



Technical Document

Configuring HPE Intelligent Management Center (IMC) for SNMPv3 communications with NuDesign Agent Service

NuDesign Technologies, Inc.

This document is provided for informational purposes only, 'as is' and without warranty of any kind. This document may be copied, however without any modification, and all pages and notices must be included.



Table of Contents

DOCUMENT HISTORY..... 3

INTRODUCTION..... 4

CONFIGURING IMC..... 5

DEFAULT USM USERS..... 16

ABOUT NUDESIGN TECHNOLOGIES..... 17

This document is provided for informational purposes only, 'as is' and without warranty of any kind. This document may be copied, however without any modification, and all pages and notices must be included.

Document History

Date	Rev.	Remarks	Author
2018/08/17	A01	Created	Brian Munshaw

Introduction

This document explains how to configure HPE's **Intelligent Management Center (IMC)** to communicate with a **NDT SNMPv3 Agent Service**, using default SNMPv3 credentials to verify SNMPv3 communications with your NDT SNMPv3 Agent Service's installation.

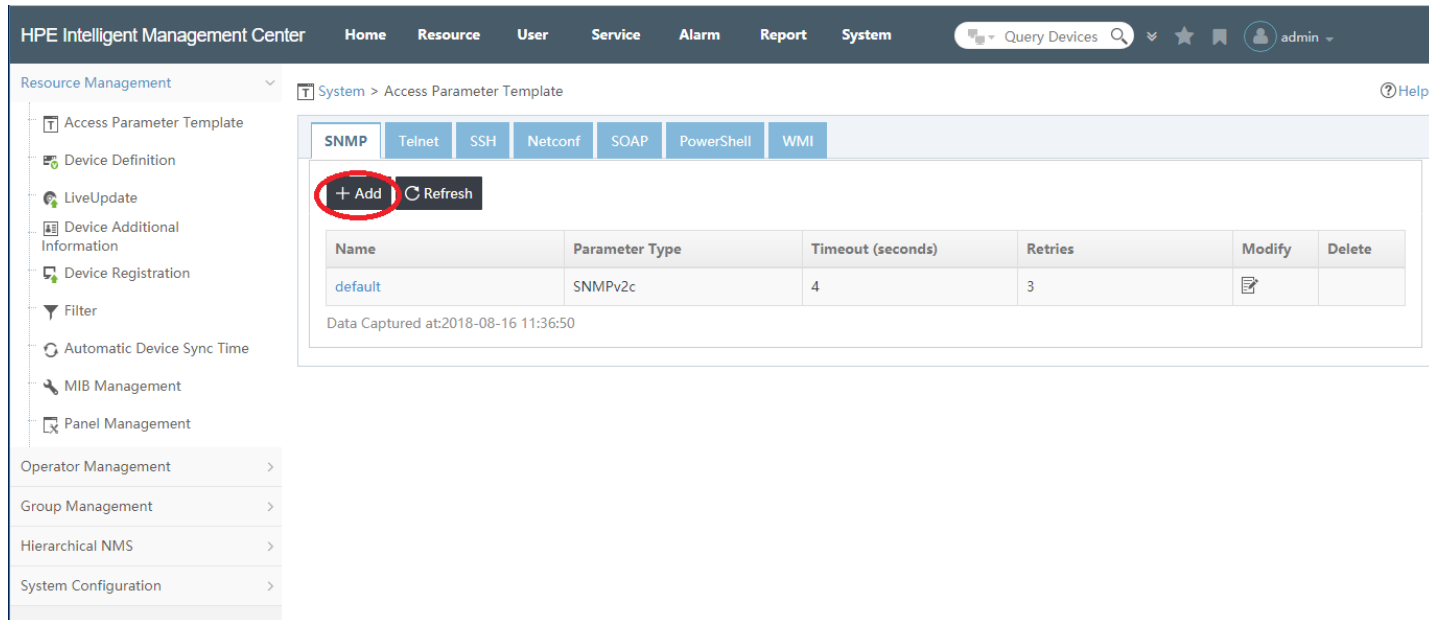
Specifically, this document will show you how to configure **IMC** with the default USM User "**shaaes**" which provides an authenticated and encrypted SNMPv3 communication channel. It will also show you how to set up a "Device" which will be the **NDT SNMPv3 Agent Service**.

The document then will take you through some steps to interact with the **NDT SNMPv3 Agent Service**, using the **IMC**, to verify that the service is operational and communicating with **SNMPv3**.

Configuring IMC

When initially run, **IMC** only has a **SNMP** communication template set up for **SNMPv2**. So the first step is to create a template for **SNMPv3** and in particular for the default **USM User "shaaes"**.

To do this, go to the "System|Access Parameter Template" page on IMC and select "+ Add".



The screenshot displays the HPE Intelligent Management Center (IMC) interface. The top navigation bar includes 'Home', 'Resource', 'User', 'Service', 'Alarm', 'Report', and 'System'. The main content area is titled 'System > Access Parameter Template'. On the left, a sidebar lists various management options under 'Resource Management' and 'System Configuration'. The main panel shows a tabbed interface with 'SNMP' selected. Below the tabs, there are '+ Add' and 'Refresh' buttons. A table lists the existing templates:

Name	Parameter Type	Timeout (seconds)	Retries	Modify	Delete
default	SNMPv2c	4	3		

Data Captured at: 2018-08-16 11:36:50

Next, you'll see the following page (note: some entries already have been filled in, see below):

System > SNMP Template > Add SNMP Template

Name *	shaaes	?
Parameter Type *	SNMPv3 Priv-Aes128 Auth-Sha	▼
Username *	shaaes	?
Authentication Password *	
Encryption Password *	
Context Name		?
Timeout (1-60 seconds) *	4	
Retries (1-20) *	3	
Public	<input checked="" type="checkbox"/>	

OK Cancel

On this page, Set and Select the following:

- Set "**Name**" to anything you like, but I've used "**shaaes**", just for consistency.
- Select from the "**Parameter Type**" drop down, "**SNMPv3 Priv-Aes 128 Auth-Sha**"
- Set "Username" to "**shaaes**"
- Set "**Authentication Password**" to "**shaaesauth**"
- Set "**Encryption Password**" to "**shaaespriv**"

- Press "**OK**"

In the SNMP template page you should now see another SNMP row for "**shaaes**":

System > Access Parameter Template

Help

SNMP	Telnet	SSH	Netconf	SOAP	PowerShell	WMI
+ Add Refresh						
Name	Parameter Type	Timeout (seconds)	Retries	Modify	Delete	
default	SNMPv2c	4	3			
shaaes	SNMPv3 Priv-Aes128 Auth-Sha	4	3			

Data Captured at:2018-08-16 14:38:02

Now Select **"Resource | Device View"** and you should see the following page:

Resource > Device View-All-Exclude Desktops

Device Management System Management

Template Management

Add to My Favorites Help

Generate Chart Delete Manage Unmanage Synchronize Refresh More View Export Excel

Search device IP,label,status: 🔍

Status	Device Label	Model	IP Address	Device Category	Operation
No match found.					

0-0 of 0. Page 1 of 1.

Data Captured at 2018-08-16 11:56:44

Now drop down **"Device Management"** and select **"Add Device"**.

Resource > Device View-All-Exclude Desktops

Device Management Add Device Import Device Auto Discovery

Template Management

Add to My Favorites Help

Generate Chart Delete Manage Unmanage Synchronize Refresh More View Export Excel

Search device IP,label,status: 🔍

Status	Device Label	Model	IP Address	Device Category	Operation
No match found.					

0-0 of 0. Page 1 of 1.

Now you should see something like (note: some entries already have been filled in, see below):

Resource > Add Device

Basic Information

Host Name/IP * 192.168.2.196

Device Label Host WS

Mask 255.255.255.0

Device Group

Login Type None

Automatically register to receive SNMP traps from supported devices

Support Ping Operation

Add the device regardless of the ping result

Use the loopback address as the management IP

SNMP Settings

[Configure](#)

Parameter Type	SNMPv2c
Read-Only Community String	*****
Read-Write Community String	*****
Timeout (seconds)	4
Retries	3

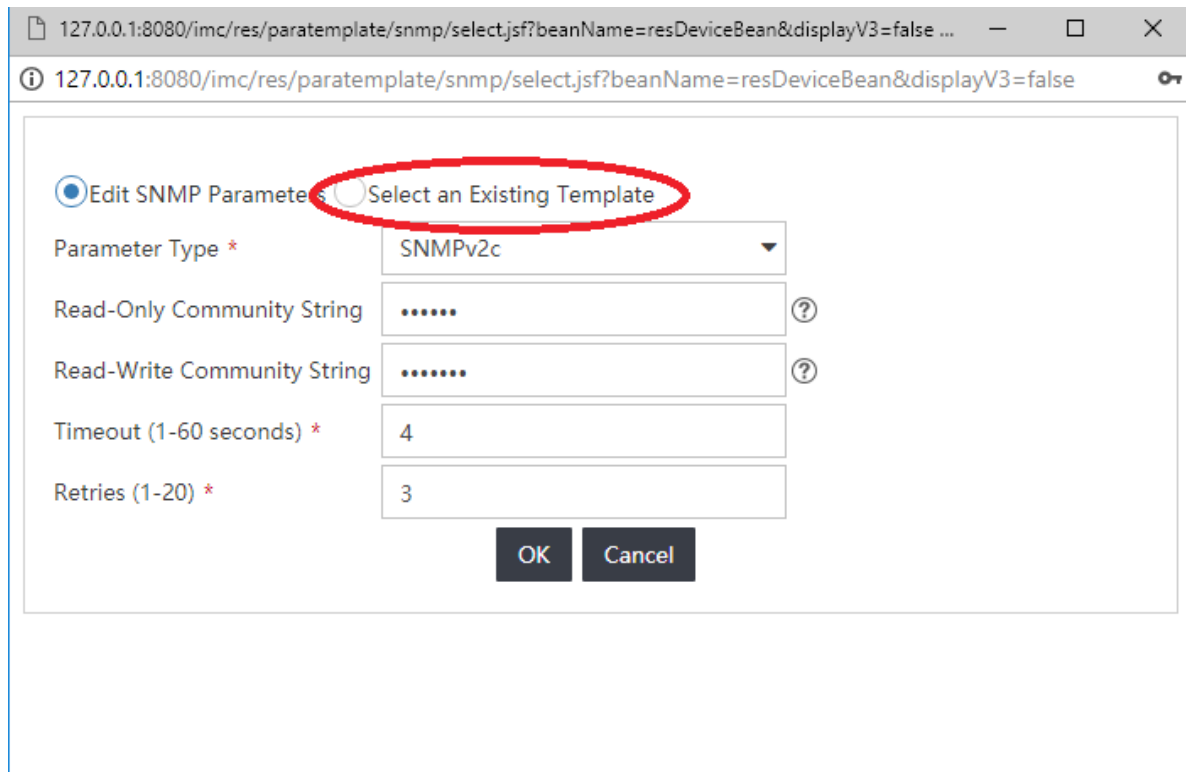
+ Telnet Settings

+ SSH Settings

Set and Select:

- Set "**Hostname/IP**" for the device running our **NDT SNMPv3 Agent Service** (with the default configuration). In this e.g. "**192.168.2.196**"
- Set "**Device Label**" to something to identify this device. In this e.g. "**Host WS**"
- Set "**Mask**" to an appropriate network mask for the IP address of the device running our service with the default configuration. In this e.g. "**255.255.255.0**"
- Leave "**Login Type**" to "**none**"
- Note: I've unchecked "Support Ping Operation" since if you can't ping the device, this step will not complete successfully.
- Select the "**Configure**" link.

Now you should see something like:



The screenshot shows a web browser window with the URL `127.0.0.1:8080/imc/res/paratemplate/snmp/select.jsf?beanName=resDeviceBean&displayV3=false`. The main content area contains a form with two radio buttons at the top: Edit SNMP Parameters and Select an Existing Template. The second radio button is circled in red. Below the radio buttons are several input fields: a dropdown menu for 'Parameter Type' set to 'SNMPv2c', two text boxes for 'Read-Only Community String' and 'Read-Write Community String' (both masked with dots), a text box for 'Timeout (1-60 seconds)' set to '4', and a text box for 'Retries (1-20)' set to '3'. At the bottom of the form are 'OK' and 'Cancel' buttons.

Select the **"Select an Existing Template"**.

After selecting "Select an Existing Template" and you should see:

127.0.0.1:8080/imc/res/paratemplate/snmp/select.jsf?beanName=resDeviceBean&displayV3=false - Google Chrome

127.0.0.1:8080/imc/res/paratemplate/snmp/select.jsf?beanName=resDeviceBean&displayV3=false

Edit SNMP Parameters Select an Existing Template ! The templates do not have mapping relationship with the device parameters

	Name	Parameter Type	Username	Timeout (seconds)	Retries
<input type="radio"/>	default	SNMPv2c		4	3
<input checked="" type="radio"/>	shaaes	SNMPv3 Priv-Aes128 Auth-Sha	shaaes	4	3

1-2 of 2. Page 1 of 1. « < 1 > »

Select "**shaaes**" and press "**OK**"

Now the "Add Device" page should look like:

Resource > Add Device ? Help

Basic Information

Host Name/IP *

Device Label

Mask ?

Device Group ?

Login Type ?

Automatically register to receive SNMP traps from supported devices

Support Ping Operation ?

Add the device regardless of the ping result ?

Use the loopback address as the management IP

SNMP Settings

[Configure](#)

Parameter Type	SNMPv3 Priv-Aes128 Auth-Sha
Username	shaaes
Authentication Password	*****
Encryption Password	*****
Timeout (seconds)	4
Retries	3

+ Telnet Settings

+ SSH Settings

Once you press "OK" at the bottom of the page.

Once you press "OK" at the bottom of the page above, you should see the following page, confirming the configuration:

The screenshot shows a web application interface with a dark grey top navigation bar containing buttons for 'Generate Chart', 'Delete', 'Manage', 'Unmanage', 'Synchronize', 'Refresh', 'More', 'View', and 'Export Excel'. Below the navigation bar, the breadcrumb 'Resource > Device Information' is visible, along with a 'Help' icon. A light grey message box contains the text 'Device successfully added. You can continue to:'. Below this message, three options are listed: 'Device Details' (circled in red), 'Clone to Add', and 'Add Device'. Each option has a corresponding description: 'Device Details' leads to 'List the details of the newly added device.', 'Clone to Add' leads to 'Use the SNMP, Telnet and SSH parameters of the last new device to add a device.', and 'Add Device' leads to 'Use the default template to add a device.'.

Device successfully added. You can continue to:	
Device Details	List the details of the newly added device.
Clone to Add	Use the SNMP, Telnet and SSH parameters of the last new device to add a device.
Add Device	Use the default template to add a device.

From this page, select the "Device Details".

Once "Device Details" are selected, then a page similar to following will be displayed:

The screenshot displays a network management interface for a device labeled "Host WS(192.168.2.196)". The interface includes a top navigation bar with buttons for "Generate Chart", "Delete", "Manage", "Unmanage", "Synchronize", "Refresh", "More", "View", and "Export Excel". Below this, the breadcrumb "Resource > Host WS(192.168.2.196)" is shown, along with "Add to My Favorites" and "Help" options.

The main content area is titled "Device Details" and contains the following information:

- Device Label:** Host WS [Modify]
- Device Status:** Normal
- IP Address:** 192.168.2.196
- Mask:** 255.255.255.0
- sysOID:** 1.3.6.1.4.1.311.1.1.3.1.1
- Device Model:** Microsoft Windows Workstation
- Device Category:** Servers [Modify]
- System Name:** WS [Modify]
- Contact:** www.ndt-inc.com [Modify]
- Location:** Toronto [Modify]
- Runtime:** 20 day(s) 0 hour(s) 9 minute(s) 5 second(s) 420 millisecond(s)
- Last Poll:** 2018-08-16 12:06:24
- Login Type:** None [Modify]
- Interfaces:** 66 [Interface List]
- System Description:** Hardware: Intel64 Family 6 Model 62 Stepping 4 AT/AT COMPATIBLE - Software: Windows Version 10.0 (Build 14393 Multiprocessor Free)
- Maintenance Tag:** No Maintenance Tag [Modify]

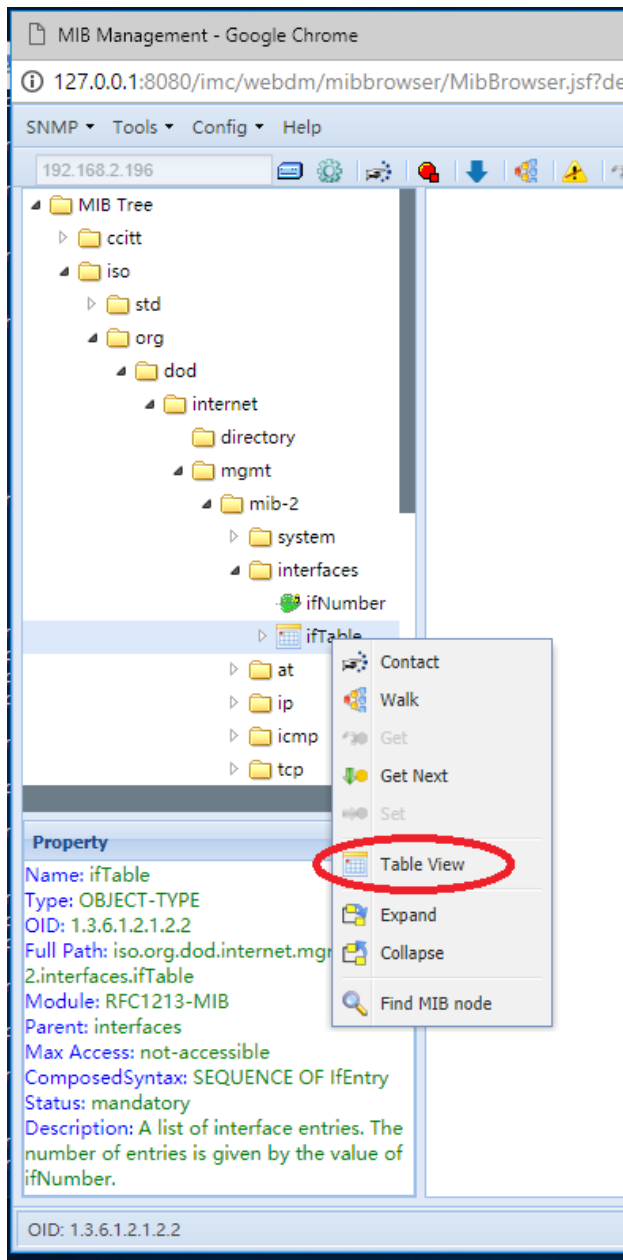
On the right side, an "Action" menu is open, listing various operations: Synchronize, Refresh, Unmanage, Delete, Telnet, Open Web Manager, Ping, Traceroute, View Topology, **MIB Management** (circled in red), Telnet/SSH Proxy, Open Device Panel, and SSH. Below the action menu are links for "Configure", "Performance Monitor", and "Device Management".

Below the device details, there are tabs for "Service Monitoring", "Trap Destination", and "Network Assets". The "Service Monitoring" tab is active, showing "Monitoring Service" with "Total Items: 0" and a "Customize" link. Below this is a "Performance Monitor" section with a table:

Monitor Index	Monitored Value	Operation
Average CPU Usage (%) in Last Hour - [CPU:.6]	--	Stop Monitor
Average CPU Usage (%) in Last Hour - [CPU:.7]	--	Stop Monitor
Average CPU Usage (%) in Last Hour - [CPU:.8]	--	Stop Monitor

The information in this page was extracted from the service using **SNMPv3** with the "**shaaes**" **USM User**. You can further interact with the service with **SNMPv3**, if you select the "**MIB Management**" link, on the right.

When you do, you can navigate the MIB and view values. The following shows navigating to the "ifTable".



and selecting "Table View".

If you select "Table View" on "ifTable", you'll see a page similar to the following:

Instance	ifindex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets
1	1	Software Loopback ...	softwareLoopb...	1500	1073741824		up(1)	up(1)	0:00:00.00	0
2	2	Microsoft 6to4 Ada...	131	0	0		down(2)	6	0:00:00.00	0
3	3	Bluetooth Device (R...	other(1)	0	0		down(2)	6	0:00:00.00	0
4	4	Microsoft Hosted N...	71	0	0		down(2)	6	0:00:00.00	0
5	5	WAN Miniport (IKE...	131	1480	0		up(1)	down(2)	0:00:00.00	0
6	6	WAN Miniport (Net...	ethernet-csmac...	1500	0		up(1)	up(1)	0:00:00.00	0
7	7	VMware Virtual Eth...	ethernet-csmac...	1500	100000000	00:50:56:C0:00:01	up(1)	up(1)	0:00:00.00	3207
8	8	Microsoft IP-HTTPS...	131	0	0		down(2)	6	0:00:00.00	0
9	9	Microsoft Wi-Fi Dir...	71	0	0		down(2)	6	0:00:00.00	0
10	10	Microsoft Wi-Fi Dir...	71	0	0		down(2)	6	0:00:00.00	0
11	11	WAN Miniport (PPP...	ppp(23)	1494	0		up(1)	down(2)	0:00:00.00	0
12	12	Realtek PCIe GBE F...	ethernet-csmac...	0	0	E0:3F:49:7D:2A:...	down(2)	6	0:00:00.00	0
13	13	Broadcom 802.11ac...	71	1500	505250000	54:27:1E:55:86:62	up(1)	down(2)	0:00:00.00	0
14	14	WAN Miniport (IPv6)	ethernet-csmac...	1500	0		up(1)	up(1)	0:00:00.00	0
15	15	Microsoft Kernel De...	ethernet-csmac...	0	0		down(2)	6	0:00:00.00	0
16	16	Microsoft Wi-Fi Dir...	71	1500	0	56:27:1E:55:86:62	up(1)	down(2)	0:00:00.00	0
17	17	WAN Miniport (PPTP)	131	1464	0		up(1)	down(2)	0:00:00.00	0
18	18	WAN Miniport (L2TP)	131	1460	0		up(1)	down(2)	0:00:00.00	0
19	19	WAN Miniport (SSTP)	131	4091	0		up(1)	down(2)	0:00:00.00	0
20	20	Microsoft Teredo T...	131	0	0		down(2)	6	0:00:00.00	0
21	21	VMware Virtual Eth...	ethernet-csmac...	1500	100000000	00:50:56:C0:00:08	up(1)	up(1)	0:00:00.00	3208
22	22	Microsoft Hosted N...	71	1500	0	54:27:1E:55:86:62	up(1)	down(2)	0:00:00.00	0

This is the current contents of the ifTable. The actual content will be different, but similar on your installation.

Default USM Users

As noted earlier, the example configuration above is based on the default configuration for a NuDesign SNMPv3 agent service. NuDesign agents ship with the following pre-configured* USM users:

Name	Authentication		Privacy	
	Protocol	Password	Protocol	Password
public	none		none	
md5	MD5	md5auth	none	
md5nopriv	MD5	md5noprivauth	none	
sha	SHA	shaauth	none	
shanopriv	SHA	shanoprivauth	none	
md5des	MD5	md5desauth	DES	md5despriv
shades	SHA	shadesauth	DES	shadespriv
md5aes	MD5	md5aesauth	AES128	md5aespriv
shaaes	SHA	shaaesauth	AES128	shaaespriv

* These users are supplied for evaluation purposes only. They are **NOT** suggested for a production environment.

User "**shaaes**", as used in the above example, is mapped to "**grpAll**" in the **VacmSecurityToGroupTable**. This gives any **SNMPv3** messages using these parameters "read-write" access.

About NuDesign Technologies

NuDesign provides software development tools, libraries, components and applications for the management and monitoring of networks, systems, services, applications, desktop and embedded devices. The company also provides professional services to customers requiring specific management solutions.

NuDesign's focus is on industry standard management protocols like SNMP and emerging management protocols using HTTP and XML/SOAP transport.

NuDesign's customers are Original Equipment Manufacturers, System Integrators, Service Providers and End Users worldwide.

The benefits of deploying NuDesign's management software technologies are lower costs and reliable, low risk, quick-to-market solutions:

- The End User management products are feature rich, extensible, yet very easy to use out of a box.
- The middleware components come with easy to understand and re-use coding examples.
- The highly automated agent development tools with associated tutorials enable fast prototyping and development, and facilitate organization and design process while supporting multiple target environments with generation of very complete and immediately compilable agent code.

NuDesign's products and services include:

- SNMP development tools and components - SNMP / WEB / CLI agent code visual generation tools for multiple desktop and embedded targets, with standalone Agent and Master Agent / Extension Subagent architectures.
- SNMP components for development of management applications and SNMP MIB building / browsing, managing and testing applications.
- SNMP Management Applications - supporting SNMPv3 Agent and MIB management features, including Graphing, Get, Set, Walk, SNMP packet Trace and Scripting capabilities, Trap Send / Receive applets.
- Host resource monitoring products, and IP services and infrastructure monitoring products.
- Design and Support Services - specific network / element management & monitoring products, porting SNMP code to custom embedded hardware, developing custom management applications. Developing new products that require SNMP / WEB based management interfaces or adding WEB interfaces to existing products.

For more information please visit www.ndt-inc.com, it contains SNMP and MIB development tools and management product descriptions, tutorials and full feature product evaluations packages or call 416 737 0328 to discuss your specific needs.