NOKIA

IPSO 3.7
Getting Started Guide and Release Notes

Part No. N451062001 Rev A

Published June, 2003

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Internet Communications. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: ipsecurity.na@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: ipsecurity.emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: ipsecurity.apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/		
Email:	tac.support@nokia.com		
Americas		***Europe***	
Voice:	1-888-361-5030 or 1-613-271-6721	**Voice:**	+44 (0) 125-286-8900
Fax:	1-613-271-8782	**Fax:**	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

021216

Contents

1 New Features in Nokia IPSO 3.7

Nokia is pleased to introduce a new version of the IPSO operating system used on Nokia appliances. IPSO 3.7 BUILD 023 contains the following new features and enhancements to existing features:

- Runs on all IPSO platforms
- Clustering improvements
- Simplified VRRP configuration
- Transparent mode
- Session management
- CLI improvements
- Secure Shell enabled by default (new systems only)
- SSH and SSL upgraded
- SNMP enhancements
- Routing enhancements
- TCP MSS configuration
- Voyager AuditLog
- New IPSO build naming convention
- Supports new versions of partner applications

See "Downloading IPSO 3.7 and Related Files" on page 32 for information about downloading IPSO 3.7 and other items from the Nokia customer support Web site.

Runs on All Platforms

IPSO 3.7 runs on all Nokia IPSO appliances, including the IP350 and IP380.

Clustering Improvements

IPSO's clustering feature provides load balancing by distributing traffic across the multiple appliances (nodes) in a cluster. It provides fault tolerance, because a cluster continues to function if a node fails or is taken out of service for maintenance purposes. The nodes in a cluster share IP addresses and appear as a single system to the networks on either side.

IPSO's clustering capabilities have been significantly enhanced in version 3.7, as explained below. For a detailed explanation of how to use IPSO clustering, see the *IPSO 3.7 Clustering Configuration Guide.* (You can find this document in the Doc folder of your IPSO CD and on the Nokia customer support Web site.)

Simplified Configuration

IPSO 3.7 makes it easier to set up clusters. When systems join an existing cluster (including a one-node cluster), they automatically learn configuration information from the first node and configure themselves with the appropriate settings. This facilitates cluster configuration and helps you avoid issues that can arise because of inconsistencies on different nodes.

The automatic method of setting up IPSO clusters is optional. Should you prefer, you can manually configure each cluster node.

Cluster Management

With IPSO 3.7, you can manage all the nodes of a cluster simultaneously—that is, you can manage multiple nodes as if they are a single device. This feature makes it easier to configure and manage clusters.

IPSO 3.7 offers two new ways to manage clusters:

- Cluster Voyager (a web-based interface based on Nokia Network Voyager)
- Cluster command line interface (CCLI)

Backup Cluster Protocol Network

IPSO 3.7 eliminates the cluster protocol network as a potential single point of failure. You can now configure a backup network that will carry the cluster protocol traffic should there be any failure on the primary cluster protocol network. In the event of a failover, there is no interruption in cluster services.

Additional Clustering Mode

IPSO clusters now have two modes of operation—multicast mode and forwarding mode. Nokia provides this choice so that IPSO clusters can work in different network environments.

Multicast mode usually offers better throughput because it uses network bandwidth more efficiently. If you use this mode, routers and servers adjacent to the cluster must be able to accept ARP replies that contain a multicast MAC address. Switches connected directly to the cluster must be able to forward packets destined for a single (multicast) MAC address out multiple switch ports.

Forwarding mode allows you to use IPSO clustering if the routers and switches on either side of the cluster do not support multicast MAC addresses.

Simplified VRRP Configuration

You can use IPSO's Virtual Router Redundancy Protocol (VRRP) feature to create redundant firewall configurations. IPSO versions previous to 3.7 include monitored-circuit functionality that enhances the capabilities of standard VRRP.

IPSO 3.7 includes the original method for configuring monitored circuit and also offers a simplified method for setting up VRRP in a monitored-circuit configuration.

Transparent Mode

IPSO 3.7 introduces transparent mode, a feature that lets you avoid network reconfiguration issues that can arise when deploying a VPN or firewall device. Transparent mode allows an IPSO appliance to function as if it is a layer 2 device such as a switch or bridge and still run VPN-1/FireWall-1. If you use this mode, you can add VPN and firewall functionality without reconfiguring your network or changing existing IP addresses.

You can specify which interfaces act like bridge ports, and these interfaces form a transparent mode group. Interfaces that are not part of the group can be configured for routing, so you can configure an IPSO appliance to act like a bridge and router simultaneously.

You can use VRRP with transparent mode to provide redundancy. You cannot use transparent mode and IPSO clustering on the same appliance.

Session Management

IPSO session management lets administrators prevent multiple users from making simultaneous configuration changes. This feature lets you acquire an exclusive configuration lock so that other users cannot make configuration changes to an appliance while you are logged into it. Sessions are logged out automatically after a time period that you can specify, and you can also

manually log out from any configuration or monitoring screen. You can view the history of log ins and log outs in the system logs.

Session management is enabled by default but can be easily disabled.

CLI Improvements

IPSO's command-line interface (CLI) has been enhanced to add functionalities similar to those of standard Unix shells.

SSH Enabled by Default

If you purchased an appliance with IPSO 3.7 installed, Secure Shell (SSH) is enabled by default. This means that you can use an SSH client application to connect to a network interface on the appliance and use the IPSO command shell or command-line interface (CLI). Telnet is also enabled by default. Nokia recommends that you disable telnet and use an SSH client to manage the appliance. See "Using the CLI" on page 26 for more information.

If you upgrade a system to IPSO 3.7, SSH is enabled by default only if it was enabled before the upgrade.

SSH and SSL Upgraded

IPSO 3.7 incorporates the following open source modules for Secure Shell (SSH) and Secure Sockets Layer (SSL):

- OpenSSH Version 3.1p1, which includes:
  - support for RSA keys for SSH version 2
  - support for secure FTP (SFTP and SCP)
- OpenSSL Version 0.9.6d
- Mod SSL Version 2.8.8

SNMP Enhancements

IPSO 3.7 includes the following SNMP enhancements:

- You can now limit the SNMP access to SNMPv3 only. If you configure SNMP this way, you cannot configure community strings, and they are not shown in the SNMP configuration page. IPSO continues to support SNMP v1 and v2.
- Support for three new hardware traps:
  - systemPowerSupplyFailure
  - systemFanFailure
  - systemOverTemperature.
- The configuration of the Trap PDU Agent address is changed in accordance with RFC 2089. If you do not configure a Trap PDU Agent address, the system identifies the PDU Trap Agent address as 0.0.0.0 in SNMP traps. In previous releases of IPSO, the default is to use the IP address of the first valid interface.
- Both the online Voyager documentation and the *IPSO 3.7 CLI Reference Guide* now include information about the most common SNMP error messages.
- SNMP proxy for the Check Point MIB (see the next section for details).

SNMP Proxy for Check Point MIB

IPSO 3.7 uses a proxy to support SNMP GET and SNMP GETNEXT requests for Check Point objects. The following are guidelines and limitations of which you should be aware:

- You must use the Check Point version of the Check Point MIB (CP-MIB) text file in $FWDIR/lib/snmp of your network management tool.

- Whenever IPSO SNMPd is started or restarted, it searches for the CheckPoint-MIB.txt. The following is an example of a message you may see as a result of the search:

  ```
  IP650 [admin]# Jan 31 12:17:19 IP650 [LOG_ERR] snmpd:
  Cannot find module (CheckPoint-MIB) : At line 1 in
  (none)
  ```

  You can ignore this message.

- Any SNMP requests sent to the CP-MIB when the Check Point SNMPd (CP-SNMPd) is not running will time out. (The IPSO SNMPd will not respond.)
- The SNMP Proxy is not a trap proxy and will only proxy SNMP GET and SNMP GETNEXT requests.
- When simultaneous SNMP queries arrive, the SNMP Proxy will return valid values to only one request.
- The SNMP Proxy is hard-coded to work only with the CP-SNMPd. It is not a generic proxy that can be used for accessing other MIBs. If you change the following default configurations, the SNMP Proxy for the CP-MIB will not work:
  - CP-SNMPd must continue to run on port 260.
  - CP-SNMPd must continue to accept SNMPv1 and have a read community set to “public.”
  - CP-SNMPd must continue to be accessible through “localhost” on the IPSO device.

Because IPSO uses a proxy to support the Check Point MIB, please reference the Check Point documentation for any limitations of CP-SNMPd.

Using cpsnmp_start

If you use VPN-1/FireWall-1 NG FP3, you must run the cpsnmp_start script to make sure CP-SNMPd is running. You do this by first enabling the IPSO SNMPd from Voyager and then enabling the CP-SNMPd using /bin/cpsnmp_start on the command line. Whenever you use the **`cprestart`**,

cpstop, or **cpstart** commands, you must run the cpsnmp_start script to restart CP-SNMPd.

Using FloodGate with VPN-1/FireWall-1 NG FP3 causes SNMP query operations to fail, even for non-FloodGate CheckPoint MIB objects—you must restart CP-SNMPd to support SNMP query operations.

Routing Enhancements

IPSO 3.7 contains the routing enhancements explained below.

PIM High-Availability Mode

IPSO 3.7 includes an enhancement to PIM Sparse-Mode that supports a high-availability (HA) mode for situations in which two routers are configured to back each other up for forwarding multicast traffic. HA mode ensures that if any PIM-enabled interface goes down, all PIM-enabled interfaces become unavailable and remain in that state until all the interfaces are back up. Because it is not necessary, HA mode is not supported with PIM Dense-Mode.

EBGP TTL Configuration

IPSO's implementation of the Border Gateway Protocol (BGP) has been enhanced. You can now specify a TTL value when configuring multihop for external BGP neighbors that are not physically connected.

TCP MSS Configuration

IPSO 3.7 allows you to configure the TCP maximum segment size (MSS) that IPSO advertises for incoming packets. This is also the maximum segment size for packets generated by the appliance. You can use this feature—which you access under the link Advanced System Tuning in the System Configuration

section on the main configuration page—to configure the system so that the packets it sends and receives are as large as possible without causing fragmentation.

You can use this feature to maximize the performance of Check Point security servers or similar products that require a Nokia appliance to terminate TCP connections.

Voyager AuditLog

The Voyager AuditLog tracks each time the *Apply* and *Save* buttons are clicked. Each time these buttons are clicked, the log records the names of the user, Voyager page, and button. The log records the button clicks regardless of whether the operation succeeded. (The log does not record whether or not the operation was successful.)

New IPSO Build Naming Convention

Beginning with IPSO 3.7, Nokia is using a new method for naming IPSO builds. Specific builds are identified by the word “BUILD” and a build number on the Voyager home page and in other locations. IPSO builds are no longer identified with “FCS” and an accompanying number.

Partner Applications

The Nokia IPSO 3.7 operating system supports the following partner applications on Nokia appliances. The features and operation of the available applications are described in separate documents.

- Check Point VPN-1/FireWall-1 Next Generation, Feature Pack 3, with Hot Fix 2 (or later)
- Check Point VPN-1/FireWall-1 Next Generation with Application Intelligence

- RealSecure for Nokia, Version 7.0 (intrusion detection system)

2 Performing the Initial Configuration

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

- You can perform the configuration in an automated fashion by using the built-in dynamic host configuration protocol (DHCP) client.
- You can do it manually by using a console (direct serial) connection.

After you decide which method to use, follow the instructions under "Using DHCP to Configure the System" (below) or "Using the Console to Configure the System" on page 22 to perform the initial configuration. Regardless of which method you use, see "Performing Additional Configuration" on page 26 for important information about how to proceed after you complete the initial configuration.

Using DHCP to Configure the System

IPSO's DHCP feature allows a properly configured DHCP server to provide your system with a

- Host name
- IP address
- Default route

You can then use Nokia Network Voyager to reconfigure any of these settings. Once you do so, Voyager keeps the modified settings. (DHCP is not used if configuration information already exists.) The 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 the DHCP server.
2. Run the DHCP client on the Nokia system.

Configure the DHCP Server

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

- A host name for the Nokia system
- The serial number of the appliance
- A static IP address for the appliance

(IPSO also supports MAC-address based configuration.)

The minimum IP address lease required is one year.

Note
The DHCP server must be on the same network as the Nokia appliance or DHCP/BOOTP relay must be configured on the intermediate routers.

Below is an example of 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 time-offset              -8;
   option domain-name-servers      24.5.207.179;

   range dynamic-bootp 10.1.1.20 10.1.1.100;
   default-lease-time -1;
   max-lease-time -1;

   host IP710fixed {
      # serial number of the box
      option dhcp-client-identifier "123456";

      fixed-address 10.1.1.11;
      option host-name "IP710";
   }
}
```

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 appliance.

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

The DHCP client program in the system starts automatically, and the 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 the DHCP server to provide to the Nokia system.

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

4. Connect to the system 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.

See "Performing Additional Configuration" on page 26 for information about how to proceed. If you intend to use the IPSO CLI or shell, be sure to see "Using the CLI" on page 26.

Using the Console to Configure the System

If you are installing a new appliance 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 appliance.
- An IP address that you will assign to the appliance.
- The appropriate network mask length.
- The IP address of the default gateway for the appliance.

- An appropriate password to assign to the administrator account.

Performing the Configuration

1. Establish a physical console connection to the appliance.

   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 appliance.

      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 appliance on.

3. 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 I*nstallation Guide* for troubleshooting suggestions.

4. 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 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.

c. Enter

```
rm /config/active
```

or

```
mv /config/active /config/active.old
```

d. Reboot the appliance.

e. Respond to the configuration prompts in a timely manner.

5. When you see the message

```
You can configure your system in two ways:
  1) configure an interface and use our Web-based
  Voyager via a remote browser
  2) VT100-based Lynx browser
Please enter a choice [ 1-2, q ]:
```

type 1.

6. 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 example above `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 you want to configure. Remember that this is the interface you will connect to with Voyager or the CLI to continue with the configuration.

7. When prompted, enter the IP address and subnetwork mask length when prompted to do so.
8. When you see the message

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

   choose y (the default option). If you choose n, you cannot use 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 appliance using a system that is on the same network as a configured interface on the appliance.
9. If you have a modem installed, you see a message similar to the following:

   ```
   Modem detected on /dev/cuaa1.
   Enable logins on this modem [y,n]:
   ```

   If you want to enable logging into the appliance through the modem, you can configure the modem now or you can configure it in Voyager or the IPSO CLI after you complete the installation.

   If you want to configure the modem for logins now, type y. You are then prompted to configure a country code for the modem. See "Modem Country Codes" on page 51 for a list of the valid country codes.
10. 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

- Nokia Network Voyager
- the IPSO CLI

Using Voyager

To log into the system using Voyager, follow these steps:

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

Using the CLI

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

- Use an SSH client. This is the recommended approach. See "Using an SSH Client" for more information.

  If you do not want users to be able to access the system with an SSH client, see "Disabling SSH" on page 29 for information about how to disable SSH.

- Connect to the configured network interface using telnet or rlogin.

To maintain optimum security, Nokia recommends that you disable telnet and use an SSH client. See "Disabling Telnet" on page 28 for information about how to disable telnet.

Note
SSH does not apply to console connections. Regardless of whether SSH is enabled, you can always access the appliance over a console connection.

Using an SSH Client

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

At a minimum, you should use a host key as explained under "Using a Host Key." For even better security, use authorized keys as well. For more information about how to use SSH with your Nokia system, see the *Voyager Reference Guide* (available on the Nokia Security Platform Software CD that came with your appliance) or press the Doc button in Voyager.

Using a Host Key

IPSO automatically generates a host public/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 appliance, 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.

Once a workstation has the host public key (regardless of how it received it), the SSH client program will be able to connect to the Nokia system as long as the host public/private key pair is valid.

Disabling Telnet

You can use Voyager or the IPSO CLI to disable telnet.

Note
You must have telnet enabled on your Nokia appliances for Nokia Horizon Manager to communicate with the appliances in the unsecure mode. See the Horizon Manager documentation for more information.

Using Voyager to Disable Telnet

1. Log into the appliance using Voyager.

   Enter the user name `admin` and the password you configured for this user when you performed the initial configuration.
2. On the Voyager home page, click the link *Security and Access Configuration*.
3. Click the link *Network Access and Services.*
4. Next to **ALLOW TELNET ACCESS,** click **NO.**
5. Click *Apply.*

Using the CLI to Disable Telnet

Follow these steps to use the IPSO CLI to disable telnet:

1. Establish a console connection to the appliance.
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 Voyager or the IPSO CLI to disable SSH.

Note
SSH must be enabled on your Nokia appliances for Horizon Manager to communicate with the Nokia appliances in the secure mode. See the Horizon Manager documentation for more information.

Using Voyager to Disable SSH

Follow these steps to use Voyager to disable SSH:

1. Log into the appliance using Voyager.

   Enter the user name `admin` and the password you configured for this user when you performed the initial configuration.
2. On the Voyager home page, click the link *Security and Access Configuration*.
3. Click the link *SSH (Secure Shell)*.
4. Next to **ENABLE SSH SERVICE (DAEMON SSHD)**, click **NO**.
5. Click *Apply.*

Using the CLI to Disable SSH

Follow these steps to use the IPSO CLI to disable SSH:

1. Establish a console connection to the appliance.
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 ssh server enable off
   ```

3 Upgrading to IPSO 3.7

You can upgrade directly to IPSO 3.7 from the following IPSO versions:

- 3.4.1
- 3.4.2
- 3.5
- 3.5.1
- 3.6

You can also revert to those earlier versions of IPSO from IPSO 3.7 if they were previously installed on your appliance. Reverting to earlier versions of IPSO that were not installed on your appliance can be problematic (in rare cases) and is not guaranteed.

Caution
IP350 and IP380 appliances can be upgraded to IPSO 3.7, but they cannot be upgraded or downgraded to IPSO 3.6. These systems do not work with versions of IPSO other than 3.5.1 and 3.7

Note
If you use Nokia Horizon Manager to manage your appliances, you can upgrade and revert to earlier versions of IPSO on all your appliances simultaneously or in groups of multiple appliances. Horizon Manager employs “Do No Harm” intelligence to prevent incompatible package installations on Nokia appliances.

If you attempt to install a version of IPSO on an appliance that does not support that version, the installation process does not proceed and you see a message explaining the issue.

You can obtain IPSO 3.7 from the CD-ROM that is provided with the Nokia IPSO 3.7 Release Pack. You can also obtain IPSO 3.7 by downloading the software from the Nokia support site at https://support.nokia.com.

You can install IPSO and packages using

- Nokia Horizon Manager (on multiple Nokia appliances simultaneously)
- Nokia Network Voyager (on a single Nokia appliance at a time)
- IPSO CLI
- IPSO command shell (console session)

You can also install IPSO and packages on multiple cluster nodes simultaneously using Cluster Voyager or the Cluster CLI. See the *IPSO 3.7 Clustering Configuration Guide* for more information.

Downloading IPSO 3.7 and Related Files

To download IPSO 3.7 and related files and documentation, follow this procedure.

1. Access the Nokia customer support Web site at https://support.nokia.com.
2. Log in using your user name and password.
3. In the pull-down menu under Product Homepages, select IP Security Platforms.

4. On the IP Security Platforms page, click the link for IPSO 3.7 under Software Downloads.
5. Click the links for the items you want to download.

   If you want to download IPSO 3.7, continue with this procedure.
6. Locate the link for downloading ISO 3.7.

   Before you click the link to download IPSO 3.7, copy or take note of the MD5 value displayed near the link.
7. Click link for downloading IPSO 3.7.
8. Download the `ipso.tgz` file to an FTP server or workstation.

You can now install IPSO 3.7 remotely from the FTP server or workstation. (See "Installing IPSO 3.7 from Voyager or the Command Shell" on page 37.)

Using Nokia Horizon Manager to Install IPSO and Packages

You can use Nokia Horizon Manager 1.3 to automate the process of installing, upgrading, and enabling IPSO 3.7 and software packages on multiple Nokia appliances. Horizon Manager employs "Do No Harm" intelligence to prevent any incompatible IPSO version upgrades. Use the OS Install action to install IPSO 3.7 on as many as 2500 platforms in a single data set. Horizon Manager 1.3 also provides actions that automate the installation and upgrade of software packages, such as Check Point NG and associated feature packs. Horizon Manager automates the entire installation process, including backing up configuration information prior to the upgrade and rebooting appliances 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 may not need to use this document further.

See the Horizon Manager documentation for detailed information about the installation and upgrade process.

Before You Install IPSO from Voyager or the Command Shell

You need at least 140 megabytes of free disk space in your root partition to install an IPSO 3.7 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 140000 K bytes, you should make more space available in the root partition by deleting the temporary files specified below if they are present. (These files may 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
rm -f /image/VERSION
mount -ur /
```

If you use the `df` command after you install IPSO 3.7 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 3.7, you can safely ignore this output from `df`.

Once you have enough space in the root partition, follow the instructions under "Putting ipso.tgz on the Appliance" on page 34.

Putting ipso.tgz on the Appliance

After you make sure that there is a least 140000 K bytes available on the root partition, you need to put `ipso.tgz` on an FTP server and then transfer this file to the appliance. There are two approaches you can take for transferring `ipso.tgz`:

- You can FTP it to the appliance and install IPSO in one procedure.

Follow the appropriate instructions under "Installing IPSO 3.7 from Voyager or the Command Shell" on page 37.

- You can FTP it to the appliance first and then install IPSO in a separate procedure.

  Follow the instructions under "Transferring ipso.tgz" and "Verifying MD5 Values" on page 36 and then follow the appropriate instructions under "Installing IPSO 3.7 from Voyager or the Command Shell."

Caution
If you perform a fresh installation of IPSO, you must download `ipso.tgz` and perform the installation at one time. Do not copy the `ipso.tgz` to the appliance first—it will be overwritten during the installation procedure. For more information, see "Overwriting Existing Images (Fresh Installation)" on page 41.

Transferring ipso.tgz

Transferring IPSO 3.7 to your appliance 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 appliance. To do so:
   a. On the Voyager home page, click *Config*.
   b. In the *Security and Access Configuration* section, click the *Network Access and Services* link.
   c. In the *Allow FTP access* field, click *Yes*.
   d. Click *Apply*
   e. Click *Save* to make your change permanent.

2. To copy IPSO 3.7 from a workstation:
   a. Insert the CD-ROM into the CD drive of the workstation.
   b. Make sure that you can connect to the Nokia appliance over the network.
3. Open the directory on the FTP server or workstation that contains `ipso.tgz` (this can be the `image` directory on the CD-ROM).
4. Begin an FTP session to your appliance.

   By default, the current directory should be `var/admin`. Do not change the current directory.
5. At the prompt, enter

   `bin`
6. Transfer `ipso.tgz` to the appliance. At the prompt, enter

   `put ipso.tgz`
7. Close the FTP session.

Verifying MD5 Values

Use the MD5 application to verify that the `ipso.tgz` file originated at Nokia and did not change during the download process.

1. Log on to the appliance through a console connection.
2. At the prompt, enter

   `md5 nkipflash.bin.`

   You should see a response that displays the same MD5 value that matches the MD5 value shown at the Nokia support site. For example, you should see something like

   `MD5 (nkipflash.bin) = 1b248152586d0599e27130b1251c38c6`

Note
The preceding MD5 value is an example only. You will see a different value.

3. Compare the MD5 value you see to the value posted on the Nokia support site.

   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.

To complete your installation of IPSO, proceed to the following section.

Installing IPSO 3.7 from Voyager or the Command Shell

Note
If you intend to upgrade Check Point's VPN-1/FireWall-1, do so before you upgrade IPSO. See "Upgrading Check Point VPN-1/FireWall-1 NG with the IPSO Command Shell" on page 50. IPSO 3.7 supports VPN-1/FireWall-1 FP3 with Hot Fix 2 (and later).

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

- You can 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 easily revert to the earlier versions stored on the appliance. When you do so, your configuration information is not affected.

  If you copied `ipso.tgz` to the appliance you are upgrading as described in "Transferring ipso.tgz" on page 35, you must use this method.

You can use Voyager, the IPSO shell, or the IPSO CLI to add an image. The procedures for using Voyager and the IPSO shell are explained below. See the *IPSO 3.7 CLI Reference Guide* for information about how to add an image using the IPSO CLI.

- You can 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.

  "Overwriting Existing Images (Fresh Installation)" on page 41 explains how to perform a fresh installation.

Adding an IPSO Image Using Voyager

Note
If you intend to upgrade Check Point VPN-1/FireWall-1, do so before you upgrade IPSO. See "Upgrading Check Point VPN-1/FireWall-1 NG with the IPSO Command Shell" on page 50. IPSO 3.7 supports VPN-1/FireWall-1 FP3 with Hot Fix 2 (and later).

Using Voyager is a convenient way to add an IPSO image to an appliance. To see the instructions about how to do this, follow these steps:

1. On the Voyager home page, click *Doc*.
2. Click *System Configuration*.
3. Scroll down to the section Installing New IPSO Images and click *Upgrading the IPSO Image.*

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 using the CLI, see the "System Configuration Commands" section of the *CLI Reference Guide for IPSO 3.7*. To access this document, click Doc on the Voyager home page, then click the link for the *CLI Reference Guide*. The *CLI Reference Guide* is also included on the Nokia Security Platform Software CD that came with your appliance.)

Note
When you add an image or perform a fresh installation using the IPSO command shell, use a console connection (rather than 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 1 describes the options you can use with the `newimage` command.

Table 1 newimage options

`-i`	Load a new image interactively. Interactive mode supports anonymous FTP, FTP with a user name and password, access to a CD-ROM (IP440 only), and access to the local file system.
`-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 (not supported on IP440).
`-r image_name`	Specify image to run at next boot.

`-t image_name`	Specify image to run at next test boot (not supported on IP440).
`-k`	Do not deactivate existing packages. The `-k` option keeps all the previously installed packages in their current states. If a package from a previous version of IPSO was enabled and configured to start at boot, it continues to do so. (The default is for all packages to be disabled by the `newimage` command.)
`-v`	Verbose FTP.

Note
You must reboot your appliance after you use the `newimage` command to upgrade the IPSO image. Save your current configuration before installing the new image.

Follow this procedure to add an IPSO image.

1. Log on to your appliance using a console connection.

Note
If you originally downloaded IPSO 3.7, use the MD5 application to check that the file originated at Nokia and did not change during the download process. (See "Verifying MD5 Values" on page 36.)

2. Perform one of the following, depending on whether you copied `ipso.tgz` to your appliance or will install it from an FTP server:
   - If the IPSO image is copied to your appliance, 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-3.7-FCS1-releng 849
02.12.2001-102644

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.

3. When prompted, choose the image to load after the next reboot.
4. Reboot your appliance when prompted.

Overwriting Existing Images (Fresh Installation)

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

Before you begin, make sure that you know:

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

The following sections describe a fresh installation of the IPSO image using the `install` command. The procedure differs depending on your appliance.

To perform a fresh installation on an IP440, see "Fresh Installation on the IP440" on page 44.

To perform a fresh installation on an appliance other than the IP440, go to the following section.

Fresh Installation on Appliances Other Than IP440

1. Log on to your appliance through a console connection.
2. At the prompt, enter **`reboot`**.
3. If you see the message

   ```
   Verifying DMI Pool Data ........
    1 . . . Bootmgr
    2 . . . IPSO
   ```

   You do not have to press anything. You can also press 1.
4. When the system enters autoboot mode and displays the message

   ```
   Type any character to enter command mode
   ```

   press any key to display the boot manager prompt.
5. At the boot manager prompt, enter **`install`**.

   If a password is configured, the system prompts you to enter the boot manager password.
6. The installation script runs.

   Follow the steps to install the new IPSO image from an FTP server.
7. At the end of the installation procedure, enter **`reboot`**.
8. After your appliance reboots, follow the prompts to configure basic settings.

9. When you see the message

   ```
   You can configure your system in two ways:
     1) configure an interface and use our Web-based
     Voyager via a remote browser
     2) VT100-based Lynx browser
   Please enter a choice [ 1-2, q ]:
   ```

   type 1.

10. When you see the message

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

    choose y (the default option). If you choose n, you cannot use 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 appliance using a system that is on the same network as a configured interface on the appliance.

11. If you have a modem installed, you see a message similar to the following:

    ```
    Modem detected on /dev/cuaa1.
    Enable logins on this modem [y,n]:
    ```

    If you want to enable logging into the appliance through the modem, you can configure the modem now or you can configure it in Voyager or the IPSO CLI after you complete the installation.

    If you want to configure the modem for logins now, type y. You are then prompted to configure a country code for the modem. See "Modem Country Codes" on page 51 for a list of the valid country codes.

12. When you are prompted to log into the appliance, you are ready to continue configuring your appliance. You probably want to do one of the following:

- Log into the appliance and then use the `newpkg` command to install packages. For more information, see "Using the newpkg Command" on page 49.
- Use Voyager to complete the configuration (including installing packages). To log in using Voyager, put the IP address you configured for the appliance in the URL field of your browser.

Fresh Installation on the IP440

When you perform a fresh installation of IPSO on an IP440, the installation procedure differs slightly depending on whether you install IPSO from an FTP server or the CD-ROM.

Caution
This procedure deletes any existing images and configuration information on your appliance. Back up any files that you want to keep and copy them back to the appliance after you have installed the new system.

IPSO on FTP Server

Use the following procedure to perform a fresh installation when `ipso.tgz` is on an FTP server.

1. Insert the boot disk into the appliance disk drive.
2. Boot the appliance.
3. The installation script runs. Follow the prompts to install the new IPSO image from an FTP server.
4. At the end of the installation procedure, enter **`reboot`**.
5. After your appliance reboots, follow the prompts to configure basic settings.

6. When you see the message

   ```
   You can configure your system in two ways:
     1) configure an interface and use our Web-based
     Voyager via a remote browser
     2) VT100-based Lynx browser
   Please enter a choice [ 1-2, q ]:
   ```

   type 1.

7. When you see the message

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

   choose y (the default option). If you choose n, you will not be able to use 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 appliance using a system that is on the same network as a configured interface on the appliance.

8. If you see the message

   ```
   Modem detected on /dev/cuaa1.
   Enable logins on this modem [y,n]:
   ```

   do not be concerned if a modem is not installed in your appliance. Type n and continue.

9. When you are prompted to log into the appliance, you are ready to continue configuring your appliance. You probably want to do one of the following:

   - Log into the appliance and then use the `newpkg` command to install packages. See "Using the newpkg Command" on page 49 for more information.
   - Use Voyager to complete the configuration (including installing packages). To log in using Voyager, put the IP address you configured for the appliance in the URL field of your browser.

IPSO on CD-ROM

Use the following procedure to perform a fresh installation when you install `ipso.tgz` directly from the CD-ROM.

Note
While the installation or setup program is running, you cannot remove the CD-ROM. Ensure you have the proper CD-ROM in the system before starting.

1. Insert the CD-ROM into the appliance CD-ROM drive.
2. Insert the boot disk into the appliance's floppy disk drive.
3. Boot the appliance.
4. The installation script runs. Enter the required information at the prompts.
5. When you are prompted for the installation method, type 1 to install from the CD-ROM.
6. When you are prompted for the path to `ipso.tgz` and the name of the image file, press Enter to accept the default values.
7. When prompted, remove the boot disk and reboot the system.

From this point, the CD-ROM installation proceeds from step 5 on page 44.

Installing and Activating Packages

After you install IPSO, you may want to install Nokia documentation and third party packages (for Check Point VPN-1/FireWall-1 NG, for example). If you added a new version of IPSO using `newimage` 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 appliance are turned off, but they are not deleted. To turn these packages on again, see "Activating Packages" on page 49.

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

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

For information about using the CLI to install and activate packages, see the *CLI Reference Guide for IPSO 3.7*, which is on the Nokia Security Platform Software CD that came with your appliance. You can also get the *CLI Reference Guide* by clicking *Doc* on the Voyager home page or 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 49. For information about how to install packages, see the following section.

Using Voyager to Install Packages

To install Nokia documentation and third party packages using Voyager, perform the following procedure:

1. Log on to your appliance using Nokia Network Voyager.
2. On the Voyager home page, click the *System Configuration* link.
3. Click *Manage Installed Package*s.
4. Click *FTP and Install Package*s.
5. Enter the name or IP address of the FTP server.

6. Enter the path to the directory on the FTP server where the packages are stored.
7. If necessary, enter the appropriate user name and password.
8. Click *Apply.*

   The names of the available packages appear in the Site Listing window.
9. Select the packages you want to install.
10. Click *Apply.*

    The selected package is downloaded to the appliance. When the download is complete, the package appears in the Unpack New Packages field.
11. Select the package in the Unpack New Packages field.
12. Click *Apply.*
13. Click the link to install/upgrade the package.
14. (Optional) To display all installed packages, click Yes next to Display all packages; then click *Apply.*
15. (Optional) To perform a first-time installation, click Yes next to Install; then click *Apply.*
16. (Optional) To upgrade a package, Click Yes next to Upgrade.
17. (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*.
18. Click *Apply.*
19. Click *Save* to make your changes permanent.

Activating Packages

To turn on optional packages that were deactivated when you added a new version of IPSO using `newimage`, perform the following procedure.

1. Log on to the appliance using Nokia Network Voyager.
2. On the Voyager home page, click the *System Configuration* link.
3. Click *Manage Installed Packages*.
4. Click On next to the packages you want to turn on.
5. Click *Apply.*
6. Click *Save.*
7. Reboot your appliance.

Your installation of IPSO 3.7 is complete, and the packages that you selected are activated.

Using the newpkg Command

Use the `newpkg` command to add documentation and third party packages. To use the configuration files from a previously installed version of a package, use Voyager to upgrade the package.

The syntax of `newpkg` is

`newpkg [-d] [-h] [i] [-l` *`user_name`*`] [-m` *`media_type`*`] [-n` *`path`*`]`
`[-o` *`path`*`] [-p` *`password`*`] [-s` *`server_ipaddrs`*`] [-S] [-v]`

Table 2 describes the options you can use with the `newpkg` command.

Table 2 newpkg options

`-d`	Print debug messages.
`-h`	Display help lines for command-line parameters.
`-i`	Install only (do not activate).

`-l` *`user_name`*	User name for FTP.
`-m` *`media_type`*	Media type; for example, FTP, CD, and so on.
`-n` *`path`*	Full path to new package.
`-o` *`path`*	Full path to old package for upgrade.
`-p` *`password`*	Password for FTP.
`-s` *`server_ipaddrs`*	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.

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 49.

Upgrading Check Point VPN-1/FireWall-1 NG with the IPSO Command Shell

If you intend to upgrade VPN-1/Firewall-1 NG FP3 and IPSO simultaneously, you can do so with only one reboot by upgrading VPN-1/Firewall-1 first. This procedure is explained below. If you intend to upgrade to VPN-1/Firewall-1 NG_AI, you should upgrade IPSO first (because versions of IPSO previous to 3.7 do not support NG_AI).

To Upgrade VPN-1/FireWall-1 and IPSO with One Reboot

1. Log on to your appliance console; at the prompt, enter **newpkg**.
2. Choose the installation method that allows you to upgrade from an FTP server.
3. The system prompts you to enter the pathname to the directory on your server that contains package files.
4. The system prompts you step-by-step to install VPN-1/FireWall-1.
5. Upgrade to IPSO 3.7. (See "Adding an IPSO Image from the Command Shell" on page 38.)
6. Reboot the system.

Modem Country Codes

If you configure a Nokia-supported PC card modem while you are installing IPSO, use the tables in this section to choose the appropriate country code.

Table 3 Country Codes for Ositech Five of Clubs Modem

Country Code	Country
22	USA
20	Canada
1	Australia
2	Belgium
3	Denmark
4	Finland
5	France

Country Code	Country
6	Germany
17	Greece
99	Iceland
7	Ireland
8	Italy
9	Luxembourg
10	The Netherlands
11	Norway
12	Portugal
13	Spain
14	Sweden
25	Switzerland
16	United Kingdom

Table 4 Country Codes for Ositech Five of Clubs II Modem

Country Code	Country
B5	USA
20	Canada
09	Australia
0F	Belgium

Country Code	Country
31	Denmark
3C	Finland
3D	France
42	Germany
46	Greece
57	Iceland
59	Italy
69	Luxembourg
7B	The Netherlands
82	Norway
B8	Portugal
A0	Spain
A5	Sweden
A6	Switzerland
B4	United Kingdom

4 Limitations

Nokia wants to hear about information you might have regarding these limitations. See the contact information at the beginning of this document for information about how to contact Customer Service.

For a more comprehensive listing of resolutions to problems, see the online knowledge base after logging in at https://support.nokia.com. Consult the knowledge base occasionally because records are continually added after the completed cases are reported to the Customer Service Center.

The following section describes known limitations associated with IPSO 3.7.

Limited SSL Access After Upgrade

If you use Internet Explorer 5.0 or higher, you cannot use Voyager to connect to the appliance if you configured SSL to use 3DES as the required encryption. To connect to the appliance, use a different Web browser or change the required encryption level.

To change the encryption level to 128-bit key, enter the following CLI command:

```
set voyager ssl-level 128
```

Transparent Mode and VPN-1/FireWall-1

When you use SmartDashboard to configure the Gateway Cluster properties of a VRRP cluster that uses IPSO transparent mode, do not enter any interface information in the Topology window of the cluster object.

Cluster Voyager Issue

If you log into Cluster Voyager, the buttons on the Cluster Voyager page might appear dimmed. In this case, you cannot manage the cluster. To resolve the situation, follow this procedure:

1. Close and reopen your browser.
2. Enter the URL for the cluster node again.
3. On the login screen that appears, click *Log In with Advanced Options*.
4. Enter **`admin`** for the user name and the appropriate password for this user.
5. Click YES next to both of the options below the user name and password fields.
6. Click the *Login* button.

   You are logged into the system as an admin user and Voyager appears.
7. Log out of the system.
8. On the login screen that appears, click *Log In with Advanced Options*.
9. Enter **`cadmin`** for the user name and the appropriate password for this user.
10. Click YES next to both of the options below the user name and password fields.
11. Click the *Login* button.

    Cluster Voyager appears, and you can manage the cluster

CLI BGP Command Not Available

The BGP log-state-transitions command in the IPSO command-line interface (CLI) does not work. Use the Voyager BGP page to configure logging for the BGP peer.

Monitoring Limitations

This section explains issues related to the monitoring features of IPSO 3.7.

New Format for Authentication Failure Message

The format for user authentication failure system message logs has been changed in IPSO 3.7. The following table shows a comparison of the old message format and the new format.

Old Format	Feb 1 01:44:07 nokia-fw [LOG_NOTICE] PAM_httpd[340]: authentication failure; admin(uid=0) -> admin for httpd service
New Format	Feb 1 18:35:42 nokia-fw [LOG_NOTICE] httpd: PAM_httpd: authentication failure; admin(uid=65534) -> admin for httpd service

Luna VPN Accelerator Card Statistics

Statistics for the Luna VPN Accelerator Card are not available on the Cryptographic Accelerator Statistics page in Voyager.

SNMP Limitations and Changes in Behavior

This section explains issues related to IPSO 3.7 support for SNMP.

Support for RFC 1213 Deprecated

The MIB defined in RFC 1213 was deprecated in IPSO 3.6, but continues to be supplied with the system.

For more information on any supported MIB, see the /etc/snmp/mibs directory.

SNMP Fix for VRRP and System Configuration Traps

IPSO 3.7 includes fixes to vrrpTrapNewMaster and vrrpAuthFailure. They now contain the correct trap-code and OIDs. Previously, for trap sinks configured for SNMPv1, VRRP traps contained incorrect enterprise OID and enterprise-specific code. For trap sinks configured SNMPv2, VRRP traps were missing a zero (0) in the snmpTrapOID.

IPSO 3.7 also includes a fix to systemTrapConfigurationChange. The format of the OID was corrected to <OIDprefix>.0.<specific trap code>. Previously, the value zero (0) was missing.

Malicious HTML Tags

To protect your appliance from malicious HTML tags embedded in client Web requests, do not connect to untrusted Web sites with your browser while you have an active Voyager session.

Backup and Restore Warning Messages

After you select a local or remote file to use to restore an archived system configuration, click *Apply*, but do not click *Save*. Follow the *Reboot* link at the bottom of the page and ignore the “Any unsaved changes will be lost” messages you receive before you reboot the system.