accumulators on Flash-based Platforms
- Reverting to Previous Check Point Versions

### Overview of the Upgrade Process

Upgrade the management server, GUI clients, and enforcement points in the following order:

1. Upgrade the SmartCenter server.
2. Install SmartConsole NGX R62 on the Microsoft Windows hosts. For information on how to install SmartConsole, see Chapter 4, “Installing SmartConsole NGX R62.”
3. Upgrade the VPN-1 Power or VPN-1 UTM gateways.

This chapter describes how to update Nokia IP security platforms to NGX R62. For information on upgrading other platforms, see the The Upgrade Guide from Check Point.
If you are upgrading IP clusters or VRRP virtual routers and can afford some network downtime, you can upgrade each gateway individually as described in this chapter. If, however, you need to perform an upgrade with zero downtime, consult the “Upgrading ClusterXL” chapter in *The Upgrade Guide* from Check Point for information on performing a zero-downtime upgrade.

**Obtaining the Software**

Before you begin the upgrade, download Nokia IPSO, if needed, and the Check Point NGX R62 applications to an FTP server on your server.

The latest builds of IPSO, their documentation and their release notes are available at the Nokia support Web site. You must be running IPSO 3.9 or later to upgrade to NGX R62. See the Nokia support Web site for current information on which IPSO releases are supported.

**Note**

On flash-based platforms, you can have a maximum of two IPSO images installed at a time.

The Check Point software, documentation, and release notes are available in the Downloads section of the Check Point Web site at http://www.checkpoint.com. What you should download depends on your type of platform:

- **Disk-based platforms:**
  - Comprehensive R62 wrapper for Nokia IPSO (IPSO_wrapper_R62.tgz)
    Use this file to upgrade the VPN-1 Power or VPN-1 UTM enforcement module or SmartCenter server (or both) on a Nokia IP security platform.
  - SmartConsole R62 (SmartConsole_R62_xxxxxxxxx_x_Win.zip)
    Use this package to install the Microsoft Windows SmartConsole GUIs. The package is available under the Windows OS in the Check Point Download selector for NGX R62.

- **Flash-based platforms:**
  - VPN-1 Power/UTM NGX R62 for flash-based platforms (fw1_R62_xxxxxxxxx_x_IPSO.tgz)
    Use this package to upgrade enforcement modules running on Nokia flash-based platforms.
  - CPInfo Tool NGX R62 for IPSO platforms (cpinfo_R62_xxxxxxxxx_x_IPSO.tgz)
  - SmartConsole R62 (SmartConsole_R62_xxxxxxxxx_x_Win.zip)
    Use this package to install the SmartConsole GUIs on Microsoft Windows hosts. The package is available under the Windows OS in the Check Point Download selector for NGX R62.
Preparing an IP265 Platform

To upgrade to NGX R62, you must have the IP265 platform already configured to use the external flash for storing packages. NGX R62 will not install on an IP265 that is not configured for optional disk storage of packages.

If your platform is not configured to use the external flash for packages, consult resolution ID 1350360 at the Nokia support Web site for instructions on how to configure your platform.

Upgrading Security Platforms

To perform the upgrades, you can use:

- Nokia Horizon Manager.
  
  If you are using Nokia Horizon Manager, skip the remainder of this chapter and consult the Nokia Horizon Manager documentation.

- Nokia Network Voyager, the IPSO CLI, or the newpkg command. This section contains detailed procedures for Network Voyager and the newpkg command. For the CLI, see the CLI Reference Guide for the IPSO version you are using.

To upgrade a security platform

1. Upgrade to Nokia IPSO 3.9 or a later supported version, if needed. See the Getting Started Guide and Release Notes for your IPSO version for information on how to upgrade IPSO.

   Note
   You cannot run Check Point NGX R62 on a version of Nokia IPSO that is earlier than IPSO 3.9.

2. Reboot the platform.

3. Make sure that the current version of the Check Point software is enabled.

4. Install the NGX R62 package as an upgrade:
   - On disk-based platforms, install the comprehensive wrapper package.
   - On flash-based platforms, separately install the VPN-1 Power/UTM and CPinfo packages, installing the VPN-1 Power/UTM package first.

5. Rerun cpconfig to add a local license if desired and to confirm the configuration.

6. Reboot the security platform if it hosts an enforcement module.
To upgrade by using newpkg

Note
On flash-based platforms:

If you plan to install from the local file system (that is, download the package to the platform first and then install from that directory), Nokia recommends that you use /var/tmp or a directory you create in /var as your installation directory. The installation files will be automatically deleted when you reboot the system, freeing up space in flash memory.

If you plan to install from an FTP server, Nokia recommends that you delete the contents of /preserve/opt/tmp before and after you perform the installation. newpkg uses this directory to store packages while installing them. Use the following command to delete the directory contents:

```
rm -R /preserve/opt/tmp
```

1. Log in to the platform with a console connection.
2. Enter `newpkg` to start the package installation script.
   
   The following options appear:
   1. Install from CD-ROM.
   2. Install from anonymous FTP server.
   3. Install from FTP server with user and password.
   4. Install from local filesystem.
   5. Exit new package installation.
3. Enter the number (1 through 4) next to the installation method to use, or enter 5 to exit.
4. The installation script guides you through the rest of the upgrade process.
   - If you are installing from your current working directory in the local filesystem, you can enter a period (.) when asked for the pathname to the packages.
   - Make sure that you select option 2 (Upgrade from an old package) when the name of your package is displayed.
5. On flash-based platforms, repeat steps 2 through 4 to install CPinfo after you have installed VPN-1 Power/UTM.
6. When the upgrade is finished, log off, then log back on to set the environmental variables.
7. To confirm the upgrade, see the procedure “To confirm the installation” on page 42.

To upgrade by using Nokia Network Voyager

1. In the Network Voyager, navigate as follows:
   - IPSO 3.9: System Configuration > Manage Installed Packages > FTP and Install Packages
   - IPSO 4.1 or later: Configuration > System Configuration > Packages > Install Package
2. Enter the host name or IP address of the FTP site where you downloaded the package.
3. Enter the directory name where the file reside on the FTP site.
4. Enter the user account and password to use when you connect to the FTP site and click
Apply.
   If you leave these fields empty, the anonymous account is used.

   **Note**
   If you specify a user account and password, you must re-enter the password whenever
   you change the FTP site, FTP directory, or FTP user on future requests. A list of files
   from the specified FTP directory appears in the Site Listing field.

5. Select a file from Site Listing, then click Apply.
   After the download completes, the package appears in the Select a Package to Unpack box.

6. Select the package, then click Apply.
   The package is unpacked into the local file system.

   **Note**
   The version field in the package information always shows 3.9, regardless of the actual
   IPSO version.

7. Click the Click here to install/upgrade /opt/packages/packagename link.

8. Click the radio button next to Upgrade and then select the package to upgrade from. Click
   Apply.
   Wait until Network Voyager refreshes this page with a link to the Manage Packages screen.

9. Click the link to return to the Manage Packages screen.
   If you are installing the comprehensive wrapper, the installation of the applications within
   the comprehensive wrapper can take several minutes to complete: as long as 10 to 20
   minutes on some platforms.
   During the initial installation phase, the wrapper appears under the Security Applications
   heading. If you wait several minutes and click Apply, a warning message appears telling you
   that the installation is still in progress as the wrapper continues to unpack and install the
   Check Point applications in the package.
   You can click Apply to refresh the page and monitor the installation process. When the
   installation is complete, the warning message disappears and the Check Point NGX R62
   application packages appear in the installed packages section.
   If you are installing individual packages on a flash-based platform, repeat steps 1 through 9
   to install CPinfo after you install VPN-1 Power/UTM.

10. Confirm the upgrade is correct as described in “To confirm the installation” on page 42.
To confirm the installation

1. On the Manage Packages page in Network Voyager, confirm that the Check Point VPN-1 Power/UTM NGX R62 package appears under Security Applications and is enabled.
   If the package is not enabled, click On, and then click Apply and Save.

2. Confirm that the Check Point CPinfo package under Applications is enabled.
   If the package is not enabled, click On, and then click Apply and Save.

3. Enable any of the other Check Point packages you want to have enabled and click Apply and Save.

4. If you are logged onto the platform with a IPSO shell session, log off and then log on again.
   When you enable the packages, Network Voyager sets new shell environmental variables that are necessary for executing firewall commands. However, they do not take effect until the next time you log on. For this reason, you need to log off after you enable the packages.

5. Rerun cpconfig to confirm the installation and to add a new license, if desired.

6. Reboot the platform if it hosts an enforcement module.

---

**Note**
Starting with NGX R60, the SVN Foundation, FloodGate-1, and Policy Server components are no longer installed as separate application packages. Instead, they are included as part of the VPN-1 Power/UTM package.

---

**Installing HotFix Accumulators on Flash-based Platforms**

Nokia recommends you follow these guidelines when installing HFAs on flash-based platforms:

- Do not download the HFAs to your home directory. Files in user home directories are preserved after reboots and consume valuable space in flash memory. Instead, download to /var/tmp or create a directory in /var and install the HFA from there. The installation files will be automatically deleted when you reboot after installing the HFA.

- After you extract the HFA files from the archive.tgz file, delete the archive file and then install the HFA as described in the HFA release notes.

- The IP265 platform must be configured with an external flash (optional disk) for type “Packages” for HFA installation.

---

**Reverting to Previous Check Point Versions**

If you are reverting to an NG or NGX version that is compatible with your current IPSO version, deactivate the NGX R62 products, making sure to deactivate VPN-1 Power/UTM last, and then reactivate the previous product versions.

If you need to revert to a previous Check Point version that is not supported by your current IPSO version, use the following procedure.
To revert to a previous version

1. Using the IPSO Image Management page in Network Voyager, select the previous IPSO image and reboot.
   When you revert to the previous image, IPSO automatically reverts to using the saved configuration set associated with that image.

2. On the Manage Packages page, confirm that the previous versions of Check Point packages are enabled and the NGX R62 versions are disabled.

---

**Note**

On flash-based platforms, the NGX R62 packages will no longer appear in the Manage Packages page since they were never part of the previous configuration set.

---

If, after reverting, you wish to upgrade again to NGX R62, you will need to manually reselect the correct configuration set as described in the following procedure.

To upgrade again to NGX R62

1. Using the IPSO Image Management page in Network Voyager, select the IPSO image that supports NGX R62 and reboot.

2. Using the Configuration Set Management page, select the configuration set associated with that image and then click Save.
   Network Voyager logs you out and you will have to log in again.

3. Reboot the platform.

4. On the Manage Packages page, confirm that the previous versions of Check Point packages are disabled and the NGX R62 versions are enabled.