Administrator’s Guide for
Nokia IPSO-LX

IPSO-LX 7.1
### Nokia Contact Information

#### Corporate Headquarters

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

#### Regional Contact Information

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

#### Nokia Customer Support

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice:</td>
<td>+44 (0) 125-286-8900</td>
</tr>
<tr>
<td></td>
<td>+44 (0) 125-286-5666</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice:</td>
<td>+65-67232999</td>
</tr>
<tr>
<td></td>
<td>+65-67232897</td>
</tr>
</tbody>
</table>

050602
## Contents

**About This Guide** ................................................................. 9  
Conventions This Guide Uses .................................................. 10  
Notices ....................................................................................... 10  
Text Conventions ......................................................................... 10  
Menu Items .................................................................................. 11  
Related Documentation .............................................................. 11

### 1 Overview ........................................................................... 13  
About Nokia IPSO-LX. ............................................................... 13  
About Nokia Network Voyager .................................................... 13  
Using Nokia Network Voyager .................................................... 14  
  Logging In to Network Voyager ................................................ 14  
  Navigating in Nokia Network Voyager ....................................... 16  
  Making Configuration Changes ................................................... 16  
  Accessing Documentation and Help ........................................... 18  
  Reference Guides ....................................................................... 18  
  Page Help .................................................................................. 18

### 2 Configuring Interfaces ......................................................... 19  
Overview of Ethernet and Loopback Interfaces ............................. 19  
Ethernet Interfaces ........................................................................ 20  
Loopback Interface ....................................................................... 23

### 3 Configuring and Using System Functions ............................... 25  
Configuring the Domain Name Service ........................................ 25  
Configuring the System Time ....................................................... 26  
  Configuring NTP ........................................................................ 27  
Configuring Host Entries ............................................................. 29  
Configuring System Logging ......................................................... 30  
  Sending and Receiving System Log Messages ............................ 30  
  Configuring Logging of Configuration Changes .......................... 32  
  Configuring the Logging of Network Voyager Operations .......... 33  
Changing the Hostname ................................................................. 33  
Backing Up and Restoring Files .................................................. 33  
  Creating Backup Files ............................................................... 34  
  Transferring Backup Files ......................................................... 36
4 Configuring SNMP ................................................. 51
   About SNMP .................................................. 51
   IPSO-LX SNMP Implementation ............................... 51
   SNMP Security Considerations ................................. 52
   Enabling SNMP and Selecting the Version .................... 53
   Configuring an Agent Address ................................ 54
   Configuring SNMP Authentication ................................ 54
   Setting the Read-Only Community String ...................... 54
   Configuring SNMPv3 USM Users ............................... 55
   Entering Location and Contact Information ................... 56
   Configuring Traps ............................................. 56
   Enabling Set Operations ...................................... 58

5 Managing Security and Access ................................. 59
   Changing Passwords ........................................... 60
   Managing Users ............................................... 62
   Managing Groups ............................................. 64
   Role-Based Administration ................................... 67
   Managing Feature Sets ....................................... 67
   Managing Roles ............................................... 68
   Assigning Roles and Access Mechanisms to Users .......... 69
   Configuring Nokia Network Voyager Access ................ 70
   Configuring Basic Nokia Network Voyager Options .......... 70
   Generating and Installing SSL/TLS Certificates ............ 71
   Troubleshooting SSL/TLS Configuration ..................... 73
   Session Management .......................................... 74
   Configuring Session Timeouts ................................ 74
   Secure Shell (SSH) ............................................ 75
   Initial SSH Configuration ..................................... 75
   Configuring Advanced Options for SSH ...................... 77
   Obtaining and Generating Host Keys ......................... 79
   Configuring Secure Shell Authorized Keys .................. 79
Changing SSH Key Pairs ...................................................... 80
Auditing User Actions ................................................. 81

6 Configuring Routing .................................................. 83
Configuring Static Routes ........................................... 83
Configuring the Default Route .................................. 83
Adding or Editing Static Routes ................................. 84

7 Monitoring the System .............................................. 87
Viewing Basic System Information ............................ 87
Viewing Hardware and Software Information ....... 88
Viewing Configuration Information ......................... 88
Viewing System Use Information .............................. 90
CPU and Memory Utilization ................................... 90
Disk and Swap Space Utilization ............................ 91
Monitoring Process Utilization ................................. 91
Interface Usage .......................................................... 92
Viewing System Logs ............................................... 93
System Message Log (syslog) ................................. 93
Web Server Access and Error Logs ....................... 93
Generating Monitor Reports ..................................... 94
Using the Customer Support Tool ............................ 95

A Nokia IPSO-LX Boot Manager .................................. 97
How to Enter the Boot Manager Command Mode .......... 97
Boot Manager Commands ........................................... 98

Index ................................................................. 99
About This Guide

This guide provides information about how to configure and monitor Nokia IPSO-LX systems. This guide provides conceptual information about system features and instructions on how to perform tasks using Nokia Network Voyager, the Web-based interface for Nokia IPSO-LX.

This guide is intended for experienced network administrators who configure and manage Nokia IP security platforms. It assumes a working knowledge of networking and TCP/IP protocol principals and some experience with UNIX- or Linux-based systems.

This guide is organized into the following chapters:

- **Chapter 1, “Overview”** describes the Nokia IPSO-LX operating system, Nokia Network Voyager, how to use Network Voyager, and how to access documentation and help pages.
- **Chapter 2, “Configuring Interfaces”** describes how to configure and monitor physical interfaces.
- **Chapter 3, “Configuring and Using System Functions”** describes how to configure basic system functions such as DNS, system time and NTP, host entries, system logging, and the hostname. It also describes how to backup and restore files, manage and upgrade system images, reboot the system, and manage packages.
- **Chapter 4, “Configuring SNMP”** describes how to configure Simple Network Management Protocol (SNMP), the protocol used to exchange management information between network devices.
- **Chapter 5, “Managing Security and Access”** describes how to change or reset passwords, manage users and groups, assign access permissions to using roles, configure Web connections using SSL, and configure Secure Shell (SSH), which is used to provide secure connections for the CLI.
- **Chapter 6, “Configuring Routing”** describes how to change the default route, add or edit static routes, and configure routing options and traces.
- **Chapter 7, “Monitoring the System”** describes the information about your system that you can obtain by using Network Voyager and the command line interface.
- **Appendix A, “Nokia IPSO-LX Boot Manager”** describes how to use the IPSO-LX boot manager and the boot manager commands.
Conventions This Guide Uses

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

Notices

⚠️ Caution
Cautions indicate potential equipment damage, equipment malfunction, loss of performance, loss of data, or interruption of service.

---

Note
Notes provide information of special interest or recommendations.

---

Text Conventions

Table 1 describes the text conventions this guide uses.

Table 1  Text Conventions

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

Menu items in procedures are separated by the greater than sign.

For example, choose Actions > Package Upgrade indicates that you first choose Actions, then choose Package Upgrade from the menu.

Related Documentation

In addition to this guide, user documentation for this product includes the following:

- **Release Notes for Nokia IPSO-LX**
  This document contains a list of new features for the current Nokia IPSO-LX release, upgrade and initial configuration instructions, and known limitations.

- **CLI Reference Guide for Nokia IPSO-LX**
  This guide contains the commands that you can implement from the command-line interface (CLI) for IPSO-LX.

You can find the latest versions of these documents at the Nokia Support Web site, [https://support.nokia.com](https://support.nokia.com).
1 Overview

The contents of this chapter are as follows:

- About Nokia IPSO-LX
- About Nokia Network Voyager
- Using Nokia Network Voyager
- Accessing Documentation and Help

About Nokia IPSO-LX

Nokia IPSO-LX is a version of the Nokia IPSO operating system based on Linux and is used on select Nokia IP security platforms. Nokia IPSO-LX is an appliance-optimized, security-hardened version of the Linux operating system. It is based on the Gentoo Linux 2005.1 distribution, which in this case uses a Linux 2.4.31 derived kernel.

Nokia IPSO-LX is security hardened and features that are not needed in a network appliance or gateway and that pose security risks, such as compilers and development tools, have been removed. In addition, it has added features designed to make Nokia appliances easy to deploy, configure, and maintain.

Note
To view a list of copyrights that are applicable to IPSO-LX software, choose Configure > Asset Management in the tree view and then click Copyright Information.

About Nokia Network Voyager

Nokia Network Voyager is a Web-based interface that you can use to manage Nokia IPSO-LX systems from any authorized location. Network Voyager is part of the Nokia IPSO-LX operating system software and is accessed from a client using a browser.
Using Nokia Network Voyager

Nokia Network Voyager is supported by the following browsers:

- Internet Explorer 6.x
- Mozilla 1.4 and above
- Netscape 7.x
- Opera 7.x

**Note**
JavaScript must be enabled in the browser for Network Voyager to function correctly.

Logging In to Network Voyager

**To open Network Voyager**

1. Open a Web browser on a workstation with network connectivity to the IPSO-LX system.
2. In the Location or Address text box, enter the IP address of the initial interface you configured for the appliance.
   
   Because SSL is enabled by default, you will receive warning messages about the sample certificate on the system. Accept the connection.
3. Enter your username and password. If this is the first login, enter the Admin username and the password you entered when you performed the initial configuration.
   
   You can select to log in with or without an exclusive lock on configuration changes. For more information, see “Obtaining a Configuration Lock” on page 15.

**Note**
If the login screen does not appear, you might not have a physical network connection between the host and your appliance, or you might have a network routing problem. Confirm the information you entered during the initial configuration and check that all cables are firmly connected.

**Note**
The system logs messages about both successful and unsuccessful attempts by users to log in. These are stored in the /var/log/messages file.

Logging Off

When you are finished with your Network Voyager session, or if you need to log in to a new session, log out by clicking Log Off at the top of the Network Voyager window.
Obtaining a Configuration Lock

To keep users making conflicting changes at the same time, Network Voyager provides an exclusive configuration lock.

When you log in with exclusive configuration lock, no other user will be able to change the system configuration until one of the following occurs:

- You log out
- The idle session timer elapses
- Another user manually overrides your configuration lock. For instructions about how to override a configuration lock, see “To override a configuration lock.”

Users who have one or more read/write access privileges (as defined by the administrator under role-based administration) automatically acquire configuration locks unless they uncheck the Acquire Exclusive Configuration Lock check box when they log in. However, their read/write access is limited as defined by the administrator even though the configuration lock is in effect for all features.

Users who do not have read/write access privileges cannot acquire a configuration lock.

To log in with exclusive configuration lock

1. At the login, enter your user name.
2. Enter your password.
3. Verify that the Acquire Exclusive Configuration Lock check box is checked. By default, you are given an exclusive configuration lock.
4. Click Log In.

Note
Logging in with an exclusive configuration lock in Network Voyager prevents you or other users from using the CLI to configure the system while your browser session is active.

To log in without exclusive configuration lock

1. At the login, enter your user name.
2. Enter your password.
3. Uncheck the Acquire Exclusive Configuration Lock check box.
4. Click Log In.

You are given read-only access and will not be able to make configuration changes. You will see the status message “Configuration lock not acquired” at the bottom of each Network Voyager page and the Submit button will be disabled.
To override a configuration lock

**Note**  
Only users with read/write access privileges are allowed to override an exclusive configuration lock.

1. From the login page, click Log In with Advanced Options.  
2. Verify that the Acquire Exclusive Configuration Lock check box is checked. This is the default choice.  
3. Check the Override Locks Acquired by Other Users check box.  
4. Enter your user name and password.  
5. Click Log In.

**Navigating in Nokia Network Voyager**

To navigate to individual pages in the Network Voyager interface, click the appropriate link in the tree view on the left side of each page. Expand or collapse the tree as needed to find the page you are looking for.

**Note**  
Avoid using the Back and Forward buttons on your browser when you use Network Voyager. Because the browser caches the HTML page information, using Back and Forward might not display the latest configuration and diagnostic information as you move from page to page. Use the links in the Network Voyager tree view on the left side of the window to get the most current data.

The links that are available to you in the tree view depends on the role or roles assigned to you as a user. For more information about role-based administration, see Chapter 5, “Managing Security and Access.”

You can enter a URL in the browser Address or Location text box to access a Network Voyager page. If you do not have permission to access that page, you receive an error message. Any URL you type in persists in the Address or Location text box even if you then use the navigation tree to access other pages.

**Making Configuration Changes**

You make configuration additions and changes by entering text in text fields, checking and unchecking check boxes, selecting items from drop-down lists, and clicking Submit for the additions and changes to be saved. Gray check boxes indicate options that you cannot modify. A red asterisk and yellow color indicate text fields for required information.

The Submit, Reset, and Help buttons appear on most Network Voyager pages and are described in the following table. Other buttons are described in the help for each page.
### Reloading Pages

If the page seems to have outdated information, click the page link in the tree view to reload the page. Avoid using your browser Refresh button when you use Network Voyager, because Network Voyager does not update the browser URL when you use the navigation tree, and the URL you access might be different from the URL you intended.

You can also clear your browser memory and disk caches. Consult your browser help for more information.

Some configuration changes are not reflected in your current session. For example, if you did not acquire an exclusive configuration lock or if someone else overrode your configuration lock, then their configuration changes will not be reflected in your current session. To see all configuration changes to date, log off and log back in to Network Voyager.

### Viewing and Restoring Messages

Voyager displays two kinds of messages in a message box: Error messages, which are framed in red, and information messages, which are framed in blue. You can restore messages that you closed by clicking Message.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit</td>
<td>Applies the settings on the current page to the running configuration and the saved configuration on disk. If no new changes are pending, or if you do not have an exclusive configuration lock, the button is inactive.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the settings on the current page to the settings when the page was loaded. If no new changes are pending, or if you do not have an exclusive configuration lock, the button is inactive.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays an help page that describes all elements of the current Network Voyager page.</td>
</tr>
</tbody>
</table>
1 Overview

Accessing Documentation and Help

You can access this manual, the Administrator’s Guide for Nokia IPSO-LX, and page help from the Network Voyager interface links shown in Figure 1.

Figure 1 Accessing IPSO-LX Documentation and Network Voyager Page Help

Reference Guides

This guide, the Administrator’s Guide for Nokia IPSO-LX for the IPSO-LX version that you are running, is the comprehensive reference source for IPSO-LX administration and using the Network Voyager interface. You can access this guide from the following locations:

- Network Voyager
  Click the links under Documentation on the Network Voyager interface tree view, as shown in Figure 1.
- Nokia support site (https://support.nokia.com).
- On the product CD, if one was included with your appliance.

Page Help

Page help supplies information about the current displayed page. To access help for a Network Voyager page, click the Help button at the top of the page.

To print the page help, click Print at the bottom of the Help page.
This chapter describes how to configure Ethernet and loopback interfaces. It also describes the interface statistics that you can view. This chapter contains the following sections:

- Overview
- Ethernet Interfaces
- Loopback Interface

### Overview of Ethernet and Loopback Interfaces

For each physical port on a network interface card (NIC) installed in the appliance, the system automatically supplies a default name. Each port has exactly one physical interface. Physical interface names have the form:

\[ \text{<type>-s<slot>p<port>} \]

where:

- \text{<type>} is a prefix indicating the device type: for example, \text{eth} for Ethernet.
- \text{<slot>} is the number of the slot the NIC occupies in the appliance.
- \text{<port>} is the port number of the NIC. The first port on a NIC is port one. For example, a two-port Ethernet NIC in slot 2 is represented by two physical interfaces: \text{eth-s2p1} and \text{eth-s2p2}.

Built-in ethernet interfaces do not have slot and port numbers and are numbered consecutively (for example, eth1, eth2, and so on).

An additional loopback interface provides an entry for the localhost in the hosts table.

To make an interface functional, you need to configure the physical interface. Use Network Voyager to set the attributes of an interface, such as line speed and duplex mode, and IP address.

You can also create up to 30 aliases for each Ethernet interface and up to 6 for the loopback interface. An interface alias is an additional IP address assigned to a physical interface.
Ethernet Interfaces

For each Ethernet interface, you can:

- Enable (make active) or disable the interface.
- Set or change the IP address for the interface.
- Change the speed and duplex mode, or choose to enable auto-negotiation for these settings.
- Create IP aliases.

You can also view the status of an Ethernet interface, as described in “To monitor the status of an interface” on page 22.

To configure an Ethernet interface

1. Click Interfaces under Configure in the tree view.
2. Click the name of the interface.
3. Configure any of the options listed in Table 2 on page 20, then click Submit.

Note

If you have the Sourcefire Sensor on Nokia application running on the appliance, it might have control of an interface. When the application has control of the interface, the interface is shown as locked. The only changes you can make on a locked interface is to change the Enable Auto-Negotiation, Link Speed, and Duplex Mode options.

Table 2 Interface Configuration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Interface</td>
<td>Check to enable the interface, uncheck to disable the interface. You can perform the same action with the Active check box on the main Interfaces page.</td>
</tr>
</tbody>
</table>
| Enable Auto-Negotiation | Check this box to use Ethernet auto-negotiation to determine the speed and duplex mode of the interface. Uncheck to set the speed and duplex mode manually.  
                          **Note:** Autonegotiation works only if it is enabled on both sides of the link. If the link partner is set to forced speed/duplex settings, you must set the interface to the same speed/duplex settings. |
| Link Speed           | Select the link speed from the drop-down box. This field is disabled if auto-negotiation is enabled. The speed must be equal to or less than the speed of the port to which it is connected if auto-negotiation is enabled on that port. |
Table 2 Interface Configuration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplex Mode</td>
<td>Select Full Duplex or Half Duplex from the drop-down list. This selection is disabled if auto-negotiation is enabled. The duplex mode must be the same as for the port to which it is connected. If the duplex setting of an Ethernet interface is incorrect, it might not receive data, or it might receive duplicates of the data it sends.</td>
</tr>
<tr>
<td>Interface Comment</td>
<td>(Optional) In the Interface Comment text box, enter any comment or description that you might find useful in identifying the interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>In the IP address text box, enter the IP address for the device.</td>
</tr>
<tr>
<td>Note</td>
<td>Do not change the IP address for the interface you use to access Network Voyager or you will lose access to Network Voyager.</td>
</tr>
<tr>
<td>Mask Length</td>
<td>Enter the mask length for the network to which the new IP address belongs. For example, for a 24-bit network mask, enter 24. Range: 8 to 30</td>
</tr>
<tr>
<td>Delete</td>
<td>Check the delete box to delete the local IP address.</td>
</tr>
<tr>
<td>IP Aliases</td>
<td>Enter aliases for this interface, one alias to a line. For example, 205.226.10.1/24 You can add a maximum of 30 aliases for each interface.</td>
</tr>
</tbody>
</table>

To view configuration summaries of all interfaces
1. Click Interfaces under Configure in the tree view.
2. View the following interface configuration information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Shows the name of the physical interface. Click the physical interface name to go to the configuration page for that interface.</td>
</tr>
</tbody>
</table>
| State      | Indicates the state of the physical port:  
  • (Green) Up—the physical interface is ready for use. It is enabled and connected to the network.  
  • (Red) Down—either the physical interface is disabled or the device is not detecting a connection to the network.  
  • (Blue) Locked—An application running on the appliance has control of the interface. You can change the auto-negotiation, link speed, and duplex mode options, but you cannot change any other settings. |
2 Configuring Interfaces

To monitor the status of an interface

1. Click Interfaces under Configure in the tree view.
2. Click the physical interface link to view information about an interface.

The following information is available under Physical Status.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| State    | Indicates the state of the physical port:  
  • Green—the physical interface is ready for use. It is enabled and connected to the network.  
  • Red—either the physical interface is disabled or the device is not detecting a connection to the network.  
  • (Blue) Locked—An application running on the appliance has control of the interface. You can change the auto-negotiation, link speed, and duplex mode options, but you cannot change any other settings. |
| Type     | Shows the type of interface, in this case Ethernet. |
| Speed    | Shows the line speed of the device, in bits per second (bps). |
| Duplex Mode | Shows the duplex mode for the Ethernet interface. |
| MTU      | Shows the maximum length of frames, in bytes, that can be transmitted over this device. This value limits the MTU of any network protocols that use this device. |
| MAC Address | Shows the physical address of the device. |

The following information is available under Statistics.
The loopback interface provides an entry in the hosts table for the local host and is used by the system to send locally-originated packets back to itself. The loopback address provides a stable address for protocols to use so that if the physical interface becomes inactive the protocols are not affected (the loopback interface is always active) or to avoid monopolizing a physical interface. The loopback interface is also useful for testing services without using remote network access or to ping the loopback interface to test that the IP stack is working properly.

You cannot change the IP address for the loopback interface (127.0.0.1), which is an industry standard.

You can configure up to six aliases for the loopback interface.

**To configure a loopback alias**

1. Click Interfaces under Configure in the tree view.
2. Click the lo link.
3. Enter up to six IP aliases in the text box putting each entry on a new line.
4. Click Submit.

**To view status of the loopback interface**

1. Click Interfaces under Configure in the tree view.
2. Click the lo link.

The following information is available under Physical Status.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Number of bytes that this interface received or transmitted since the last reboot.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets that this interface received or transmitted since the last reboot.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Number of multicast packets that this interface received since the last reboot.</td>
</tr>
<tr>
<td>Errors</td>
<td>Number of transmit or receive errors that this interface encountered since the last reboot.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Indicates the state of the physical interface. The loopback interface is always active (up).</td>
</tr>
</tbody>
</table>
The following information under Statistics.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Number of bytes that this interface received or transmitted since the last reboot.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets that this interface received or transmitted since the last reboot.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Number of multicast packets that this interface received since the last reboot.</td>
</tr>
<tr>
<td>Errors</td>
<td>Number of transmit or receive errors that this interface encountered since the last reboot.</td>
</tr>
</tbody>
</table>
3 Configuring and Using System Functions

This chapter provides information on basic system administration tasks and contains the following sections:

- Configuring the Domain Name Service
- Configuring the System Time
- Configuring Host Entries
- Configuring System Logging
- Changing the Hostname
- Backing Up and Restoring Files
- Upgrading and Managing IPSO-LX Images
- Performing a Fresh Installation of IPSO-LX
- Rebooting or Shutting Down the System
- Managing Packages
- Managing Processes

Configuring the Domain Name Service

Nokia IPSO-LX uses the Domain Name Service (DNS) to translate hostnames into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system; you can also specify secondary and tertiary DNS servers. When resolving hostnames, the system consults the primary name server first, followed by the secondary and tertiary name servers if a failure or time-out occurs.

You can also specify a list of domain names which the system can append to DNS lookups. Use this list to allow users to enter a hostname that is not fully qualified. When a user tries to connect by entering a hostname, the system performs additional DNS lookups by appending each string in your search list successively to the string entered by the user.

For example, if the fully qualified hostname is dart.ecom.companyname.com you might enter two strings in the Search list field:

ecom.companyname.com companyname.com
If the user tries to connect by entering `dart`, the system appends the first search list item and does a DNS search on `dart.ecom.companyname.com`.

**To configure DNS**

1. Choose Configure > System Configuration in the tree view and then click DNS.

2. In the Search list field, enter a list of domain names that might be appended to names users enter when trying to connect. Separate each name with a space.

   A valid domain name is made up of subdomain strings separated by periods. Subdomain strings must begin with a letter and can consist only of alphanumeric characters and hyphens.

   **Note**
   
   Domain name syntax is described in RFC 1035 (modified slightly in RFC 1123).

   The maximum length of the entire search list is 256 characters. The maximum number of items in the search list is 6.

3. In the Primary Name Server field, enter the IP address of the first server to use when resolving hostnames.

   This address should be a host running a DNS server.

4. (Optional) In the Secondary Name Server field, enter the IP address of the server to use when resolving hostnames if the primary server does not respond. This address should be a host running a DNS server.

5. (Optional) In the Tertiary Name Server field, enter the IP address of the server to use when resolving hostnames if the primary and secondary servers do not respond. This address should be a host running a DNS server.

6. Click Submit.

   **Note**
   
   You can also view your existing DNS setup by clicking Configuration Summary under Configure in the tree view.

---

**Configuring the System Time**

Synchronized clock times are critical for a variety of purposes, including distributed applications that require time synchronization, analyzing event logs from different devices, ensuring crontab jobs execute at the correct time, and ensuring that applications that use system time to validate certificates find the correct time. For example, in the case of audit logs, the time stamps on different network devices should be accurate to within about a second of each other to correlate events across multiple devices.

You can view the current system time at the top of any Network Voyager page.
You can set the system time using any of the following methods:
- Set the date and time manually.
- Access a time server once.
- Configure NTP to access time servers for continuing clock synchronization.

**Setting the System Time**

Set the system time either manually or by using a time server when you initially configure the system. You might need to set it again when you bring the system up after it has been down for a period of time. Use this procedure also to specify the local time zone.

**Note**
When you reset the system time, the routing table is reset and existing connections might be terminated.

**To set system time once**
1. Choose Configure > System Configuration in the tree view and click Time.
2. Select the appropriate time zone in the Time Zone list box.
   By default, the time zone is set to GMT.
3. Either set the time manually or specify a time server:
   a. To set the date and time manually, enter the time and date units to change. You do not need to fill in all fields; blank fields default to their existing values. Specify hours in 24-hour format.
   b. To set the time using a time server, enter the name or IP address of the time server in the NTP Time Server text box. Choosing this option sets the time once; it does not update on a regular basis.
4. Click Submit.

**Configuring NTP**

Network Time Protocol (NTP) is an Internet standard protocol used to accurately synchronize the clocks of computers in a network. Running as a continuous background client program on a computer, NTP sends periodic time requests to the NTP servers that you configure, obtaining server time stamps and using them to adjust the client's clock. The client then interacts periodically with the NTP server to maintain the high level of accuracy of the system time.

The time server begins to provide time information 5 minutes after it is configured.

For more information on NTP, go to [http://www.ntp.org](http://www.ntp.org).

Table 3 describes the parameters that you can use to configure NTP on your appliance.
To configure system time using NTP

1. Choose Configure > Router Service in the tree view and click NTP.

2. In the Add New NTP Server text field, enter the IP address for an NTP server and click Add.
   The server appears in the NTP Servers table.

3. Configure parameters for the server as described in Table 3.

### Table 3  NTP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable NTP              | Select this checkbox to enable NTP on your appliance. It is disabled by default.  
Because of the length of time necessary to refine the frequency estimate, you should operate the NTP daemon on a continuous basis and minimize the intervals when for some reason it is not running. |
| Server IP address       | Enter the IP address or domain name of a valid NTP server. Generally, you should configure at least 3 NTP servers. Select these servers from different operating administrations, where possible. |
| NTP version             | NTP version 4 is the default. Change this setting only if you know that the NTP server only supports a lower version or the NTP server does not respond to queries from your NTP client. |
| Give preference         | Optionally, you can select a checkbox for an NTP server which you want to use as the primary time source.                                      |
| Use                     | Select this box when you want the appliance to use this server. This box is automatically selected when you add a server by using Add New NTP Server. |
| Options                 | These burst options tell the system to use a number of packets instead of the usual one packet when polling a time server. You can select the burst to be sent either when the server is reached or during initial connect request.  
If the time on your appliance has gotten out of sync, select one of these options to decrease the period it takes to achieve synchronization. Deselect it after the time is re-synchronized. |
| Min. and max. poll intervals | The system dynamically adjusts the poll frequency within the window that is defined by the minimum and maximum settings.  
The default setting for minimum poll interval is 64 seconds; the default setting for maximum poll interval is 1024 seconds.  
Generally, you do not need to adjust these settings. |
| Delete server           | Check this box and click Submit to delete the entry for an NTP server.                                                                         |
Generally, you only need to select the Use check box and you can accept the default settings for all other parameters.

4. Add additional NTP servers.
   Generally, you should configure at least 3.

5. Click Enable NTP.

6. Click Submit.

Limitations for NTP

Nokia IPSO-LX supports only client mode for NTP and does not support symmetric mode. This means that the appliance can obtain time synchronization from a remote server but will not provide time synchronization to a peer.

Nokia IPSO-LX does not support authentication for NTP.

Best Practices for NTP

If the clock on your appliance differs significantly from the time on the NTP servers, you may experience a delay of up to an hour or more for the system to synchronize the clock. This might occur in the following circumstances:

- The system is brand new.
- You halt the system for period of time for maintenance.
- The interface used for NTP goes down for a period of time.
- You disable NTP for a period of time.

Under these circumstances the local appliance time diverges from UTC by an amount that depends on the intrinsic error of the clock oscillator and the time since it was last synchronized.

If the system time for your appliance varies by more than 1000 seconds or so (approximately 17 minutes) from the NTP server time and you want to reduce the time it takes for the clock to re-syncronize, you can perform one of the following actions.

- Set one of the burst options, either Send Packet Burst When Server Reached or Send Packet Burst During Initial connect. Follow the procedure “To configure system time using NTP” on page 28.
- Set the time once by using a time server and then configure the NTP client to keep it synchronized. To set the time, follow the procedure “To set system time once” on page 27.

Configuring Host Entries

Choose Configure > System Configuration and click Host Address to perform any of the following tasks:

- View the entries in the hosts table.
- Add an entry to the list of hosts.
- Modify the IP address of a host.
Delete a host entry.

Note
The localhost address is configured by default as 127.0.0.1 and cannot be modified or deleted.

You should add host addresses for systems that will communicate frequently with the system you are configuring.

To add a host entry
1. Choose Configure > System Configuration in the tree view and click Host Address.
2. Enter the new hostname in the Host Name text box under Add New Host.
3. Click Add.
   The new hostname appears in the list of Current Host Address Assignments.
4. Enter the IP address of the new host in the text box next to the new name.
5. Click Submit.

To delete a host entry
1. Choose Configure > System Configuration in the tree view and click Host Address.
2. Check the Delete check box next to the host to delete.
3. Click Submit.

Configuring System Logging
IPSO-LX logs system events, using syslog-ng. The default destination for system log messages is /var/log/messages. In addition to logging to this local file, IPSO-LX allows you:

- Send system messages of a specified severity level to remote devices
- Receive system messages from remote devices
- Log configuration changes made through Network Voyager or the IPSO-LX CLI
- Log Network Voyager submit operations

For information on how to view the system messages file and on how IPSO-LX manages the messages file, see “System Message Log (syslog)” on page 93.

Sending and Receiving System Log Messages
You can configure system logging to send logging messages to a remote device (see “To send system log messages to a remote device” on page 31) or to accept unfiltered system log messages from remote devices (see “To accept system messages sent from a remote device” on page 32).
Configuring System Logging

Caution
Do not configure two devices to send system logging messages to each other either directly or indirectly. Doing so creates a forwarding loop, which causes any system log message to be repeated indefinitely on both devices.

Any log messages sent to remote devices are also stored in the local log directories. You can use this feature, for example, to send logs to a device that is configured for more secure storage or to reduce the risk of losing log information if you run out of disk space on your Nokia IPSO-LX appliance. You might also choose to send all of the logs from multiple computers to one centralized log server, possibly one that is configured for high availability.

You can select the following severity levels of messages to send to remote devices:
- All messages
- Only emergency messages
- Any messages that are equal to or more severe than the level specified

You can also enable your system to accept unfiltered system log messages from remote devices. If you enable logging from remote systems, network system log packets are tagged with the hostname of the sending device and logged as if the messages were generated locally. If logging from remote systems is disabled, network system log packets are ignored.

To send system log messages to a remote device
1. Choose Configure > System Configuration in the tree view and click System Logging.
2. Enter the IP address of the host device to which you are sending system log messages in the Add New Remote Logging System address field.
   The IP address appears in the Current Systems Logged To table.
3. Select a severity level from the Messages Logged drop-down list to specify the level of messages to forward to this IP address.
   The choices are:
   - Emergency Only
   - Alert and Above
   - Critical and Above
   - Error and Above
   - Warning and Above
   - Notice and Above
   - Info and Above
   - Debug and Above
4. Click Submit.
To accept system messages sent from a remote device
1. Choose Configure > System Configuration in the tree view and click System Logging.
2. Check the Accept Syslog Messages from Remote Machines check box.
3. Click Submit.

Configuring Logging of Configuration Changes

You can configure how configuration changes made with Network Voyager or the IPSO CLI are logged. The options are:

- **Logging Disabled**—the system logs a minimal message that states that a configuration change was made and includes the name of the host from which the change was made, and the name of the user who made the change. No specific information about the change is included. For example:

  May 8 14:47:04 myhost xpand[1128]: Configuration changed from localhost by user admin

- **Logging of Changes**—the system logs a message that provides specific information about the configuration change. The message include the user name, host name from which the change was made, and specific configuration database bindings that have been changed. For example:

  May 8 15:11:43 myhost xpand[1128]: admin localhost t +process:snmpd t
  May 8 15:11:58 myhost xpand[1128]: admin localhost t +snmp:writecommunity:private t

  The first message indicates that the configuration has been changed to enable SNMP (snmpd); the second message indicates the SNMP read-write community string has been set to “private.”

- **Log file**—you can specify that messages about configuration changes be sent to another log file in addition to the default /var/log/messages file. To do so, enter the filename here. For example: /var/log/configchanges.

To configure auditing level and system log file location
1. Choose Configure > System Configuration in the tree view and click System Logging.
2. Under Auditing of Configuration Changes, select one of the following:

   - Logging of Changes
   - Logging Disabled

3. In the Log File text box, enter the name of the file to which the system logging messages should be sent.
   
   The default is /var/log/messages.

4. Click Submit.
Configuring the Logging of Network Voyager Operations

You can configure the system to log a message in /var/log/messages each time a user clicks Submit on a Network Voyager page. The action is logged whether or not the operation succeeds. The message includes the user name and the name of the Network Voyager page. For example:

```
May  8 15:18:50 myhost ipstcl: Voyager audit: User admin pressed button submit on page snmp.tcl
```

To log Network Voyager Submit operations

1. Choose Configure > System Configuration in the tree view and click System Logging.
2. Check the Auditing of Voyager Operations check box to enable auditing or uncheck it to disable auditing of Network Voyager operations.
3. Click Submit.

Changing the Hostname

You set the hostname during initial configuration. To identify the hostname (system name) of your appliance, choose Configure > System Configuration in the tree view and click Hostname. The hostname is also displayed in each page header.

You can change the hostname at any time.

To change the hostname

1. Choose Configure > System Configuration in the tree view and click Hostname.
2. Enter the new hostname in the Change Hostname To text box.
   The name can be up to 63 alphanumeric characters and must not include spaces.
3. Click Submit.

Backing Up and Restoring Files

You can perform manual backups of files or you can configure your system to run regularly scheduled backups. These tasks are described in “Creating Backup Files” on page 34. You can also use Network Voyager to manage your backup files, including the following tasks:

- Restore from locally stored files.
  See “To restore files” on page 37.
- Transfer backup files to, and restore them from, a remote server.
  See “To transfer backup files to a remote server” on page 36 and “To restore files” on page 37.
- Delete backup files that are stored on the local system.
  See “To delete local manual backup files” on page 35.
Creating Backup Files

You can create a backup file manually at any time (see “To create a backup file manually” on page 34), or configure the system to run scheduled backups automatically (see “To configure scheduled backups” on page 35).

By default, the backup file contains everything in the following directories:

- configuration (the /config directory)
- cron (the /var/spool/cron directory)
- etc (the /var/etc directory)

You can also choose to include the following in your backup file:

- User home directories (the /var/home directory)
- Log files (the /var/log directory)
- Application packages, if they support IPSO-LX backup and restore.

**Note**

An application might not support backup and restore through Network Voyager and the CLI. Only applications that support backup and restore appear in the list.

Backup files are given the name you specify, with the date of the backup automatically appended to the file name. Backup files that manual runs produce are in the /var/backup directory and backup files that automatically scheduled runs produce are in the /var/backup/sched directory. Only seven backup files are maintained in the /var/backup/sched directory at time. IPSO-LX automatically overwrites the oldest file of the seven each time it does a scheduled backup.

You can transfer backup files to a remote server (see “To transfer backup files to a remote server” on page 36) or download them to your workstation (see “To download backup files to your workstation” on page 37).

**To create a backup file manually**

1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. Enter a file name for your backup file in the Backup File Name text box.
   
   If you do not enter a name, the backup file is not created.
3. Select any additional directories to include in the backup file:
   a. To include the home directories of all active users in the backup file, check the Backup Home Directories check box.
   b. To include log files in the backup file, check the Backup Log Files check box.
   c. To include application package files in the backup file, check the check box for each package to include in the backup file.
Backing Up and Restoring Files

Only packages that support backup are listed.

4. Click Submit.

After you successfully perform a manual backup, an entry for that backup file appears under Download Backup File, the Manual Backup File drop-down list under Restore from Local File, and under Delete Backup Files.

**To delete local manual backup files**

1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. In the Delete Backup Files field, check the Delete check box next to the name of each backup file to delete.
3. Click Submit.

The entry for the backup file disappears.

**To configure scheduled backups**

1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. In the Scheduled Backup field, click the Frequency drop-down list and select Daily, Weekly, or Monthly to configure how often to perform a regular backup.
   
   Additional text boxes appear in the Configure Scheduled Backup section.
3. Select times and dates for the scheduled backup from the drop-down lists.
   
   - For a daily backup, select the hour and minute.
   - For a weekly backup, select the day of the week, hour, and minute.
   - For a monthly backup, select the date of the month, hour, and minute.
     
     If you select a date for monthly backups that does not occur every month of the year, such as 31, those months are omitted from the backup schedule.
4. Enter a name for your backup file in the Backup File Name text box.
   
   If you do not enter a name, the backup file is not created.
5. Select any additional directories to include in the backup file:
   
   a. To include the home directories of all active users in the backup file, check the Backup Home Directories check box.
   
   b. To include your log files in the backup file, check the Backup Log Files check box.

   c. To include package files in your backup file, select the check box next to the name of each package to include in the backup file.

     Only packages that support backup are listed.
6. Click Submit.
Note
For daily, weekly, and monthly backups, the system overwrites the oldest backup log file when number of backups exceeds 7.

To cancel a regularly scheduled backup
1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. In the Frequency drop-down list, select None.
3. Click Submit.

Transferring Backup Files
You can transfer backup files to a remote server or download them to the workstation from which you are running Network Voyager. When you transfer backup files to a remote server, they also remain in the /var/backup directory on your system.

To transfer backup files to a remote server
1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. In the Transfer Backup to Remote Server section, complete the following.
   a. From the Protocol drop-down list, select Secure Copy Protocol (SCP).
      Secure Copy Protocol, like SSH, uses secure shell encryption to transfer files. You must select a protocol to be able to transfer a backup file to a remote server.
   b. In the Remote Site field, enter the IP address of the remote server to which to transfer the backup file.
   c. In the Remote Dir field, enter the path to the directory in which to save the backup files.
   d. In the Remote User field, enter the name of the user account for connecting to the remote server.
   e. In the Remote Password field, enter password for connecting to the remote server.
      The password is not stored in the database. Enter the password each time you want to transfer files to a remote server, even if you are using the same remote server.
   f. In either the Manual Backup File or Scheduled Backup File drop-down lists, select the file to transfer.
      Manually backed-up files are in the /var/backup directory and scheduled backup files are in the /var/backup/sched directory. The drop-down lists contain lists of all archive files in these directories, but some of the files might not be backup files.
3. Click Submit.
To download backup files to your workstation

1. Choose Configure > System Configuration in the tree view and click Backup and Restore.
2. In the Download Backup section, click the link for any listed backup file to download to your computer.
   A browser download dialog box appears for the file you are downloading.
3. Follow the dialog box instructions as necessary to complete the download process.

Restoring from Backup Files

To restore files to the system, you must first create backup files as described in “Creating Backup Files.”

You can restore either from files stored on the local appliance or from files stored on a remote machine.

To restore files

1. Verify that the following prerequisites are met:
   - Enough disk space is available on your platform.

Caution
If you try to restore files and you do not have enough disk space, you risk damaging the operating system.

- Your system is running the same version of the operating system and the same packages as those of the backup files from which you restore files.

Caution
Using incompatible versions can result in problems with configuration and data files, which might, or might not, be immediately detectable.

2. Choose Configure > System Configuration in the tree view and click Backup and Restore.
3. If the file you are restoring from is stored on the local appliance, go to the Restore from Local section.
   a. Select the name of the backup file from either the Manual Backup File or the Scheduled Backup File drop-down lists, depending on the type of file to restore.
      Manually backed-up files are in the /var/backup directory and scheduled backup files are in the /var/backup/sched directory. The drop-down lists contain lists of all the files in these directories, but some of the files might not be backup files.
   b. Proceed to step 5.
4. If the file you are restoring from is stored on a remote device, go to the Restore From Remote section of the page:
   a. From the Protocol drop-down list, select Secure Copy Protocol (SCP).
      If you select None from the Protocol drop-down list, an error is generated when you click Submit. Secure Copy Protocol (SCP) must be selected for the file transfer to execute successfully.
   b. In the Remote Site text box, enter the IP address of the remote server that stores the backup files.
   c. In the Remote Directory text box, enter the path to the directory on which the backup files are stored.
   d. In the Remote User text box, enter the user name to use for connecting to the remote server.
   e. In the Remote Password text box, enter the password to use for connecting to the remote server.
   f. In the File name text box, enter the name of the file to restore.
5. Click Submit.
   A message appears asking if you are sure.

⚠️ Caution
Restoring from a backup file overwrites your existing files.

6. In response to the confirmation message, click either Yes or No.
   If you click No, the restore is cancelled. If you click Yes, a status page appears showing the status of the restore operation. The status page refreshes until the restore is complete. If the restore completes successfully, the system automatically reboots.

⚠️ Note
Do not go to another page before the restore is complete. If you do, the system might not reboot automatically. If the system does not reboot automatically, do not perform a manual reboot; the manual reboot is a different process and does not restore the files. You must begin the restore again and allow the automatic reboot to occur.

Upgrading and Managing IPSO-LX Images

An IPSO-LX image is the operating system kernel and binary files that run the system. You can store multiple versions of the IPSO-LX image on your appliance and you can choose which image is used when you reboot.

When the system boots, it reads the kernel file in the directory indicated by the current pointer. To identify the current image, you can either look on the Home page or choose
Configure > System Configuration > Images, click Manage Images and look in the State column. For information about how to change the current image, see “To select a new current image” on page 39.

You can upgrade the IPSO-LX image on your platform with Network Voyager. When you upgrade, the system configuration and installed packages are retained. For information about how to replace the current image with a new image, see “To upgrade the system image” on page 39. You can test a new IPSO-LX image by performing a test boot, which allows you to choose whether to commit the image used for the test boot or to revert to the previous image. If you do not select either option, the system automatically reboots in five minutes using the previous image. For information about how to test a new image, see “To test an image before committing to it” on page 41.

For information about how to delete images, see “To delete an image” on page 41. When there are too many images on your system, the directory gets full and precludes you from logging in. To prevent this problem, delete old images before you install a new image so that you do not have more than three or so images on your system.

**To select a new current image**

1. Choose Configure > System Configuration > Images in the tree view and click Manage Images.
2. Click the button for the image you want to select.

**Note**
The word current in the State column of the table indicates the current image.

3. From the System Boot drop-down list, select Reboot.
4. Click Submit to reboot the system and activate the new image.

   The system takes a few minutes to reboot.

**To upgrade the system image**

1. Install the image on an HTTP server, FTP server, or local file system. You can obtain the image from the Nokia CD or from the Technical Support download site.
2. In Network Voyager, choose Configure > System Configuration > Images in the tree view and click Upgrade Image.
3. Enter the HTTP, FTP, or file URL to the image location:
   - Example of an HTTP URL:
     http://test.acme.com/ipso-lx.tgz
   - Example of an FTP URL that uses an absolute path:
     ftp://test.acme.com/tmp/ipso-lx.tgz

   For FTP URLs, if the path is absolute rather than relative to your home directory, it must contain a double slash (//) after the domain name. If you enter a path that is relative to the
home directory of the user whose name and password you enter in step 4, use the standard URL format.

- Example of an FTP URL that uses a relative path:
  ftp://test.acme.com/admin/images/ipso-lx.tgz

- Example of a file URL:
  file:///tmp/ipso-lx.tgz

**Note**
If you enter a URL, the system must be configured to use a valid DNS server on the DNS Configuration page.

4. If the server on which the IPSO-LX image is stored requires authentication, enter the user name and password in the Username and Password text boxes.

**Note**
To use an anonymous login, you might need to delete the user name and password if these fields are pre-filled.

5. Click Submit.

6. A message appears that tells you that the upgrade process might take a long time if the network is slow. Click the checkbox and click Submit again.

   The system begins to download the specified image file.

7. To view the status of the download and installation process, click New Image Installation Status.

   When you click this link, the first page of this process appears, and a message box is displayed that is periodically refreshed with new information as the download progresses.

8. The following message at the end of the list of messages indicates that the download and installation process is complete:

   Will use /image/<image> as root for next boot

   The image referred to in this message is the current one, not the new one.

9. To make the new image the current running image, you must select it as described in “To select a new current image” on page 39 and reboot. You can also perform a test boot of the image, as described in the following procedure.

**Note**
After you upgrade to a new image and reboot, you need to enable your application package. Packages are disabled after an image upgrade.
To test an image before committing to it

1. Choose Configure > System Configuration > Images in the tree view and click Manage Images.
2. Click Next Boot Image for the image to test.

**Note**
The word *current* in the State column of the table indicates the current image.

3. Select Testboot from the drop-down list.
4. Click Submit.
The system takes a few minutes to reboot.
5. Reconnect and login again.
6. Click Manage Images.
The page displays the options Commit the Testboot Image and Revert to Previous Image.
7. Select the appropriate option and click Submit.
   You may need to click one radio button then click back in the other radio button in order to activate the Submit button.

**Note**
If you do not select either option (Commit the Testboot Image or Revert to Previous Image), the system reboots and reverts to the previous image after five minutes.

To delete an image

1. Choose Configure > System Configuration > Images in the tree view and click Manage Images.
2. Check the check box for the image to delete.
   You cannot delete the current image.
3. Click Submit.

Performing a Fresh Installation of IPSO-LX

You might have an occasion where you need to perform a fresh installation of IPSO-LX. A fresh installation deletes any existing images and configuration information. It also deletes any installed applications, log files, and user files.

Make sure you back up any files you want to keep. For information on backing up and restoring files, see “Backing Up and Restoring Files” on page 33.

Before you begin a fresh installation:
Download the IPSO-LX image and the lxinstaller file to an FTP server to which your platform has network connectivity.

Make sure you know:
- The IP address or URL of the FTP server.
- The path to the lxinstaller file on the FTP server.
- The path to the ipso-lx.tgz file.
- 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 and root accounts.

A fresh installation is a three-step process:
1. Loading and configuring the boot manager install program
2. Downloading and installing the IPSO-LX image
3. Performing the initial configuration of the new installation

To load and configure the boot manager install program
1. Establish a console connection to the platform and then reboot the platform.
2. Type 2 when you see the following prompt:
   
   LILO 22.5.9
   1 ipso
   2 bootmgr
   Press key '2' to enter BOOTMGR command mode

   If you do not type 2 within 5 seconds after the prompt appears, the platform will continue the reboot instead of entering the boot manager.
3. When the boot manager prompt appears, type install.
4. Enter the IP address for the management interface the boot manager will use.
5. Type y in response to the question about entering a default gateway and then provide the IP address for the gateway.
6. Choose the physical interface to be used for the management interface from the list of interfaces displayed.
7. Choose whether you want to download and install the IPSO-LX image by using the web-based boot manager GUI or by continuing in command-line mode.

   The default is to use the web-based GUI; if you want to use the command line, you must type n.

   If you chose to use the boot manager GUI to download and install the IPSO-LX image, continue with procedure “To install the IPSO-LX image using the boot manager GUI” on page 43.
Performing a Fresh Installation of IPSO-LX

If you chose to use the boot manager command-line interface to download and install the IPSO-LX image, continue with procedure “To install the IPSO-LX image using the command line” on page 43.

**To install the IPSO-LX image using the boot manager GUI**

Skip to the next procedure if you chose to install the IPSO-LX image using the boot manager command line.

1. Confirm that the management interface information you have supplied the boot manager is correct.
2. Open a browser and enter the IP address of the management interface in the location or address field.
3. Fill in the fields on the initial boot manager page as follows:
   - **DNS Server IP**—Enter the IP address of a DNS server if you will be entering the FTP server address as a URL. Otherwise, leave blank.
   - **FTP Server**—Enter the IP address or URL of the FTP server on which the IPSO-LX image resides.
   - **User Name**—Enter the user name and password for the server. The boot manager GUI defaults to the anonymous user with a password of user@nokia.com.
   - **Installer File**—Enter the path to the lxinstaller file, including the lxinstaller name. For example:
     
     downloads/IPSO-LX/1xinstaller
   
   The remaining fields are already filled in with the information you provided to the boot manager install program.
4. Click the Connect button.
   
   After a few moments, the installer screen appears.
5. Confirm that the FTP server and directory information is correct and then click the Show Files button.
6. From the pulldown list, select the IPSO-LX image file, usually called ipso-lx.tgz.
7. Click the Install button.
8. When you see the “Installation completed” message, reboot the appliance. You can do so from the boot manager command line prompt by entering the `boot` command.
   
   When the appliance finishes rebooting, you must perform the initial configuration from the console connection as described in “To perform the initial configuration” on page 44.

**To install the IPSO-LX image using the command line**

Skip this procedure if you chose to download and install the IPSO-LX image using the web-based GUI.

1. Enter the FTP server IP address.
2. Enter the user name and password for your account on the FTP server.
The defaults are for the anonymous account.

3. Enter the full pathname for the lxinstaller file on the FTP server. For example:
   /downloads/IPSO-LX/lxinstaller

4. Confirm that the information you have given the boot manager so far is correct.
   The boot manager downloads and runs the lxinstaller.

5. Confirm that you want to continue with the installation process, which will destroy all
   existing files and data.
   If you do not want your existing files destroyed, enter **n** to stop the lxinstaller from
   proceeding with the installation process.

6. Confirm that the configuration for downloading the IPSO-LX image is correct.

7. Enter the path to the IPSO-LX image or accept the default path shown by pressing Enter.

8. Enter the name of the image file or accept the default name, ipso-lx.tgz, by pressing Enter.

9. Select option 3, Retrieve no packages.

10. Confirm the settings you have selected.
    The image download and install begins.

11. When prompted, reboot the appliance by pressing Enter.
    When the appliance finishes rebooting, you must perform the initial configuration from the
    console connection as described in “To perform the initial configuration” on page 44.

**To perform the initial configuration**

1. The initial configuration begins with the following prompt on the console connection:
   
   **Hostname?**
   
   If the Hostname? prompt does not appear on the console, see the *Installation Guide* for your
   appliance for troubleshooting suggestions.

2. Answer the prompts for hostname, user admin password, and user root password.

3. 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 using CLI after reboot
   Please enter a choice [ 1-2, q ]:

4. Select the physical interface that will be used for the management interface:
   
   Select an interface from the following for configuration:
   1) eth1
   2) eth2
   3) eth3
   4) eth4
Rebooting or Shutting Down the System

You must shut down your system properly to ensure data integrity and safe unmounting of the file systems.

To reboot or shut down the system

1. Choose Configure > System Configuration > in the tree view and click Reboot or Shut Down System.
   
   This page shows the IPSO-LX image that loads when the system reboots. To load another image when you reboot, see “To select a new current image” on page 39.

2. From the System Boot drop-down list, select:

   - Reboot
     
     System flushes the file system cache to disk and reboots using current selected image.

   - Halt
     
     System flushes the file system cache to disk and stops. After the system stops, you can turn off power to the system.

3. Click Submit.
Managing Packages

Packages are software bundles that are ready to install on an IPSO-LX system. To be installed on an IPSO-LX system, a package must be a .tgz, .tar, .tar.gz, .tar.z, or relocatable .rpm file that has been designed to work with IPSO-LX packagement management. Each package is installed as a subdirectory of the /opt directory.

You can use Network Voyager to easily install, upgrade, and remove packages. You also use Network Voyager to enable packages (make them active).

Installing and Upgrading Packages

Using Network Voyager, you can load packages installation files on your appliance from either an FTP server or from your local workstation. You can then instruct the system to extract (unpack) the installation file contents and then install the package or upgrade an existing package.

Note
Some applications might not permit more than one version of a package to be installed on the platform or might not permit you to upgrade a package using Network Voyager. See your application documentation for information on package installation and upgrade.

Note
If an error prevents the complete installation of a package file that is a duplicate of a file that is already on the system, the system deletes the previously installed file because, being partially overwritten, it might be in an unpredictable state.

To install or upgrade a package uploaded from your workstation

1. Choose Configuration > System Configuration > Packages in the tree view and click Install Packages.
2. Click the Upload radio button.
3. In the Upload Packages box, click the Browse button and browse to the package.
4. Open the package.
   The package path now appears in the File Path field.
5. Click Submit to upload the package to the appliance.
   After the upload is complete, the package appears in the Unpack Package box. Previously loaded packages that have not been deleted also appear.
6. Select the package to unpack from the list.
   You can select only one package to unpack at a time.
7. Click Submit.
Managing Packages

The package is unpacked into the local file system in preparation for installation. Information is displayed about the package so that you can ensure that it is the correct one.

8. Click the link:

   Click Here To Install/Upgrade /opt/packages/<packagename>

   The Package Installation and Upgrade page appears.

9. Select one of the following:
   - To perform a first-time installation, select Install.
   - To upgrade a package, select Upgrade and then the package from which you want to upgrade.

   **Note**
   If the application does not permit package upgrades using Network Voyager, you will not see the Upgrade option.

10. Click Submit.

   A package might take some time to finish installing. To monitor installation status, click the link provided. Network Voyager will then refresh its message about installation status every three seconds. When the package installation finishes, the status message will end with “End of Package Installation.” You can click on Manage Packages in the tree view to see the package in the list of installed packages.

**To install or upgrade a package downloaded from an FTP server**

1. Choose Configuration > System Configuration > Packages in the tree view and click Install Packages.

2. Click the FTP radio button.

3. In the FTP Site text box, enter the hostname or IP address of the FTP site where the packages are located.

4. In the FTP Path/File text box, enter the directory the package is in on the FTP site. Do not include the name of the file itself.

5. Enter the user account and password to use when connecting to the FTP site in the User Name and Password fields.
   
   If you leave these fields empty, the Anonymous account is used.

6. Click Submit.

   After a short wait, the Site Listing box appears. The Site Listing box shows the names of all files in the specified FTP directory that have a correct extension for an installable file.

7. Select the package you want to install and click Submit.

   The selected package is downloaded to the Nokia appliance. After the download is complete, the package appears in the Unpack Package box. Previously loaded packages that have not been deleted also appear.
8. Select the package to unpack from the list.
   You can select only one package to unpack at a time.

9. Click Submit.
   The package is unpacked into the local file system in preparation for installation.
   Information is displayed about the package so that you can ensure that it is the correct one.

10. Click the link Click Here To Install/Upgrade filename.
   - To perform a first-time installation, select Install.
   - To upgrade a package, select Upgrade and then the package from which you want to upgrade.

   **Note**
   If the application does not permit package upgrades using Network Voyager, you will not see the Upgrade option.

11. Click Submit.
   A package might take some time to finish installing. To monitor installation status, click the link provided. Network Voyager will then refresh its message about installation status every three seconds. When the package installation finishes, the status message will end with “End of Package Installation.” You can click on Manage Packages in the tree view to see the package in the list of installed packages.

### Enabling and Disabling Installed Packages

Use the Manage Packages page to enable or disable packages.

The actions that occur when you enable or disable a package depends on the application. For example, when you enable a package, one or more of the following might occur:

- The application starts.
- Application-specific Network Voyager pages become available from the Network Voyager navigation tree.
- Application features are added to role-based administration.
- Global or application-specific environmental variables are set.

See the application documentation for more information on enabling or disabling a package.

**Note**
A reboot might be necessary after you enable or disable a package. Whether or not a reboot is required is application-dependent: check your application documentation.
To enable or disable installed packages

1. Choose Configure > System Configuration > Packages in the tree view and click Manage Packages.
2. To enable or disable a package, check or uncheck the Enable check box for the package.
3. Click Submit.

Deleting Packages

You can delete an installed package. You can also independently delete the package installation file (the .rpm or .tgz). An installed package must be disabled before it can be deleted.

To delete packages

1. Choose Configure > System Configuration > Packages in the tree view and click Delete Packages.
2. Check the check box next to packages and .rpm or .tgz files to delete.
   The Packages Available for Deletion section lists all files that are disabled. To delete a package listed in the Active Packages section, you must first go to the Manage Packages page and uncheck the Enable check box.
3. Click Submit.
   The package or file is deleted.

Managing Processes

Nokia IPSO-LX manages processes transparently. You do not need to configure process management settings. The information in this section is provided for informational purposes only.

Critical IPSO-LX processes are monitored by the process monitor (PM). The PM is responsible for:
- Starting and stopping the processes under its control.
- Automatically restarting the processes if they abnormally terminate.

PM checks the status of the processes it monitors frequently and typically takes less than a second to notice if a process has terminated abnormally. It then attempts to restart it. If the process fails to start, PM continues to try to restart it at regular intervals, with each interval increasing by a factor of two (for example, 2 seconds, 4 seconds, 8 seconds, 16 seconds, and so on). If PM fails to start the process after 900 seconds, it stops trying. PM’s process monitoring behavior is not user configurable.
4 Configuring SNMP

This chapter describes the IPSO-LX implementation of the Simple Network Management Protocol (SNMP) and how to configure SNMP. This chapter contains the following sections:

- About SNMP
- IPSO-LX SNMP Implementation
- SNMP Security Considerations
- Enabling SNMP and Selecting the Version
- Configuring an Agent Address
- Configuring Traps
- Enabling Set Operations

About SNMP

The Simple Network Management Protocol (SNMP) is the Internet standard protocol used to exchange management information between network devices. A network that is managed by SNMP consists of three major components: managed devices, SNMP agents, and management systems:

- Managed devices, such as your IPSO-LX appliance, collect and store management information.
- SNMP agents, such as IPSO-LX snmpd, reside on a managed devices and translate the management information collected by the devices into Management Information Bases (MIBs), which are used by SNMP. Agents also respond to requests by the management systems and send event notifications, or traps, to management systems.
- Management systems listen to SNMP notifications sent by agents and send requests for MIB information from the agents or to change (set) MIB information.

IPSO-LX SNMP Implementation


IPSO-LX supports SNMPv1, SNMPv2, and SNMPv3. For SNMPv3, IPSO-LX supports the User-based Security Model (USM), using the MD5 hash function for the user authentication key.
and DES encryption algorithm for encrypting SNMP messages. IPSO-LX does not support View-Based Access Control (VACM).

**Note**  
The Nokia implementation of SNMPv3 does not support SNMPv3 traps.

IPSO-LX supports the public MIBs listed in Table 4.

**Table 4  Nokia IPSO-LX Supported MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Resources MIB</td>
<td>RFC 1514</td>
<td>Provides information about the system, such as hardware, software, processes, CPU use, disk use and so on.</td>
</tr>
<tr>
<td>IF MIB</td>
<td>RFC 2233</td>
<td>Describes generic objects for network interface sub-layers.</td>
</tr>
<tr>
<td>IP MIB</td>
<td>RFC 2011</td>
<td>Provides management information for IP and ICMP implementations.</td>
</tr>
<tr>
<td>SNMPv2 MIB</td>
<td>RFC 1907</td>
<td>Defines SNMPv2 entities.</td>
</tr>
</tbody>
</table>

**Note**  
The warmStart trap is not supported.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP MIB</td>
<td>RFC 2012</td>
<td>Provides management information of TCP implementations.</td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>RFC 2013</td>
<td>Provides statistics about UDP implementations.</td>
</tr>
</tbody>
</table>

These standard MIBs are supplied with the system. To view more detailed information about the MIBs, see the `/usr/local/share/snmp/mibs` directory.

**SNMP Security Considerations**

SNMP is disabled by default on IPSO-LX systems for security purposes. When SNMP is disabled, all SNMP requests are rejected.

**Caution**  
If you do not plan to use SNMP to manage the network, do not enable it. Enabling SNMP opens potential attack vectors for surveillance activity by enabling an attacker to learn about the configuration of the device and the network.

If you choose to enable SNMP, be aware of the following security issues:
SNMPv1 and SNMPv2 do not have strong security. They use a single community name to authenticate all read-only requests or all read-write requests to a device, instead of per-user authentication. In addition, these versions do not encrypt SNMP traffic. For this reason, Nokia recommends that if your management systems support SNMPv3, you use only SNMPv3, which has much stronger security.

If you enable SNMPv1 and SNMPv2, make sure that you change the default Read-Only community string, which is set to the industry standard default, public. Choose a community string which is difficult to guess.

By default, the SNMP agent will listen to requests listen to and respond to requests on all interfaces. You can increase security by configuring SNMP to listen only on a secure internal interface.

SNMP set operations are disabled by default. Nokia recommends that unless you have strong reason to do otherwise, you leave set operation disabled.

Enabling SNMP and Selecting the Version

The SNMP daemon is disabled by default as a basic security precaution. If you choose to use SNMP, you can enable the daemon and configure it according to your security requirements.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system or to allow SNMPv3 access only. If your management station supports SNMPv3, select to use only v3 on your Nokia IPSO-LX system, since it provides better security.

Once the SNMP daemon is enabled, the system might restart it at times, such as when users are added or deleted, or when passwords are changed.

To enable SNMP

1. Choose Configure in the tree view and click SNMP.
2. Check the Enable SNMP Daemon check box.
3. Click Submit.
   The SNMP configuration options appear.
4. From the SNMP version drop-down list, select the version of SNMP to run:
   - v1/v2/v3
     Select this option if your management station does not support SNMPv3.
   - v3-Only
     Select this option if your management station supports SNMPv3. SNMPv3 provides a higher level of security than v1 or v2.
5. Click Submit.
Configuring an Agent Address

An agent address is a specific IP address at which the SNMP agent listens and responds to requests. The default behavior is for the SNMP agent to listen to and respond to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as another way to limit SNMP access. For example, you can limit SNMP access to one secure internal network that uses a particular interface by configuring that interface as the only agent address.

To set an SNMP agent address

1. Choose Configure in the tree view and click SNMP.
2. Enter the valid IP address of a configured interface in the Agent New Address field.
   You can use the IP address of any existing and valid interface.
3. Click Submit.
   The IP address and a corresponding Delete check box appear on the Network Voyager page.

**Note**
If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces.

Configuring SNMP Authentication

SNMPv1/v2 and SNMPv3 use different means of authenticating user requests:

- SNMPv1/v2 use community strings to control read-only and read/write access to network device information. The community string is like a password; it is sent along with each SNMP request and allows (or denies) access to the system.
- SNMPv3 uses the User-Based Security Model (USM). Authentication is done on a user basis, using a secret authentication key for the user.

If you have selected SNMPv3 only, the fields in Network Voyager for configuring SNMPv1/v2 community strings do not appear.

Setting the Read-Only Community String

SNMP v1 and v2 use community strings to control read-only and read/write access to network device information. The community string is like a password; it is sent along with each SNMP request and allows (or denies) access to the system.
Configuring SNMP Authentication

---

**Caution**
When you enable SNMP, change the default setting of the read-only community string to keep intruders from getting information about the network setup. Even read-access can divulge information about the system that a remote attacker might use to compromise the system.

The read-write community string is not configured by default. This disables any set operations. Add a read-write community string only if you want to enable set operations.

**To change the read-only community string**

1. Choose Configure in the tree view and click SNMP.
2. Enter a name in the Read-Only Community String text box.
   - Use alphanumeric characters without spaces. The default is `public`. For security purposes, change the read-only community string.
3. Click Submit.

**To add a read-write community string**

---

**Caution**
Do not enter a read-write community string unless you intend to enable set operations. For more information, see “Enabling Set Operations” on page 58.

1. Choose Configure in the tree view and click SNMP.
2. Enter a name in the Read-Write Community String text box.
   - Use alphanumeric characters without spaces. Certain values that are commonly used in the industry as defaults for this value (such as `private`) are not allowed. You do not receive an error when you configure `private` as the Read-Write community string, but set operations are not allowed.
3. Click Submit.

---

**Configuring SNMPv3 USM Users**

When you add a user to system and give the user with a password that is eight characters or longer in length, IPSO-LX automatically creates a USM user and the associated authentication and encryption keys for you.

You add, delete, or edit USM users using the same procedures for managing any user account on the platform, as described in “Managing Users” on page 62. The only requirement is that users who will also be USM users must have passwords that are eight characters or longer. If a user meets this requirement, the user will be listed in the SNMPv3 USM Users table.

By default, USM users are given read-only access. If you want to enable set operations for a particular user, you must change the user permissions.
To change permissions for a USM user
1. Choose Configure in the tree view and click SNMP.
2. In the SNMPv3 USM Users table, select the permission level from the drop-down list associated with the user.
3. Click Submit.

Entering Location and Contact Information
The settings for location and contact information provide information to the management system about where your device is located and who to contact about it.
Set the location and contact strings when you perform the initial configuration for SNMP on your system.

To enter SNMP location and contact information
1. Choose Configure in the tree view and click SNMP.
2. In the SNMP location string field, enter the physical location of the device.
3. In the SNMP contact string field, enter the department or person who has administrative responsibility for the device.
4. Click Submit.

Configuring Traps
Managed devices use trap messages to report events to the network management station (NMS). When certain types of events occur, the platform sends a trap to the management station.

Note
The Nokia IPSO-LX implementation of SNMPv3 does not yet support SNMPv3 traps. You can select either SNMPv1 or v2 for the trap receiver. SNMPv1 traps are used by default.

To configure traps, you must specify the following information:
- Which types of traps to enable
  To enable trap types, follow the steps in “To enable types of traps” on page 57.
- The location of the trap receiver (management station)
  To configure trap receivers, follow the steps in “To configure trap receivers” on page 57.
- An agent address to be included in each trap message sent to the management station to identify which network device generated the trap
  To set the agent address, follow the steps in “To set the agent address that trap messages use” on page 57.
To enable types of traps
1. Choose Configure in the tree view and click SNMP.
2. In the Trap Messages section, check the check box next to the name of the type of trap to enable. You can enable the following types of traps.
   - Authorization traps: Supplies notification to the management station when it receives a packet with an incorrect community string.
   - Coldstart traps: Supplies notification to the management station when the SNMP agent is reinitialized.
3. Click Submit.
The system now sends a trap message when that type of event occurs. For example, if you enable authorization traps, the system sends a trap message to the management station when it receives a packet with an incorrect community string.

To configure trap receivers
1. Choose Configure in the tree view and click SNMP.
2. Enter the IP address (or the hostname if DNS is configured) of a receiver that accepts traps from this device in the Add New Trap Receiver field.
3. Enter the community string for the specified receiver in the Community String for new Trap Receiver field.
   This is the community string used on your management station (receiver) to control access.
4. Select the Trap SNMP Version for the trap receiver in the drop-down menu.
   The options are v1 or v2, and the default is v1. This is the version of SNMP used by your management station.
5. Click Submit.
The trap receiver is added to the Configured Trap Receivers. You can change the configuration of the trap receiver or delete the receiver by editing its entry in the table and clicking Submit.

To set the agent address that trap messages use
1. Choose Configure > System Configuration in the tree view and click SNMP.
2. In the Agent Address to be used in Trap Messages text box, enter the IP address for the device.
   This address is included in the protocol data unit of each trap message sent to the management station that uses it to identify which network device generated the trap.
   This address must belong to a configured interface.
   If you do not configure an agent address for traps, the system identifies the trap agent address as 0.0.0.0 in SNMP traps (in accordance with RFC 2089).
3. Click Submit.
Enabling Set Operations

Enable set operations only if you know that your network is secure. How you enable set operations depends on which version of SNMP you are using:

- **SNMPv1/SNMPv2**—specify a read-write community string. Any user who knows the read-write community string will be able to perform set operations.
- **SNMPv3**—Grant certain USM users read/write permissions. Only those USM users granted read/write permissions will be able to perform set operations.

**To enable set operations for SNMPv1/SNMPv2**

1. Choose Configure in the tree view and click SNMP.
2. Enter a string in the Read-Write Community String text box.
   
   The read-write community string has no default. Use alphanumeric characters without spaces. Certain values that are commonly used in the industry as defaults for this value (such as `private`) are not allowed. You do not receive an error when you configure `private` as the Read-Write community string, but set operations are not allowed.

   **Caution**
   
   Do not enter a read-write community string unless you want to enable set operations. Only do this if you know that your network is secure.

3. Click Submit.

**To enable set operations for SNMPv3**

1. Choose Configure in the tree view and click SNMP.
2. In the SNMPv3 USM Users table, select Read/Write from the drop-down list associated with the user to whom you want to grant permission to perform set operations.
3. Click Submit.
5 Managing Security and Access

This chapter contains the following sections:

- Changing Passwords
- Managing Users
- Managing Groups
- Role-Based Administration
- Configuring Nokia Network Voyager Access
- Session Management
- Secure Shell (SSH)
- Auditing User Actions

Nokia IPSO-LX systems use role-based administration to provide separation of duties and simplify administration of user access. Administrators define roles and then provide users with access to features by including the features in roles and assigning the roles to users.

Use the following objects when you administer user access:

- **Users**—create a user account with a unique name for each user. This account specifies a home directory and default shell for the user. Assign one or more roles to each user, as described in “Assigning Roles and Access Mechanisms to Users” on page 69.
- **Groups**—primarily for Linux-based operations. Not used in assigning access privileges.
- **Features**—each feature corresponds to the main menu items in the Nokia Network Voyager menu tree view and the corresponding CLI commands.
- **Feature sets**—create bundles of features for easier use when you add features to roles.
- **Roles**—create roles that include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to still other features.
- **Access mechanism**—limit access to the IPSO-LX system through either Nokia Network Voyager or the CLI. You can assign each user permission to use both, or only one access mechanism.

**Note**
To view lists of and information about existing users, groups, and roles, click Configuration Summary under Configure in the tree view.
Network Voyager and the CLI will log a user out after a configurable period of inactivity. For information on configuring the Network Voyager session timeout, see “Configuring Basic Nokia Network Voyager Options” on page 70. For information on configuring the CLI timeout period, see “Configuring Advanced Options for SSH” on page 77.

Changing Passwords

You can change your own password, and administrators with privileges to the Users feature can reset the passwords of any user without providing the current password. You can also reset the Admin user password or the root user password if you lose them.

**To change the current user’s password**

1. For the current user only, click Current Password under Configure in the tree view.
2. Enter your old password.
3. Enter your new password and enter it again in the Confirm New Password field.
4. Click Submit.

**To change another user’s password**

1. Log in as a user who has permissions for the User feature.

   **Note**

   Admin users or any user with the User feature assigned to them can change a user’s password without providing an old password.

2. Choose Configure > Security and Access > Users in the tree view and click Manage User.
3. Click the username of the user whose password you want to change.
   The Edit User page appears.
4. Enter the new password in the New Password text box and again in the Confirm New Password text box.
5. Click Submit.

   **Note**

   You cannot change the password of a hidden user. To change the password, you must first unhide the user by unchecking the Hidden box and clicking Submit.

Do not change the passwords for hidden users that are created by applications running on the system.

If you lose the password for the Admin user, you can reset it by using the procedure in “To reset the Admin password without knowing the current password.”
To reset the Admin password without knowing the current password

1. Log in to the system as the root user.
2. Open a CLI shell by entering the following command:
   ```
   su - admin
   ```
   This operation does not require a password.
3. If the default shell for Admin is not clish, enter the clish command.
4. Enter the following command:
   ```
   set user admin passwd
   ```
5. At the prompt **Old password**, press Enter without typing a password.
6. At the **New password** and **Verify new password** prompts, enter the new password and press Enter.
   The password is now reset.

If you know the existing password for the root user, you can set a new password by using the passwd command. However, if you lose this password, you can reset the root password by using the procedure in “To reset the password for root user.” You must have physical access to the device to perform this procedure.

To reset the password for root user

1. From a console connection, reboot the system, watching the message that appear on the console.
2. Enter the boot manager by typing **2** when you see the following message:
   ```
   LILO 22.5.9
   1    ipso
   2    bootmgr
   Press key '2' to enter BOOTMGR command mode
   boot:
   ```
   You must do this within 5 seconds or else the reboot continues.
3. When you see the BOOTMGR[1]> prompt, enter the following command:
   ```
   overpw
   ```
   This is a hidden command and is not in the help menu. The root password is reset to " ", that is, there is no password.
4. Continue the boot process by entering the following command:
   ```
   boot
   ```
5. Log in as root (no password)
6. Enter the following command:
   ```
   passwd root
   ```
7. Set a new password for root.
Managing Users

You can use Network Voyager to add users to your IPSO-LX system, and to edit the user ID, group ID, home directory, and default shell for a user. You can also enter a new password for the user. For information about how to give privileges to users, see “Role-Based Administration” on page 67.

For security reasons, you can also define certain users to be hidden users. Only users with read/write privileges for the Users feature can view hidden users.

The Admin and Monitor users are created by default and cannot be deleted.

- **Admin**—has full read/write capabilities to all features accessible through Network Voyager and the CLI. Does not have superuser (root) privileges for the underlying operating system.
- **Monitor**—has read-only capabilities for all features in Network Voyager and the CLI, and can change its own password. You must establish a password for monitor before the account can be used.

When you add a new user, the user is given read-only privileges (defaultROAccess) to the Network Voyager home page and CLI prompt but they cannot access other Network Voyager pages or execute commands from the CLI prompt.

After you create a new user, go to Role-Based Administration > Assign Role to Users to grant the user additional access privileges. For more information, see “Role-Based Administration” on page 67.

**To display current users**

1. Choose Configure > Security and Access > Users in the tree view and click Manage Users. The Manage Users page appears with information on current users.
2. If you wish to display hidden users as well, check the Show Hidden Users box and click Submit.
   When the page refreshes after you click Submit, the hidden users are displayed and the check box disappears. The next time you or another user displays this page, the hidden users will again be hidden and check box available.

**To add a user account**

2. Enter the login name of the user (between 1 and 8 characters) in the Username text box.
3. In the Full Name text box, enter the full name of the user you are adding.
4. In the User ID text box, enter the numeric user ID that identifies the user.
   Each user ID must be unique and in the range of 1 to 65535.

**Note**
Some user ID numbers are reserved; for example, zero (0) is reserved for the root user, number 100 for the Admin user, and number 101 for the Monitor user.
5. In the Group Name text box, enter a name (between 1 and 8 characters).

6. In the Group ID text box, enter the numeric group ID that identifies the primary group to which the user belongs.

   The range for this value is 101 to 65530. (Numbers 1 to 99 are reserved for system use and number 100 is reserved for the predefined Users group.)

   Membership in other groups is controlled from the Group Management page. For valid group IDs, see the Group Management page. For information about how to assign and use group IDs, see “Managing Groups” on page 64.

7. In the Home Directory text box, enter the user's home directory as the full Linux pathname where the user is placed on login.

   If the directory does not exist, the system creates it.

   User home directories must be in the /var/home directory. For example, if the name of the new user is tester, you can enter a path /var/home/tester for the home directory.

8. In the Default Shell text box, enter the path to the user's command interpreter, which is invoked on login.

   For valid login shells, see the /etc/shells file. The default setting is /etc/cli.sh.

9. Enter a password in the Password text box.

   Passwords can contain alphanumeric and special characters.

   You can leave this text box blank when you create the user initially, however, the user cannot log in with a blank password.

   Nokia recommends the password length be between 8 and 20 characters. The system accepts a password that is as few as six characters long, but does not automatically generate USM keys to allow users to use SNMPv3.

10. Enter the same new password in the Confirm Password text box.

11. Check the Hidden box if you want the user to be a hidden user. Only users with read/write privileges for the User feature can view hidden users.

12. Click Submit.

   A blank Add User page appears so that you can add another user.

**To edit a user account**

1. Select Configure > Security and Access > Users in the tree view and click Manage Users.

   If the user you want to edit is a hidden user, you must first check the Show Hidden Users box and click Submit in order to display the hidden user name.

2. Click the name of the user account you want to edit.
Note
Do not edit hidden user accounts that were created by an application running on the system.

3. Modify the user account as needed and click Submit.

Note
You cannot change the password of a hidden user. To change the password, you must first unhide the user by unchecking the Hidden box and clicking Submit.

To delete users
   If the user you want to delete is a hidden user, you must first check the Show Hidden Users box and click Submit in order to display the hidden user name.
2. Check the Delete check box next to the user’s name.
3. Click Submit.

Note
You cannot delete the admin or monitor user.

You also cannot delete hidden users. If you want to delete a hidden user, you must unhide it first. Click on the hidden user name to display the Edit User page and change the Hidden setting. Do not delete hidden users created by an application running on the system.

Note
When you remove a user, the user can no longer log in. However, the user’s home directory remains on the system. Use the system shell to remove the user’s directory.

Managing Groups

You can define and configure groups with IPSO-LX as you can with similar Linux-based systems. This capability is retained under IPSO-LX for advanced applications and for retaining compatibility with Linux.

Two groups are created by default and cannot be deleted:

- **Users group**—all users are assigned by default to the Users group. If you edit a user’s primary group ID to be something other than the default, you can use the Edit Group page to add the user to the Users group. All of the users in the Users group might not appear in the
list of current members, because the list does not show users who are added to the group by
default, only users who are explicitly added.

- **Wheel group**—controls which users have root access to the system. Users must be members
  of the wheel group to use the `su` command to log in as root.

For security reasons, you can define certain groups to be hidden groups. Only users with read/
write privileges for the Groups feature can view hidden groups.

Use groups for the following purposes:

- Specify Linux file permissions. By default all users are assigned to the Users group.
- Use the Wheel group to control which users have root access to the system.
- Control who can log in through SSH.

For most other functions that are generally associated with groups, use the role-based
administration feature, described in “Role-Based Administration” on page 67.

**To display current groups**

1. Choose Configure > Security and Access > Groups in the tree view and click Manage
   Groups.

   The Manage Groups page appears with information on current groups.

2. If you wish to display hidden groups as well, check the Show Hidden Groups box and click 
   Submit.

   When the page refreshes after you click Submit, the hidden groups are displayed and the 
   check box disappears. The next time you or another user displays this page, the hidden 
   groups will again be hidden and check box available.

**To add a group**


2. Enter a name in the Group name field (eight or fewer characters).

3. In the GID field, enter or edit a numeric ID.

   The number must be unique.

   **Note**
   
   Suggested values are between 100 and 65535.

4. Check the Hidden box if you want the group to be hidden. Only users with read/write
   privileges for the Groups feature can view hidden groups.

5. Add or remove user accounts that are members of the group.

   - To add a member to the group, select the name in the Available Members list box and 
     click Add to move the member to the Current Members list box.

   - To remove a member from the group, select the name in the Current Members list box 
     and click Remove to move the member to the Available Members list box.
Press Shift-click to select a range of members, or Ctrl-click to select multiple members one at a time.

6. Click Submit.

To edit a group

1. Choose Configure > Security and Access > Groups in the tree view, then click Manage Groups.
   If the group you want to edit is a hidden group, you must first check the Show Hidden Groups box and click Submit in order to display the hidden group name.

2. Select the name of the group you want to edit.

   **Note**
   Do not edit hidden group accounts that were created by an application running on the system.

3. Modify the group as needed and click Submit.

   **Note**
   You cannot modify the members of hidden groups. You need to unhide the group before you can modify its members.

To delete a group

   If the group you want to edit is a hidden group, you must first check the Show Hidden Groups box and click Submit in order to display the hidden group name.

2. Check the Delete Group check box next to the group name.

3. Click Submit.

   **Note**
   You cannot delete the users or wheel groups.
   You also cannot delete hidden groups. If you want to delete a hidden group, you must unhide it first. Click on the hidden group name to display the Edit Group page and change the Hidden setting. Do not delete hidden groups created by an application running on the system.
Role-Based Administration

When you add a new user, the user is given read-only privileges to the Nokia Network Voyager home page and CLI prompt but cannot access other Network Voyager pages or execute commands from the CLI prompt. You must assign roles to the user to provide additional access privileges.

With role-based administration, the administrator can assign access to a feature by including it in a role and assigning the role to users. Each defined role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to still other features.

To assign a set of access permissions to a user, create a role that specifies levels of access to features you want to include, then assign this role to the relevant user. You can use feature sets to bundle features for convenience.

You can also specify which access mechanisms (Network Voyager or the CLI) are available to the user when you assign a role to the user.

Managing Feature Sets

You can use feature sets to create bundles of features for easier use when you add features to roles. You can include both individual features and feature sets in a role. Within a role, you specify either read/write or read-only permission to each feature set or individual feature that you include.

To view a list of existing feature sets, choose Configure > Security and Access > Role Based Administration in the tree view and click Manage Feature Sets.

To add or edit a feature set

1. Select one of the following:
   a. To add a feature set, click Add Feature Set under Configure > Security and Access > Role Based Administration in the tree view.
   b. To edit a feature set, choose Configure > Security and Access > Role Based Administration in the tree view, click Manage Feature Sets, then click the name of the feature set to edit.

2. If you are adding a feature set, enter a name in the Feature Set Name field.
   The name can be any combination of letters and numbers, but must start with a letter and contain no spaces or special characters.
   You cannot edit the name of an existing feature set.

3. Add or remove features:
   - To add a feature to the feature set, select the name in the Available System features list box and click Add to move the feature to the Features in Feature Set list box.
   - To remove a feature from the feature set, select the name in the Available System features list box and click Remove to remove the feature from the Features in Feature Set list box.
Press Shift-click to select a range of features, or Ctrl-click to select multiple features one at a time.

**Note**
Each feature set must include at least one feature.

4. Click Submit.

**To delete feature sets**

1. Choose Configure > Security and Access > Role Based Administration in the tree view and click Manage Feature Sets.
2. Check the Delete check box for the feature set.
3. Click Submit.

**Managing Roles**

To view a list of existing roles on the system, choose Configure > Security and Access > Role Based Administration in the tree view and click Manage Roles.

The following roles are predefined on the system:

- **superUser**—gives the user read/write access to every feature on the system.
- **monitorRole**—gives the user read-only access to every feature on the system.
- **shellAccess**—gives the user access to a regular UNIX shell from the CLI and the user can use the shell command to escape to a shell. Assign this role only to trusted users because these users will have access to the complete Linux shell without limitation.
- **changeSelfPasswd**—gives the user the ability to change own password.
- **defaultROAccess**—gives the user access to the Home page of Network Voyager and to basic commands from the CLI, such as show clienv, set clienv, quit, exit, and so on, but no access to any commands that show or set the system configuration. This role is assigned to every user by default and cannot be deleted from any user's access.

**To add or edit a role**

1. Select one of the following:
   - To add a role, choose Configure > Security and Access > Role Based Administration in the tree view and click Add Role.
   - To edit a role, choose Configure > Security and Access > Role Based Administration in the tree view, click Manage Roles, then click the name of the role.
2. If you are adding a role, enter a name in the Role Name field.
The role name can be any combination of letters and numbers, but it must start with a letter. You cannot edit the name of an existing role.
3. Add features or feature sets by moving them to the Read/Write or Read Only columns, depending on the permission level you want to give to this role.

Remove the features by moving them back to the Available column.

Press Shift-click to select a range of features or feature sets, or Ctrl-click to select multiple features or feature sets one at a time.

4. Click Submit.

To delete a role

1. Choose Configure > Security and Access > Role Based Administration in the tree view and click Manage Roles.
2. Check the Delete check box for the role.
3. Click Submit.

Note
You cannot delete the roles of superUser, monitorRole, shellAccess, changeSelfPassword, and defaultROAccess, which are default roles.

Assigning Roles and Access Mechanisms to Users

To give a user permissions for various features, assign the role or roles that contain the feature permissions to the user. You can also specify whether a user can use Network Voyager or the CLI by assigning access mechanisms to the user.

To assign roles and access mechanisms to users

1. Choose Configure > Security and Access > Role Based Administration in the tree view and click Assign Role to Users.
2. Click the name of the user to which you want to assign roles.

An Assign Roles to User page appears. On that page, you can assign or remove roles to or from the user. Press Shift-click to select a range of features or feature sets, or Ctrl-click to select multiple features or feature sets one at a time.

Note
You cannot remove the defaultROAccess role from any user. You also cannot change the roles assigned to the Admin or Monitor users.

3. Click Submit.
Configuring Nokia Network Voyager Access

When you set up your system for the first time, perform the following tasks:

- Configure basic Network Voyager options.
- Change your SSL/TLS certificate from the default certificate.

SSL is enabled by default. HTTP access is automatically redirected to HTTPS.

Configuring Basic Nokia Network Voyager Options

You can configure the following options for Nokia Network Voyager access:

- Allow Network Voyager access (enabled by default).
- Enable session timeout
- Set a Network Voyager IP address to restrict Network Voyager communication to a single interface.
- Specify a Network Voyager SSL/TLS port number.
- Specify the encryption level required.

Note

Changes to some of these settings might make Network Voyager unusable. You can use the CLI `set voyager` commands to regain access.

To configure Web access for Nokia Network Voyager

2. Check the Allow Voyager Web access check box.
   The check box is checked by default.

Caution

If you uncheck the check box, you must use the CLI to access your appliance.

3. Enter the time interval for which a Network Voyager user is allowed to be logged in without activity in the Session Timeout in Minutes text box.
   The default value is 20 minutes. If the user closes the browser without logging out, the exclusive configuration lock remains in effect until the session time-out interval expires.
4. In the Network Voyager IP address, enter the IP address of an interface to restrict Network Voyager communication to this interface.
   If you use the default setting (0.0.0.0), the system allows Network Voyager connections on all interfaces (in other words, the httpd daemon listens on all interfaces).
5. Enter the number of the port to use for SSL/TLS-secure connections in the port number text box.  
   The default is port 8443.  
   Using the default port allows users to connect to Network Voyager without specifying a port number in the URL. If you change the port number, users must specify a port number in the URL: for example, https://hostname:<portnumber>/.

   **Note**  
   Certain applications use the standard HTTPS port, port 443. Do not change the Network Voyager default port to the standard HTTPS port unless you know for certain this will not cause a conflict with an application installed on your appliance.

6. Select the appropriate encryption level for your security needs from the Require Encryption drop-down list; for example, *40-bit key or stronger*.  
   The default is 128-bit key or stronger.

   **Note**  
   When you enter the encryption level, you are entering the minimum level of encryption you require. You can obtain stronger encryption by default if your Web browser supports it.

7. Click Submit.

**Generating and Installing SSL/TLS Certificates**

Nokia IPSO-LX uses the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol to secure connections over the Internet from the Nokia Network Voyager client to the IPSO-LX system. SSL/TLS, the industry standard for secure Web connections, gives you a secure way to connect to Network Voyager. Creating a unique private key for your appliance and keeping it secret is critical to preventing a variety of attacks that could compromise the appliance security.

When you set up your system for the first time, change your SSL/TLS certificate from the default certificate. IPSO-LX includes a default sample certificate and private key in the `/var/etc/voyager_ssl_server.crt` and `/var/etc/voyager_ssl_server.key` files respectively.

The certificate and private key are for testing purposes only and do not provide a secure SSL/TLS connection. You must generate a certificate, and the private key associated with the certificate, to create a secure connection by using SSL/TLS.

   **Note**  
   For security purposes, generate the certificate and private key over a trusted connection.
To generate a certificate and its associated private key

1. Choose Configure > Security and Access > Voyager in the tree view and click Generate Certificate for SSL.

2. Choose the Private Key Size from the drop-down list that is appropriate for your security needs.
   The larger the bit size, the more secure the private key. The default and recommended choice is 1024 bits.

3. (Optional) Enter a passphrase in the Enter Passphrase field.
   The passphrase must be at least four characters long.

4. (Optional) Enter the passphrase in the Re-Enter Passphrase field to confirm the phrase.
   If you use a passphrase, you must enter the phrase later when you install your new key.

5. From the Generate drop-down list, select one of the following:
   - Certificate Signing Request (CSR)
     Select this option if you are requesting a certificate from a certification authority.
   - Self-Signed X.509 Certificate
     Select this option to create a certificate that you can use immediately, but that will not be validated by a certification authority.

6. In the Distinguished Information section, enter identifying information for your system:
   a. In the Country Name field, enter the two-letter code of the country in which you are located.
   b. In the State or Province Name field, enter the name of your state or province.
   c. (Optional) In the Locality (Town) Name field, enter the name of your locality or town.
   d. In the Organization Name field, enter the name of your company or organization. If you are requesting a certificate from a certification authority, the certificate authority may require the official, legal name of your organization.
   e. (Optional) In the Organizational Unit Name field, enter the name of your department or unit within your company or organization.
   f. In the Common Name (FQDN) field, enter the common name that identifies exactly where the certificate will go. The common name is most commonly the fully qualified domain name (FQDN) for your platform: for example, www.ship.wwwidgets.com. If you are generating a certificate signing request for a CA, that CA might impose a different standard.
   g. (Optional) In the Email Address field, enter the email address to use to contact the person responsible for this system or for its certificate.

7. Click Submit.
8. If you generated a certificate signing request, a screen appears that contains a certificate request—New X.509 certificate signing request—and its associated private key—New private key.
   a. Send the New X.509 certificate signing request to your certification authority. Be sure to include the lines -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----.
   b. Store the new private key that your certification authority securely sends. Install the private key and the certificate. (See Installing a Certificate later in this section.)

9. If you generated a self-signed certificate, a screen appears that contains a certificate (New X.509 Certificate) and its associated private key.
   If you generate a self-signed certificate, the page that is returned gives you the option of having the certificate and key automatically installed. If you use this option, you do not need to cut and paste as described in step 3 in “To install the certificate and its associated private key” on page 73.

To install the certificate and its associated private key
1. Choose Configure > Security and Access > Voyager in the tree view and click Install Certificate for SSL.
2. Open the files that contain your certificate and private key.
3. Perform a cut-and-paste operation on your certificate to move it to the New server certificate field in the Install Certificate for SSL page.
   Be sure to include the lines -----BEGIN CERTIFICATE ----- and -----END CERTIFICATE ----.-
4. Perform a cut-and-paste operation on your private key to move it to the Associated private key field in the Install Certificate for SSL page.
   Be sure to include the lines -----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----.
5. If you entered a passphrase when you generated the certificate and private key, you must enter the passphrase in the Passphrase field.
6. Click Submit.

Troubleshooting SSL/TLS Configuration
You might have trouble accessing Nokia Network Voyager if SSL/TLS is not configured correctly. If you have trouble accessing Network Voyager, try the following remedies.

■ Check that you are using the correct URL. When you enable SSL/TLS, you must use https rather than http when you connect through your Web browser, unless the Redirect HTTP Requests to HTTPS option is enabled.

■ Check that you are using the correct PEM-encoded certificate and private key, and that they are installed properly with the dashed begin and end lines. (See “To install the certificate and
You can view the certificate and private key in the /var/etc/voyager_ssl_server.crt and /var/etc/voyager_ssl_server.key files respectively.

- Check the HTTP daemon error message log. You can find the messages in the following logs: /var/log/httpd_error_log, which you can view using Network Voyager (Monitor > System Logs), and /var/log/ssl_engine_log. The messages can help you troubleshoot further and might contain important information for Customer Support should you contact them.

### Session Management

Nokia IPSO-LX session management prevents multiple administrators from making simultaneous configuration changes, whether they are using Network Voyager or the CLI. When you log in to Network Voyager, you can 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 period of inactivity that you can specify, or the user can manually log out at any time.

When you start a CLI session, you automatically acquire an exclusive configuration lock, if a configuration lock is not already in effect. The lock you acquire remains in effect until you exit the CLI or until the session idle timeout is reached. If a configuration lock is in effect when you start a CLI session, you can execute show commands, but you will be unable to use execute commands such as the add and set commands.

**Note**

Network Voyager uses cookies to keep track of HTTP sessions. Network Voyager cookie-based session management does not store user names or passwords in any form in the cookies. Continue to access Network Voyager from a secure workstation.

### Configuring Session Timeouts

You can adjust the time interval that Network Voyager allows a user to be logged in without activity. When the session timeout expires, the user is logged out. If the user closes the browser without logging out, the configuration lock remains in effect until the session timeout interval expires.

**To set the session timeout interval**

2. In the Session Timeout text box, enter the time in minutes. The default is 20 minutes.
3. Click Submit.
Secure Shell (SSH)

Nokia IPSO-LX uses the Secure Shell (SSH) program to provide secure connections for the IPSO-LX CLI and Linux shell. SSH allows you to securely log in to another computer over a network, execute commands on a remote platform, and move files from one platform to another platform. SSH provides a connection similar to Telnet or rlogin, except that the traffic is encrypted and both ends are authenticated.

Properly used, SSH provides you with session protection from the following security threats:

- DNS spoofing
- Interception of passwords
- IP spoofing
- IP source routing
- Person-in-the-middle attacks

You must use SSH, instead of utilities such as Telnet or rlogin that are not secure, to connect to the system. You can also tunnel HTTP over SSH to use Network Voyager to securely manage your platform.

To use SSH, you must obtain an SSH client for the other end of the connection. SSH clients are available for a number of platforms. Some are free while others are commercial. An SSH client is already installed on your platform; however, you probably want a client to connect from another host, such as your desktop computer, and you must install a client there as well.

**Note**
The SSH server on this system supports only SSH protocol version 2.

Initial SSH Configuration

When you first activate your system, SSH is already enabled and host keys for your platform are generated and installed. SSH automatically authenticates users who log in with the standard password mode of login.

No other configuration needs to be done, unless you want users to be able to use public-key authentication as well. To permit public-key authentication, you must first authorize the users’ client identity keys for this system, as described in “Configuring Secure Shell Authorized Keys” on page 79.

**Note**
All references to SSHv2 in this section refer to SSH protocol version 2 (not SSH software version 2).
To configure SSH

1. Choose Configure > Security and Access > SSH (Secure Shell) in the tree view and click SSH Configuration.

2. The Enable SSH Service check box is checked by default.
   If you disable SSH service, you cannot make remote terminal connections to the platform.

3. Select whether the root user can log in with SSH.
   - **Yes**—the root user can log in and can use the password mode of authentication to do so. This is the default setting.
   - **No**—the root user cannot log in.
   - **Without Password**—the root user can log in, but must use public-key authentication to do so.

4. In the Configure Server Authentication of Users section, check the check box for each type of authentication to use.
   The default is to allow both.
   - **Allow Access using Public Key Authentication**—allows pure DSA or RSAv2 authentication.
     You must authorize the users' public keys by using the SSH Authorized Keys page before users can connect.
   - **Allow Access using Password Authentication**—allows user authentication through the standard login passwords.
     If you disable the use of password authentication, you can only use public key authentication of users.

5. Host keys are generated automatically.
   For more information on this section, see “Obtaining and Generating Host Keys” on page 79.

6. Click Submit.

**Note**

The first time you enable SSH it generates both RSA v2 and DSA host keys. This process takes a few minutes.
Configuring Advanced Options for SSH

Table 5 lists additional options that you can configure for SSH on your system. To configure any of these options, choose Configure > Security and Access > SSH (Secure Shell) in the tree view and click SSH Server Advanced Options.

Table 5  SSH Configuration Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control—who can use SSH to log in</td>
<td></td>
</tr>
<tr>
<td>Names of groups and users</td>
<td>If you specify names in the allowed or forbidden fields, only those users and groups will be allowed or forbidden. Group settings apply only to a user’s primary group (the GID setting in the Voyager Password page). To view or modify a user’s group, see “To add a user account” on page 62. To view or modify the membership of a group, see “To add a group” on page 65. You can use wild card characters when you specify multiple group or user names separated by spaces.</td>
</tr>
<tr>
<td>Permit root user to log in</td>
<td>• Yes—the root user can log in and can use the password mode of authentication to do so. • No—the root user cannot log in. • Without Password—the root user can log in, but must use public-key authentication to do so.</td>
</tr>
</tbody>
</table>

**Note**
A user becomes root user by using the su command (after logging in). To use the su command, the user must be a member of the Wheel group.

Server authentication of users—kinds of authentication that the SSH server allows

| Allow Access using Public Key Authentication | Allows pure DSA or RSAv2 authentication. You must use the SSH Authorized Keys page to authorize users' public keys before they can connect. |
| Allow Access using Password Authentication  | Allows user authentication through the standard login passwords. If you disable the use of password authentication, only public-key authentication of users can be used. |

User Login Environment

| Print message of the day on login       | Specifies that sshd displays the text from /etc/motd when a user logs in interactively. This is the default setting. |
| Use login(1) program for interactive logins | Specifies to use the login utility for interactive logins. This is not normally necessary. |
### Table 5 SSH Configuration Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Protocol Details</strong></td>
<td></td>
</tr>
<tr>
<td>Ciphers to Use</td>
<td>Select which ciphers the protocol uses. By default, all ciphers are selected. To deselect a cipher, click on it. You must leave at least one cipher selected; if you deselect all ciphers, this field returns to its default value of all ciphers selected.</td>
</tr>
<tr>
<td>Send Keepalives to the Other Side</td>
<td>Indicate whether the system should send keepalive messages to the other side. If it does and network connectivity is lost, the server detects this action and drops the connection.</td>
</tr>
<tr>
<td>Listen on Address</td>
<td>Enter the IP address of the interface on which the SSH server listens for incoming connections. If you do not specify an address, the server listens on all IP interfaces.</td>
</tr>
<tr>
<td>Listen on Second Address</td>
<td>Enter an additional IP address on which the SSH server listens for incoming connections.</td>
</tr>
<tr>
<td>TCP Port Number for SSH Service</td>
<td>Enter the TCP port number on which the SSH server listens. The standard port number is 22.</td>
</tr>
<tr>
<td><strong>Service Details</strong></td>
<td></td>
</tr>
<tr>
<td>Allow Remote Connections to Forwarded Ports</td>
<td>Allows remote hosts to connect to ports forwarded for the client. Nokia recommends that you use the default behavior of not allowing such connections for security reasons.</td>
</tr>
<tr>
<td>Login Grace Time</td>
<td>Enter the number of seconds to wait for a user to log in. Enter 0 to impose no time limit. The default is 60.</td>
</tr>
<tr>
<td>Max Unauthenticated Connections</td>
<td>Enter the maximum number of unauthenticated connections allowed at one time. Additional connections are dropped until one of the existing connections is either authenticated or rejected. The default is 10.</td>
</tr>
<tr>
<td><strong>Server Implementation Details</strong></td>
<td></td>
</tr>
<tr>
<td>Message Logging Level</td>
<td>Select the verbosity level that the SSH server uses when it logs messages. Nokia recommends that you not use logging with DEBUG, which violates the privacy of users.</td>
</tr>
<tr>
<td>Strict Checking of File Modes</td>
<td>Set the SSH server to check file modes and ownership of certain user files and directories before a user is allowed to log in. (This check is not made when password authentication is used.)</td>
</tr>
</tbody>
</table>
Obtaining and Generating Host Keys

The host keys are used to identify this system to SSH clients. The SSH server automatically generates host RSA and DSA keys (1024 bits in size) whenever it is enabled, if host keys do not already exist. You can generate new host keys at initial enablement or any subsequent time.

Note
If you generate new keys, you might need to configure each SSH client for the new public key; otherwise, the clients might display warnings when the users attempt to connect. Consult your client documentation.

Configuring Secure Shell Authorized Keys

The Secure Shell (SSH) Authorized Keys feature lets you allow clients to access accounts on your system without using a password—public-key authentication is used instead.

To configure an authorized key, you need information about the clients’ keys. For SSHv2 implementations, you need to enter the RSA/DSA key. File names on your SSH client that are used for storing this information are id_dsa.pub and id_rsa.pub. For more information, consult your SSH client software documentation.

To configure SSH authorized keys

1. Choose Configure > Security and Access > SSH (Secure Shell) in the tree view and click SSH Authorized Keys.

   Note
   If you previously configured authorized keys for user accounts, the information appears in the View/Delete Per-User Authorized Keys table.

2. Do one of the following:
   - To add a DSA authorized key: under Add a New Authorized Key (DSA, for protocol version 2), select the user name from the Username drop-down list, enter the DSA key in either OpenSSH format or SSHv2 format, depending on your client, and a comment (optional).
   - To add an RSA authorized key: under Add a New Authorized Key (RSA, for protocol version 2), select the user name from the Username drop-down list, enter the RSA key, in either OpenSSH format or SSHv2 format, depending on your client, and a comment (optional).

3. Click Submit.
Changing SSH Key Pairs

The following procedure describes how to generate new key pairs. When you generate new keys, you may need to change configurations of each client, or the client might give you errors. For more information, see your SSH client documentation.

To generate new SSH key pairs

1. Choose Configure > Security and Access > SSH (Secure Shell) in the tree view and click SSH Key Pairs.
2. Optional) To generate an RSA host key, select the key size, listed in bits, from the Generate Key of Size drop-down list.
   The recommended value is 1024 bits.
3. (Optional) To generate a DSA host key, select the key size, listed in bits, from the Generate Key of Size drop-down list.
   The recommended value is 1024 bits.
4. Click Submit.

Note
Re-creating keys might cause problems with some clients, because the server is using a key different from the one it used before. You can reconfigure the client to accept the new key.

On the SSH Key Pairs page, you can also view whether RSA or DSA identity keys are assigned to users defined for your system. This information is provided under Per-User Identity Keys. To generate an initial or new RSA or DSA key for the user, click Link next to the user entry and perform the following procedure on the displayed SSH Identity Keys page.

To create an RSA identity

1. Under Generate New RSA v2 Identity, select the key length in the Generate Key of Size drop-down list.
2. (Optional) To protect the private key with a passphrase, enter a passphrase in the Enter password field, then enter it again to verify it.
3. Click Submit.

To create a DSA identity

1. Under Generate New DSA v2 Identity, select the key length in the Generate Key of Size drop-down list.
2. (Optional) To protect the private key with a passphrase, enter a passphrase in the Enter password field, then enter it again to verify it.
3. Click Submit.
Auditing User Actions

You can use Network Voyager to view auditing information in certain log files. Auditing information is contained in the following files.

- /var/log/messages

  This is the default destination for system log messages about events that occur on the system. You can view the syslog messages, for example, to determine whether only authorized users are making configuration changes to the system. For information on configuring your system to send messages to this file about configuration changes made by users, see “Configuring Logging of Configuration Changes” on page 32.

  Select Monitor > System Logs > System Messages Log to view this log. See “System Message Log (syslog)” on page 93 for how to search for specific message types, time periods, or key words.

- /var/log/httpd_access_log

  Provides information about Network Voyager pages that have been accessed.

  Select Monitor > System Logs > HTTPD Access Log to view this log.

- /var/log/httpd_error_log

  You can view information about errors that occur when users are using Network Voyager. You might want to reference this file if you are trying to determine the reason for authentication failures.

  Select Monitor > System Logs > HTTPD Error Log to view this log.
Configuring Static Routes

Use static routes to specify the next hop for packets addressed to destinations outside the directly attached network segments. If your platform directs traffic to destinations outside the directly attached network segments, then you will need to configure a default route and one or more static routes.

You can add additional static routes easily, either one at a time or by entering a list of many.

Configuring the Default Route

The default route specifies where the system should send packets with destinations that are outside the directly attached network segments but do not match any entries in the static route table. You usually set the default route during the initial configuration script. You can change the default route subsequently by using Nokia Network Voyager.

**Caution**

Misconfiguring the default static route can cause loss of connectivity to the platform beyond the directly attached network segment.

To change the default route

1. Choose Configure > Routing > Static Routes in the tree view and click Manage Static Routes.
2. Click Default Route.
3. (Optional) Enter a description in the Description field.
4. From the Next Hop Type drop-down list, select Normal.
You can also choose Reject as the next-hop type. This type or route discards packets to a given destination and sends an ICMP unreachable message back to the sender of the packet.

5. Delete the next-hop gateway address, and enter the IP address of the new gateway in the Gateway Address field.

The gateway address specifies the IP address of the default gateway (router) to which packets are to be forwarded if the packet does not match any specified in the static routes. This address must be that of a router that is directly connected to the same network segment as the system you are configuring.

6. Click Submit.

Adding or Editing Static Routes

You can add one static route to a destination network at a time or add routes to multiple destinations at the same time. You can also edit an existing static route.

To add or edit a static route

1. Select one of the following:
   a. To add a static route, choose Configure > Routing > Static Routes in the tree view and click Add Static Routes.
   b. To edit a static route, choose Configure > Routing > Static Routes in the tree view, click Manage Static Routes and click the name of the static route.

2. If you are adding a static route, enter the network address in the Destination Network Address field and the mask length (number of bits) of the network address in the Mask Length text box.

   You cannot edit the destination address of an existing route.

3. (Optional) Enter a description in the Description text box.

4. Select the type of next hop for the static route to take from the Next Hop Type drop-down list.
   - **Normal**—forwards packets for a given destination to the next hop.
   - **Reject**—discards packets that match the destination and sends an ICMP unreachable message back to the sender of the packet.

5. Enter the IP address of the new gateway in the Gateway Address field and click Add.

   This address must be that of a router that is directly connected to the same network segment as the platform.

---

**Note**

Although you can add multiple next-hop addresses, these currently have no effect and they are not used for this route if the first gateway is unavailable.

6. Click Submit.
To add multiple static routes

1. Choose Configure > Routing > Static Routes in the tree view and click Quick Add Static Routes.

2. In the Next-Hop Type drop-down list, select normal or reject.
   - **Normal**—forwards packets for a given destination to the next hop.
   - **Reject**—discards packets that match the destination and sends an ICMP unreachable message back to the sender of the packet.

3. In the Enter Route Definitions text box, enter a list of static route definitions, with each route on a separate line, using the following format:
   
   **destination_IP_address/mask_length next_hop_IP_address**
   
   - IP addresses must be specified in a dotted-quad format ([0-255],[0-255],[0-255],[0-255])
   - Mask length range is 1 to 32.

   For example, to add a static route to 205.226.10.0 with a mask length of 24 and next hops of 10.1.1.1 and 10.1.1.2, enter:
   
   ```
   205.226.10.0/24 10.1.1.1 10.1.1.2
   ```

4. Click Submit.

   The newly configured additional static routes appear on the Manage Static Routes page. The text box displays any entries that contain errors.
This chapter provides information on monitoring your system. You can use Network Voyager to monitor many aspects of your Nokia appliance to better maintain performance and security. You can, for example, monitor state information for each interface, view real-time CPU and memory usage, view system logs, and generate reports on resource use, such as interface throughput, over specific periods of time.

This chapter covers:

- Viewing Basic System Information
- Viewing Hardware and Software Information
- Viewing Configuration Information
- Viewing System Use Information
- Viewing System Logs
- Generating Monitor Reports
- Using the Customer Support Tool

### Viewing Basic System Information

You can view basic information about your system from the Home page.

To access the Home page, click Home under Configure in the tree view. This page shows the following information:

**Table 6 Home Page Information**

<table>
<thead>
<tr>
<th>Section heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Model number of the platform as obtained from the /proc/sys/nvram/serial system file.</td>
</tr>
<tr>
<td>Software Release</td>
<td>Release number of the current operating system image that uniquely identifies the specific binary build. This number consists of a Linux kernel version numbering scheme followed by IPSO-LX-N.N-BUILDnnn, where N.N indicate the release version and nnn indicates the number of the build.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version number (date stamp) of the current operating system image.</td>
</tr>
</tbody>
</table>
The Asset Management Summary page provides a summary of hardware and software system resources.

- The hardware summary includes information about the CPU, BIOS, motherboard, including the serial number, model number, or date, as appropriate. The summary also displays the amount of memory on the appliance.
- The operating system summary lists which software release and version of that release is running on the system.

The Asset Management Summary page is available under Configure > Asset Information > Asset Summary.

### Viewing Configuration Information

You can use the Configuration Summary page to view configuration information on the features for which you have read or read/write permissions.

To view summary information, click Configuration Summary under Configure in the tree view. Table 7 shows the configuration information that appears on the Configuration Summary page.

<table>
<thead>
<tr>
<th>Section heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Serial number of the platform as obtained from the /proc/sys/nvram/product system file.</td>
</tr>
<tr>
<td>Current time</td>
<td>Current system time configured on the platform. For information about how to change the time, see &quot;Configuring the System Time&quot; on page 26</td>
</tr>
<tr>
<td>Uptime</td>
<td>Amount of time since the last boot or reboot operation.</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>Total physical RAM installed on the platform.</td>
</tr>
<tr>
<td>User</td>
<td>User name of the user currently logged in.</td>
</tr>
<tr>
<td>Active Packages</td>
<td>The application packages currently installed and enabled.</td>
</tr>
</tbody>
</table>

**Note**
The only features that appear on the Configuration Summary page are features that are configured for access in your user account.
### Table 7 Configuration Summary Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>IPSO-LX version number and the uptime (amount of time since the last boot).</td>
</tr>
<tr>
<td>Interfaces</td>
<td>All interfaces, whether they are active or not. Includes the type, IP address, and destination address. For information about interfaces, see “Configuring Interfaces” on page 19.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name and domain name servers (primary, secondary, and tertiary) that are configured for your system to enable DNS lookups. For more information, see “Configuring the Domain Name Service” on page 25.</td>
</tr>
<tr>
<td>Host Address</td>
<td>Entries in the Hosts table. For more information, see “Configuring HostEntries” on page 29.</td>
</tr>
<tr>
<td>System Logging</td>
<td>Logging configuration settings for your system. For more information, see “Configuring System Logging” on page 30.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of your system. For more information, see “Changing the Hostname” on page 33.</td>
</tr>
<tr>
<td>Backup and Restore</td>
<td>Base names used for backup files; whether a scheduled backup is configured, and, if so, when; and the names of backup files that are stored locally. For more information, see “Backing Up and Restoring Files” on page 33.</td>
</tr>
<tr>
<td>Manage Images</td>
<td>File names of each image installed on the system and identifies the current image. For more information, see “Upgrading and Managing IPSO-LX Images” on page 38.</td>
</tr>
<tr>
<td>Packages</td>
<td>Packages installed on your system. For more information, see “Managing Packages” on page 46.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Whether the SNMP daemon is on, and, if it is on, the SNMP version number and information about community strings and SNMP users configured for your system. For more information, see “Configuring SNMP” on page 51.</td>
</tr>
<tr>
<td>Users</td>
<td>All users configured on your system and the user ID, group ID, home directory, default shell, default page, and full name for each user. For more information, see “Managing Users” on page 62.</td>
</tr>
<tr>
<td>Groups</td>
<td>All groups configured for your system and the group ID and names of members for each group. For more information, see “Managing Groups” on page 64.</td>
</tr>
<tr>
<td>Role-Based Administration</td>
<td>All roles configured for your system and the access permissions associated with each. For more information, see “Role-Based Administration” on page 67.</td>
</tr>
</tbody>
</table>
Table 7 Configuration Summary Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voyager</td>
<td>Network Voyager options, such as SSL port and session timeout, configured for your system. For more information, see “Session Management” on page 74.</td>
</tr>
<tr>
<td>SSH (Secure Shell)</td>
<td>SSH configuration settings for your system. For more information, see “Secure Shell (SSH)” on page 75.</td>
</tr>
<tr>
<td>Static Routes</td>
<td>Static routes configured on your system. For more information, see “Configuring Static Routes” on page 83.</td>
</tr>
<tr>
<td>NTP</td>
<td>Whether NTP is enabled and the settings for each NTP server specified on your system. For more information, see “Configuring the System Time” on page 26.</td>
</tr>
<tr>
<td>Asset Summary</td>
<td>Information on hardware and software resources. For more information, see “Viewing Hardware and Software Information” on page 88.</td>
</tr>
</tbody>
</table>

Viewing System Use Information

Use the system utilization pages, which provide real-time information on resource use, to monitor and tune the allocation of system resources. For example, if the percentage shown under file system capacity becomes a high percentage, you should take action, such as deleting old IPSO images and packages or moving your log files to a remote system.

To view information on system resource use, look under Monitor > System Utilization in the Network Voyager tree view and select one of the following:

- CPU and Memory Utilization
- Disk and Swap Space Utilization
- Process Utilization
- Interface Usage

These pages show real-time use and update every twenty or thirty seconds. If you want to see historical usage, use the report pages under Monitor > Reports as described in “Generating Monitor Reports” on page 94.

CPU and Memory Utilization

The CPU and Memory Utilization page shows real-time CPU and memory usage. This page retrieves the updated CPU and memory usage every 20 seconds.

The CPU Utilization table summarizes CPU load averages, which are the number of processes in the system run queue averaged over the last 1, 5, and 15 minutes, respectively. Load averages that are high, such as over 2 in all three fields, indicate that the system is under continuous heavy load.
The Memory Utilization table summarizes memory usage in KBs. Free memory (memory that is available to the operating system) is defined as free pages + cache pages. The remainder is active memory (memory the operating system is currently using). The free memory might differ (will mostly be higher) as compared to output of a vmstat command.

**Disk and Swap Space Utilization**

The Disk and Swap Space Utilization page shows system resources use, including disk and swap space use. This page retrieves the updated disk and swap space use every 20 seconds.

For each file system, you can monitor the number of kilobytes used and available, the percentage of disk space being used, and the location where the filesystem is mounted.

For swap space, you can monitor the name of the device, total number of swap data blocks on the device, the number of used and free swap data blocks on the device, and the type of device.

**Note**

You should monitor the /config, /var, and /opt partitions, since these store the configuration files and logs and optional user software. Unlike read-only partitions, these can grow dynamically.

**Monitoring Process Utilization**

The Process Utilization page shows the status of processes. You must monitor and control processes to manage CPU and memory resources.

This page retrieves the updated process status every 30 seconds. When you access this page, a table displays the following fields for each process:

- **USER**—User who initiated or executed the process.
- **PID**—Identifier used by the kernel to uniquely identify the process.
- **%CPU**—Percentage of CPU used by the process while active. This is a decaying average taken over a time period of up to the previous minute. Because the time base over which CPU utilization of the process is computed varies (processes might be very young), the sum of all CPU fields can exceed 100%.
- **%MEM**—Percentage of real memory used by the process while active.
- **VSZ**—Virtual size of the process in KBs (also called vsize).
- **RSS**—Real memory (resident set) size of the process in KBs.
- **WCHAN**—Wait channel (as a symbolic name). This is the event on which a process waits.
- **STAT**—Symbolic process state given as a sequence of letters. For example, R indicates a runnable process (R) that is a session leader (s). For more information, see the process status man page (man ps).
- **STARTED**—Time the command started.
- **TIME**—Accumulated CPU time: user plus system (alias cputime).
Critical IPSO-LX processes are monitored by the process monitor (PM). The PM is responsible for:

- Starting and stopping the processes under its control
- Automatically restarting the processes if they terminate abnormally

The Nokia IPSO-LX processes that the PM monitors are listed in the following table. In addition, the PM might also monitor application package processes.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clishd</td>
<td>CLI server process that provides a dedicated child-process to serve each CLI session.</td>
</tr>
<tr>
<td>xntpd</td>
<td>Network time protocol daemon. This daemon sets and maintains a UNIX system time-of-day in compliance with Internet standard time servers.</td>
</tr>
<tr>
<td>monitord</td>
<td>System monitor daemon. This daemon monitors system health, collects and stores statistical information, and displays the data on request.</td>
</tr>
<tr>
<td>httpd</td>
<td>Web server daemon.</td>
</tr>
<tr>
<td>sshd</td>
<td>Secure shell daemon.</td>
</tr>
<tr>
<td>xpand</td>
<td>Configuration daemon (also called configd). This daemon processes and validates all user configuration requests, updates the system configuration database, and calls other utilities to carry out the request.</td>
</tr>
<tr>
<td>snmpd</td>
<td>SNMP agent. Responds to queries via SNMP.</td>
</tr>
<tr>
<td>syslogd</td>
<td>Puts system log messages in the system log file.</td>
</tr>
</tbody>
</table>

The PM frequently checks the status of the processes it monitors and typically takes less than a second to notice if a process has terminated abnormally. It then attempts to restart the process. If the process fails to start, the PM continues to try to restart it at regular intervals, with each interval increasing by a factor of two (for example, 2 seconds, 4 seconds, 8 seconds, 16 seconds, and so on). If the PM fails to start the process after 900 seconds, it stops trying. Each unsuccessful attempt is logged in the system message log. The process monitoring behavior of the PM is not user configurable.

### Interface Usage

The interface traffic statistics table provides information for each physical interface and is refreshed every 20 seconds. The information provided includes:

- Current state of the interface
- Input and output byte counters
- Input and output errors
- Type of interface
**Viewing System Logs**

System logs include the following:

- System message log (syslog)
- Web server access log
- Web server error log

You can view these logs in Network Voyager under Monitor > System Logs.

**System Message Log (syslog)**

The system message log is available in `/var/log/messages`. To keep the system logs from growing uncontrollably, IPSO-LX automatically empties the message file each month, after compressing and archiving its contents. IPSO-LX keeps seven months of archive files, named messages.0.gz through messages.6.gz. Each month it rotates the names of the archive files, so that message.0.gz becomes messages.1.gz and so forth, as it creates a new messages.0.gz from the contents of the messages file.

You can view both the current system message log and the archived message logs under Monitor > System Logs > System Message Log in Network Voyager. Using the search capabilities provided by Network Voyager, you can:

- View the entire contents of the current log or any archived log
- Display only log messages of certain types, such as warning messages
- Display messages for a particular month or particular date
- Search and display messages that contain a specific key word or phrase

You can combine search criteria: for example, you can search for only messages of type LOG_WARNING that occurred on a specific date and that contained a specific key word or phrase.

To configure system logging (for example, logging to a remote syslog server), see “Configuring System Logging” on page 30.

**Web Server Access and Error Loggs**

The Web server access log shows accesses to the Network Voyager interface using HTTP or HTTPS. Messages include IP Address from which the local host did an http access to the system, user, date, time, and HTTP access command.

The Web server error log shows error messages from the HTTPD error log file, including date and time the error occurred, transaction (type of log message), location, and contents of log message.

You can view either log under Monitor > System Logs in Network Voyager.
Generating Monitor Reports

IPSO-LX collects resource use information and maintains it for certain lengths of time. You can generate reports of this data.

To generate a report, click the link for the appropriate report under Monitor > Reports in the tree view. Table 8 lists the kind of resource usage reports available.

Table 8 Reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Throughput</td>
<td>Shows historical throughput for each interface. You can often use this information to optimize network performance or troubleshoot issues network traffic congestion. You can choose to include packet throughput, byte throughput, or errors in your report.</td>
</tr>
</tbody>
</table>
| CPU Utilization   | Shows historical CPU use data, including percentages of CPU time for each of the following:  
  • **User%** —Percentage of CPU time spent in User-level instructions.  
  • **Nice%** —Percentage of CPU time spent in "Nice" processes.  
  • **System%** —Percentage of CPU time spent in System level instructions.  
  • **Interrupt%** —Percentage of CPU time spent in servicing interrupts.  
  • **Idle%** —Percentage time CPU was idle. |
| Memory Utilization | Shows historical memory use, including:  
  • **Active Real Memory** —Kilobytes of real memory being used in a given time interval.  
  • **Free Real Memory** —Kilobytes of real memory free in a given time interval. |

To display reports

1. Click the name of the report under Monitor > Reports in the tree view.
2. Under Select Report Type, select one of the following kinds of reports:
   - **Hourly**—data for 1 hour intervals, with up to 7 days of data.
   - **Daily**—data for 1 day intervals, with up to 35 days of data.
   - **Weekly**—data for 7 day intervals, with up to 52 weeks of data.
   - **Monthly**—data for 1 month intervals, with up to a 60 months of data.
   - **Detailed Search**—select a specific time period. These reports have a set data interval of one minute and up to 167 hours of data.
3. For the Interface Throughput, select All Physical or a specific interface name from the Select Interface drop-down list and select any combination of packets, bytes, or errors.

4. Under Select Format, choose Text View or Delimited Text.
   - If you select Delimited Text, select Semi-Colon (;), Comma (,), or Tab from the Delimiter drop-down list.
   - The Text View option displays the data in table format for on-screen reading. The Delimited Text option displays the report in a new page from which you can download the information and import into another application.

5. Click Submit.

Using the Customer Support Tool

If you contact Customer Support for assistance with an issue, you can use the Customer Support Tool (CST) to provide information about your appliance or gateway. Use this tool to generate a tar file that contains all of the data from your appliance or gateway.

For information on contacting Customer Support, see “Nokia Contact Information” on page 3.

The archive file generated by the CST tool contains the following files, which are extracted by Customer Support and used in analyzing your problem.

<table>
<thead>
<tr>
<th>Table 9 Files Contained in CST tar file</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>index.html</td>
</tr>
<tr>
<td>IPSO Configuration Summary</td>
</tr>
<tr>
<td>Ipsoinfo Summary</td>
</tr>
<tr>
<td>Additional IPSO Debug Data</td>
</tr>
<tr>
<td>Log Files Summary</td>
</tr>
<tr>
<td>Raw Log Files</td>
</tr>
<tr>
<td>CPU Statistics</td>
</tr>
<tr>
<td>Memory Statistics</td>
</tr>
</tbody>
</table>
To send system information to Customer Support

1. From the system shell command line, login as root. Or from the CLI, use the shell command followed by the su -l command to become the root user in the system shell.

2. Enter the command /etc/cst.

   The file begins to generate. This process takes a minute. The final line of the output lists the name of the tar.gz file produced by the CST. The file is placed in the directory from which the cst command was run.

3. Upload the output file to your case record on the Nokia Support Site (http://support.nokia.com/).

   If necessary, for example, if the file is very large ( > ~150MB) Nokia Support can provide an FTP server address for file upload. If the file is very small (< 10MB), you can send it as an email attachment.

4. For security purposes, you may want to move your archive file to a secure location.

   **Note**

   If you open the Configuration Summary or Additional IPSO Debug Data sections of the CST data file, you might see the following message:

   *Could not acquire the config lock...*

   *This message can be disregarded.*
This appendix describes how to enter the command mode of the IPSO-LX boot manager and the commands available from the boot manager. The primary use of the boot manager is to perform a fresh installation of IPSO-LX.

### Note
If you are accustomed to the IPSO boot manager, you will notice that the IPSO-LX boot manager is designed to be simpler and contains fewer commands.

## How to Enter the Boot Manager Command Mode

To enter the boot manager command mode:

1. Establish a console connection to the platform.
2. Enter the reboot command.
3. Monitor the messages on the console during the reboot until you see the following:
   ```
   LILO 22.5.9
   lipso
   2bootmgr
   Press key '2' to enter BOOTMGR command mode
   boot:
   ```
4. Type **2** to interrupt the reboot process and enter boot manager command mode.
   You must type **2** within five seconds after the `boot:` prompt appears. If you do not, the system will continue the reboot process.

When the boot manager command prompt, `BOOTMGR[1]>`, appears, you have entered the boot manager command mode.
## Boot Manager Commands

Table 10 describes the boot manager commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot</td>
<td>Boots the IPSO-LX operating system.</td>
</tr>
<tr>
<td>halt</td>
<td>Halts the system. Nokia recommends that you use the halt command to shut down your system to ensure that all of your mounted file systems are unmounted.</td>
</tr>
<tr>
<td>help</td>
<td>Displays a list of the available commands.</td>
</tr>
<tr>
<td>install</td>
<td>Performs a fresh installation of IPSO-LX. See &quot;Performing a Fresh Installation of IPSO-LX&quot; on page 41 for step-by-step instructions</td>
</tr>
<tr>
<td>ls [directory]</td>
<td>Displays the contents of directories on the disk drives in your IP security appliance. The default directory is /image.</td>
</tr>
<tr>
<td>ping</td>
<td>Tests whether a particular host is reachable across an IP network</td>
</tr>
<tr>
<td>sysinfo</td>
<td>Displays information about the CPU, memory, disk devices, and interfaces.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Determines the route taken by packets across an IP network.</td>
</tr>
<tr>
<td>version</td>
<td>Displays the kernel version.</td>
</tr>
</tbody>
</table>
Index

A
access
  providing SSH login 77
access mechanisms
  assigning to users 69
access permissions
  associated with roles 89
adding Nokia IPSO-LX images 97
Admin user
  described 62
  initial configuration 14
agent address
  SNMP 54
  used in trap messages 57
aliases
  creating ethernet interface 21
application packages
  enabling and disabling 49
  installation directory 46
  installing or upgrading 46, 47
  supported file types 46
Asset Management Summary 88
auditing user actions 81
authentication
  password 76, 77
  public key 76, 77
auto-negotiation
  enabling 20

B
backup files
  creating 34
  transferring 36
backups
  viewing configuration of 89
BIOS 88

certificate, SSL
  default certificate and private key 71
  generating 72
  installing 73
changeSelfPasswd role 68
ciphers, server protocol 78
community strings 54, 55
configuration locks
  overview 74
configuration summary, viewing 88
configuring
  default route 83
  interfaces 19
  multiple static routes 85
  network devices 19
  routing 83
  SSH 75
  static route 84
connections
  number of unauthenticated allowed 78
to forwarded ports 78
CPU
  historical use of 94
  information on model 88
  real-time use of 90
CPU utilization report 94
cron jobs, scheduled times 26
Customer Support Tool (CST) 95

D
date/time setting 26
default route
  configuring 83
defaultROAccess role 68, 69
disk utilization 91
DNS
  configuring 26
  protection from spoofing 75
documentation 11
  accessing 18
  conventions 10
domain name
  viewing 89
change current image 39
change hostname 33
change passwords 60
configure a loopback alias 23
configure an Ethernet interface 20
configure DNS 26
enable SNMP sets 58
enable SNMP traps 57
enable SSH 76
generate an SSL certificate 72
log configuration changes 32
navigate in Network Voyager 16
open Network Voyager 14
provide SSH access 77
schedule backups 35
set community strings 55
set system time 27
test an image 41
transfer backup files 36
upgrade image 39
HTTP daemon (HTTPD)
  access log 93
  error log 74, 93
HTTP requests
  redirecting to HTTPS 73
httpd 92
httpd daemon
  restricting 70
httpd_access_log file 81
httpd_error_log 81
images, IPSO-LX 38
installing
  packages 46, 47
interface throughput report 94
interfaces
  enabling ethernet 20
  list of 89
loopback 23
overview 19
real-time statistics on 92
viewing historical throughput 94
interfaces, ethernet
  adding an identifying string 21
  creating aliases 21
  setting duplex mode 21
  setting speed 20
viewing information about all 21
viewing information about an 22

change current image 39
change hostname 33
change passwords 60
configure a loopback alias 23
configure an Ethernet interface 20
configure DNS 26
enable SNMP sets 58
enable SNMP traps 57
enable SSH 76
generate an SSL certificate 72
log configuration changes 32
navigate in Network Voyager 16
open Network Voyager 14
provide SSH access 77
schedule backups 35
set community strings 55
set system time 27
test an image 41
transfer backup files 36
upgrade image 39
HTTP daemon (HTTPD)
  access log 93
  error log 74, 93
HTTP requests
  redirecting to HTTPS 73
httpd 92
httpd daemon
  restricting 70
httpd_access_log file 81
httpd_error_log 81
images, IPSO-LX 38
installing
  packages 46, 47
interface throughput report 94
interfaces
  enabling ethernet 20
  list of 89
loopback 23
overview 19
real-time statistics on 92
viewing historical throughput 94
interfaces, ethernet
  adding an identifying string 21
  creating aliases 21
  setting duplex mode 21
  setting speed 20
viewing information about all 21
viewing information about an 22
IP spoofing 75
IPSO-LX
  adding images 97
  deleting images 41
  described 13
  managing images 38
  selecting images 39
  software copyrights 13
  testing images 41
  upgrading image 39

K
keepalive messages 78
key pairs, SSH 79

L
link speed
  setting interface 20
localhost
  address 30
  entry in hosts table 23
log 81
logging
  configuration changes 32
  how to configure system logging 30
  Network Voyager submits 33
  receiving from remote machine 30
  to remote syslog server 30
  viewing configuration settings for 89
  see also system message log (syslog)
login
  grace time 78
loopback interface 23

M
memory
  viewing historical use 94
  viewing real-time use of 90
  viewing total physical on Asset Management
    Page 88
  viewing total physical on home page 88
memory utilization report 94
menu items, Voyager 11
messages, Voyager error
  viewing 17
MIBs 52
model number 87
Monitor user 62
monitord process 92
monitoring
  an interface 22
  historical use of system resources 94
  interfaces 21
  physical interface traffic 22
  real-time use of system resources 90
  monitorRole role 68
  MTU 22

N
network devices, configuring 19
network interface card (NIC) 19
Network Voyager
  described
  navigating in 16
  opening 14
  restricting access to 70
  troubleshooting access problems 70
  Web access options 70
NMS 56
NTP
  description 27

O
opening Voyager 14

P
packages
  deleting 49
  disabling 49
  enabling 49
  installing 46, 47
  list of installed 89
  overview 46
  unpacking 46, 47
  viewing list of active packages 88
passwords
  changing 60
  interception 75
  length requirements 63
  resetting 60
physical interfaces 19
ports
  forwarded 78
  on NIC 19
private keys
  sample SSL 71
process
  process monitor (PM) 92
status of 91

R
read-write community strings 58
rebooting 45
refreshing pages 17
release number 87, 88
reloading pages 17
remote terminal connections 76
reports
displaying historical use statistics 94
Reset button 17
restoring
from backup files 37
restoring files
overview 33
rlogin utility 75
role-based administration
overview 67
roles
adding 68
assigning to users 69
deleting 69
editing 68
overview 68
predefined system 68
viewing list of 68, 89
root user
controlling root access 65
in Wheel group 65
login using SSH 76
routing
configuring 83
creating a default route 83
creating a static route 84
creating multiple static routes 85
RSA
authentication for SSH 77
generation of host keys 76
RSS (Resident Set Size) 91

S
Secure Copy Protocol (SCP) 36, 38
Secure Shell. See SSH
Secure Socket Layer See SSL
Self-Signed X.509 Certificate 72
serial number, platform 88
server protocol 78
session management
overview 74
specifying timeout 70
viewing settings 90
set operations
enabling 58
setting time/date 26
shellAccess role 68
shutting down 45
SNMP
agent address 54
community strings 54
daemon status 89
enabling 53
enabling traps 57
entering contact information 56
sending traps 57
version number 89
snmpd process 92
software release number 87, 88
SSH
advanced options 77
checking of file modes 78
checking of file ownership 78
configuring 75
configuring client with new keys 79
disabling 76
enabling 76
features 75
host keys 79
IP listen address 78
key pairs 79
logging level 78
obtaining SSH client 75
overview 9, 75
TCP port number for 78
viewing configuration settings 90
sshd process 92
SSL
generating certificate 72
installing certificate 73
sample keys for connection testing 71
specifying encryption level 71
specifying port number 70, 71
troubleshooting configuration 73
static host
adding 29
static routes
adding 84
configuring 84
configuring multiple 85
ing 84
edit 84
mask length 84
overview 83
viewing list of 90
Submit button 17
superUser role 68
swap space utilization 91
syslogd 92
syslogd process 92
system 81
system message log (syslog) 93
  compression and rotation of archive files 93
  configuring 30
  remote syslog server 30
  viewing and searching 93
  where stored 93
system name See hostname
system resources
  monitoring real-time use of 90
  viewing summary 88
system time, current 88

T
Telnet 75
time and date
  setting 26
  viewing current system 88
timeout, session 70
trap messages 56
traps
  agent address in messages 57
  enabling authorization 57
  sending 57
troubleshooting
  providing system information to Customer Support 95

U
unauthenticated connections, number of allowable 78
uptime 88, 89
users
  creating accounts 62, 63
  deleting 64
  editing accounts 62, 63
  home directories 64
  login grace time 78
  providing SSH access for 77
  specifying login environment for 77
  viewing current Network Voyager user 88
  viewing list of 89
Users group 64

V
version number 89
Voyager See Network Voyager
VSZ 91

W
WCHAN (wait channel) 91
web server
  access and error log 93
  access and error logs 93
Wheel group 65

X
xntpd process 92
xpand process 92