



# Getting Started Guide and Release Notes for Nokia IPSO 6.1

Part No. N450000851 Rev 002

Build 038

Published February 2009

## **COPYRIGHT**

©2009 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.

090101

## Nokia Contact Information

### Corporate Headquarters

---

|                     |   |
|---------------------|---|
| <b>Web Site</b>     | <a href="http://www.nokia.com">http://www.nokia.com</a>                 |
| <b>Telephone</b>    | 1 914 368 0400  |
| <b>Mail Address</b> | Nokia Inc.<br>102 Corporate Park Drive<br>White Plains, NY 10604<br>USA |

---

### Regional Contact Information

---

|  |  |  |
|--|--|--|
| <b>Americas</b>                                | Nokia Inc.<br>102 Corporate Park Drive<br>White Plains, NY 10604<br>USA          | Tel: 1 877 997 9199<br>E-mail: <a href="mailto:usa@nokiaforbusiness.com">usa@nokiaforbusiness.com</a>  |
| <b>Europe,<br/>Middle East,<br/>and Africa</b> | Nokia House, Summit Avenue<br>Southwood, Farnborough<br>Hampshire GU14 ONG<br>UK | Tel: (UK) 44 161 601 8908<br>Tel: (France) 33 170 708 166<br>Tel: (Middle East, Africa, Dubai) 971 4 3697600<br>E-mail: <a href="mailto:europe@nokiaforbusiness.com">europe@nokiaforbusiness.com</a><br>E-mail: <a href="mailto:mea@nokiaforbusiness.com">mea@nokiaforbusiness.com</a> |
| <b>Asia-Pacific</b>                            | 438B Alexandra Road<br>#07-00 Alexandra Technopark<br>Singapore 119968           | Tel: 603 9145 1032<br>E-mail: <a href="mailto:asia@nokiaforbusiness.com">asia@nokiaforbusiness.com</a>   |

---

### Nokia Global Technical Assistance Center

|          |   |                |
|----------|---|----------------|
| Web Site | <a href="https://support.nokia.com">https://support.nokia.com</a> |                |
| Voice    | Americas  | 1 888 361 5030 |
|          | Europe, Middle East, Africa                                       | 44 1252 868900 |
|          | Asia-Pacific  | 65 6723 2999   |
|          | International   | 1 613 271 6721 |

### Non-Technical Support

For non-technical support issues, including your Nokia Support Agreement, licensing, and Web site access, use the following contact information:

E-mail: [es.service@nokia.com](mailto:es.service@nokia.com)

---

080919



# Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>What's New in Nokia IPSO 6.1 Build 038</b>  | <b>9</b>  |
|          | Enhancements and Fixes in IPSO 6.1 Build 038   | 9         |
|          | Supports 10Gb and 1Gb Ethernet Cards           | 10        |
|          | 10 Gigabit Ethernet Cards                      | 10        |
|          | 1 Gigabit Ethernet Cards                       | 11        |
|          | VRRP Enhancement for Load Balancers            | 11        |
|          | Enhancement for Configuration Summary Tool     | 12        |
|          | Enhancement for IP Broadcast Helper            | 12        |
|          | Enhancement for ICMP Reply Throttling          | 13        |
|          | Enhancement for Argentina Time Zone Changes    | 13        |
|          | Fix for Security Vulnerability                 | 13        |
|          | Fix for Issue with UDP Connection Buildup      | 13        |
|          | Fix for Copper Ethernet Link Issue             | 14        |
|          | Fix for 25 Day Timer Issue                     | 14        |
|          | Fix for Cluster Hashing                        | 14        |
|          | Fix for Single-Node Cluster in Forwarding Mode | 15        |
|          | Fix for Multicast Transport                    | 15        |
|          | Fix for High CPU Utilization Problem           | 15        |
|          | Fix for ADP Dashboard Display Issue            | 16        |
|          | Fix for Platform Status LED                    | 16        |
| <b>2</b> | <b>New Features in Nokia IPSO 6.1</b>          | <b>17</b> |
|          | Performance Monitoring                         | 18        |
|          | Connection Dashboard                           | 18        |
|          | Connection Map Dashboard                       | 19        |
|          | Traffic Dashboard                              | 20        |

|  |    |
|--|----|
| Forwarding Dashboard . . . . .                               | 20 |
| Interface Dashboard . . . . .                                | 20 |
| System Dashboard . . . . .                                   | 21 |
| ADP Dashboard . . . . .                                      | 21 |
| Custom Dashboard . . . . .                                   | 21 |
| Support for Netflow Services . . . . .                       | 21 |
| Defining Flows. . . . .                                      | 22 |
| Flow Records . . . . .                                       | 23 |
| Enhancement for ACL Rules . . . . .                          | 23 |
| High-Availability Enhancements. . . . .                      | 24 |
| HA Voyager. . . . .  | 24 |
| Configuring VRRP with HA Voyager . . . . .                   | 25 |
| IP Clustering Enhancements. . . . .                          | 26 |
| Simplified Clustering. . . . .                               | 26 |
| Cluster Topologies . . . . .                                 | 26 |
| Advanced Cluster Tuning. . . . .                             | 27 |
| ISP Redundancy Supported. . . . .                            | 27 |
| Configuration Migrator . . . . .                             | 27 |
| IPSO Automated Configuration . . . . .                       | 28 |
| Enhanced Configuration Summary Tool . . . . .                | 29 |
| Enhancement for Increased Network Voyager Security . . . . . | 32 |
| Routing Enhancements . . . . .                               | 32 |
| OSPF and BGP Graceful Restart Helper . . . . .               | 32 |
| Enhancements for RIP and OSPF Route Tags. . . . .            | 33 |
| Support for USB Modem . . . . .                              | 34 |
| Enhancement for Firewall Kernel Tuning. . . . .              | 34 |
| Changes to Upgrade and Installation Process. . . . .         | 36 |
| Supported Platforms . . . . .                                | 36 |
| Supported Memory Configurations . . . . .                    | 37 |
| Supported Applications . . . . .                             | 39 |
| Detailed Comparison with IPSO 4.2 and 6.0 . . . . .          | 39 |

|          |  |           |
|----------|--|-----------|
| <b>3</b> | <b>Performing the Initial Configuration</b>              | <b>47</b> |
|          | Using DHCP to Configure the System                       | 47        |
|          | Configuring Your DHCP server                             | 48        |
|          | Running the DHCP Client on the Nokia System              | 49        |
|          | Using the Console to Configure the System                | 50        |
|          | Performing the Configuration                             | 51        |
|          | Performing Additional Configuration.                     | 54        |
|          | Using Nokia Network Voyager                              | 54        |
|          | Using the IPSO CLI                                       | 54        |
|          | Using an SSH Client                                      | 55        |
|          | Disabling Telnet   | 56        |
|          | Disabling SSH  | 57        |
| <b>4</b> | <b>Upgrading to Nokia IPSO 6.1</b>                       | <b>59</b> |
|          | Changes to Upgrade and Installation Procedures           | 59        |
|          | Boot Security  | 60        |
|          | Downloading Nokia IPSO and Related Files                 | 61        |
|          | Using Nokia Horizon Manager to Install IPSO and Packages | 61        |
|          | Before You Install IPSO 6.1                              | 62        |
|          | IP2450 Might Require BIOS Upgrade                        | 62        |
|          | If You Use Link Redundancy Before Upgrading to 6.1       | 63        |
|          | Change to rc.local Support                               | 64        |
|          | Verify Free Space in Root Partition                      | 64        |
|          | Fresh Installation on a 1 GB Flash-Based Platform        | 65        |
|          | Putting the ipso.tgz file on Your Platform               | 65        |
|          | Verifying File Integrity                                 | 66        |
|          | Installing Nokia IPSO 6.1                                | 67        |
|          | Adding an IPSO Image Using Voyager                       | 68        |
|          | Adding an IPSO Image from the Command Shell              | 68        |
|          | Overwriting Existing Images (Fresh Installation)         | 71        |
|          | Performing a Fresh Installation                          | 72        |
|          | Installing IPSO 4.x                                      | 75        |

|  |           |
|--|-----------|
| Performing a Fresh Installation . . . . .                          | 75        |
| Installing and Activating Packages . . . . .                       | 78        |
| Using Nokia Network Voyager to Install Packages . . . . .          | 79        |
| Activating Packages . . . . .                                      | 81        |
| Using the newpkg Command . . . . .                                 | 82        |
| Upgrading Check Point NGX . . . . .                                | 84        |
| <b>5 Limitations and Configuration Tips . . . . .</b>              | <b>85</b> |
| Configuration Tips . . . . .                                       | 85        |
| Authentication Change . . . . .                                    | 86        |
| Cabling an IP2450 Platform . . . . .                               | 86        |
| Use Half Duplex with Hubs . . . . .                                | 86        |
| Optional Disks Erased when Selected . . . . .                      | 86        |
| Configuring Remote Core Dump Servers . . . . .                     | 87        |
| Complete All Fields When Creating Users . . . . .                  | 87        |
| Providing User Access to Monitor Pages . . . . .                   | 87        |
| SNMP User privpassphrase Option Inaccurately Displayed . . . . .   | 87        |
| Audit Log Setting Not Permanently Saved . . . . .                  | 88        |
| Terminal Emulator Display Configuration . . . . .                  | 88        |
| Do Not Insert or Remove PC Card During Boot . . . . .              | 89        |
| Route Maps with BGP Confederations . . . . .                       | 89        |
| Workaround to Disable ifwd Daemon . . . . .                        | 89        |
| Limitations . . . . .  | 90        |
| PBR Does Not Work with VPNs . . . . .                              | 90        |
| Issue with UDLD Under Heavy Traffic . . . . .                      | 90        |
| Issue with ADP Interface LEDs . . . . .                            | 90        |
| Issue with IKE Acceleration and IP690 ADP Module . . . . .         | 90        |
| Error Message When Deleting NGX R65 for IPSO 6.0 Package . . . . . | 91        |
| Silent Mode Support in newpkg . . . . .                            | 91        |



# 1

## What's New in Nokia IPSO 6.1 Build 038

Nokia is pleased to announce Nokia IPSO 6.1 Build 038, a new build of the IPSO 6.1 operating system used on Nokia IP security platforms.

This chapter describes the enhancements and fixes that Nokia has added to IPSO 6.1 since its original release. For information about the new features in the original release, see Chapter 2, [New Features in Nokia IPSO 6.1](#) on page 17.

For information about how to download IPSO 6.1 and other items from the Nokia customer support Web site, see [“Downloading Nokia IPSO and Related Files”](#) on page 61.

### Enhancements and Fixes in IPSO 6.1 Build 038

IPSO 6.1 Build 038 includes the following enhancements and fixes:

- [Supports 10Gb and 1Gb Ethernet Cards](#)
- [VRRP Enhancement for Load Balancers](#)
- [Enhancement for Configuration Summary Tool](#)
- [Enhancement for IP Broadcast Helper](#)
- [Enhancement for ICMP Reply Throttling](#)
- [Enhancement for Argentina Time Zone Changes](#)
- [Fix for Security Vulnerability](#)

- [Fix for Issue with UDP Connection Buildup](#)
- [Fix for Copper Ethernet Link Issue](#)
- [Fix for 25 Day Timer Issue](#)
- [Fix for Cluster Hashing](#)
- [Fix for Single-Node Cluster in Forwarding Mode](#)
- [Fix for Multicast Transport](#)
- [Fix for High CPU Utilization Problem](#)
- [Fix for ADP Dashboard Display Issue](#)
- [Fix for Platform Status LED](#)

The numbers in angle brackets after the headings in the following sections are the tracking numbers for the issues in Nokia's internal database of problem resolutions. Reference the appropriate number if you contact Nokia about any of these items.

## Supports 10Gb and 1Gb Ethernet Cards

IPSO 6.1 Build 038 supports the release of 10 Gigabit Ethernet and 1 Gigabit Ethernet cards as optional add-ons for the following Nokia network security platforms:

- IP2450
- IP1280
- IP690

These cards deliver high throughput for network environments that do not require the specialized acceleration offered by Nokia ADP modules.

### 10 Gigabit Ethernet Cards

Nokia offers new dual-port 10 Gigabit Ethernet cards in two versions:

- Network interface card with XMC connectors for Nokia IP2450 and Nokia IP1280
- Network interface card with PMC connectors for Nokia IP690

Both versions include sockets that accept interchangeable SFP+ transceivers.

These cards can help your network meet the increasing demands of transporting content types such as video and VoIP or accommodate virtualization.

## 1 Gigabit Ethernet Cards

Nokia offers new four-port 1 Gigabit Ethernet cards in two versions:

- Network interface card for Nokia IP1280 and Nokia IP2450 with integrated RJ-45 connectors
- Network interface card for Nokia IP1280 and Nokia IP2450 with sockets that accept interchangeable SFP transceivers available in 1000Base-T, 1000Base-SX, and 1000Base-LX versions

These cards implement a new design that leverages the latest technological advances and connect directly to the PCI-e data bus to improve the speed and efficiency of moving packets between the interfaces and the multiple CPU cores.

## VRRP Enhancement for Load Balancers [<PR 81562>](#)

The Virtual Router Redundancy Protocol (VRRP) uses virtual MAC addresses to ensure that traffic continues to flow if the VRRP master fails. In the event of a failure, the new VRRP master takes ownership of the virtual IP and MAC addresses, and attached routers send traffic to the new master.

IPSO uses the virtual MAC address as the source MAC for VRRP protocol traffic and uses the “real” (physical) MAC address as the source for all other traffic. Some load balancing devices cache the physical MAC address information for optimization purposes and continue to send traffic to that address even if the associated virtual router fails, which causes the traffic to be dropped.

IPSO 6.1 Build 038 includes the Source from Virtual MAC option, which you can enable to prevent this problem from occurring. This option is available on the Legacy VRRP Configuration Voyager page for monitored-circuit VRRP and VRRPv2. The option is not available if you use simplified monitored-

circuit VRRP or HA Voyager (which requires simplified monitored-circuit VRRP).

When you enable the Source from Virtual MAC option for an interface, all the traffic sent from the interface uses the virtual MAC address as the source MAC. (When the option is disabled—the default setting—only VRRP protocol traffic uses the virtual MAC address as the source. The physical MAC address is used as the source for all other traffic.) Enabling the option causes attached devices to send all traffic to the virtual MAC, so traffic continues to flow when a new master assumes ownership of the virtual MAC.

## Enhancement for Configuration Summary Tool [<PR 83276>](#)

If you open support case with Nokia, you might be asked to provide an ECST file. To create this file, you use the Enhanced Configuration Summary Tool (ECST), which allows you to capture your current IPSO configuration, log files, core dumps and other information in a single file.

With IPSO 6.1 Build 038, ECST provides more data for analysis by capturing Accelerated Data Path (ADP) kernel and core files that the system dumps when an ADP subsystem crashes. The file names begin with `kcore` and `kaza`, as in the following examples:

```
kcore-uls1-1.23.2009-014731.Z  
kaza.perf_g-uls1-1.23.2009-014731.Z
```

## Enhancement for IP Broadcast Helper [<PR 82402>](#)

You can use IPSO's IP Broadcast Helper to relay broadcast UDP packets as unicasts to one or more remote servers. With IPSO 6.1 Build 033, the maximum packet size for UDP packets relayed by this feature is 1480 bytes. With Build 038, IP Broadcast Helper can relay packets as large as 16000 bytes without fragmenting them.

## Enhancement for ICMP Reply Throttling <PR 83729>

To protect networks, IPSO 6.1 Build 033 throttles ping replies that exceed certain limits. Because this rate limiting might affect other network devices that use ping for health check purposes, Build 038 lets you disable the throttling by entering the following command at the IPSO shell prompt:

```
ipsctl -w net:ip:icmp:ratelimit:enable disable
```

To reenable the rate limiting function, enter

```
ipsctl -w net:ip:icmp:ratelimit:enable enable
```

## Enhancement for Argentina Time Zone Changes <PR 81415>

IPSO 6.1 Build 038 includes an enhancement to support recent time zone changes in Argentina.

## Fix for Security Vulnerability <PR 82357>

IPSO 6.1 Build 033 is vulnerable to the issue described at <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5162>.

Build 038 fixes this problem.

## Fix for Issue with UDP Connection Buildup <PR 81678>

Nokia network security platforms running IPSO 6.1 Build 033 can drop UDP traffic as a result of a large number of UDP connections being stored in the firewall connection table. This can occur even when the load on the system is light and can happen with all UDP traffic, but it is most likely to affect DNS packets. When the issue occurs with DNS traffic, it can cause name resolution failures and long delays in connection establishment.

With Build 038 you can prevent this problem from happening by configuring the system using `ipsctl` commands. See Knowledge Base Resolution

1513808 on the customer support site (<https://support.nokia.com>) for more information about this issue and how to configure your system to prevent it.

## Fix for Copper Ethernet Link Issue <PR 72981>

If a Nokia network security platform running IPSO 6.1 Build 033 restarts, any links that use copper Ethernet might not be reactivated after the reboot. This issue is most likely to occur with the IP390 but can occur with any platform running IPSO 6.1 Build 033. It does not occur with fiber optic links.

Build 038 fixes this problem.

## Fix for 25 Day Timer Issue <PRs 81927, 82978>

Nokia network security platforms running IPSO 6.1 Build 033 can experience problems after 25 days of continuous operation. After running for this length of time, platforms might drop traffic, hang, or experience other issues related to incorrect timer scheduling.

Build 038 fixes this problem.

## Fix for Cluster Hashing <PR 81976>

When you use IP clustering for high availability, you set the interface hash option to configure the manner in which IPSO balances connections among cluster nodes. If you use NAT in the protected networks and want to force connections to be symmetric (one cluster node handles both sides of the connection), you should configure these options as indicated below:

- For external cluster interfaces, use the on-src-ip option.
- For internal cluster interfaces, use the on-dest-ip option.

You might want to do this for performance reasons—supporting asymmetric connections requires more packets to be sent to the firewall, and this can have a cumulative effect on performance.

These options do not work correctly in IPSO 6.1 Build 033, with the result that connections are forced to be asymmetric instead of symmetric.

Build 038 fixes this problem.

## **Fix for Single-Node Cluster in Forwarding Mode** <PRs 81454, 81778>

If you have a single-node cluster with forwarding mode enabled on a system running IPSO 6.1 Build 033, a problem can occur if an interface is deactivated and reactivated or disconnected and reconnected. In this situation, IPSO stops sending gratuitous ARP replies from the affected interface, which can cause the ARP table entry for the interface to be deleted from an attached network switch. If this happens, traffic will not be sent to that interface.

This problem occurs only with single-node clusters and only if the cluster uses forwarding mode. Build 038 fixes the issue.

## **Fix for Multicast Transport** <PR 82555>

The only multicast transport protocol supported by IPSO 6.1 Build 033 is UDP. Using any other protocol for this purpose can cause systems running this build to panic and crash.

With Build 038, you can use any protocol other than TCP to transport multicast traffic.

## **Fix for High CPU Utilization Problem** <PR 76602>

If you configure an interface on a platform running IPSO 6.1 Build 033 but do not physically connect the interface to complete the link, a problem can occur that causes high CPU utilization even if no traffic is flowing through the system. Build 038 fixes this problem. To prevent the issue on a platform running Build 033, make sure that all the configured interfaces are physically connected and the links are active.

## Fix for ADP Dashboard Display Issue <PR 83578>

IPSO 6.1 provides a detailed view of your system's performance through the performance monitoring graphs you can access by clicking Monitor > Performance Monitoring on the Network Voyager navigation tree. On platforms running IPSO 6.1 Build 033, the ADP CPU Utilization graphs might incorrectly indicate show negative values.

This is a display issue only and is fixed in Build 038.

## Fix for Platform Status LED <PRs 65714, 82702>

If you install IPSO 6.1 Build 033 on a Nokia network security platform, the green status LED on the front panel might not illuminate after the installation is complete. This does not indicate any problem with the functionality of the platform.

If you install IPSO 6.1 Build 038, the green status LED does illuminate.



# 2

## New Features in Nokia IPSO 6.1

Nokia IPSO 6.1 includes the following new features and enhancements:

- [Performance Monitoring](#)
- [Support for Netflow Services](#)
- [Enhancement for ACL Rules](#)
- [High-Availability Enhancements](#)
- [Configuration Migrator](#)
- [IPSO Automated Configuration](#)
- [Enhanced Configuration Summary Tool](#)
- [Enhancement for Increased Network Voyager Security](#)
- [Routing Enhancements](#)
- [Support for USB Modem](#)
- [Enhancement for Firewall Kernel Tuning](#)

This chapter also contains information on the following topics:

- [Changes to Upgrade and Installation Process](#)
- [Supported Platforms](#)
- [Supported Memory Configurations](#)
- [Supported Applications](#)
- [Detailed Comparison with IPSO 4.2 and 6.0](#)

## Performance Monitoring

IPSO 6.1 provides a detailed and comprehensive view of your system's performance by allowing you to monitor a variety of historical information presented in graphical format. You can configure the graphs to show a wide range of time periods.

Use the information provided by this feature to tune your system for optimum performance, troubleshoot difficult performance issues, or simply confirm that traffic patterns are as expected. For example, you can compare how much of your traffic has been accelerated by SecureXL versus the amount that has been sent to the firewall for processing and see how much traffic has been forwarded by Nokia Accelerated Data Path (ADP) interfaces versus non-ADP interfaces.

The performance monitoring graphs are organized into configurable dashboards that you access by clicking Monitor > Performance Monitoring on the Network Voyager navigation tree. (The dashboards replace the Voyager pages that you access in previous IPSO versions by clicking Monitor > Reports.)

The following sections describe the new dashboards and their component graphs.

---

**Note**

You will not be able to display historical performance data captured by a previous IPSO release after you upgrade to IPSO 6.1. If you want to preserve this data, do so before you upgrade by using Network Voyager to display the data in delimited format and copying it into a spreadsheet or other application.

---

## Connection Dashboard

- **Connection Life histogram:** Displays the number of connections within a configurable time and their lifetimes in IPSO. The lifetime of a connection is the amount of time it occupies IPSO memory.

- **Transaction Size histogram:** Displays the transaction sizes associated with different connections within a configurable time. The transaction size is the number of bytes exchanged in the context of a connection from the start to the end of the connection.
- **Templates vs. Non-Templates:** Displays the percentage of connections created by SecureXL templates within a configurable time. You can use this information to help you define a firewall policy so that more connections are created by templates (and are therefore accelerated).
- **Transactions vs. Connections:** Displays the rates of connection and transaction creation within a configurable time. For TCP, connection creation is defined as the arrival of a SYN packet, and transaction creation is defined as the completion of 3-way handshake. For non-TCP connections, connection and transaction creation occurs at the same rate.

## Connection Map Dashboard

- **Accelerated Connections Map:** Displays the total number of connections within a configurable time and the number that were accelerated. The difference between the total number of connections and the number of accelerated connections gives the number of connections for which every packet was inspected by the firewall. Accelerated connections are further classified as connections accelerated by ADP and connections accelerated by IPSO.
- **VPN Connections Map:** Displays the total number of connections within a configurable time and the number that required VPN services.
- **NAT Connections Map:** Displays the total number of connections within a configurable time and the number that required NAT services.
- **TCP Connections Map:** Displays the total number of connections within a configurable time and the number of TCP connections. The difference between total connections and TCP connections gives the number of non-TCP connections, such as UDP, ICMP, etc.

## Traffic Dashboard

- **IPSO Packet Size Map:** Displays the distribution of packet sizes forwarded by IPSO within a configurable time. This information is helpful in understanding which packet sizes are dominant.
- **ADP Packet Size Map:** This graph is present only on platforms on which an ADP module is detected. It displays the distribution of packet sizes that were forwarded by ADP interfaces. This information is helpful in understanding which packet sizes are dominant in traffic transiting ADP interfaces.

## Forwarding Dashboard

- **Accelerated Traffic Map:** Displays the total number of packets that were forwarded by IPSO and the number of packets that were accelerated by IPSO within a configurable time. The difference between the total number of packets and the number of accelerated packets is the number of packets that were forwarded to the firewall.
- **VPN Traffic Map:** Displays the total number of packets that were forwarded by IPSO and the number of packets that required VPN services within a configurable time. This information is helpful in understanding the percentage of traffic that requires VPN services.
- **NAT Traffic Map:** Displays the total number of packets that were forwarded by IPSO and the number of packets that required NAT services within a configurable time. This information is helpful in understanding the percentage of traffic that requires NAT services.

## Interface Dashboard

- **Packet Throughput:** Displays the rates of incoming and outgoing packets on a given interface within a configurable time.
- **Byte Throughput:** Displays the rates of incoming and outgoing bytes on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.

- **Multicast Throughput:** Displays the rates of incoming and outgoing multicast packets on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.
- **Broadcast Throughput:** Displays the rates of incoming and outgoing broadcast packets on a given interface within a configurable time. This information is helpful in determining if a link is reaching its capacity.

## System Dashboard

- **CPU Utilization:** Displays the CPU utilization for all the CPU cores within a configurable time.
- **Memory Utilization:** Displays the memory utilization in IPSO within a configurable time.

## ADP Dashboard

This dashboard displays the number of packets that were forwarded by IPSO and number of packets that were forwarded by the ADP subsystem within a configurable time. You can also see the average and maximum number of buffers utilized at the interface layer in incoming and outgoing directions within a configurable time. This information is helpful in understanding the value provided by ADP modules.

## Custom Dashboard

Use this dashboard to create custom profiles that include your choice of performance graphs. After you have created profiles, click the Custom Dashboard link again to select a profile to display.

## Support for Netflow Services

IPSO 6.1 introduces support for Netflow services, which you can use to collect information about network traffic patterns and volume. To provide this

information, IPSO tracks network “flows.” A flow is a unidirectional stream of packets that share a given set of characteristics. Click Configuration > Traffic Management > Netflow to access the Netflow Configuration page.

IPSO exports information about flows in flow records. To gather and analyze flow records, you must export them to a Netflow collector. Nokia has tested the following collectors:

- NetFlow Analyzer (AdventNet, Inc.): supports Versions 5 and 9
- Scrutinizer (Plixer International): supports Versions 5 and 9

## Defining Flows

You control how IPSO defines flows by using metering modes:

- Flows mode: If you use this mode, a flow is any sequence of packets that share
  - Source and destination IP addresses
  - Source and destination port numbers
  - IP protocol

When you use flows mode, IPSO exports each flow in an individual flow record.

This mode requires that a firewall is running and SecureXL is enabled.

---

### Note

When you enable flows mode, IPSO automatically reduces the concurrent connection capacity by 25 percent. If you later disable flows mode, IPSO automatically increases the connection capacity to the previous value. When you enable or disable this mode, you should make the same adjustment in Check Point’s SmartDashboard application.

---

- ACL mode: If you use this mode, you define flows by configuring ACL rules. Traffic that matches a rule is a flow. (You must also enable the Netflow Metering option for any rule that you want to use for this

purpose.). When you use ACL mode, all the traffic that matches a rule is exported in one flow record.

You can use both modes simultaneously. In this case, traffic that matches an ACL rule is reflected in a Flows mode flow and also in an ACL mode flow.

## Flow Records

You configure IPSO to export flow records using the formats specified by Cisco for NetFlow Versions 5 and 9. (Version 9 is specified in RFC 3954.) Regardless of which export format you choose, IPSO exports values for the following fields:

- source IP address
- source subnet mask (used only when record is generated by an ACL flow)
- destination IP address
- destination subnet mask (used only when record is generated by an ACL flow)
- source port
- destination port
- input physical interface index (defined by SNMP)
- output physical interface index (defined by SNMP)
- packet count for this flow
- byte count for this flow
- start of flow timestamp (FIRST\_SWITCHED)
- end of flow timestamp (LAST\_SWITCHED)
- IP protocol number

## Enhancement for ACL Rules

When you create an access control list (ACL), you populate the ACL with rules that take configurable actions when traffic matches a pattern specified by the rule. With IPSO 6.1, one of the actions you can configure for a rule is

Bypass-FW, which causes ICMP traffic to bypass the firewall. You might use this action to prevent disruptive traffic that always comes from a known and trusted source from reaching the firewall.



---

**Caution**

Lengthy ACLs can degrade performance because all traffic first must be compared to the ACL. Use ACLs with caution.

---

## High-Availability Enhancements

IPSO 6.1 includes new features and enhancements for the high-availability configurations that you can create using Nokia's implementation of the Virtual Router Redundancy Protocol (VRRP).

### HA Voyager

IPSO 6.1 introduces a new approach that you can use to create and manage VRRP configurations. The main VRRP configuration page now includes a link for creating an HA VRRP configuration. Using this option allows you to configure and manage all the members of a VRRP group in a centralized way by using HA Voyager on one system. (When you use HA Voyager to configure VRRP, you create a simplified monitored-circuit configuration.)

When you create an HA VRRP configuration, Voyager displays a new tab (labeled HA Voyager) in the navigation tree. Clicking this tab displays many of the same links that appear under the System tab in the navigation tree. When you access a configuration page by using the HA Voyager navigation tree, any changes you make are implemented on all the members of the group. This simplifies your work and helps you keep the configuration of the group members synchronized.



---

**Note**

You can use HA Voyager on any member of the group. Regardless of which member you log into, your changes will be implemented on all the other members.

---

Once you create an HA configuration group on one system, you can use HA Voyager on that system to add members to the group.

You probably want to configure certain settings to be identical on all of your HA configuration group members. For example, you probably want each member to have the same static routes and settings for DNS, time, and Voyager web access. HA Voyager makes it easy for you to configure the members in this way by providing the Configuration Cloning option.

The IPSO online documentation and the *Network Voyager Reference Guide* include a configuration example that provides step-by-step instructions for using HA Voyager.

## Configuring VRRP with HA Voyager

You can use HA Voyager to easily configure VRRP on all the members of an HA configuration group. This is the simplest way to configure VRRP, and it also makes it easy for you to ensure that the global VRRP options are set identically on all the members.

When you use HA Voyager to configure VRRP, you create a simplified monitored-circuit configuration, and all the requirements of simplified monitored-circuit apply. For example, before you create a VRRP backup (virtual) address you must make sure that each member has an address with the same network address as the backup address. For example, the following is a valid combination:

- Member A address: 10.1.1.1
- Member B address: 10.1.1.2
- VRRP backup address: 10.1.1.3

For complete information on configuring simplified monitored-circuit VRRP, see the chapter “High Availability Solutions” in the IPSO online documentation and the *Network Voyager Reference Guide*.

## IP Clustering Enhancements

IPSO 6.1 introduces the following enhancements to Nokia’s IP clustering high availability solution:

- Simplified clustering
- Cluster topology choices
- Advanced cluster tuning
- ISP redundancy supported

### Simplified Clustering

IPSO 6.1 makes it easier for you to configure an IP cluster and put it into service by providing the new Simplified Clustering Configuration page. This page allows you to set up a cluster by making an absolute minimum set of configuration choices. When you create a cluster in this way, IPSO chooses default values for a variety of cluster settings. You can still change any of these settings by using the Cluster Configuration page.

### Cluster Topologies

IPSO 6.1 gives you more flexibility in designing IP clusters by providing the following choices of cluster topologies:

- Load balancing: All the nodes in the cluster will be active, and connections will be assigned to all of them. This is the default choice and is only the topology used in previous versions of IPSO.
- N+1: N is the (configurable) number of nodes that will be active and will have connections assigned to them. The remaining node will be in hot standby mode, which means that connections are synchronized with the node on an ongoing basis so that it is immediately ready for service

should one of the active nodes fail. The load will be balanced among the active nodes.

- **Active/Hot Standby:** One node will be active and the other will be in hot standby mode. Use this topology for two-node clusters in which you want only one node to be active. This topology is similar to an active/passive VRRP configuration except that failover happens faster because existing connections are continually synchronized with the standby node.

## Advanced Cluster Tuning

IPSO 6.1 provides some advanced cluster options that can be used to prevent certain issues that can occur in very specific circumstances.

## ISP Redundancy Supported

Previous versions of IPSO do not support the use of Check Point's ISP Redundancy feature with IP clusters. This constraint is removed with IPSO 6.1.

# Configuration Migrator

There are times when you might want to copy much of the configuration information from one Nokia network security platform to another. For example, when you replace a Nokia network security platform with another Nokia platform, you might want to migrate much of the configuration from the system being replaced to the new system. You can do this with IPSO 6.1 by using Network Voyager and the Configuration Migration feature. You can access the Voyager pages for this feature by clicking Tools > Configuration Migration at the bottom of the Voyager navigation tree.

When using the Migrate Configuration feature, keep the following terms in mind:

- **Source platform:** This is the platform from which you will acquire the configuration information. If you are replacing a platform, you probably want to use the platform being replaced as the source.

- **Target platform:** This is the platform on which you will apply the migrated configuration. If you are replacing a platform, the target is the new (replacement) platform.

It is important to understand that the Migrate Configuration feature is designed to copy configuration from one platform to another, not to make configuration changes on the target. If you want to make configuration changes on the target platform—for example, if you want to assign new IP addresses that are not assigned to the source platform—do so after you complete the migration. Think of it as a two or three step process:

1. Migrate the configuration from the source to the target.
2. Make any required changes on the target.
3. If desired, export the configuration from the target to another system.

Migrate Configuration allows you to map interface configuration across the platforms. For example, you can map interface A on the source to interface B on the target so that interface B is configured identically to A.

You can also choose whether to migrate configuration information for specific features. For example, if you use Protocol-Independent Multicast (PIM) on the source but don't want to use it on the target, you can choose not to migrate it. You might also choose not to migrate PIM if you do intend to use it on the target but want to configure it from scratch. Choosing to not migrate a feature means only that the configuration information for that feature is not migrated. The feature itself is still available on the target. In this example, PIM is still be available on the target after the migration but it is not enabled or configured.

## IPSO Automated Configuration

You can use a USB storage device to install IPSO images, IPSO configuration files, and package files, such as Check Point package files, onto Nokia security appliances that have IPSO 6.1 installed but have not yet been configured.

---

**Note**

You cannot use this feature to configure systems running a version of IPSO previous to 6.1.

---

This feature allows experienced personnel at a central site to set up a USB device with the appropriate files for deploying new appliances at another site and then provide the USB device to a person at the other site to perform the deployment. The local operator inserts the USB device in an appliance to be configured and boots the system. The IPSO automated configuration feature installs the specified software and configuration on the appliance, with no intervention needed by the operator. The USB device can hold specific configuration information for different appliances, allowing multiple appliances to be configured from the same USB device.

See the document *Read Me: IPSO Automated Configuration* for complete information about how to use this feature.



---

**Caution**

If you use a USB memory device (or a USB modem) with an IP290 or IP690 running IPSO 6.1, the following BIOS versions are required:

- IP290: version 02.06.8030 or later
- IP690: version 02.06.8025 or later

If you use a USB device with an IP290 or IP690 that does not meet this requirement, the system might hang if it is restarted with the USB device attached. See *Read Me: Updating a Nokia Platform BIOS*, which is available on the IPSO 6.1 download page, for more information.

---

## Enhanced Configuration Summary Tool

The Enhanced Configuration Summary Tool (ECST) allows you to capture your current IPSO configuration, log files, core dumps and other information in a single file that can be sent to Nokia customer support for analysis.

Typically, you would run ECST if you have opened a case with Nokia support and you have been asked to provide an ECST file. You can access the Voyager pages for this feature by clicking Tools > ECST Configuration at the bottom of the Voyager navigation tree.

When you run ECST, you can include any or all of the following information in the output file:

- Offline Network Voyager pages—captured Network Voyager pages that show your current configuration and that can be viewed offline by Nokia customer support.

You must supply your user name and password for ECST to capture the Network Voyager pages. To ensure that all the configuration information is captured, you should have at least read-only access to all IPSO features.

When you include offline Network Voyager pages, ECST saves your current configuration before it captures the pages.

- Firewall information—firewall status, objects, tables, and diagnostics, as captured from utilities such as `cpinfo`, `cpstat`, and `fw tab`.
- IPSO information—captured output from the utilities listed below. :

|                             |                                |
|-----------------------------|--------------------------------|
| <code>date</code>           | <code>arp -a</code>            |
| <code>uname -a</code>       | <code>vmstat -mis</code>       |
| <code>ifconfig -v -a</code> | <code>dbget -rv dynamic</code> |
| <code>ps -auxw</code>       | <code>ipsctl -a</code>         |
| <code>df -k</code>          | <code>ntpd -pn</code>          |
| <code>pstat -ks</code>      | <code>ls -l</code>             |
| <code>netstat</code>        |                                |

- IPSO log files—copies of the syslog log files, httpd access logs, httpd error logs, cron logs, and other logs.

- IPSRD/Core dumps—copies of the configuration files in /config, user directories in /var/emhome, IPSRD and core dumps, and firewall logs.

All ECST output files are stored in /opt/ecst\_output on the appliance. Because the ECST output files can be quite large if you include the Network Voyager offline pages, Nokia recommends that you do not keep more than three output files on your appliance at a time.

You can also run ECST from the IPSO shell, using the command:

```
# ecst [ -cfhilv ]
```

If you include no options, ECST collects information based on the configuration in its current configuration file. The contents of this file are determined by the Service Summary selections in Network Voyager. If no configuration file exists, ECST collects all information.

If you specify options, ECST ignores the configuration file and collects just the information specified by the options. The options are described in [Table 1](#).

**Table 1 ECST Options**

| Option | Description   |
|--------|---|
| -c     | Specifies that the core dump files, configuration files, and user home directories should be collected.         |
| -f     | Specifies that firewall information should be collected.  |
| -h     | Displays help for the ecst command.   |
| -i     | Specifies that the output of various utilities should be captured (same content as the legacy ipsoinfo utility) |
| -l     | Specifies that the log files should be collected.   |
| -v     | Specifies that Network Voyager pages should be captured for offline viewing.                                    |

The files produced by ECST are in the /opt/ecst\_output directory.

## Enhancement for Increased Network Voyager Security

With previous versions of IPSO, Network Voyager is vulnerable to an exploit known as cross-site request forgery. In IPSO 6.1, this vulnerability has been eliminated.

All URLs in Network Voyager now contain a random secret that is generated for each authenticated session. Any request made without this secret will be considered a breach and the user will be re-directed to the login page. When the user logs off or the authenticated session times out, the URL random string becomes invalid.

The secret is not displayed in the browser address bar. Because of this, you will be returned to the login page if you use:

- The refresh button
- Bookmarks to reach a Network Voyager page
- Typed URL to reach a Network Voyager page

Nokia recommends that you use the navigation pane for navigation within Network Voyager.

## Routing Enhancements

This section explains the enhancements in IPSO 6.1 for routing protocols.

### OSPF and BGP Graceful Restart Helper

When a router running OSPF or BGP restarts, all the routing peers detect that the session failed and recovered. This transition results in a routing flap and causes routes to be recomputed, updates to be generated, and unnecessary churn to the forwarding tables.



With IPSO 6.1 you can enable a Graceful Restart Helper option on the OSPF Configuration and BGP Peer Configuration pages. Enabling this option can minimize the negative effects caused by peer routers restarting by maintaining the forwarding state advertised by peer routers even when they restart.

To use the IPSO CLI to configure the Graceful Restart Helper option, use the following commands:

```
set ospf graceful-restart-helper <on|off>

set bgp external remote-as as_number peer ip_address
    graceful-restart-helper <on|off>
    graceful-restart-helper-stalepath-time seconds
```

In the above BGP command, the stalepath time is the maximum amount of time that routes previously received from a restarting router are kept so that they can be revalidated. The timer is started after the peer sends an indication that it has recovered.

## Enhancements for RIP and OSPF Route Tags

If a Nokia platform running IPSO 4.2 receives a route tag in a RIP update, it passes the tag along in RIP updates that it sends out. (IPSO 6.0 does not forward RIP tags.) However, IPSO 4.2 does not forward OSPF route tags or let you create tags for RIP or OSPF. IPSO 6.1 does forward OSPF route tags, and you can now also create RIP and OSPF tags using Network Voyager and the IPSO CLI.

You can create route tags by using the following Voyager pages:

- Redistribute from OSPF External to RIP
- Redistribute from BGP (AS NUMBER) to RIP
- Redistribute from ASPATH to RIP
- Redistribute from BGP (AS NUMBER) to OSPF
- Redistribute from ASPATH to OSPF

To create route tags using the IPSO CLI, use the following commands:

```
set routemap rm_name id <1-65535> action
    ospfautomatictag tag
    ospfmanualtag tag
    riptag tag
```

## Support for USB Modem

IPSO 6.1 includes support for the Radicom V92MB-U-E USB modem. You can use this modem for dialup or dialup/callback access.



### Caution

If you use a USB modem (or USB memory device) with an IP290 or IP690 running IPSO 6.1, the following BIOS versions are required:

- IP290: version 02.06.8030 or later
- IP690: version 02.06.8025 or later

If you use a USB device with an IP290 or IP690 that does not meet this requirement, the system might hang if it is restarted with the USB device attached. See *Read Me: Updating a Nokia Platform BIOS*, which is available on the IPSO 6.1 download page, for more information.

---

## Enhancement for Firewall Kernel Tuning

You can use Voyager to modify Check Point firewall kernel variables by using the Firewall Kernel Tuning Configuration page. This page provides the same functionality as the `modzap` shell command.



### Caution

Use this feature only in consultation with a customer service representative. Do not modify firewall kernel variables unless instructed to do so by a service representative.

---

When you install IPSO or run Voyager for the first time on a new platform, the Firewall Kernel Tuning Configuration page does not appear. If a customer service representative instructs you to use this page, you must first display it by performing these steps:

1. Establish a command line connection to the platform (using a network connection or a console connection).
2. At the IPSO shell prompt, enter  
**dbset advanced:loader t**
3. Run Voyager (or exit Voyager and run it again if Voyager was open when you entered the previous command).
4. Click Configuration > Tools > Firewall Kernel Tuning in the navigation tree.

To use this page, enter the firewall kernel variables as instructed by your customer service representative and then click Apply. Clicking Apply applies the firewall kernel variables and also saves the Voyager configuration so that the Firewall Kernel Tuning Configuration page will appear again if you reboot the platform.

If you do not want Voyager to display the Firewall Kernel Tuning Configuration page, perform these steps:

1. Establish a command line connection to the platform (using a network connection or a console connection).
2. At the IPSO shell prompt, enter  
**dbset advanced:loader**
3. Run Voyager (or exit Voyager and run it again if Voyager was open when you entered the previous command).

When you run Voyager after entering this command, the Firewall Kernel Tuning Configuration page does not appear, but your settings for firewall kernel variables are preserved. If you also want to undo all the settings you implemented, delete the file `/image/current/loader.conf` and reboot the platform. After the reboot, any variables you configured by using the Firewall Kernel Tuning Configuration page have their previous values.

## Changes to Upgrade and Installation Process

In some circumstances, the process of upgrading or installing IPSO 6.1 (and 6.0) requires additional steps that are not necessary when upgrading or installing versions of IPSO previous to 6.0. For details, see “[Changes to Upgrade and Installation Procedures](#)” on page 59 and “[Before You Install IPSO 6.1](#)” on page 62 for more information.

For more information about upgrading to R65 for IPSO 6.0, see the *Check Point for Nokia IPSO Getting Started Guide*, which is available at <https://support.nokia.com>.

## Supported Platforms

[Table 2](#) lists the platforms supported by IPSO 6.1 and includes the platforms supported by IPSO 4.2 and 6.0 for comparison.

**Table 2 Supported Platforms**

| Platforms      | IPSO 4.2 | IPSO 6.0                           | IPSO 6.1                           |
|----------------|----------|------------------------------------|------------------------------------|
| IP45, IP60     | no       | no                                 | no                                 |
| IP150          | yes      | no                                 | yes                                |
| IP260, IP265   | yes      | no                                 | no                                 |
| IP290          | yes      | no                                 | yes                                |
| IP390          | yes      | no                                 | yes                                |
| IP560          | yes      | no                                 | yes                                |
| IP690          | yes      | yes (leverages multiple CPU cores) | yes (leverages multiple CPU cores) |
| IP1220, IP1260 | yes      | no                                 | no                                 |
| IP1280         | yes      | yes (leverages multiple CPU cores) | yes (leverages multiple CPU cores) |
| IP2250, IP2255 | yes      | no                                 | no                                 |
| IP2450         | yes      | yes (leverages multiple CPU cores) | yes (leverages multiple CPU cores) |

## Supported Memory Configurations

For information about the number of connections supported for specific amounts of memory, consult [Table 3](#) and [Table 4](#). Use the maximum connection values to determine which value to enter in Check Point's SmartDashboard for the maximum number of connections.

The values in both tables assume that you use SecureXL. If you do not use SecureXL (and do use firewall flows instead), IPSO supports roughly twice the number of connections listed in the second column.

A platform does not create more connections than its memory supports (even if you enter a value greater than the appropriate one listed here). If you configure IPSO to collect and export Netflow flow records, IPSO supports a smaller number of connections, as indicated in the tables.

**Table 3 Disk-Based IP Security Platforms**

| DRAM   | Check Point<br>maximum<br>connections  | Hash table<br>size | Memory<br>pool size | Maximum<br>memory pool<br>size |
|--------|--|--------------------|---------------------|--------------------------------|
| 1 GB   | 360,000<br>(270,000 with<br>Netflow)   | 8 MB               | 400 MB              | 512 MB                         |
| 2–4 GB | 1,048,000<br>(786,000 with<br>Netflow) | 16 MB              | 800 MB              | 1100 MB                        |

**Table 4 Flash-Based IP Security Platforms**

| DRAM   | Check Point<br>maximum<br>connections | Hash table<br>size | Memory<br>pool size | Maximum<br>memory pool<br>size |
|--------|---------------------------------------|--------------------|---------------------|--------------------------------|
| 1 GB   | 225,000<br>(168,750 with<br>Netflow)  | 8 MB               | 256 MB              | 400 MB                         |
| 2–4 GB | 725,000<br>(543,750 with<br>Netflow)  | 16 MB              | 800 MB              | 900 MB                         |

## Supported Applications

IPSO 6.1 supports NGX R65 for IPSO 6.0 and does not support any other version of the Check Point firewall. You can upgrade to this version of the firewall from several earlier versions, but you cannot upgrade to NGX R65 for IPSO 6.0 from NGX R65.

The features and operation of NGX R65 for IPSO 6.0 are described in separate documents.

## Detailed Comparison with IPSO 4.2 and 6.0

IPSO 6.0 does not support some features that are supported by previous versions of IPSO. IPSO 6.1 reintroduces support for most of these features. The tables in this section present a detailed comparison of the features supported by IPSO 4.2, IPSO 6.0, and IPSO 6.1.

**Table 5 Interface Features**

| Features               | IPSO 4.2                 | IPSO 6.0          | IPSO 6.1                 |
|------------------------|--------------------------|-------------------|--------------------------|
| Transparent Mode       | yes                      | no                | yes                      |
| Link Aggregation       | yes (dynamic and static) | yes (static only) | yes (dynamic and static) |
| Link Redundancy        | yes                      | no                | yes                      |
| PPPoE                  | yes                      | no                | no                       |
| ARP Mirroring for VRRP | yes                      | no                | yes                      |

**Table 6 System Configuration Features**

| <b>Features</b>                    | <b>IPSO 4.2</b> | <b>IPSO 6.0</b> | <b>IPSO 6.1</b> |
|------------------------------------|-----------------|-----------------|-----------------|
| Banner and MOTD                    | yes             | yes             | yes             |
| DHCP and DNS                       | yes             | yes             | yes             |
| Disk Mirroring                     | yes             | yes             | yes             |
| Optional Disk                      | yes             | yes             | yes             |
| Hybrid Mode                        | yes             | yes             | yes             |
| Logging to Optional Disk           | yes             | yes             | yes             |
| Core Dump to Optional Disk         | yes             | not required    | yes             |
| Core Dump to Remote Server         | yes             | yes             | yes             |
| System Failure Notification        | yes             | yes             | yes             |
| Mail Relay                         | yes             | yes             | yes             |
| Autokey Authentication for NTP     | no              | yes             | yes             |
| Daylight Savings Time Enhancements | yes             | yes             | yes             |
| Syslog                             | yes             | yes             | yes             |
| Configuration Sets                 | yes             | yes             | yes             |
| Backup and Restore                 | yes             | yes             | yes             |
| Job Scheduler                      | yes             | yes             | yes             |



|                             |     |  |                                       |
|-----------------------------|-----|--|---------------------------------------|
| Licenses                    | yes | yes                                      | yes                                   |
| Advanced System Tuning      | yes | yes (TCP MSS configuration not included) | yes (TCP MSS moved to interface page) |
| Upgrade Images              | yes | yes                                      | yes                                   |
| Upgrade and Manage Packages | yes | yes                                      | yes                                   |
| Asset Information           | yes | yes                                      | yes                                   |

**Table 7 High Availability Features**

| Features                   | IPSO 4.2                            | IPSO 6.0 | IPSO 6.1                   |
|----------------------------|-------------------------------------|----------|----------------------------|
| VRRP                       | yes                                 | yes      | yes (including HA Voyager) |
| IP Clustering              | yes                                 | yes      | yes                        |
| IP Clustering Unicast Mode | yes                                 | no       | yes                        |
| External Load Balancer     | yes                                 | no       | yes                        |
| Single License VRRP        | yes (but violates Check Point EULA) | no       | no                         |

**Table 8 Security and Access Features**

| Features                        | IPSO 4.2 | IPSO 6.0   | IPSO 6.1   |
|---------------------------------|----------|--|--|
| Users                           | yes      | yes  | yes  |
| Groups                          | yes      | yes  | yes  |
| Enhanced Password Configuration | yes      | yes  | yes  |
| AAA                             | yes      | yes ( nonlocal users not supported with TACACS+) | yes ( nonlocal users are supported with TACACS+) |
| Network Access and Services     | yes      | yes  | yes  |
| Role Based Administration       | yes      | yes  | yes  |
| Voyager Web Access              | yes      | yes  | yes  |
| SSH                             | yes      | yes  | yes  |
| IPSec                           | yes      | no   | no   |
| Miscellaneous Security Settings | yes      | no   | no   |

**Table 9 Routing Features**

| Features          | IPSO 4.2 | IPSO 6.0 | IPSO 6.1 |
|-------------------|----------|----------|----------|
| BGP               | yes      | yes      | yes      |
| BGP Route Refresh | yes      | no       | yes      |

|  |                    |     |                          |
|--|--------------------|-----|--------------------------|
| BGP Graceful Restart                       | no                 | no  | yes                      |
| Remove Private AS Numbers from BGP Updates | yes                | no  | yes                      |
| OSPF                                       | yes                | yes | yes                      |
| OSPF Route Tags (create and forward)       | no                 | no  | yes                      |
| OSPF Graceful Restart                      | no                 | no  | yes                      |
| OSPFv3 with VRRPv3                         | yes                | no  | yes                      |
| RIP  | yes                | yes | yes                      |
| RIP Route Tags                             | yes (forward only) | no  | yes (create and forward) |
| IGRP                                       | yes                | yes | yes                      |
| IGMP                                       | yes                | yes | yes                      |
| IGMP local and static groups               | yes                | no  | yes                      |
| PIM  | yes                | yes | yes                      |
| PIM Over VTIs                              | yes                | no  | yes                      |
| PIM SSM                                    | yes                | no  | yes                      |
| PIM dense mode state refresh               | yes                | no  | yes                      |
| DVMRP                                      | yes                | yes | yes                      |
| Static Routes                              | yes                | yes | yes                      |

|                         |                      |    |     |
|-------------------------|----------------------|----|-----|
| Static Multicast Routes | yes                  | no | yes |
| Mobile IPv4             | yes<br>(unsupported) | no | no  |

**Table 10 Miscellaneous Features**

| Features   | IPSO 4.2 | IPSO 6.0 | IPSO 6.1 |
|--|----------|----------|----------|
| IPv6   | yes      | yes      | yes      |
| Traffic Management (including QoS)   | yes      | no       | yes      |
| Policy Based Routing   | yes      | no       | yes      |
| PIM accelerated  | yes      | no       | yes      |
| SNMP   | yes      | yes      | yes      |
| Voyager and CLI monitoring Features  | yes      | yes      | yes      |
| Enhanced Graphing for Monitoring Pages (requires Adobe Flash version 8.0 or newer in the client browser) | no       | yes      | yes      |

**Table 11 Command Line Features**

| Features         | IPSO 4.2 | IPSO 6.0 | IPSO 6.1 |
|------------------|----------|----------|----------|
| ipsctl           | yes      | yes      | yes      |
| dbset, dbget     | yes      | yes      | yes      |
| top              | no       | yes      | yes      |
| vmstat           | yes      | yes      | yes      |
| fw commands      | yes      | yes      | yes      |
| fwaccel commands | yes      | yes      | yes      |

|   |     |   |   |
|---|-----|---|---|
| clish   | yes | yes   | yes   |
| bash shell  | no  | yes—default shell   | yes—default shell   |
| tcsh shell  | no  | yes   | yes   |
| sh shell  | yes | yes (but is not the default)  | yes (but is not the default)  |
| Default Shell Inactivity Timeout (configured on Voyager User Management page) | no  | yes   | yes   |
| rc.local support  | yes | yes (but see <a href="#">“Change to rc.local Support”</a> on page 64) | yes (but see <a href="#">“Change to rc.local Support”</a> on page 64) |

# 3

## Performing the Initial Configuration

When you turn on a Nokia IP security platform for the first time, you must provide it with some initial configuration information. You can use two methods to perform the initial configuration:

- In an automated fashion by using the built-in dynamic host configuration protocol (DHCP) client.
- Manually by using a console (direct serial) connection.

After you decide which method to use, follow the instructions in [“Using DHCP to Configure the System”](#) or [“Using the Console to Configure the System”](#) on page 50 to perform the initial configuration. Regardless of which method you use, see [“Performing Additional Configuration”](#) on page 54 for important information about how to proceed after you complete the initial configuration.

### Using DHCP to Configure the System

The Nokia IPSO DHCP feature allows a properly configured DHCP server to provide your system with the following information:

- Host name
- IP address
- Default route

You can then use Nokia Network Voyager to reconfigure any of these settings. When you do so, Voyager keeps the modified settings. (DHCP is not used if configuration information already exists.) Your DHCP server automatically sets the administrative password of the IP system to `password`.

To use DHCP to configure your system, perform the following steps (which are explained in the following sections):

1. Configure your DHCP server.
2. Run the DHCP client on the Nokia system.

## **Configuring Your DHCP server**

Configure a DHCP server with (at a minimum) mappings for:

- A host name for the Nokia system.
- The serial number of the Nokia IP security platform.
- A static IP address for the platform.

IPSO also supports MAC-address based configuration.

Beginning with Nokia IPSO 3.8, the DHCP client accepts the lease time for the IP address that the server provides. When the lease expires, the DHCP client contacts the server. Previously, the client accepted only IP address leases that were at least a year long.

---

### **Note**

Your DHCP server must be on the same network as the Nokia platform or the DHCP/BOOTP relay must be configured on the intermediate routers.

---



The following example shows relevant DHCP configuration information:

```
ddns-update-style ad-hoc;
subnet 10.1.1.0 netmask 255.255.255.0 {

    # default gateway
    option routers                10.1.1.1;
    option subnet-mask            255.255.255.0;

    option domain-name-servers   24.5.207.179;

    range dynamic-bootp 10.1.1.20 10.1.1.100;

    host IP2450fixed {
        # serial number of the box
        option dhcp-client-identifier "123456";

        fixed-address 10.1.1.11;
        option host-name "IP2450";
    }
}
```

## Running the DHCP Client on the Nokia System

---

### Note

Do not perform the following procedures unless you configured an appropriate DHCP server with configuration information for your platform.

---

1. Connect a NIC installed in your platform to your network.
2. Turn the platform on.

The DHCP client program in the system starts automatically, and your DHCP server provides the appropriate configuration information. (This can require 5 to 10 minutes.)

3. From a computer on the same network, ping the IP address that you configured your DHCP server to provide to the Nokia system.

When you receive replies from `ping`, you can use Nokia Network Voyager to connect to the system.

4. Connect to the system by using Voyager.

To connect, start a Web browser and enter the IP address or host name of the system in the address or URL field of the browser.

5. Enter the user name **admin** and the password **password**.
6. Modify the configuration of the system as appropriate.

---

**Note**

Nokia strongly recommends that you change the password.

---

For information about how to proceed, see [“Performing Additional Configuration”](#) on page 54. If you intend to use the IPSO CLI or shell, be sure to see [“Using the IPSO CLI”](#) on page 54.

## Using the Console to Configure the System

If you are installing a new Nokia IP security platform and are not using DHCP to perform the initial configuration, follow the instructions in this section to perform the initial configuration.

Before you begin, make sure that you know:

- A host name to assign to the platform.
- An IP address that you will assign to the platform.
- The appropriate network mask length.
- The IP address of the default gateway for the platform.
- An appropriate password to assign to the administrator account.

## Performing the Configuration

1. Establish a physical console connection to the Nokia IP security platform.

The console can be any standard VT100-compatible terminal or terminal emulator with the following properties:

- RS-232 data terminal equipment (DTE)
- 9600 bps
- 8 data bits
- No parity
- 1 stop bit

You can also use a data communications equipment (DCE) device.

To establish the physical console connection, follow these steps:

- a. Connect the appropriate cable to the local console port on the front panel of the platform.

If the console is DTE, use the supplied null-modem cable (console cable). If the console is DCE, use a straight-through cable.

- b. Connect the other end of the cable to the console system.

2. Turn the platform on.

After some miscellaneous output appears on the console connection, the following prompt appears:

Hostname?

If the `Hostname?` prompt does not appear on the console, see the *Installation Guide* for troubleshooting suggestions.

3. Respond to the `Hostname?` prompt within 30 seconds to prevent the DHCP client from starting.

If you wait more than approximately 30 seconds before you type a response to the host name prompt, the DHCP client program starts automatically, and the system might be provided with a host name and IP address that is unknown to you. (This could happen if a DHCP server on

your network is configured to supply configuration information to any system that requests it.)

If this happens, follow these steps:

- a. Establish a console connection to the platform.
  - b. Log into the system using the user name **admin** and the password **password**.
  - c. Enter:  

```
rm /config/active
```

or  

```
mv /config/active /config/active.old
```
  - d. Reboot the platform.
  - e. Respond to the configuration prompts in a timely manner.
4. Respond to the following prompts.

When you see the following message, type 1:

You can configure your system in two ways:

- 1) configure an interface and use our Web-based Voyager via a remote browser
- 2) configure an interface by using the CLI

Please enter a choice [ 1-2, q ]:

**5.** You are prompted to select a network interface to configure:

Select an interface from the following for configuration:

- 1) ser-s2p1
- 2) eth-s3p1
- 3) eth-s4p1
- 4) eth-s5p1
- 5) quit this menu

Enter choice [1-5]:

The list of interfaces that you see depends on the NICs that are installed. In the preceding example, ser-s2p1 is a serial interface in chassis slot 2, port 1, and eth-s3p1 is an ethernet interface in chassis slot 3, port 1.

Type the number for the interface to configure. Remember that this is the interface you will connect to with Nokia Network Voyager or the CLI to continue with the configuration.

**6.** At the prompt, enter the IP address and subnetwork mask length.

**7.** When you see the following message, choose y (the default option):

Do you wish to set the default route [ y ] ?

If you choose n, you cannot use Network Voyager unless you do one of the following:

- Perform the installation procedure again and set a default route.
- Use the command-line interface over a console connection to create a default route or static route.
- Connect to the platform by using a system that is on the same network as a configured interface on the platform.

**8.** When you are prompted to reboot the system, type:

**reboot**

and press Enter.

## Performing Additional Configuration

After you reboot the system, you are ready to continue configuring it. You can connect to the network interface you configured and perform the additional configuration using either:

- Nokia Network Voyager
- The IPSO CLI

### Using Nokia Network Voyager

To log in to the system by using Network Voyager, follow these steps:

1. Start a Web browser on a workstation that has network connectivity to the Nokia IP security platform.
2. In the Location or Address field of the browser, enter the IP address of the interface you configured on the platform.
3. Enter the user name **admin** and the password you entered when you performed the initial configuration in the appropriate fields.

### Using the IPSO CLI

After the system reboots, SSH is on by default as a security measure. This means that you have two options to connect to a network interface and use the IPSO CLI (or the IPSO shell):

- Use an SSH client. This is the recommended approach. For more information, see [“Using an SSH Client.”](#)

If you do not want users to be able to access the system with an SSH client, see [“Disabling SSH”](#) on page 57 for information about how to disable SSH.

- Connect to the configured network interface by using Telnet if it is enabled. Telnet is disabled by default if you:
  - purchase a platform with IPSO 6.1 installed

- perform a fresh installation of IPSO 6.1 (use the boot manager `install` command)
- load a factory default configuration database

To maintain optimum security, Nokia recommends that you disable Telnet and use an SSH client. For more information about how to disable Telnet, see “[Disabling Telnet](#)” on page 56.

---

**Note**

SSH does not apply to console connections. Regardless of whether SSH is enabled, you can always access the Nokia IP security platform over a console connection.

---

## Using an SSH Client

To communicate with your Nokia system by using SSH, you must have an SSH client program installed on a workstation that has network connectivity to the Nokia IP security platform. You can get information about SSH client programs at <http://www.freessh.org>.

At a minimum, you should use a host key as explained in “[Using a Host Key](#).” For even better security, use authorized keys as well.

### Using a Host Key

IPSO automatically generates a host public and private key pair after you perform the initial configuration. For maximum security, you can install the public part of this key on the workstations that you will use to connect to the Nokia system. Having the host public key installed allows the SSH client program to verify that it really is communicating with the Nokia system and not a system that is falsely purporting to be the Nokia system.

If you do install the host public key on workstations, the most secure way to transport the key is to use an out-of-band method, such as transporting the key on a floppy disk. This reduces the possibility that the key could be stolen in transit.

If you do not install the public host key on a workstation that you use to connect to the platform, the Nokia system asks the SSH client to accept the key the first time you attempt to connect:

- If you choose to accept the key, the connection is established. This procedure is potentially less secure because the SSH client cannot be sure that the host key is really being supplied by the Nokia system.
- If you choose to not accept the key, you are not able to connect to the Nokia system.

When a workstation has the host public key (regardless of how it received it), the SSH client program can connect to the Nokia system as long as the host public and private key pair is valid.

## Disabling Telnet

You can use Nokia Network Voyager or the IPSO CLI to disable Telnet.

---

### Note

You must have Telnet enabled on your Nokia IP security platforms for Nokia Horizon Manager to communicate with the platforms in the unsecure mode. See the Horizon Manager documentation for more information.

---

### To use Nokia Network Voyager to disable Telnet

1. Log into the platform by using Nokia Network Voyager.  
Enter the user name **admin** and the password you configured for this user when you performed the initial configuration.
2. In the Network Voyager navigation tree, select Configuration > Security and Access > Network Access and Services.
3. Click No for the Allow TELNET Access field.
4. Click Apply.
5. Click Save to make your change persistent across reboots.



### To use the CLI to disable Telnet

1. Establish a console connection to the platform.
2. Log in using the user name **admin** and the password you configured for this user when you performed the initial configuration.
3. Start the CLI by entering:

```
clish
```

4. Enter:

```
set net-access telnet no
```

### Disabling SSH

You can use Nokia Network Voyager or the IPSO CLI to disable SSH.

---

#### Note

SSH must be enabled on your Nokia IP security platforms for Horizon Manager to communicate with the Nokia platforms in the secure mode. For more information, see the Horizon Manager documentation.

---

### To use Nokia Network Voyager to disable SSH

1. Log in to the platform by using Network Voyager.  
Enter the user name **admin** and the password you configured for this user when you performed the initial configuration.
2. In the Network Voyager navigation tree, select Configuration > Security and Access > SSH (Secure Shell) > SSH Configuration.
3. Click No for Enable SSH service (daemon sshd).
4. Click Apply.
5. Click Save to make your change persistent across reboots.

### **To use the IPSO CLI to disable SSH**

1. Establish a console connection to the platform.
2. Log in by using the user name **admin** and the password you configured for this user when you performed the initial configuration.
3. Start the CLI by entering:  
**clish**
4. Enter:  
**set ssh server enable off**

# 4 Upgrading to Nokia IPSO 6.1

This chapter explains the requirements and procedures for installing or upgrading to IPSO 6.1.

You can obtain IPSO 6.1 by downloading the software from the Nokia customer support site. You can install IPSO and packages by using the following:

- Nokia Horizon Manager (on multiple Nokia platforms simultaneously)
- Nokia Network Voyager
- IPSO CLI
- IPSO command shell (console session)

## Changes to Upgrade and Installation Procedures

With the introduction of IPSO 6.x, there are significant changes to the upgrade and installation procedures. Note the following important requirements:

- If you use Network Voyager or the `newimage` shell command to upgrade to Nokia IPSO 6.1, see [“Boot Security”](#) on page 60 for information about a change to this procedure.
- If you perform a fresh installation of IPSO 6.1 on a platform running IPSO 4.x (if you use the boot manager to perform the installation), you must follow the instructions in [“Overwriting Existing Images \(Fresh Installation\)”](#) on page 71. The process is different from installing IPSO 4.x, and you *must* follow the new procedure to perform a successful installation of IPSO 6.1.

- If you fresh install IPSO 4.x on a system running IPSO 6.x, you must perform a fresh installation following the procedure described in [“Installing IPSO 4.x”](#) on page 75. The process has been changed with IPSO 6.x, and you *must* follow the new procedure to perform a successful installation of IPSO 4.x.
- The file ipso.tgz is included in the file ipso-6\_1-bld037.zip. Download and unzip this file to get the IPSO 6.1 version of ipso.tgz.

## Boot Security

When a Nokia platform boots a version of IPSO previous to 6.x, it immediately loads the Check Point firewall module and default filter (assuming that the firewall is installed and enabled). This provides security until IPSO and the firewall become fully active. When you boot IPSO 6.x, it cannot load a module for any firewall version other than NGX R65 for IPSO 6.0. Therefore, until you install and enable NGX R65 for IPSO 6.0, the firewall cannot provide security during the bootup phase.

When you upgrade from IPSO 4.x to IPSO 6.x, IPSO 6.x initially provides security by installing a set of rules using ipfw, the FreeBSD firewall. When IPSO detects that NGX R65 for IPSO 6.0 is installed, this temporary security measure is disabled.

---

### Note

When the ipfw rules are in effect, you can access the platform using SSH and HTTPS. To do so, you must enable SSH and SSL (for HTTPS) in IPSO 4.x before you begin the upgrade. You can also access the platform during this time using a console connection or SmartUpdate.

---

## Downloading Nokia IPSO and Related Files

### To download IPSO and related files and documentation:

1. Access the Nokia customer support Web site at <https://support.nokia.com>.
  2. Log in using your user name and password.
  3. Click the Software tab.  
The Software Downloads page appears.
  4. If the IPSO build you want is listed in the table, click the appropriate link and skip to [step 9](#). Otherwise, continue to step 5.
  5. Click the appropriate link that appears above the table.
  6. Continue to click the appropriate links that appear above the table until you see the link for the version of IPSO you want.
  7. Click the link for appropriate IPSO version.  
Links for the available builds of this version appear in the table.
  8. Click the link for the build you want.
  9. Before you click the link to download the build, copy or take note of the SHA1 or MD5 value displayed for the build.
  10. Download the appropriate zip file to an FTP server or workstation.
  11. Unzip the zip file to get `ipso.tgz` and other files.
  12. Download related files and the IPSO Release Notes, as appropriate.
- You can now install IPSO 6.1 remotely from the FTP server or workstation.  
(See [“Installing Nokia IPSO 6.1”](#) on page 67.)

## Using Nokia Horizon Manager to Install IPSO and Packages

You can use Nokia Horizon Manager to automate the process of installing, upgrading, and enabling IPSO 6.1 and software packages on multiple Nokia

platforms. Horizon Manager employs Do No Harm intelligence to prevent any incompatible IPSO version upgrades. Use the OS Install action to install IPSO 6.1 on as many as 2500 platforms in a single data set. Horizon Manager also provides actions that automate the installation and upgrade of software packages, such as Check Point NGX and associated feature packs. Horizon Manager automates the entire installation process, including backing up configuration information before the upgrade and rebooting platforms to activate the new version of IPSO.

If you are using Horizon Manager to automate the process of installing or upgrading IPSO or software packages, you might not need to use this document further.

For detailed information about the installation and upgrade process, see the Horizon Manager documentation.

## Before You Install IPSO 6.1

This section explains information you should know and some tasks that you should perform before you install IPSO 6.1.

### IP2450 Might Require BIOS Upgrade

On the IP2450, IPSO 6.1 requires version 2.12 or later of the system BIOS. (If you purchased an IP2450 with IPSO 6.1 already installed, the BIOS does not need to be upgraded.) Before you install IPSO 6.1 on a platform, verify the BIOS version by navigating to Configuration > Asset Information > Asset Summary in Network Voyager. The following examples show how to identify the version:

- 8.6.1.21 V2.9 (version 2.9—must be upgraded)
- 8.6.1.29 V2.12 (version 2.12—does not need to be upgraded)
- V2.14.9 or later (recommended for performance but not required)

---

**Note**

If your IP1280 or IP2450 has BIOS version 2.12, Nokia recommends that you update to V2.14.9 or later to improve performance with IPSO 6.1, but this upgrade is not required.

---

If necessary, upgrade the BIOS by performing this procedure:

1. Download the BIOS file (for example, IP2450\_BIOS\_v2\_14\_10) to the platform you will upgrade.

This file is available on the Nokia support site on the same page as the IPSO 6.1 image.

2. Log on to the platform using a console connection if you have not done so already.
3. Navigate to the directory in which you stored IP2450\_BIOS\_v2\_14\_10.
4. Make sure that there were no download errors by creating a SHA1 or MD5 value for the file and verifying that it matches the value posted on the download page.

If the values are identical, the download was successful and the file is good. If not, download the file (in binary) again and repeat this procedure.

5. Enter:

```
biosprog IP2450_BIOS_v2_14_10
```

6. Reboot the platform.

## If You Use Link Redundancy Before Upgrading to 6.1

If you create a link redundancy group with IPSO 6.1, the maximum number of ports in the group is two. However, this constraint does not apply if you have a link redundancy group with more than two ports in IPSO 4.x and upgrade to IPSO 6.1 by adding the 6.1 image. In this case, all the ports work after the upgrade but you cannot add any more ports to the group.

## Change to rc.local Support

You can use the optional rc.local file to run site-specific commands when a system is booted. If you use an rc.local file, please be aware of the following:

- IPSO 6.x looks for the rc.local file in /etc rather than in /var/etc as earlier IPSO releases did. After you upgrade to IPSO 6.x, create a symbolic link file in /etc that references /var/etc/rc.local file by executing the following commands:

```
# cd /etc
# mount -uw /
# ln -s /var/etc/rc.local /etc/rc.local
```

- Because the /etc directory is overwritten every time you perform an IPSO image upgrade, you must recreate the symbolic link after an upgrade.

## Verify Free Space in Root Partition

On all platforms, you should have at least 180 MB of free disk space in your root partition to install an IPSO 6.1 image. To determine the available disk space, log in to the IPSO shell through a terminal or console connection and enter **df -k**. If the first number in the Avail column (which shows the available space in the root partition) is less than 180000 Kbytes, you should make more space available in the root partition by deleting the temporary files specified in the following command if they are present. (These files might not be present, depending on how the upgrades were done on your system.)

Execute the following commands to delete the list of unwanted files:

```
mount -uw /
rm -f /image/*/bootmgr/*.sav
rm -f /image/*/bootmgr/*.tmp
sync
mount -ur /
```

If you use the **df** command after you install IPSO 6.1 as a third image, you might see that the root partition is more than 100 percent full. If no errors were displayed while you installed IPSO 6.1, you can safely ignore this output from **df**.



When you have enough space in the root partition, follow the instructions in [“Putting the ipso.tgz file on Your Platform.”](#)

## Fresh Installation on a 1 GB Flash-Based Platform

If you use the boot manager to install IPSO 6.1 on a flash-based platform with one gigabyte of DRAM, do not choose to install packages when you see the message `Retrieve all valid packages, with no further prompting?` Your system does not have enough memory to extract the Check Point wrapper package, and the package installation will fail.

After you successfully install IPSO 6.1, use Network Voyager or the `newpkg` command to install your packages.

## Putting the ipso.tgz file on Your Platform

After you make sure that at least 180000 Kbytes are available on the root partition, put the `ipso.tgz` file on an FTP server and transfer this file to the platform. You can transfer the `ipso.tgz` in either one of the following two ways:

- FTP the `ipso.tgz` file to the platform and install IPSO in one procedure.

Follow the appropriate instructions in [“Installing Nokia IPSO 6.1”](#) on page 67.

- FTP the `ipso.tgz` file to the platform first and then install IPSO in a separate procedure.

Follow the instructions in [“Transferring the ipso.tgz file”](#) and [“Verifying File Integrity”](#) on page 66 and then follow the appropriate instructions under [“Installing Nokia IPSO 6.1”](#) on page 67.



### Caution

If you perform a fresh installation of IPSO, you must download the `ipso.tgz` file and perform the installation at one time. Do not copy the `ipso.tgz` file to the platform first—it will be overwritten during

the installation procedure. For more information, see [“Overwriting Existing Images \(Fresh Installation\)”](#) on page 71.

---

### Transferring the ipso.tgz file

Transferring IPSO 6.1 to your platform as a separate step allows you to perform a local installation (as opposed to a remote installation from an FTP server).

1. Use Nokia Network Voyager to enable FTP access to the platform.

To do so, select the *Network Access and Services* link under Security and Access. Then:

- a. In the *Allow FTP access* field, click *Yes*.
- b. Click *Apply*
- c. Click *Save* to make your change permanent.

2. Open the directory on the FTP server that contains the `ipso.tgz` file.

3. Begin an FTP session to your platform.

By default, the current directory should be `var/emhome/admin`. Do not change the current directory.

4. At the prompt, enter:

```
bin
```

5. Transfer the `ipso.tgz` file to the platform.

At the prompt, enter:

```
put ipso.tgz
```

6. Close the FTP session.

### Verifying File Integrity

Make sure that there were no download errors by creating a SHA1 or MD5 value for the `ipso.tgz` file and verifying that it matches the value posted on the download page.

If the values are identical, the download was successful and the file is good. If not, download the file (in binary) again and repeat this procedure.

## Installing Nokia IPSO 6.1

You can change the version of IPSO running on your platform in either of the following ways:

- Add the new version of IPSO (also known as an IPSO image) without removing the existing images or your configuration information. If you add a new version, you can revert to the earlier versions stored on the platform. When you do so, your IPSO configuration information is not affected.

If you copied the `ipso.tgz` file to the platform you are upgrading as described in [“Transferring the ipso.tgz file”](#) on page 66, you must use this method.

You can use Nokia Network Voyager, the IPSO shell, or the IPSO CLI to add an image. The procedures for using Network Voyager and the IPSO shell are explained below. For information about how to add an image using the IPSO CLI, see the *CLI Reference Guide for Nokia IPSO*.

When you add an IPSO image, the IPSO boot manager is upgraded automatically if your system does not have the boot manger for the image you are adding.

---

### Note

On flash-based platforms, you can have a maximum of two IPSO images installed at a time. If needed, delete an older IPSO image before you add IPSO 6.1.

---

- Perform a fresh installation, which removes the existing images and your configuration information. If you perform a fresh installation, you can restore versions of IPSO that were previously installed, but the process is more involved and all of your configuration information is removed again.

For information about how to perform a fresh installation, “[Overwriting Existing Images \(Fresh Installation\)](#)” on page 71.

Before performing a fresh installation, you must install the IPSO 6.1 boot manager. If you later want to perform a fresh installation of IPSO 4.x, you must reinstall the IPSO 4.x boot manager. The following summarizes the constraints:

- You cannot use the IPSO 6.1 boot manager to perform a fresh installation of IPSO 4.x.
- You cannot use the IPSO 4.x boot manager to perform a fresh installation of IPSO 6.1.

---

**Note**

The installation process takes longer on flash-based systems than on comparable disk-based systems. For example, if you install an image (using either of the above methods) on a flash-based IP690 and a disk-based IP690, the installation time is noticeably longer on the flash-based system. This is expected and does not indicate any problem.

---

## Adding an IPSO Image Using Voyager

Using Network Voyager is a convenient way to add an IPSO image to a platform. For instructions about how to do this, refer to the “Configuring System Functions” of the *Nokia Network Voyager Reference Guide*.

If the documentation package has been installed and enabled on your platform, you access the guide from the IPSO Documentation link in the Network Voyager navigation tree.

## Adding an IPSO Image from the Command Shell

This section describes how to install IPSO by using the IPSO command shell over a console connection.

(For instructions about how to install IPSO by using the CLI, see the “System Configuration Commands” section of the *CLI Reference Guide for Nokia IPSO*. You can get the *CLI Reference Guide* from Network Voyager, if the IPSO documentation package is installed, or by visiting the Nokia customer support web site.)

**Note**

When you add an image or perform a fresh installation by using the IPSO command shell, use a console connection (rather than by Telneting to an interface that is already configured).

To add a new image from the IPSO command shell, use the **newimage** command. The syntax is:

```
newimage [[-i | -l local_file] [-b] [-R | -T]] [-r | -t
image_name]
[-k] [-v]
```

[Table 12](#) describes the options you can use with the **newimage** command.

**Table 12 newimage Options**

|               |  |
|---------------|--|
| -i            | Load a new image interactively. Interactive mode supports anonymous FTP, FTP with a user name and password, and access to the local file system. If you use this option, do not choose to install from a CD-ROM if your system does not have a CD-ROM drive. |
| -l local_file | Extract the new image from a local file.   |
| -b            | Force upgrade of boot manager.   |
| -R            | Use newly installed image at next reboot.  |
| -T            | Test boot using newly installed image .  |
| -r image_name | Specify image to run at next boot.   |
| -t image_name | Specify image to run at next test boot.  |

- |    |   |
|----|---|
| -k | Specify that any installed packages should be kept. |
| -v | Verbose.  |

---

**Note**

You must reboot your platform after you use the **newimage** command to upgrade the IPSO image. Save your current configuration before you install the new image.

---

### To add an IPSO image

1. Log on to your platform by using a console connection.

---

**Note**

If you downloaded IPSO 6.1, make sure that the file originated at Nokia and did not change during the download process. (See [“Verifying File Integrity”](#) on page 66.)

---

2. Perform one of the following, depending on whether you copied the `ipso.tgz` file to your platform or will install it from an FTP server:

- If the IPSO image is copied to your platform, enter:

```
newimage -k -l ipso.tgz
```

You should see a response similar to the following:

```
ipso.tgz Validating image...done.
```

```
Version tag stored in image: IPSO-6.1-BETA027A-releng-  
1-09.17.2008-034503
```

```
Installing new image...done [example]
```

- If the IPSO image is on an FTP server, enter:

```
newimage -i -k
```

The installation procedures prompt you for the IP address of the FTP server and the path to the ipso.tgz file.

---

**Note**

On some appliances, installing the image can take some time. The newimage program might display the message "Setting up new image..." for several minutes with no other sign of activity.

---

3. If you are prompted to choose the image to load after the next reboot, choose the image you just added.
4. At the prompt, reboot your platform.

## Overwriting Existing Images (Fresh Installation)



---

**Caution**

The following procedure deletes any existing images and configuration information on your platform. Back up any files that you want to keep and copy them back to the platform after you install the new system.

---

Before you begin, make sure that you know:

- The serial number of your platform. The number is on a sticker attached to the platform and is preceded by "S/N."
- Whether the platform will run IGRP.
- Whether the platform will run BGP.
- An IP address that you will assign to the platform.
- The appropriate network mask length.
- The IP address of the FTP server.
- The path to the ipso.tgz file on the FTP server.
- The IP address of the default gateway for the platform.

- A host name to assign to the platform.
- An appropriate password to assign to the administrator account.
- The boot manager password (if any). If you need information about this password, see the *Nokia IPSO Boot Manager Reference Guide*.

---

**Note**

If you perform a fresh installation and later downgrade to an earlier version of Nokia IPSO, all current configuration information except basic connectivity information is deleted. For example, if you perform a fresh installation of IPSO 6.1 and later downgrade to IPSO 4.2, everything except your connectivity configuration is deleted after you reboot your platform.

---

The following section describes how to perform a fresh installation of the IPSO image using the **install** command.

## Performing a Fresh Installation

1. Download nkipflash-6.1.bin to the platform you will upgrade.

This file contains the IPSO 6.1 boot manager and is available on the Nokia support site on the same page as the IPSO 6.1 image.

---

**Note**

Nokia strongly recommends that you use the IPSO 6.1 boot manager to fresh install IPSO 6.1. If you install IPSO 6.1 on a platform running 6.0, using the 6.1 boot manager instead of the 6.0 boot manager can provide improved performance. You cannot use an IPSO 4.x boot manager to install IPSO 6.1.

---

2. Log on to the platform using a console connection if you have not done so already.
3. Navigate to the directory in which nkipflash-6.1.bin is stored.



4. Make sure that there were no download errors by creating a SHA1 or MD5 value for the file and verifying that it matches the value posted on the download page.

If the values are identical, the download was successful and the file is good. If not, download the file (in binary) again and repeat this procedure.

5. Enter:

```
upgrade_bootmgr [boot_device] nkipflash-6.1.bin
```

in which you should replace *boot\_device* with **wd0** or **wd1** as indicated below:

- Flash-based platforms: **wd0**
- Disk-based platforms (except IP2450): **wd1**
- Disk-based IP1280/IP2450: **wd0**

If the platform is currently running IPSO 6.0, you do not need to specify the boot device.

6. If you see a message similar to the following, type **y** to continue the upgrade. This message is misleading and can be safely ignored.

```
*** WARNING ***
```

```
wd1 does not look like a boot manager device.
```

```
Are you sure you want to write the boot manager image  
to wd1?
```

```
Continue? [n]
```

7. When the system indicates that the boot manager upgrade is complete, enter:

```
reboot
```

8. When the system enters autoboot mode and displays the following message

```
Type any character to enter command mode  
press any key to display the boot manager prompt:
```

9. At the boot manager prompt, enter:

```
set-defaults
```

- 10.** At the boot manager prompt, enter:

`install`

If a password is configured, the system prompts you to enter the boot manager password.

The installation script runs.

Follow the prompts to install the new IPSO image from an FTP server.

- 11.** If you are asked whether you want to upgrade the boot manager, choose to do so.

- 12.** If you are installing IPSO on a flash-based platform with one gigabyte of DRAM, do not choose to install packages when you see the message Retrieve all valid packages, with no further prompting? Your system does not have enough memory to extract the Check Point wrapper package, and the package installation will fail.

After you successfully install IPSO 6.1, use Network Voyager or the `newpkg` command to install your packages.

- 13.** At the end of the installation procedure, press Enter when you see this prompt:

Installation completed.

Reset system or hit <Enter> to reboot.

- 14.** After your platform reboots, follow the prompts to configure basic settings such as hostname and admin password.

- 15.** When you see the following message, type 1:

You can configure your system in two ways:

- 1) configure an interface and use our Web-based Voyager via a remote browser
- 2) configure an interface by using the CLI

Please enter a choice [ 1-2, q ]:

- 16.** Configure the appliance interface by responding to the prompts. When you see the following message, choose y (the default option):

Do you wish to set the default route [ y ] ?

If you choose n, you cannot use Network Voyager unless you do one of the following:

- Perform the installation procedure again and set a default route.
- Use the command-line interface over a console connection to create a default route or static route.
- Connect to the platform by using a system that is on the same network as a configured interface on the platform.

- 17.** When you are prompted to log in to the platform, you are ready to continue configuring your platform. Do one of the following:

- Log into the platform and use the `newpkg` command to install packages. For more information, see [“Using the newpkg Command”](#) on page 82.
- Use Nokia Network Voyager to complete the configuration (including installing packages). To log in by using Network Voyager, enter the IP address you configured for the platform in the URL field of your browser.

## Installing IPSO 4.x

When you install IPSO 4.x on a system running IPSO 6.1, you must install the 4.x boot manager and use it to perform a fresh installation—you cannot use Network Voyager or the `newimage` command. If you try to use Network Voyager or the `newimage` command, the installation will fail.

## Performing a Fresh Installation

When you install IPSO 4.x on a flash-based system running IPSO 6.1, follow the procedure explained below. (These instructions assume that you are installing IPSO 4.2.)

---

**Note**

To successfully install IPSO 4.x on a flash-based system, you *must* follow this procedure.

---

Note the following:

- If you use the boot manager for IPSO 4.2 Build 096 or later, the fresh installation procedure is identical for disk-based and flash-based systems. Nokia recommends that you use this boot manager when possible.
- If you do not use the boot manager for IPSO 4.2 Build 096 or later, you must perform additional steps on flash-based systems. These additional steps are clearly identified.

These instructions also apply to hybrid platforms—flash-based systems that have a disk for logging purposes.

1. Download the IPSO 4.2 boot manager (nkipflash-4.2.bin) to the system.
2. Log on to the platform using a console connection if you have not done so already.
3. Navigate to the directory in which nkipflash-4.2.bin is stored.
4. Make sure that there were no download errors by creating a SHA1 or MD5 value for the file and verifying that it matches the value posted on the download page.

If the values are identical, the download was successful and the file is good. If not, download the file (in binary) again and repeat this procedure.

5. Enter:

```
upgrade_bootmgr nkipflash-4.2.bin
```

6. When the system indicates that the boot manager upgrade is complete, enter:

```
reboot
```

7. When the system enters autoboot mode and displays the following message

Type any character to enter command mode  
press any key to display the boot manager prompt:

8. Proceed according to the situation applicable to you:

- If you installed the boot manager for IPSO 4.2 Build 096 or later, proceed to [step 12](#).
- If you did *not* install the boot manager for IPSO 4.2 Build 096 or later but you are installing IPSO 4.x on a disk-based platform, proceed to [step 12](#).
- If you did *not* install the boot manager for IPSO 4.2 Build 096 or later but are installing IPSO 4.x on a flash-based platform (including hybrid platforms), perform to [step 9](#) through [step 11](#).

9. Enter the following commands:

```
BOOTMGR> sh
# disklabel -r /dev/wd0s4 > /tmp/label
# disklabel -R /dev/wd0s4 /tmp/label
```

10. If you are installing IPSO 4.x on a hybrid platform (flash-based systems that have a disk for logging purposes) and are *not* using the boot manager for IPSO 4.2 Build 096 or later, follow the appropriate instructions in this step.

- If you are installing IPSO 4.x on a hybrid IP1280 or hybrid IP2450, enter the following commands:

```
# disklabel -r /dev/sd0s1 > /tmp/label
# disklabel -R /dev/sd0s1 /tmp/label
```

- If you are installing IPSO 4.x on a hybrid platform other than the IP1280 or hybrid IP2450, enter the following commands:

```
# disklabel -r /dev/wd1s1 > /tmp/label
# disklabel -R /dev/wd1s1 /tmp/label
```

11. Enter the following command:

```
# exit
```

12. Enter the following command at the `BOOTMGR>` prompt:

**install**

13. If you are installing IPSO 4.x on a flash-based platform (including hybrid platforms), enter **0** when you see the prompt

Select # of entry to install diskless image:

Otherwise, skip this step.

14. When prompted, choose an installation method for installing the IPSO 4.x image and continue with the installation process.

15. When prompted, reboot the platform.

## Installing and Activating Packages

After you install Nokia IPSO, you probably want to install Nokia documentation and Check Point packages. If you added a new version of IPSO by using the **newimage** command and the **-k** (keep) option, your previous packages are active with the new IPSO version. If you used **newimage** without **-k** option, all the optional packages currently installed on the platform are turned off, but they are not deleted. To turn these packages on again, see [“Activating Packages”](#) on page 81.

---

### Note

Nokia recommends that you install the latest documentation package whenever you upgrade IPSO.

---

If you performed a fresh installation of IPSO, you must install and activate the packages you want to use. You can do this by using Nokia Horizon Manager, Nokia Network Voyager, the command-line interface (CLI), or the **newpkg** command at the IPSO command shell.

---

**Note**

The installation process takes longer on flash-based systems than on comparable disk-based systems. For example, if you install a package on a flash-based IP690 and a disk-based IP690, the installation time is noticeably longer on the flash-based system. This is expected and does not indicate any problem.

---

You can download, install, or activate packages by using Horizon Manager on all of your Nokia platforms simultaneously or on groups of multiple devices simultaneously. Horizon Manager employs Do No Harm intelligence to prevent the installation of incompatible packages on Nokia platforms.

For information about how to use the CLI to install and activate packages, see the *CLI Reference Guide for Nokia IPSO*. You can get the *CLI Reference Guide* from Network Voyager, if the IPSO documentation package is installed, or by visiting the Nokia customer support web site. For information about using Horizon Manager to install and activate packages, see the *Horizon Manager User's Guide*.

For information about the `newpkg` command, see [“Using the newpkg Command”](#) on page 82. For information about how to install packages, see [“Using Nokia Network Voyager to Install Packages”](#) on page 79.

## Using Nokia Network Voyager to Install Packages

To install Nokia documentation and third-party packages by using Network Voyager:

1. Log on to your platform by using Nokia Network Voyager.
2. In the Network Voyager navigation tree, select Configuration > System Configuration > Packages > Install Package.
3. Enter the name or IP address of the FTP server.
4. Enter the path to the directory on the FTP server where the packages are stored.

5. If necessary, enter the appropriate user name and password.
6. Click Apply.  
The names of the available packages appear in the Site Listing window.
7. Select the package you want to install.
8. Click Apply.  
The selected package is downloaded to the platform. When the download is complete, the package appears in the Unpack New Packages field.
9. Select the package in the Select a package to unpack field.
10. Click Apply.
11. Click the link to install or upgrade the package.
12. (Optional) To display all installed packages, click Yes next to Display all packages; then click Apply.
13. (Optional) To perform a first-time installation, click Yes next to Install; then click Apply.
14. (Optional) To upgrade a package, click Yes next to Upgrade.
15. (Optional) To upgrade a package, click the button of the package that you want to upgrade under *Choose one of the following packages to upgrade from*.
16. Click Apply.
17. Click Save to make your changes permanent.

The packages are automatically activated as part of the installation process. To confirm the package installation and activation, check the Manage Packages page. If a package has not been activated, you can activate as described in [“Activating Packages.”](#)



### Caution

When you install a package using Voyager, you see the following message:

Voyager environment has been updated with the latest



package info.

The telnet session environment will be updated by:  
logging out and logging in again the telnet session.

This message might not be accurate. Click Manage Packages to verify that the package is installed. Refresh the page periodically until you see that the installation is complete.

---

---

**Note**

When the IPSO documentation package is activated, a link to the documentation is placed in the Network Voyager navigation tree. If you do not see that link after package installation or if the link takes you a previous version of the IPSO documentation, refresh your browser.

---

## Activating Packages

To turn on optional packages that were deactivated when you added a new version of Nokia IPSO by using the **newimage** command:

1. Log on to the platform using Nokia Network Voyager.
2. In the Network Voyager navigation tree, select Configuration > System Configuration > Packages > Manage Packages.
3. Click On next to the packages you want to turn on.
4. Click Apply.
5. Click Save.
6. Reboot your platform.

Your installation of IPSO 6.1 is complete, and the packages that you selected are activated.

## Using the newpkg Command

Use the **newpkg** command to add or upgrade documentation and third-party packages.

The syntax of **newpkg** is:

```
newpkg [-d] [-h] [-q] [i] [-u] [-D] [-help] [-?] [-l  
user_name] [-m media_type] [-n path]  
[-o path] [-p password] [-s server_ipaddrs] [-S] [-v]
```

[Table 13](#) describes the options you can use with the **newpkg** command.

**Table 13 newpkg Options**

|                         |   |
|-------------------------|---|
| -d                      | Print debug messages.   |
| -h                      | Display help lines for command-line parameters.   |
| -q                      | Query for currently installed packages.   |
| -i                      | Install only (do not activate). If you use this option to install the firewall wrapper package, the wrapper might not use this option when it installs its component packages. In that case, the component packages are activated after they are installed. |
| -u                      | Uninstall a currently installed package.  |
| -D                      | Deactivate a currently installed package.   |
| -a                      | Activate a currently installed package.   |
| -l <i>user_name</i>     | User name for FTP.  |
| -m <i>media_type</i>    | Media type; for example, FTP, CD, and so on.  |
| -n <i>path</i>          | Full path to new package.   |
| -o <i>path</i>          | Full path to old package for upgrade.   |
| -p <i>password</i>      | Password for FTP.   |
| -s <i>server_ipaddr</i> | The server IP address if media type is FTP/AFTP.  |
| -S                      | Silent mode. Silent mode requires the following options: -o, -m, -n. If the media type is FTP/AFTP, silent mode also requires -s. If the media type is FTP, silent mode also requires -l, -p.   |
| -v                      | Verbose FTP.  |
| -help                   | Display help text.  |
| -?                      | Display help text.  |

---

**Note**

The `newpkg` command is automatically invoked if you perform a fresh installation. You are prompted to install or skip each package.

---

To turn on the installed packages, continue with the procedure in “[Activating Packages](#)” on page 81.

## Upgrading Check Point NGX

IPSO 6.1 supports NGX R65 for IPSO 6.0 and does not support any other version of the Check Point firewall. You can upgrade to this version of the firewall from several earlier versions, but you cannot upgrade to NGX R65 for IPSO 6.0 from NGX R65. See the Check Point *Upgrade Guide* to learn whether you can upgrade to this release from the version you have.

For more information about upgrading to R65 for IPSO 6.0, see the *Check Point for Nokia IPSO Getting Started Guide and Release Notes*, which is available at <https://support.nokia.com>.

# 5

## Limitations and Configuration Tips

Nokia wants to hear about information you might have regarding the limitations in this chapter. For information about how to contact Nokia Customer Service, see the contact information at the beginning of this document.

The following sections describe configuration tips and known limitations associated with IPSO 6.1. To see the most current list of limitations, see the version of this document available on the Customer Support Web site. The number in angle brackets after each heading is the tracking number for the issue in Nokia's internal database of problem resolutions. Reference this number if you contact Nokia about an item in this chapter.

For the most current information about resolutions to problems, see the Customer Support Web site at <https://support.nokia.com>. Records are continually added to this site.

### Configuration Tips

This section provides suggestions that you might find useful when configuring IPSO 6.1 on a Nokia IP security platform.

## Authentication Change [<PR 62264>](#)

Nokia IPSO implements Pluggable Authentication Modules (PAM), an industry-standard framework for authenticating and authorizing users. Using PAM, authentication, account management, and session management algorithms are contained in shared modules that you configure on your appliance. If you configure a system so that users can be authenticated only by a PAM-based method (you disable local authentication), you cannot log in using a console connection.

## Cabling an IP2450 Platform [<PR 59433>](#)

When cabling an IP2450 platform with copper cables, follow these guidelines:

- If you directly connect two IP2450 platforms (back-to-back), use a crossover cable.
- If you connect an IP2450 to a switch or hub, use a straight-through cable.

## Use Half Duplex with Hubs [<PRs 58700, 64217>](#)

When connecting a Nokia network security platform to a hub, configure the Nokia interface to use half duplex duplicity. If you set the interface to full duplex, the link will come up but many collisions will occur, which could cause the link to flap or fail.

## Optional Disks Erased when Selected

When you select a hard disk or card as an optional disk, any existing data on the device is erased. If you remove a PC card that contains log files and want to permanently store the data, insert the card into a PC or other computer and save the data to that system before reinserting the card into a Nokia flash-based platform. [<PR 45065>](#)

The IPSO CLI allows you to reselect an optional disk that you have already selected by reissuing a `set optional-disk` command. Doing so repartitions the optional disk. [<PR 56513>](#)

## Configuring Remote Core Dump Servers [<PR 59010>](#)

You can configure flash-based systems to transfer both application and kernel core files to a remote FTP server. When you do so, IPSO uses the user name `ftp` and the password `passwd` to log into the remote server anonymously. Some FTP servers do not allow this user name and password for anonymous logins. If this is true of your FTP server, you must create a user with this user name and password to allow IPSO to transfer application and kernel core files to the server.

## Complete All Fields When Creating Users [<PR 52479>](#)

When you create a new user, you must fill in the fields for Username and UID and complete the entry for Home Directory. The home directory should be `/var/emhome/<username>`. If you do not complete these fields, an error message appears that says “not all fields are complete”.

## Providing User Access to Monitor Pages [<PR 51692>](#)

When you assign a role that provides access to a feature, the user gets access to the configuration pages for that feature but not to the monitor pages. To provide access to the monitor pages, you must include the monitor privilege for that feature in the role definition.

## SNMP User `privpassphrase` Option Inaccurately Displayed [<PR 51849>](#)

When you use the tab completion feature of the CLI to view the options for adding or modifying an SNMP user that has a security level of `authNoPriv`,

the `privpassphrase` option is displayed. You do not need to set a privacy pass phrase for a user with a security level set to `authNoPriv` and you can ignore this option in this case. If you attempt to set a privacy pass phrase, a message appears indicating that this is not necessary.

## Audit Log Setting Not Permanently Saved [<PR 51861>](#)

The system configuration audit log setting is not saved in the configuration file. You must reset it after a reboot to enable logging again. You set the system configuration audit log using Network Voyager by clicking System Logging under Configuration > System Configuration and selecting either Logging of Transient Changes or Logging of Transient and Permanent changes. With the CLI, you set this parameter with the following command:

```
set syslog auditlog <disable | transient | permanent>
```

## Terminal Emulator Display Configuration [<PRs 53184, 53382>](#)

If you use a terminal emulator (such as Microsoft Windows HyperTerminal) to connect to an IP390 or IP560, the system may display undesirable foreground and background colors as selected by the emulator software. To allow the IP390 or IP560 to automatically select the colors (typically white letters on a black background), configure your terminal emulation software to recognize ANSI characters with full ISO color emulation.

To configure HyperTerminal in this way, perform these steps:

1. Pull down the File menu and select Properties.
2. In the Properties dialog box, select the Settings tab.
3. Set the emulation to ANSI.
4. Click OK.

As an alternative approach, you can disable ANSI emulation and manually configure the foreground and background colors.



## Do Not Insert or Remove PC Card During Boot <PR 55218>

Do not insert or remove a PC card while a Nokia platform is starting up (for example, before you see the login prompt at the command line). Doing this can cause the system to hang.

## Route Maps with BGP Confederations <PR 51672>

You cannot use route maps in BGP confederations. To configure route filters and redistribution for BGP confederations, use the Inbound Route Filters and Route Redistribution pages in Network Voyager.

## Workaround to Disable ifwd Daemon <PR 56616>

Check Point firewall versions NGX R60 and later do not require the ifwd daemon. Whether the ifwd daemon is running or not has no affect on the firewall operation.

If you want to permanently disable the ifwd daemon, perform these steps:

1. In the Network Voyager navigation tree, select Firewall and Other Packages.
2. Click the Check Point Firewall-1 link.
3. Click the off radio button after the Run ifwd daemon to monitor interface changes? question.
4. Click Apply.
5. Because there is no Save button on this page, you need to save your changes from another Network Voyager page:
  - a. Go to any other Network Voyager configuration page.
  - b. Click in a text box on the page. This enables the Save button.
  - c. Click Save.

## Limitations

This section includes information about limitations in IPSO 6.1.

### **PBR Does Not Work with VPNs** <PR 80124>

Policy based routing (PBR) does not work if a VPN is enabled on the system.

### **Issue with UDLD Under Heavy Traffic** <PRs 5548, 80246>

If you enable the Cisco Unidirectional Link Detection (UDLD) protocol on a fiber-optic interface (to improve detection of partial link failures), a problem can occur if the platform receives very heavy traffic. Under this condition, some UDLD packets might get dropped, which causes IPSO to see the link as unidirectional and deactivate the interface.

If IPSO deactivates a UDLD interface, a connected Cisco switch also deactivates the corresponding port and does not reactivate that port without user intervention unless configured to do so.

### **Issue with ADP Interface LEDs** <PR 59595>

If you have an RJ-45 only ADP services module (one that does not use SFP modules) in an IP2450 or IP1280, a problem occurs if you disable the Autoadvertise option for an interface while there is no cable connected to the interface. In this situation, the interface link LED on the module illuminates, incorrectly indicating that the link is active. Voyager also incorrectly indicates that the link is active. This problem does not occur with fiber optic interfaces or with RJ-45 SFP modules.

### **Issue with IKE Acceleration and IP690 ADP Module** <PR 67665>

If you attempt to enable IKE acceleration for a VPN tunnel that terminates at an interface on an Accelerated Data Path (ADP) module installed in an IP690

platform, the system does not accelerate IKE traffic and you see console errors similar to the following:

```
Dec 3 11:07:56 IP690-zulu <daemon.[LOG_ERR]>openCryptokiModule
[1460]: PKCS11 config initialization: No Hardware Tokens
Present
```

## Error Message When Deleting NGX R65 for IPSO 6.0 Package <PR 64890>

If you delete the NGX R65 for IPSO 6.0 package using Network Voyager, you might see an error similar to the following in the Success notice box:

```
*****
ERROR: Fail to find /opt/Cpsuite-R65/Cpinstall/Xinstall
*****
/opt/Cpsuite-R65/UNINSTALL:/opt/Cpsuite-R65/Cpinstall/
xinstall:not Found
/opt/Cpsuite-R65/UNINSTALL:/opt/Cpsuite-R65/Cpinstall/
xinstall:not Found
```

You can ignore this error. The package has been deleted successfully.

## Silent Mode Support in newpkg <PR 64839>

The newpkg command does not support silent mode (-S) for package activation (-a) or deactivation (-D). The newpkg help incorrectly documents it as doing so.

