SNMP Version 3 Tools Implementation Guide

Last Modified: 2022-05-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Preface

This preface includes the following sections:

Obtaining Documentation and Submitting a Service Request

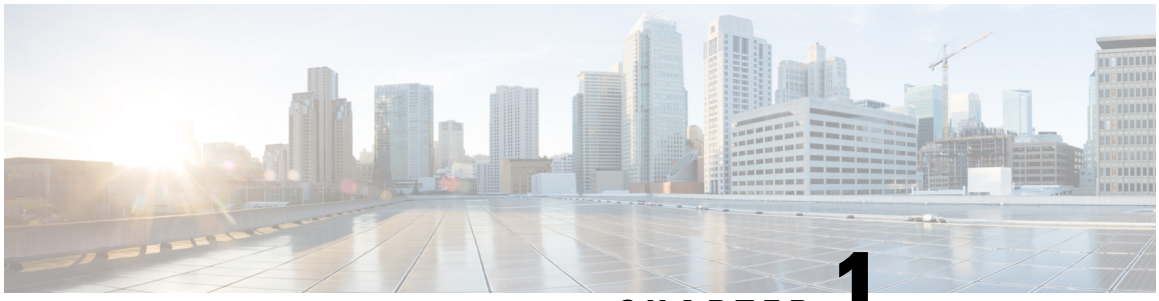
For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation at*: https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Obtaining Additional Tools Application Documentation

For more tools application information, see the following list of documents:

- Net-SNMP Version 5.1.2 documentation and online help (Linux)
- IWL Silvercreek Test Suite tutorial and online help (most recent version)
- HP OpenView NNM SPI Version 7.53 documentation
- Ipswitch WhatsUp Gold Version 12.3 documentation and online help
- CiscoWorks for Windows LMS Version 3.1 online help and tutorials



CHAPTER 1

Overview

SNMP Version 3 provides secure communication of SNMP transactions with an SNMP agent by providing authentication and privacy options through the User-based Security Model (USM) and View-based Access Control Model (VACM). SNMP Versions 1 and 2c have no knowledge of the user for access control to MIBs, nor do they provide encrypted privacy options for authentication. VACM support has been deferred to a future release.

This chapter describes the installation, configuration, and use of CiscoWorks and several third-party tools that can communicate with the Secure Firewall ASA through SNMP Version 3 on a device running ASA software Version 8.2(1) or higher.

The chapter includes the following sections:

Network Management Tools

This document describes the following network management tools:

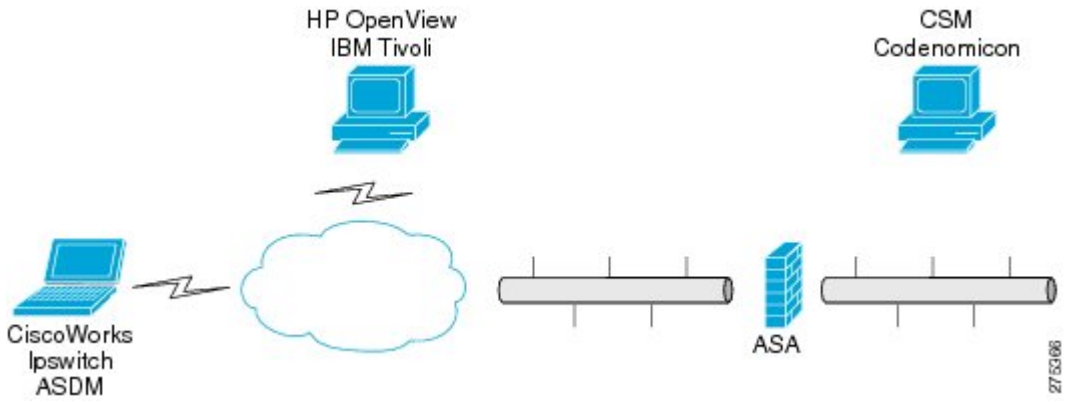
- Net-SNMP (CLI application)
- IWL SilverCreek, the SNMP Test Suite
- Ipswitch WhatsUp Gold
- HP OpenView NNM
- CiscoWorks for Windows LMS

Cisco has tested these tools for interoperability between the NMS and the ASA.

Network Topology

The following figure shows the network topology for implementing SNMP Version 3.

Figure 1: Network Topology for SNMP Version 3 Implementation



ASA Setup

The ASA requires that you configure the SNMP server group, the SNMP server user associated with the group, and the SNMP server host, which specifies the user for receiving SNMP traps.

To configure SNMP Version 3 operations, the required sequence of commands is as follows:

- **snmp-server group**
- **snmp-server user**
- **snmp-server host**

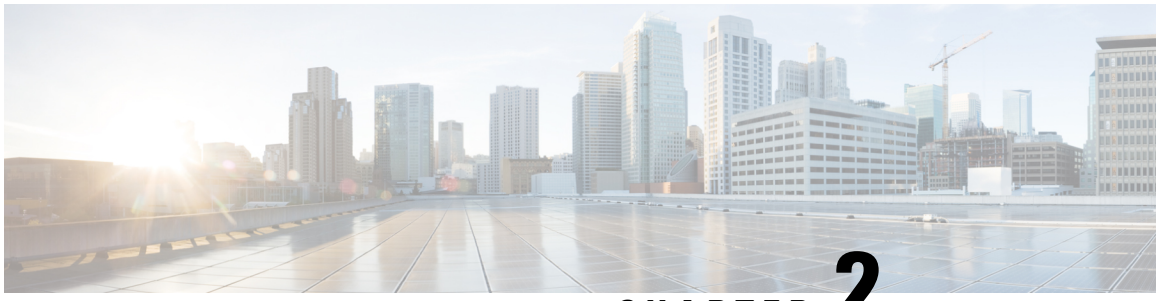
The following shows an example ASA configuration:

```
ciscoasa# snmp-server group authPriv v3 priv
ciscoasa# snmp-server group authNoPriv v3 auth
ciscoasa# snmp-server group noAuthNoPriv v3 noauth

ciscoasa# snmp-server user md5des authPriv v3 auth md5 mysecretpass priv des passphrase
ciscoasa# snmp-server user md5user authNoPriv v3 auth md5 mysecretpass
ciscoasa# snmp-server user noauthuser noAuthNoPriv v3

ciscoasa# snmp-server host mgmt 10.0.0.1 version 3 md5des
ciscoasa# snmp-server host mgmt 10.0.0.2 version 3 md5des
ciscoasa# snmp-server host mgmt 10.0.0.3 version 3 md5des

ciscoasa# snmp-server location Anywhere, USA
ciscoasa# snmp-server contact admin@example.com
ciscoasa# snmp-server enable traps snmp authentication linkup linkdown coldstart
ciscoasa# snmp-server enable traps syslog
ciscoasa# snmp-server enable traps ipsec start stop
ciscoasa# snmp-server enable traps entity config-change fru-insert fru-remove
ciscoasa# snmp-server enable traps remote-access session-threshold-exceeded
```



CHAPTER 2

Using Network Management Tools

This chapter describes CiscoWorks and several third-party network management tools, and includes the following sections:

Net-SNMP

Net-SNMP Version 5.1.2 provides the following tools and libraries:

- An extensible agent
- An SNMP library
- Tools to request or set information from SNMP agents
- Tools to generate and handle SNMP traps

You can download the Net-SNMP network management tool from the following URL: http://sourceforge.net/projects/net-snmp/

This section includes the following topics:

Polling a MIB

To poll a MIB, after you have finished configuring the ASA, run the **snmpwalk** command from the NMS to the ASA:

Note No specific configuration is required for Net-SNMP on Linux when you run the **snmpwalk** command.

```
[root@iLinux2 ~]# snmpwalk -v3 -u md5des -l authPriv -a MD5 -A mysecretpass -x des -X
passphrase 10.31.8.254 1.3.6.1.2.1.1
```

The following is sample output from the **snmpwalk** command:

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Adaptive Security Appliance Version 8.2(0)227
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.915
SNMPv2-MIB::sysUpTime.0 = Timeticks: (486600) 1:21:06.00
SNMPv2-MIB::sysContact.0 = STRING: admin admin
SNMPv2-MIB::sysName.0 = STRING: ciscoasa
SNMPv2-MIB::sysLocation.0 = STRING: sjc - 190 W Tasman Drive, San Jose, CA 95134
USA
SNMPv2-MIB::sysServices.0 = INTEGER: 4
```

Sending a Trap

When the ASA sends a trap, it is authoritative, which means that the user created within the **snmptrapd** command must be associated with the EngineID sending the trap.

To establish this association, perform the following steps:

Step 1 In the /var/net-snmp/snmptrapd.conf file, enter the following statement:

```
createUser -e ENGINEID myuser authentication protocol "my authentication pass" AES "my
privacy pass"
```

For this statement, define the listed parameters, which include the following:

- *ENGINEID*—The EngineID of the application that is going to be sending the trap
- *myuser*—The USM username that is going to be sending the trap
- *authentication protocol*—The authentication type (SHA or MD5, with SHA the preferred setting.)
- *"my authentication pass"*—The authentication pass-phrase to use to generate the secret authentication key. Enclose the pass-phrase in quotation marks if it includes spaces.
- *privacy protocol*—The encryption type to use (AES or DES, with AES the preferred setting)
- *"my privacy pass"*—The encryption pass-phrase to use to generate the secret encryption key. Enclose the pass-phrase in quotation marks if it includes spaces. If you do not enclose the encryption pass-phrase in quotation marks, it is set to the same value as the authentication pass-phrase.

Step 2 In the /tmp/snmptrapd.conf file, enter the following statement:

```
createUser -e 80000009fe8949e0b20319e2d175b93fe7dc24af0dff7db915 md5des MD5 mysecretpass
DES passphrase
```

Step 3 Run the **snmptrapd** command, pointing to that file.

Note This process runs in the foreground, uses only the specified configuration file, and logs messages to the stderr file.

```
[root@iLinux2 net-snmp]# snmptrapd -f -C -c /tmp/snmptrapd.conf -Le
```

Step 4 Run the **snmptrap** command from the ASA to send a linkdown or linkup trap by entering the following commands:

```
cicoasa (config)# int g3/1.391
cicoasa (config-if)# shut
cicoasa (config-if)# no shut
```

The following is sample output from the **snmptrap** command:

```
2009-03-18 23:52:06 NET-SNMP version 5.1.2 Started.
2009-03-18 23:52:20 10.31.8.254 [10.31.8.254]:
SNMPv2-MIB::sysUpTime.0 = Timeticks: (938700) 2:36:27.00 SNMPv2-MIB::snmp
TrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.1 = INTEGER: 1 IF-MIB::
ifAdminStatus.1 = INTEGER: down(2) IF-MIB::ifOperStatus.1 = INTEGER: down(2
)
2009-03-18 23:52:22 10.31.8.254 [10.31.8.254]:
SNMPv2-MIB::sysUpTime.0 = Timeticks: (939000) 2:36:30.00 SNMPv2-MIB::snmp
TrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.1 = INTEGER: 1 IF-MIB::ifAdminS
tatus.1 = INTEGER: up(1) IF-MIB::ifOperStatus.1 = INTEGER: up(1)
```

SilverCreek SNMP Test Suite

The SilverCreek SNMP test suite enables the detection of SNMP compliance problems and implementation errors in private and standard MIBs. You can download a free version of the software from the following URL: http://www.iwl.com/trial-downloads/silvercreek-trial.html?Itemid=

This section includes the following topics:

Running SilverCreek

To run the SilverCreek software, choose **Start** > **All Programs** > **SilverCreekMx Evaluation** > **Run Test Suite and Tools (Start Here)**.

When the application starts, along with the SilverCreek main window, a console window appears that shows the following information:

- Logging messages
- Debugging messages
- Other message exchanges that occur between the NMS and the SNMP Version 3 agent
- MIBs that are loaded

Figure 2: SilverCreek Main Window

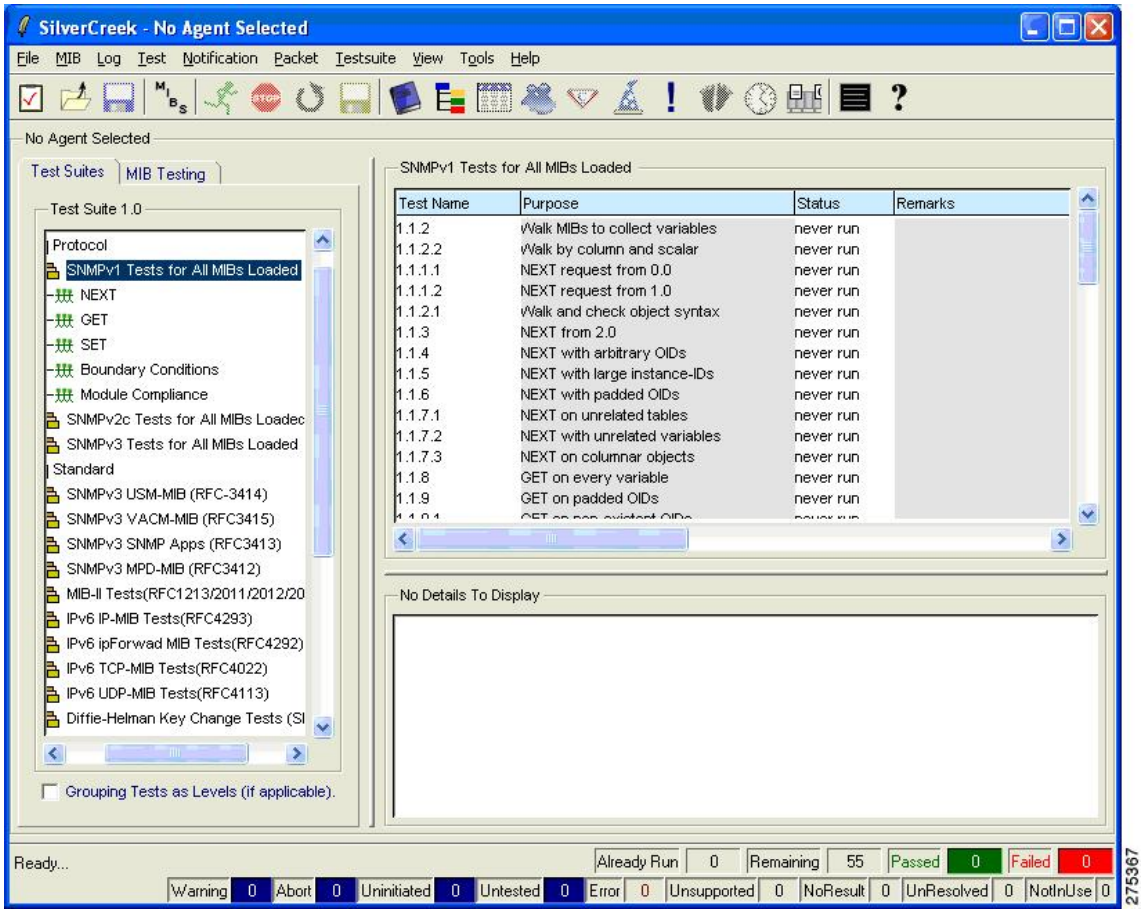


Figure 3: SilverCreek Console Window

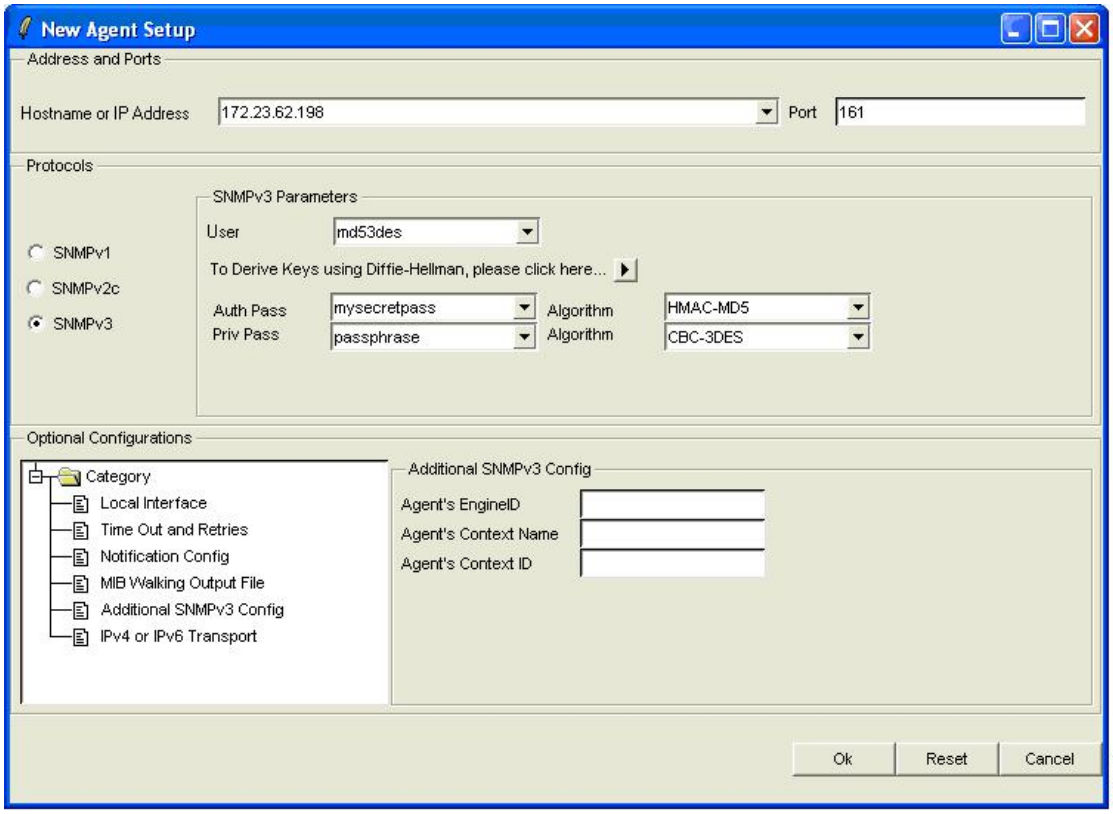
Setting up an SNMP Version 3 Agent

To set up the SNMP Version 3 agent, perform the following steps:

Step 1 Choose**File** > **New Agent Setup** .

The following figure shows how the new agent must be configured.

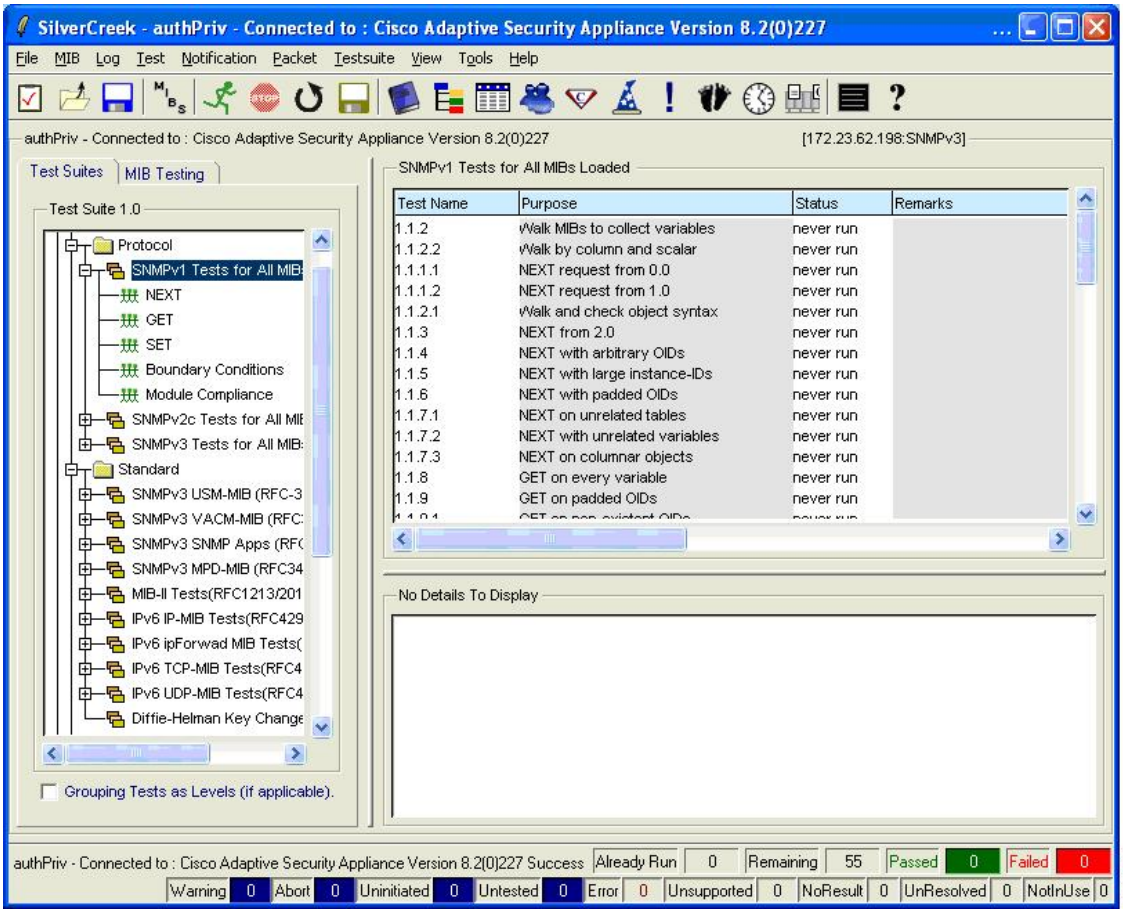
Figure 4: New Agent Setup Dialog Box



Step 2 Enter the hostname or the IP address, port number, and SNMP Version 3 parameters.

After the agent is connected, as shown in the following figure, you can run SNMP test suites from the Test Suites tab in the left pane.

Figure 5: SilverCreek Main Window Showing Connected SNMP Agent



Loading and Deleting MIBs

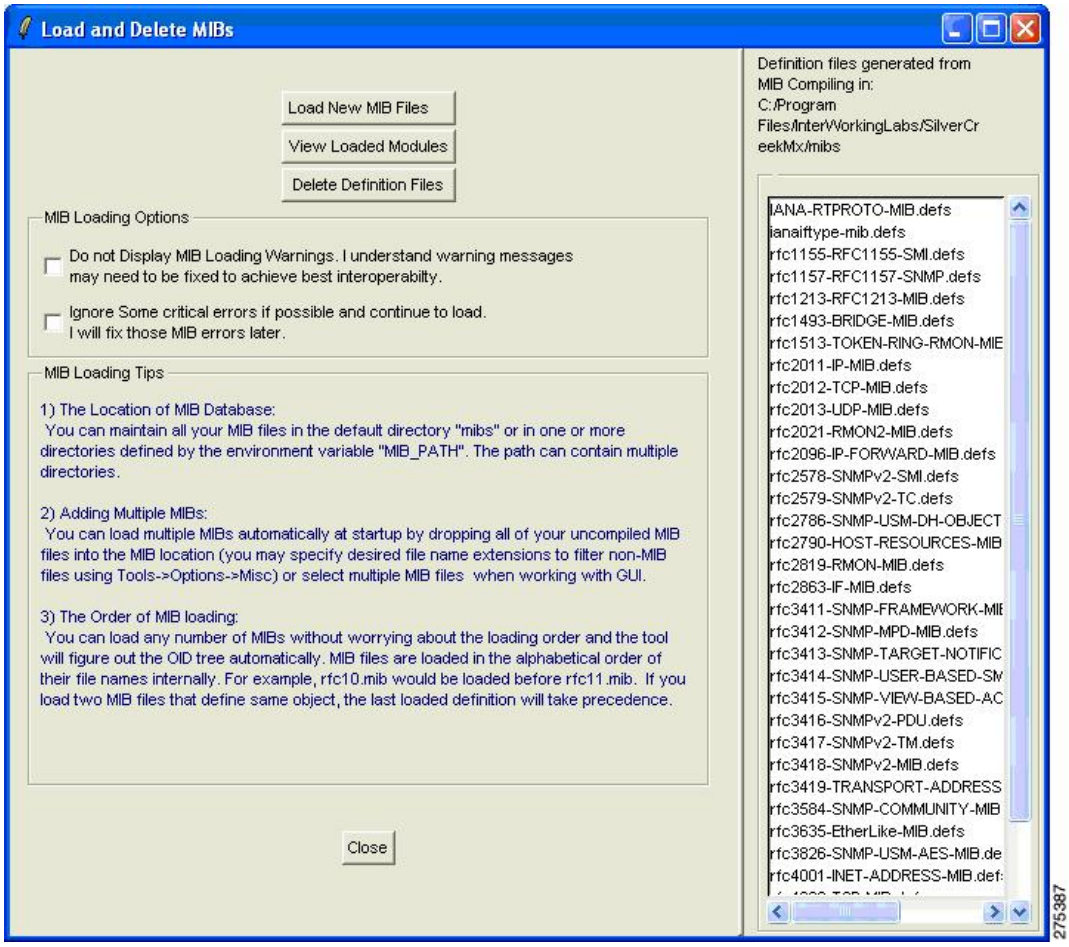
To load and delete MIBs, perform the following steps:

Step 1 To manually load and delete MIBs, choose **MIB** > **Load | Delete MIBs**.

Step 2 To view the loaded MIBs, click **View Loaded Modules**.

You can maintain all the MIB files in the default mibs directory, which is defined by the environment variable, MIB_PATH.

Figure 6: Load and Delete MIBs Dialog Box



Running a Test Suite

To run a test suite, perform the following steps:

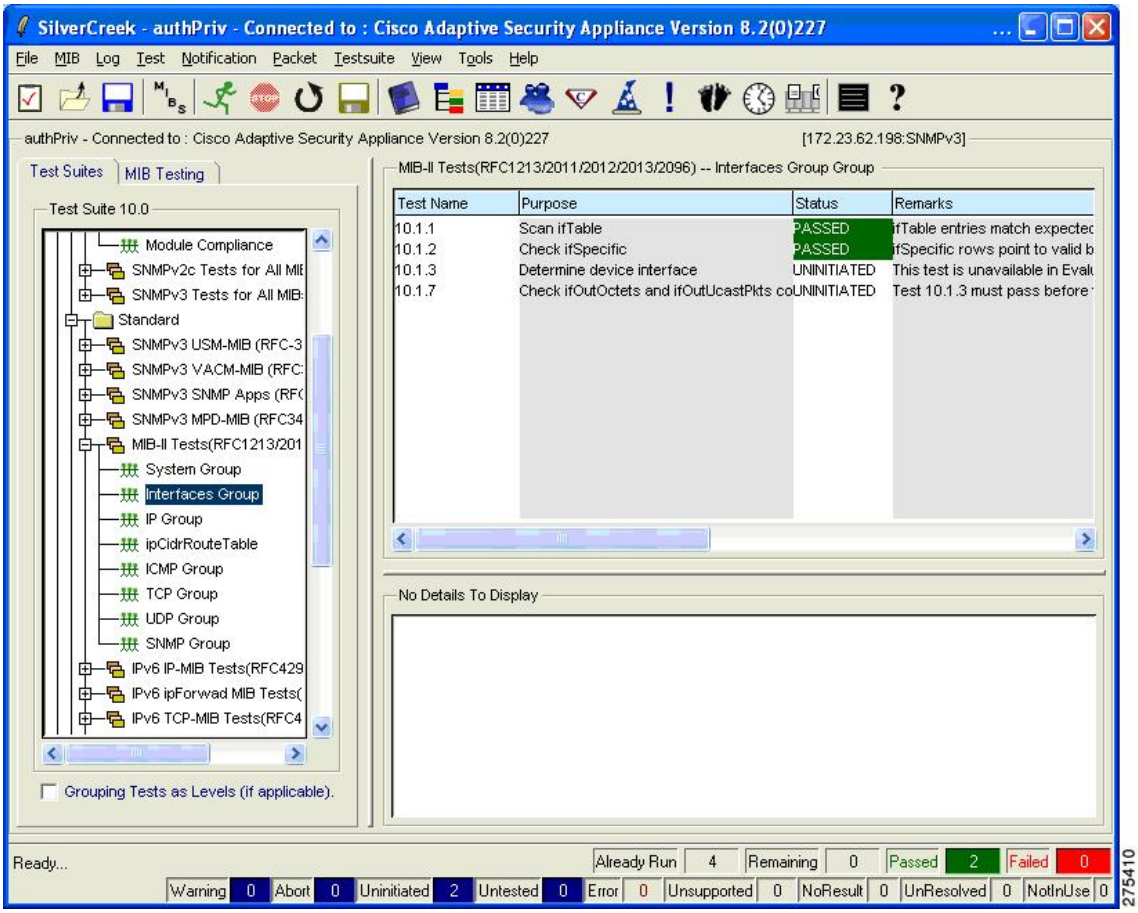
Step 1 In the main window, select a test category (for example, MIB-II tests) in the left pane (see figure below).

The list of available tests for the selected test category appears in the right pane, and test details appear in the bottom pane.

Step 2 Select a single test or multiple tests, and click **Run All or Selected Tests**.

The test status appears in the Status column. The total number of tests run, passed, failed, and so on appears at the bottom of the window.

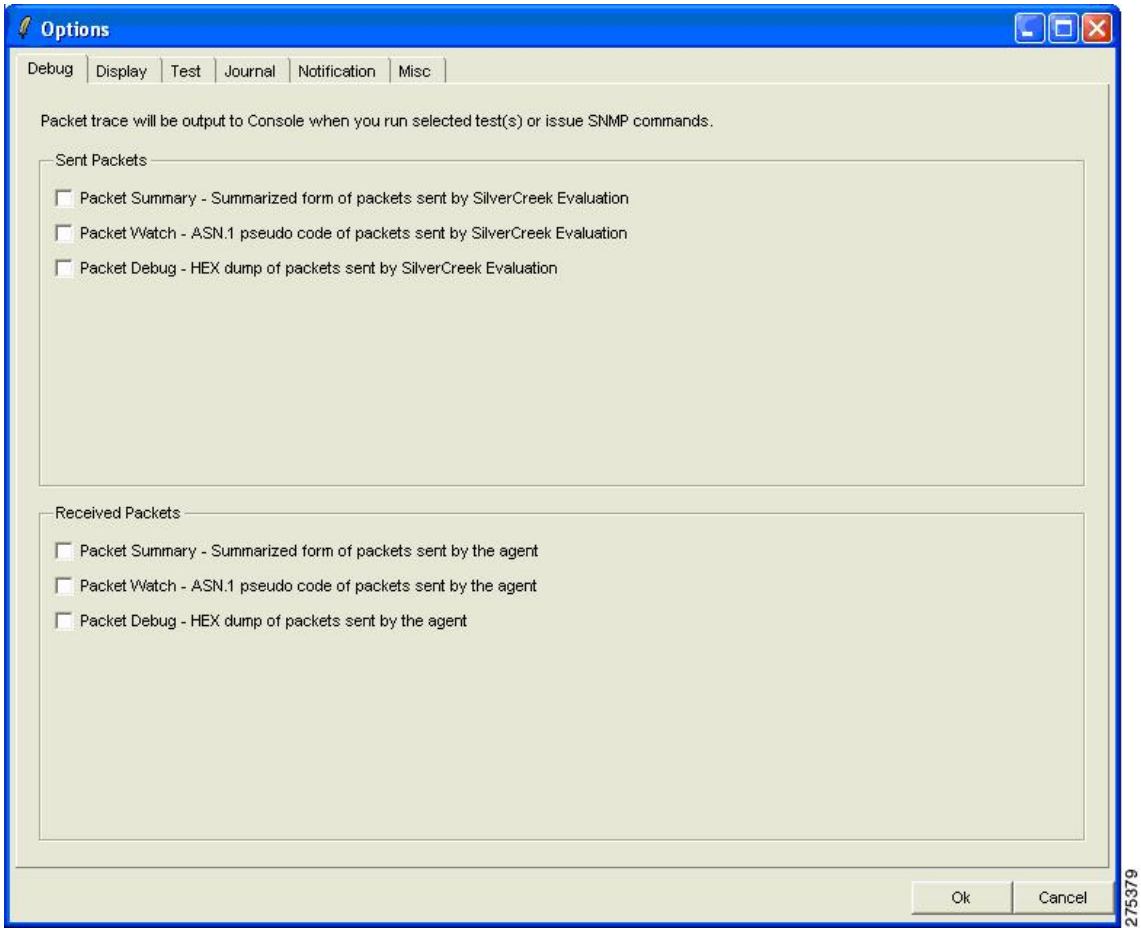
Figure 7: SilverCreek Main Window Showing Selected Tests



Enabling Debugging

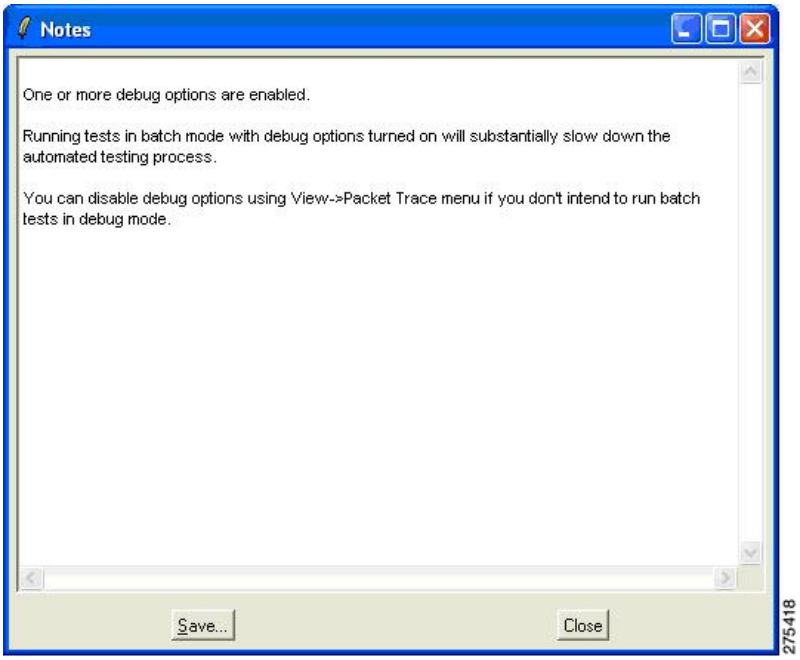
To enable debugging, choose **Tools** > **Options**.

Figure 8: Debug Tab of the Options Dialog Box



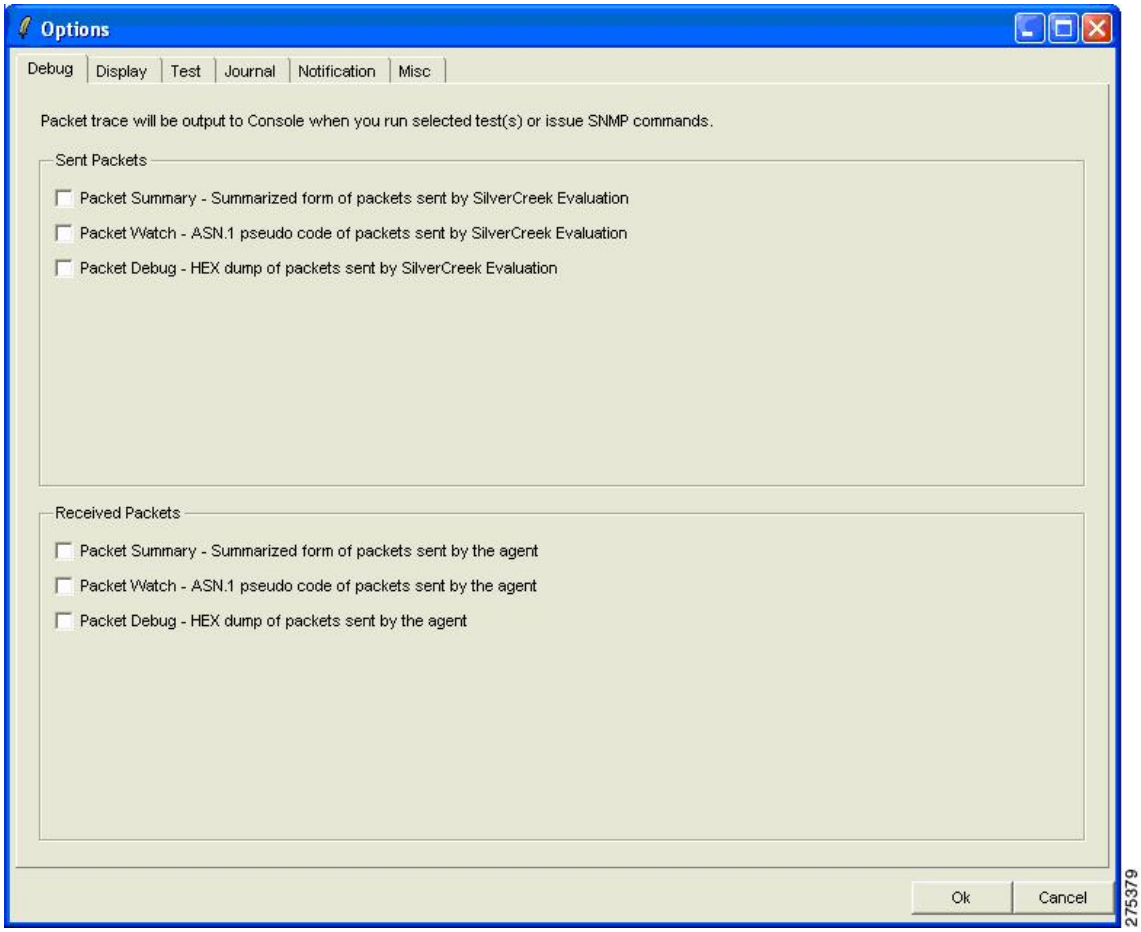
The following figure shows the warning message that appears to indicate that the test runs more slowly with debugging turned on.

Figure 9: Warning Notes Dialog Box



The following figure shows the console dialog box that lists the debugging messages, which appear when you run a test.

Figure 10: Console Dialog Box Listing Debugging Messages



Testing MIBs

To test MIBs, perform the following steps:

Step 1 In the left pane of the main window, click the **MIB Testing** tab.

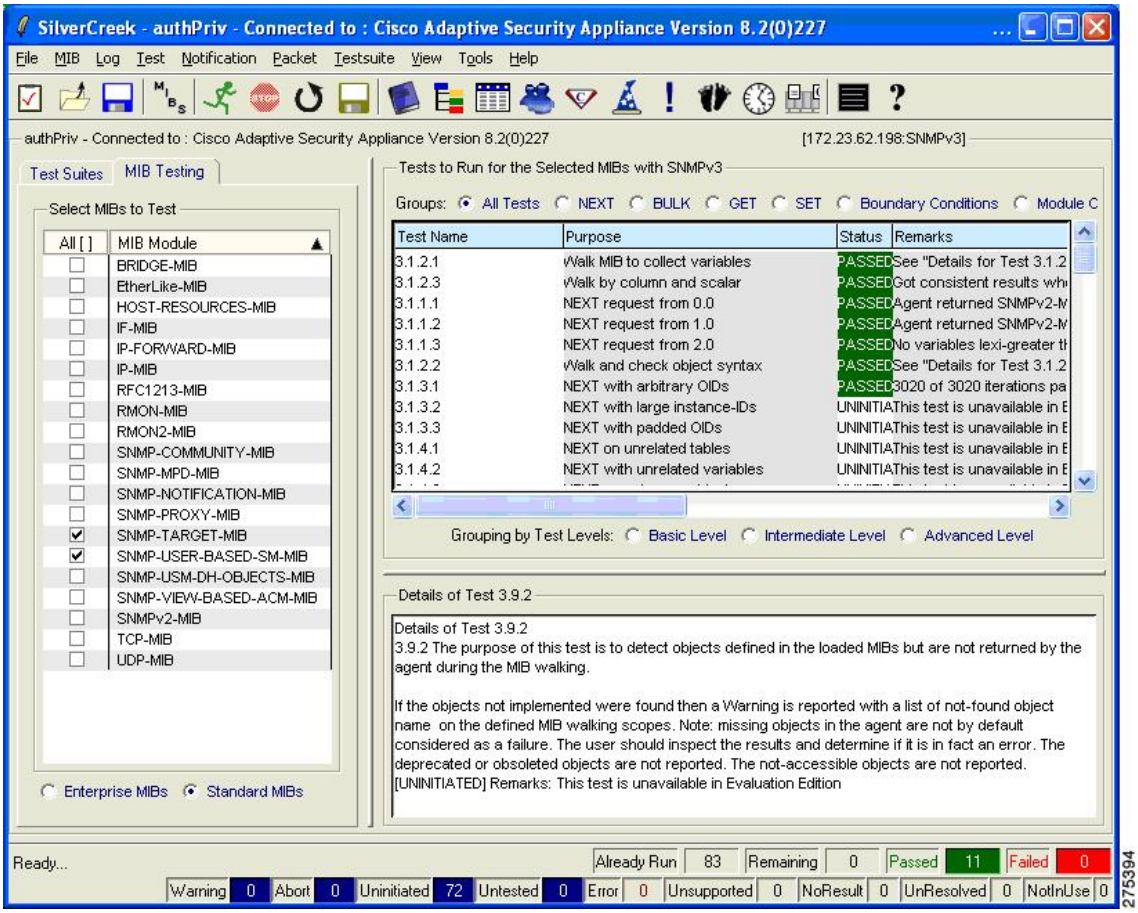
All the MIB modules that are loaded and available for testing appear.

Step 2 Click the radio buttons for the MIBs that need to be tested.

Step 3 In the right pane, select the tests that need to be run.

The purpose and details of the tests appear in the bottom pane.

Figure 11: SilverCreek Main Window Showing MIB Testing Details



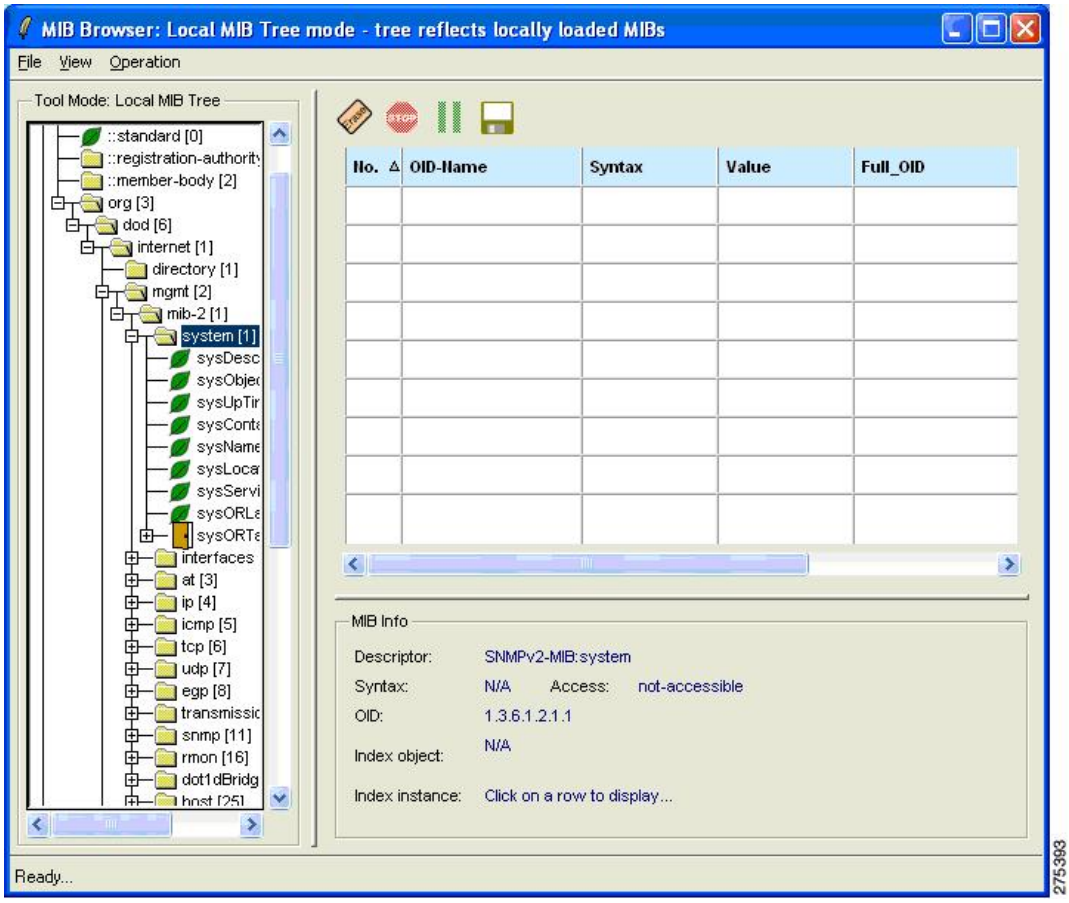
Accessing The MIB Browser

To access the MIB Browser, perform the following steps:

Step 1 In the main window, choose **MIB** > **MIB Browser**.

The MIB Browser provides more detailed access to the agent MIBs, including the ability to poll an individual MIB, walk a selected tree, and so on.

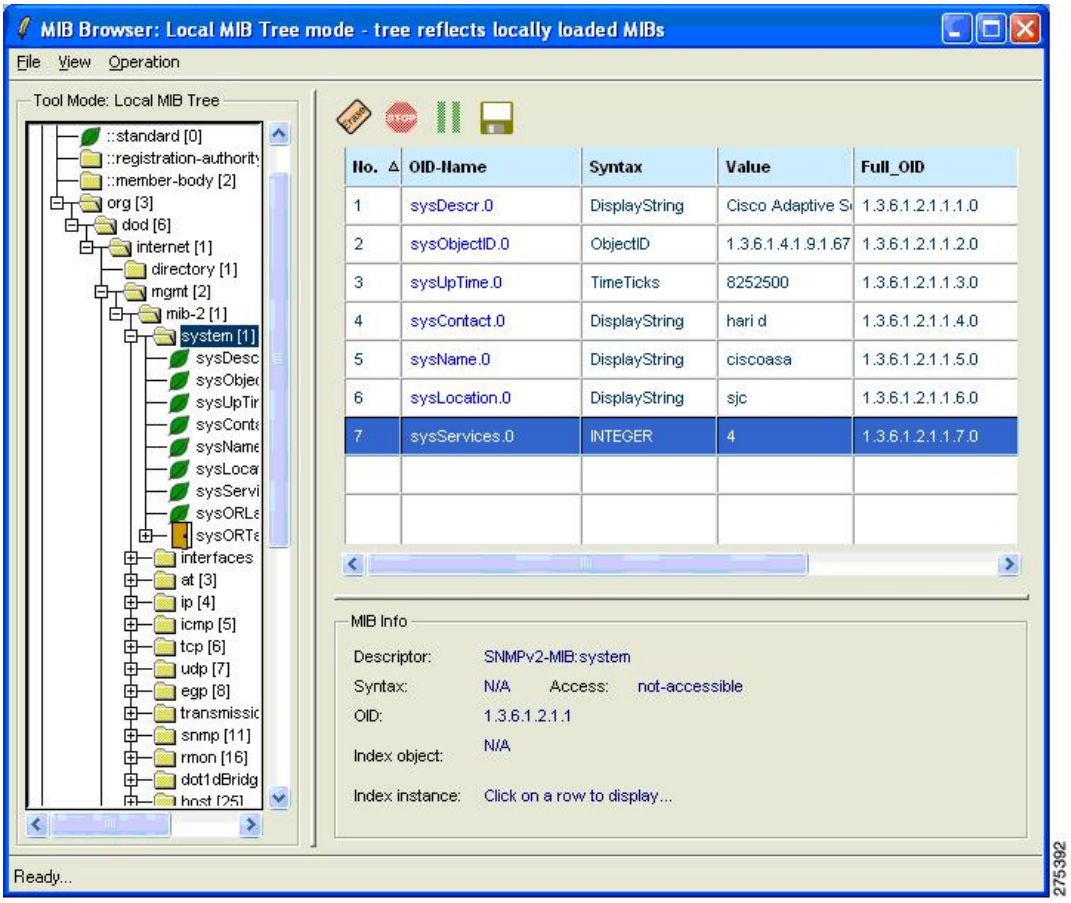
Figure 12: MIB Browser: Local MIB Tree Mode Dialog Box



Step 2 Scroll down to the OID, .iso.org.dod.internet.mgmt.mib-2.system and right-click system; then choose the option to walk this tree.

The MIB browsing results appear in the right pane, as shown in the following figure.

Figure 13: MIB Browser: Local MIB Tree Mode Dialog Box Showing MIB Results



Note See the *Release Notes for the Cisco ASA 5500 Series* for a list of the open caveats that apply to SNMP MIBs.

Receiving Notification Trap Messages

To receive notification trap messages, perform the following steps:

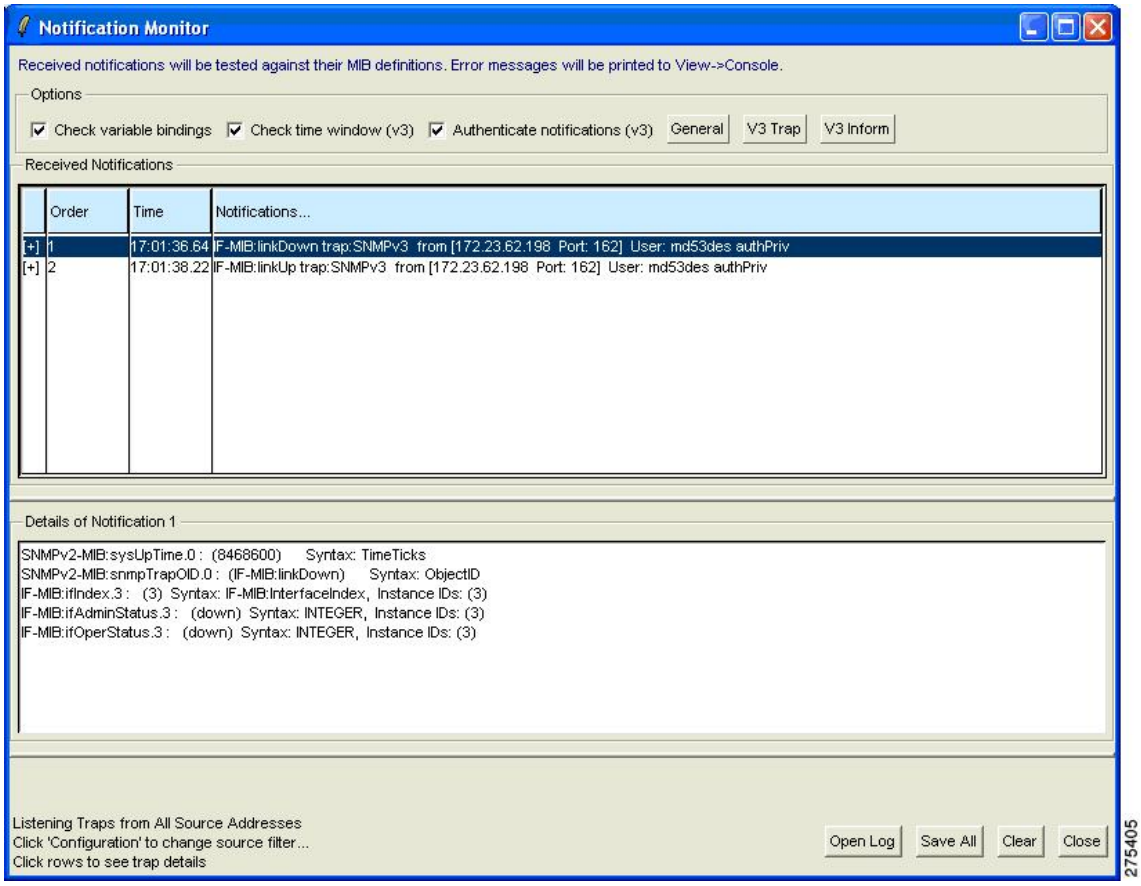
Step 1 In the main window, choose **Notifications** > **Notifications Monitor**.

Step 2 To configure the agent-specific information, click **V3 Inform**.

The Received Notifications dialog box shows the trap messages that are received, along with the notification details displayed at the bottom.

Note SNMP Version 3 does not send authentication failure traps; an SNMP Version 3 agent sends a PDU report instead.

Figure 14: Notification Monitor Dialog Box



Testing Performance

To test performance, perform the following steps:

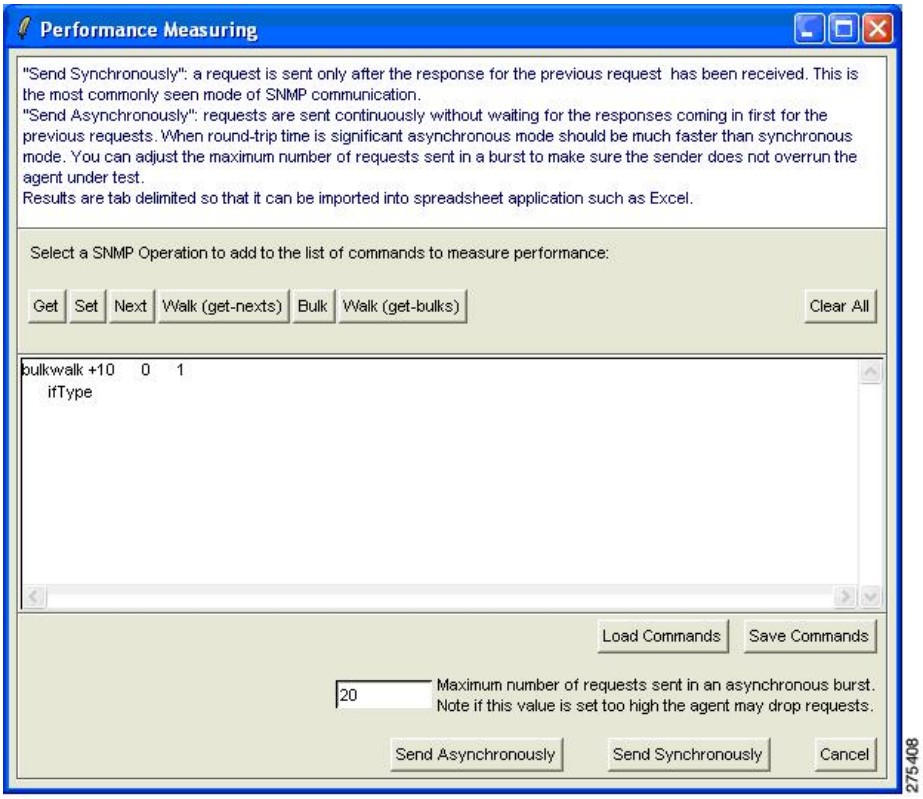
Step 1 Choose **Tools** > **Performance Monitoring Tool**, select an operation that you want to perform (for example, Walk (get-bulks), and provide an Object name. You can run various commands multiple times.

Step 2 Click **Send Synchronously**.

The selected SNMP operations start. Results appear in a separate window.

The following example uses ifType, asks how many times you want to repeat the operation, and uses the value, 10.

Figure 15: Performance Measuring Dialog Box



IPswitch WhatsUp Gold

Ipswitch WhatsUp Gold is network management software that enables network discovery, and SNMP monitoring and polling. You can download a free version of the software at the following URL: http://www.whatsupgold.com/products/download/

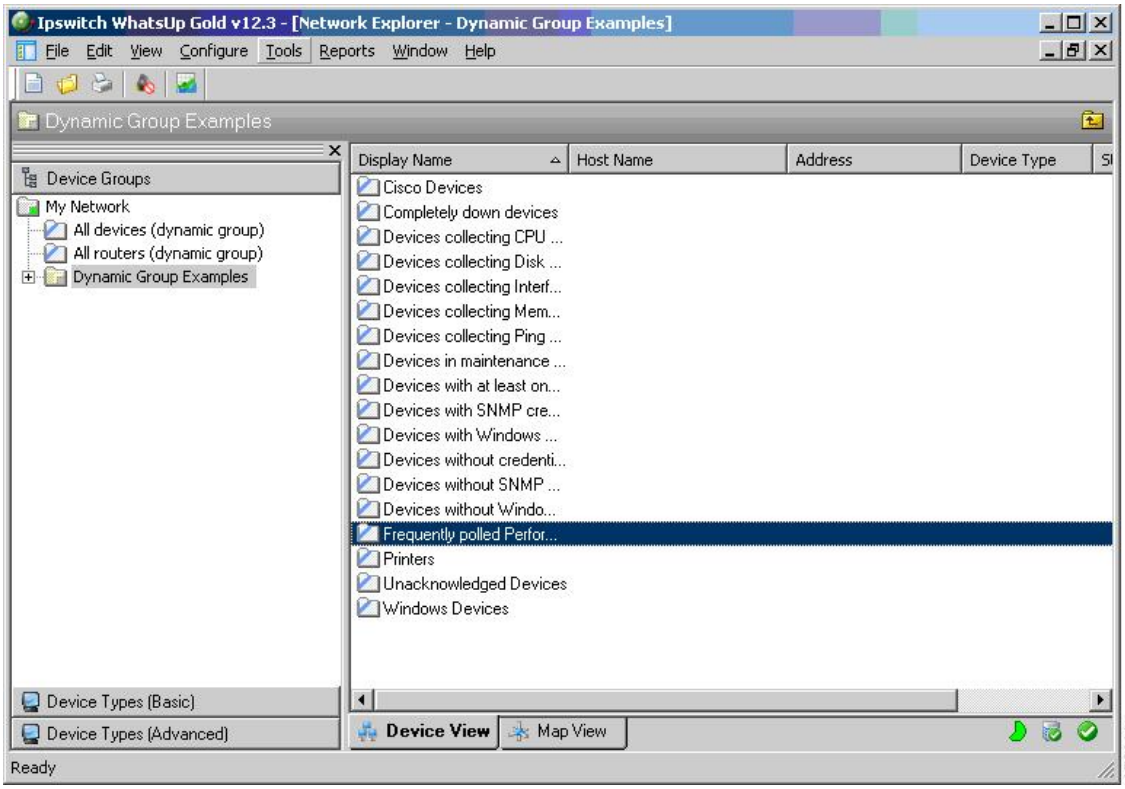
This section includes the following topics:

Starting IPswitch WhatsUp Gold

To start the Ipswitch WhatsUp Gold application, choose **Start** > **Programs** > **Ipswitch WhatsUp Gold 12.3** > **WhatsUp Gold**.

The main network explorer window appears.

Figure 16: Network Explorer Main Window



Adding a new SNMP Agent

To add a new SNMP agent, perform the following steps:

Step 1 Choose **File** > **New** > **New Device**.

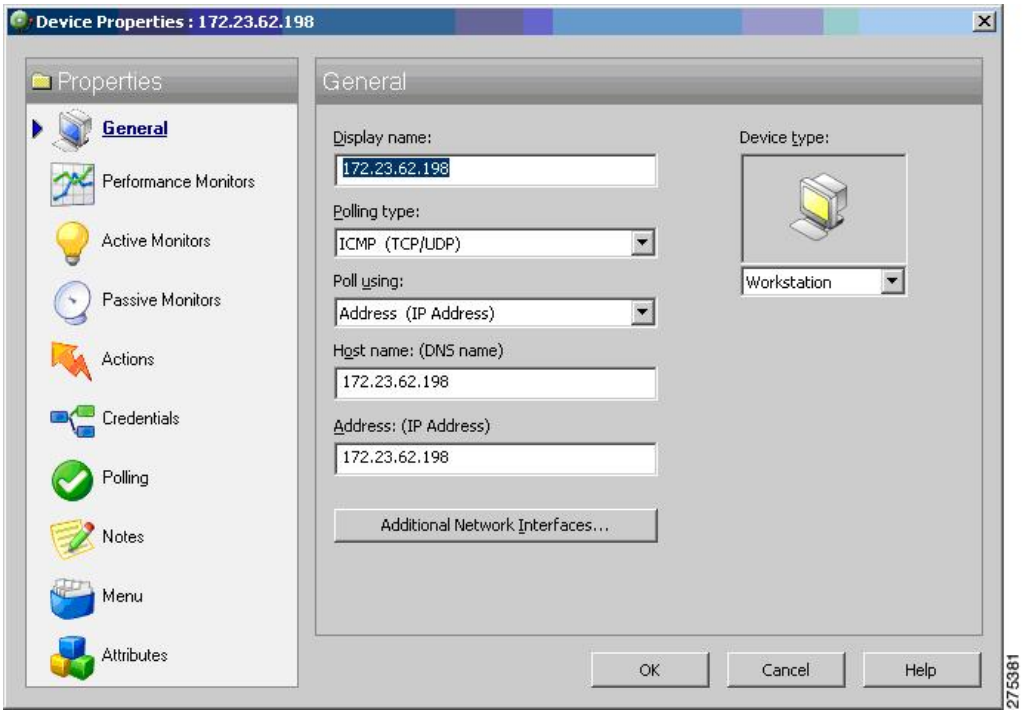
The Add New Device dialog box appears.

Figure 17: Add New Device Dialog Box

Step 2 Enter the IP address or hostname.

Step 3 After the device has been added, enter device properties in the General pane, as shown in the following figure.

Figure 18: Device Properties Dialog Box

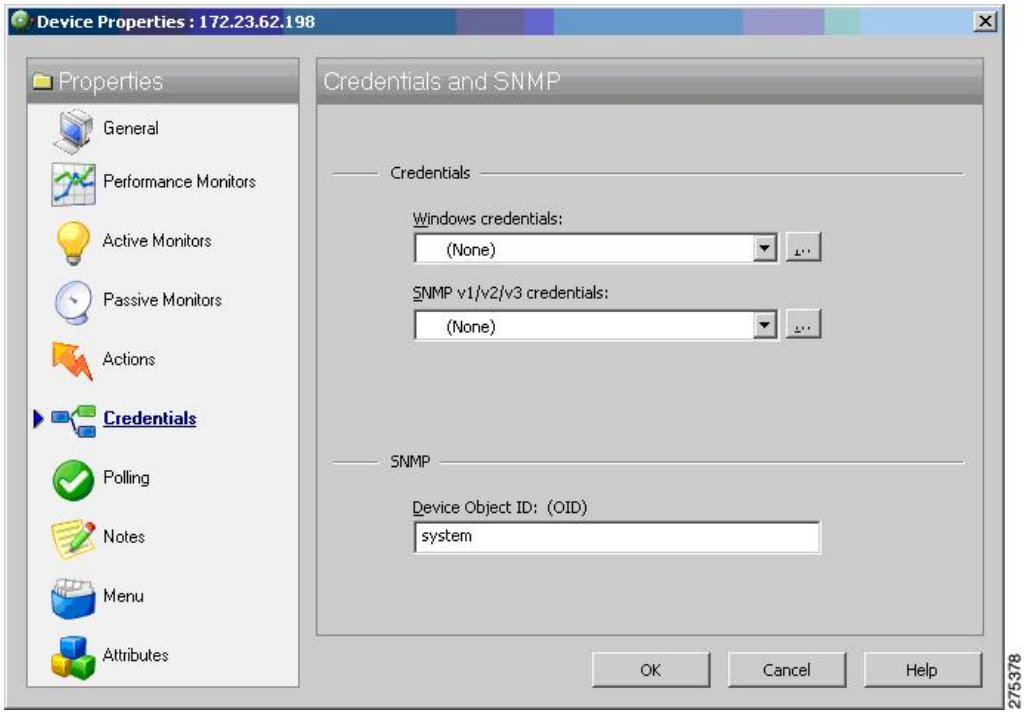


Adding SNMP Version 3 Credentials

To add SNMP Version 3 credentials, perform the following steps:

Step 1 Click the **Credentials** link, and enter the SNMP device object ID information.

Figure 19: Device Properties Dialog Box Showing SNMP Credentials



Step 2 Click the button next to the SNMP v1/v2/v3 credentials drop-down list and enter the username, authentication and encryption algorithms, and corresponding passwords, then click **OK**.

Figure 20: Edit SNMP v3 Credential Type Dialog Box

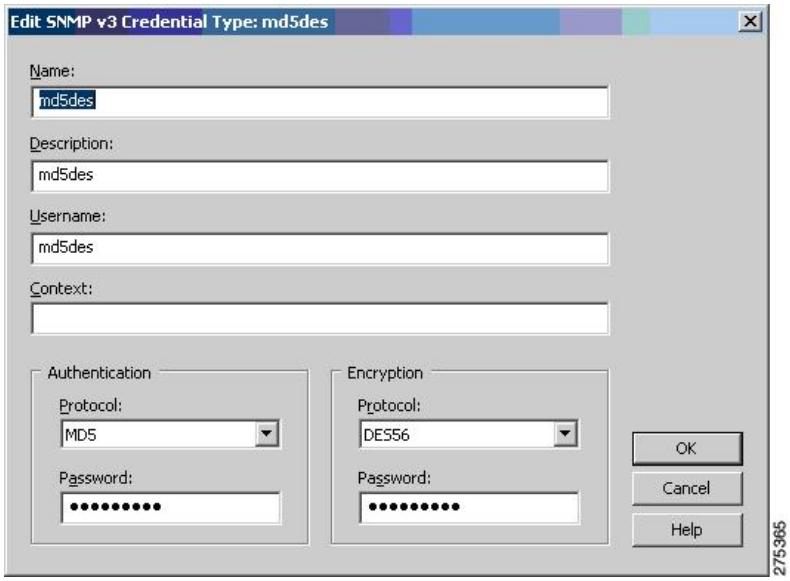
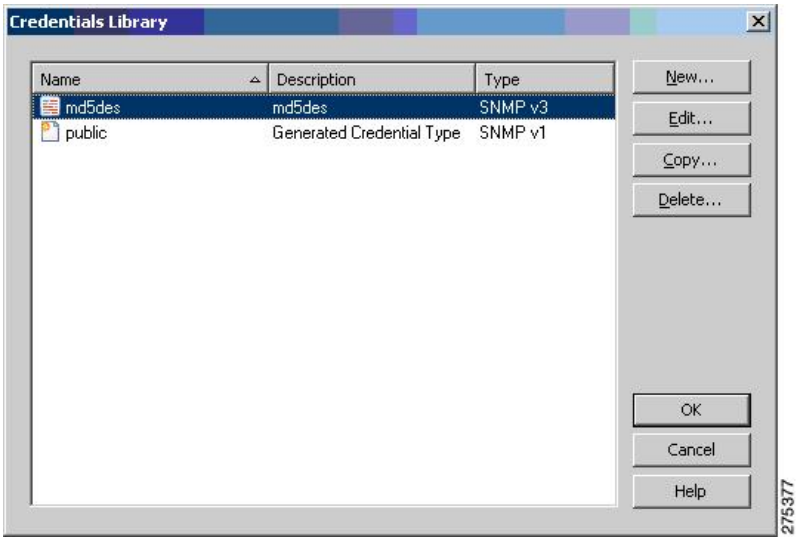
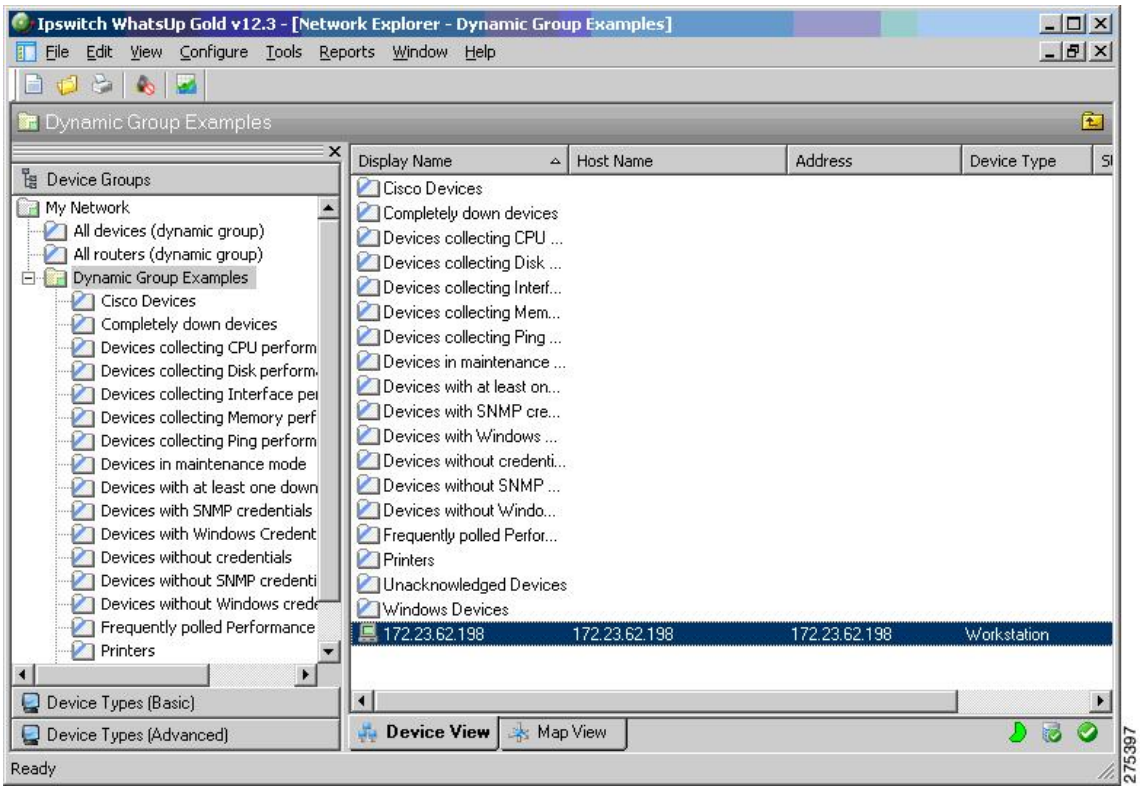


Figure 21: Credentials Library Dialog Box



The following figure shows the added SNMP Version 3 node on the network.

Figure 22: Network Explorer Window with Added SNMP Version 3 Node



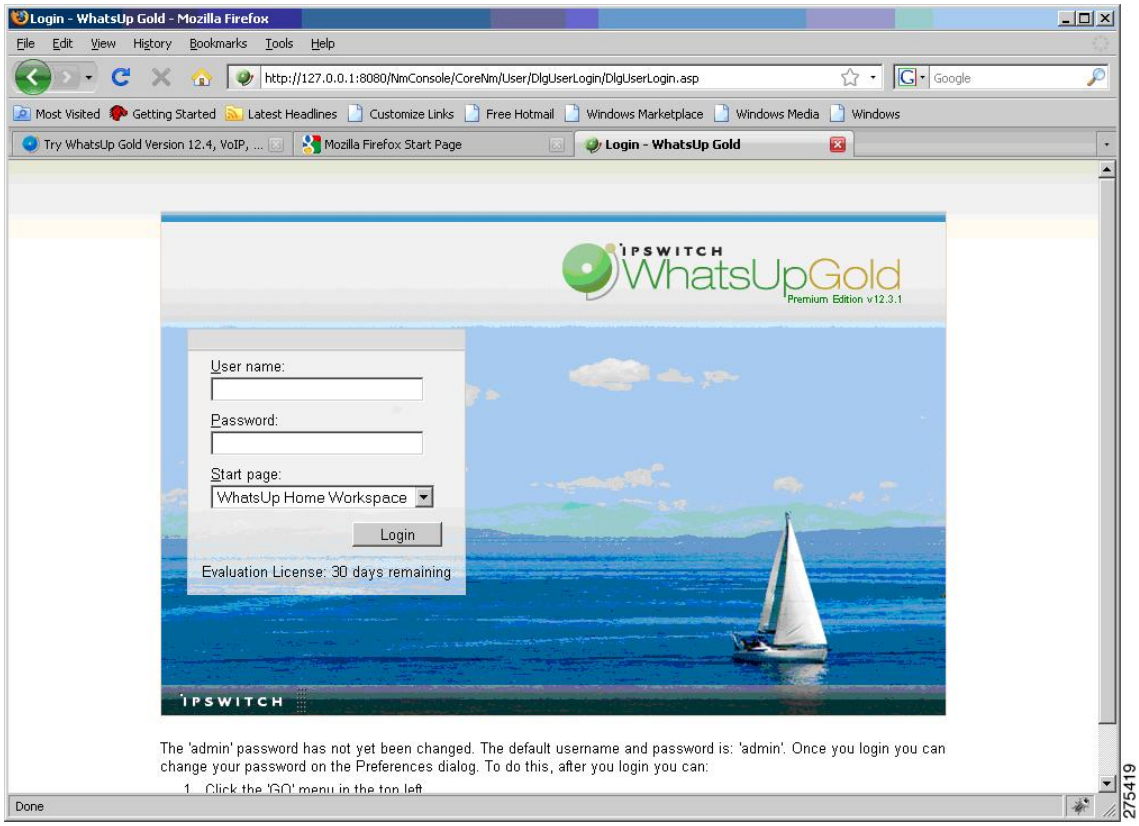
Using the WhatsUp Gold Web Interface

To start the WhatsUp Gold application, perform the following steps:

Step 1 Choose **Start** > **Programs** > **IpSwitch WhatsUp Gold v12.3** > **WhatsUp Web Interface**. You can perform SNMP Version 3 walks and polls from this location.

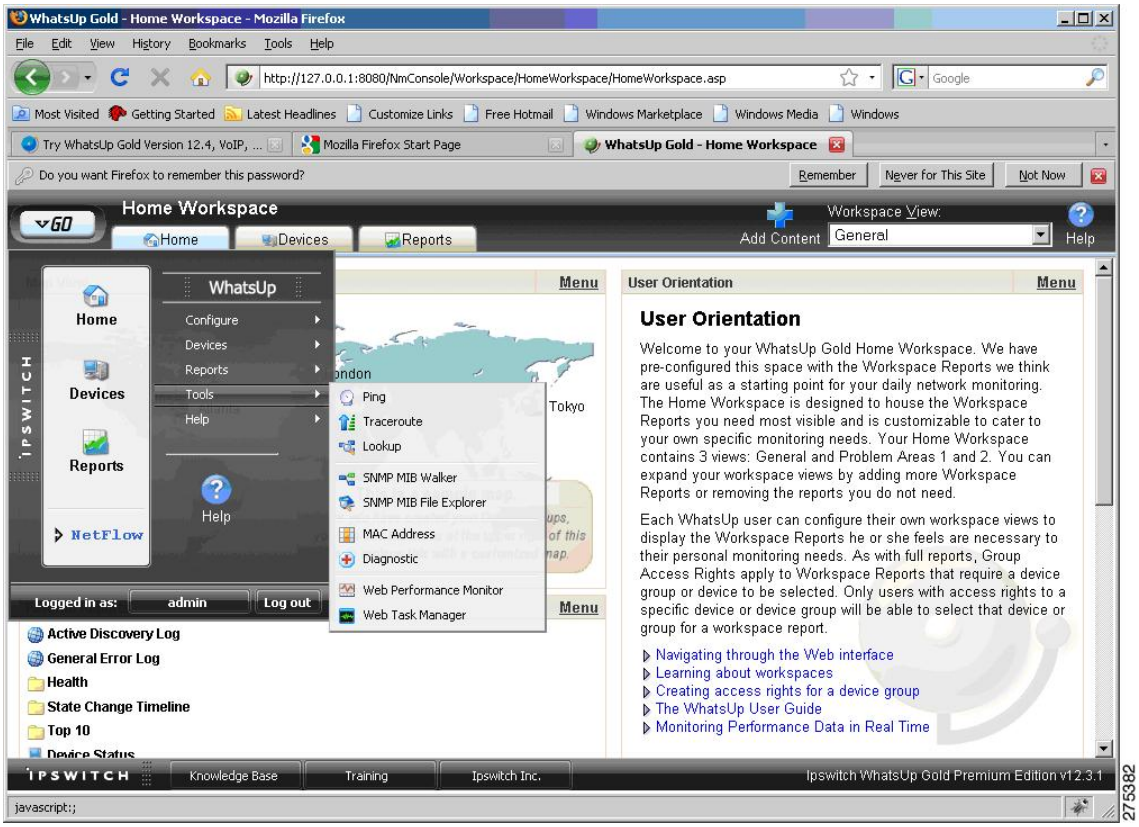
Step 2 The following figure shows the initial login window. Enter the default username and password, which is “admin.”

Figure 23: WhatsUp Gold Login Window for Web Interface



The following figure shows the Home Workspace pane that appears after the user logs in.

Figure 24: WhatsUp Gold Home Workspace Pane

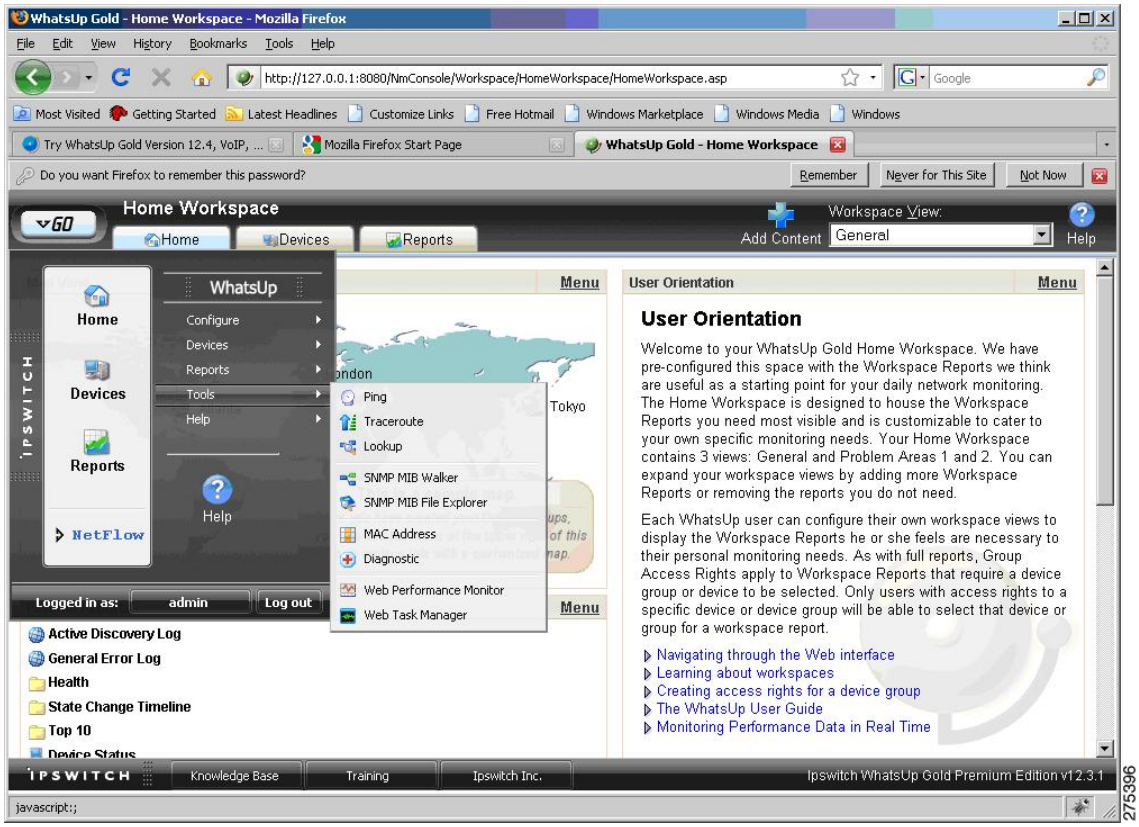


Walking an SNMP MIB or an OID

To walk a MIB or an OID, perform the following steps:

Step 1 Choose **GO** > **Tools** > **SNMP MIB Walker**.

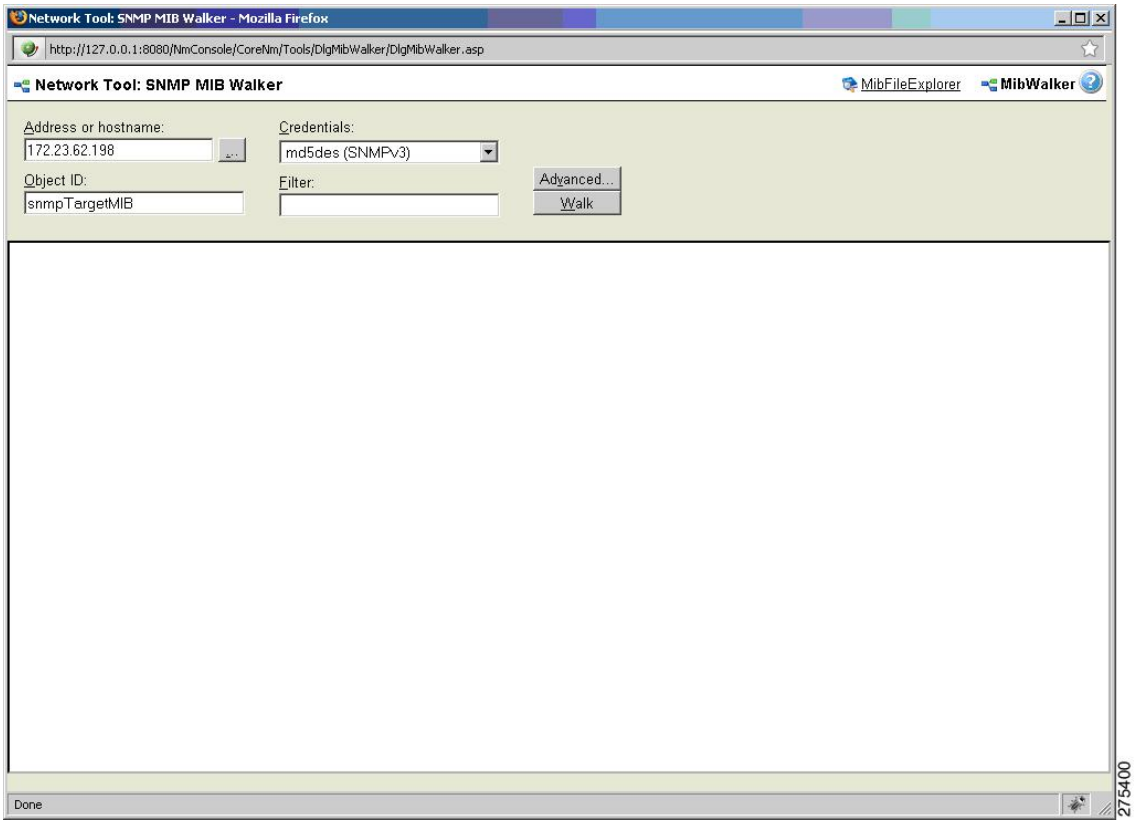
Figure 25: SNMP MIB Walker Menu Option



Step 2 In the Network Tool: SNMP MIB Walker dialog box, enter the following information:

- The agent IP address or hostname
- The OID or MIB that needs to be walked
- The SNMP Version 3 credentials

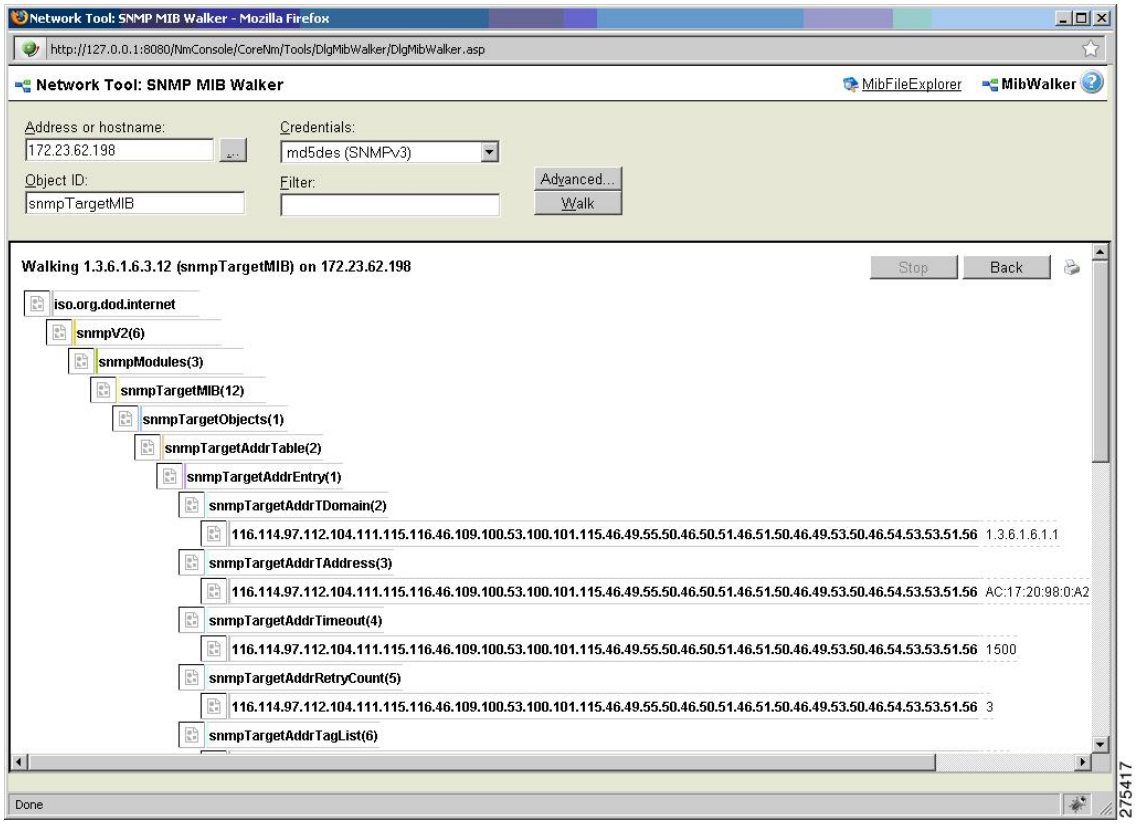
Figure 26: Network Tool: SNMP MIB Walker Dialog Box



Step 3 Click **Walk**.

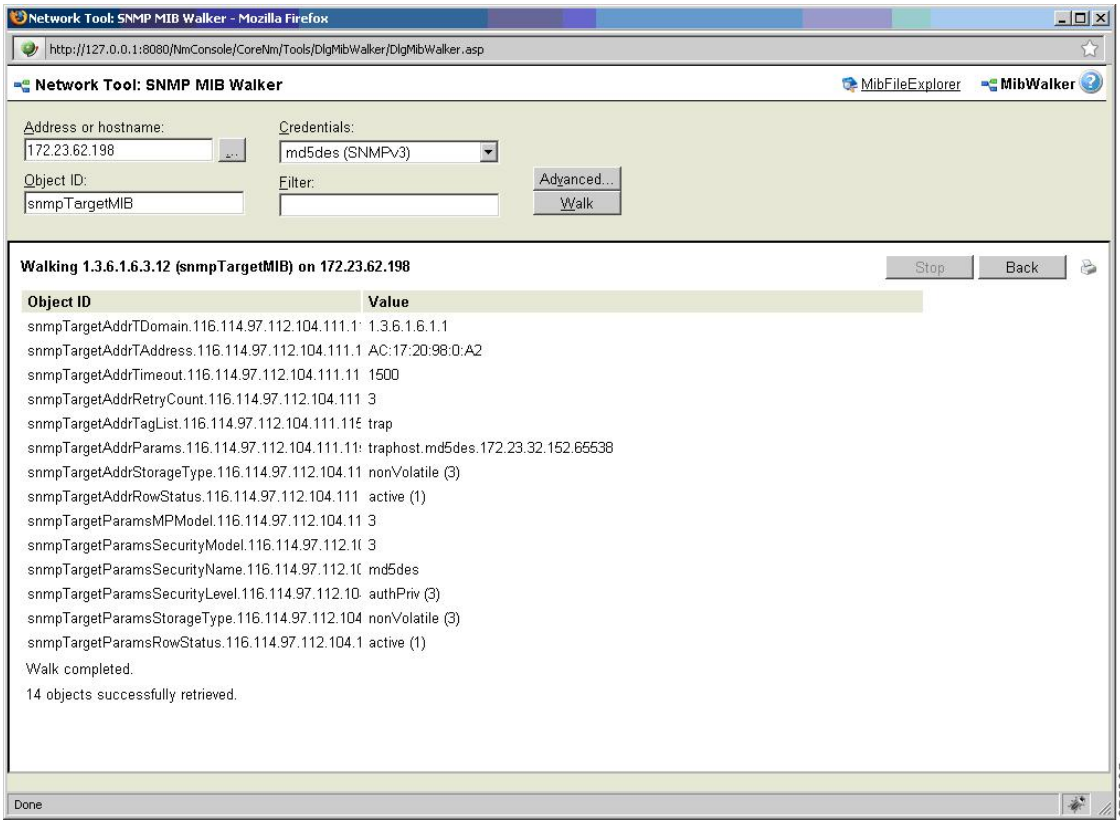
The following figure shows the walk results in a tree format.

Figure 27: Network Tool: SNMP MIB Walker Results - Tree View



The following figure shows the results in sequence.

Figure 28: Network Tool: SNMP MIB Walker Results Window

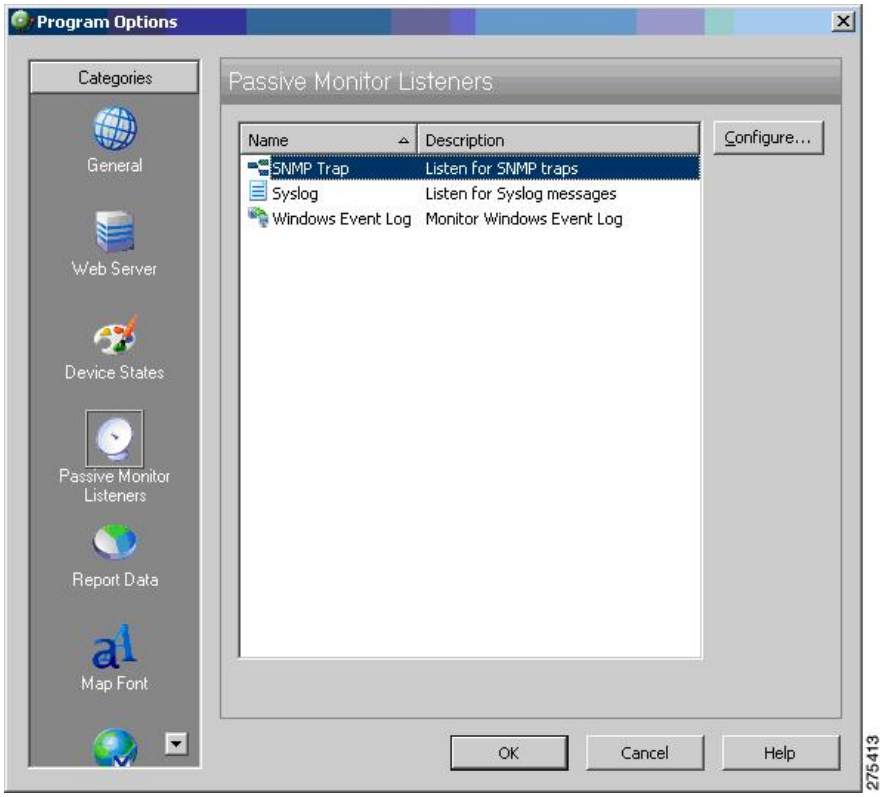


Configuring SNMP Traps

To configure SNMP traps, perform the following steps:

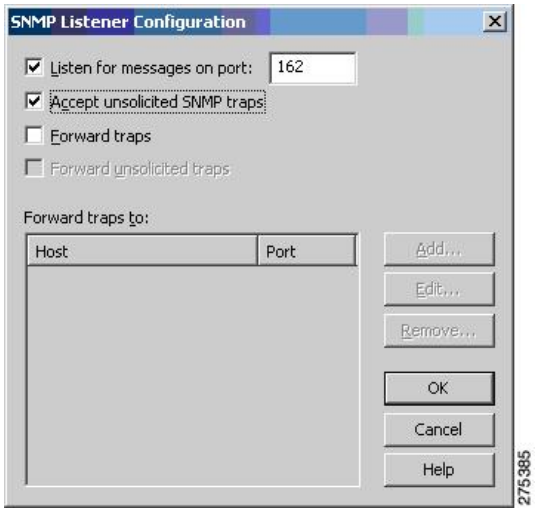
Step 1 Choose **Program Options** > **Passive Monitor Listeners** > **SNMP Trap** > **Configure**.

Figure 29: Program Options – Passive Monitor Listeners Dialog Box



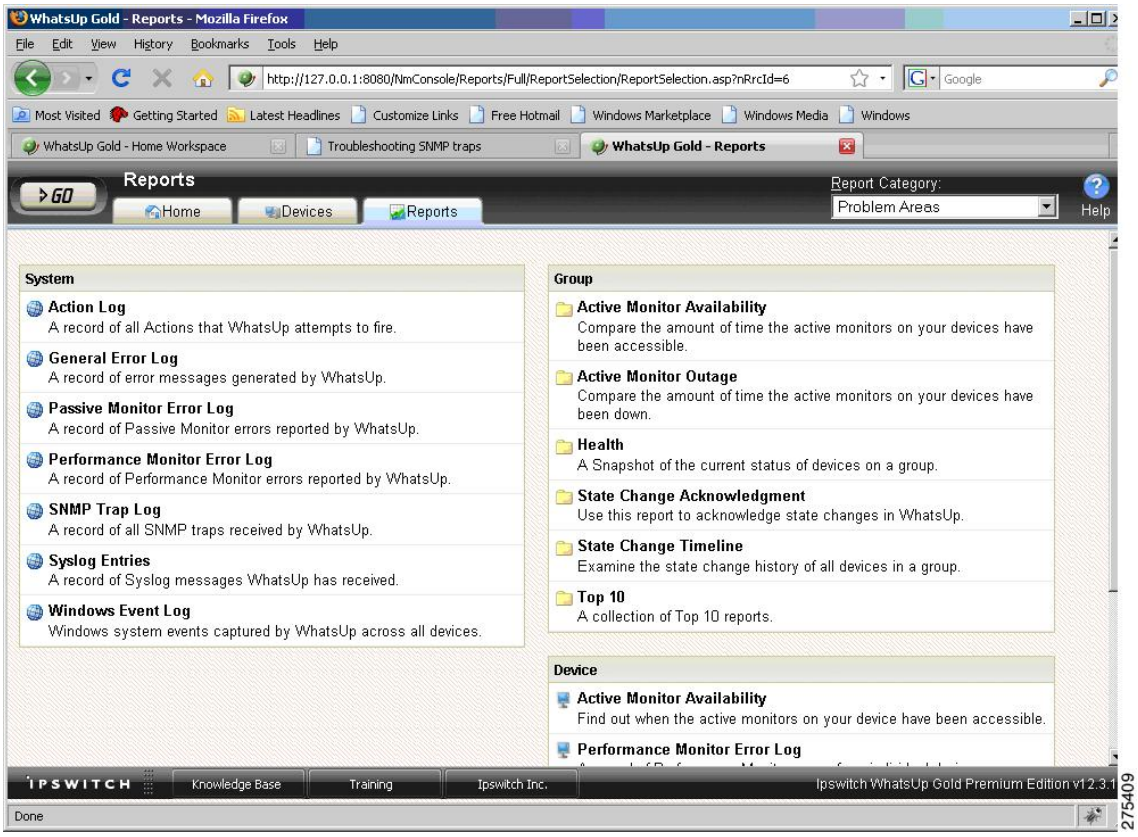
The SNMP Listener Configuration dialog box appears. From here you can configure the listener port and forward traps to a host.

Figure 30: SNMP Listener Configuration Dialog Box



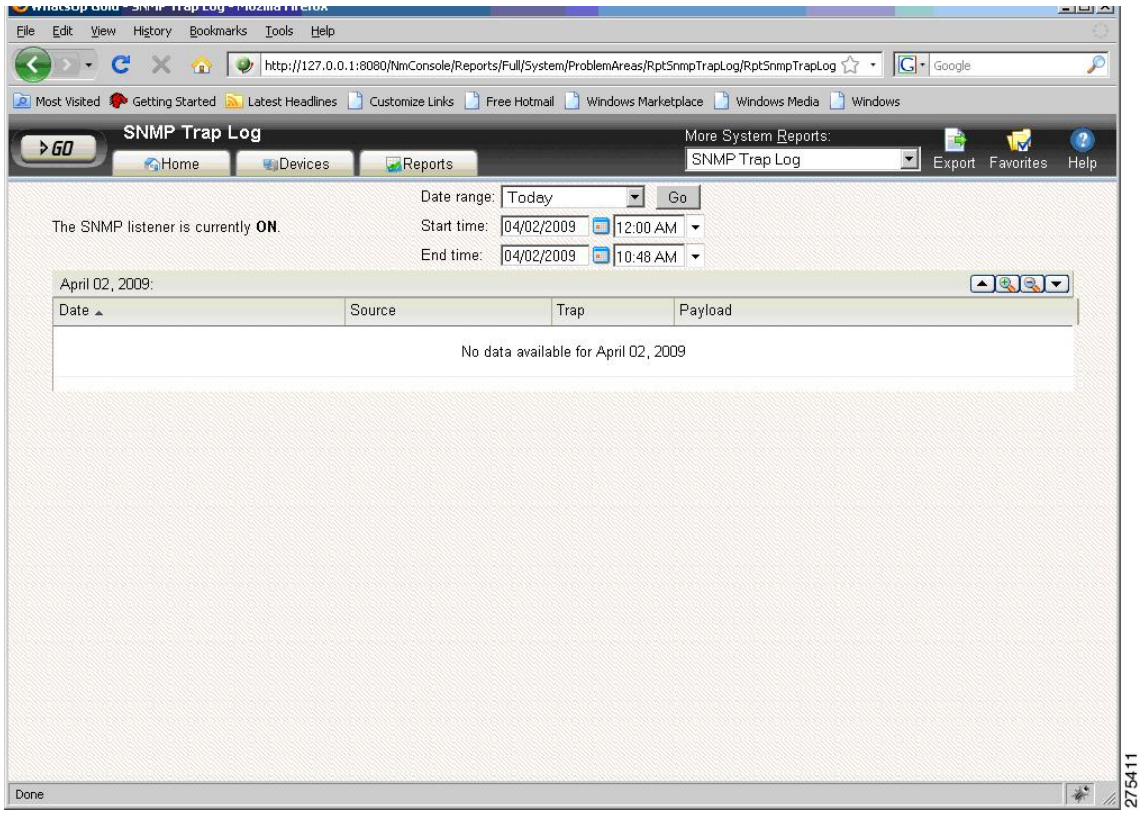
Step 2 Click the **Reports** tab and select **SNMP Trap Log**.

Figure 31: SNMP Reports Pane



The following figure shows the SNMP trap log.

Figure 32: SNMP Trap Log Pane



HP OpenView Network Node Manager

HP OpenView Network Node Manager (NNM) 7.53 is a management tool that is used to automatically create network topologies, manage devices, and monitor device health. The ASA is integrated into the HP NNM device topology, and communicates device statistics and SNMP traps using SNMP Version 3.

Note See the *Release Notes for the Cisco ASA 5500 Series* for a list of the open caveats that apply to NNM 8.x.

This section includes the following topics:

Installing NNM

NNM 7.53 was tested on the Windows 2003 Server platform. A trial version with the required installation instructions is available at the following URL:

https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119%5E1155_4000_100__

Starting the NNM

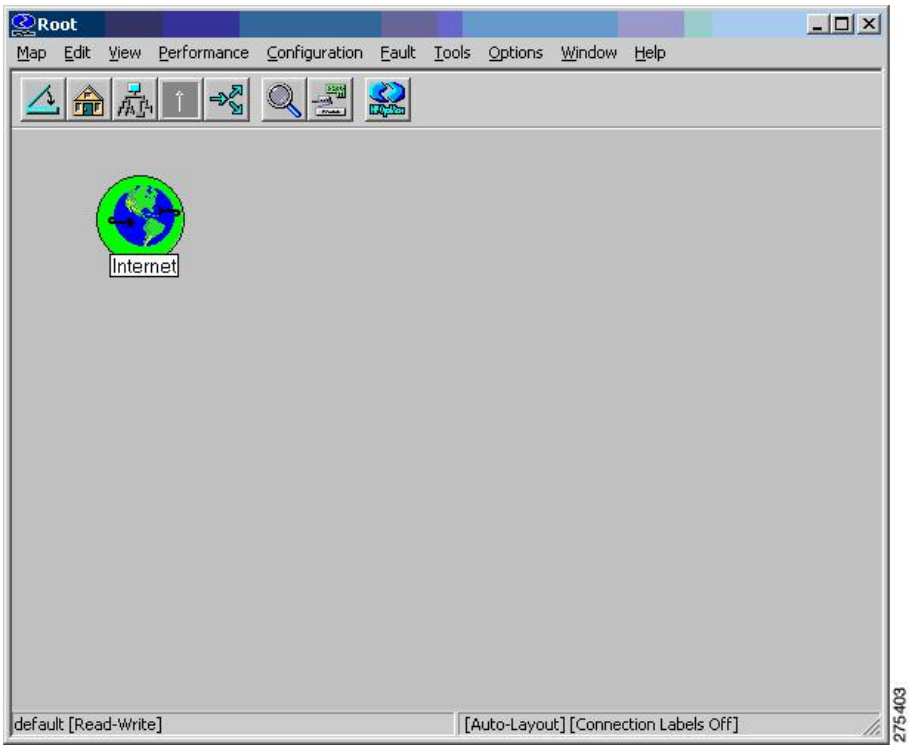
To start the NNM, perform the following steps:

Step 1 From the command prompt of the NNM server, choose one of the following:

- **Start** > **Programs** > **HP OpenView** > **Network Node Manager Admin** > **Network Node Manager**.
- Double-click the **ovw.exe** file, located in C:\Program Files\HP OpenView\bin.

The Root window appears, with the Internet map icon displayed.

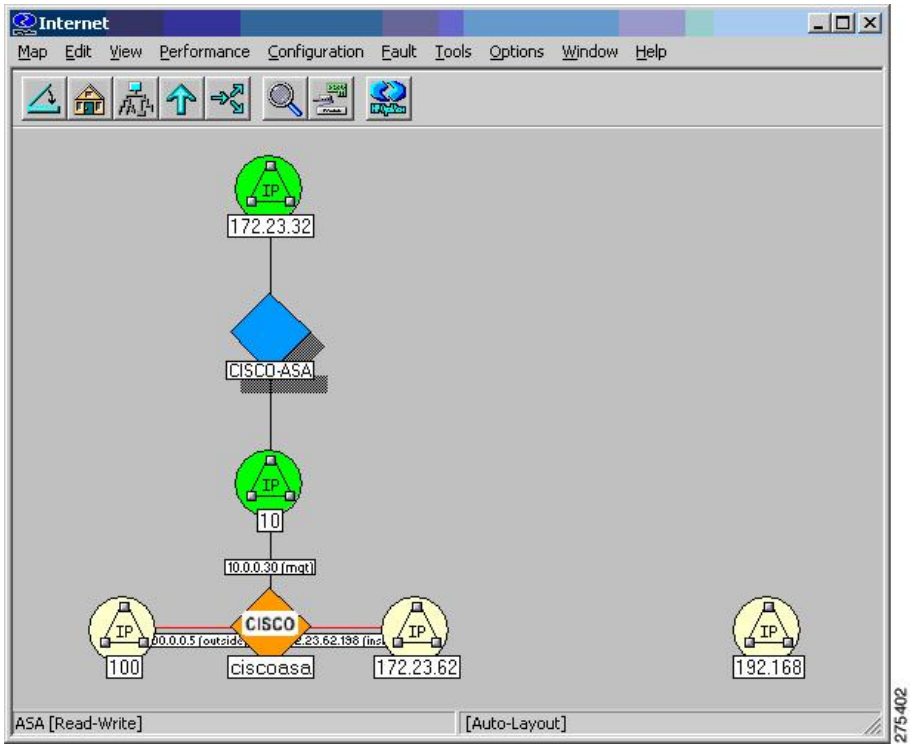
Figure 33: NNM Console Root Window



Step 2 Double-click the **Internet map** icon.

The Internet window appears, with the network nodes displayed.

Figure 34: NNM Console Internet Window Showing Network Nodes



Loading MIBs

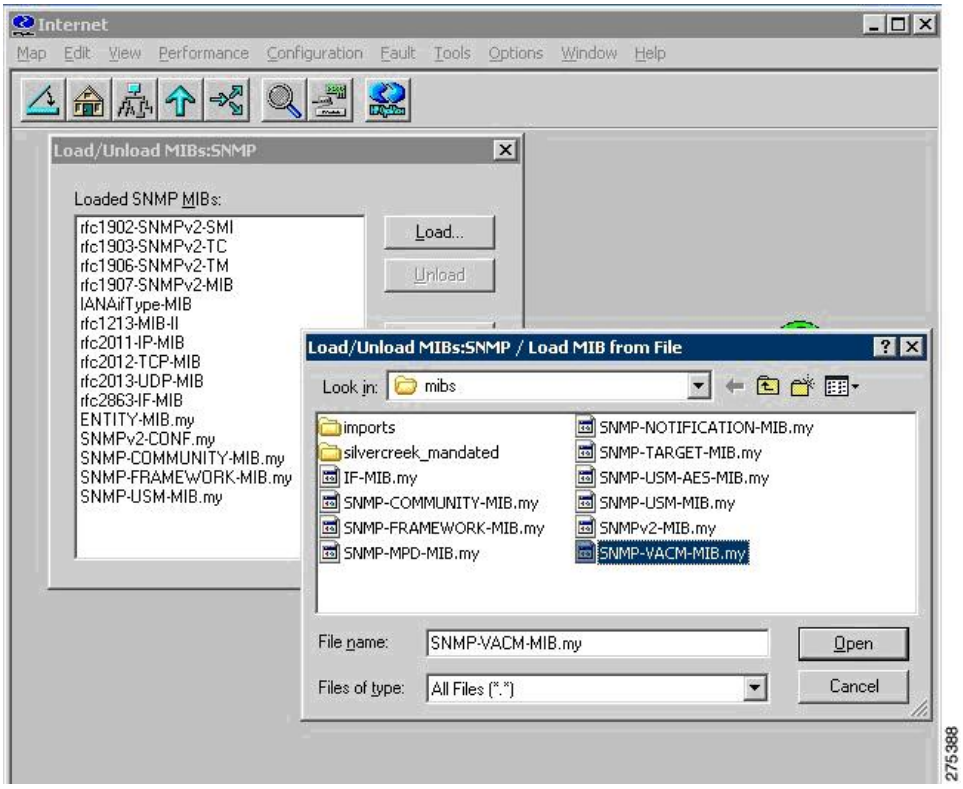
To load MIBs, perform the following steps:

Step 1 In the NNM main window, choose **Options** > **Load/Unload MIBs:SNMP**.

A list of currently loaded MIBs appears.

Step 2 Click **Load** to select additional MIBs from the server file system.

Figure 35: Load/Unload MIBs: SNMP Dialog Box



Adding a Network to the Current Map

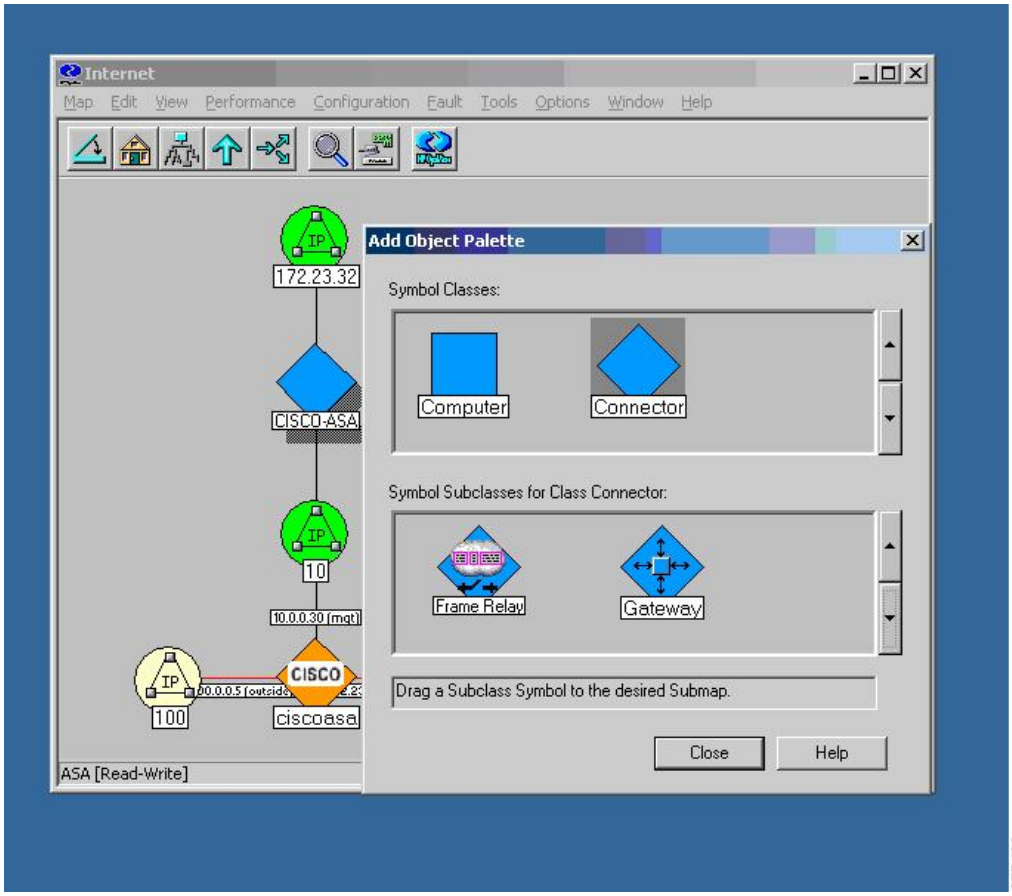
To add a network to the current map, perform the following steps:

Step 1 Find the IP address and hostname of at least one high-traffic device within the network that you want to add

Step 2 In the Internet-level submap, choose **Edit** > **Add Objects**.

The Add Object Palette dialog box appears.

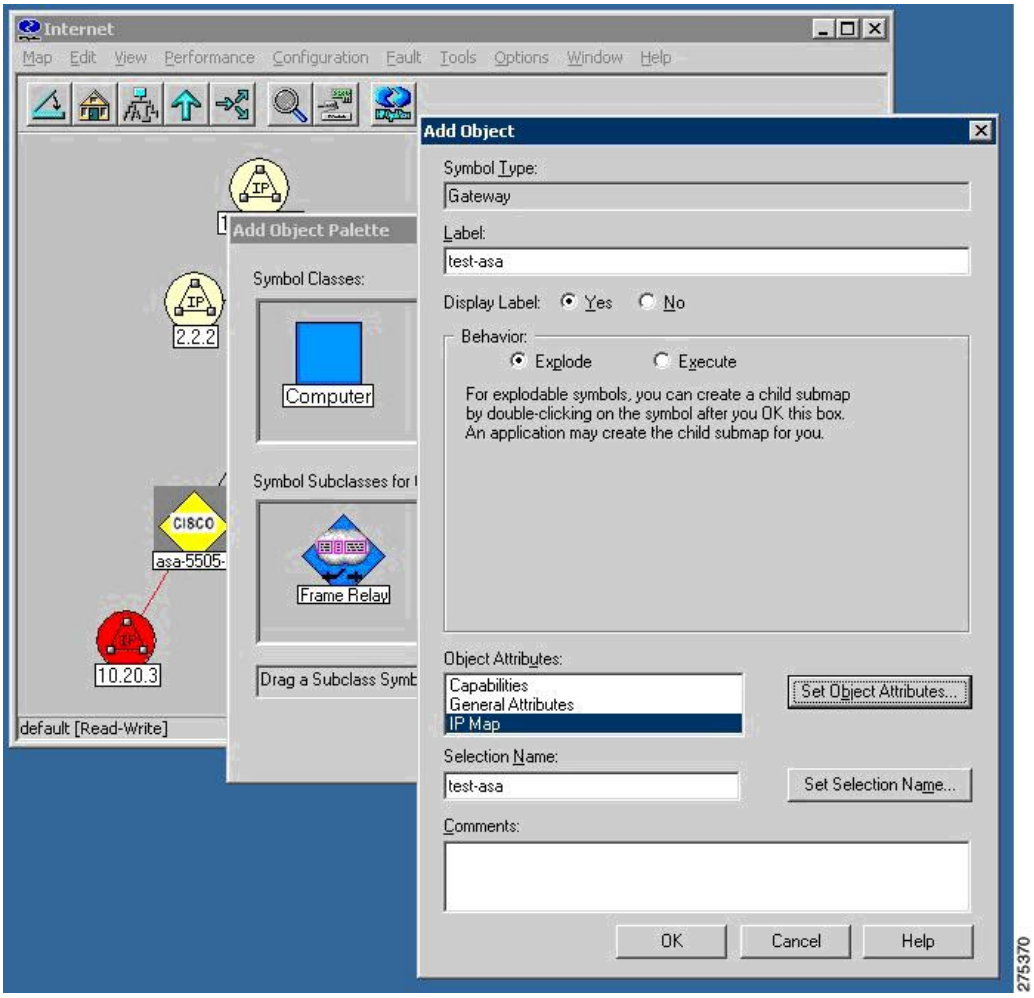
Figure 36: Add Object Palette Dialog Box



Step 3 Click the Connector Symbol Class icon, and drag the Gateway Symbol Subclass icon onto the Internet-level submap. Choose this gateway connector, regardless of the type of device you are using to start the discovery.

The Add Object dialog box appears.

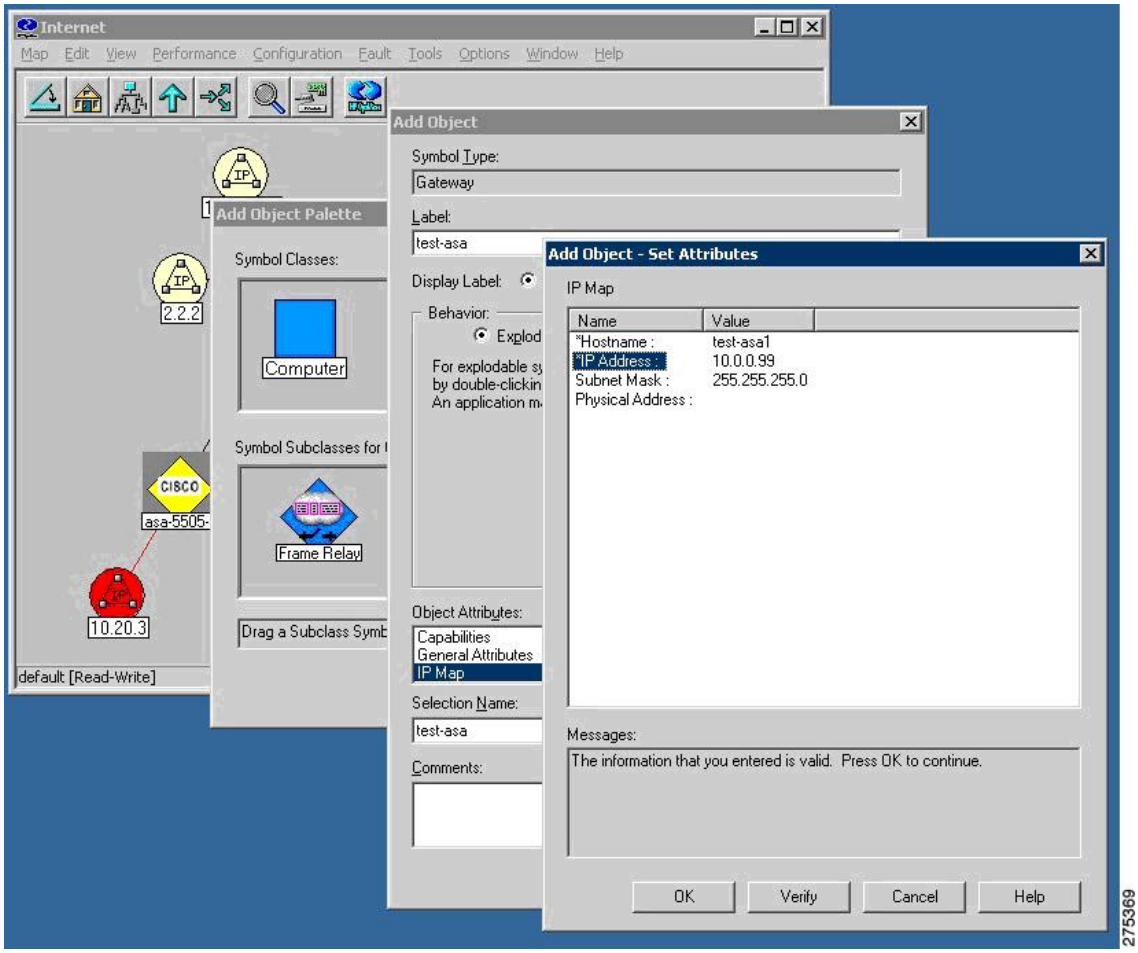
Figure 37: Add Object Dialog Box



Step 4 Double-click **IP Map**.

The Add Object – Set Attributes dialog box appears.

Figure 38: Add Object – Set Attributes Dialog Box



Step 5 Type the IP address and hostname of an SNMP-enabled device within the network that you want to add to your management domain, and click **Verify**.

Step 6 After NNM checks the configuration, NNM corrects the symbol choice and (if necessary) its placement for you. The device is now configured to be managed by NNM and should be visible on the Internet map.

Configuring Specific SNMP Version 3 Parameters

To configure credentials for specific SNMP nodes, perform the following steps:

Step 1 Double-click the **xnmsnmpconf.exe** file, located in C:\Program Files\HP OpenView\bin.

Step 2 In the NNM main window, choose **Options** > **SNMP Configuration**.

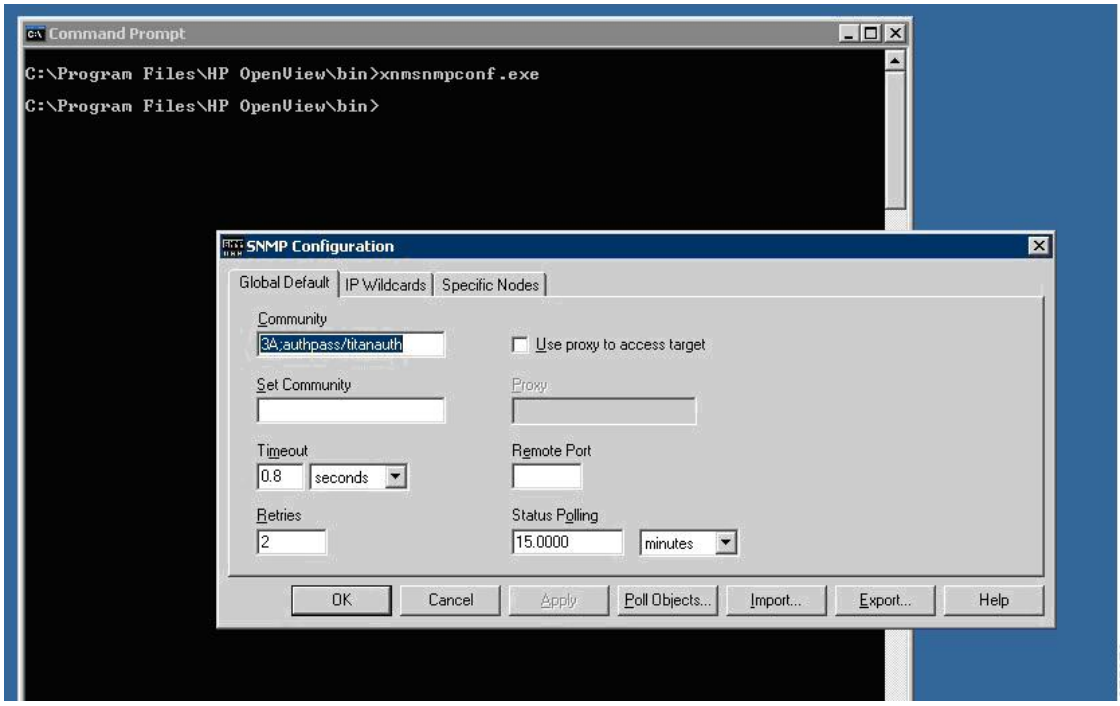
A configuration pane appears.

Note When you set SNMP Version 3 credentials, you must use the overloaded SNMP string. For more information, see Step 2 in the Configuring the NNM MIB Browser.

Setting Global SNMP Version 3 Credentials

To set global SNMP Version 3 credentials, in the Global Settings section, enter an SNMPv3 user and password to be used for default communication. For the format of the community string, see Step 2 in the Configuring the NNM MIB Browser.

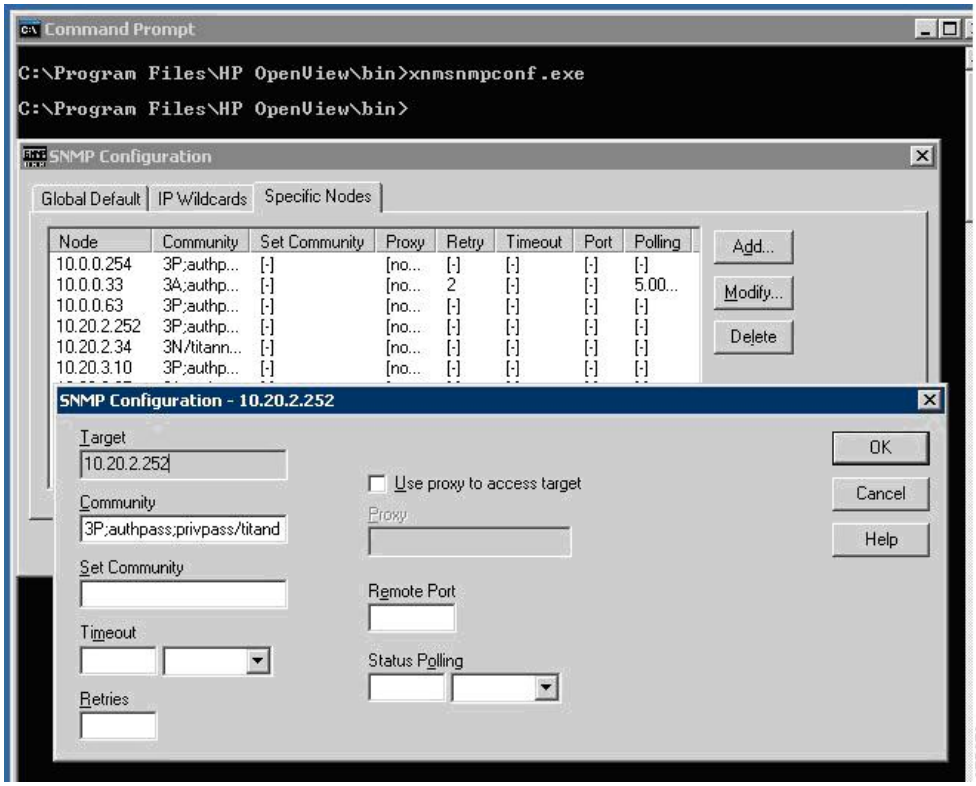
Figure 39: SNMP Configuration



Setting Specific SNMP Version 3 Credentials

To set specific SNMP Version 3 credentials, enter SNMP Version 3 users and passwords for individual SNMP nodes by clicking the **Specific Nodes** tab.

Figure 40: SNMP Configuration Dialog Box



Viewing Node Information

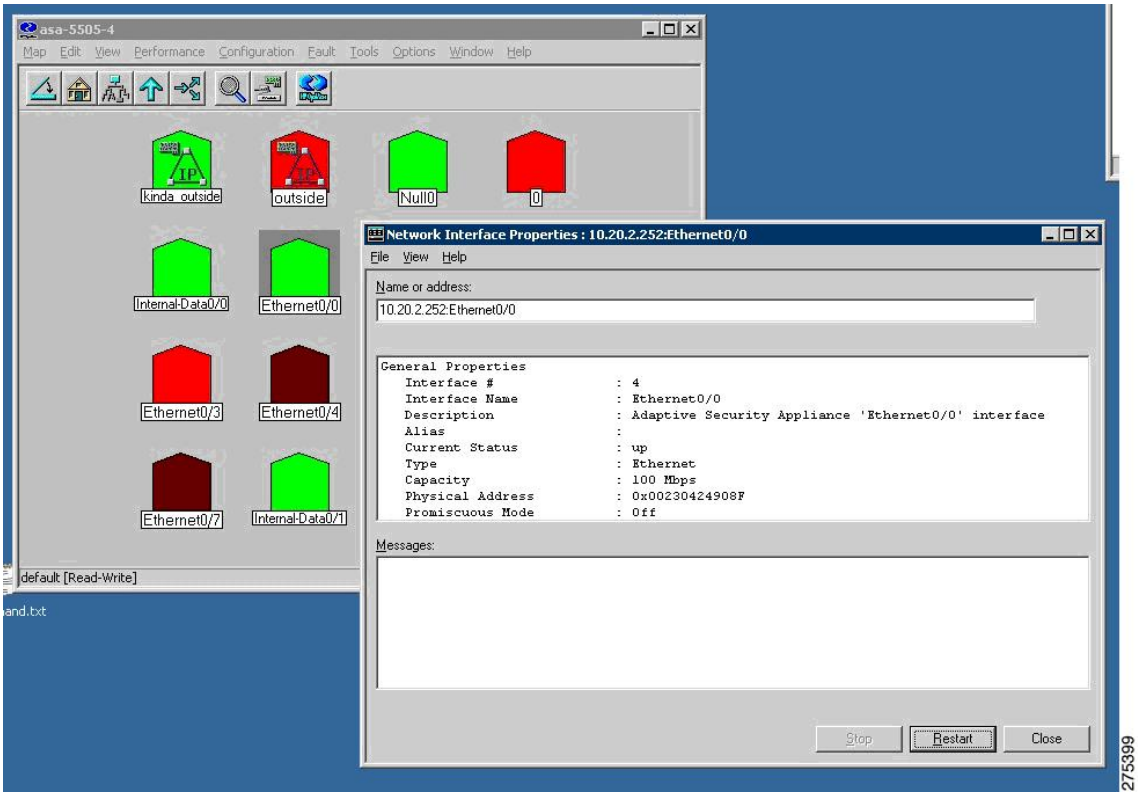
To view node information, perform the following steps:

Step 1 From the Internet map, drill down to a specific node for a view of all available interfaces.

Step 2 To view additional interface information, right-click an interface, then choose **Interface Properties** or **Interface Status**.

The Network Interface Properties dialog box appears.

Figure 41: Network Interface Properties Dialog Box



Configuring the NNM MIB Browser

To configure the NNM MIB Browser, perform the following steps:

Step 1 From the NNM server command prompt, start the MIB Browser, located in C:\Program Files\HP OpenView\bin\xnmbrowser.exe.

Step 2 Enter the IP address of the SNMP host and the community string. For SNMP Version 3 connections, the community string uses the syntax for the overloaded community string.

The following is an example of the syntax used for the overloaded community string:

```
SNMPv3 noAuthNoPriv
3N[/KEEP]/[ [contextEngineID] [-contextName]/ ]username
SNMPv3 authNoPriv
3A[;[MD5^|SHA^]authKey[/KEEP]]/[ [contextEngineID] [-contextName]/
]username
SNMPv3 authPriv
3P[;[MD5^|SHA^]authKey[;[DES^|AES^|3DES^]privKey][/KEEP]]/[
[contextEngineID] [-contextName]/ ]username
```

Note The default authentication is MD5, and the default encryption is DES.

This section includes the following topics:

Configuring SNMP Version 3 No-auth/No-Priv Connections

To configure SNMP Version 3 No-auth/No-priv connections, perform the following steps:

Step 1 To configure the UUT group, enter the **snmp-server group asanoauth v3 noauth** command.

Step 2 To configure the UUT user, enter the **snmp-server user titannoauth asanoauth v3** command.

Step 3 For the community name, enter **3N/titannoauth**.

Configuring SNMP Version 3 MD5 Auth/No-priv Connections

To configure SNMP Version 3 MD5 Auth/No-priv connections, perform the following steps:

Step 1 To configure the UUT group, enter the **snmp-server group asaauth v3 auth** command.

Step 2 To configure the UUT user, enter the **snmp-server user titanauth asaauth v3 auth md5 authpass** command.

Step 3 For the community name, enter **3A:authpass/titanauth**.

Configuring SNMP Version 3 SHA Auth/No-priv Connections

To configure SNMP Version 3 SHA Auth/No-priv connections, perform the following steps:

Step 1 To configure the UUT group, enter the **snmp-server group asaauth v3 auth** command.

Step 2 To configure the UUT user, enter the **snmp-server user titanshaauth asaauth v3 auth sha authpass** command..

Step 3 For the community name, enter **3A:SHA^authpass/titanshaauth**.

Configuring SNMP Version 3 MD5 Auth/Priv Connections

To configure SNMP Version 3 MD5 Auth/Priv connections, perform the following steps:

Step 1 To configure the UUT group, enter the **snmp-server group asapriv v3 priv** command.

Step 2 To configure the UUT user, enter the **snmp-server user titandes asapriv v3 auth md5 authpass privdes privpass** command.

Step 3 For the community name, enter one of the following:

- **3P:authpass:privpass/titandes**
- **3P:MD5^authpass:DES^privpass/titandes**

Configuring SNMP Version 3 SHA Auth/Priv Connections

To configure SNMP Version 3 SHA Auth/Priv connections, perform the following steps:

Step 1 To configure the UUT group, enter the **snmp-server group asapriv v3 priv** command.

Step 2 To configure the UUT user, enter the **snmp-server user titanshades asapriv v3 auth sha authpass privdes privpass** command.

Step 3 For the community name, enter **3P:SHA^authpass:DES^privpass/titanshades**.

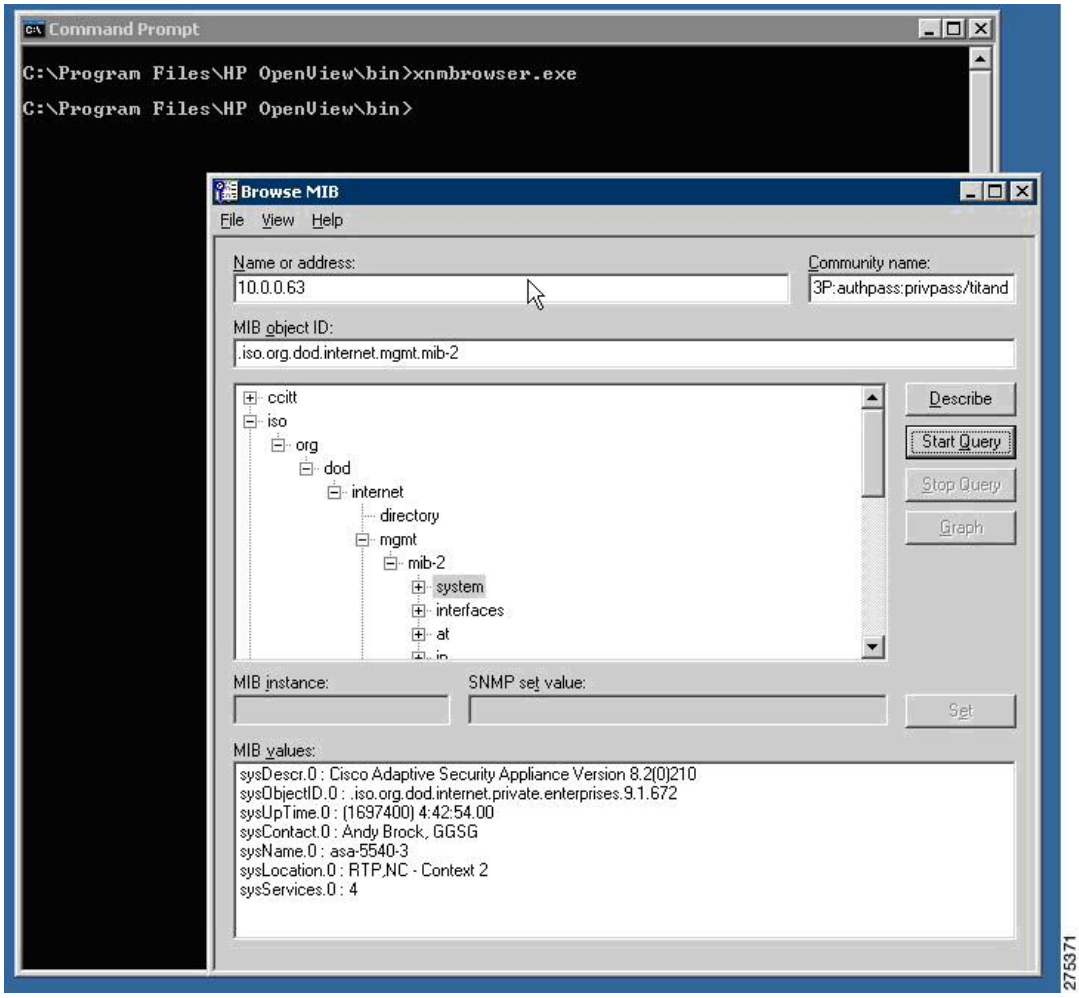
Browsing a MIB

To browse a MIB, perform the following steps:

Step 1 Drill down to the OID, .iso.org.dod.internet.mgmt.mib-2.system, and select the **system** object.

Step 2 Click **Start Query** to fill in the MIB Values field with the DUT description.

Figure 42: Browse MIB Dialog Box

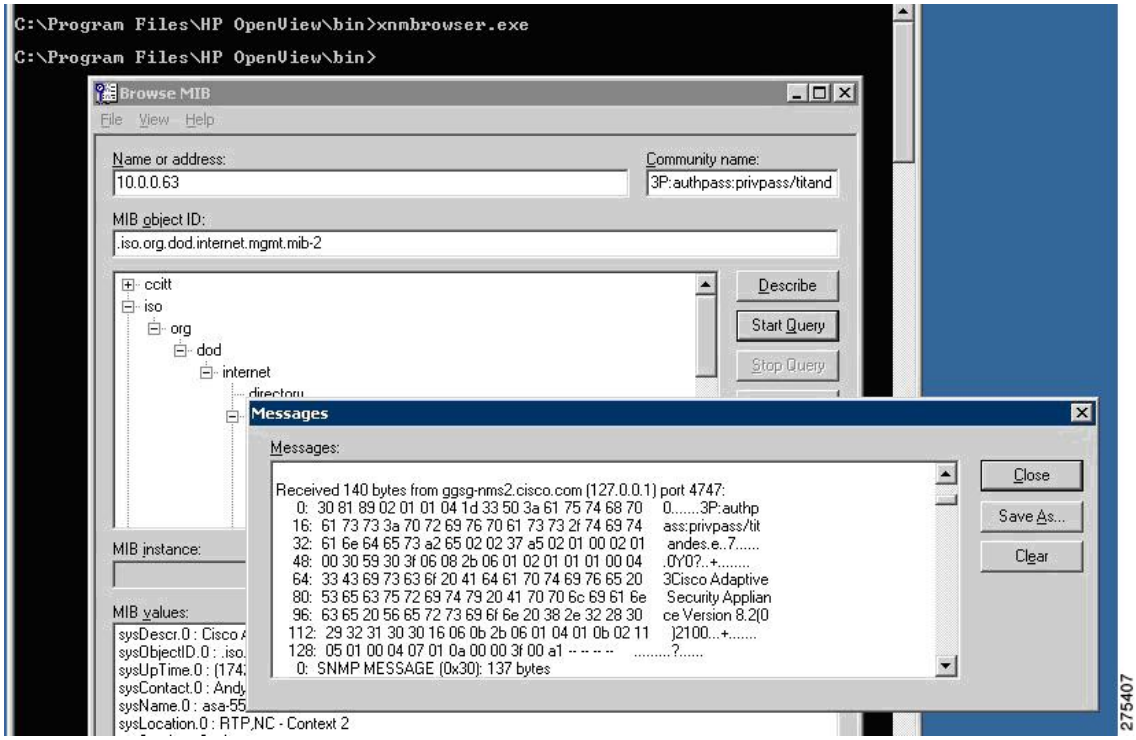


Running a MIB Browser Packet Trace

To run a MIB Browser packet trace, in the MIB Browser dialog box, choose **View** > **SNMP Packet Trace** .

The Messages dialog box appears, which shows the packet contents of the SNMP communication between the MIB Browser and the SNMP agent. This information is helpful for debugging.

Figure 43: Packet Trace in the Messages Dialog Box



Using the NNM SNMP Version 3 Trap Viewer

When using the NNM SNMP Version 3 Trap Viewer, perform the following steps:

Step 1 Make sure that the SNMP Version 3 credentials of a user on the SNMP agent are cached in the NNM.

Step 2 When using the MIB Browser to query an SNMP agent, enter the following community string:

```
3P:authpass:privpass/KEEP/titandes
```

Note By using the **KEEP** parameter in the overloaded community string, you save the user credentials in the NNM configuration file, which is required because secure SNMP Version 3 traps and inform requests are sent from the SNMP agent to the NNM, and authentication must occur. The user information is included in the configuration file, located in C:\etc\srconf\mgr\mgr.cnf. You can modify this file directly. For instructions, see the NNM SPI SNMP Version 7.53 documentation.

Alternatively, you can use the **snmpget** command, as shown in the following example:

```
C:\Program Files\HP OpenView\bin>snmpget-c "3P;MD5^authpass;DES^privpass/KEEP/titandes"
10.0.0.33 sysDescr.0
```

Step 3 To configure the SNMP agent to send traps, enter the following command on the ASA:

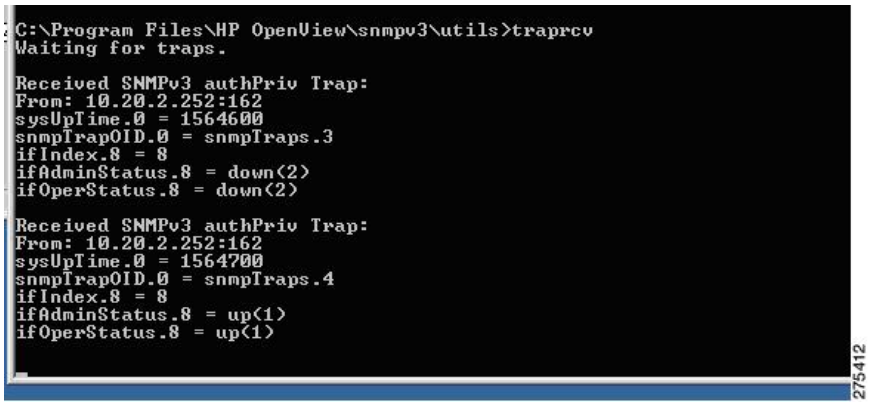
```
cicoasa (config)# snmp-server host inside 10.0.0.10 traps version 3 titandes
```

Note The command syntax may differ slightly between ASA platforms. The user configured in this example is the same as the user defined in the community string in the Configuring the NNM MIB Browser.

The NNM traprcv utility is a command-line tool that receives SNMP trap messages and responds to SNMP inform requests from remote SNMP entities. It binds to the SNMP trap port (udp/162) to listen for notifications, and as a result, must be run as root. It prints standard output messages about the notifications that it has received. The traprcv utility can receive SNMP Version 1 traps, SNMP Version 2c traps, SNMP Version 2c inform requests, SNMP Version 3 traps, and SNMP Version 3 inform requests. For more information, see the NNM SPI SNMP Version 7.53 documentation.

Step 4 Run the traprcv utility and wait for traps on the SNMP agent. The utility is available at the following location: C:\Program Files\HP OpenView\snmpv3\utils\traprcv.exe.

Figure 44: SNMP Trap Receiver



Using the HP OpenView NNM Web Application

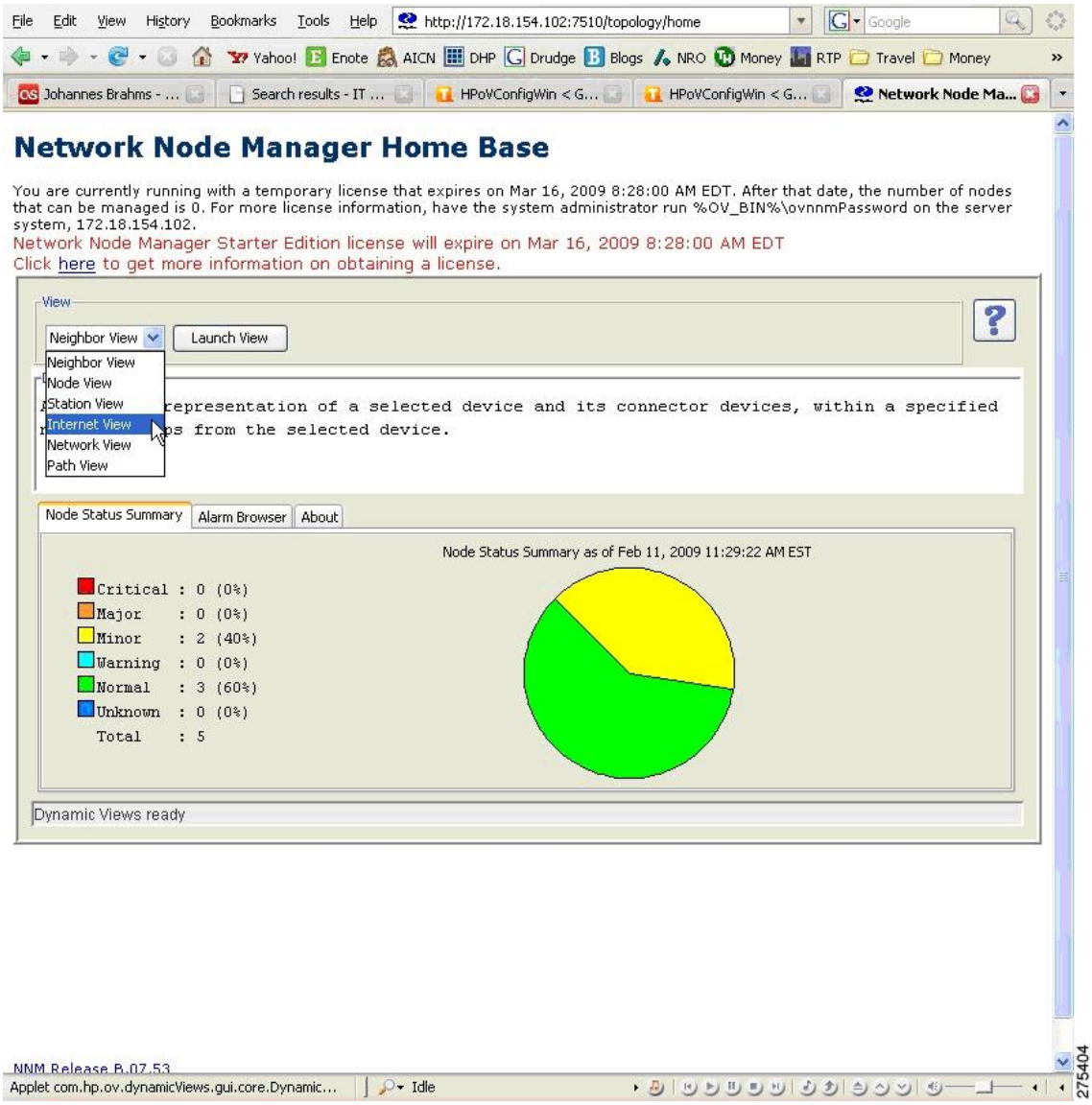
To start the NNM web application, perform the following steps:

Step 1 In a web browser, go to the following URL: http://%3CNNM-Server-IP-Address%3E:7510/topology/home

Step 2 To view SNMP nodes, from the drop-down menu, choose **Internet View**.

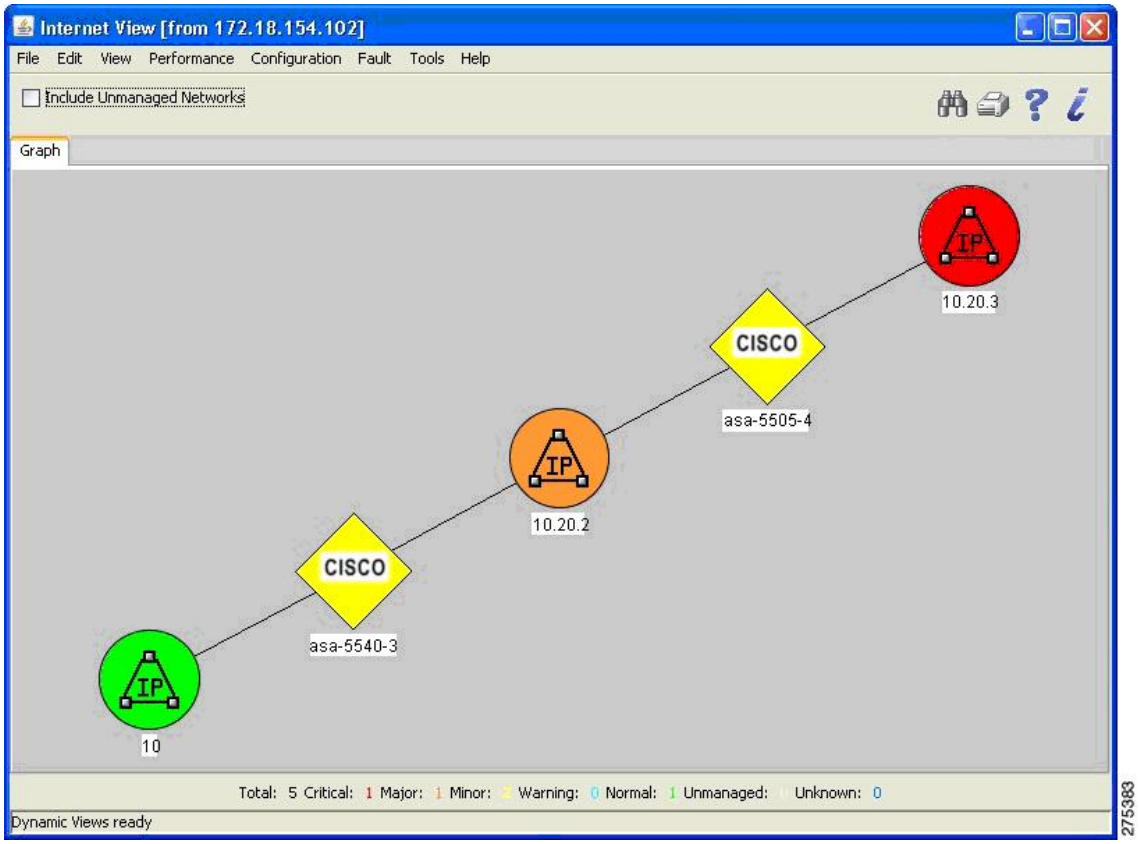
The Internet View window appears.

Figure 45: NNM Home Base Window



Step 3 To view node properties, double-click the selected node to open a new browser window with the node information.

Figure 46: Internet View Window



CiscoWorks

CiscoWorks LAN Management Solution (LMS) is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. For more information, see the following URL: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html

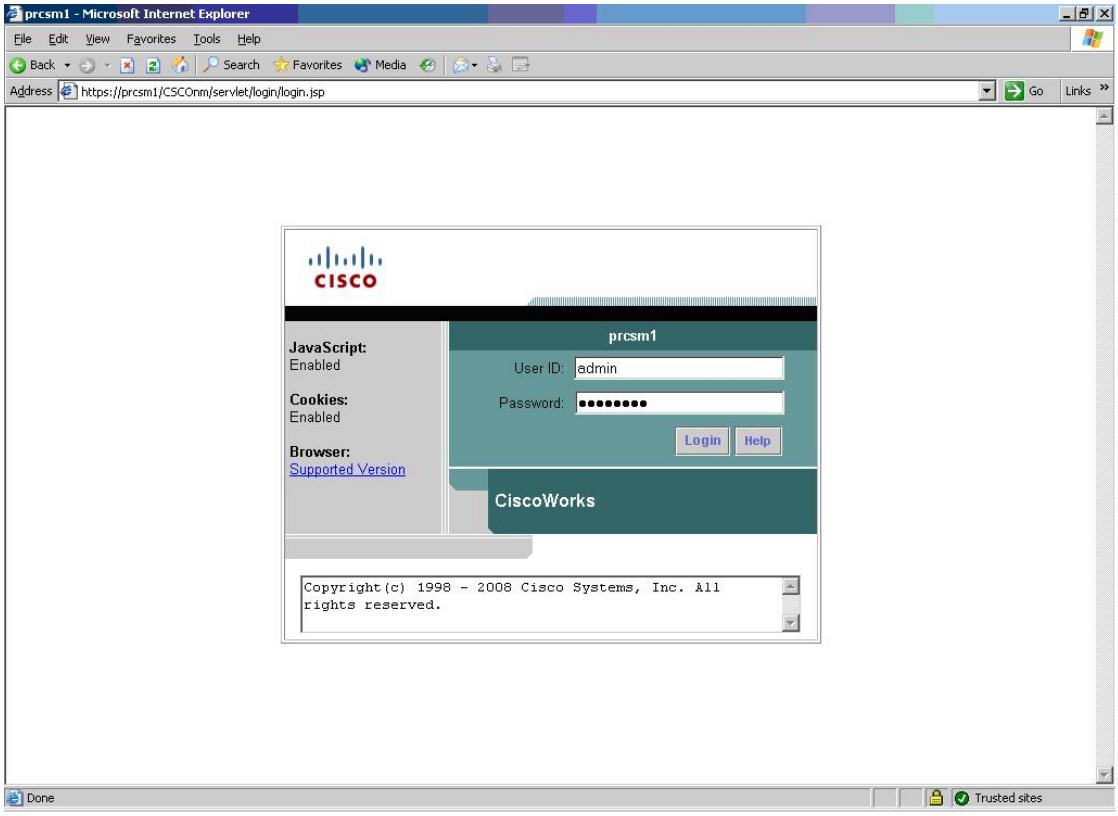
This section includes the following topics:

Starting CiscoWorks

To start CiscoWorks on a Windows 2003 server, perform the following steps:

Choose **Start** > **All Programs** > **CiscoWorks**. The following figure shows the login page.

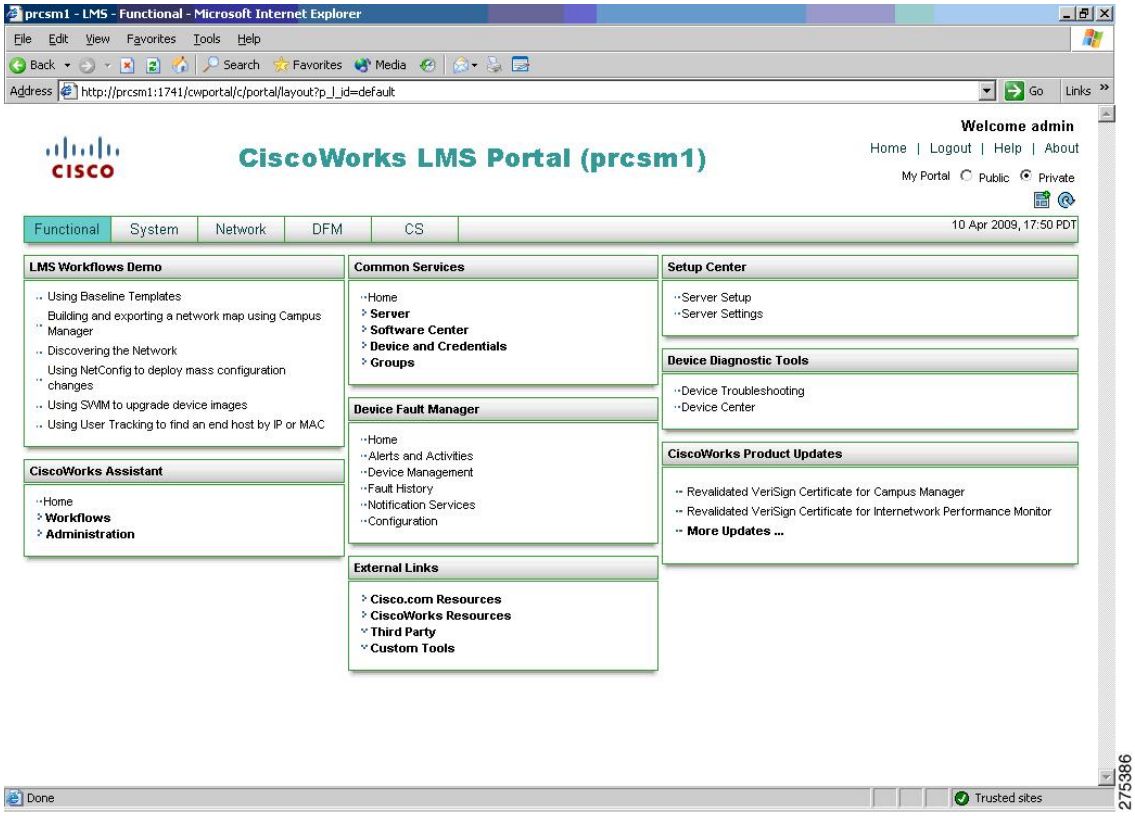
Figure 47: Login Page



Getting Started with the CiscoWorks LMS Portal

The CiscoWorks LMS Portal is the first page that appears when you start the LMS application. This page serves as the interface, starting point, and top-level navigation for the frequently used functions in the application.

Figure 48: CiscoWorks LMS Portal Page



Using the Device Center

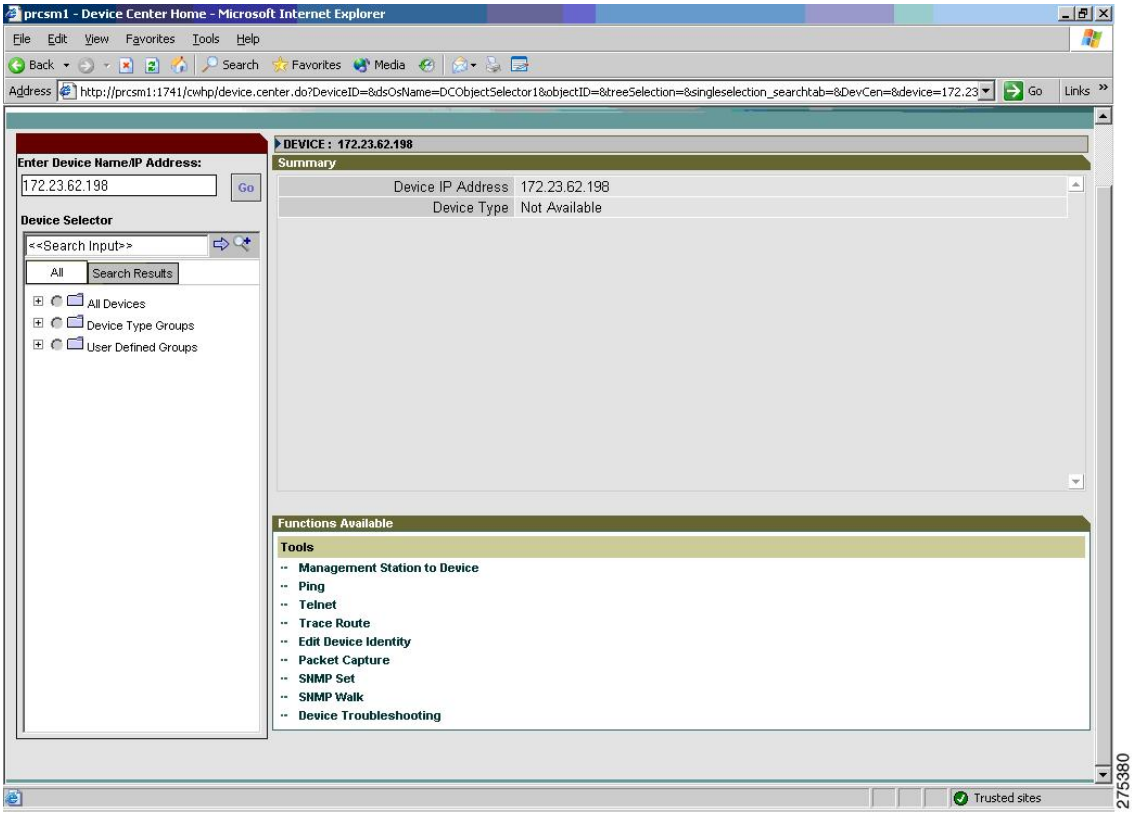
To manage devices, perform the following steps:

Step 1 Choose **Device Diagnostic Tools** > **Device Center**.

The Device Center Home page appears with the Device Selector in the left pane and Device Center summary information in the right pane.

Step 2 Enter the IP address or device name or choose a device from the list in the Device Selector pane, and click **Go**.

Figure 49: Device Center Home Window



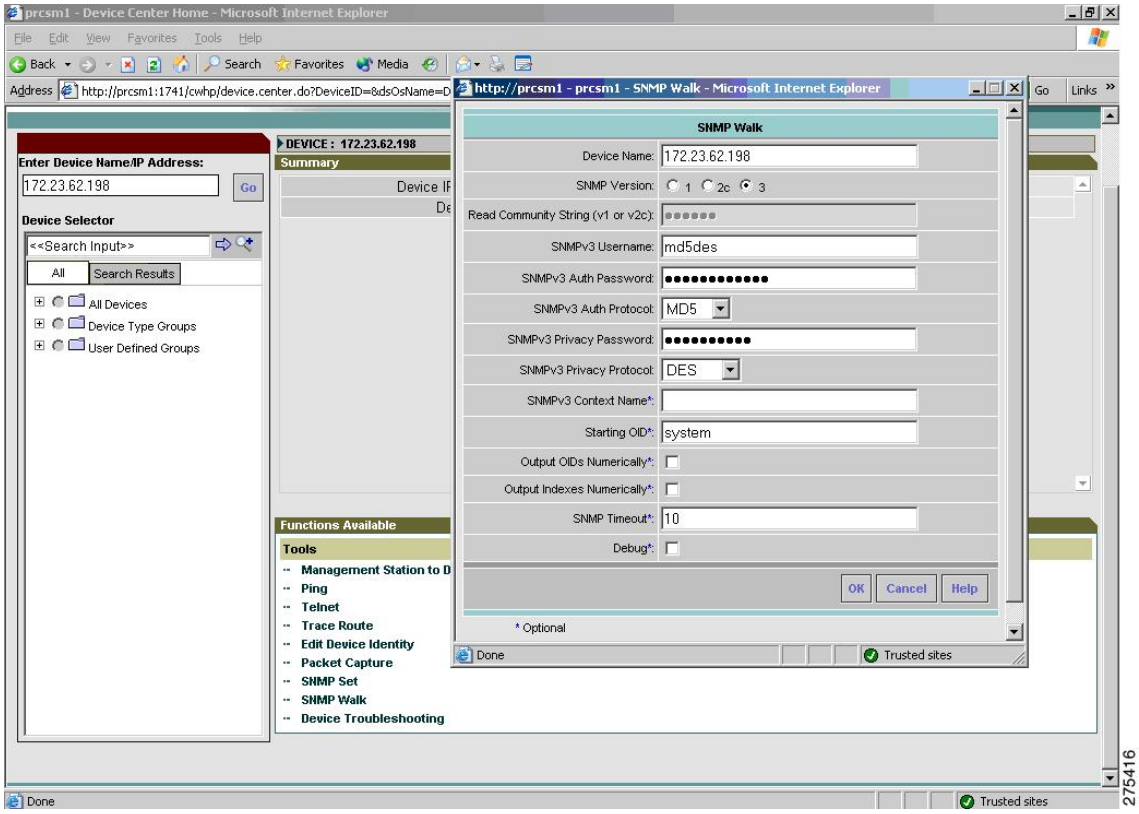
Performing an SNMP Walk

To perform an SNMP walk, perform the following steps:

Step 1 In the Functions Available pane, click the **SNMP Walk** link.

The SNMP Walk dialog box appears.

Figure 50: SNMP Walk Dialog Box



Step 2 Choose the SNMP version to use from the following options:

- For SNMP Version 3 (NoAuthNoPriv and AuthNoPriv Security Levels)
  - **a.** Enter the SNMPv3 Username.
  - **b.** Enter the SNMPv3 Auth Password.
  - **c.** Choose the SNMP v3 Auth Protocol from the drop-down list (either MD5 or SHA).
  - **d.** Enter the SNMP Context Name.

    Note Because the ASA does not support contexts, you must leave the SNMP Context Name blank.

- For SNMP Version 3 (AuthPriv Security Level)
  - **a.** Enter the SNMPv3 Username.
  - **b.** Enter the SNMPv3 Auth Password.
  - **c.** Specify the SNMP v3 Auth Protocol. Choose either MD5 or SHA.
  - **d.** Enter the Privacy Password.
  - **e.** Choose a privacy protocol from the drop-down list. The available values are DES, 3DES, AES128, AES192, and AES256.
  - **f.** Enter the SNMP Context Name.

Note Because the ASA does not support contexts, you must leave the SNMP Context Name blank.

g. (Optional) Enter the starting OID. If you leave this field blank, the tool starts from 1.

h. Enter the SNMP Timeout. The default value is 10 seconds.

i. (Optional) Check the **Output OIDs Numerically** check box to print the output OIDs numerically.

j. By default, the corresponding OID name is printed in the output window.

k. (Optional) Check the **Output Indexes Numerically** check box to show the output index numerically.

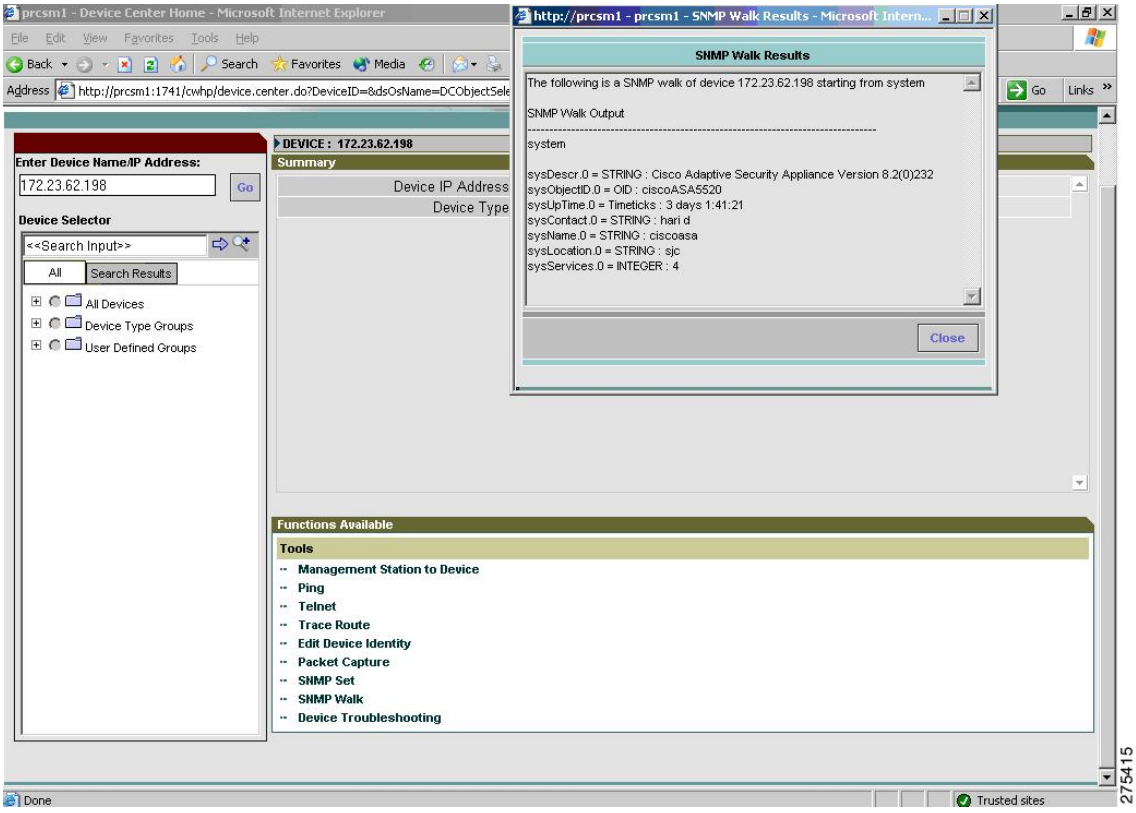
l. (Optional) Check the **Debug** check box to enable the debugging option. All the fields are case-sensitive.

m. Click **OK** to obtain the results, which are based on the parameters that you entered.

n. When the walk is complete, save it as a text file.

Note A full walk may take a long time to finish.

Figure 51: SNMP Walk Results Example



The read-write username and password for SNMP Version 3 and the read-write community string for SNMP Versions 1 and 2c are case sensitive. The SNMP Walk dialog box displays the credentials (SNMP Versions 1, 2c, and 3) for the device from the Device and Credential Repository (DCR), if they are available. Otherwise, the default values for the respective SNMP versions appear.

If you use the SNMP Walk feature with Network Operator/Help Desk access privileges, device credential fetching fails and the fields of the read/write community strings for SNMP Versions 1, 2c, and 3 credentials are set to default values.

The following figure shows the list of privacy protocols supported. You must manually enter SNMP Versions 1, 2c, and 3 credentials.

Figure 52: SNMP Walk Dialog Box

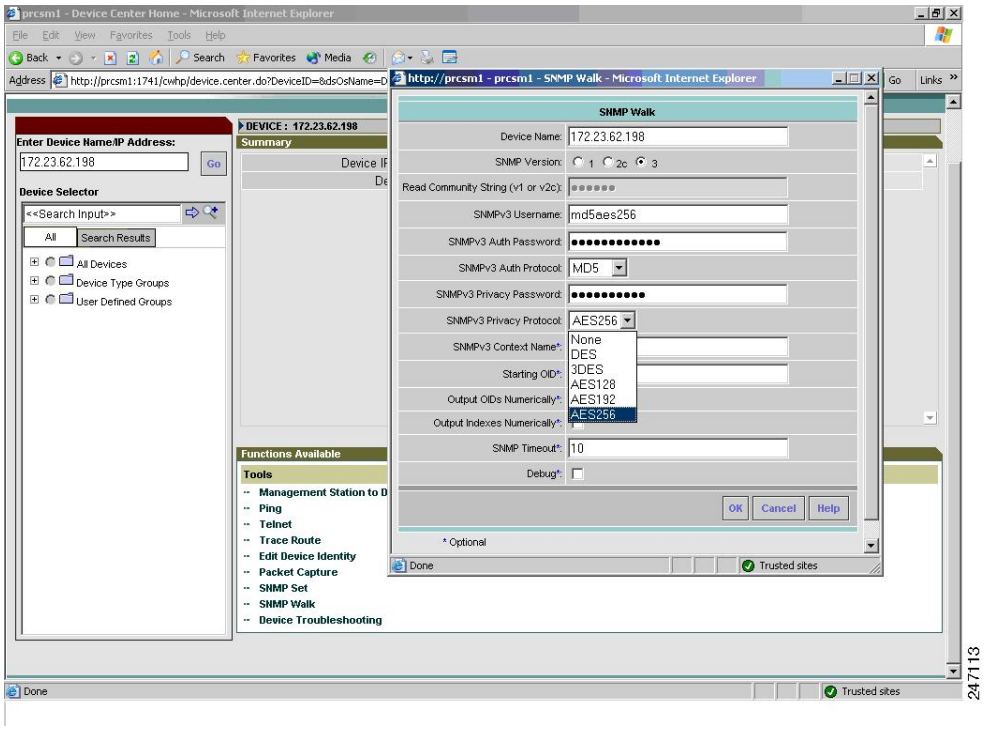
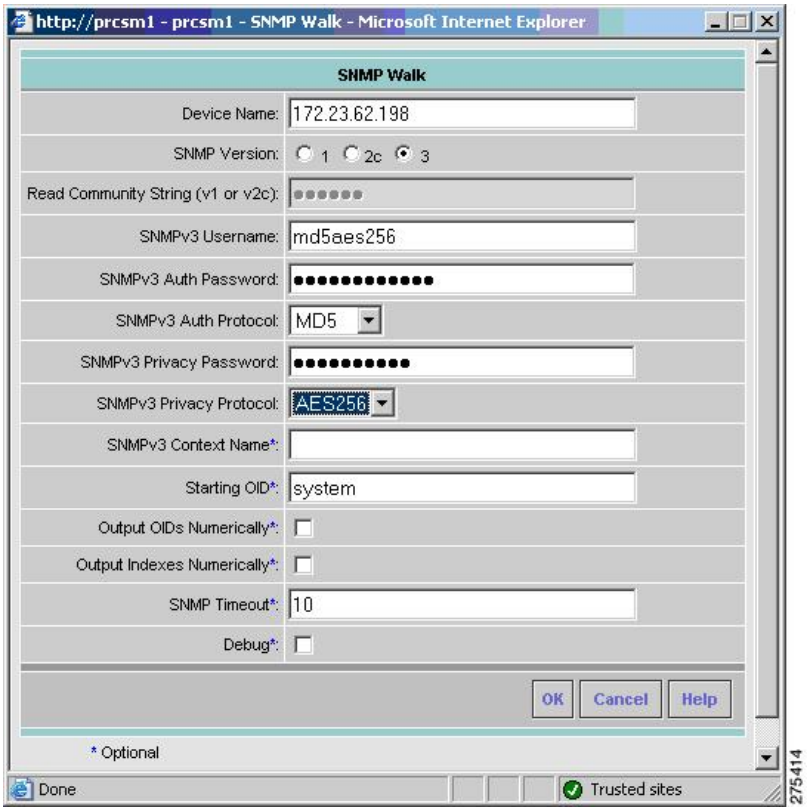


Figure 53: SNMP Version 3 Parameters



The following figure shows the SNMP walk results for the MD5 authentication and AES256 encryption algorithm settings.

Figure 54: SNMP Walk Results Dialog Box

Using the Management Station to Device Tool

To troubleshoot problems with unmanaged or unresponsive devices, you can check the device connectivity by protocol. The Management Station to Device tool helps you diagnose Layer 4 (application) connectivity problems.

Layer 4 tests include the following key services essentials that are needed to manage network devices:

- Debugging and measurement tools (UDP and TCP)
- Web server (HTTP)
- File transfer (TFTP)
- Terminal (Telnet)
- Read-write access (SNMP)

The management station to device check occurs only for protocol connectivity. Credentials for the corresponding protocols are not tested or verified. If you enter a hostname instead of an IP address, the tool performs a name lookup to discover the address. This task fails if the tool cannot find an address.

You can use this tool to send an SNMP GET request to the destination device for an SNMP read test (SNMPR). The tool also sends an SNMP SET request to the device for an SNMP write test (SNMPW). This protocol is supported for SNMP Versions 1, 2c, and 3.

If you start the Management Station to Device tool with Network Operator/Help Desk access privileges, device credential fetching fails and the fields of the read-write community strings for SNMP Versions 1, 2c, and 3 credentials are set to default values. You must manually enter SNMP Versions 1, 2c, and 3 credentials.

To start the Management Station to Device tool, perform the following steps:

Step 1 Choose **Device Diagnostic Tools** > **Device Center**.

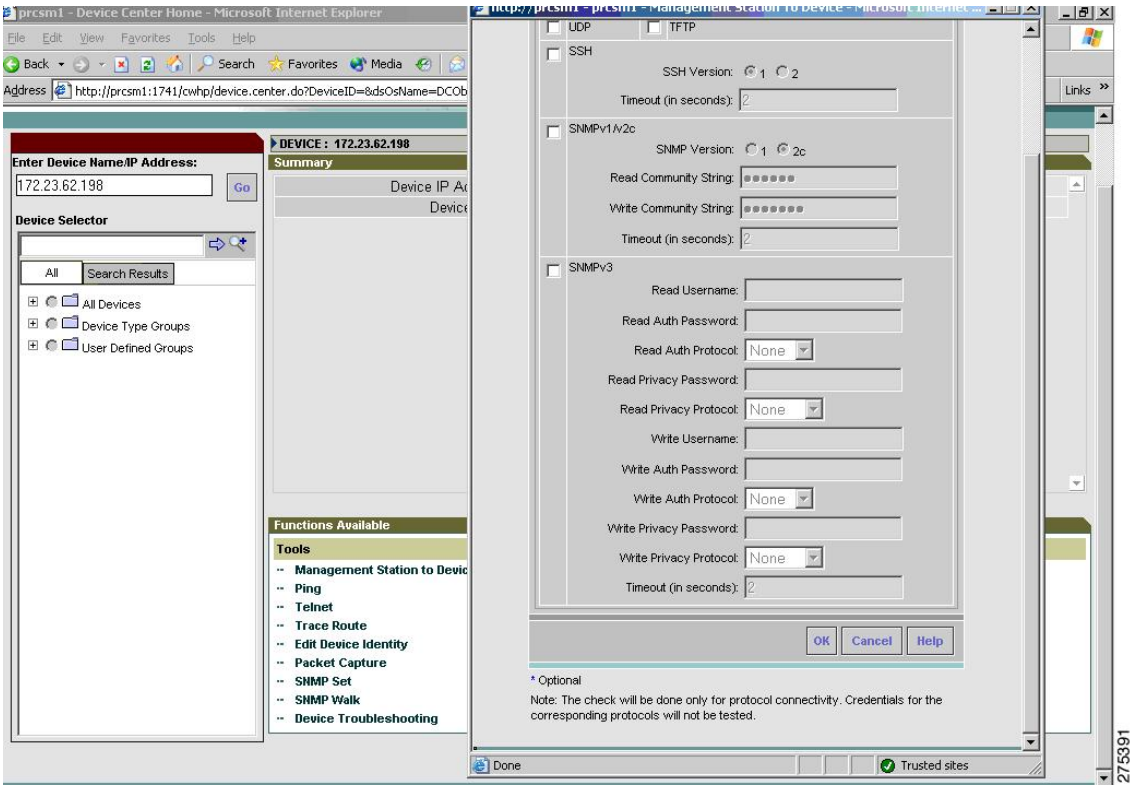
Step 2 Enter the name or IP address, fully qualified domain name, or hostname of the device that you want to check in the Device Selector field or select the device from the list, and click **Go**.

The Summary and Functions Available panes appear.

Step 3 Click **Management Station to Device** in the Functions Available pane.

The Management Station to Device dialog box appears.

Figure 55: Management Station to Device Dialog Box



Step 4 Choose the connectivity applications that you want to include from the following options. All fields are case sensitive.

- If you choose SNMP v3 (NoAuthNoPriv Security Level), enter the following information:
  - Read Username.
  - Write Username.
  - Timeout (in seconds). The default value is two seconds.
- If you choose SNMP v3 (AuthNoPriv Security Level), enter the following information:
  - Read Username.
  - Read Auth Password.
  - Read Auth Protocol. Choose either MD5 or SHA from the drop-down list.
  - Write Username.
  - Write Auth Password.
  - Write Auth Protocol. Choose MD5 or SHA from the drop-down list.
  - Timeout (in seconds). The default value is two seconds.
- If you choose SNMP v3 (AuthPriv Security Level), enter the following information:
  - Read Username.

- Read Auth Password.
- Read Auth Protocol. Choose MD5 or SHA from the drop-down list.
- Read Privacy Password.
- Read Privacy Protocol. Choose a privacy protocol from the drop-down list. The available protocols are DES, 3DES, AES128, AES192, and AES256.
- Write Username.
- Write Auth Password.
- Write Auth Protocol. Choose MD5 or SHA from the drop-down list.
- Write Privacy Password.
- Write Privacy Protocol. Choose a privacy protocol from the drop-down list. The available protocols are DES, 3DES, AES128, AES192, and AES256.
- Timeout (in seconds). The default value is two seconds.

The Interface Test Results dialog box displays the results (see Figure 2-55). The Interface Details Results dialog box shows the interfaces tested and the test results for each option.

Note The read-write username and password for SNMP Version 3 and the read-write community string for SNMP Versions 1 and 2c are case sensitive.

Figure 56: Management Station Device Results Dialog Box