

Using Network Management Tools

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

- Net-SNMP, on page 1
- SilverCreek SNMP Test Suite, on page 3
- IPswitch WhatsUp Gold, on page 17
- HP OpenView Network Node Manager, on page 30
- CiscoWorks, on page 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
- Sending a Trap

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 ~]# <mark>snmpwalk -v3 -u md5des -l authPriv -a MD5 -A mysecretpass -x des -X</mark> 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

SilverCreek - No Agent Selected Jee MIB Log Test Notification Packet Tests	uite <u>V</u> iew T <u>o</u> ols	Help		
🔽 🛃 🔚 M _{'Bs} 💐 🚭 🕐 🔚	🛸 📴 🖪	🛯 🔌 🔽 🔬 🖠 🕪 🤇) 💵 🗖	?
No Agent Selected				
Test Suites MIB Testing	-SNMPv1 Tests	or All MIBs Loaded		
Test Suite 1.0	Test Name	Purpose	Status	Remarks
Test Suite 1.0	1.1.2	Walk MIBs to collect variables	never run	
Protocol	1.1.2.2	Walk by column and scalar	never run	
A SNMPv1 Tests for All MIBs Loaded	1.1.1.1	NEXT request from 0.0	never run	
-# NEXT	1.1.1.2	NEXT request from 1.0	never run	<u> </u>
	1.1.2.1	Walk and check object syntax	never run	
-쁐 GET	1.1.3	NEXT from 2.0	never run	
一册 SET	1.1.4	NEXT with arbitrary OIDs	never run	
-## Boundary Conditions	1.1.5	NEXT with large instance-IDs	never run	
-III Module Compliance	1.1.6	NEXT with padded OIDs	never run	
SNMPv2c Tests for All MIBs Loadec	1.1.7.1	NEXT on unrelated tables	never run	
	1.1.7.2	NEXT with unrelated variables	never run	
SNMPv3 Tests for All MIBs Loaded	1.1.7.3	NEXT on columnar objects	never run	
Standard	1.1.8	GET on every variable	never run	
SNMPv3 USM-MIB (RFC-3414)	1.1.9	GET on padded OIDs	never run	
A SNMPV3 VACM-MIB (RFC3415)	1101	OFT on non-aviatant OIDa	DOLLOK KUD	
A SNMPv3 SNMP Apps (RFC3413)	<			>
SNMPv3 MPD-MIB (RFC3412)				
B MIB-II Tests(RFC1213/2011/2012/20				
	-No Details To I	Jispiay		
IPv6 IP-MIB Tests(RFC4293)				
IPv6 ipForwad MIB Tests(RFC4292)				
IPv6 TCP-MIB Tests(RFC4022)				
IPv6 UDP-MIB Tests(RFC4113)				
Diffie-Helman Key Change Tests (SI 🚃				
Grouping Tests as Levels (if applicable).				
	1			
Ready		Already Run 0 R	Remaining 55	Passed Constant Failed O
	ninitiated 0 Ur	ntested 0 Error 0 Unsupported	[]	0 UnResolved 0 NotInUse 0

Figure 1: SilverCreek Main Window

Figure 2: SilverCreek Console Window

<u>Eile View E</u> dit	
WARNING: redefining OID for mib-2	~
Loading MIB BRIDGE-MIB	
Loading MIB TOKEN-RING-RMON-MIB	
_oading MIB IP-MIB	
_oading MIB TCP-MIB	
Loading MIB UDP-MIB	
_oading MIB RMON2-MIB	
_oading MIB IP-FORWARD-MIB	
Loading MIB SNMPv2-TC	
_oading MIB SNMP-USM-DH-OBJECTS-MIB	
Loading MIB HOST-RESOURCES-MIB	
Loading MIB HOST-RESOURCES-TYPES	
Loading MIB RMON-MIB	
_oading MIB IF-MIB	
Loading MIB SNMP-FRAMEWORK-MIB	
Loading MIB SNMP-MPD-MIB	
oading MIB SNMP-TARGET-MIB	
Loading MIB SNMP-NOTIFICATION-MIB	
Loading MIB SNMP-PROXY-MIB	
Loading MIB SNMP-USER-BASED-SM-MIB	
Loading MIB SNMP-VIEW-BASED-ACM-MIB	
_oading MIB SNMPv2-TM	
Loading MIB SNMPv2-MIB	
oading MIB TRANSPORT-ADDRESS-MIB	
Loading MIB SNMP-COMMUNITY-MIB	
Loading MIB EtherLike-MIB	
Loading MIB SNMP-USM-AES-MIB	
Loading MIB INET-ADDRESS-MIB	
Loading MIB TCP-MIB	
WARNING: redefining OID for top	
Loading MIB UDP-MIB	
WARNING: redefining OID for udp	
Loading MIB IP-FORWARD-MIB	
WARNING: redefining OID for ipForward	
Loading MIB IP-MIB AVARNING: redefining OID for ip	
WARNING: redefining OID for icmp	
Console display active (Tcl8.4.4 / Tk8.4.4)	
SilverCreekMx) 1 %	~

Setting up an SNMP Version 3 Agent

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

Step 1 ChooseFile > New Agent Setup .

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

Figure 3: New Agent Setup Dialog Box

🗸 New Agent Setup							
 Address and Ports 							
Hostname or IP Address	172.23.62.19	8			▼ Port 161		
Protocols							
© SNMPv1 © SNMPv2c ☞ SNMPv3	– SNMPv3 Paran User To Derive Keys Auth Pass Priv Pass	md53des), please click here Algorithm	HMAC-MD5 CBC-3DES	•		
Optional Configurations Category E Local Interface D Time Out and F D Notification Co MIB Walking Ou Additional SNM I IPv4 or IPv6 Tr	Retries nfig utput File 1Pv3 Config	Agent's I Agent's I	nal SNMPv3 Config EngineID Context Name Context ID				
					Ok	Reset	Cancel

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.

SilverCreek - authPriv - Connected to : Cis	co Adaptive	Security Appliance Version 8.	2(0)227	🗖 🗖 🔀
File MIB Log Test Notification Packet Testsuite	<u>V</u> iew T <u>o</u> ols	Help		
🗹 🖆 🔚 🔤 🛠 🍩 🛈 🔚 🕇	👂 🖬 🛅	1 🍓 💎 🔬 ! 🂔 🔇	9 💵 🗖	?
authPriv - Connected to : Cisco Adaptive Security Applia	nce Version 8.2	2(0)227	[172.23.62	.198:SNMPv3]
Test Suites MIB Testing	SNMPv1 Tests	for All MIBs Loaded		
	To al block	Duran	0	Remarks 💦
Test Suite 1.0	Test Name	Purpose	Status	Remarks
	1.1.2	Walk MIBs to collect variables	never run	
	1.1.2.2 1.1.1.1	Walk by column and scalar	never run	
	1.1.1.2	NEXT request from 0.0 NEXT request from 1.0	never run never run	
	1.1.2.1	Walk and check object syntax	never run	
	1.1.3	NEXT from 2.0	never run	
LI LI SET	1.1.4	NEXT with arbitrary OIDs	never run	
	115	NEXT with large instance-IDs	never run	
Module Compliance	1.1.6	NEXT with padded OIDs	never run	
	1.1.7.1	NEXT on unrelated tables	never run	
	1.1.7.2	NEXT with unrelated variables	never run	
E B SNMPv3 Tests for All MIB:	1.1.7.3	NEXT on columnar objects	never run	
	1.1.8	GET on every variable	never run	
E SNMPV3 USM-MIB (RFC-3	1.1.9	GET on padded OIDs	never run	
E SNMPV3 VACM-MIB (RFC:	14.04	OFT on hon evident OIDe	DOUOK NUD	×
E	<			>
	No Dotoilo To Di	ianleu .		
	No Details To Di	врюу		
IPv6 IP-MIB Tests(RFC429				
IPv6 ipForwad MIB Tests(
IPv6 TCP-MIB Tests(RFC4				
IPv6 UDP-MIB Tests(RFC4				
🛛 🗌 🖵 🖫 Diffie-Helman Key Change 🔔				
Grouping Tests as Levels (if applicable).				
i Grouping rests as Levels (ir applicable).				
I.				ile j
uthPriv - Connected to : Cisco Adaptive Security Appliance			emaining 55	Passed 0 Failed 0
Warning 0 Abort 0 Uniniti	iated 0 Unt	tested 0 Error 0 Unsupported	0 NoResult	0 UnResolved 0 NotInUse 0

Figure 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.

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

Figure 5: Load and Delete MIBs Dialog Box

		Definition files generated from
	Load New MIB Files	MIB Compiling in: C:/Program
	View Loaded Modules	Files/InterWorkingLabs/SilverCr eekMx/inibs
	Delete Definition Files	
	ading Warnings. I understand warning messages to achieve best interoperabilty.	IANA-RTPROTO-MIB.defs ianaiftype-mib.defs rfc1155-RFC1155-SMI.defs rfc1157-RFC1157-SNMP.defs
I will fix those MIB err	rrors if possible and continue to load. ors later.	rfc1213-RFC1213-MIB.defs rfc1493-BRIDGE-MIB.defs rfc1513-TOKEN-RING-RMON-MIE rfc2011-IP-MIB.defs
directories defined by the directories. 2) Adding Multiple MIBs: You can load multiple MIB files into the MIB location (files using Tools->Options 3) The Order of MIB loadir You can load any numbe will figure out the OID tree their file names internally.	MIB files in the default directory "mibs" or in one or more environment variable "MIB_PATH". The path can contain multiple Is automatically at startup by dropping all of your uncompiled MIB (you may specify desired file name extensions to filter non-MIB >Misc) or select multiple MIB files when working with GUI.	ric2012-TCP-MIB.defs ric2013-UDP-MIB.defs ric2021-RMON2-MIB.defs ric2096-IP-FORWARD-MIB.defs ric2578-SNMPv2-SMI.defs ric2579-SNMPv2-TC.defs ric2786-SNMP-USM-DH-OBJECT ric2790-HOST-RESOURCES-MIB ric2819-RMON-MIB.defs ric2811-SNMP-FRAMEWORK-MIE ric3411-SNMP-FRAMEWORK-MIE ric3412-SNMP-MPD-MIB.defs ric3413-SNMP-TARGET-NOTIFIC ric3413-SNMP-TARGET-NOTIFIC ric3415-SNMP-VEW-BASED-AC ric3416-SNMPv2-PDU.defs ric3416-SNMPv2-PMIB.defs
	Close	rtc3419-TRANSPORT-ADDRESS rtc3584-SNMP-COMMUNITY-MIB rtc3635-EtherLike-MIB.defs rtc3826-SNMP-USM-AES-MIB.de rtc4001-INET-ADDRESS-MIB.def:

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.

L

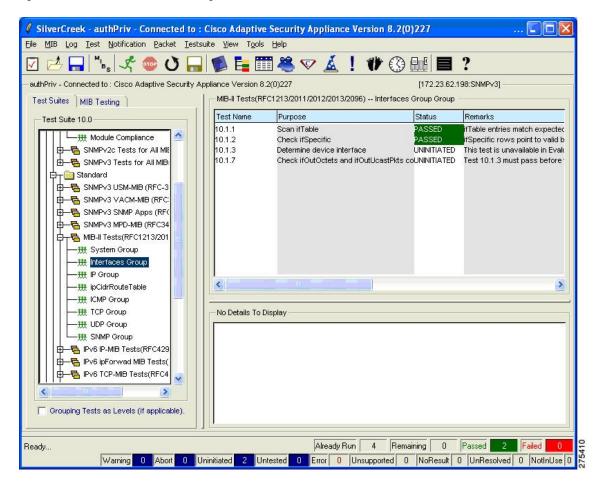


Figure 6: SilverCreek Main Window Showing Selected Tests

Enabling Debugging

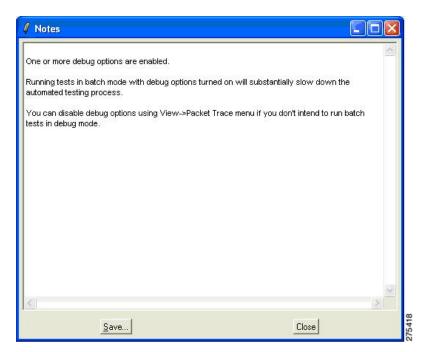
To enable debugging, choose Tools > Options.

Figure 7: Debug Tab of the Options Dialog Box

🧳 Options		
Debug Display Test Journal Notification Misc		
Packet trace will be output to Console when you run selected test(s) or issue SNMP commands.		
Sent Packets		
Packet Summary - Summarized form of packets sent by SilverCreek Evaluation		
Packet Watch - ASN1 pseudo code of packets sent by SilverCreek Evaluation		
Packet Debug - HEX dump of packets sent by SilverCreek Evaluation		
Received Packets		
Packet Summarized form of packets sent by the agent		
Packet Watch - ASN:1 pseudo code of packets sent by the agent		
Packet Debug - HEX dump of packets sent by the agent		
The out of the adding of proceed on they are again.		
	Ok	Cancel

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

Figure 8: Warning Notes Dialog Box



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

Ø Options	
Debug Display Test Journal Notification Misc	
Packet trace will be output to Console when you run selected test(s) or issue SNMP commands.	
- Sent Packets	
Packet Summary - Summarized form of packets sent by SilverCreek Evaluation	
Packet Watch - ASN1 pseudo code of packets sent by SilverCreek Evaluation	
Packet Debug - HEX dump of packets sent by SilverCreek Evaluation	
Received Packets	
Packet Summary - Summarized form of packets sent by the agent	
Packet Watch - ASN.1 pseudo code of packets sent by the agent	
Packet Debug - HEX dump of packets sent by the agent	
	Ok Cancel

Figure 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.
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.

	🚽 📲 📲 🗸 🌑 🖸 🖡		🐣 💎 🔬 ! 🌵 🔇 🖩	
thPriv - Co	nnected to : Cisco Adaptive Securit			[172.23.62.198:SNMPv3]
est Suites	MIB Testing	Tests to Run for t	the Selected MIBs with SNMPv3	
-Select MI	Bs to Test	Groups: 💿 All T	ests CINEXT CIBULK CIGET CIS	SET 🦳 Boundary Conditions 🦳 Module C
AI[]	MIB Module	Test Name	Purpose	Status Remarks
	BRIDGE-MIB	3.1.2.1	Walk MIB to collect variables	PASSEDSee "Details for Test 3.1.2
	EtherLike-MIB	3.1.2.3	Walk by column and scalar	PASSEDGot consistent results whe
	HOST-RESOURCES-MIB	3.1.1.1	NEXT request from 0.0	PASSEDAgent returned SNMPv2-M
	IF-MIB	3.1.1.2	NEXT request from 1.0	PASSEDAgent returned SNMPv2-M
	IP-FORWARD-MIB	3.1.1.3	NEXT request from 2.0	PASSEDNo variables lexi-greater th
	IP-MIB	3.1.2.2	Walk and check object syntax	PASSEDSee "Details for Test 3.1.2
	RFC1213-MIB	3.1.3.1	NEXT with arbitrary OIDs	PASSED3020 of 3020 iterations pa
	RMON-MIB	3.1.3.2	NEXT with large instance-IDs	UNINITIAThis test is unavailable in E
	RMON2-MIB	3.1.3.3	NEXT with padded OIDs	UNINITIAThis test is unavailable in E
	SNMP-COMMUNITY-MIB	3.1.4.1	NEXT on unrelated tables	UNINITIAThis test is unavailable in E
	SNMP-MPD-MIB	3.1.4.2	NEXT with unrelated variables	UNINITIAThis test is unavailable in E
	SNMP-NOTIFICATION-MIB	<u> </u>	· · · · ·	
	SNMP-PROXY-MIB	<		>
V	SNMP-TARGET-MIB	Grouping	by Test Levels: C Basic Level C Intern	nediate Level C Advanced Level
V	SNMP-USER-BASED-SM-MIB			
	SNMP-USM-DH-OBJECTS-MIB	-		
	SNMP-VIEW-BASED-ACM-MIB	Details of Test 3.	9.2	
	SNMPv2-MIB			
	TCP-MIB	Details of Test 3.9	The second se	
	UDP-MIB	agent during the N	e of this test is to detect objects defined in the	ne loaded MIDS but are not returned by the
		agent during the K	nio waiking.	
		If the objects not i	mplemented were found then a Warning is i	reported with a list of not-found object
			ned MIB walking scopes. Note: missing obje	
		considered as a f	ailure. The user should inspect the results a	and determine if it is in fact an error. The
			soleted objects are not reported. The not-ac	
C Enterpr	ise MIBs (Standard MIBs	[UNINITIATED] Ren	narks: This test is unavailable in Evaluation I	Edition

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

MIB Browser: Local MIB Tree mo Elle View Operation	de - tree reflects locally	oaded MIBs			
Tool Mode: Local MIB Tree	🖉 💿 II 🔒				
cregistration-authorit; cregistration-authori	No. △ OID-Hame	Syntax	Value	Full_OID	
Image: Construction of the system of the	OID: 1.3.6.1.2.1 Index object: N/A	ccess: not-acc	essible		

Figure 11: 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.

I

ool Mode: Local MIB Tree	Ø (
.:registration-authority .:member-body [2]	No. A	OID-Name	Syntax	Value	Full_OID
Ġ _T 🔄 org [3]	1	sysDescr.0	DisplayString	Cisco Adaptive S	1.3.6.1.2.1.1.1.0
白, dod [6] 日, internet [1]	2	sysObjectID.0	ObjectID	1.3.6.1.4.1.9.1.67	1.3.6.1.2.1.1.2.0
└── 📴 directory [1] □ ┬── 🛐 mgmt [2]	3	sysUpTime.0	TimeTicks	8252500	1.3.6.1.2.1.1.3.0
⊡ mib-2 [1] □ system [1]	4	sysContact.0	DisplayString	hari d	1.3.6.1.2.1.1.4.0
-Ø sysDesc	5	sysName.0	DisplayString	ciscoasa	1.3.6.1.2.1.1.5.0
<i>—∭</i> sysObjec <i>—∭</i> sysUpTir	6	sysLocation.0	DisplayString	sjc	1.3.6.1.2.1.1.6.0
	7	sysServices.0	INTEGER	4	1.3.6.1.2.1.1.7.0
	 MIB Info Descrip Syntax OID: Index o Index in 	otor: SNMPv2-M : N/A A 1.3.6.1.2.1 bbject: N/A	ccess: not-acce:	ssible	×

Figure 12: 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 13: Notification Monitor Dialog Box

Notification Monitor
Received notifications will be tested against their MIB definitions. Error messages will be printed to View->Console.
Check variable bindings 🔽 Check time window (v3) 🔽 Authenticate notifications (v3) General V3 Trap V3 Inform
- Received Notifications
Order Time Notifications
[+] 1 17:01:36.64 F-MIB:tinkDown trap:SNMPv3_from [172:23.62.198_Port: 162] User: md53des authPriv [+] 2 17:01:38.22 F-MIB:tinkUp trap:SNMPv3_from [172:23.62.198_Port: 162] User: md53des authPriv
- Details of Notification 1
SNMPv2-MIB:sysUpTime.0: (8468600) Syntax: TimeTicks SNMPv2-MIB:smmpTrapOID.0: (IF-MIB:InterfaceIndex, Instance IDs: (3) IF-MIB:IfIndex.3: (3) Syntax: IF-MB:InterfaceIndex, Instance IDs: (3) IF-MIB:IfOperStatus.3: (down) Syntax: INTEGER, Instance IDs: (3) IF-MIB:IfOperStatus.3: (down) Syntax: INTEGER, Instance IDs: (3)
Listening Traps from All Source Addresses Click 'Configuration' to change source filter Click rows to see trap details

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 if Type, asks how many times you want to repeat the operation, and uses the value, 10.

Figure 14: Performance Measuring Dialog Box

Performance Measuring		
he most commonly seen mode of SNMP co Send Asynchronously": requests are sent previous requests. When round-trip time is node. You can adjust the maximum number agent under test.	nly after the response for the previous request has be mmunication. continuously without waiting for the responses comin significant asynchronous mode should be much faster r of requests sent in a burst to make sure the sender do nported into spreadsheet application such as Excel.	g in first for the than synchronous
Select a SNMP Operation to add to the list Get Set Next Walk (get-nexts) Bulk		Clear All
ulkwalk +10 0 1		6
ulkwalk +10 0 1 ifType		<u>×</u>
	Load Commands	Save Commands
	Load Commands 20 Maximum number of requests sent in an Note if this value is set too high the age	asynchronous burst.

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.

Cisco Devices My Network Device Group Examples Devices (dynamic group) All routers (dynamic group) Devices collecting Disk Devices collecting Interf Devices collecting Ping Devices collecting Ping Devices collecting Ping Devices with at least on Devices with Vindows Devices without credenti Devices without SMMP Devices without SMM	Ipswitch WhatsUp Gold v12.3 - [Net Eile Edit View Configure Tools F		c Group Examples]		
Display Name Host Name Address Device Type Image: Device Groups Image: Cisco Devices Image: Cisco Devices<	🖹 🧔 🍃 💊 🖌 🚮				
Image: Device Groups Display Name A Host Name Address Device 1ype Image: Device Groups Cisco Devices Cisco Devices Device collecting CPU Devices collecting Disk Image: Devices Collecting Disk Devices collecting Interf Devices collecting Ping Devices collecting Ping Image: Devices with at least on Devices with SIMP cre Devices with SIMP cre Devices without credenti Image: Devices without SIMP Devices without Credenti Devices without SIMP Image: Devices without SIMP Devices without SIMP Devices without SIMP Image: Devices without SIMP Devices without SIMP Devices without SIMP Image: Devices without SIMP Devices without SIMP Devices without SIMP Image: Devices without SIMP Devices without SIMP Devices without SIMP Image: Devices without SIMP Devices without SIMP Devices without SIMP Image: Devices without SIMP Printers Unacknowledged Devices	🖥 Dynamic Group Examples				1
My Network Completely down devices All devices (dynamic group) Devices collecting CPU All routers (dynamic group) Devices collecting Disk Dynamic Group Examples Devices collecting Mem Devices collecting Ping Devices with at least on Devices with SNMP cre Devices with SNMP cre Devices with Out credenti Devices without credenti Devices without SNMP Devices without SNMP Devices without SNMP Unacknowledged Devices		X Display Name	A Host Name	Address	Device Type
	My Network My Network All devices (dynamic group) All routers (dynamic group)	Completely down de Devices collecting (Devices collecting (Devices collecting (Devices collecting (Devices collecting (Devices with at leas Devices with at leas Devices with sNinf Devices with wind Devices without vit Devices without vit Devices without Vit Frequently polled P Printers Unacknowledged D	CPU Disk Mem Ping ance st on c cre over denti MP ndo		
Device Types (Basic)	🛃 Device Types (Basic)				
🖳 Device Types (Advanced) 🙀 Device View 🌸 Map View 🤳 🐻	🛃 Device Types (Advanced)	🙀 Device View 🗔	🗴 Map View) 🗟 🖉

Figure 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.

Figure 16: Add New Device Dialog Box

Add New Device	×
IP address or host name of the new device:	<u>A</u> dvanced
[] 5	ОК
Example: 192.168.200.123 or www.somedomain.com Add device immediately without scanning	Cancel
	Help

- **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 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, and enter the SNMP device object ID information.

Device Properties : 172.23.62.1	198	x
Properties	Credentials and SNMP	
General Performance Monitors	Credentials	
Q Active Monitors	Windows credentials:	
Passive Monitors	SNMP v1/v2/v3 credentials:	
Actions		
Credentials	SNMP	
C Polling	Device Object ID: (OID)	
📝 Notes	system	
Menu 🖉		
🛃 Attributes	OK Cancel H	Help

Figure 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**.

Figure 19: Edit SNMP v3 Credential Type Dialog Box

	nd5des	X
<u>V</u> ame:		
md5des		
Description:		
md5des		
<u>I</u> sername:		
md5des		
Iontext:		
Fouriexr:		
_oncext:		_
Authentication	Encryption	
Authentication	Protocol:	T
Authentication Protocol: MD5	Protocol: DE556	• ок
Authentication	Protocol:	▼ OK Cancel

Figure 20: Credentials Library Dialog Box

Name	۵	Description	Туре	<u>N</u> ew
🗐 md5des		md5des	SNMP v3	<u>E</u> dit
🗋 public		Generated Credential Type	SNMP v1	
				<u></u> opy
				<u>D</u> elete
				OK

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

Figure 21: Network Explorer Window with Added SNMP Version 3 Node

		work Explorer - Dynamic Group Examples]		
Dynamic Group Examples Device Groups My Network All devices (dynamic group) All routers (dynamic group) All routers (dynamic group) All routers (dynamic group) All routers (dynamic group) Optimic Group Examples Cisco Devices Devices collecting Disk Devices collecting Disk Devices collecting Disk Devices collecting Disk perform Devices collecting Disk perform Devices collecting Disk perform Devices collecting Ping perform Devices collecting Ping perform Devices with SIMP credentias Devices with SIMP credentias Devices without south credentias Devices without sout credentias Devices without sout credentias Device		eports <u>W</u> indow <u>H</u> elp		_ 8
Device Groups My Network All devices (dynamic group) All devices (dynamic group) All routers (dynamic group) All routers (dynamic group) All routers (dynamic group) Dynamic Group Examples Occompletely down devices Devices collecting CPU Devices collecting CPU Devices collecting CPU perform Devices collecting Interface per Devices collecting Interface per Devices collecting Interface per Devices with at least on Devices with at least on Devices with at least on Devices with at least on down Devices without SNMP credentials Devices without credentials Devices without windows credent Devices without windows credent Devices without SNMP credentials Devices without SNMP credentials<				
Device Groups Usplay Name Address Device Type My Network Cisco Devices Completely down devices Devices collecting CPU All routers (dynamic group) All routers (dynamic group) Devices collecting Disk Devices collecting Disk Dynamic Group Examples Cisco Devices Devices collecting Interf Devices collecting Interf Devices collecting Disk perform Devices collecting Interface period Devices collecting Ping Devices with at least on Devices collecting Interface period Devices with SNMP cred Devices with SNMP cred Devices with SNMP redentials Devices without credentials Devices without SNMP redentials Devices without SNMP credentials Devices without SNMP credentials Devices without SNMP redentials Devices without SNMP redentials Devices without SNMP redentials Devices without SNMP redentials Devices without SNMP redentials Devices without SNMP redentials Devices Devices without SNMP redentials Intercementials Intercementials Devices without SNMP redentials Intercementials Intercementials Devices without SNMP redentials Intercementials Intercementintwices Devices withou	Dynamic Group Examples			ß
My Network All devices (dynamic group) All routers (dynamic group) All routers (dynamic group) Dynamic Group Examples Cisco Devices Cisco Devices Devices collecting CPU perform Devices collecting Disk perform. Devices collecting Interface per Devices collecting Interface per Devices collecting Ping perform. Devices collecting Ping perform. Devices collecting Ping perform. Devices collecting Ping perform. Devices with at least one down Devices with at least one down Devices with NMP credentials Devices without windows credentials Devices without credentials Devices without windows credentials De		Display Name 🔺 Host Name	Address	Device Type
Devices without credentials Devices without SIMP credenti Devices without Windows crede Devices without Windows crede Prequently polled Performance Printers Device Types (Basic)	My Network All devices (dynamic group) All routers (dynamic group) Dynamic Group Examples Cisco Devices Completely down devices Devices collecting CPU perform Devices collecting Disk perform Devices collecting Disk perform Devices collecting Memory perf Devices collecting Ping perform Devices with at least one down Devices with SNMP credentials	 Completely down devices Devices collecting CPU Devices collecting Disk Devices collecting Interf Devices collecting Mem Devices collecting Ping Devices collecting Ping Devices with at least on Devices with SNMP cr Devices without credenti Devices without SNMP Devices without Windo 		
Printers Printers Device Types (Basic)	Devices without SNMP credenti Devices without Windows credent	Printers Unacknowledged Devices Windows Devices		
	Printers	172.23.62.198 172.23.62.198	172.23.62.198	Workstation
	Device (ypes (basic)			

Using the WhatsUp Gold Web Interface

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

- Step 1Choose 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 22: WhatsUp Gold Login Window for Web Interface

😢 Login - WhatsUp Gold - Mozilla Firefox	
Elle Edit View History Bookmarks Tools Help	0.
🕜 主 C 🗶 🏠 🧶 http://127.0.0.1:8080/NmConsole/CoreNm/User/DlgUserLogin/DlgUserLogin.asp 🏠 🔹 🗔 -	Google 🔎
🙍 Most Visited 🏟 Getting Started <u>S</u> Latest Headlines 📋 Customize Links 📄 Free Hotmail 📄 Windows Marketplace 🌓 Windows Media 📄 Windows	
💿 Try WhatsUp Gold Version 12.4, VoIP, 🗵 👌 Mozilla Firefox Start Page 🛛 🥥 Login - WhatsUp Gold 😰	•
	-
	_
IPSWITCH	
Whatsl InGold	
Premium Edition v12.3.1	
User name:	
Password:	
Start page:	
WhatsUp Home Workspace	
Login	
Evaluation License: 30 days remaining	
іруштсн	
	-
The 'admin' password has not yet been changed. The default username and password is: 'admin'. Once you login you	
change your password on the Preferences dialog. To do this, after you login you can: 1. Click the 'GO' menu in the ton left	
Done	¥ 1.

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

L

Figure 23: WhatsUp Gold Home Workspace Pane

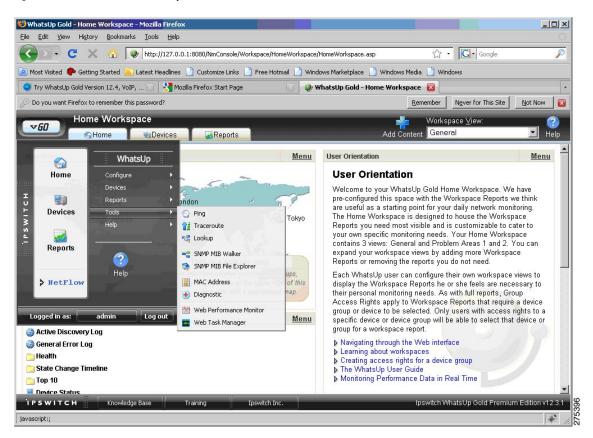


Walking an SNMP MIB or an OID

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

Step 1 Choose GO > Tools > SNMP MIB Walker.

Figure 24: 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 25: Network Tool: SNMP MIB Walker Dialog Box

Network Tool: SNMP MIB Walker	- Mozilla Firefox			_ 🗆 ×
http://127.0.0.1:8080/NmConsole/CoreNm/Tools/DigMibWalker/DigMibWalker.asp				☆
Network Tool: SNMP MIB	Walker		📚 MibFileExplorer	📲 MibWalker 📀
Address or hostname: 172.23.62.198 2bject ID: snmpTargetMIB	<u>C</u> redentials: md5des (SNMP∨3) Eilter: 	Adyanced		
ne				*

Step 3 Click Walk.

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

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

🕹 Network Tool: SNMP MIB Walker - Mozilla Firefox		-O×
http://127.0.0.1:8080/NmConsole/CoreNm/Tools/DIgMibWalker/DIgMibWalker.asp		
== Network Tool: SNMP MIB Walker	📚 <u>MibFileExplorer</u>	📲 MibWalker 📀
Address or hostname: Credentials: 172.23.62.198 md5des (SNMP∨3) Object ID: Eilter: snmpTargetMIB	xdyanced ∭alk	
Walking 1.3.6.1.6.3.12 (snmpTargetMIB) on 172.23.62.198 iso.org.dod.internet snmpV2(6) snmpTargetMIB(12) msnmpTargetMIB(12) msnmpTargetAddrTable(2) snmpTargetAddrTDomain(2)	Stop	Back
116.114.97.112.104.111.115.116.46.109.100.53.100	.101.115.46.49.55.50.46.50.51.46.51.50.46.49.53.50.46.54.53.53.51.56	1.3.6.1.6.1.1
smpTargetAddrTimeout(4)	.101.115.46.49.55.50.46.50.51.46.51.50.46.49.53.50.46.54.53.53.51.56 .101.115.46.49.55.50.46.50.51.46.51.50.46.49.53.50.46.54.53.53.51.56 .101.115.46.49.55.50.46.50.51.46.51.50.46.49.53.50.46.54.53.53.51.56	1500
Done		* //

The following figure shows the results in sequence.

Figure 27: Network Tool: SNMP MIB Walker Results Window

Network Tool: SNMP MIB Wall	ker - Mozilla Firefox	
http://127.0.0.1:8080/NmCor	nsole/CoreNm/Tools/DlgMibWalker/DlgMibWalker.asp	☆
📲 Network Tool: SNMP M	IB Walker	📚 <u>MibFileExplorer</u> 📑 MibWalker 🥝
Address or hostname: 172.23.62.198 Object ID: snmpTargetMIB	Credentials: md5des (SNMP∨3) ▼ Eilter: Adyanced Walk	
Walking 1.3.6.1.6.3.12 (snm	pTargetMIB) on 172.23.62.198	Stop Back 👌
Object ID	Value	
snmpTargetAddrTAddress.1 snmpTargetAddrTagList.116 snmpTargetAddrTagList.116 snmpTargetAddrParams.116 snmpTargetAddrParams.116 snmpTargetAddrStorageTyp snmpTargetAddrRowStatus. snmpTargetParamsMeMode snmpTargetParamsSecurityl snmpTargetParamsSecurityl snmpTargetParamsSecurityl snmpTargetParamsSecurityl	.114.97.112.104.111.115 trap .114.97.112.104.111.115 traphost.md5des.172.23.32.152.65538 e.116.114.97.112.104.111 nonVolatile (3) 116.114.97.112.104.111 active (1) il.116.114.97.112.104.113 Model.116.114.97.112.11 3 Name.116.114.97.112.11 md5des .evel.116.114.97.112.104 authPriv (3) (3) (3) (4) (4) (4) (5) (3) (4) (4) (3) (4) (4) (4) (5) (5) (5) (5) (6) (6) (7) (7) (7) (7) (7) (7) (7) (7	
Done		*

Configuring SNMP Traps

To configure SNMP traps, perform the following steps:

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

	Name 🛆	Description	<u>C</u> onfigure
General	SNMP Trap	Listen for SNMP traps	
	Syslog	Listen for Syslog messages Monitor Windows Event Log	
Web Server			
~			
)evice States			
assive Monitor Listeners			
Report Data			
-			
a			

Figure 28: Program Options – Passive Monitor Listeners Dialog Box

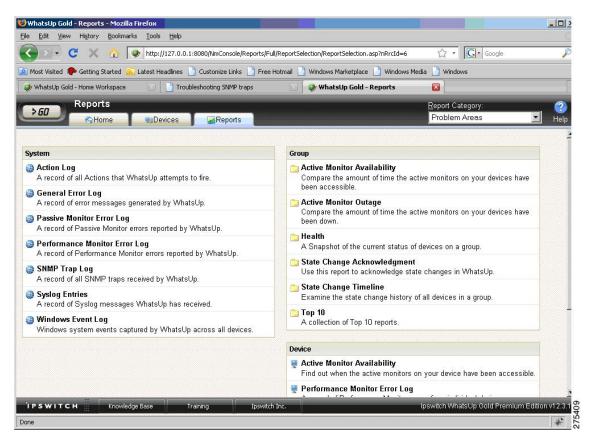
The SNMP Listener Configuration dialog box appears. From here you can configure the listener port and forward traps to a host.

Figure 29: SNMP Listener Configuration Dialog Box



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

Figure 30: SNMP Reports Pane



The following figure shows the SNMP trap log.

Figure 31: SNMP Trap Log Pane

асуор сою - эмни-ттар сод - модшати стох					حالف
<u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	\$				
🖸 🔹 😋 🗙 🍙 🕑 http://127.0	.0.1:8080/NmConsole/Reports/Fu	ll/System/ProblemAreas/Rpt	SnmpTrapLog/RptSnmpTrapLog 🏠	7 • Google	
st Visited p Getting Started 🔝 Latest Headline	s 📄 Customize Links 📄 Free	Hotmail 📄 Windows Mark	etplace 📄 Windows Media 📄 '	Windows	
SNMP Trap Log		-	More System <u>R</u> eports:		2
GD Anne Devices	Reports		SNMP Trap Log	Export Fav	
	Date range: T	oday 🔻	Go		
The SNMP listener is currently ON .	Start time: 04	and the second se	M -		
-	End time: 0	4/02/2009 🔲 10:48 A			
April 02, 2009:					
Date 🔺	Source	Trap	Payload		

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.

Ŵ

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 32: NNM Console Root Window

2R	oot										
Мар	Edit	⊻iew	Performance	Configuration	<u>E</u> ault	Tools	Options	<u>W</u> indow	Help		
				Q 🗾							
	(Inter	net								
defau	ilt [Rea	id-Writi	e]			[A	luto-Layou	ut][Conne	ction Labels	s Off]	

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

The Internet window appears, with the network nodes displayed.

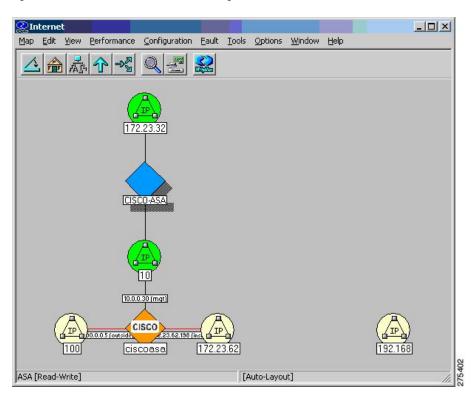


Figure 33: NNM Console Internet Window Showing Network Nodes

Loading MIBs

To load MIBs, perform the following steps:

- Step 1In 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.

스 🗟 🚑 🎓 🔩 🔍 🗄 Load/Unload MIBs:SNMP	ration Eault Iools Options		
	×		
rfc2012-TCP-MIB rfc2013-UDP-MIB rfc2083HF-MIB ENTITY-MIB.my SNMPv2-CDNF.my SNMPvC20MUNITY-MIB.my SNMP-CDMUNITY-MIB.my SNMP-FRAMEWDRK-MIB.my	Load Unload MIBs:SNMP / Load Look in: C mibs imports silvercreek_mandated IF-MIB.my SNMP-COMMUNITY-MIB.my SNMP-FRAMEWORK-MIB.my SNMP-FRAMEWORK-MIB.my	d MIB from File	? ×
	File name: SNMP-VACM-MIB.	my	<u>O</u> pen Cancel

Figure 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.

ap Edit Yew Performance Config	uration Eault Iools Options Window Help	
172.23.32	Add Object Palette	×
[CISCO ASA]	Computer Connector	•
	Symbol Subclasses for Class Connector:	
A [Read-Write]	Drag a Subclass Symbol to the desired Submap.	

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.

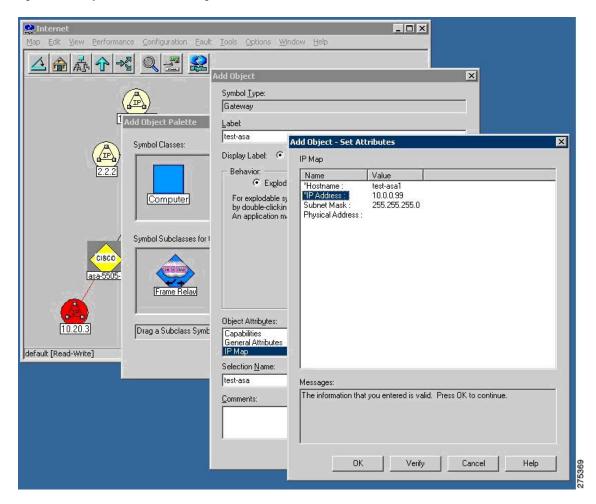
Figure 36: Add Object Dialog Box

Internet Map Edit View Performance Configuration Fault	Tools Options Window Help
	Add Object 🛛 🔀
	Symbol Type:
	Gateway
L Add Object Palette	Label: test-asa
Symbol Classes:	
	Display Label: • Yes • No
(2.2.2)	Behavior: © Explode C Execute
Computer	For explodable symbols, you can create a child submap
	by double-clicking on the symbol after you OK this box. An application may create the child submap for you.
Symbol Subclasses for 1	
CISCO	
asa-5505-	
Frame Relay	
	Object Attributes:
10.20.3 Drag a Subclass Symb	Capabilities
default [Read-Write]	General Attributes
Joeraar [Kead-write]	Selection Name:
	test-asa Set Selection Name
	Comments:
	OK Cancel Help
	UK Lancel Help

Step 4 Double-click IP Map.

The Add Object – Set Attributes dialog box appears.





- **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 38: SNMP Configuration

© Command Prompt C:\Program Files\HP OpenView\bin>xnmsnmpcon C:\Program Files\HP OpenView\bin>	f.exe
Global Default IP Wildcards Specifi Community Set Community Set Community Timeout D.8 seconds Etries 2 Etries 2	Image: Status Pglling 15.0000
OK Cancel	Apply Boll Objects Import Export Help

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 39: SNMP Configuration Dialog Box

SNMP Config		Specific Nodes	1	-		-			x
Node 10.0.0.254 10.0.0.33 10.0.0.63 10.20.2.252 10.20.2.34 10.20.3.10	Community 3P;authp 3A;authp 3P;authp 3P;authp 3N/titann 3P;authp	Set Community [-] [-] [-] [-] [-] [-]	Proxy [no [no [no [no [no [no	Retry [·] 2 [·] [·] [·]	Timeout [-] [-] [-] [-] [-] [-]	Port [-] [-] [-] [-] [-]	Polling [-] 5.00 [-] [-] [-] [-]	A <u>d</u> d Modify Dejete	
<u>I</u> arget 10.20.2.2 <u>C</u> ommunity	y ass;privpass/ti		Stoxy	proxy to a	access targ	ət			OK Cancel Help
Timeout			R <u>e</u> mote F Status P <u>c</u>						

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.

L

Sasa-5505-4 Map Edit View Performance Configuration Eault Ic	ols Options Window Help
kinda outside	
	Image: Set work Interface Properties : 10.20.2.252:Ethernet0/0 Image: Set with the set of the se
[Internal-Data0/0] Ethernet0/0	Name or address: 10.20.2.252.Ethernet0/0
Ethermet0/3 Ethermet0/4	General Properties Interface \$: 4 Interface Name : Ethernet0/0 Description : Adaptive Security Appliance 'Ethernet0/0' interface Alias : Current Status : up Type : Ethernet Capacity : 100 Mbps Physical Address : 0x002304249087 Promiscuous Mode : Off Messages:
	Stop Close

Figure 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

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 1To 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 1To configure the UUT group, enter the snmp-server group asapriv v3 priv comman	d.
--	----

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 41: Browse MIB Dialog Box

ex Command Prompt C:\Program Files\HP OpenView\bin>xnmbrowser.exe	
C:\Program Files\HP OpenView\bin>	
(鼉 Browse MIB	
Eile Yiew Help	
Name or address:	Community name:
10.0.0.63	3P:authpass:privpass/titand
MIB object ID:	
iso.org.dod.internet.mgmt.mib-2	
← ccitt	Describe Start Query Stop Query Graph
	Set
MIB values: sysDesct.0 : Cisco Adaptive Security Appliance Version 8.2(0)210 sysDbjectID.0 : .iso.org.dod.internet.private.enterprises.9.1.672 sysUpTime.0 : (1697400) 4:42:54.00 sysContact.0 : Andy Brock, GGSG sysName.0 : ass=5540-3 sysLocation.0 : RTP.NC - Context 2 sysServices.0 : 4	

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.

Browse MIB	
ile ⊻iew <u>H</u> elp	
Name or address:	Community name: 3P:authpass:privpass/titand
	Jan: autopass: privpass/titand
MIB object ID: .iso.org.dod.internet.mgmt.mib-2	
, iso.org. dod. internet. mgmt. mib-2	
⊕ ccitt	Describe
i⇔ iso i⊡- org	Start Query
ia dod	Stop Query
i⊟- internet	Stob landià
Messages:	
Received 140 bytes from gasg-rms	2 sizes see (127.0.0.1) set 4747.
0: 30 81 89 02 01 01 04 14 33 9	50 3a 61 75 74 68 70 03P:authp
16: 61 73 73 3a 70 72 69 76 70 VIIB instance: 32: 61 6e 64 65 73 a2 65 02 02	51 73 73 21 74 53 74 ass:privpass/tit
48: 00 30 59 30 3f 06 08 2b 06 (64: 33 43 69 73 63 6f 20 41 64 (
	41 70 70 6c 69 61 6e Security Applian
MIB <u>values:</u> 96: 63 65 20 56 65 72 73 69 6f 1 svsDescr.0 : Cisco / 112: 29 32 31 30 30 16 06 0b 2b	

Figure 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\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<mark>>snmpget-c "3P;MD5^authpass;DES^privpass/KEEP/titandes"</mark>
10.0.0.33 sysDescr.0
```

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

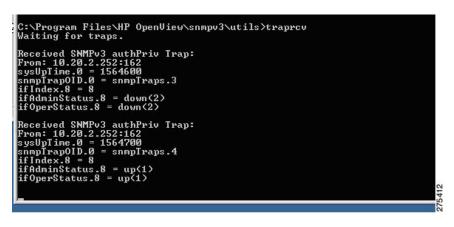
cicoasa (config) # snmp-server host inside 10.0.0.10 traps version 3 titandes

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

Figure 43: 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**.

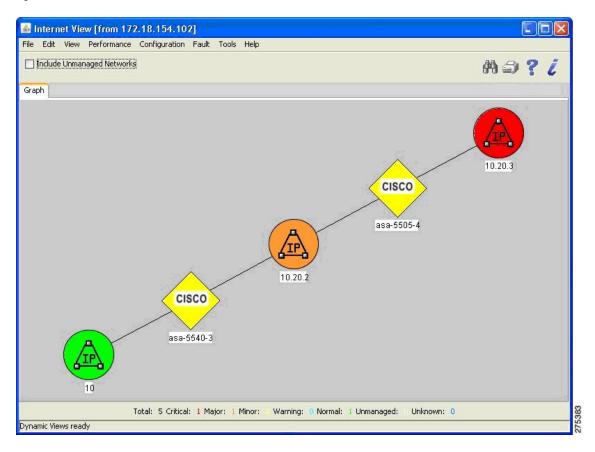
The Internet View window appears.

Figure 44: NNM Home Base Window

			on Mar 16, 2009 8		ter that date, the numb N%\ovnnmPassword or	
	ger Starter Edition I re information on ol			09 8:28:00 AM I	EDT	
w						0
eighbor View 😽 🚺	Launch View					?
ighbor View						
ternet View ps	presentation of s from the select		vice and its (connector dev:	ices, within a sp	ecified
th View						
de Status Summarv	Alarm Browser About					
aa statas saminai y	Alami browser ADOUC					
		Node St	tatus Summary as of	Feb 11, 2009 11:29:2	2 AM EST	
Critical :						
-	0 (0%)					
100 C	2 (40%)					
Warning :						
	3 (60%)		1			
Unknown :						
Total :	5					
amic Views ready						
anno viewo ieduy						

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

Figure 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

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 46: Login Page

prcsm1 - Microsoft Internet Exp	lorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
) Back 🔹 🕘 👻 😰 🔥 🔎	Search Favorites 🔮 Media 🤣 🎰 🤯 🚍	
dress 🙋 https://prcsm1/CSCOnm/s	ervlet/login/login.jsp	💌 🔁 Go 🛛 Links 🎇
	JavaScript: prcsm1 Labled User ID: admin Cookies: Password: Enabled User ID: admin Browser: Supported Version CiscoWorks CiscoWorks Copyright (c) 1998 - 2008 Cisco Systems, Inc. All rights reserved. rights reserved.	Tusted sites
50		2
Done		🕒 🖉 Trusted sites

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 47: CiscoWorks LMS Portal Page

prcsm1 - LMS - Fund le Edit View Fav	tional - M orites <u>T</u> o		net Explo	rer			_ @ ×	
) Back + 🕤 - 💌			Favorites	😽 Media 🚱	🔊 - 🖕 🔜 🗌			
dress 🖉 http://prcsm			ayout?p_l_i	id=default		-	Go Links »	
cisco		Cis	coW	orks LN	IS Portal (Welcom Prcsm1) Home Logout Help My Portal C Public	o About	
Functional Sy	stem	Network	DFM	CS		10 Apr 2009,	, 17:50 PDT	
LMS Workflows De	mo			Common Service	es	Setup Center		
and the second sec	Using Baseline Templates Building and exporting a network map using Campus			··Home > Server > Software Cen	ter	··Server Setup ··Server Settings		
Discovering the Network Using NetConfig to deploy mass configuration changes			 Device and Credentials Groups 		Device Diagnostic Tools			
Using SV/IM to upg			- MIC	Device Fault Manager		··Device Center		
CiscoWorks Assist	Using User Tracking to find an end host by IP or MAC		or MAC	···Home ···Alerts and Activ ···Device Manager		CiscoWorks Product Updates		
··Home · Workflows · Administration	··Home >Workflows			Fault History Notification Services Configuration		Revalidated VeriSign Certificate for Campus Manager Revalidated VeriSign Certificate for Internetwork Performance w More Updates	Aonitor	
-				External Links			_	
			 Cisco.com Re CiscoWorks R Third Party Custom Tools 	Resources				
Done						Trusted	sites	

Using the Device Center

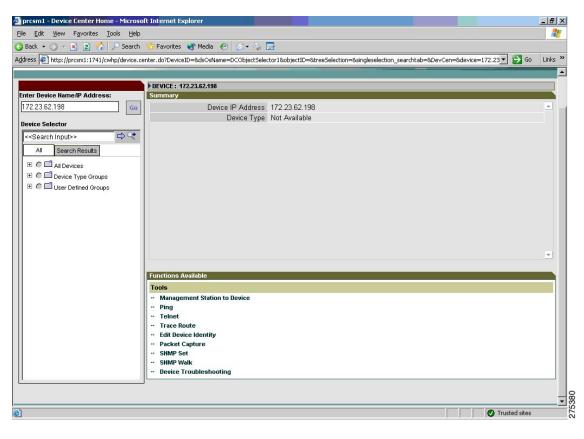
To manage devices, perform the following steps:

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 48: Device Center Home Window



Performing an SNMP Walk

To perform an SNMP walk, perform the following steps:

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

The SNMP Walk dialog box appears.

Figure 49: SNMP Walk Dialog Box

🝘 prcsm1 - Device Center Home - Microso	ft Internet Explorer				_ & ×
Eile Edit View Pavorites Iools Help					
🔇 Back 👻 🕥 👻 😰 🐔 🔎 Search					
Address Address http://prcsm1:1741/cwhp/device.ce	enter.do?DeviceID=&dsOsName=D	http://prcsm1 - prcsm1 - SNM	P Walk - Microsoft Internet Explorer	× G0	Links »
			SNMP Walk		
Enter Device Name/IP Address:	DEVICE : 172.23.62.198	Device Name:	172.23.62.198		
172.23.62.198 Go	Device IF	SNMP Version:	C1 C2c € 3		
Device Selector	De	Read Community String (v1 or v2c):			
< <search input="">> 🖘 💎</search>		SNMPv3 Username:	md5des		
All Search Results		SNMPv3 Auth Password:	1		
E C All Devices		SNMPv3 Auth Protocol:			
🗉 🌀 🗂 Device Type Groups					
E C 🖬 User Defined Groups		SNMPv3 Privacy Password:			
		SNMPv3 Privacy Protocol:	DES 💌		
		SNMPv3 Context Name*:			
		Starting OID*:	system		
		Output OIDs Numerically*:			
	-	Output Indexes Numerically*:			<u>•</u>
	Functions Available	SNMP Timeout*:	10		
	Tools	Debug*:			
	Management Station to D Ping Telnet		OKCand	el Help	
	- Trace Route	* Optional		*	
	Edit Device Identity Packet Capture	🛃 Done	🖉 Truste	ed sites	
	SNMP Set				
	- Device Troubleshooting				
p]				(c
					275416
🛃 Done				🖉 Trusted sites	27

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.
- 1. (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.

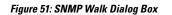
Figure 50: SNMP Walk Results Example

😰 prcsm1 - Device Center Home - Microso	ft Internet Explorer	🗿 http://prcsm1 - prcsm1 - SNMP Walk Results - Microsoft Intern 💶 💌	_ & ×
Eile Edit View Favorites Iools Help			27
🔇 Back 👻 🕤 🛩 🖹 😰 🚮 🔎 Search	💏 Favorites 🔌 Media 🥝 😥 - 🔪	SNMP Walk Results	
Address Addres	enter.do?DeviceID=&dsOsName=DCObjectSele	The following is a SNMP walk of device 172.23.62.198 starting from system	🔁 Go 🛛 Links 🎽
		SNMP Walk Output	
	DEVICE : 172.23.62.198	system	
Enter Device Name/IP Address:	Summary		
172.23.62.198 Go	Device IP Address	sysDescr.0 = STRING : Cisco Adaptive Security Appliance Version 8.2(0)232 sysObjectID.0 = OID : ciscoASA5520	
Device Selector	Device Type	sysUpTime.0 = Timeticks : 3 days 1:41:21 sysContact.0 = STRING : hari d	
< <search input="">> 🖒 🗘</search>		sysName.0 = STRING : ciscoasa	
		sysLocation.0 = STRING : sjc sysServices.0 = INTEGER : 4	
All Search Results			
E C C All Devices			
C Device Type Groups		Close	
E C 🗖 User Defined Groups			
	-		·
			·
	Functions Available		
	Tools		
	Management Station to Device Ping		
	- Telnet		
	Trace Route		
	Edit Device Identity		
	Packet Capture SNMP Set		
	SNMP Walk		
	- Device Troubleshooting		
t.	1		L
Deep.			N

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.



sas w not the cant the the week	encer doi bevicetb-basosivame-b		IP Walk - Microsoft Internet Explorer	o Links
	DEVICE : 172.23.62.198		SNMP Walk	
er Device Name/IP Address:	Summary	Device Name:	172.23.62.198	
2.23.62.198 Go	Device IF	SNMP Version:	C 1 C 2c € 3	
vice Selector	De	Read Community String (v1 or v2c):	0 0 0 0 0 0	
<search input="">> 🖙 💐</search>		SNMPv3 Username:	md5aes256	
All Search Results		SNMPv3 Auth Password	••••••	
E C C All Devices		SNMPv3 Auth Protocol:	MD5 💌	
 ⊞ ■ □ Device Type Groups User Defined Groups 		SNMPv3 Privacy Password		
		SNMPv3 Privacy Protocol	AES256 -	
		SNMPv3 Context Name*:	DES	
		Starting OID*:	3DES AES128	
		Output OIDs Numerically*:	AES192	
		Output Indexes Numerically*:	AES256	*
	Functions Available	SNMP Timeout*:	10	
	Tools - Management Station to D - Ping - Telnet - Trace Route - Edit Device Identity - Packet Capture	Debug*:		
			OK Cancel Help	
		* Optional	- -	
		Done	Trusted sites	
	SNMP Set SNMP Walk Device Troubleshooting			

Figure 52: SNMP Version 3 Parameters

	SNMP Walk	
Device Name:	172.23.62.198	
SNMP Version:	O 1 O 2c ⊙ 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*:		
Output Indexes Numerically*:		
SNMP Timeout*:	10	
Debug*:		
	OK Cancel Help	

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

Figure 53: SNMP Walk Results Dialog Box

SNMP Walk Results				
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 : sic sysServices.0 = INTEGER : 4 TNumber.0 = INTEGER : 4 Thumber.0 = INTEGER : 1 findex.1 = INTEGER : 1 findex.3 = INTEGER : 2 findex.4 = INTEGER : 3 findex.5 = INTEGER : 4 findex.5 = INTEGER : 4 findex.5 = INTEGER : 6				
findey 7 = INTEGER 17	-			
C	ose			

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 54: Management Station to Device Dialog Box

🕽 prcsm1 - Device Center Home - Microsoft Internet Explorer 🛛 🔛	ttp://presint - presint - Management Station To Device - Microsoft Internet 🖃 💷	_ <u>-</u>
Elle Edit View Favorites Iools Help	T UDP T TFTP	1
3) Back 🔹 🕤 👻 😰 🐔 🔎 Search 🔹 Favorites 😻 Media 🧑	SSH Version: © 1 C 2	
Address 🙋 http://prcsm1:1741/cwhp/device.center.do?DeviceID=&dsOsName=DCOb	Timeout (in seconds):	Links »
	☐ SNMPv1/v2c	
Enter Device Name/IP Address: Summary	SNMP Version: C 1 @ 2c	
172.23.62.198 Go Device IP Ac	Read Community String:	
Device Selector	Write Community String:	
	Timeout (in seconds):	
All Search Results	☐ SNMPv3	
	Read Username:	
	Read Auth Password:	
E C I User Defined Groups	Read Auth Protocol: None	
	Read Privacy Password:	
	Read Privacy Protocol: None	
	Write Username:	
	Write Auth Password:	
	Write Auth Protocol: None -	<u> </u>
Functions Available	Write Privacy Password:	
Tools	Write Privacy Protocot None	
Management Station to Devic Ping	Timeout (in seconds): 2	
·· Telnet		
	OK Cancel Help	
··· Packet Capture		
SNMP Set SNMP Walk	* Optional Note: The check will be done only for protocol connectivity. Credentials for the	
··· Device Troubleshooting	corresponding protocols will not be tested.	
	Done 🥥 Trusted sites	

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 55: Management Station Device Results Dialog Box

	☆ Favorites 🔮 Media 🔗 😥 🌏 🛃 anter.do?DeviceID=&dsOsName=DCObjectSelector3&object	🗿 http://prcsm1 - prcsm1 - Management Station To Device Resul 🚛 🔲 🗴
All Devices Type Groups	DEVICE : 172.23.62.198 Summary Device IP Address 172.23.62 Device Type Not Avails	Interface Test Results Note: Protocol connectivity has been checked. Credentials for the protocol have not been tested. Interface Found: 172.23.62.198 Status: UP Test Results SNMPRV3(Read) Okay Sent: 5 recvd: 5 min:0 max:0 avg:0 timeout:2 min_size: 1472 protocot snmpv3_get port: 0 SNMPVv3(Write) Failed Sent: 5 recvd:0 min:0 max:0 avg:0 timeout:2 min_size: 1472 protocot snmpv3_set port: 0 Cancel
	Functions Available Tools - Management Station to Device - Ping - Telnet - Trace Route - Edit Device Identity - Packet Capture - SNMP Set - SNMP Valk - Device Troubleshooting	