



## CHAPTER 2

# Using Network Management Tools

---

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

- [Net-SNMP, page 2-1](#)
- [SilverCreek SNMP Test Suite, page 2-3](#)
- [Ipswitch WhatsUp Gold, page 2-17](#)
- [HP OpenView Network Node Manager, page 2-30](#)
- [CiscoWorks, page 2-46](#)

## 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, page 2-1](#)
- [Sending a Trap, page 2-2](#)

## Polling a MIB

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



### 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 adaptive security appliance 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 adaptive security appliance to send a linkdown or linkup trap by entering the following commands:

```
hostname (config)# int g3/1.391
hostname (config-if)# shut
hostname (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, page 2-3](#)
- [Setting Up an SNMP Version 3 Agent, page 2-5](#)
- [Loading and Deleting MIBs, page 2-7](#)
- [Running a Test Suite, page 2-8](#)
- [Enabling Debugging, page 2-9](#)
- [Testing MIBs, page 2-12](#)
- [Receiving Notification Trap Messages, page 2-15](#)
- [Testing Performance, page 2-16](#)

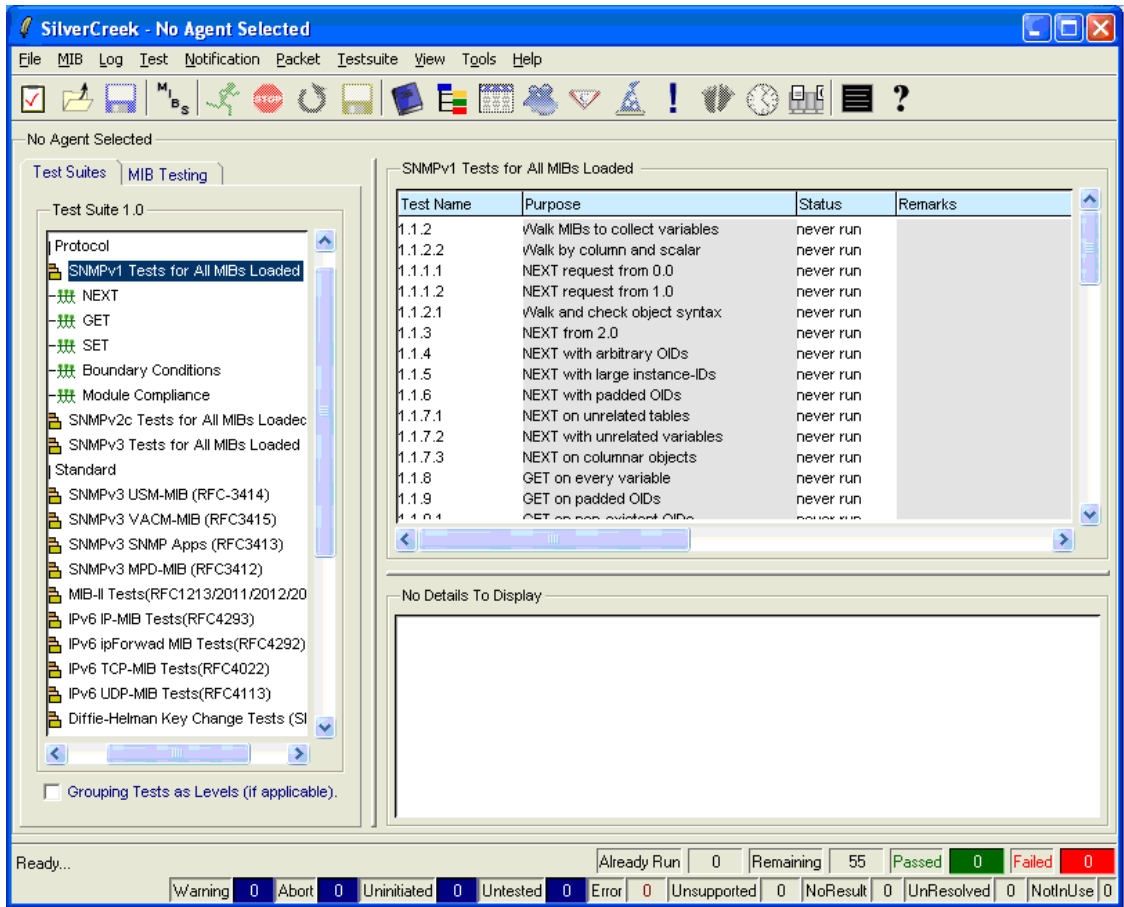
## Running SilverCreek

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

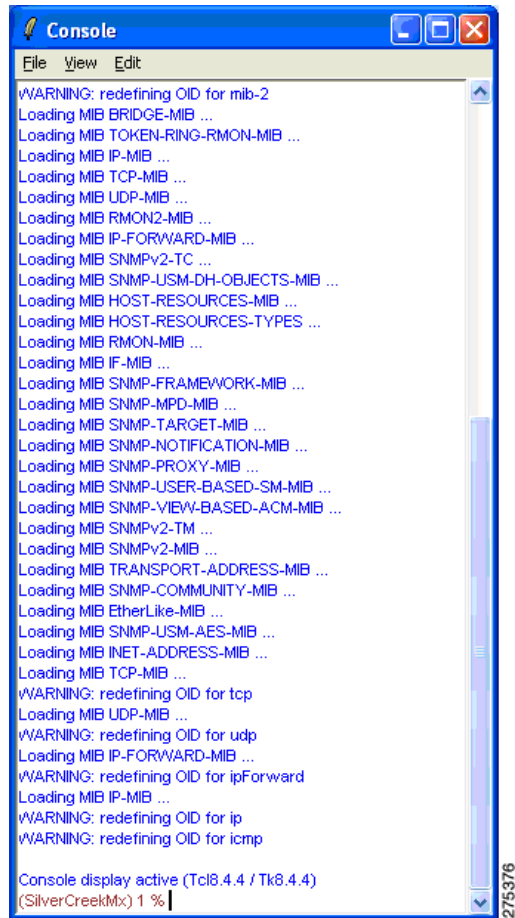
When the application starts, along with the SilverCreek main window (see [Figure 2-1](#)), a console window (see [Figure 2-2](#)) appears that shows the following information:

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

Figure 2-1 SilverCreek Main Window



275367

**Figure 2-2** SilverCreek Console Window

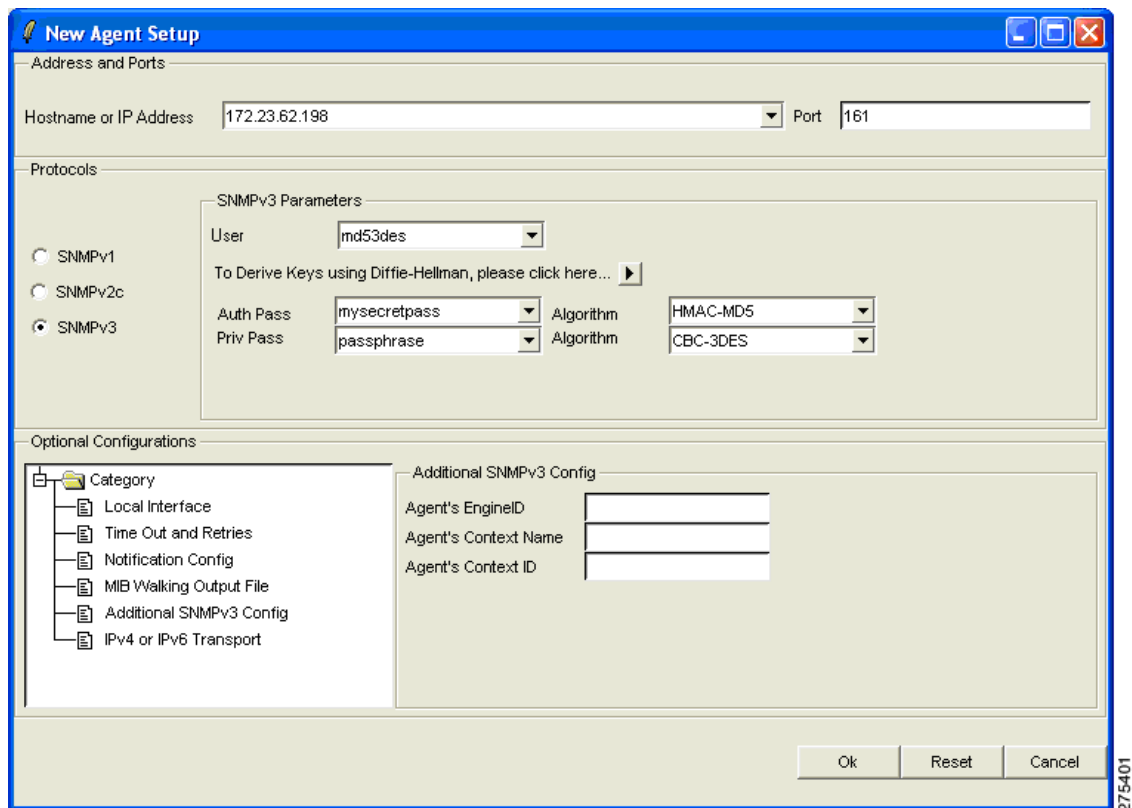
## Setting Up an SNMP Version 3 Agent

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

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

Figure 2-3 shows how the new agent must be configured.

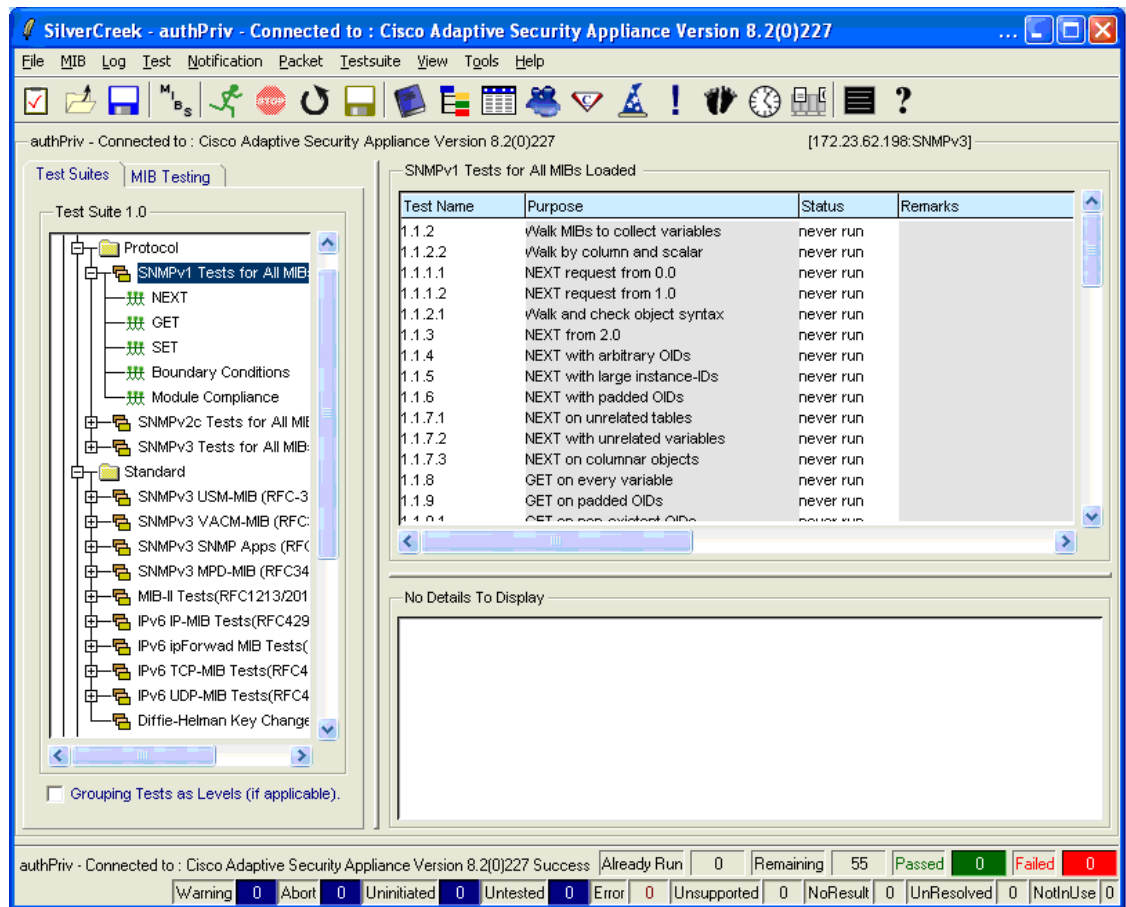
**Figure 2-3** *New Agent Setup Dialog Box*



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

After the agent is connected, as shown in Figure 2-4, you can run SNMP test suites from the Test Suites tab in the left pane.

Figure 2-4 SilverCreek Main Window Showing Connected SNMP Agent



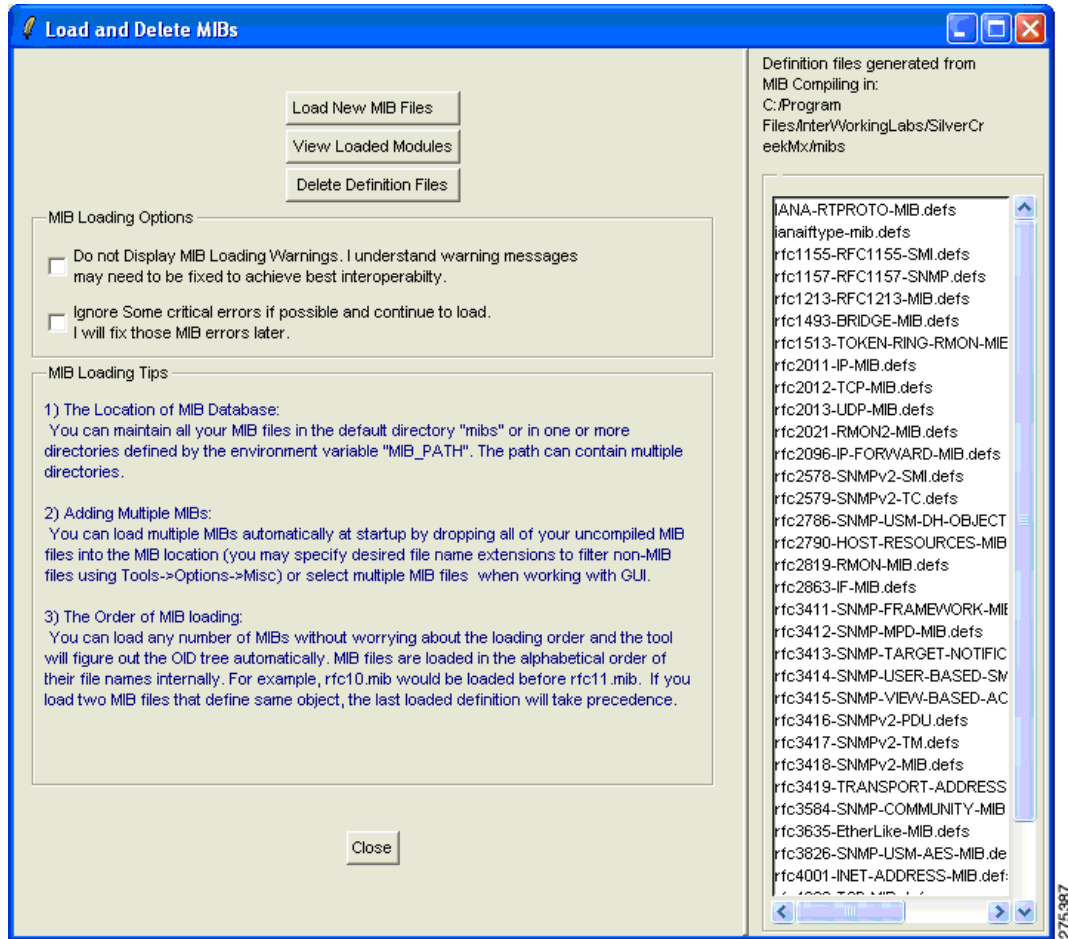
## Loading and Deleting MIBs

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** (see Figure 2-5).

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

Figure 2-5 Load and Delete MIBs Dialog Box

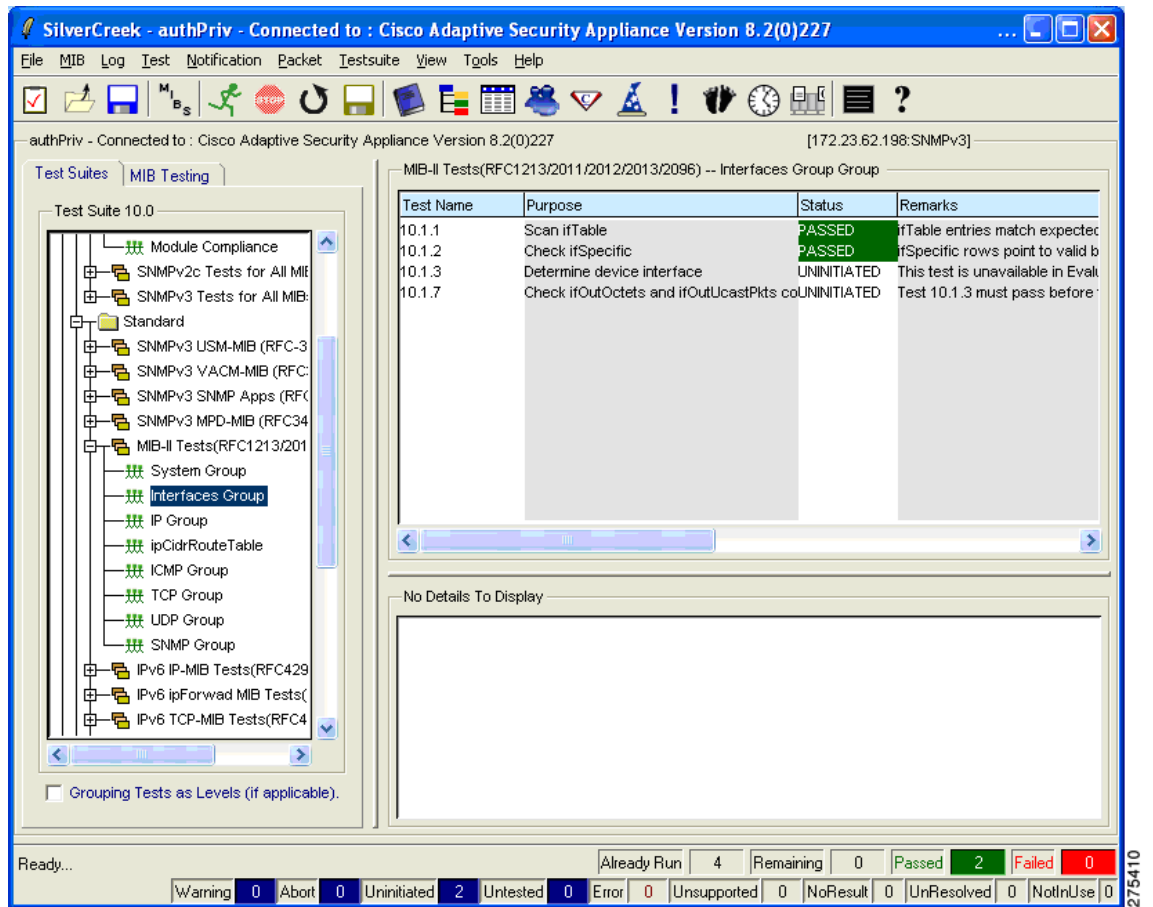


## Running a Test Suite

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 2-6](#)). 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 2-6 SilverCreek Main Window Showing Selected Tests



## Enabling Debugging

To enable debugging, choose **Tools > Options** (see [Figure 2-7](#)).

Figure 2-7 Debug Tab of the Options Dialog Box

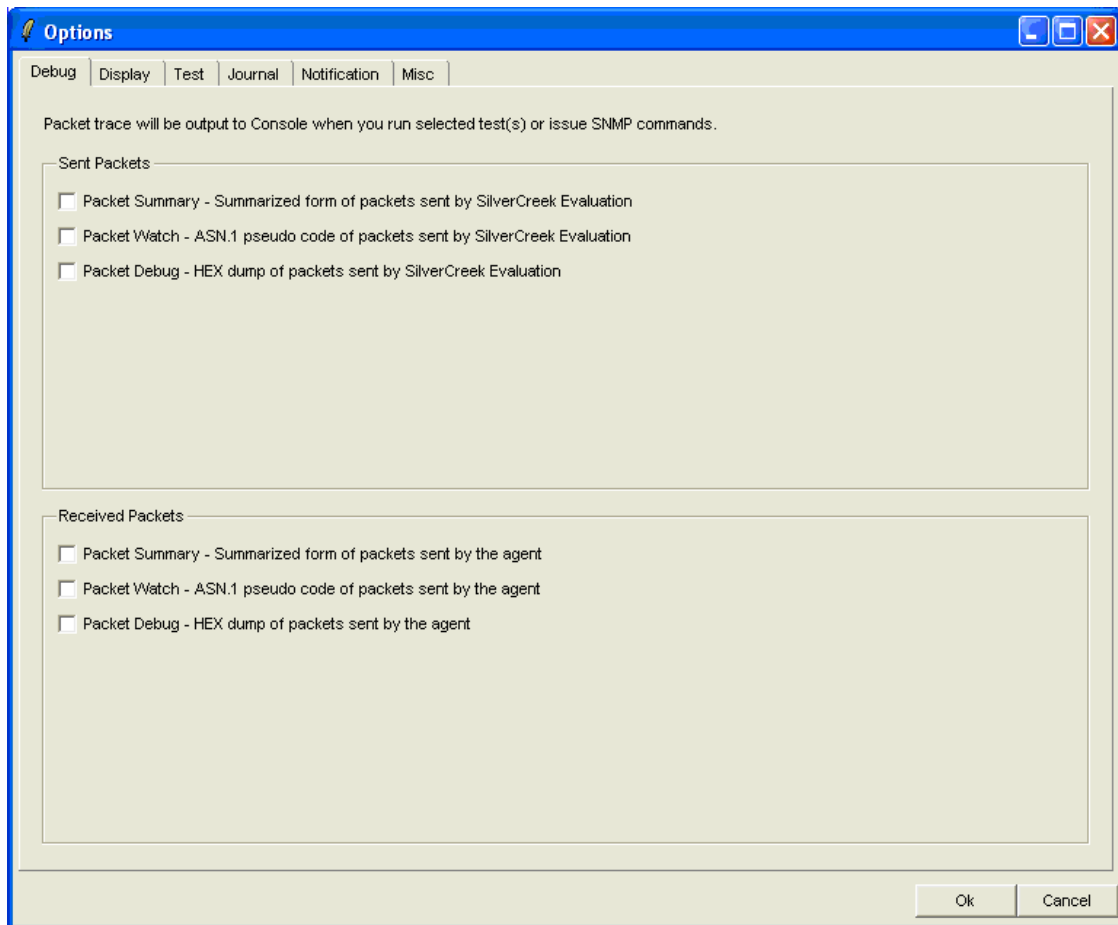


Figure 2-8 shows the warning message that appears to indicate that the test runs more slowly with debugging turned on.

**Figure 2-8** Warning Notes Dialog Box

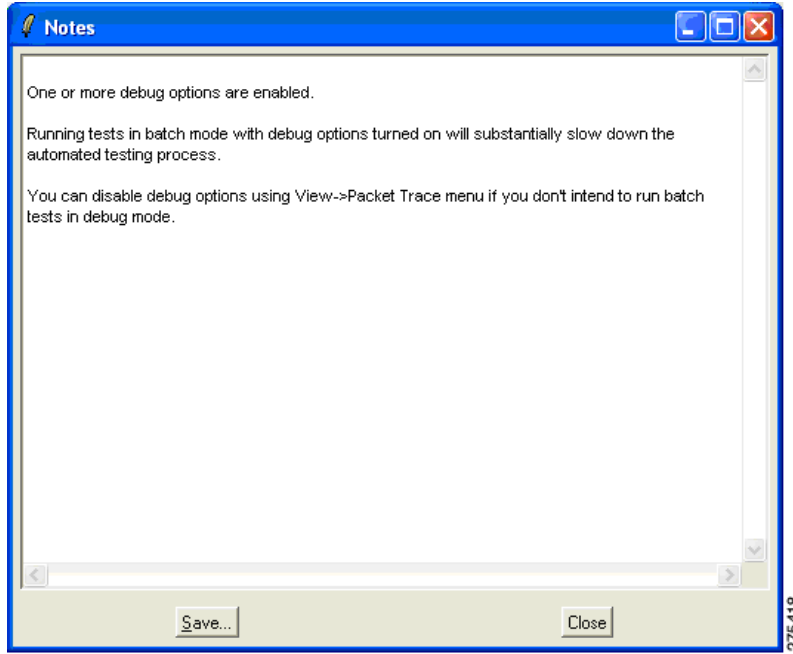
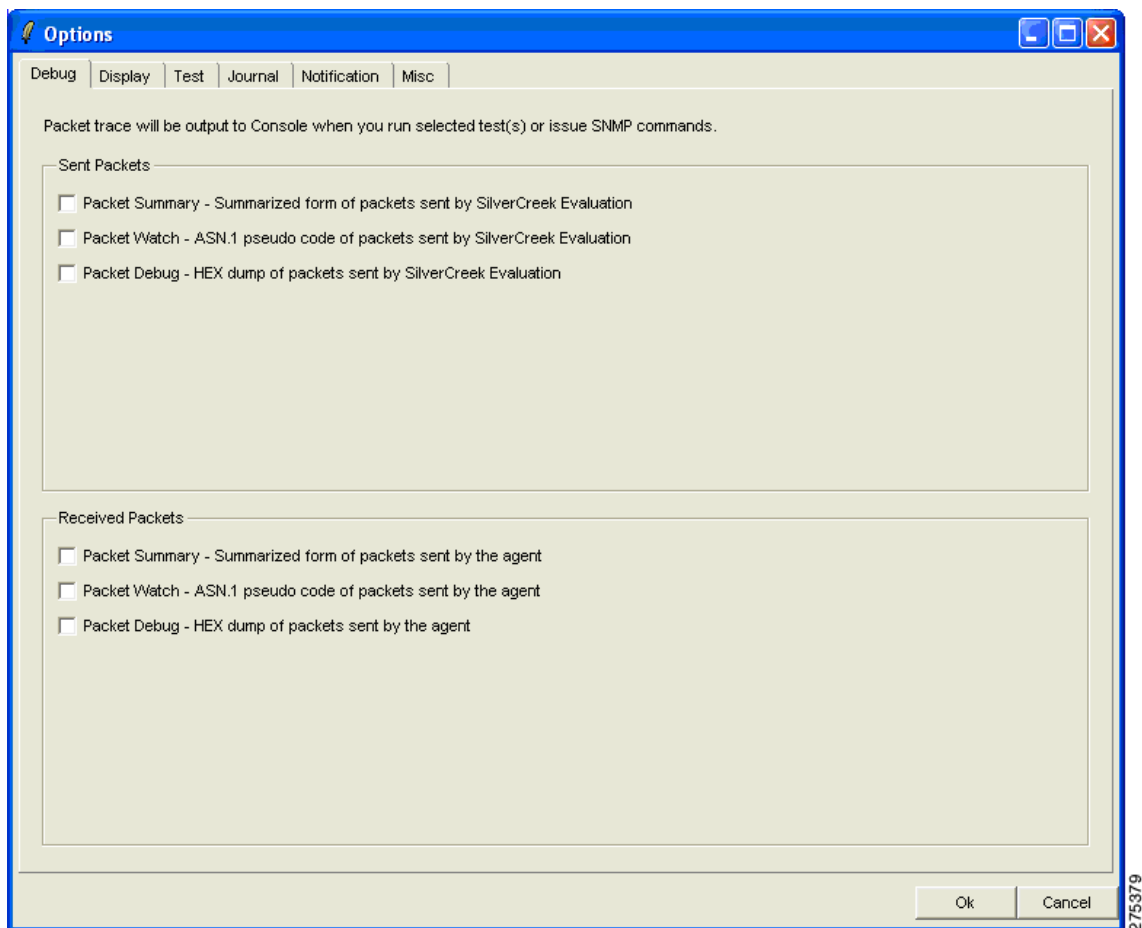


Figure 2-9 shows the console dialog box that lists the debugging messages, which appear when you run a test.

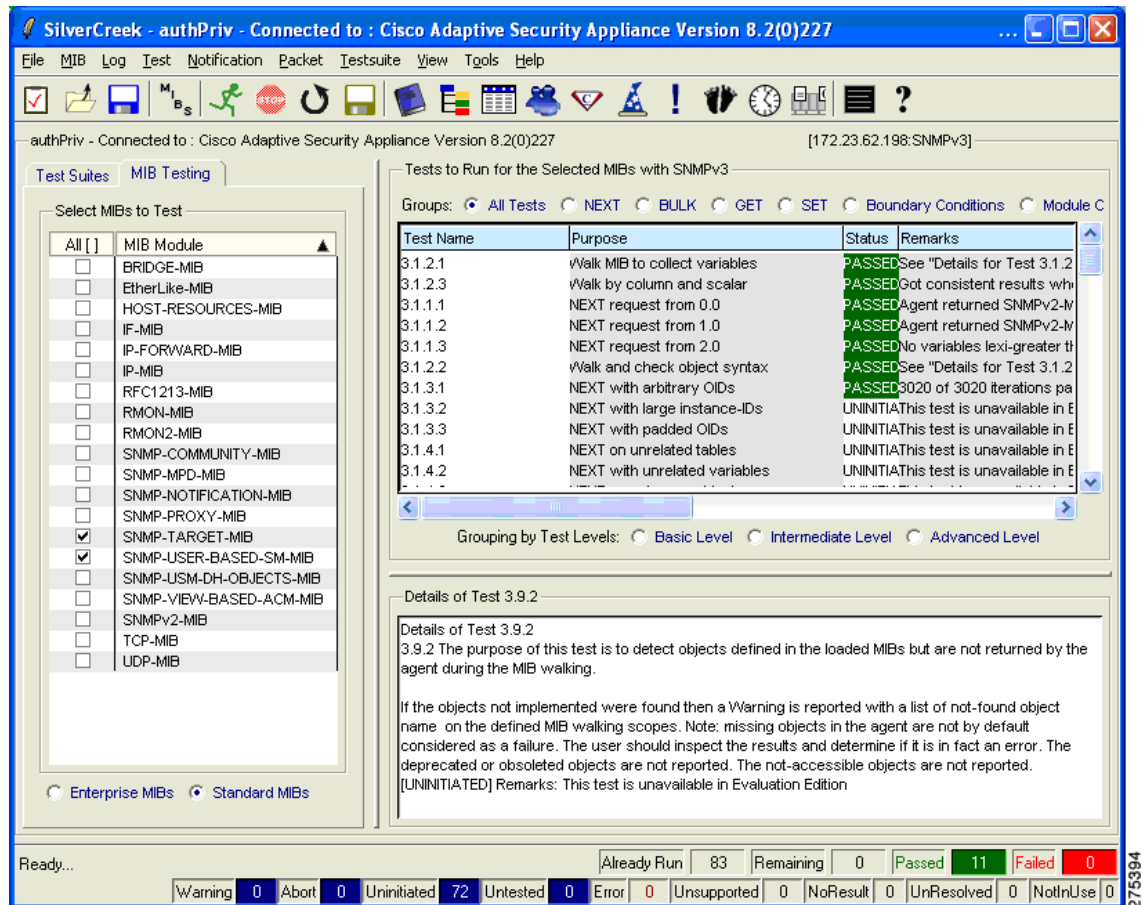
**Figure 2-9 Console Dialog Box Listing Debugging Messages**

## 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 (see [Figure 2-10](#)).
- 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 2-10 SilverCreek Main Window Showing MIB Testing Details



## Accessing the MIB Browser

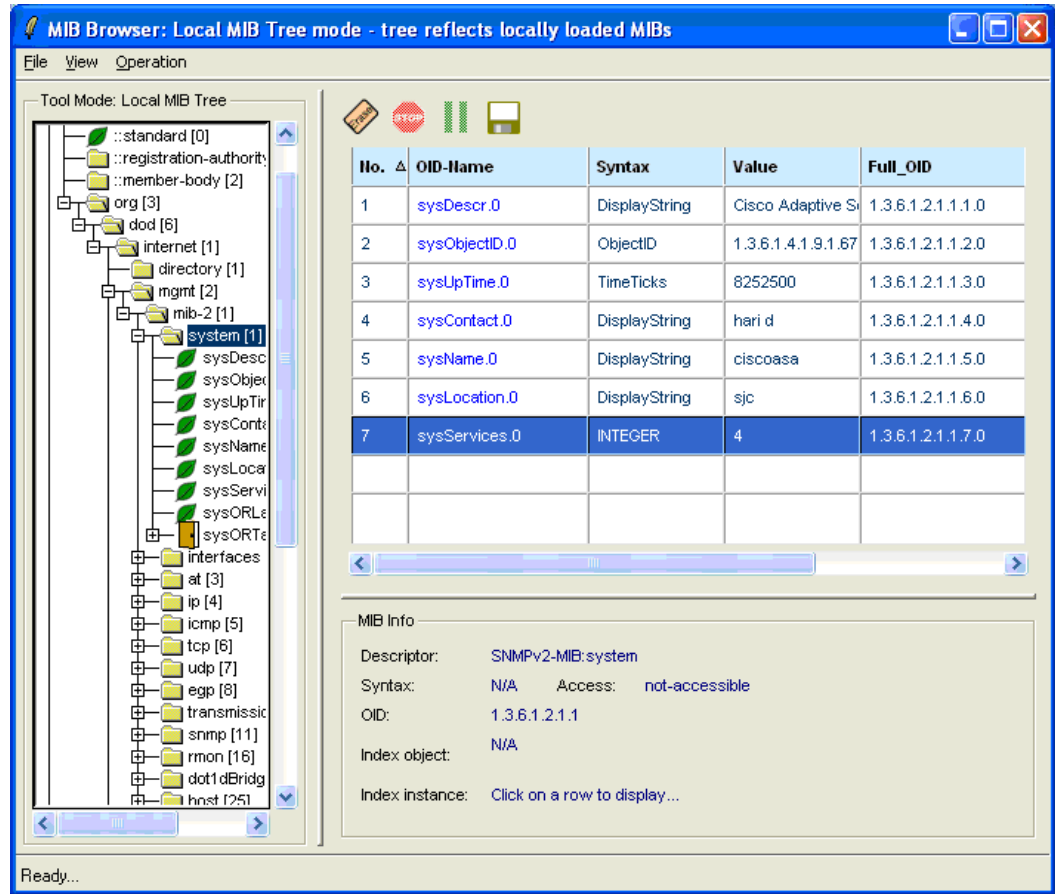
To access the MIB Browser, perform the following steps:

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

The MIB Browser (see [Figure 2-11](#)) provides more detailed access to the agent MIBs, including the ability to poll an individual MIB, walk a selected tree, and so on.



Figure 2-12 MIB Browser: Local MIB Tree Mode Dialog Box Showing MIB Results



**Note**

See the *Release Notes for the Cisco ASA 5500 Series Version 8.2(1)* 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:

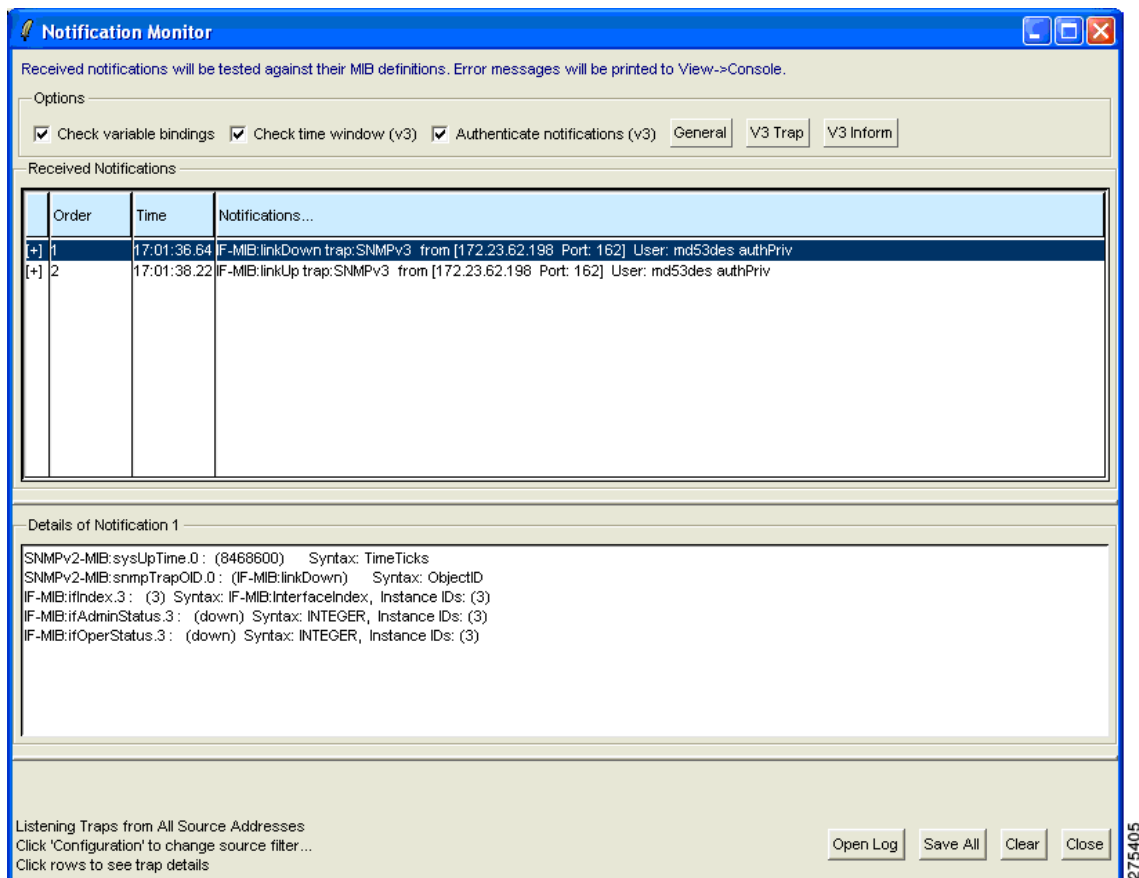
- Step 1** In the main window, choose **Notifications >Notifications Monitor**.
- Step 2** To configure the agent-specific information, click **V3 Inform**.

The Received Notifications dialog box (see Figure 2-13) 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 2-13 Notification Monitor Dialog Box



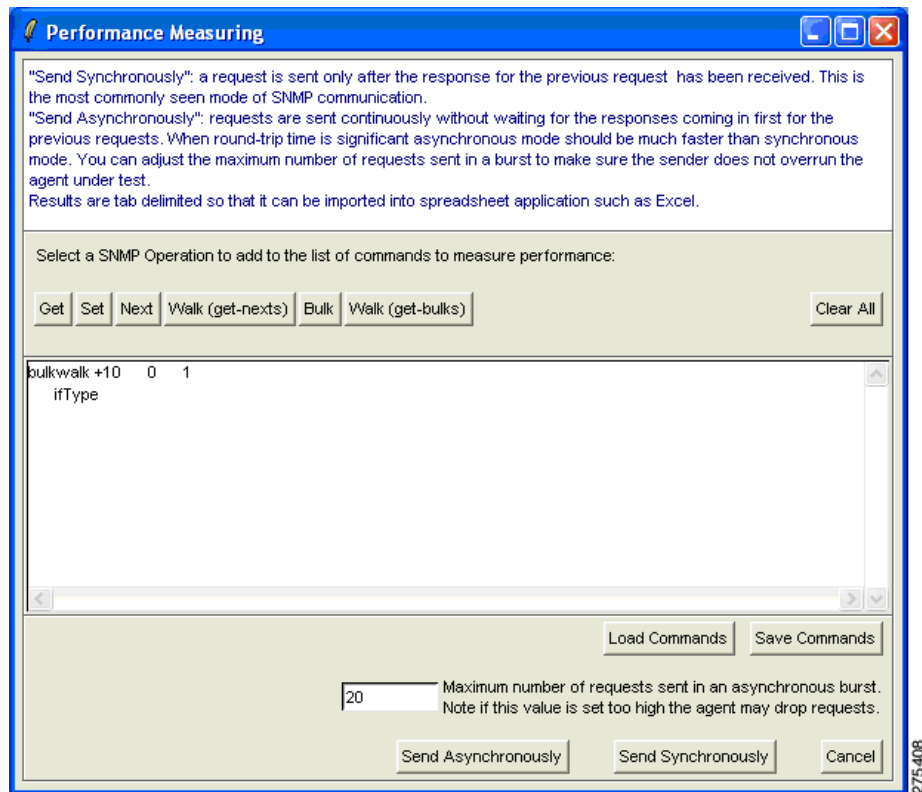
## Testing Performance

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 (see [Figure 2-14](#)) uses ifType, asks how many times you want to repeat the operation, and uses the value, 10.

Figure 2-14 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:

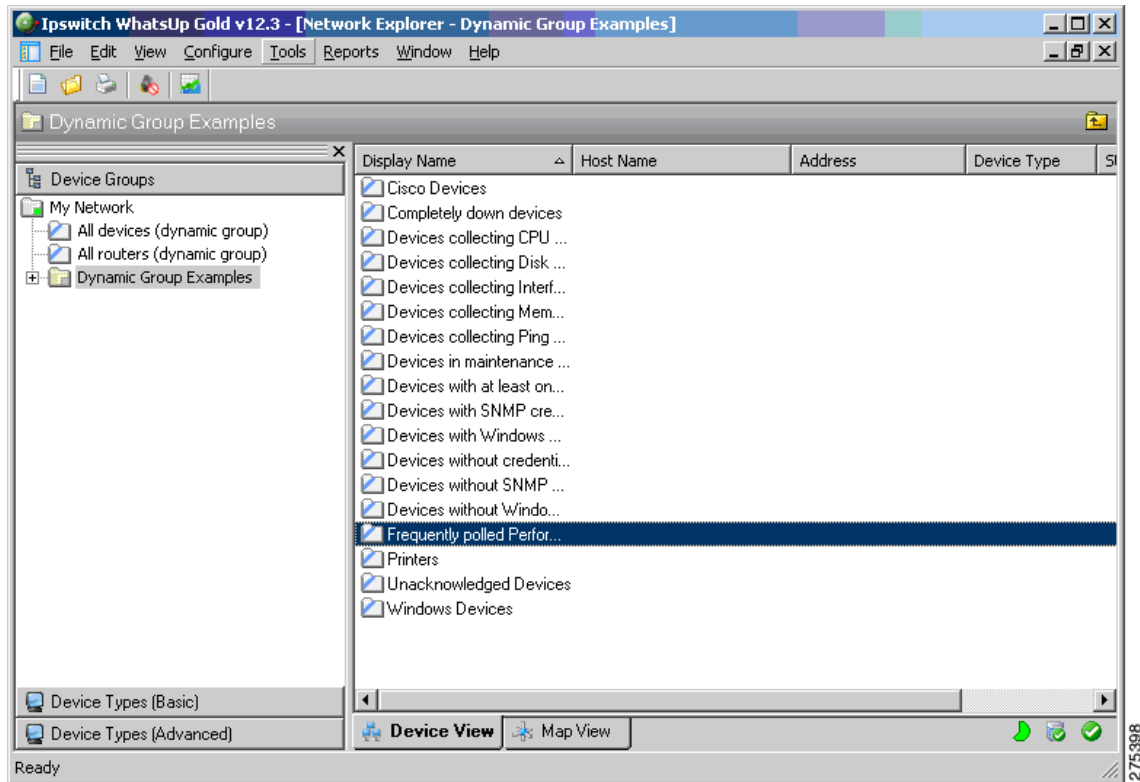
- [Starting Ipswitch WhatsUp Gold, page 2-17](#)
- [Adding a New SNMP Agent, page 2-18](#)
- [Adding SNMP Version 3 Credentials, page 2-19](#)
- [Using the WhatsUp Gold Web Interface, page 2-22](#)
- [Walking an SNMP MIB or an OID, page 2-23](#)
- [Configuring SNMP Traps, page 2-27](#)

## 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 (see [Figure 2-15](#)).

Figure 2-15 Network Explorer Main Window



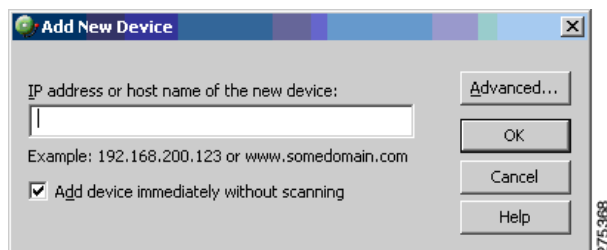
## Adding a New SNMP Agent

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

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

The Add New Device dialog box appears (see [Figure 2-16](#)).

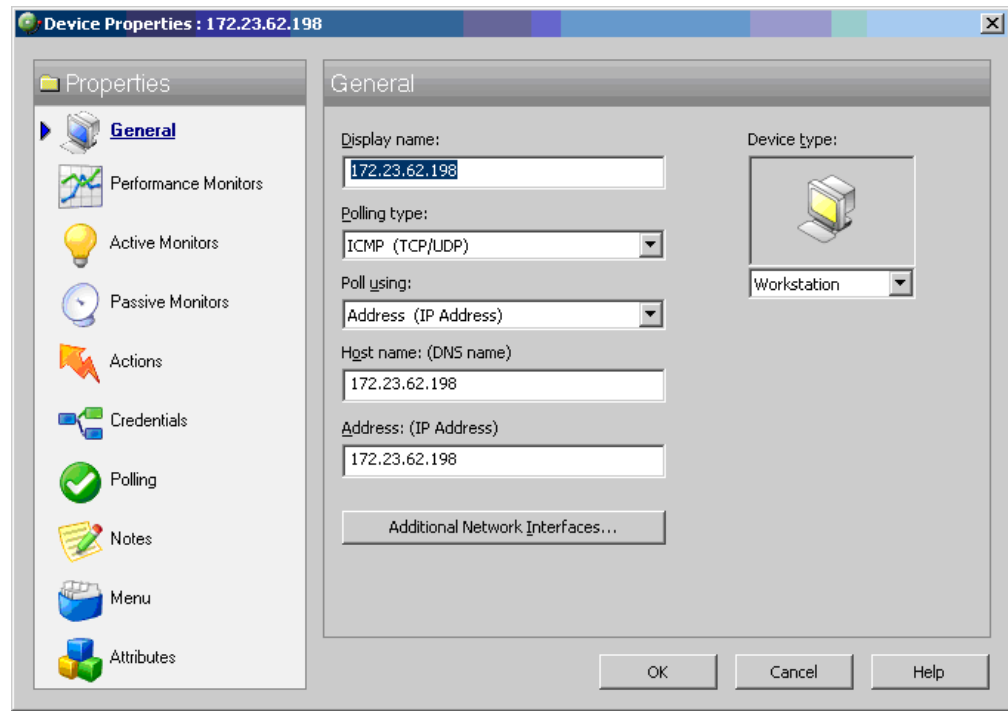
Figure 2-16 Add New Device Dialog Box



- 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 [Figure 2-17](#).

Figure 2-17 Device Properties Dialog Box

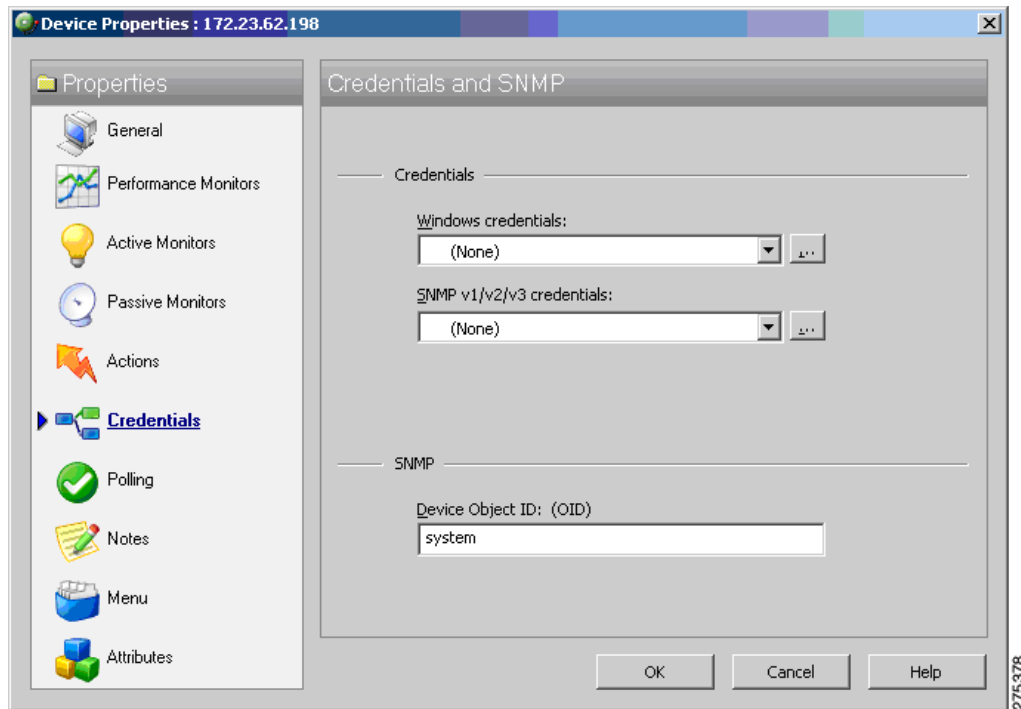


## Adding SNMP Version 3 Credentials

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

- Step 1** Click the **Credentials** link (see [Figure 2-18](#)), and enter the SNMP device object ID information.

**Figure 2-18** 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** (see [Figure 2-19](#) and [Figure 2-20](#)).

**Figure 2-19** Edit SNMP v3 Credential Type Dialog Box

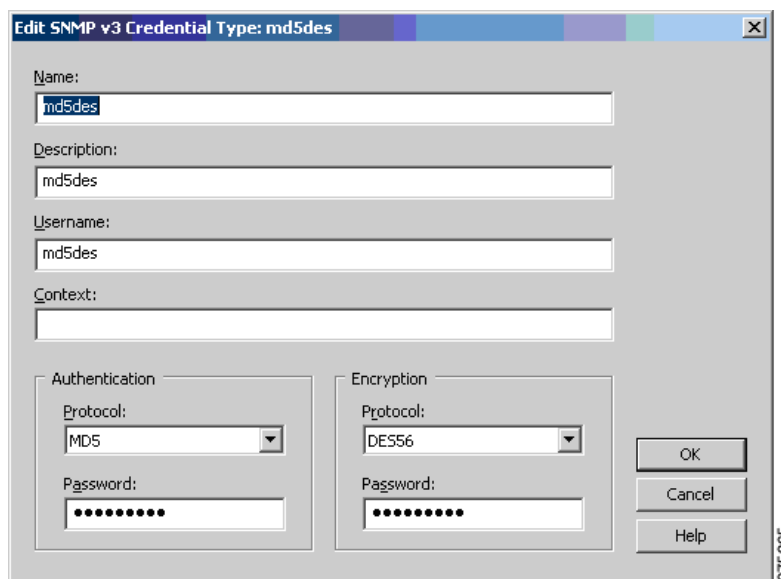


Figure 2-20 Credentials Library Dialog Box

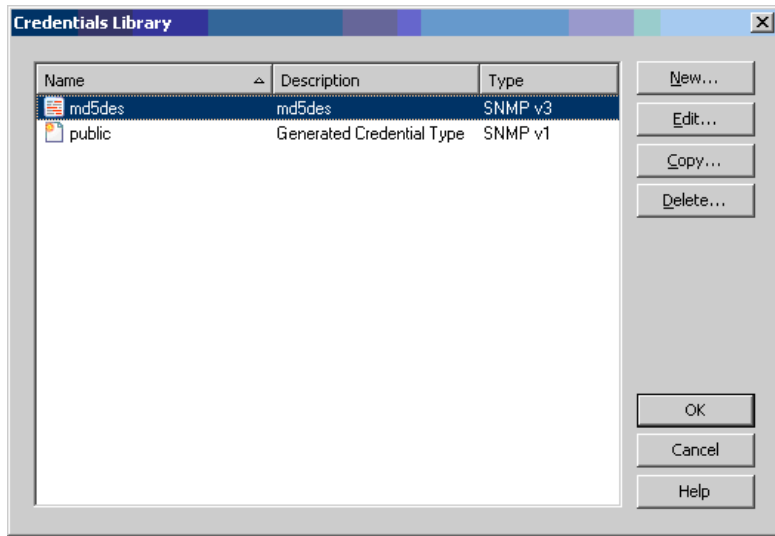
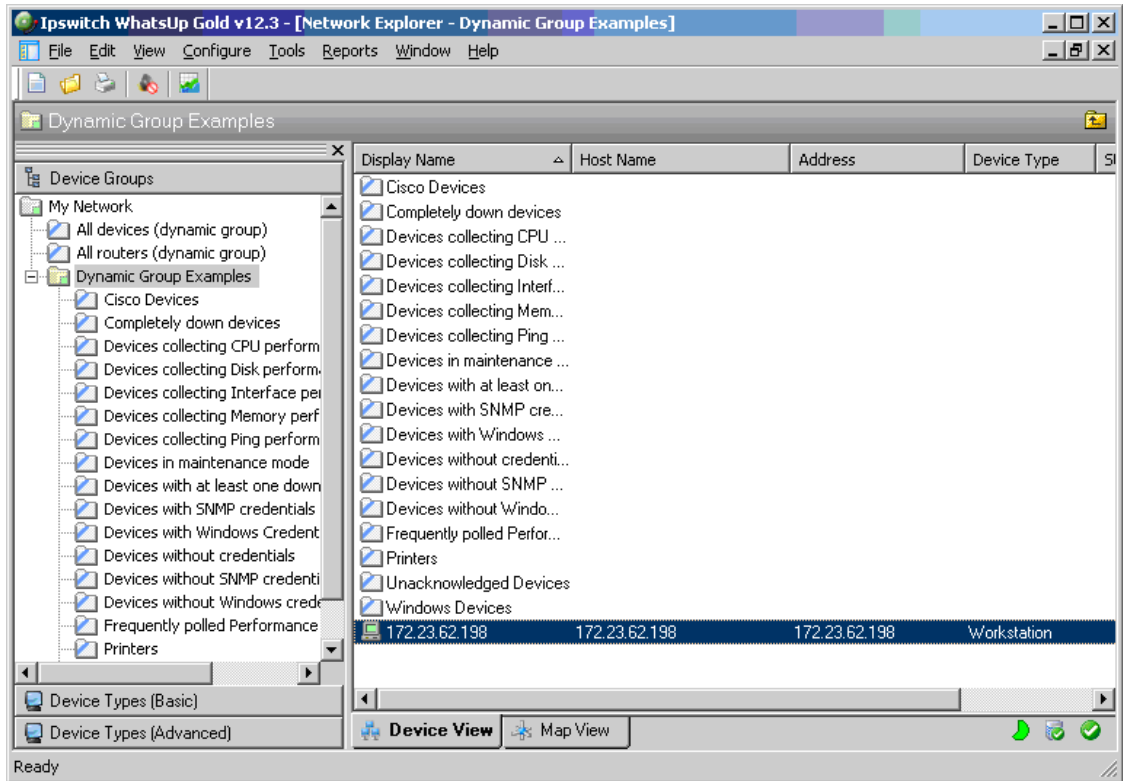


Figure 2-21 shows the added SNMP Version 3 node on the network.

Figure 2-21 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:

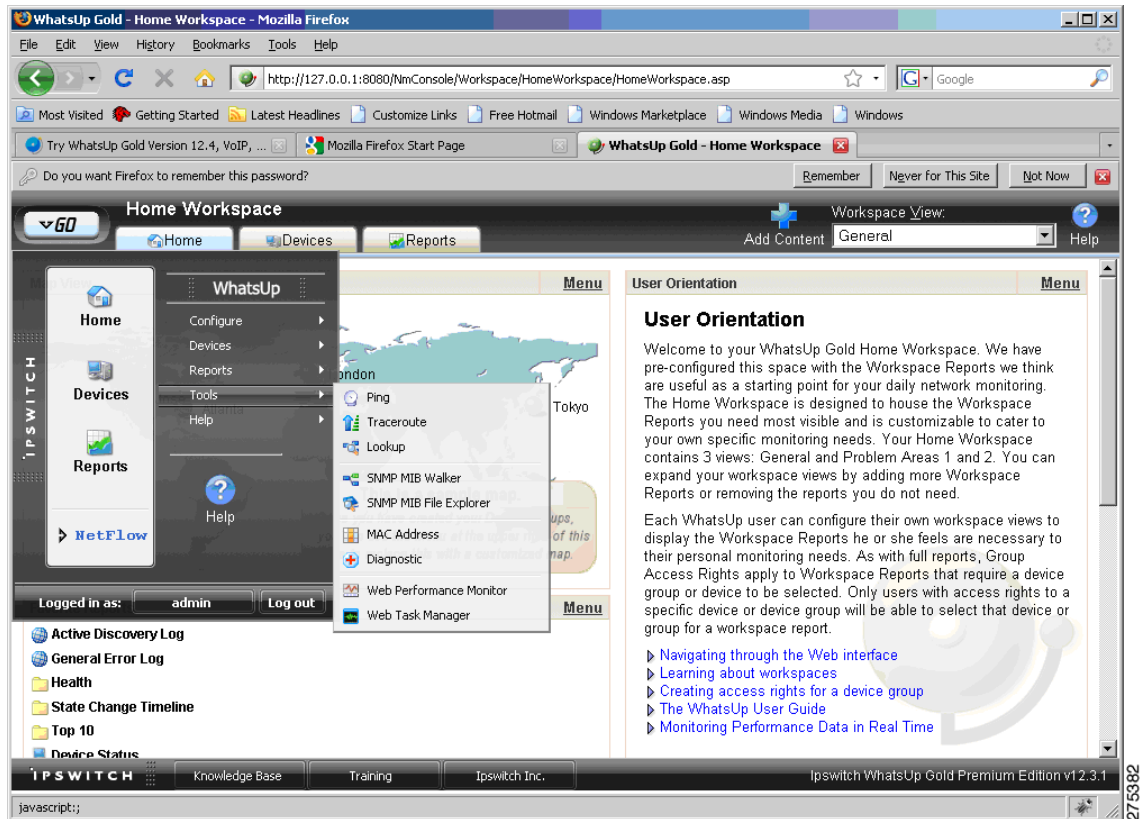
- Step 1** Choose **Start > Programs > Ipswitch WhatsUp Gold v12.3 > WhatsUp Web Interface**. You can perform SNMP Version 3 walks and polls from this location.
- Step 2** [Figure 2-22](#) shows the initial login window. Enter the default username and password, which is “admin.”

**Figure 2-22** *WhatsUp Gold Login Window for Web Interface*



[Figure 2-23](#) shows the Home Workspace pane that appears after the user logs in.

Figure 2-23 WhatsUp Gold Home Workspace Pane



## Walking an SNMP MIB or an OID

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

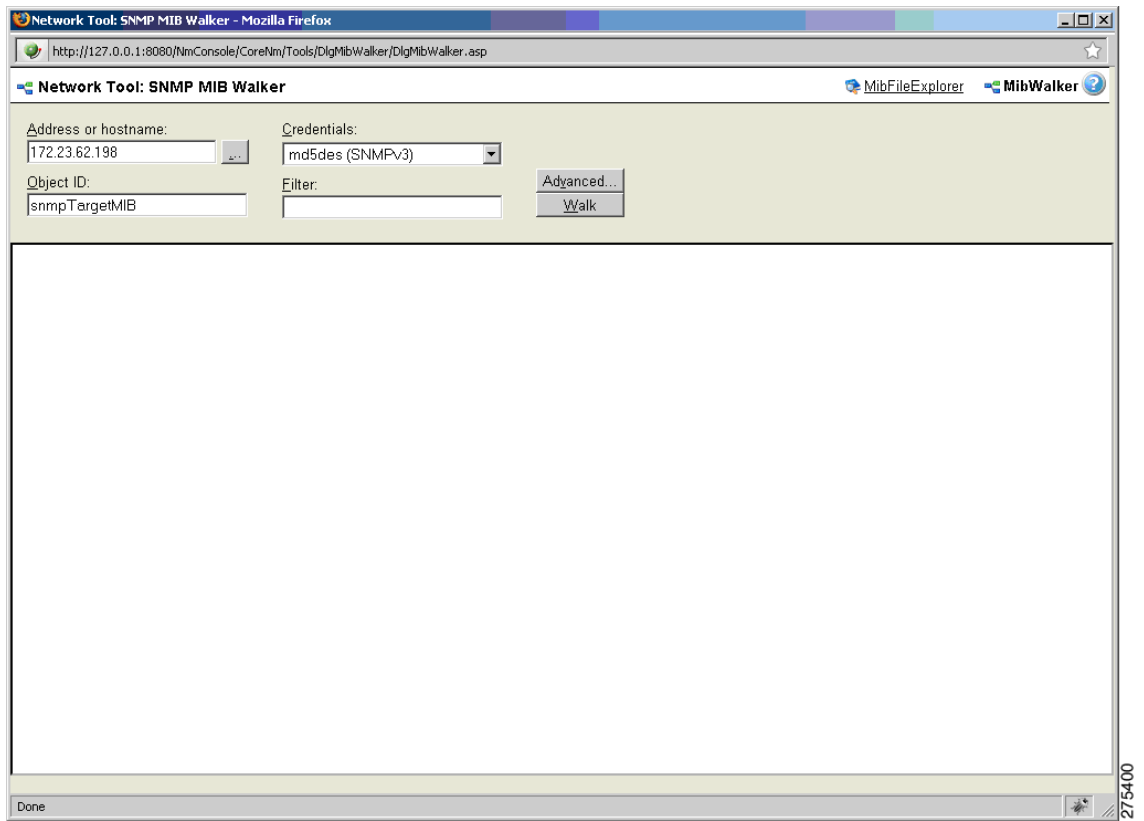
- Step 1** Choose **GO > Tools > SNMP MIB Walker** (see [Figure 2-24](#)).

Figure 2-24 SNMP MIB Walker Menu Option



**Step 2** In the Network Tool: SNMP MIB Walker dialog box (see Figure 2-25), 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 2-25 Network Tool: SNMP MIB Walker Dialog Box**

**Step 3** Click Walk.

Figure 2-26 shows the walk results in a tree format.

**Figure 2-26 Network Tool: SNMP MIB Walker Results - Tree View**

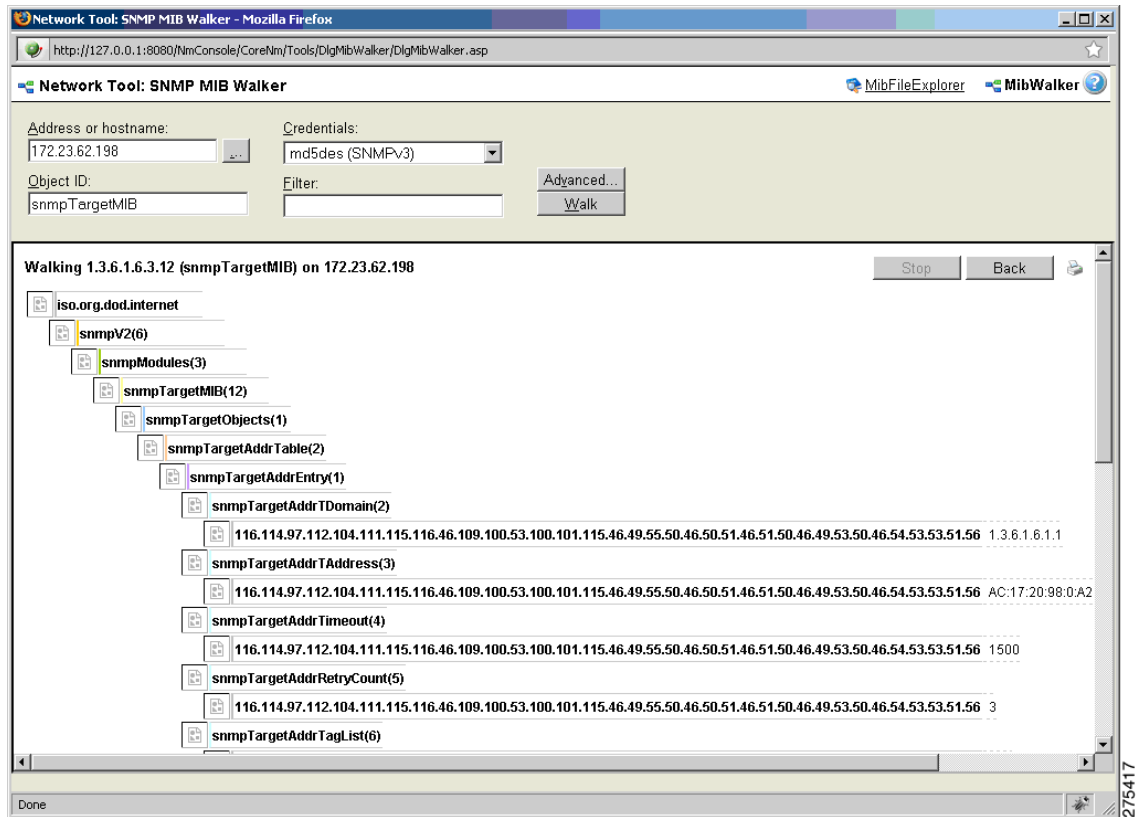
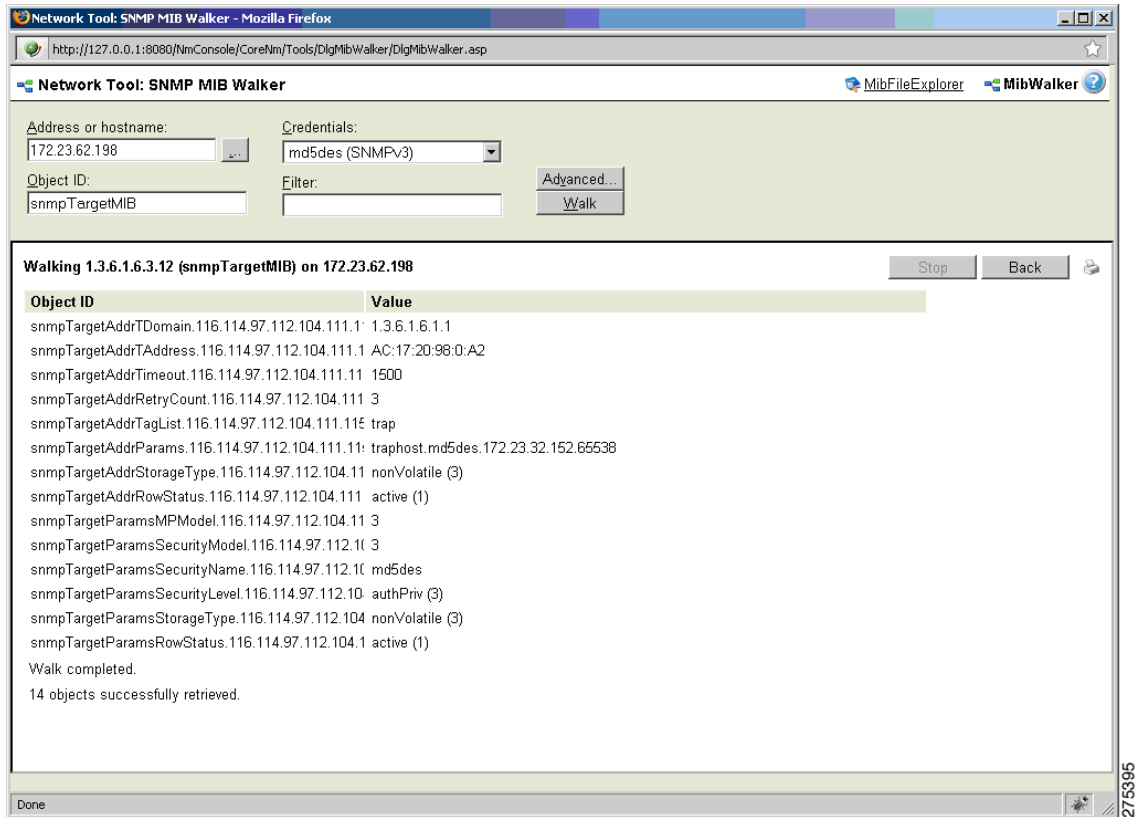


Figure 2-27 shows the results in sequence.

Figure 2-27 Network Tool: SNMP MIB Walker Results Window

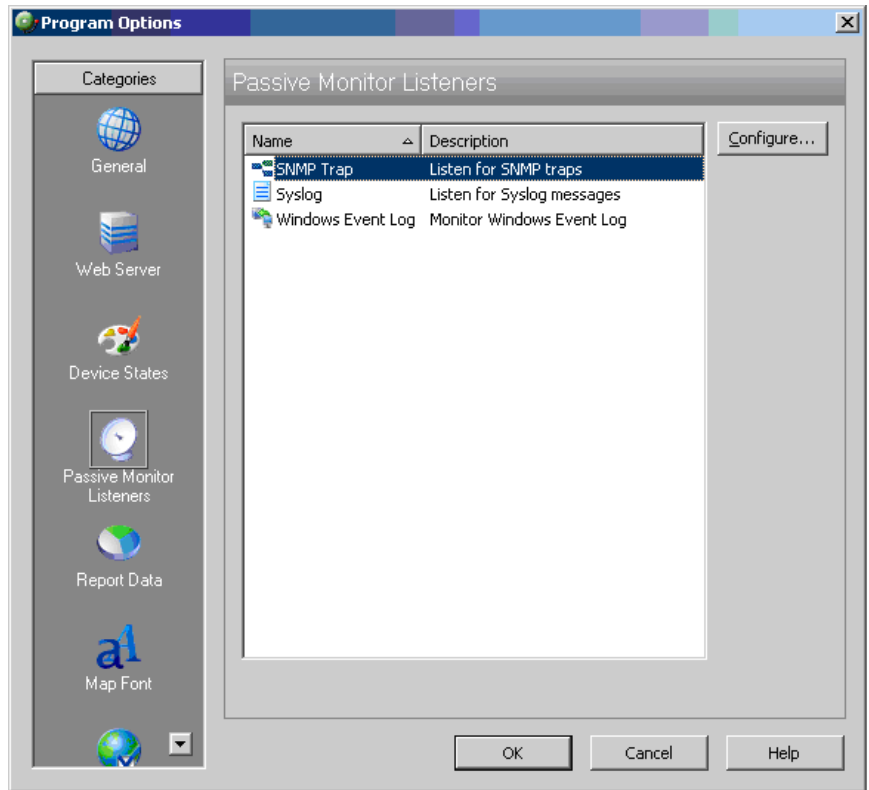


## Configuring SNMP Traps

To configure SNMP traps, perform the following steps:

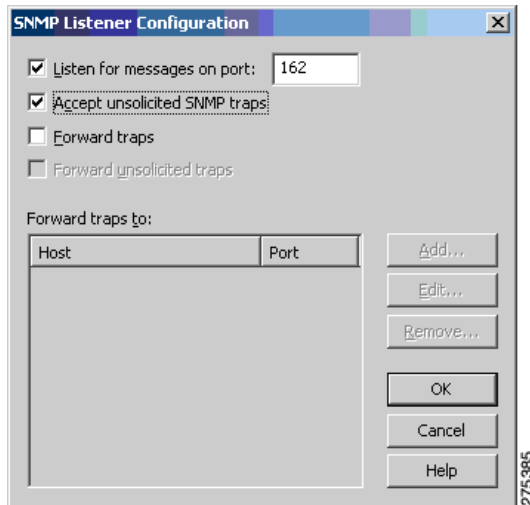
- Step 1** Choose **Program Options > Passive Monitor Listeners > SNMP Trap > Configure** (see [Figure 2-28](#)).

**Figure 2-28** Program Options – Passive Monitor Listeners Dialog Box



The SNMP Listener Configuration dialog box appears (see [Figure 2-29](#)). From here you can configure the listener port and forward traps to a host.

**Figure 2-29** SNMP Listener Configuration Dialog Box



**Step 2** Click the **Reports** tab and select **SNMP Trap Log** (see [Figure 2-30](#)).

Figure 2-30 SNMP Reports Pane

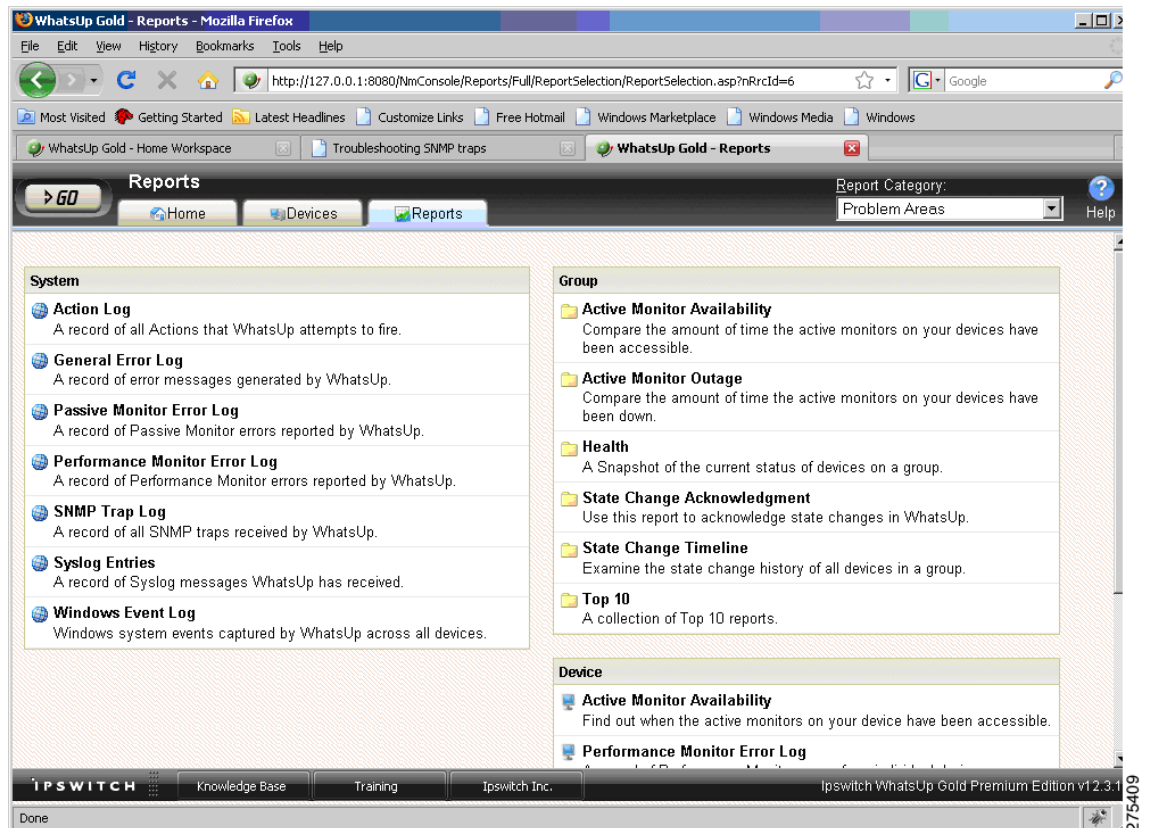
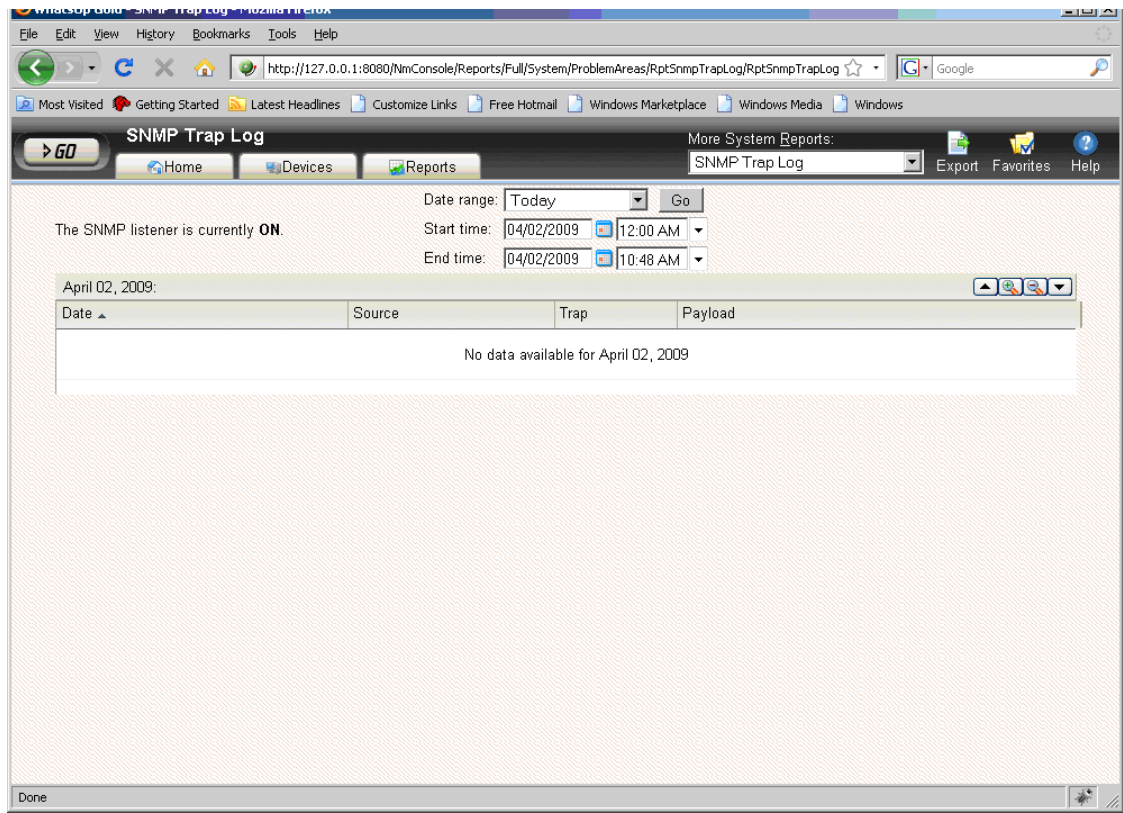


Figure 2-31 shows the SNMP trap log.

Figure 2-31 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 adaptive security appliance is integrated into the HP NNM device topology, and communicates device statistics and SNMP traps using SNMP Version 3.



### Note

See the *Cisco ASA 5500 Series Adaptive Security Appliance Version 8.2(1) Release Notes* for a list of the open caveats that apply to NNM 8.x.

This section includes the following topics:

- [Installing NNM, page 2-31](#)
- [Starting the NNM, page 2-31](#)
- [Loading MIBs, page 2-32](#)
- [Adding a Network to the Current Map, page 2-33](#)
- [Configuring Specific SNMP Version 3 Parameters, page 2-36](#)
- [Setting Global SNMP Version 3 Credentials, page 2-37](#)

- [Viewing Node Information, page 2-38](#)
- [Configuring the NNM MIB Browser, page 2-39](#)
- [Using the HP OpenView NNM Web Application, page 2-44](#)

## 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=1-11-15-119^1155\\_4000\\_100\\_\\_](https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119^1155_4000_100__)

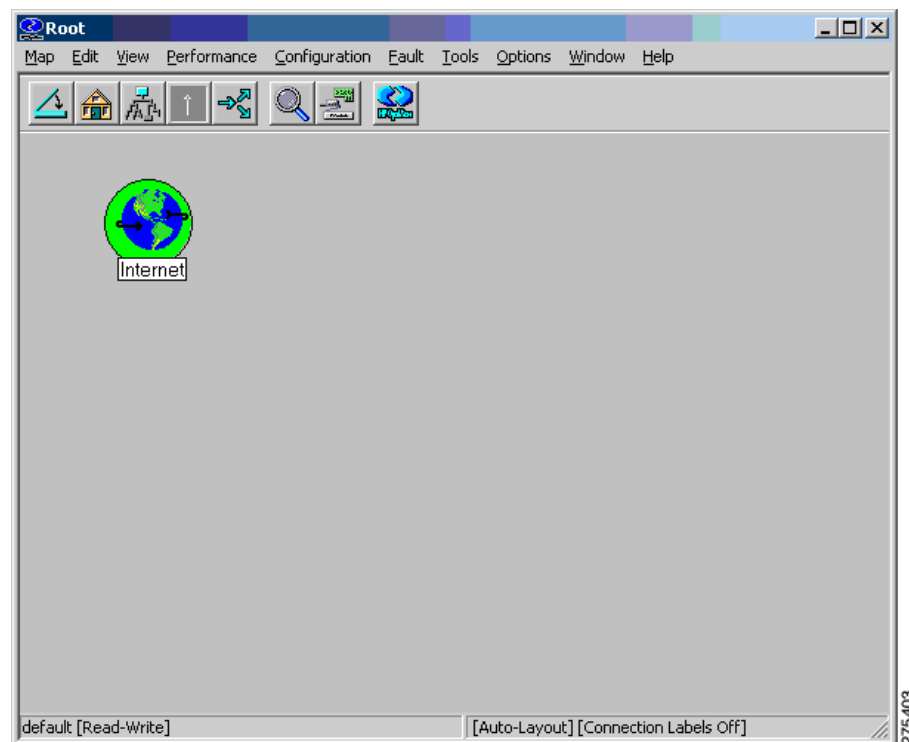
## Starting the NNM

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 (see [Figure 2-32](#)).

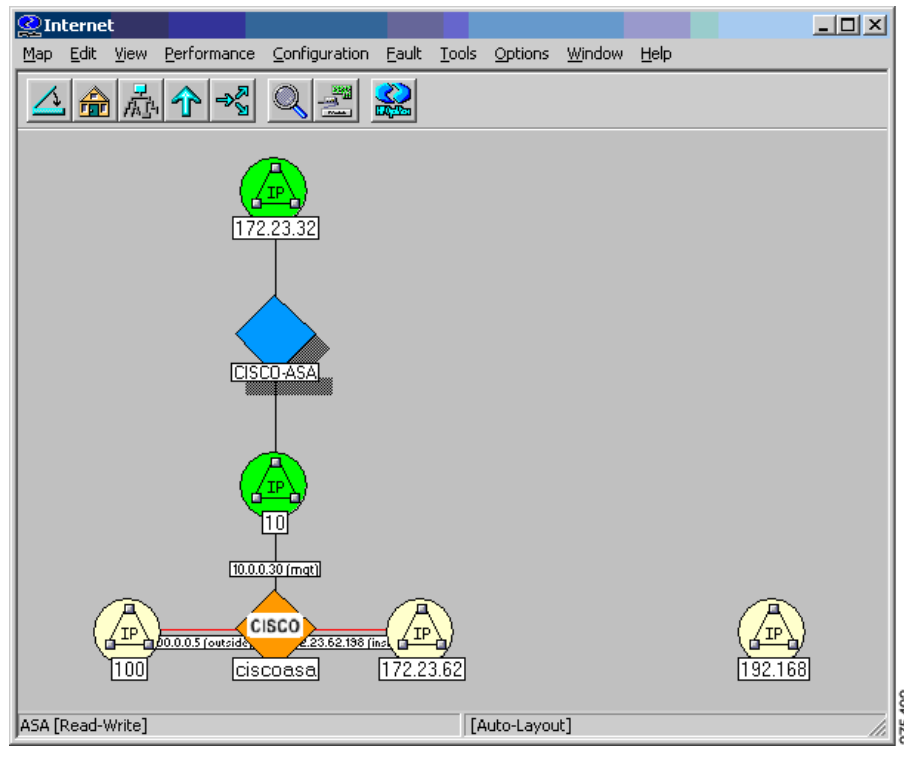
**Figure 2-32** NNM Console Root Window



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

The Internet window appears, with the network nodes displayed (see [Figure 2-33](#)).

**Figure 2-33** NNM Console Internet Window Showing Network Nodes

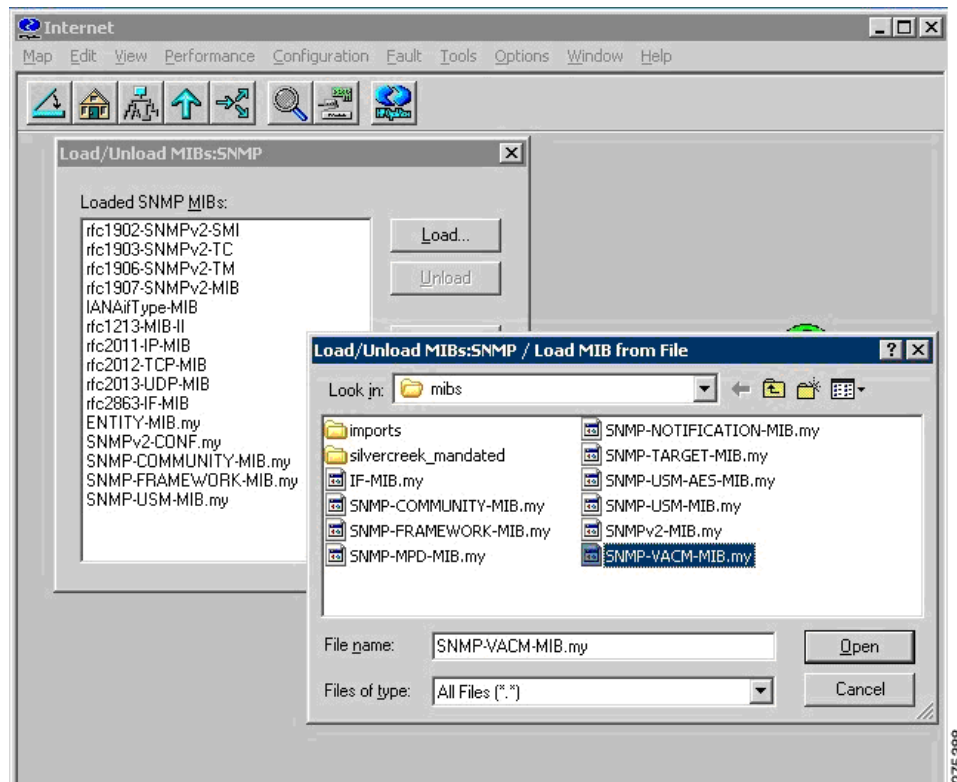


## Loading MIBs

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 (see [Figure 2-34](#)).

Figure 2-34 Load/Unload MIBs: SNMP Dialog Box

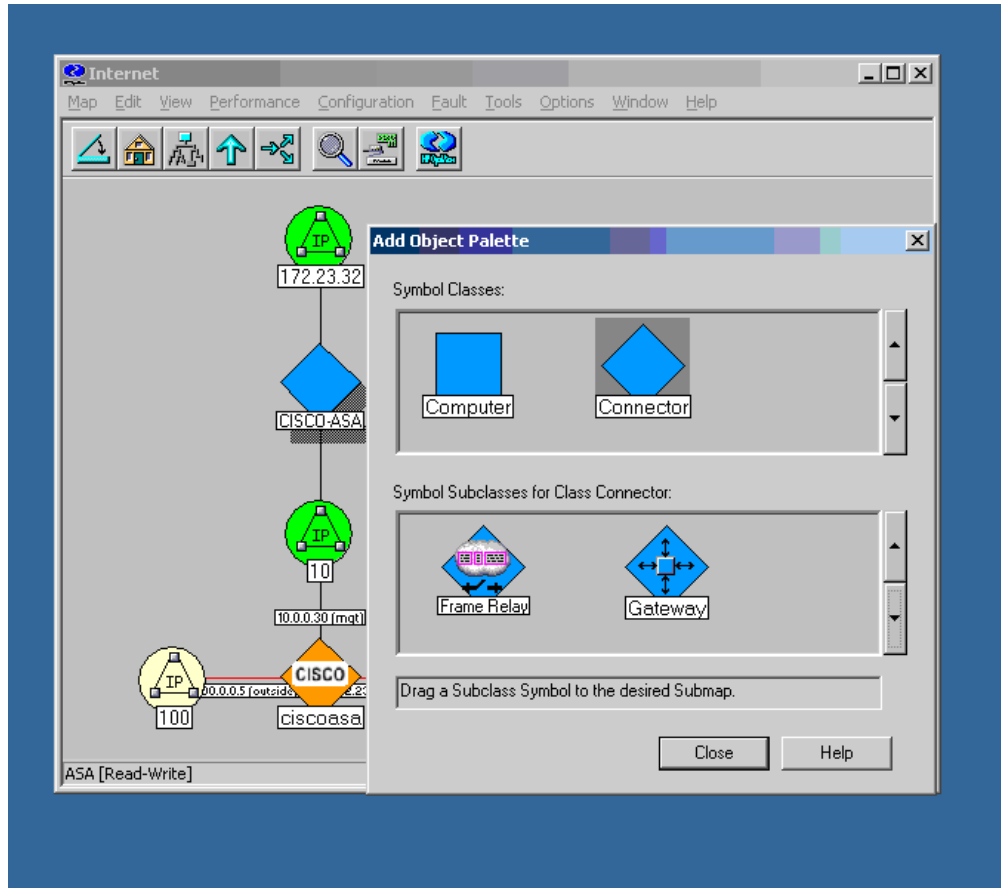


## Adding a Network to the Current Map

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 (see [Figure 2-35](#)).

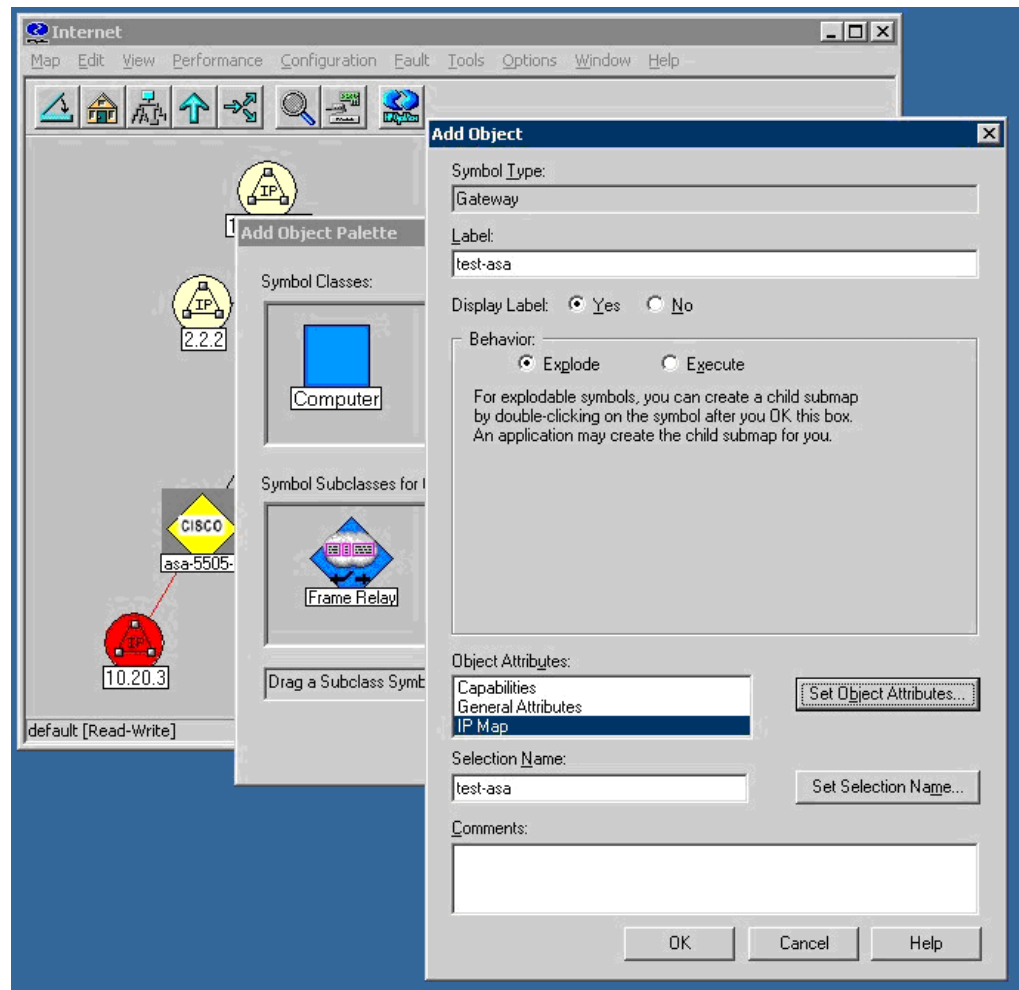
Figure 2-35 Add Object Palette Dialog Box



- 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.

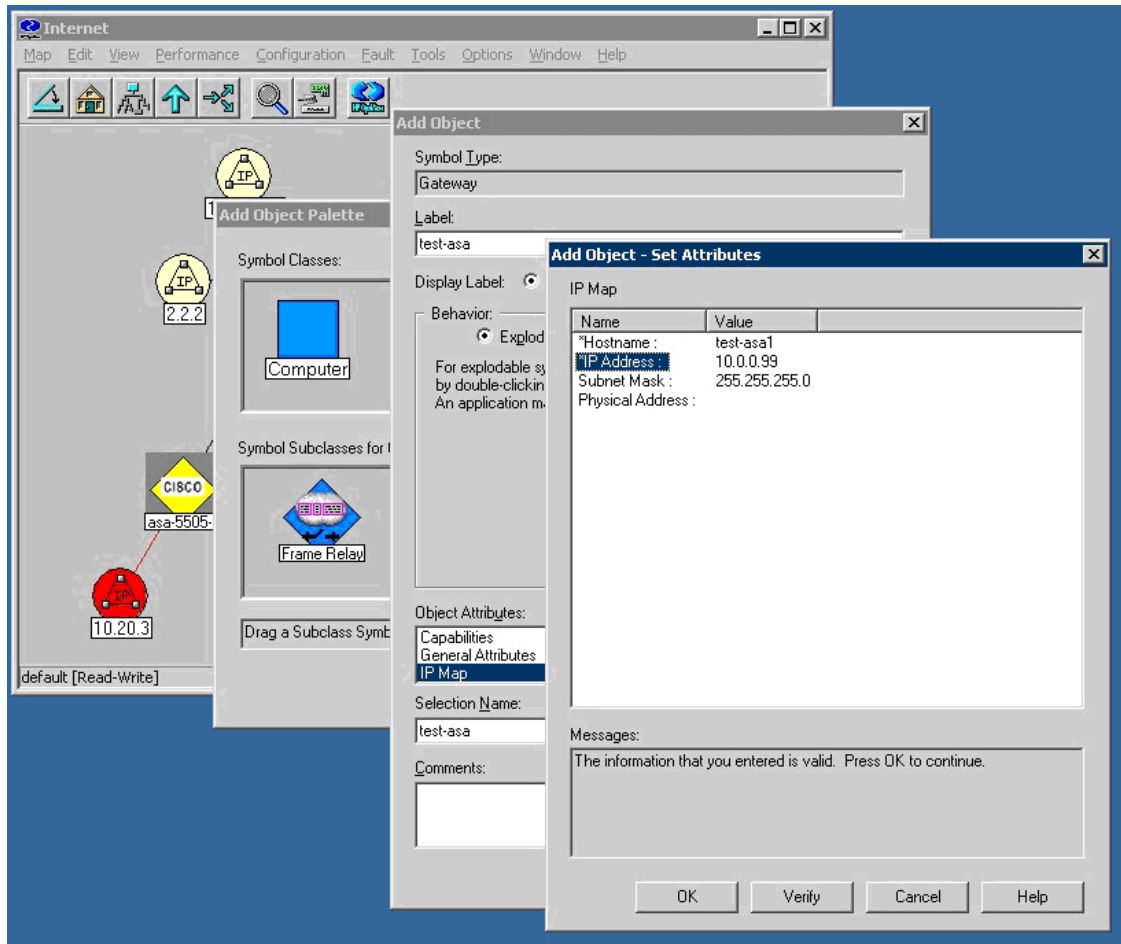
The Add Object dialog box appears (see [Figure 2-36](#)).

Figure 2-36 Add Object Dialog Box

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

The Add Object – Set Attributes dialog box appears (see [Figure 2-37](#)).

Figure 2-37 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.

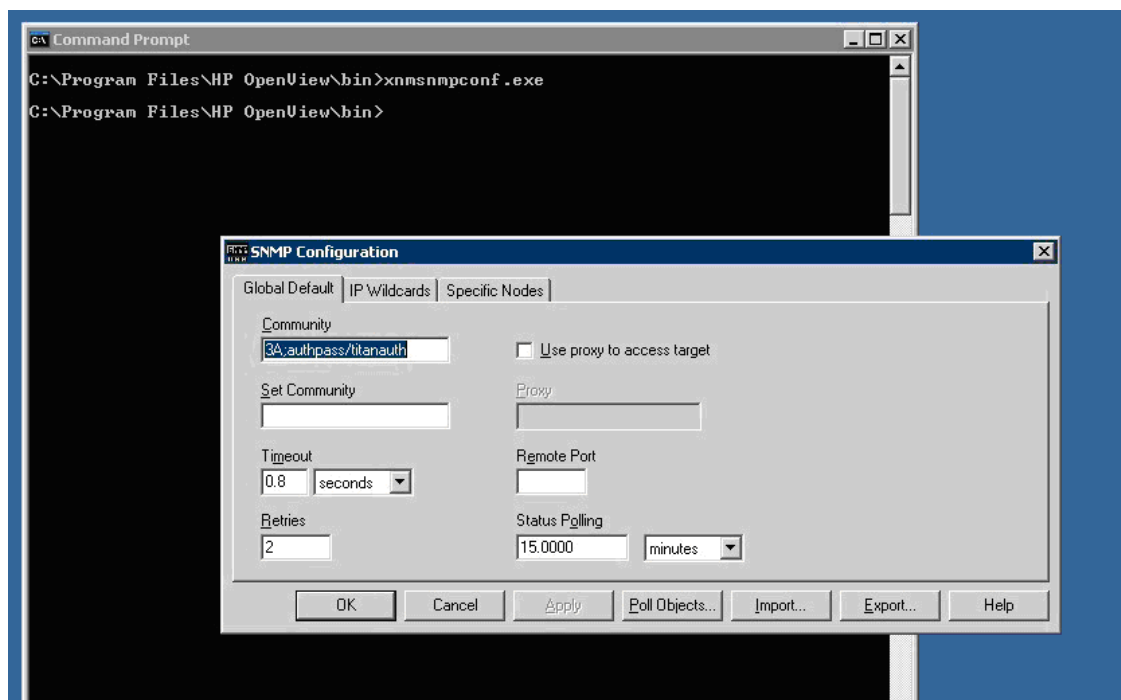
**Note**

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” section on page 2-39.

## 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 (see Figure 2-38). For the format of the community string, see Step 2 in the “Configuring the NNM MIB Browser” section on page 2-39.

**Figure 2-38** SNMP Configuration

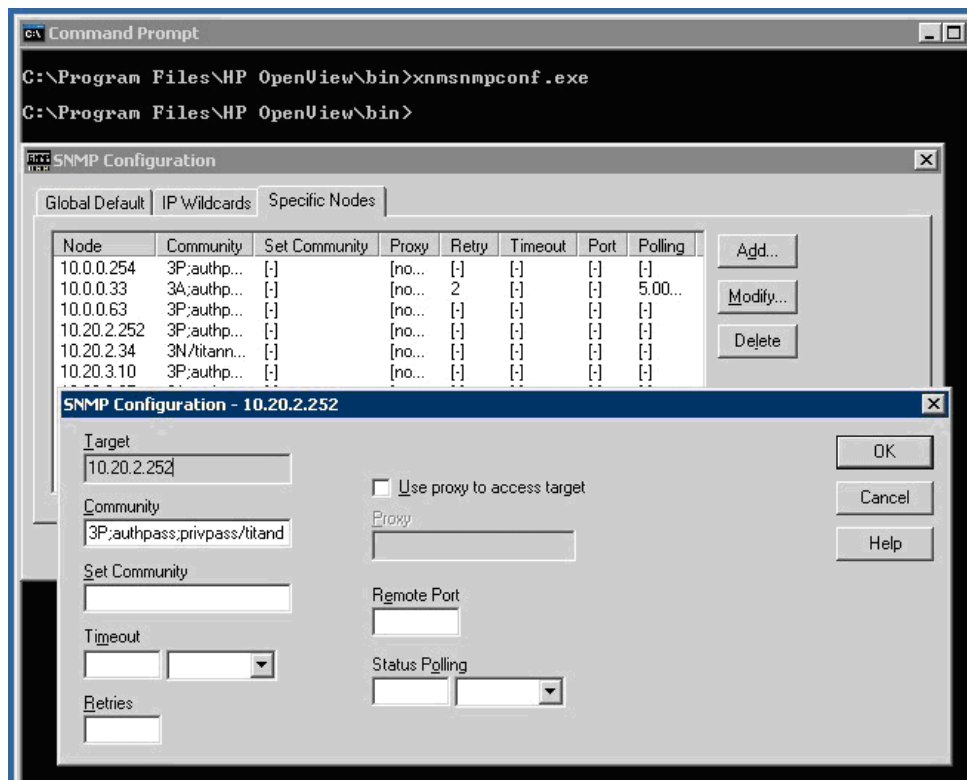


275372

## 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 (see Figure 2-39).

Figure 2-39 SNMP Configuration Dialog Box



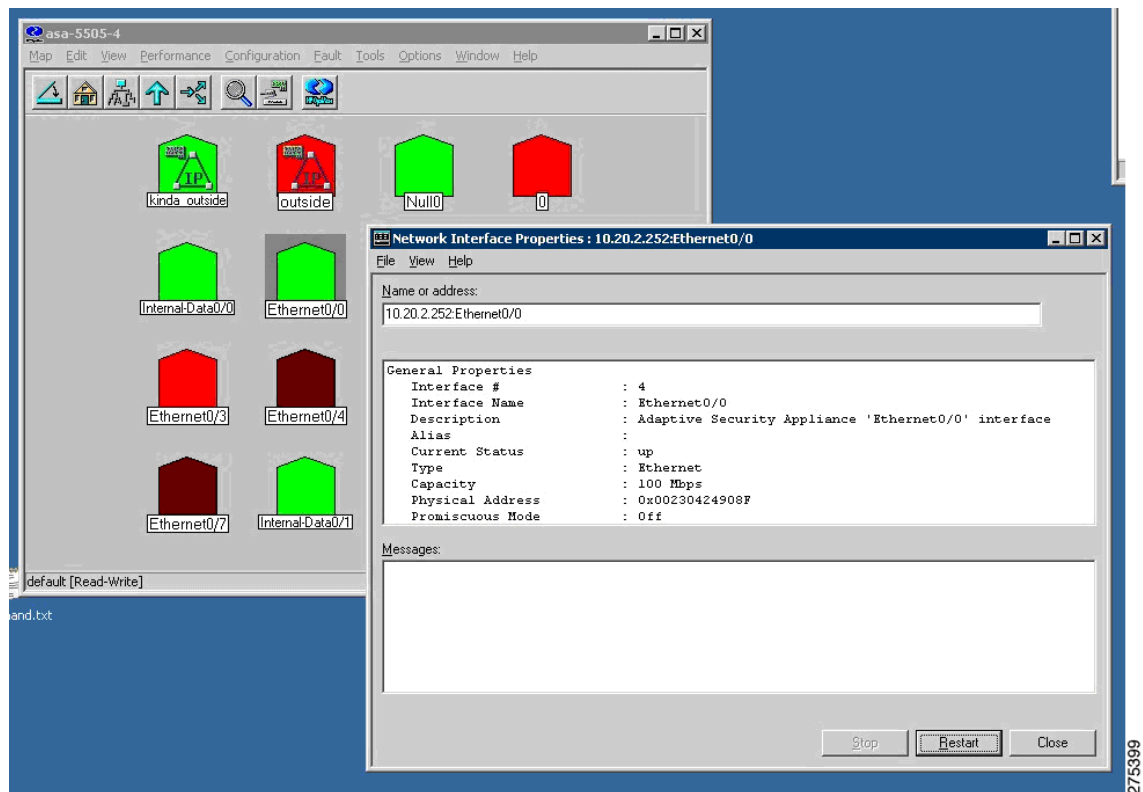
## Viewing Node Information

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 (see [Figure 2-40](#)).

Figure 2-40 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, page 2-40](#)
- [Configuring SNMP Version 3 MD5 Auth/No-priv Connections, page 2-40](#)
- [Configuring SNMP Version 3 SHA Auth/No-priv Connections, page 2-40](#)
- [Configuring SNMP Version 3 MD5 Auth/Priv Connections, page 2-41](#)
- [Configuring SNMP Version 3 SHA Auth/Priv Connections, page 2-41](#)
- [Browsing a MIB, page 2-41](#)
- [Running a MIB Browser Packet Trace, page 2-42](#)
- [Using the NNM SNMP Version 3 Trap Viewer, page 2-43](#)

## 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**.
- 

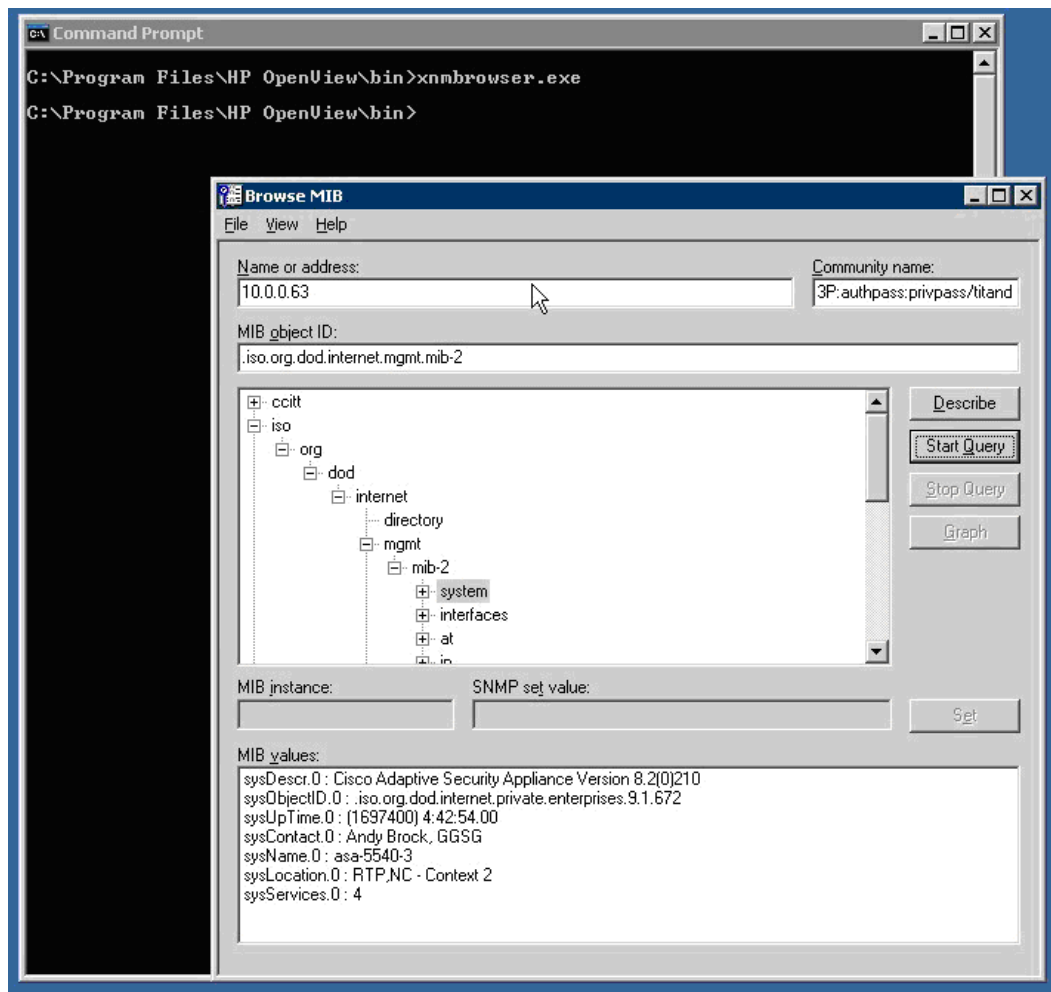
## Browsing a MIB

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 (see [Figure 2-41](#)).
-

Figure 2-41 Browse MIB Dialog Box

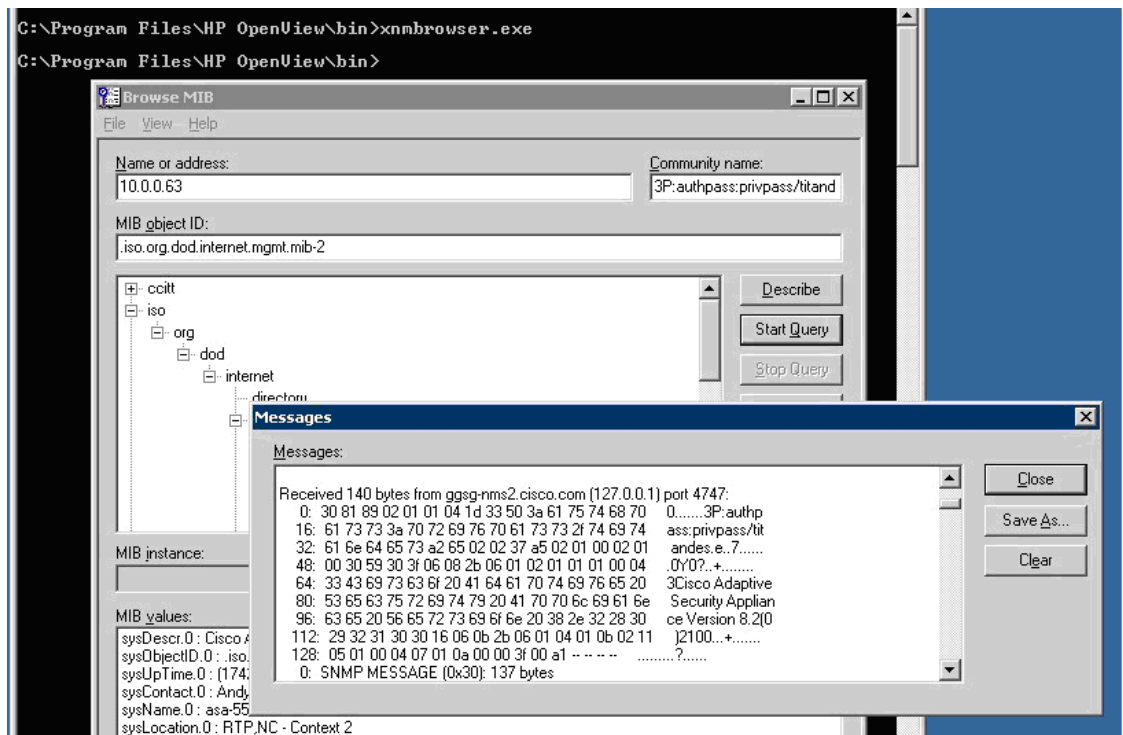


## Running a MIB Browser Packet Trace

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

The Messages dialog box appears (see [Figure 2-42](#)), which shows the packet contents of the SNMP communication between the MIB Browser and the SNMP agent. This information is helpful for debugging.

Figure 2-42 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\sconf\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 adaptive security appliance:

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



**Note** The command syntax may differ slightly between adaptive security appliance 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” section on page 2-39.

The NNM trapcv 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 trapcv 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 trapcv utility and wait for traps on the SNMP agent. The utility is available at the following location (see Figure 2-43): C:\Program Files\HP OpenView\snmpv3\utils\trapcv.exe.

**Figure 2-43** SNMP Trap Receiver

```
C:\Program Files\HP OpenView\snmpv3\utils>trapcv
Waiting for traps.

Received SNMPv3 authPriv Trap:
From: 10.20.2.252:162
sysUpTime.0 = 1564600
snmpTrapOID.0 = snmpTraps.3
ifIndex.8 = 8
ifAdminStatus.8 = down(2)
ifOperStatus.8 = down(2)

Received SNMPv3 authPriv Trap:
From: 10.20.2.252:162
sysUpTime.0 = 1564700
snmpTrapOID.0 = snmpTraps.4
ifIndex.8 = 8
ifAdminStatus.8 = up(1)
ifOperStatus.8 = up(1)
```

## 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://<NNM-Server-IP-Address>:7510/topology/home
- Step 2** To view SNMP nodes, from the drop-down menu, choose **Internet View** (see Figure 2-44).  
The Internet View window appears (see Figure 2-45).

Figure 2-44 NNM Home Base Window

File Edit View History Bookmarks Tools Help http://172.18.154.102:7510/topology/home

## Network Node Manager Home Base

You are currently running with a temporary license that expires on Mar 16, 2009 8:28:00 AM EDT. After that date, the number of nodes that can be managed is 0. For more license information, have the system administrator run %OV\_BIN%\ovnnmPassword on the server system, 172.18.154.102. Network Node Manager Starter Edition license will expire on Mar 16, 2009 8:28:00 AM EDT. Click [here](#) to get more information on obtaining a license.

View

Neighbor View  ?

- Neighbor View
- Node View
- Station View
- Internet View
- Network View
- Path View

representation of a selected device and its connector devices, within a specified scope from the selected device.

Node Status Summary Alarm Browser About

Node Status Summary as of Feb 11, 2009 11:29:22 AM EST

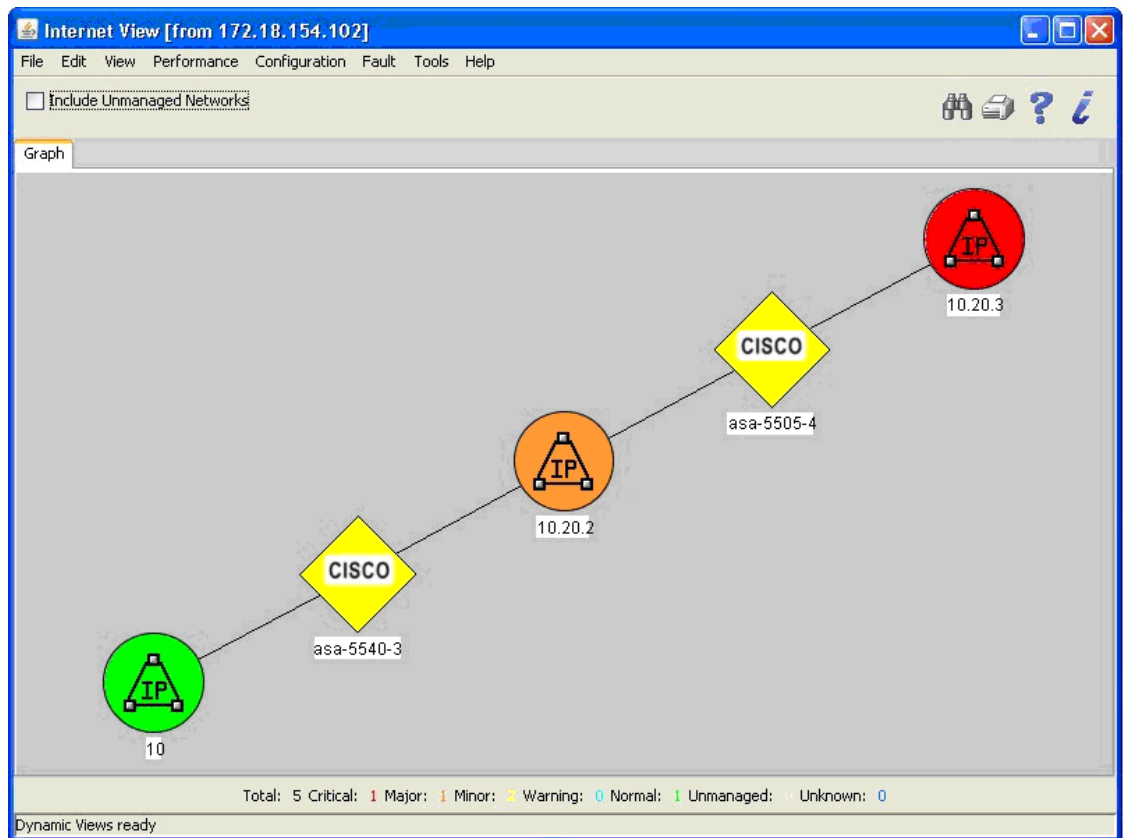
<span style="color: red;">■</span> Critical	: 0 (0%)
<span style="color: orange;">■</span> Major	: 0 (0%)
<span style="color: yellow;">■</span> Minor	: 2 (40%)
<span style="color: cyan;">■</span> Warning	: 0 (0%)
<span style="color: green;">■</span> Normal	: 3 (60%)
<span style="color: blue;">■</span> Unknown	: 0 (0%)
<b>Total</b>	<b>: 5</b>

Dynamic Views ready

NNM Release B.07.53  
Applet com.hp.ov.dynamicViews.gui.core.Dynamic... Idle

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

Figure 2-45 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:

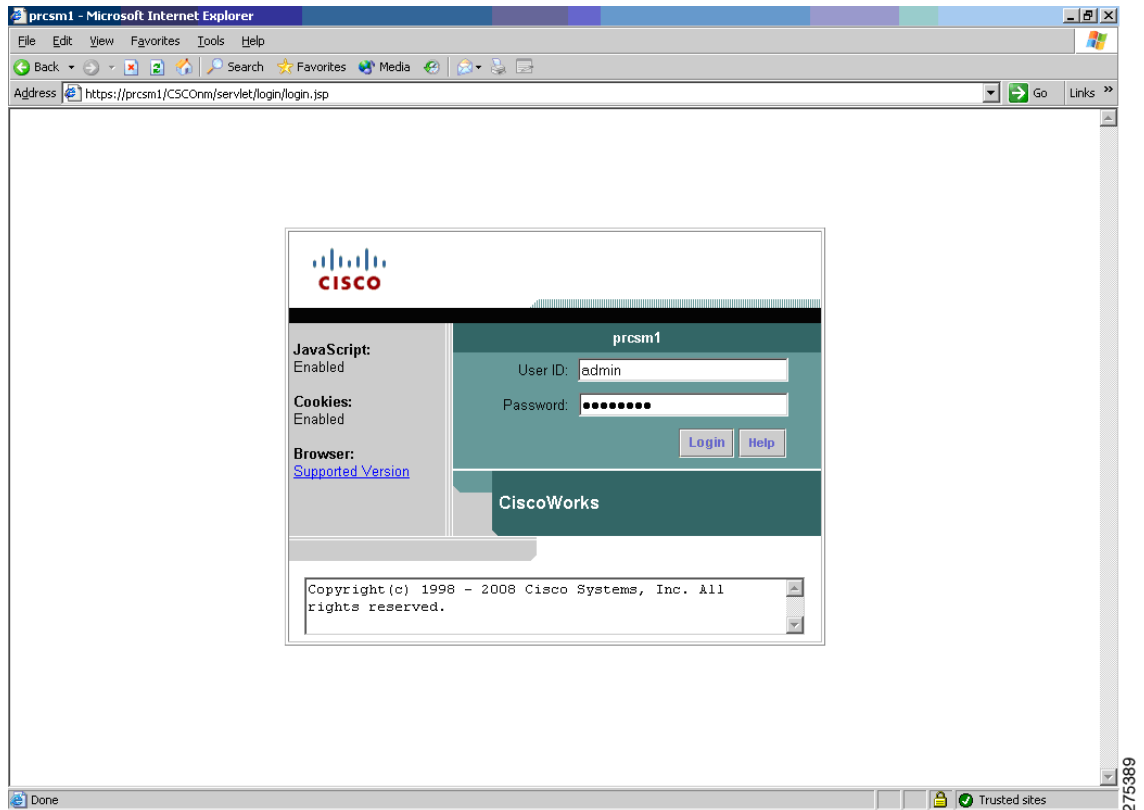
- [Starting CiscoWorks, page 2-47](#)
- [Getting Started with the CiscoWorks LMS Portal, page 2-47](#)
- [Using the Device Center, page 2-48](#)
- [Performing an SNMP Walk, page 2-49](#)
- [Using the Management Station to Device Tool, page 2-54](#)

## Starting CiscoWorks

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

Choose **Start >All Programs > CiscoWorks > CiscoWorks**. [Figure 2-46](#) shows the login page.

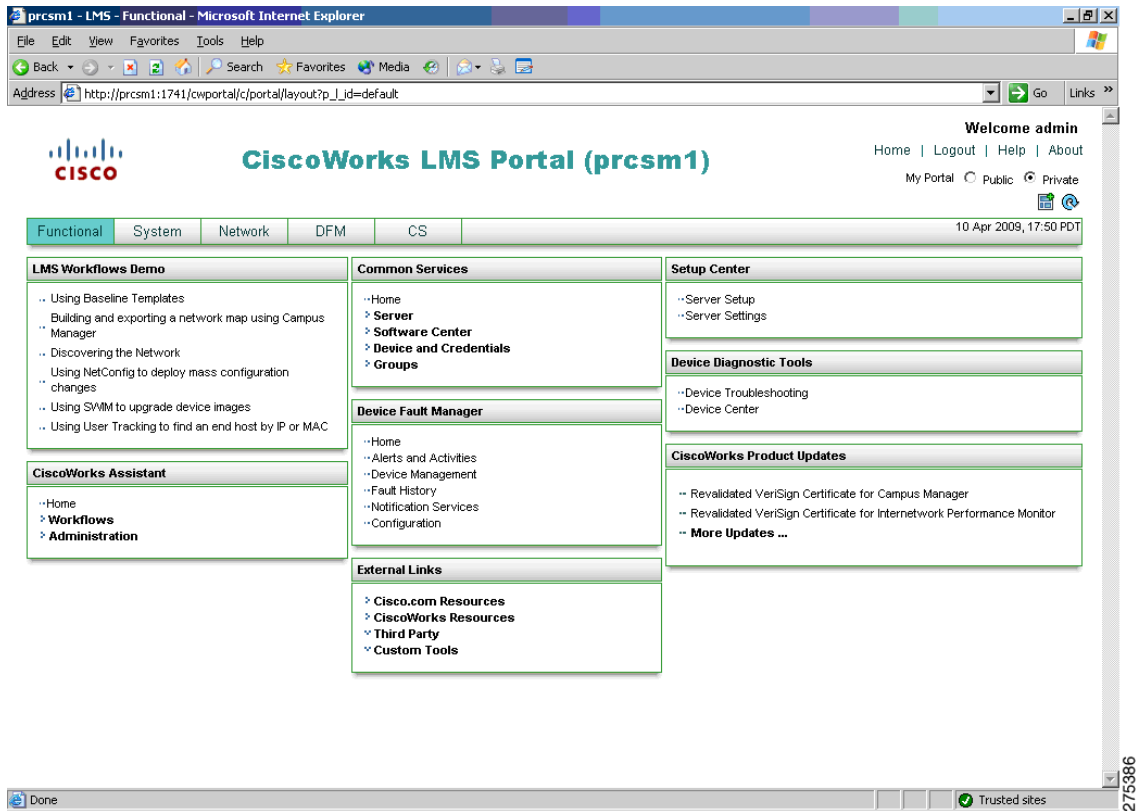
**Figure 2-46** Login Page



## Getting Started with the CiscoWorks LMS Portal

The CiscoWorks LMS Portal is the first page (see [Figure 2-47](#)) 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 2-47 CiscoWorks LMS Portal Page

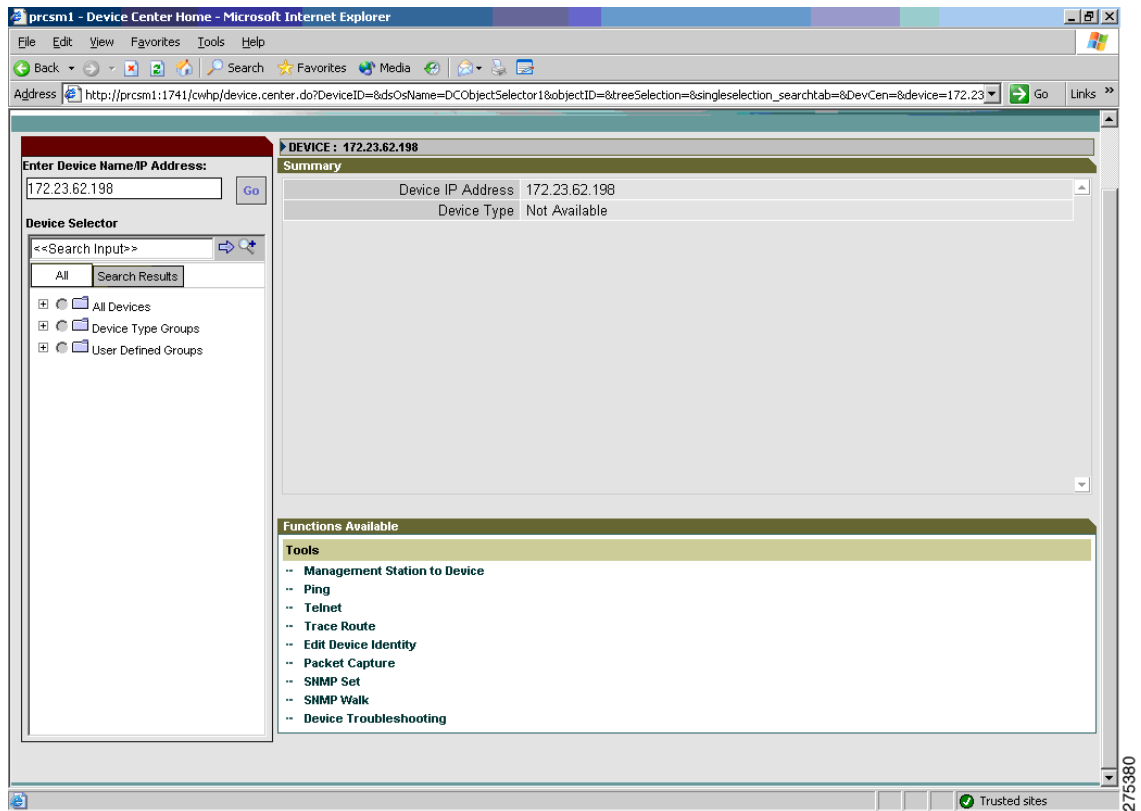


## Using the Device Center

To manage devices, perform the following steps:

- Step 1** Choose **Device Diagnostic Tools > Device Center** (see [Figure 2-48](#)).  
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 2-48 Device Center Home Window

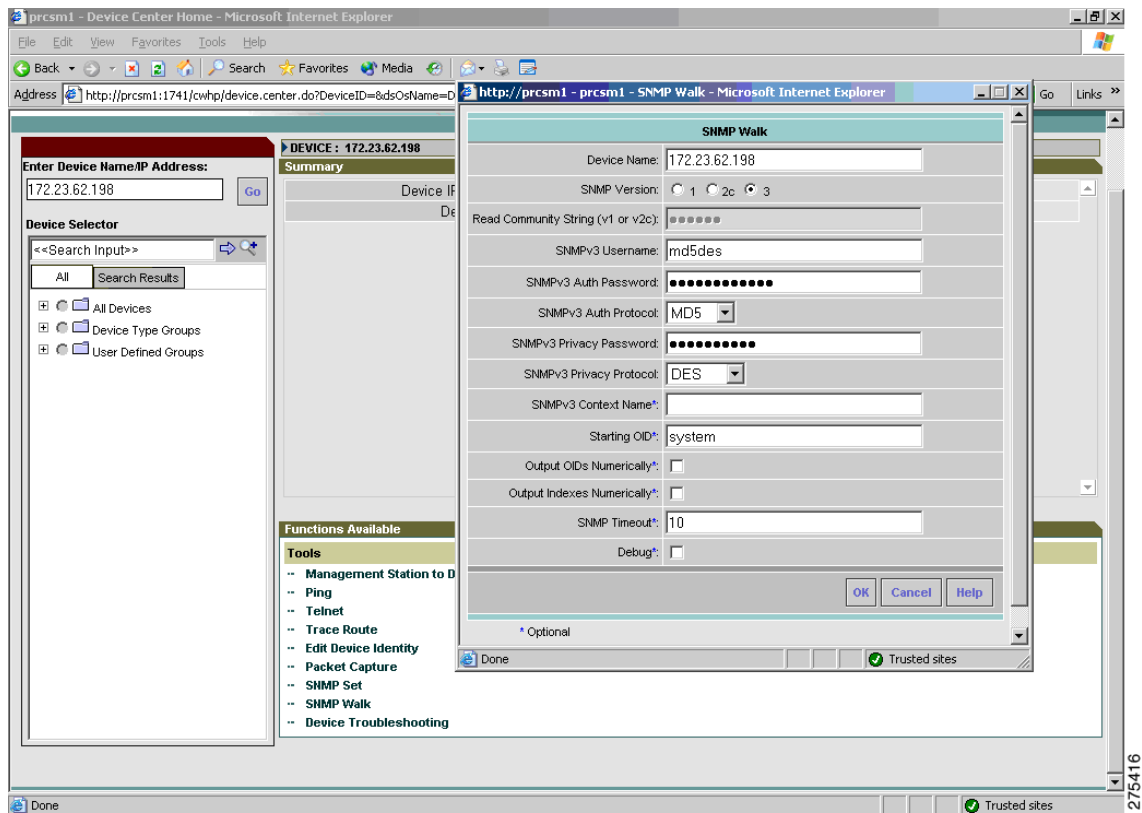


## Performing an SNMP Walk

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 (see [Figure 2-49](#)).

Figure 2-49 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 adaptive security appliance 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 adaptive security appliance 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 (see [Figure 2-50](#)).



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

**Figure 2-50** SNMP Walk Results Example

The screenshot shows the CiscoWorks interface with a window titled "SNMP Walk Results" open. The window displays the following information:

The following is a SNMP walk of device 172.23.62.198 starting from system

SNMP Walk Output

```

-----
system
sysDescr.0 = STRING : Cisco Adaptive Security Appliance Version 8.2(0)232
sysObjectID.0 = OID : ciscoASA5520
sysUpTime.0 = Timeticks : 3 days 1:41:21
sysContact.0 = STRING : hari d
sysName.0 = STRING : discasa
sysLocation.0 = STRING : sjc
sysServices.0 = INTEGER : 4
  
```

The interface also shows a "Device Selector" on the left with a search input field and a "Functions Available" section on the right listing tools such as Management Station to Device, Ping, Telnet, Trace Route, Edit Device Identity, Packet Capture, SNMP Set, SHMP Walk, and Device Troubleshooting.

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.

Figure 2-49 shows the list of privacy protocols supported. You must manually enter SNMP Versions 1, 2c, and 3 credentials (see Figure 2-52).

**Figure 2-51** SNMP Walk Dialog Box

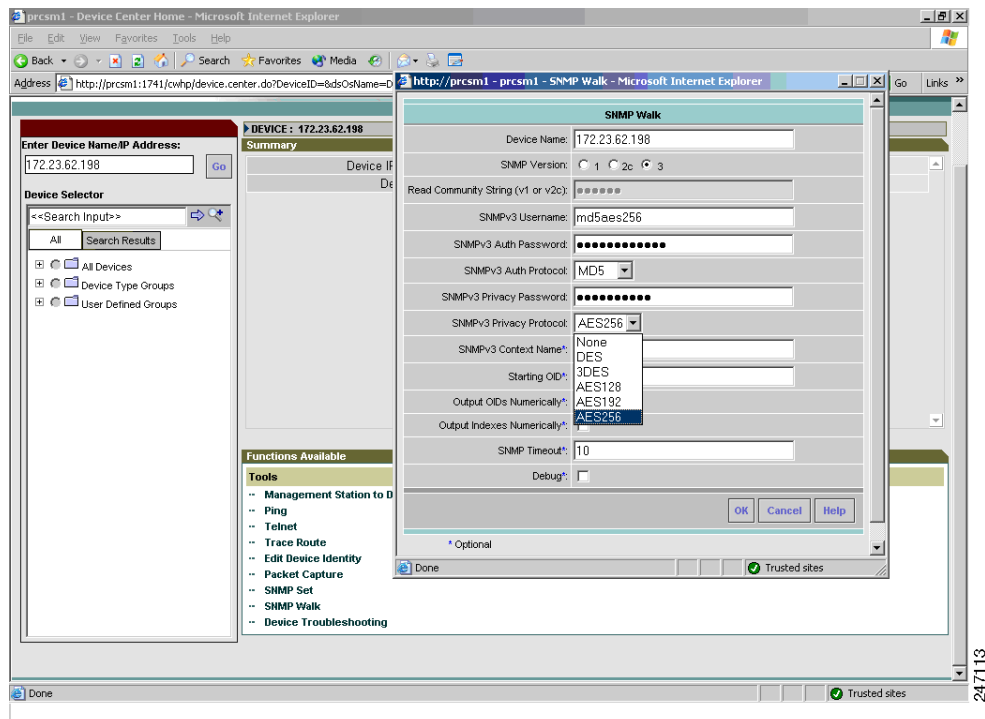


Figure 2-52 **SNMP Version 3 Parameters**

SNMP Walk	
Device Name:	172.23.62.198
SNMP Version:	<input type="radio"/> 1 <input type="radio"/> 2c <input checked="" type="radio"/> 3
Read Community String (v1 or v2c):	.....
SNMPv3 Username:	md5aes256
SNMPv3 Auth Password:	.....
SNMPv3 Auth Protocol:	MD5
SNMPv3 Privacy Password:	.....
SNMPv3 Privacy Protocol:	AES256
SNMPv3 Context Name*:	
Starting OID*:	system
Output OIDs Numerically*:	<input type="checkbox"/>
Output Indexes Numerically*:	<input type="checkbox"/>
SNMP Timeout*:	10
Debug*:	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

\* Optional

Figure 2-53 shows the SNMP walk results for the MD5 authentication and AES256 encryption algorithm settings.

Figure 2-53 **SNMP Walk Results Dialog Box**

```

sysDescr.0 = STRING : Cisco Adaptive Security Appliance Version 8.2(0)232
sysObjectID.0 = OID : ciscoASA5520
sysUpTime.0 = Timeticks : 3 days 2:7:33
sysContact.0 = STRING : hari d
sysName.0 = STRING : ciscoasa
sysLocation.0 = STRING : sjc
sysServices.0 = INTEGER : 4
ifNumber.0 = INTEGER : 8
ifIndex.1 = INTEGER : 1
ifIndex.2 = INTEGER : 2
ifIndex.3 = INTEGER : 3
ifIndex.4 = INTEGER : 4
ifIndex.5 = INTEGER : 5
ifIndex.6 = INTEGER : 6
ifIndex.7 = INTEGER : 7

```

## 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.

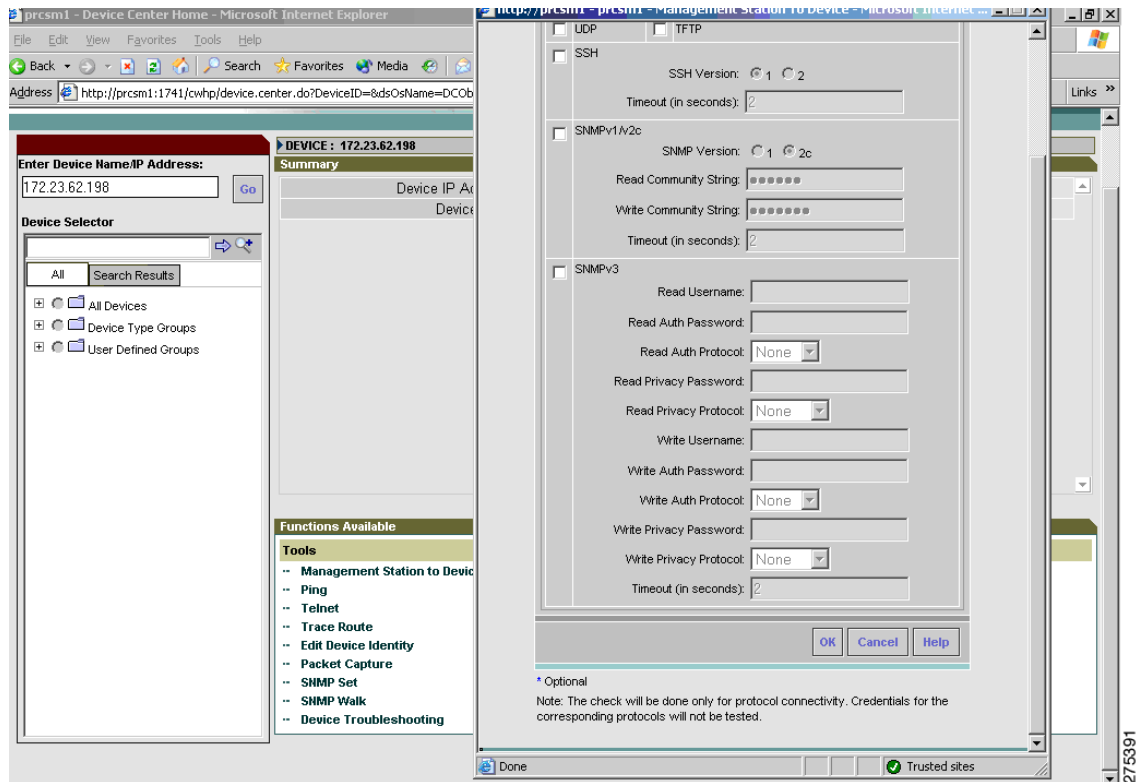
You can use this tool to send an SNMP GET request to the destination device for an SNMP read test (SNMPR). The tool also sends an SNMP SET request to the device for an SNMP write test (SNMPW). This protocol is supported for SNMP Versions 1, 2c, and 3.

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 (see [Figure 2-54](#)).

Figure 2-54 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 2-55 Management Station Device Results Dialog Box**

