

NOKIA

**SNMP configuration and asset
management summary in Voyager
for IPSO 3.8NET**

The product described in this document is still under development by Nokia Networks. However, in the interest of offering early possibility to our customers to evaluate the documentation, this documentation is provided in draft form. Therefore the customer understands that the information in this document is subject to change without notice and describes only the prototype product defined in the introduction of this documentation in its current state of development. Nokia Networks welcomes customer comments as part of the process of continuous development and improvement of its products and the documentation.

This document is not a final customer document and Nokia Networks does not take responsibility for any errors or omissions in this document. No part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia Networks. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia Networks and the customer.

Nokia Networks WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it. UNDER NO CIRCUMSTANCES SHALL NOKIA BE RESPONSIBLE FOR ANY LOSS OF USE, DATA, OR INCOME, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY OR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES HOWSOEVER CAUSED.

THE CONTENTS OF THIS DOCUMENT ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE MANDATORY LAW, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS DOCUMENT. NOKIA RESERVES THE RIGHT TO REVISE THIS DOCUMENT OR WITHDRAW IT AT ANY TIME WITHOUT PRIOR NOTICE.

This document and the product it describes are protected by copyright according to the applicable laws.

NOKIA and Nokia Connecting People are registered trademarks of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective companies, and they are mentioned for identification purposes only.

Copyright © Nokia Corporation 2003. All rights reserved. Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Contents

	Contents	3
1	SNMP configuration	5
1.1	Overview of SNMP configuration	5
1.2	Enabling and disabling the SNMP daemon	8
1.3	Setting community strings	9
1.4	Disabling community strings	9
1.5	Sending SNMP traps to network management system	10
1.6	Enabling SNMP traps	11
1.7	Configuring SNMP agent address	15
1.8	Setting SNMP trap PDU agent address	16
1.9	Entering SNMP location and contact information	16
1.10	Adding user-based security model users	17
1.11	Deleting user-based security model users	19
1.12	Modifying user-based security model user entries	20
1.13	Changing user-based security model user permissions	21
2	Viewing the asset management summary	23

1 SNMP configuration

1.1 Overview of SNMP configuration

SNMP, as implemented on the Nokia platforms, supports the following:

- SNMPGet, SNMPSet, SNMPGetNext, SNMPWalk and a select number of traps. See *Enabling SNMP traps* for more information.
- Other public and proprietary MIBs as follows:

MIB	Source	Function
Rate-Shape MIB	proprietary	Monitoring rate-shaping statistics and configuration. Monitoring system-specific parameters.
IPR System MIB	proprietary	The IPSO chassis temperature, fan group, and power-supply group function only on certain platforms.
IPR Registration MIB	proprietary	Defines the system MIB for IPSO.
OID Registration MIB	proprietary	
Unit Types MIB	proprietary	Contains OID values for the different types of circuit cards used in Nokia equipment.
Nokia Common MIB OID Registration MIB	proprietary	
Nokia Common NE Role MIB	proprietary	

MIB	Source	Function
Nokia Enhanced SNMP Solution Suite Alarm IRP	proprietary	
Nokia Enhanced SNMP Solution Suite Common Definition	proprietary	
Nokia Enhanced SNMP Solution Suite PM Common Definition	proprietary	
Nokia Enhanced SNMP Solution Suite PM IRP	proprietary	
Nokia NE3S Registration MIB	proprietary	
Nokia NTP MIB	proprietary	
TCP MIB	RFC 793	
EtherLike MIB	RFC 1650	Generic objects for Ethernet-like network interfaces.
Host Resources MIB	RFC 1514	Configures, manages, keeps statistics, and handles errors in one or more circuits of system components.
IANAifType MIB	Internet Assigned Numbers Authority	Defines the IANAifType textual convention, including the values of the ifType object defined in the MIB-II ifTable.
IF MIB	RFC 2233	Describes generic objects for network interface sub-layers
IP Forward MIB	RFC 2011	Displays CIDR multipath IP routes
VRRP MIB	proprietary	Provides dynamic fail-over statistics.
RIP MIB	RFC 1724	
SNMP Framework MIB	RFC 2571	Outlines SNMP management architecture

MIB	Source	Function
SNMP MPD MIB	RFC 2572	Provides message processing and dispatching.
SNMP User-based SM MIB	RFC 2574	Provides management information definitions for SNMP User-based Security Model
SNMP View-based ACM MIB	RFC 2575	Provides management information definitions for the View-based Access Control Model for SNMP
SNMPv2 MIB	RFC 1907	Defines SNMPv2 entities
SNMPv2 SMI	RFC 2578	
SNMPv2 TC	RFC 854	Defines textual conventions for various values reported in OIDs and Traps.
Dial-Control MIB	RFC 2128	Describes peer information for demand access and other kinds of interfaces.
Entity MIB	RFC 2737	Represents the multiple logical entities supported by a single SNMP agent
Tunnel-MIB	RFC 2667	Manages IP tunnels
UDP-MIB	RFC 2013	Manages UDP implementations
Frame Relay DTE MIB	RFC 2115	Manages and keeps statistics and errors in one or more circuits of a frame relay device.
Check Point MIB	proprietary	Statistics and version information on any firewalls currently installed.
HWM MIB	proprietary	Controls hardware management information
1213 MIB	RFC 1213	
IPSO-LBCluster-MIB	proprietary	Manages IPSO load balancing systems

Both the proprietary MIBs and the public MIBs are supplied with the system. To view more detailed information about the MIBs, see the `/etc/snmp/mibs` directory.

Use Voyager to perform the following tasks:

- Define and change one read-only community string. Define and change one read-write community string.
- Enable and disable the SNMP daemon.
- Enable and disable USM users.
- Modify USM user access privileges, that is, change permissions from read-only to read-write and vice versa.
- Add or delete trap receivers
- Enable or disable the various traps
- Enter the location and contact strings for the device
- Configure the SNMP agent address

1.2 Enabling and disabling the SNMP daemon



Steps

1. Click **Config** on the home page.
2. Click the **SNMP** link.
3. To enable the SNMP daemon, click the **Yes** radio button in the **Enable SNMP Daemon** field.
4. Click **Apply**.

Expected outcome

All possible configuration options will appear, allowing you to enter the necessary values.

5. To disable the SNMP daemon, click the **No** radio button in the **Enable SNMP Daemon** field.
6. Click **Apply**.

Expected outcome

The configuration options disappear.

7. To make your changes permanent, click **Save**.

1.3 Setting community strings



Steps

1. **Click Config on the home page.**
2. **Click the *SNMP* link.**
3. *If you want to enable or change the read-only community string*

Then

enter the name of the new string in the Read-only Community String edit box and click Apply.

Use alphanumeric characters without spaces.

4. *If you want to enable or change a read-write community string*

Then

enter the name in the Read-write Community String edit box and click Apply.

Use alphanumeric characters without spaces.

5. **To make your changes permanent, click Save.**

Further information

See *Disabling community strings*

1.4 Disabling community strings



Steps

1. **Click Config on the home page.**
2. **Click the *SNMP* link.**
3. **To disable a read-only community string, click the Disable box in the Current Read-only Community Strings field. Click Apply.**
4. **To disable a read-write community string, click the Disable box in the Current Read-write Community Strings field. Click Apply.**

5. To make your changes permanent, click Save.

Further information

See *Setting community strings*

1.5 Sending SNMP traps to network management system



Steps

1. Click **Config** on the home page.
2. Click the **SNMP** link.

For IPv4 address(es), click the *SNMP* link.

For IPv6 address(es), first click the *IPv6 configuration* link, and then the *SNMP* link.
3. Enter the IP address (or the hostname if DNS is set) of a new receiver that will accept traps from this device in the **Add New trap RECEIVER** edit box.
4. Click **Apply**.
5. **(Optional) Enter the community string, using alphanumeric characters (do not use spaces), for the specified receiver in the COMMUNITY STRING FOR New trap Receiver edit box and click Apply.**

The default is community string for the trap receiver is public.
6. To delete an existing receiver, click the **Off** radio button in the **Status** field.
7. Click **Apply**.
8. To make your changes permanent, click **Save**.

1.6 Enabling SNMP traps

Purpose

The system traps are defined in the Nokia-IPR-System-MIB. The ifLinkUpDown trap is defined in the IF-MIB. The clustering traps are defined in the Nokia-IPSO-LBCluster-MIB. The Disk Mirror traps are defined in the Nokia-IPR-System-MIB. The text files that define the MIBs are located in the /etc/snmp/mibs directory.

Below is a list of the objects associated with individual traps.

The systemTrapsConfigurationChange, systemTrapConfigurationFileChange, and systemTrapConfigurationFileSave traps are associated with the ipsoConfigGroup objects. These objects include ipsoConfigIndex, ipsoConfigFilePath, ipsoConfigFileDateAndTime, ipsoConfigLogSize, ipsoConfigLogIndex, and ipsoConfigLogDescr.

The systemTrapDiskMirrorSetCreate, systemTrapDiskMirrorSetDelete, systemTrapDiskMirrorSyncFailure, and systemTrapDiskMirrorSyncSuccess traps are associated with the ipsoDiskMirrorGroup objects. These objects include ipsoTotalDiskMirrorSets, ipsoMirrorSetIndex, ipsoMirrorSetSourceDrive, ipsoMirrorSetDestinationDrive, ipsoMirrorSetSyncPercent.

The linkUp and linkDown traps are associated with the ifIndex, ifAdminStatus, and ifOperStatus objects.



Steps

1. **Click Config on the home page.**
2. **Click the SNMP link.**
3. **(Optional) Verify that the SNMP agent has been reinitialized.**

Enable cold start traps:

- a. Click the **On** radio button next to the **Enable Coldstart Traps** field.
- b. Click **Apply**.

4. **(Optional) Verify when one of the administratively up links has either come up or been lost.**

Enable link up/link down traps:

- a. Click the **On** radio button next to the **Enable Linkup/Linkdown Traps** field.
- b. Click **Apply**.

5. (Optional) To receive notification that an SNMP operation is not correctly authenticated.

Enable the authentication failure traps:

- a. Click the **On** radio button next to the **Enable Authorization Traps** field.
- b. Click **Apply**.

6. (Optional) Enable the VRRPTrapNewMaster.

- a. Click the **On** radio button next to the **Enable VRRPTrapNewMaster Traps** field.
- b. Click **Apply**.

7. (Optional) Enable the VRRPTrapAuthFailure.

- a. Click the **On** radio button next to the **Enable VRRPTrapAuthFailure Traps** field.
- b. Click **Apply**.

8. (Optional) To receive notification that a temporary change to the system configuration has occurred

Enable the System trap Configuration Change traps:

- a. Click the **On** radio button next to the **Enable Systemtrap ConfigurationChange Traps** field.
- b. Click **Apply**.

9. (Optional) To receive notification that a different configuration file has been selected.

Enable System trap Configuration File Change traps:

- a. Click the **On** radio button next to the **Enable SystemtrapConfigurationFileChange Traps** field.
- b. Click **Apply**.

10. (Optional) To receive notification that a permanent change to the system configuration has occurred.

Enable System trap Configuration Save Change traps:

- a. Click the **On** radio button next to the **Enable SystemtrapConfigurationSaveChange Traps** field.
- b. Click **Apply**.

11. (Optional) To know when space on the system disk is low.

Enable System trap low disk space traps:

This trap is sent if the disk space utilization has reached 80% or more of its capacity. If this situation persists, a subsequent trap is sent after 15 minutes.

- a. Click the **On** radio button next to the **Enable Systemtraplowdiskspace Traps** field.
- b. Click **Apply**.

12. (Optional) To know when the system disk is full.

Enable Systemtrapnodiskspace traps:

This trap is sent if 2% or less of the disk space remains available, or if the remaining disk space is equal to or less than 1 MB. If this situation persists, a subsequent trap is sent after 15 minutes.

- a. Click the **On** radio button next to the **Enable Systemtrapnodiskspace Traps** field.
- b. Click **Apply**.

13. (Optional) To receive notification when a particular disk drive fails.

Enable Systemtrapdiskfailure traps:

- a. Click the **On** button next to the **Enable Systemtrapdiskfailure Traps** field.
- b. Click **Apply**.

14. (Optional) To receive notification when a system disk mirror set is created.

Enable Systemtrapdiskmirrorsetcreate traps:

- a. Click the **On** button next to the **Enable Systemtrapdiskmirrorsetcreate Traps** field.
- b. Click **Apply**.

15. (Optional) To receive notification when a system disk mirror set is deleted.

Enable SystemtrapDiskmirrorsetDelete traps:

- a. Click the **On** button next to the **Enable SystemtrapDiskmirrorsetDelete Traps** field.
- b. Click **Apply**.

16. (Optional) To receive notification when a system disk mirror set is successfully synced.

Enable SystemtrapDiskmirrorsyncsuccess traps:

- a. Click the **On** button next to the **Enable SystemtrapDiskmirrorsyncsuccess Traps** field.
- b. Click **Apply**.

17. (Optional) To receive notification when a system disk mirror set fails during syncing.

Enable SystemtrapdiskmirrorSYNCfailure traps:

Note

The disk mirror traps are supported only on systems where disk mirroring is supported.

- a. Click the **On** button next to the **Enable SystemtrapdiskmirrorSYNCfailure Traps** field
- b. Click **Apply**.

18. (Optional) To receive notification that a routing instance has been created, deleted or changed.

Enable sys-routing-instance-change traps:

- a. Click the **On** button next to the **Enable sys-routing-instance-change Traps** field.
- b. Click **Apply**.

19. (Optional) To receive notification that a routing instance - interface association relation has been created or removed.

Enable sys-routing-instance-mapping-change traps:

- a. Click the **On** button next to the **Enable sys-routing-instance-mapping-change Traps** field.
 - b. Click **Apply**.
- 20. To disable any of the above traps.**
- Click the **Off** radio button next to the name of the trap.
- 21. Click Apply.**
- 22. To make your changes permanent, click Save.**

1.7 Configuring SNMP agent address



Steps

- 1. Click Config on the home page**
- 2. Click the *SNMP* link.**

For IPv4 address(es), click the *SNMP* link.

For IPv6 address(es), first click the *IPv6 configuration* link, and then the *SNMP* link.
- 3. To specify the IP address to be used for the SNMP Agent, enter it in the Agent New ADDRESS field, and then click Apply.**

This address must belong to a local interface. If you do not specify the agent address, SNMP will listen on all interfaces.
- 4. Once an address is added, click On and Off to remove and add agent addresses.**
- 5. To make your changes permanent, click Save.**

Further information

See *Setting the SMNP trap PDU agent address* and *Entering SNMP location and contact information*

1.8 Setting SNMP trap PDU agent address



Steps

1. Click **Config** on the home page.
2. Click the **SNMP** link.

For IPv4 address(es), click the *SNMP* link.

For IPv6 address(es), first click the *IPv6 configuration* link, and then the *SNMP* link.

3. **(Optional) To specify the IP address to be used for sent trap PDU's, enter it in the trap PDU AGENT ADDRESS field, and then click Apply.**

The Network Management System uses the agent address to identify the network element that generated the trap. This address must belong to one of the interfaces. If you do not specify the agent address, the address of a configured and operational interface is used.

4. To make your changes permanent, click **Save**.

1.9 Entering SNMP location and contact information



Steps

1. Click **Config** on the home page.
2. Click the **SNMP** link.
3. **(Optional) In the SNMP Location String field, enter the actual location of the device. Click Apply.**
4. **(Optional) In the SNMP Contact String field, enter the department or person who has administrative responsibility for the device. Click Apply.**
5. To make your changes permanent, click **Save**.

1.10 Adding user-based security model users

Purpose

The implementation allows you to generate user accounts that make use of the user-based security model (USM) portion of SNMPv3. The SNMPv3 message encapsulates a protocol data unit (PDU) compatible with earlier versions of SNMP. SNMPv3 defines a user-based security mechanism that enables per-message authentication and encryption. See RFC 2574 for more information. You must use Voyager to create USM user accounts. SNMPv3 uses a default configuration to generate USM keys.

This procedure describes how to add a USM user.



Steps

1. **Click Config on the home page.**
2. **Click the *SNMP* link. You are now in the *SNMP* page. Click the *Add USM Users* link.**
3. **In the *Add New User* field, enter a login name for the user in the *Username* edit box.**

The range for a new user name is 1 to 8 alphanumeric characters with no spaces.

4. **In the *Add New User* field, enter a numeric value for the *User ID* in the *UID* edit box.**

The range is 0-65535. There is no default.

5. **Enter the name of the user's home directory in the *Home Directory* edit box.**

Enter the full Unix path name of the directory where the user will be placed after login. If the home directory does not exist, the system will create it.

6. **Click *Apply*.**

Expected outcome

An entry for the new user and his/her profile appears. The default shell is `/bin/csh`. The default page refers to the user's default page when he/she logs in. The default page is set to the home page.

- 7. (Optional) To modify the shell, enter the new shell path name in the Shell edit box.**

Consult the file `/etc/shells` for valid login shells.

- 8. If you want to modify the default page**

Then

enter the name of the new default page in the Default Page edit box.

- 9. Enter the new user's password in the New Password edit box.**

Leave the OLD PASSWORD edit box empty.

- 10. Enter the same password that you entered in the New Password edit box in the New Password (Verify) edit box.**

Note

The password of an SNMP USM user must be at least 8 characters long.

- 11. Click Apply.**

- 12. To make your changes permanent, click Save.**

Note

A table appears on the SNMP page with the name of each user and his/her permissions.

Further information

See *Deleting user-based security model users*, *Modifying user-based security model user entries* and *Changing user-based security model user permissions*

1.11 Deleting user-based security model users

Purpose

This procedure describes how to delete a user-based security model (USM) user.



Steps

1. Click **Config** on the home page.

2. Click the **SNMP** link.

Expected outcome

You are now on the SNMP page.

3. Click the **Add USM Users** link.

4. If you want to delete a user completely

Then

click the Off radio button next to the name of each user you want to delete and click Apply.

Expected outcome

The name of each user and his/her entry disappears from the SNMPV3 USERS list on the SNMP page.

5. If you want to remove a user's SNMPv3 functionality but keep that user as an IPSO user

Then

change the user's password.

- a. Enter the user's current password in the **Old Password** edit box.
- b. Enter a new password that is fewer than 8 characters long but at least 6 characters long in the **New Password** edit box.
- c. Enter the same password that you entered in the **New Password** edit box in the **New Password (Verify)** edit box.
- d. Click **Apply**.

Expected outcome

The name of the user and his/her entry disappears from the SNMPV3 USERS list on the SNMP page.

Further information

The name of any user whose password you change to one that has fewer than 8 characters but has at least 6 characters continues to appear on the Pass-word Setting page. To reach that page, click **Config** on the home page and then click the *Users* link in the *Security and Access Configuration* section. Click **Apply**.

6. To make your changes permanent, click **Save**.

Further information

See *Adding user-based security model users* and *Modifying user-based security model user entries*

1.12 Modifying user-based security model user entries

Purpose

This procedure describes how to modify a user-based security model (USM) user entry.

**Steps**

1. Click **Config** on the home page.
2. Click the **SNMP** link.

Expected outcome

You are now on the SNMP page.

3. Click the **Add USM Users** link.
4. Go the entry for the user whose profile you want to modify.

Click on the edit box(es) for which you want to enter a change. Enter the new value or name.

5. Click **Apply**.
6. To make your changes permanent, click **Save**.

Further information

See *Deleting user-based security model users*

1.13 Changing user-based security model user permissions

Purpose

This procedure describes how to change read and write permissions for a user-based security model (USM) user.



Steps

1. **Click Config on the home page.**
2. **Click the SNMP link.**

Expected outcome

You are now on the SNMP page.

3. **Go the SNMPv3 USM Users table.**

Find the user for which you would like to change read or write permissions. Click the radio button corresponding to the type of permission you would like for that user in the Permission column.

4. **Click Apply.**
5. **To make your changes permanent, click Save.**

Further information

See *Modifying user-based security model user entries*

2

Viewing the asset management summary

Purpose

The asset management summary page provides a summary of all system resources, including hardware, software and the operating system. The hardware summary includes information about the CPU, Disks, Bios, and motherboard, including the serial number, model number, and capacity, 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.



Steps

1. **Click Config on the home page.**
2. **Click the *Asset Management Summary* link.**

Expected outcome

You are taken to the asset management summary page. The page separates information into three tables: Hardware, FireWall Package Information, and Operating System.

3. **Click the Up button to return to the main configuration page.**