



## **CiscoWorks** およびサードパーティ製ツールを使用した **SNMP** バージョン **3** 実装ガイド

2014 年 4 月

**Cisco Systems, Inc.**  
<http://www.cisco.com/jp>

Cisco は世界各国 200 箇所にオフィスを開設しています。  
各オフィスの住所、電話番号、FAX 番号は  
当社の Web サイト  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices) をご覧ください。

Text Part Number:

**【注意】 シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。**

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。  
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリック ドメイン パージョンの一部として開発されたプログラムに適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CiscoWorks およびサードパーティ製ツールを使用した SNMP バージョン 3 実装ガイド  
© 2014 Cisco Systems, Inc. All rights reserved.



はじめに	v
マニュアルの入手方法およびテクニカル サポート	v
その他のツールに関する資料の入手	v

---

**CHAPTER 1**

概要	1-1
ネットワーク管理ツール	1-1
ネットワーク トポロジ	1-2
ASA 設定	1-2

---

**CHAPTER 2**

ネットワーク管理ツールの使用方法	2-1
Net-SNMP	2-1
MIB のポーリング	2-1
トラップの送信	2-2
SilverCreek SNMP テストスイート	2-3
SilverCreek の実行	2-3
SNMP バージョン 3 エージェントのセットアップ	2-5
MIB のロードと削除	2-7
テストスイートの実行	2-8
デバッグの有効化	2-10
MIB のテスト	2-12
MIB ブラウザへのアクセス	2-13
通知トラップ メッセージの受信	2-15
パフォーマンスのテスト	2-16
Ipswitch WhatsUp Gold	2-17
Ipswitch WhatsUp Gold の起動	2-18
SNMP エージェントの新規追加	2-18
SNMP バージョン 3 クレデンシャルの追加	2-19
WhatsUp Gold Web インターフェイスの使用方法	2-22
SNMP MIB または OID のウォーク	2-23
SNMP トラップの設定	2-27
HP OpenView Network Node Manager	2-30
NNM のインストール	2-31
NNM の起動	2-31
MIB のロード	2-32

現在のマップへのネットワークの追加	2-33
特定の SNMP バージョン 3 パラメータの設定	2-36
グローバルな SNMP バージョン 3 クレデンシヤルの設定	2-37
特定の SNMP バージョン 3 クレデンシヤルの設定	2-38
ノード情報の表示	2-38
NNM MIB ブラウザの設定	2-39
SNMP バージョン 3 の No-auth/No-priv 接続の設定	2-40
SNMP バージョン 3 の MD5 Auth/No-priv 接続の設定	2-40
SNMP バージョン 3 の SHA Auth/No-priv 接続の設定	2-40
SNMP バージョン 3 の MD5 Auth/Priv 接続の設定	2-41
SNMP バージョン 3 の SHA Auth/Priv 接続の設定	2-41
MIB の参照	2-41
MIB ブラウザのパケット トレースの実行	2-42
NNM SNMP バージョン 3 トラップ ビューアの使用法	2-43
HP OpenView NNM Web アプリケーションの使用法	2-44
CiscoWorks	2-46
CiscoWorks の起動	2-47
CiscoWorks LMS Portal の概要	2-48
Device Center の使用法	2-48
SNMP ウォークの実行	2-49
Management Station to Device ツールの使用法	2-54



## はじめに

---

この前書きは、次の項で構成されています。

- [マニュアルの入手方法およびテクニカル サポート \(v ページ\)](#)
- [その他のツールに関する資料の入手 \(v ページ\)](#)

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

「*What's New in Cisco Product Documentation*」に配信登録すると、新しい(または改訂された)シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。

## その他のツールに関する資料の入手

その他のツールについては、次の関連資料を参照してください。

- Net-SNMP Version 5.1.2 のマニュアルおよびオンライン ヘルプ (Linux)
- IWL Silvercreek テスト スイートのチュートリアルおよびオンライン ヘルプ (最新バージョン)
- HP OpenView NNM SPI Version 7.53 のマニュアル
- Ipswitch WhatsUp Gold Version 12.3 のマニュアルおよびオンライン ヘルプ
- CiscoWorks for Windows LMS Version 3.1 のオンライン ヘルプおよびチュートリアル





## 概要

SNMPバージョン3では、User-based Security Model (USM; ユーザーベースセキュリティモデル) および View-based Access Control Model (VACM; ビューベースアクセスコントロールモデル) による認証オプションやプライバシー オプションを使用することにより、SNMP エージェントによる SNMP トランザクションのセキュアな通信が実現されます。SNMPバージョン1 および SNMPバージョン2c では、MIB のアクセス コントロールを行う場合ユーザは認識されないため、暗号化されたプライバシー オプションを使用して認証を行うことはできません。VACM のサポートは、次リリース以降に先送りされました。

この章では、ASA ソフトウェアバージョン 8.2(1) 以降が稼働しているデバイス上で、SNMPバージョン3 を介して ASA と通信可能な CiscoWorks およびいくつかのサードパーティ製ツールをインストールする方法、設定する方法、および使用する方法について説明します。

この章は、次の項目を取り上げます。

- [ネットワーク管理ツール\(1-1 ページ\)](#)
- [ネットワーク トポロジ\(1-2 ページ\)](#)
- [ASA 設定\(1-2 ページ\)](#)

## ネットワーク管理ツール

このマニュアルでは、次のネットワーク管理ツールについて説明します。

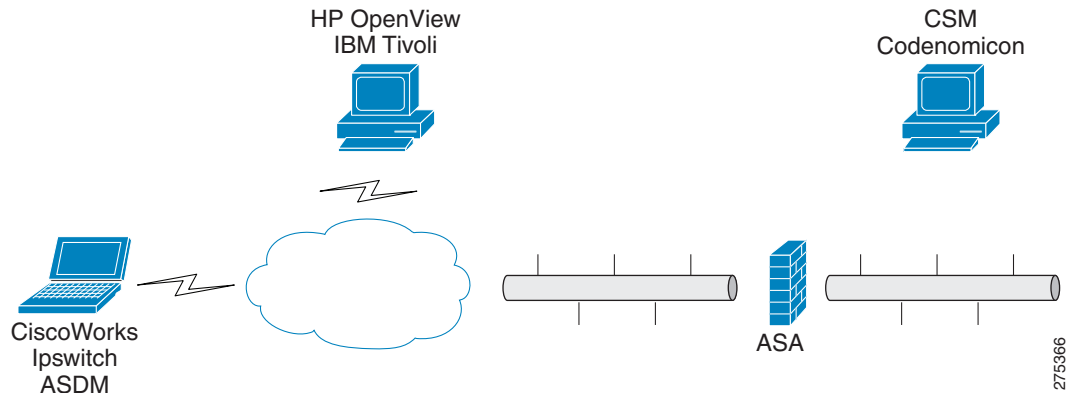
- Net-SNMP (CLI アプリケーション)
- IWL SilverCreek (SNMP テストスイート)
- Ipswitch WhatsUp Gold
- HP OpenView NNM
- CiscoWorks for Windows LMS

シスコでは、これらのツールに対して、NMS および ASA との間の相互運用性試験をすでに実施しています。

# ネットワーク トポロジ

図 1-1 は、SNMP バージョン 3 を実装するためのネットワーク トポロジを示したものです。

図 1-1 SNMP バージョン 3 を実装するためのネットワーク トポロジ



## ASA 設定

ASA を使用するためには、SNMP サーバグループ、そのグループに関連付けられた SNMP サーバユーザ、および SNMP トラップの受信ユーザを指定するための SNMP サーバホストを設定する必要があります。

SNMP バージョン 3 の動作を設定する際に必要となるコマンドは次のとおりです。

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

ASA の構成例を以下に示します。

```

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

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

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

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

```





## ネットワーク管理ツールの使用方法

この章では、CiscoWorks およびいくつかのサードパーティ製ネットワーク管理ツールについて説明します。内容は次のとおりです。

- [Net-SNMP\(2-1 ページ\)](#)
- [SilverCreek SNMP テストスイート\(2-3 ページ\)](#)
- [Ipswitch WhatsUp Gold\(2-17 ページ\)](#)
- [HP OpenView Network Node Manager\(2-30 ページ\)](#)
- [CiscoWorks\(2-46 ページ\)](#)

### Net-SNMP

Net-SNMP Version 5.1.2 には、次のようなツールおよびライブラリが用意されています。

- 拡張可能なエージェント
- SNMP ライブラリ
- SNMP エージェントに対して情報を要求または設定するためのツール
- SNMP トラップを生成および処理するためのツール

Net-SNMP ネットワーク管理ツールは次の URL からダウンロードできます。

<http://sourceforge.net/projects/net-snmp/>

この項では、次のトピックについて取り上げます。

- [MIB のポーリング\(2-1 ページ\)](#)
- [トラップの送信\(2-2 ページ\)](#)

### MIB のポーリング

ASA の設定を完了した後で MIB をポーリングする場合は、NMS から ASA に対して次のような `snmpwalk` コマンドを実行します。



(注) `snmpwalk` コマンドを実行する場合、Linux 上の Net-SNMP に対しては特別な設定を行う必要はありません。

```
[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
```

次に示すのは、**snmpwalk** コマンドを実行した場合の出力例です。

```
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
```

## トラップの送信

ASA により送信されたトラップは信頼されます。そのため、**snmptrapd** コマンド内で作成されたユーザは、そのトラップを送信した **EngineID** に関連付けられている必要があります。

関連付けを行う手順は次のとおりです。

**ステップ 1** /var/net-snmp/snmptrapd.conf ファイル内に、次のステートメントを入力します。

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

このステートメントの中に現れる次の各パラメータを定義します。

- **ENGINEID**: トラップを送信するアプリケーションの EngineID
- **myuser**: トラップを送信する USM ユーザ名
- **authentication protocol**: 認証タイプ (SHA または MD5。SHA を推奨)
- **"my authentication pass"**: 秘密認証キーを生成する際に使用する認証パスフレーズ。スペースを含むパスフレーズは引用符で囲んでください。
- **privacy protocol**: 使用する暗号のタイプ (AES または DES。AES を推奨)
- **"my privacy pass"**: 秘密暗号キーを生成する際に使用する暗号化パスフレーズ。スペースを含むパスフレーズは引用符で囲んでください。引用符で囲まない場合、その暗号化パスフレーズは認証パスフレーズと同じ値に設定されます。

**ステップ 2** /tmp/snmptrapd.conf ファイル内に、次のステートメントを入力します。

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

**ステップ 3** そのファイルを指定して、**snmptrapd** コマンドを実行します。



(注) このプロセスはフォアグラウンドで実行されます。使用されるのは指定されたコンフィギュレーションファイルのみで、ログとして **stderr** ファイルにメッセージが記録されます。

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

**ステップ 4** 次のようなコマンドを入力し、ASA から **snmptrap** コマンドを実行して、リンクダウントラップまたはリンクアップトラップを送信します。

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

次に示すのは、`snmptrap` コマンドを実行した場合の出力例です。

```
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 テストスイート

SilverCreek SNMP テストスイートを使用すると、プライベート MIB および標準 MIB から、SNMP に準拠していない部分や SNMP の実装エラーを検出できます。このソフトウェアの無償バージョンを次の URL からダウンロードできます。

<http://www.iwl.com/trial-downloads/silvercreek-trial.html?Itemid=>

この項では、次のトピックについて取り上げます。

- [SilverCreek の実行 \(2-3 ページ\)](#)
- [SNMP バージョン 3 エージェントのセットアップ \(2-5 ページ\)](#)
- [MIB のロードと削除 \(2-7 ページ\)](#)
- [テストスイートの実行 \(2-8 ページ\)](#)
- [デバッグの有効化 \(2-10 ページ\)](#)
- [MIB のテスト \(2-12 ページ\)](#)
- [通知トラップメッセージの受信 \(2-15 ページ\)](#)
- [パフォーマンスのテスト \(2-16 ページ\)](#)

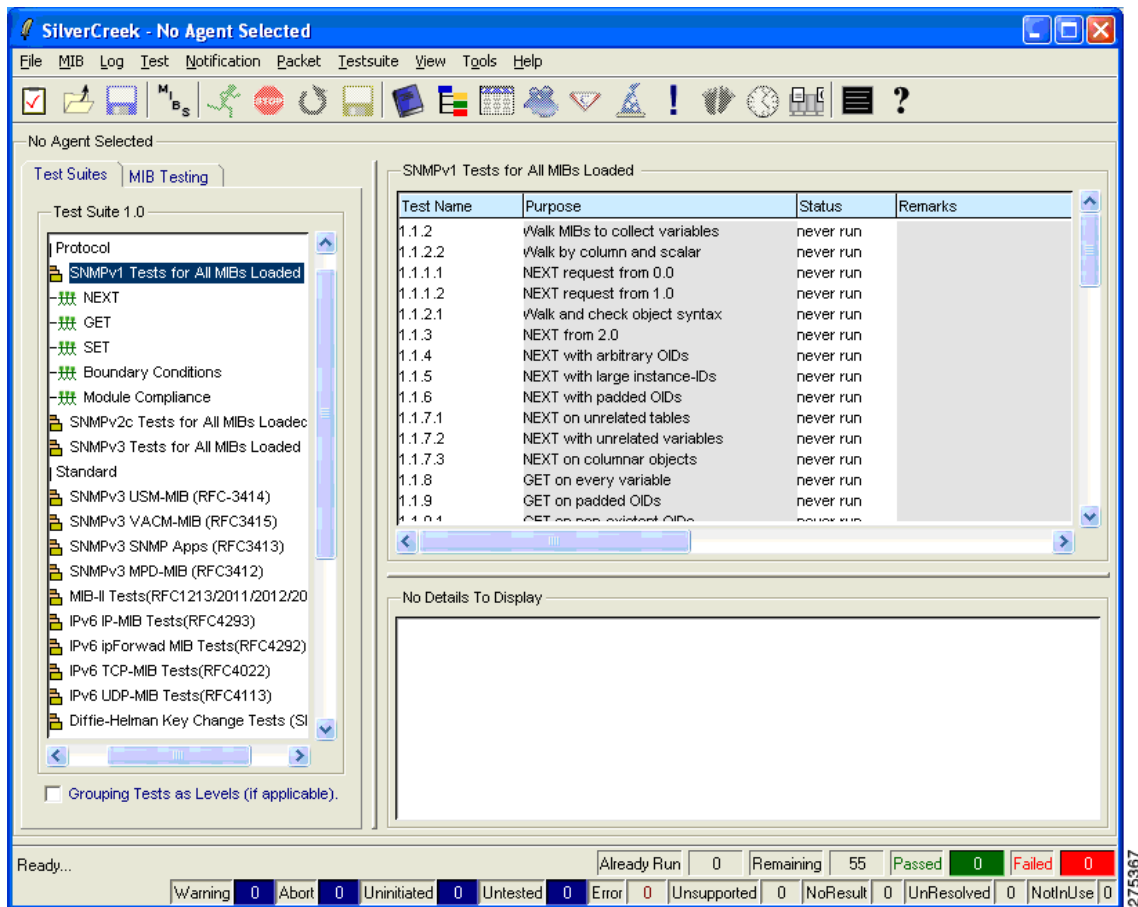
## SilverCreek の実行

SilverCreek ソフトウェアを実行する場合は、[Start] > [All Programs] > [SilverCreekMx Evaluation] > [Run Test Suite and Tools (Start Here)] を選択します。

アプリケーションが起動すると、SilverCreek のメイン ウィンドウ (図 2-1 を参照) とともにコンソール ウィンドウ (図 2-2 を参照) が開き、次のような情報が表示されます。

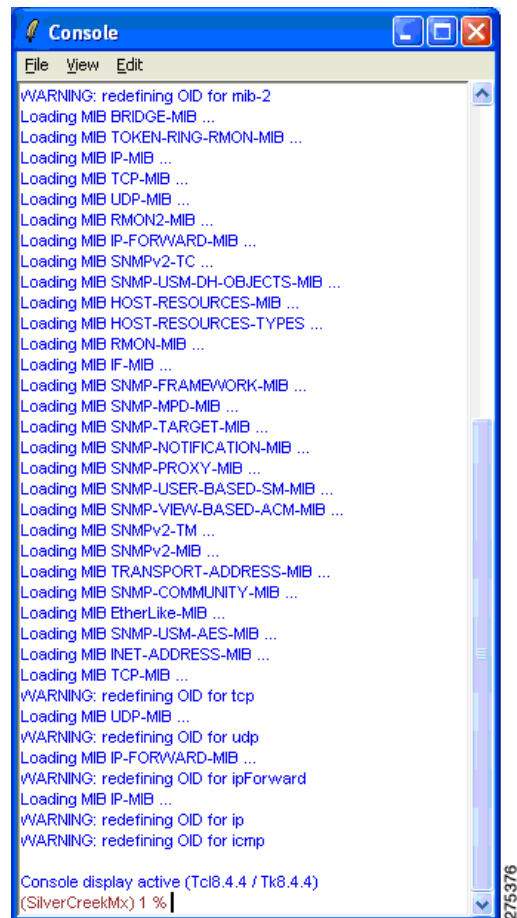
- ログメッセージ
- デバッグメッセージ
- NMS と SNMP バージョン 3 エージェントとの間でやり取りされるその他のメッセージ
- ロードされた MIB

図 2-1 SilverCreek のメイン ウィンドウ



275367

図 2-2 SilverCreek のコンソール ウィンドウ



## SNMP バージョン 3 エージェントのセットアップ

SNMP バージョン 3 エージェントのセットアップを行う手順は次のとおりです。

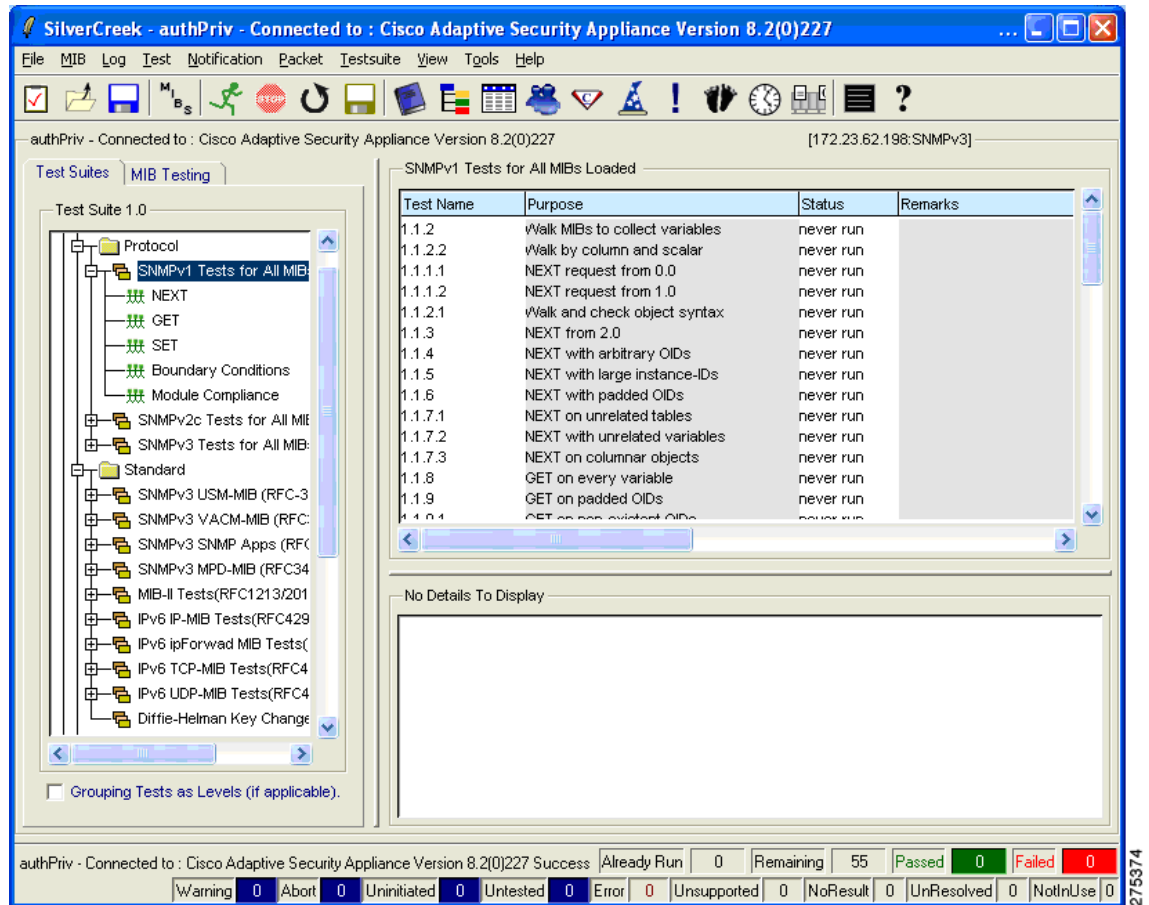
ステップ 1 [File] > [New Agent Setup] を選択します。

図 2-3 は、新しいエージェントの設定方法を示したものです。

図 2-3 [New Agent Setup] ダイアログボックス

- ステップ 2** ホスト名または IP アドレス、ポート番号、および SNMP バージョン 3 パラメータを入力します。エージェントが接続されると、左側ペインの [Test Suites] タブ (図 2-4 を参照) から SNMP テストスイートを実行できます。

図 2-4 接続済みSNMP エージェントが表示された SilverCreek のメインウィンドウ



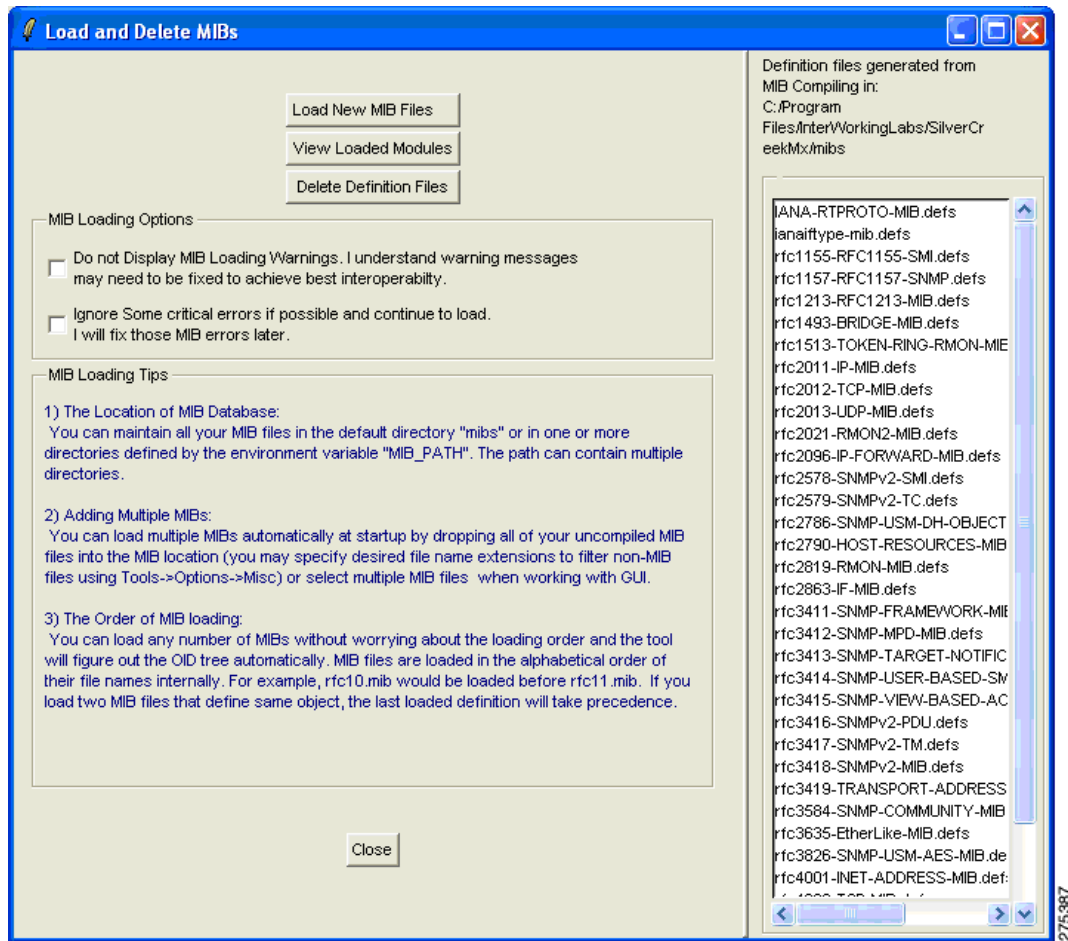
## MIB のロードと削除

MIB をロードおよび削除する手順は次のとおりです。

- ステップ 1 MIB のロードおよび削除を手動で行う場合は、[MIB] > [Load | Delete MIBs] を選択します。
- ステップ 2 ロードした MIB を表示する場合は、[View Loaded Modules] をクリックします(図 2-5 を参照)。

MIB ファイルはすべて、デフォルトの mibs ディレクトリ内に保持できます。このディレクトリは、環境変数 MIB\_PATH を使用して定義します。

図 2-5 [Load and Delete MIBs] ダイアログボックス



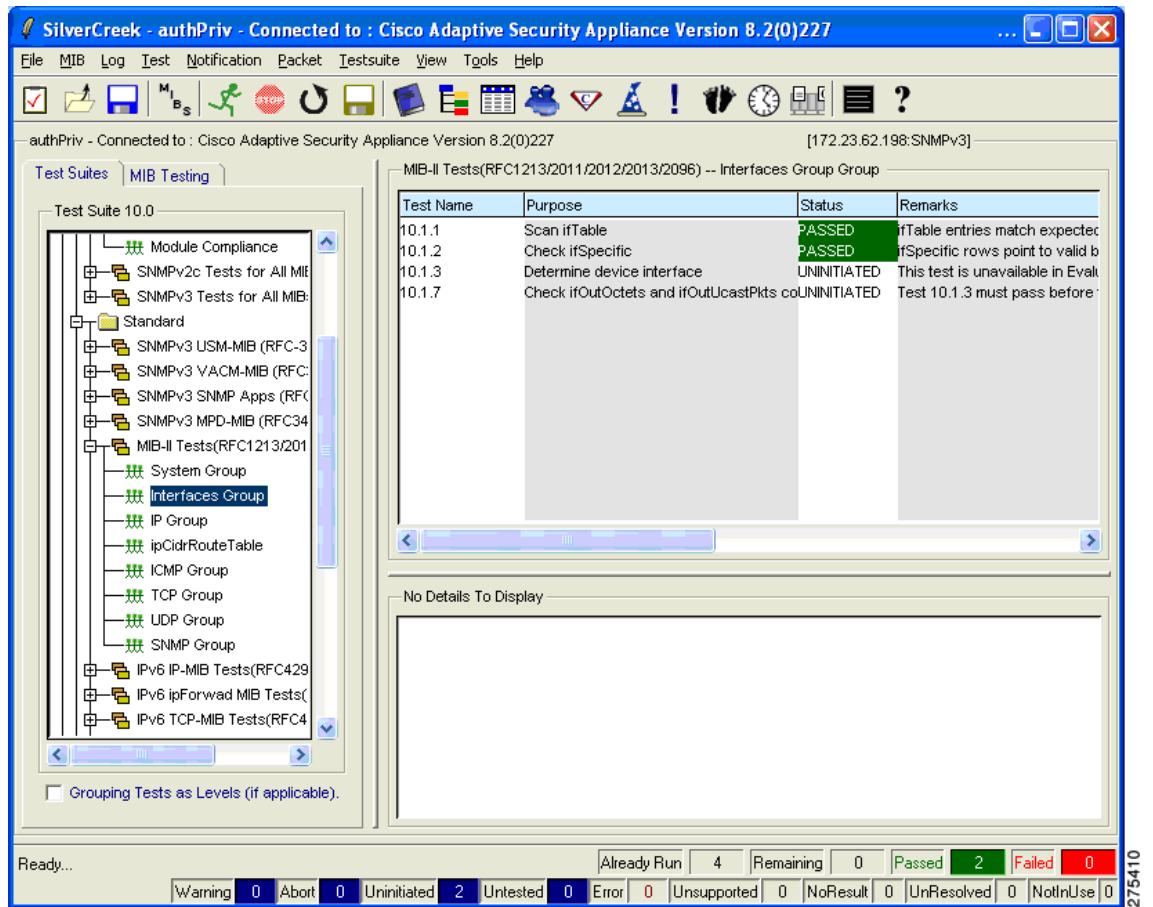
## テストスイートの実行

テストスイートを実行する手順は次のとおりです。

- ステップ 1 メイン ウィンドウの左側ペイン(図 2-6 を参照)でテスト カテゴリ (MIB-II など) を選択します。右側ペインには、選択したテスト カテゴリに対して実行できるテストがリスト表示され、下部ペインにはテストの詳細が表示されます。
- ステップ 2 1 つまたは複数のテストを選択し、[Run All or Selected Tests] をクリックします。  
[Status] 列にテストのステータスが表示されます。またウィンドウの下部には、実行されたテスト、問題なく完了したテスト、問題が検出されたテストなどの総数が表示されます。



図 2-6 選択したテストが表示されている SilverCreek のメインウィンドウ



275410

## デバッグの有効化

デバッグを有効にする場合は、[Tools] > [Options] を選択します(図 2-7 を参照)。

図 2-7 [Options] ダイアログボックスの[Debug] タブ

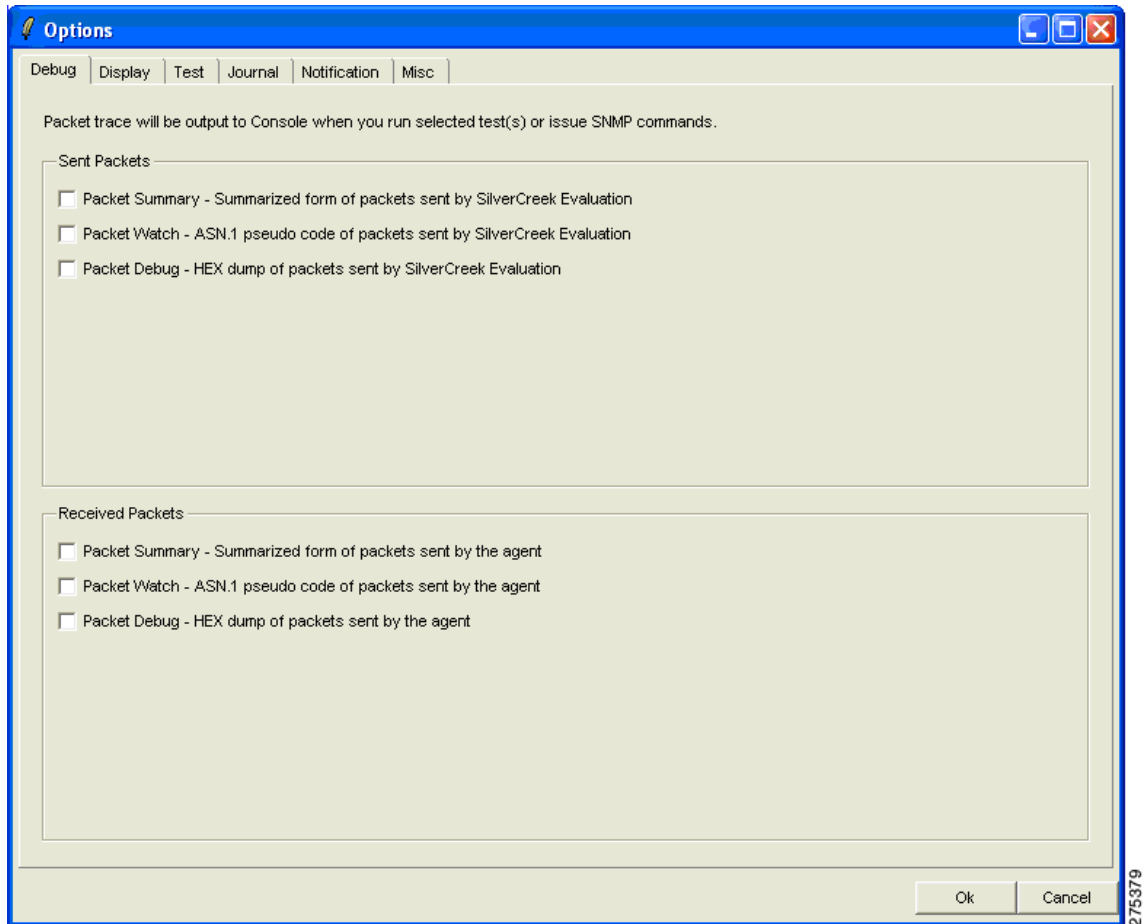


図 2-8 の画面に表示されているのは、デバッグが有効になっているためテストの実行には時間がかかるという内容の警告メッセージです。

図 2-8 警告を表示する [Notes] ダイアログボックス

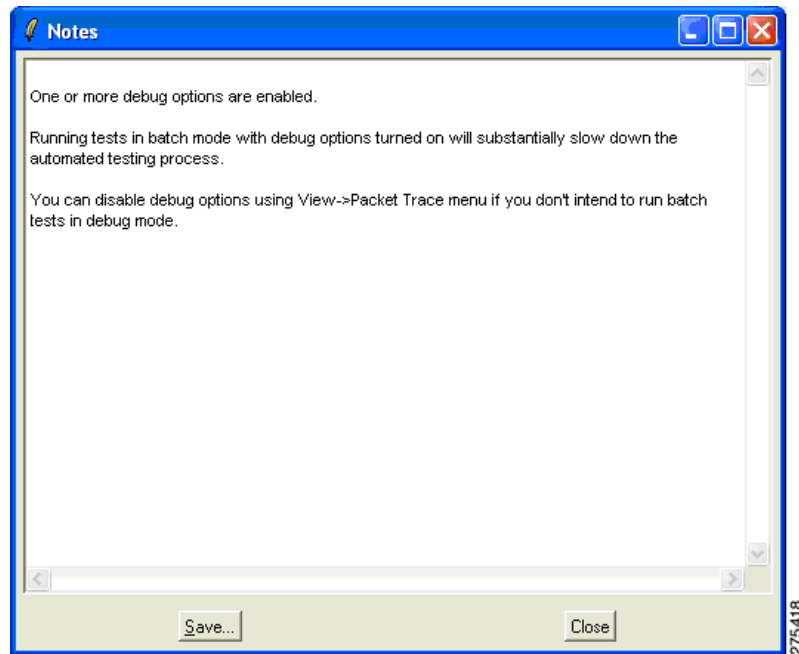
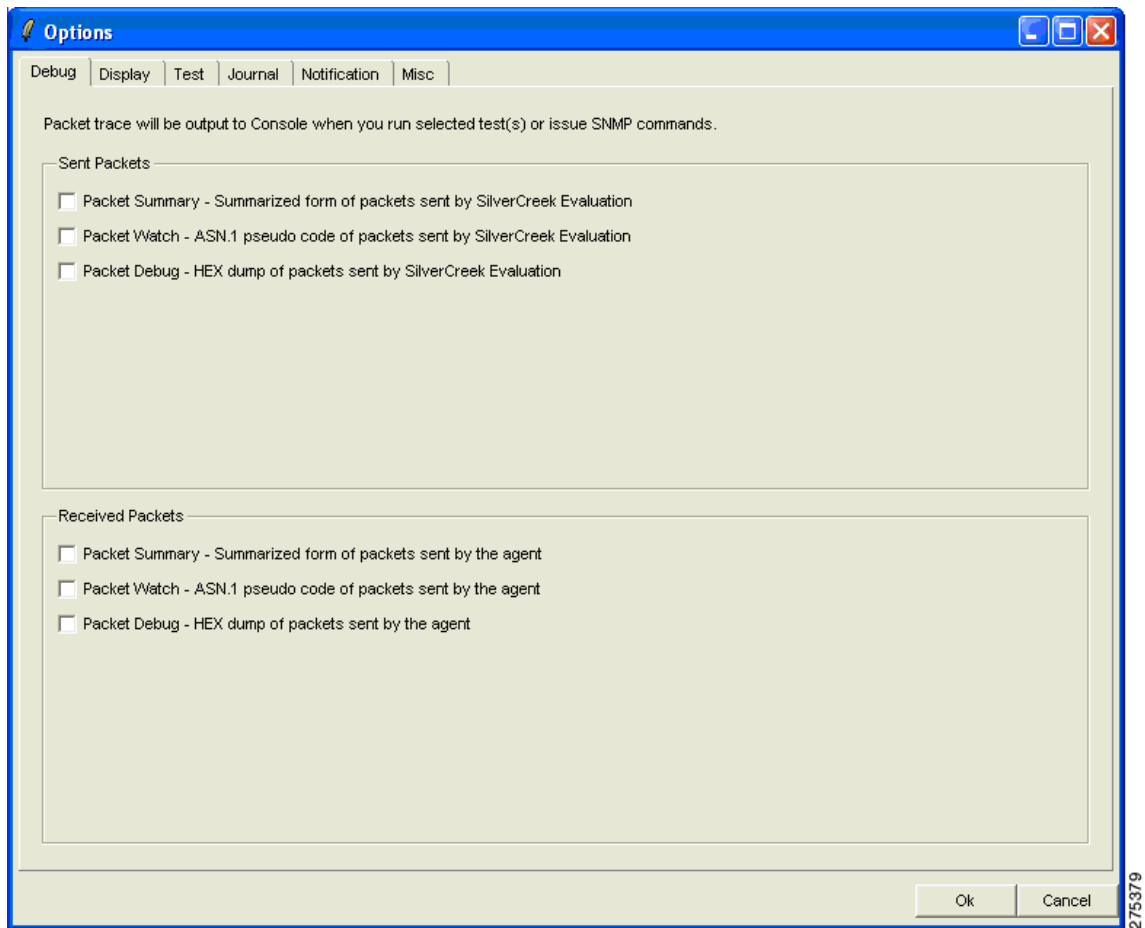


図 2-9 は、デバッグメッセージが表示されたコンソールダイアログボックスを示したものです。これらのメッセージはテストを実行した際に表示されます。

図 2-9 デバッグメッセージが表示されたコンソールダイアログボックス

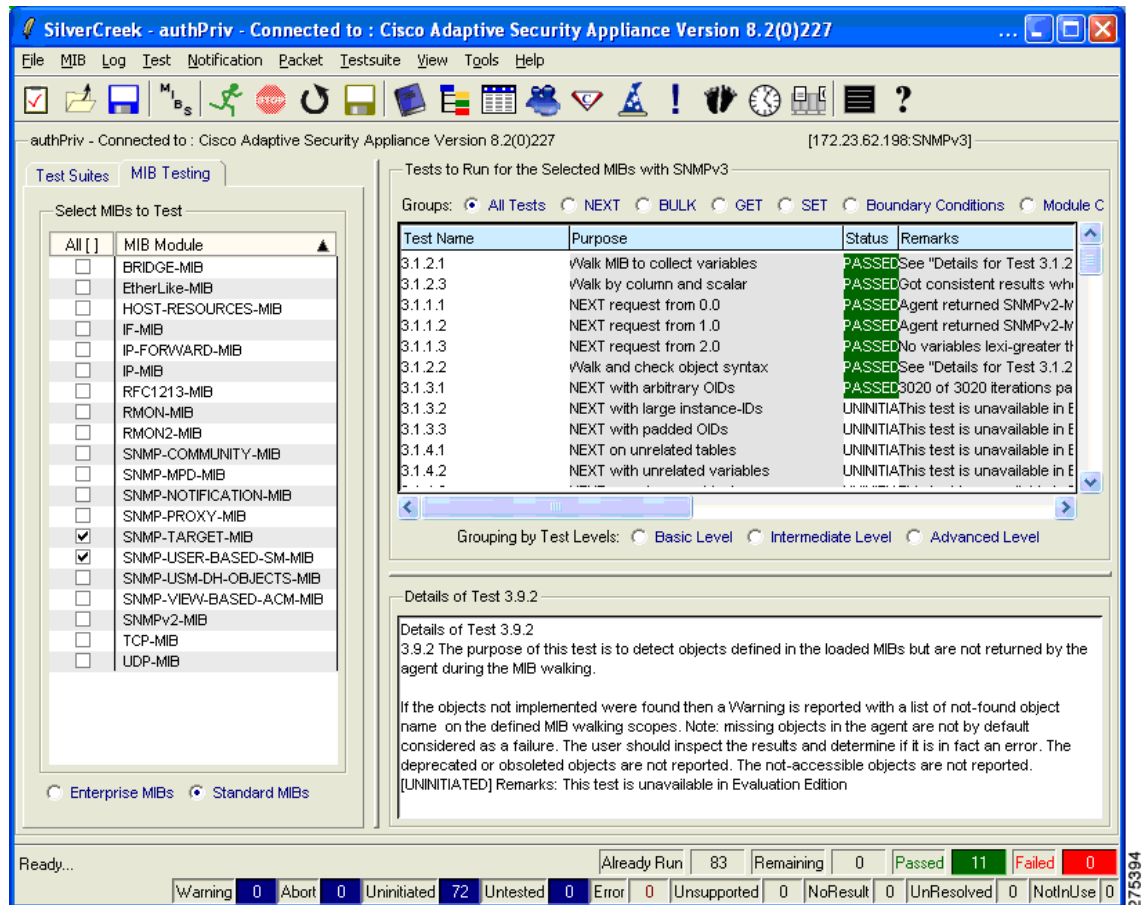


## MIB のテスト

MIB をテストする手順は次のとおりです。

- 
- ステップ 1 メインウィンドウの左側ペインにある [MIB Testing] タブをクリックします。  
ロードされ、テストに使用可能なすべての MIB モジュールが表示されます(図 2-10 を参照)。
  - ステップ 2 テストが必要な MIB に対応するオプション ボタンをクリックします。
  - ステップ 3 右側ペインで、実行する必要があるテストを選択します。  
テストの目的および詳細が下部ペインに表示されます。

図 2-10 MIB のテストの詳細が表示された SilverCreek のメイン ウィンドウ



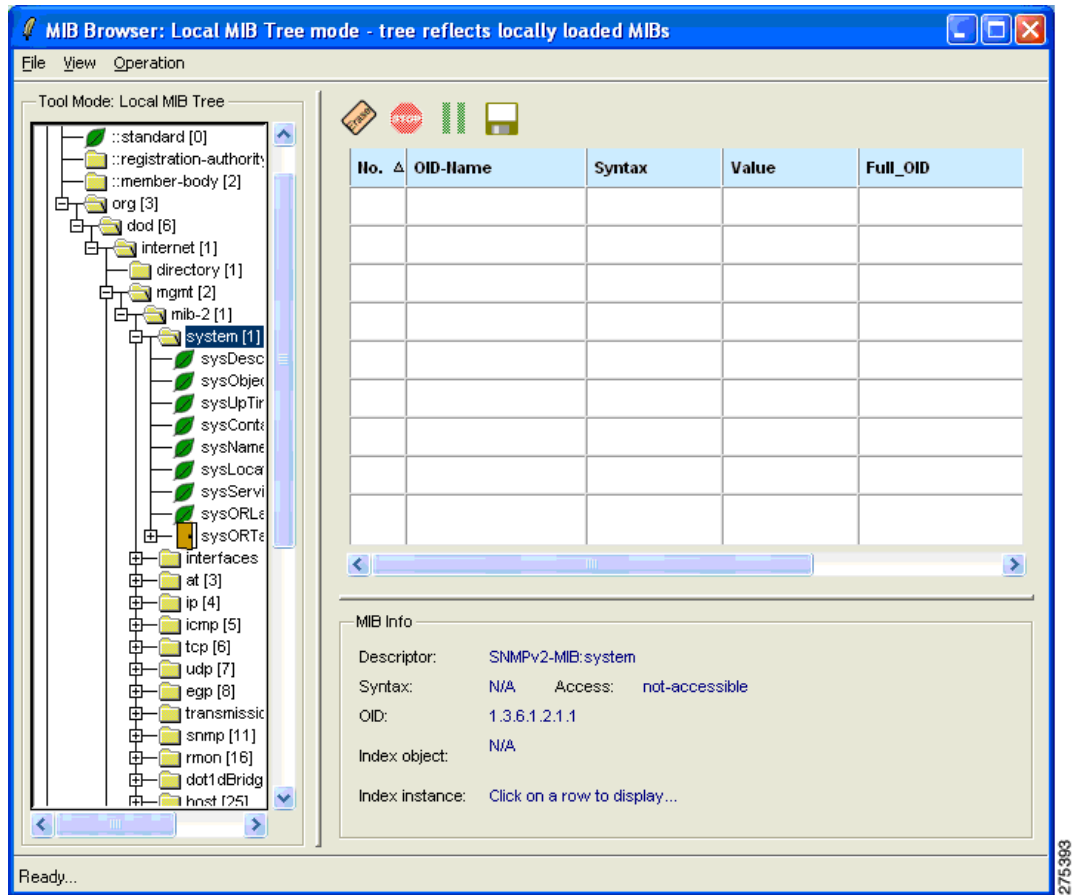
## MIB ブラウザへのアクセス

MIB ブラウザにアクセスする手順は次のとおりです。

**ステップ 1** メインウィンドウで、[MIB] > [MIB Browser] を選択します。

MIB ブラウザ(図 2-11 を参照)を使用すると、MIB の個別ポーリングや選択したツリーのウォークなど、エージェントの MIB に対してより細かい操作が可能です。

図 2-11 [MIB Browser: Local MIB Tree Mode] ダイアログボックス



- ステップ 2 目的の OID (.iso.org.dod.internet.mgmt.mib-2.system) までスクロールして [system] を右クリックし、ツリーをウォークするためのオプションを選択します。
- 右側ペインに MIB の参照結果が表示されます (図 2-12 を参照)。

図 2-12 MIB の参照結果が表示された [MIB Browser: Local MIB Tree Mode] ダイアログボックス

No.	OID-Name	Syntax	Value	Full_OID
1	sysDescr.0	DisplayString	Cisco Adaptive S	1.3.6.1.2.1.1.1.0
2	sysObjectID.0	ObjectID	1.3.6.1.4.1.9.1.67	1.3.6.1.2.1.1.2.0
3	sysUpTime.0	TimeTicks	8252500	1.3.6.1.2.1.1.3.0
4	sysContact.0	DisplayString	hari d	1.3.6.1.2.1.1.4.0
5	sysName.0	DisplayString	ciscoasa	1.3.6.1.2.1.1.5.0
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

Descriptor: SNMPv2-MIB:system  
 Syntax: N/A Access: not-accessible  
 OID: 1.3.6.1.2.1.1  
 Index object: N/A  
 Index instance: Click on a row to display...



(注) SNMP MIB に関する未解決の警告の一覧については、Cisco ASA 5500 シリーズのリリースノート  
を参照してください。

## 通知トラップメッセージの受信

通知トラップメッセージを受信する手順は次のとおりです。

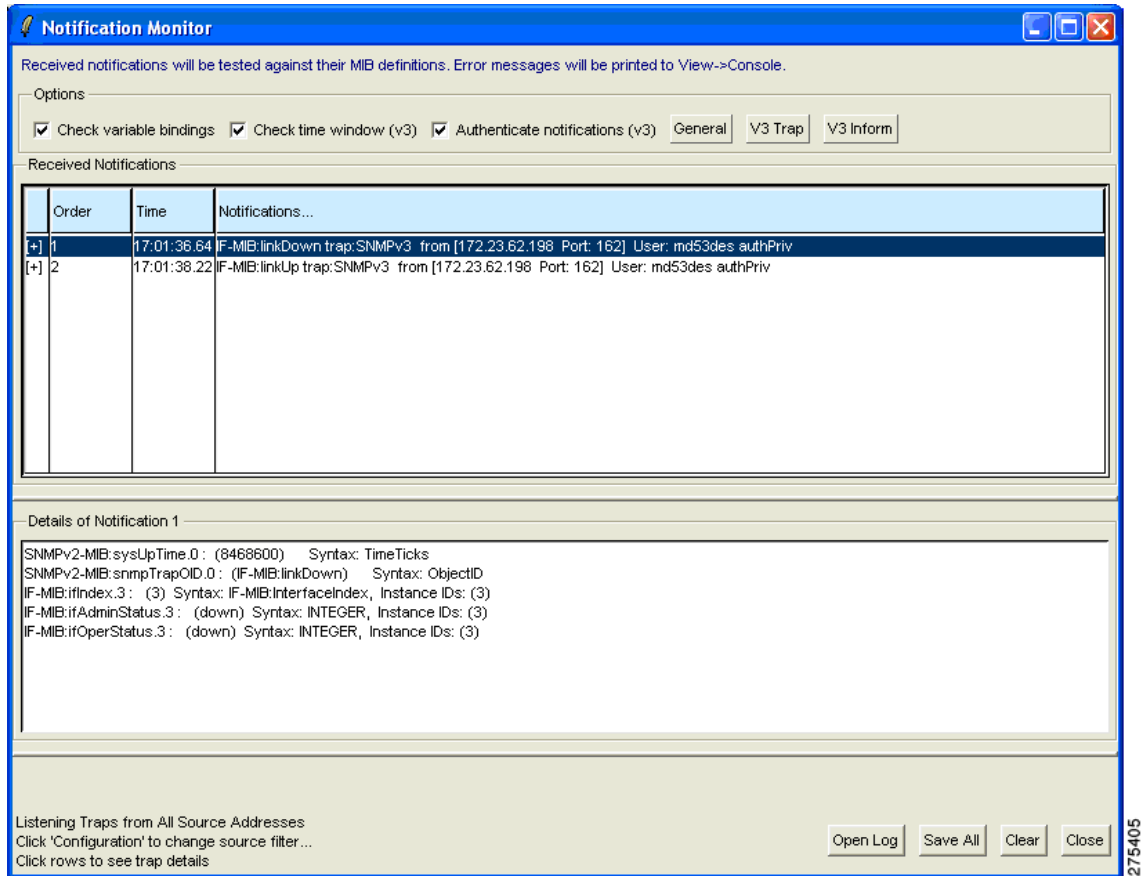
- ステップ 1 メインウィンドウで、[Notifications] > [Notifications Monitor] を選択します。
- ステップ 2 エージェント固有の情報を設定するため、[V3 Inform] をクリックします。

受信通知のダイアログボックス(図 2-13 を参照)に受信したトラップメッセージが表示され、その下部には通知の詳細が表示されます。



(注) SNMP バージョン 3 では、認証失敗トラップは送信されません。代わりに SNMP バージョン 3 エージェントからは PDU レポートが送信されます。

図 2-13 [Notification Monitor] ダイアログボックス



## パフォーマンスのテスト

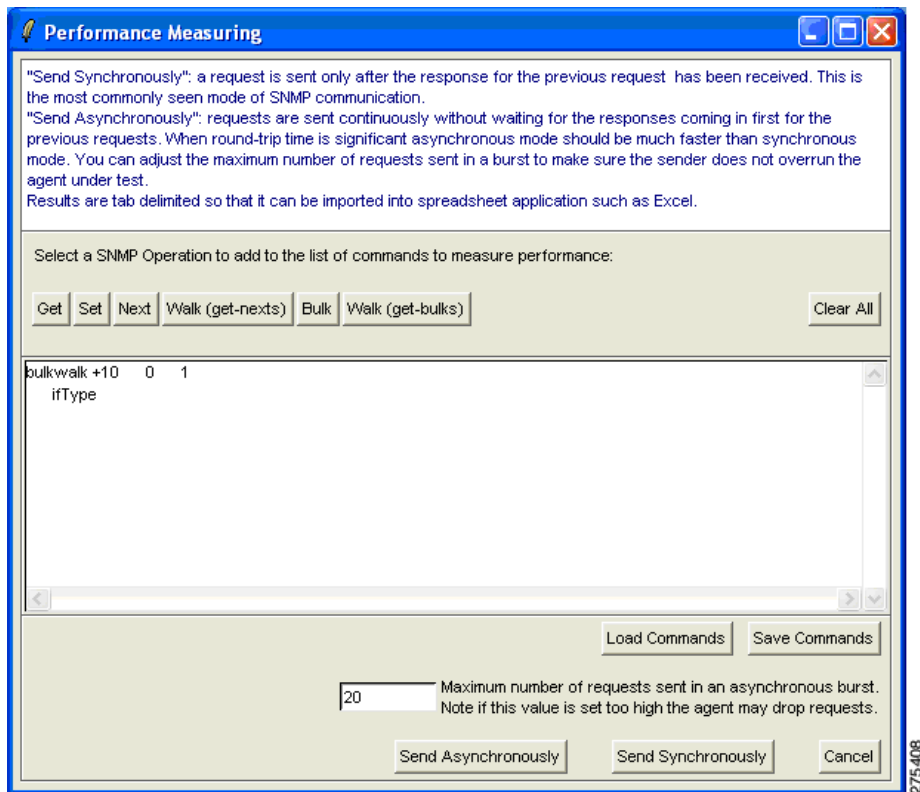
パフォーマンスをテストする手順は次のとおりです。

- ステップ 1 [Tools] > [Performance Monitoring Tool] を選択した後、実行する動作 ([Walk (get-bulks)] など) を選択し、オブジェクト名を入力します。さまざまなコマンドを繰り返し実行することができます。
- ステップ 2 [Send Synchronously] をクリックします。  
選択した SNMP の動作が開始されます。結果は別ウィンドウに表示されます。

次に示す例(図 2-14)では ifType が使用され、動作の繰り返し回数は 10 となっています。



図 2-14 [Performance Measuring] ダイアログボックス



## Ipswitch WhatsUp Gold

Ipswitch WhatsUp Gold は、ネットワーク探索、SNMP モニタリング、および SNMP ポーリングを行えるネットワーク管理ソフトウェアです。このソフトウェアの無償バージョンを次の URL からダウンロードできます。

<http://www.whatsupgold.com/products/download/>

この項では、次のトピックについて取り上げます。

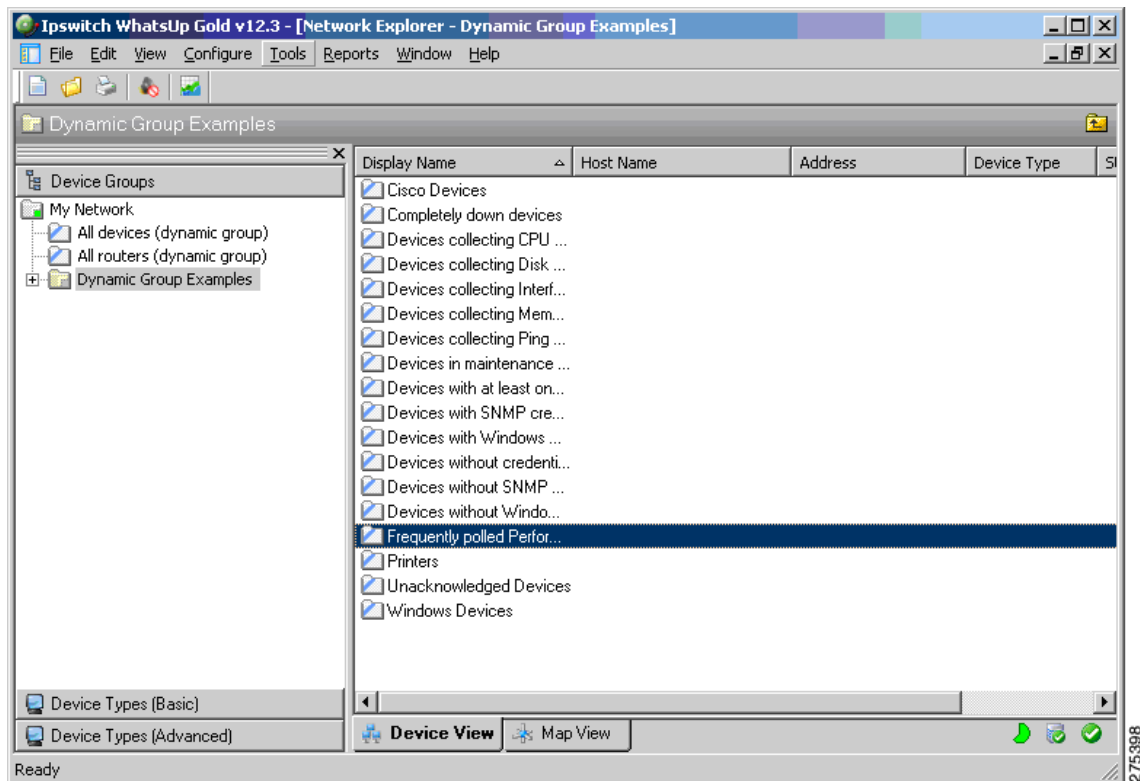
- [Ipswitch WhatsUp Gold の起動 \(2-18 ページ\)](#)
- [SNMP エージェントの新規追加 \(2-18 ページ\)](#)
- [SNMP バージョン 3 クレデンシャルの追加 \(2-19 ページ\)](#)
- [WhatsUp Gold Web インターフェイスの使用方法 \(2-22 ページ\)](#)
- [SNMP MIB または OID のウォーク \(2-23 ページ\)](#)
- [SNMP トラップの設定 \(2-27 ページ\)](#)

## Ipswitch WhatsUp Gold の起動

Ipswitch WhatsUp Gold アプリケーションを起動する場合は、[Start] > [Programs] > [Ipswitch WhatsUp Gold 12.3] > [WhatsUp Gold] を選択します。

ネットワーク エクスプローラのメイン ウィンドウが表示されます(図 2-15 を参照)。

図 2-15 ネットワーク エクスプローラのメイン ウィンドウ

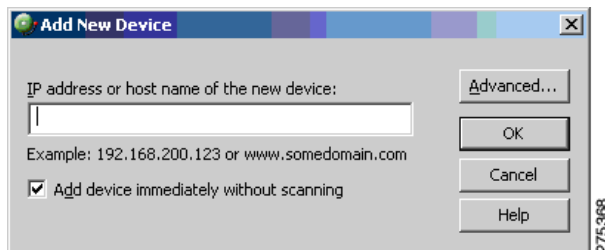


## SNMP エージェントの新規追加

SNMP エージェントを新たに追加する手順は次のとおりです。

- ステップ 1 [File] > [New] > [New Device] を選択します。  
[Add New Device] ダイアログボックスが表示されます(図 2-16 を参照)。

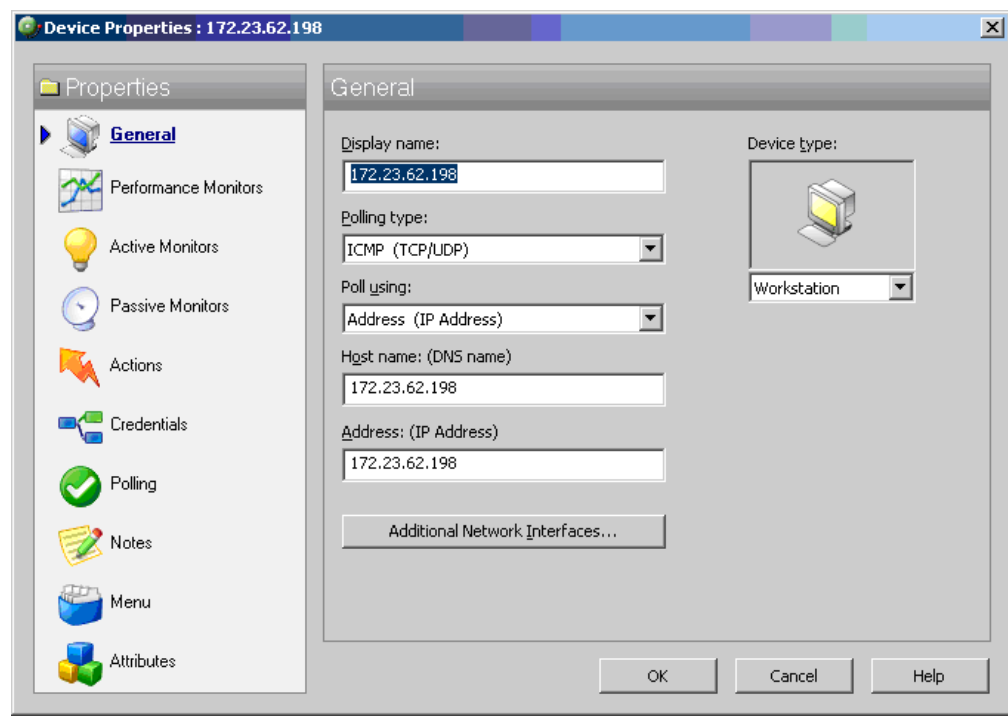
図 2-16 [Add New Device] ダイアログボックス



ステップ 2 IP アドレスまたはホスト名を入力します。

ステップ 3 デバイスが追加されたら、[General] ペイン(図 2-17 を参照)でデバイスのプロパティを入力します。

図 2-17 [Device Properties] ダイアログボックス

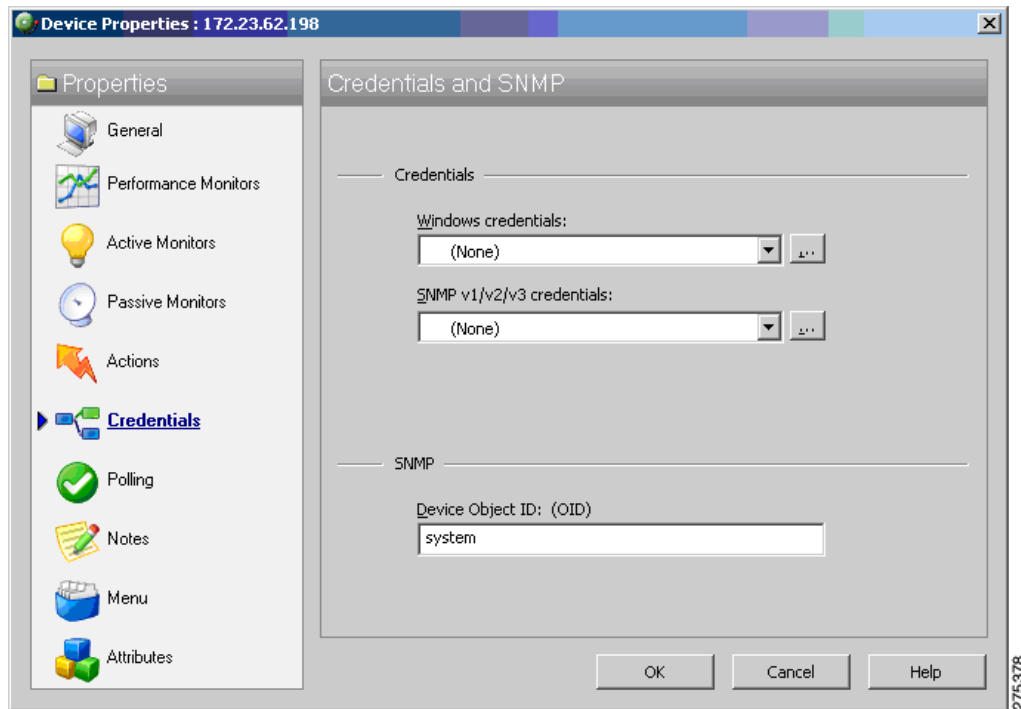


## SNMP バージョン 3 クレデンシヤルの追加

SNMP バージョン 3 クレデンシヤルを追加する手順は次のとおりです。

ステップ 1 [Credentials] リンク(図 2-18 を参照)をクリックし、SNMP デバイスのオブジェクト ID 情報を入力します。

図 2-18 SNMP クレデンシャルが表示された [Device Properties] ダイアログボックス



ステップ 2 [SNMP v1/v2/v3 credentials] ドロップダウンリストの横にあるボタンをクリックし、ユーザ名、認証アルゴリズム、暗号化アルゴリズム、および認証と暗号化のそれぞれに使用するパスワードを入力して、[OK] をクリックします(図 2-19 および図 2-20 を参照)。

図 2-19 [Edit SNMP v3 Credential Type] ダイアログボックス

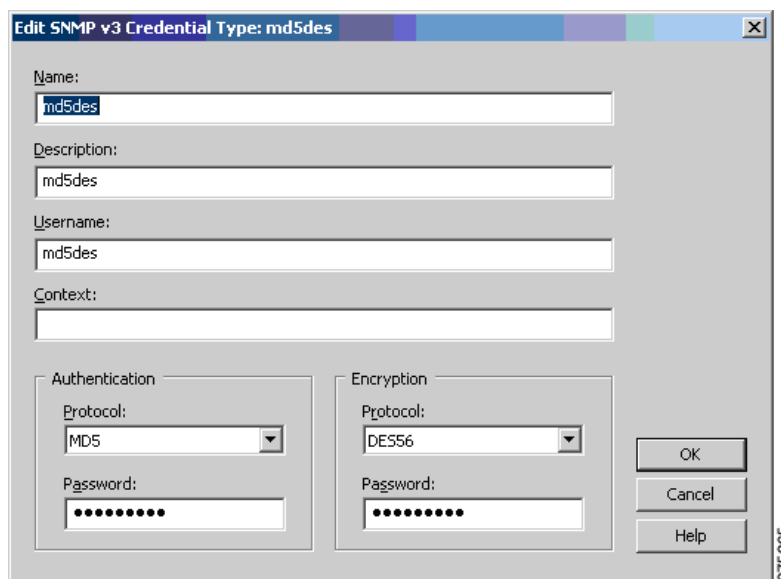


図 2-20 [Credentials Library] ダイアログボックス

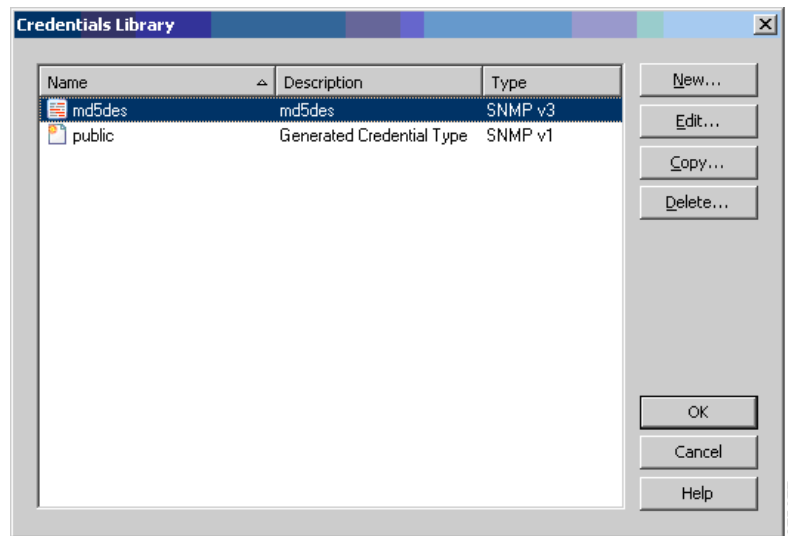
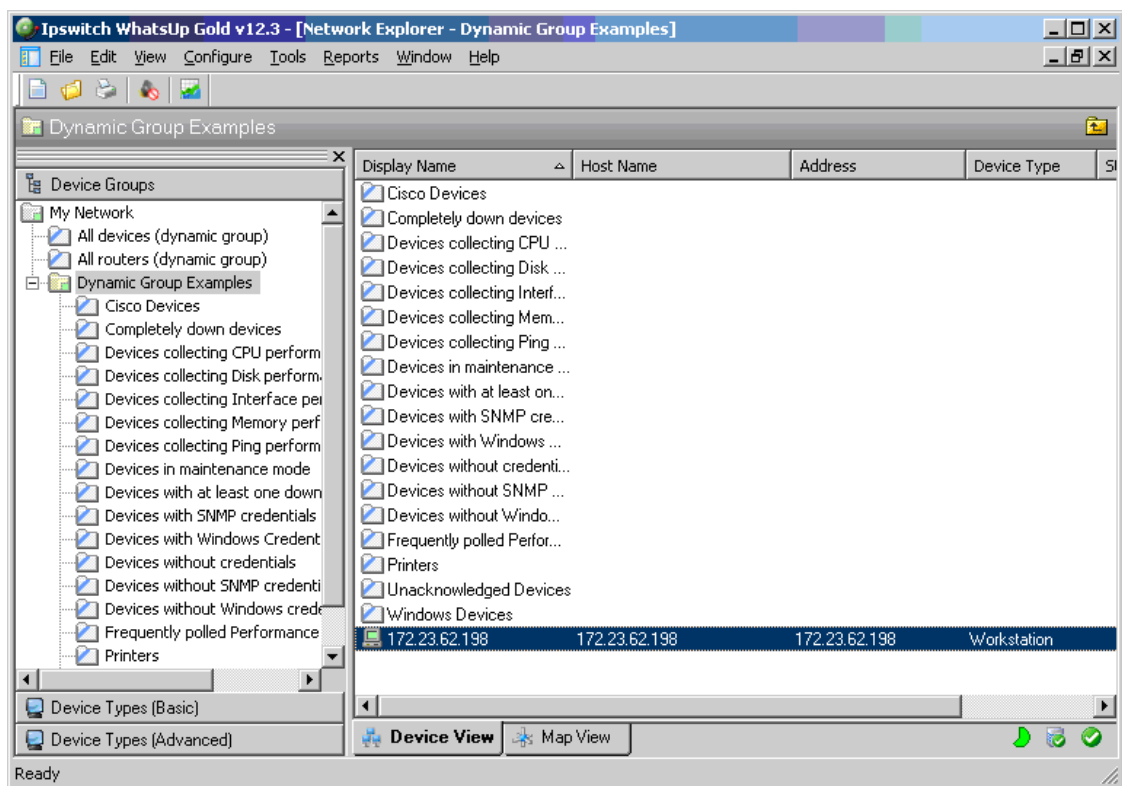



図 2-21 は、ネットワーク上に追加された SNMP バージョン 3 ノードが表示されている画面です。


図 2-21 追加された SNMP バージョン 3 ノードが表示されているネットワーク エクスプローラ ウィンドウ



## WhatsUp Gold Web インターフェイスの使用方法

WhatsUp Gold アプリケーションを起動する手順は次のとおりです。

- ステップ 1 [Start] > [Programs] > [IpSwitch WhatsUp Gold v12.3] > [WhatsUp Web Interface] を選択します。この場所から SNMP バージョン 3 のウォークおよびポーリングを実行できます。
- ステップ 2  2-22 は、初回ログイン時に表示されるウィンドウです。デフォルトのユーザ名およびパスワード(「admin」)を入力します。

 2-22 WhatsUp Gold Web インターフェイスのログインウィンドウ




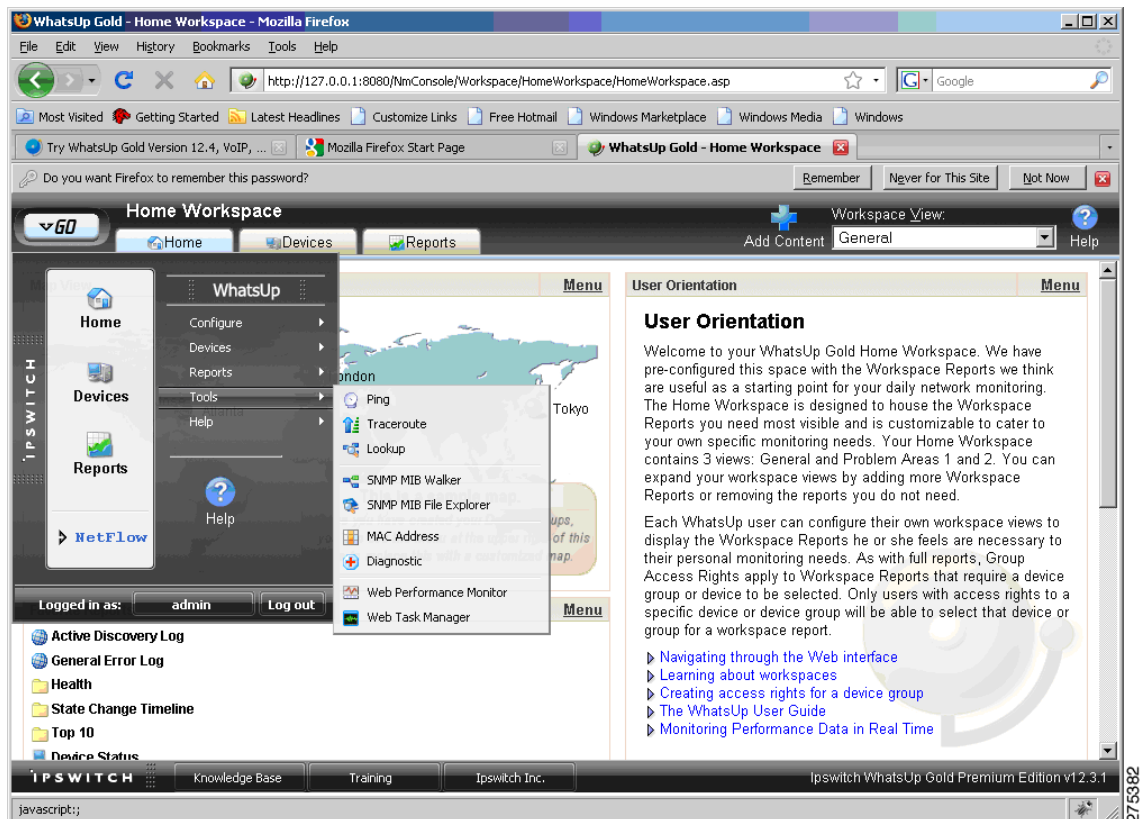
-  2-23 は、ユーザがログインした後に表示される [Home Workspace] ペインです。

図 2-23 WhatsUp Gold の [Home Workspace] ペイン

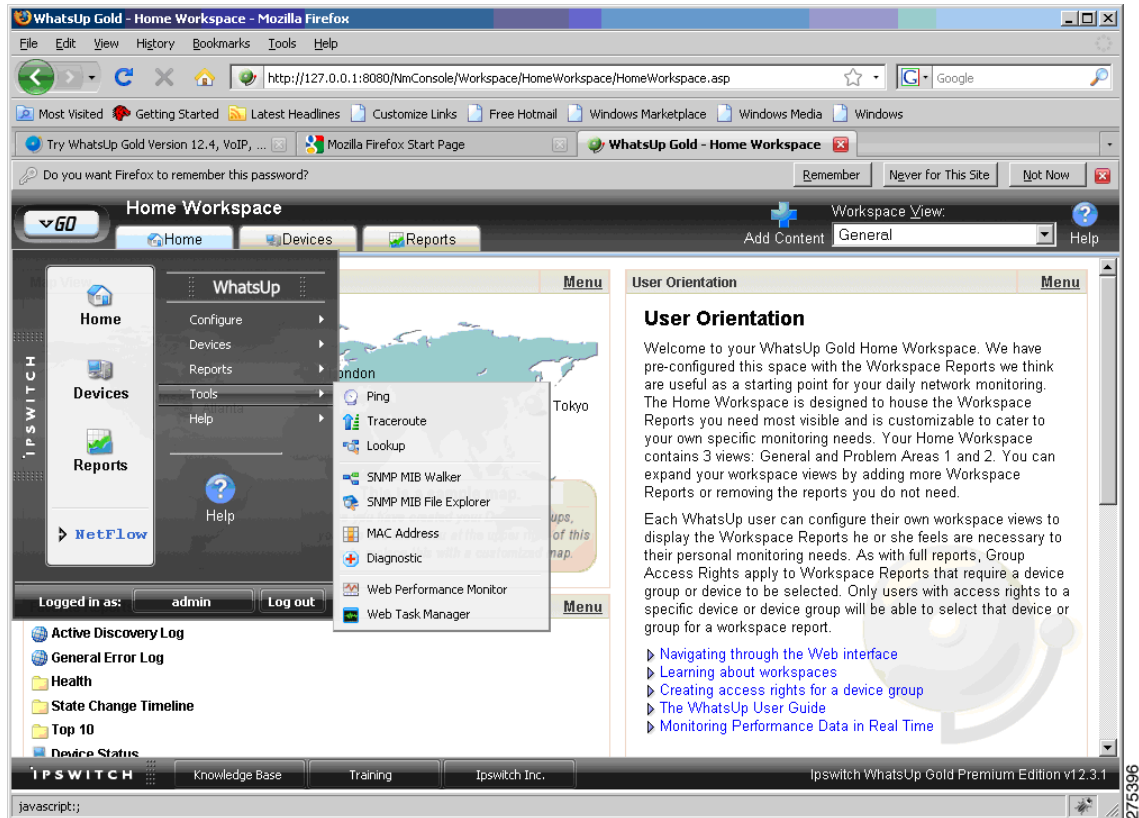


## SNMP MIB または OID のウォーク

MIB または OID をウォークする手順は次のとおりです。

ステップ 1 [GO] > [Tools] > [SNMP MIB Walker] を選択します(図 2-24 を参照)。

図 2-24 [SNMP MIB Walker] メニュー オプション

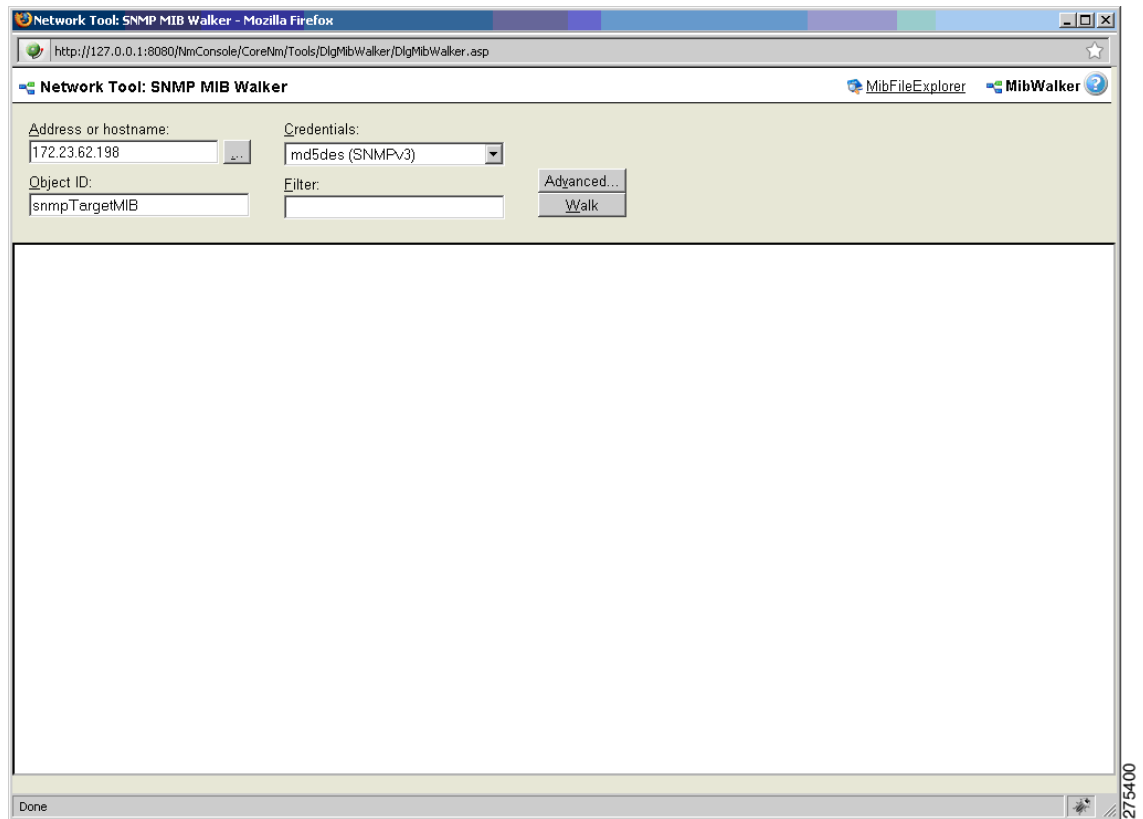


ステップ 2 [Network Tool: SNMP MIB Walker] ダイアログボックス(図 2-25 を参照)で、次の情報を入力します。

- エージェントの IP アドレスまたはホスト名
- ウォークの対象となる OID または MIB
- SNMP バージョン 3 クレデンシヤル



図 2-25 [Network Tool: SNMP MIB Walker] ダイアログボックス



ステップ 3 [Walk] をクリックします。

図 2-26 は、ツリー形式で表示されたウォークの結果を示したものです。

図 2-26 [Network Tool: SNMP MIB Walker] にツリー形式で表示されたウォークの結果

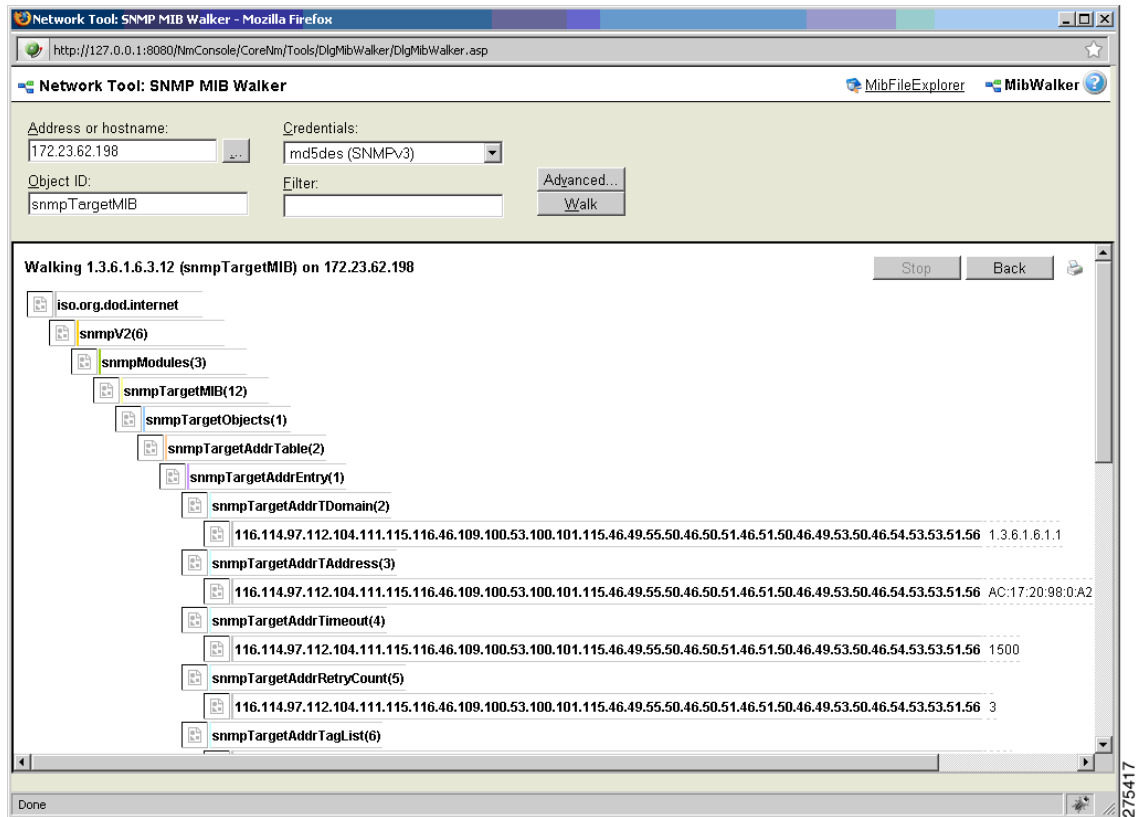
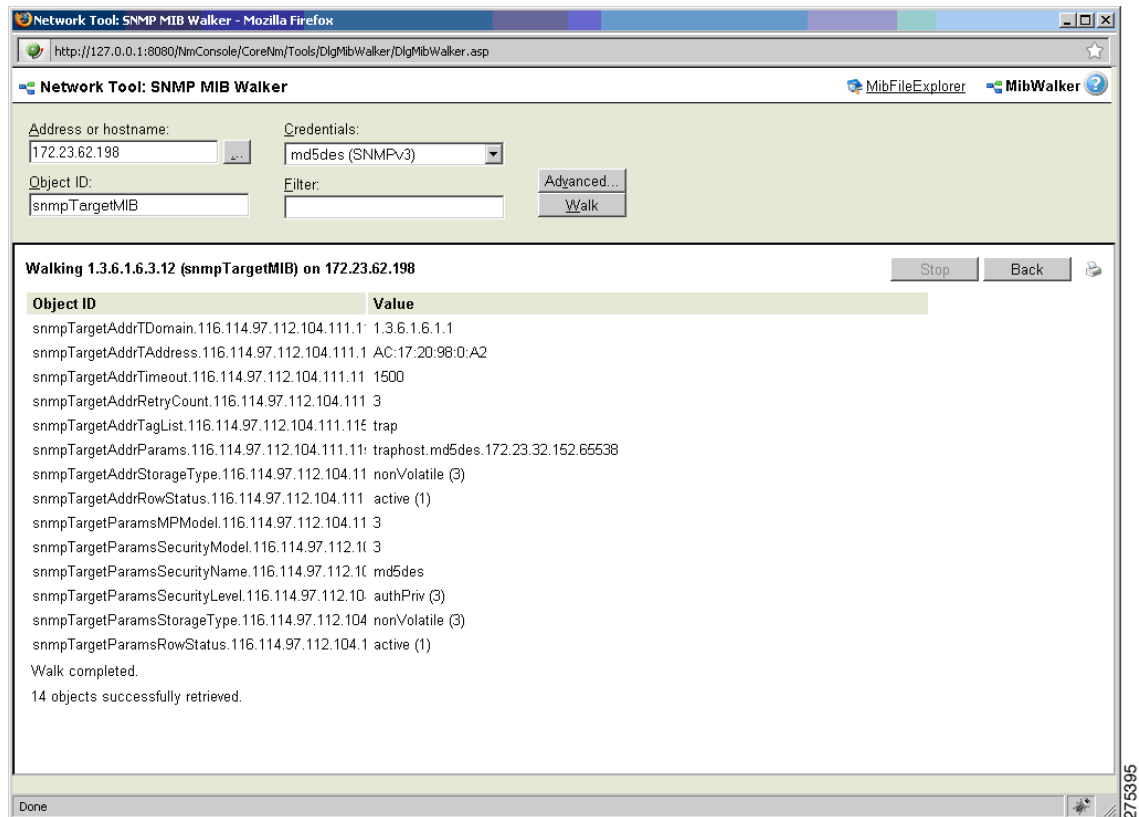


図 2-27 は、ウォーク順に表示された結果を示したものです。

図 2-27 [Network Tool: SNMP MIB Walker] の結果ウィンドウ

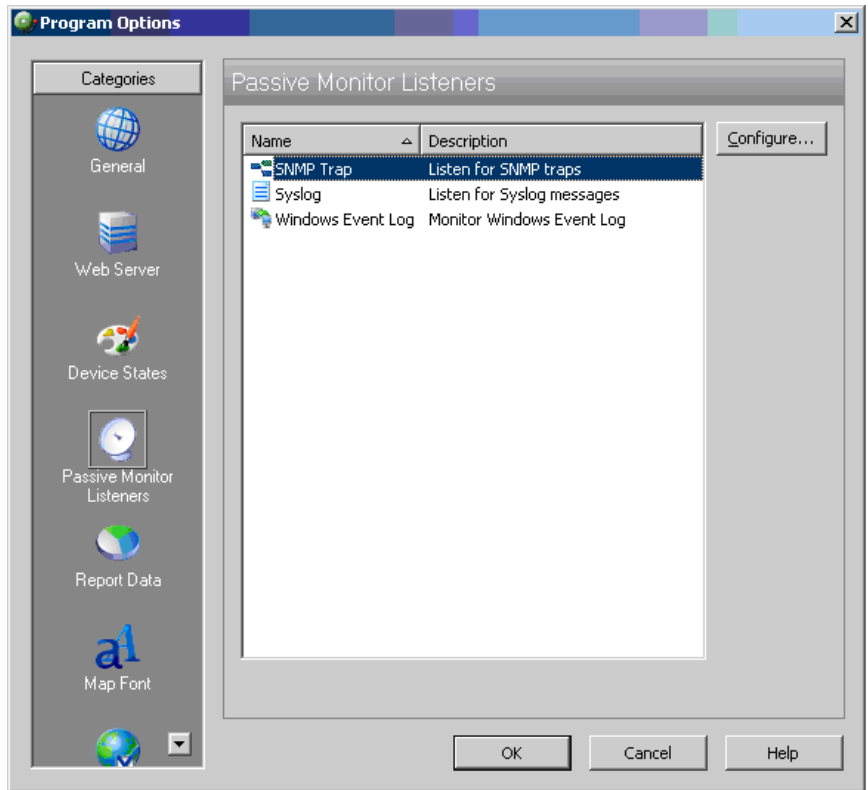


## SNMP トラップの設定

SNMP トラップを設定する手順は次のとおりです。

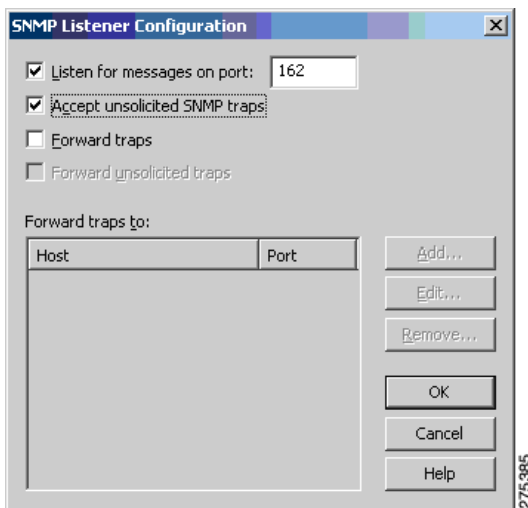
- ステップ 1 [Program Options] > [Passive Monitor Listeners] > [SNMP Trap] > [Configure] を選択します (図 2-28 を参照)。

図 2-28 [Program Options – Passive Monitor Listeners] ダイアログボックス



[SNMP Listener Configuration] ダイアログボックスが表示されます(図 2-29 を参照)。このダイアログボックスでは、リスナー ポートを設定できるだけでなく、トラップをホストへ転送することもできます。

図 2-29 [SNMP Listener Configuration] ダイアログボックス



ステップ 2 [Reports] タブをクリックし、[SNMP Trap Log] を選択します(図 2-30 を参照)。

図 2-30 SNMP レポートのペイン

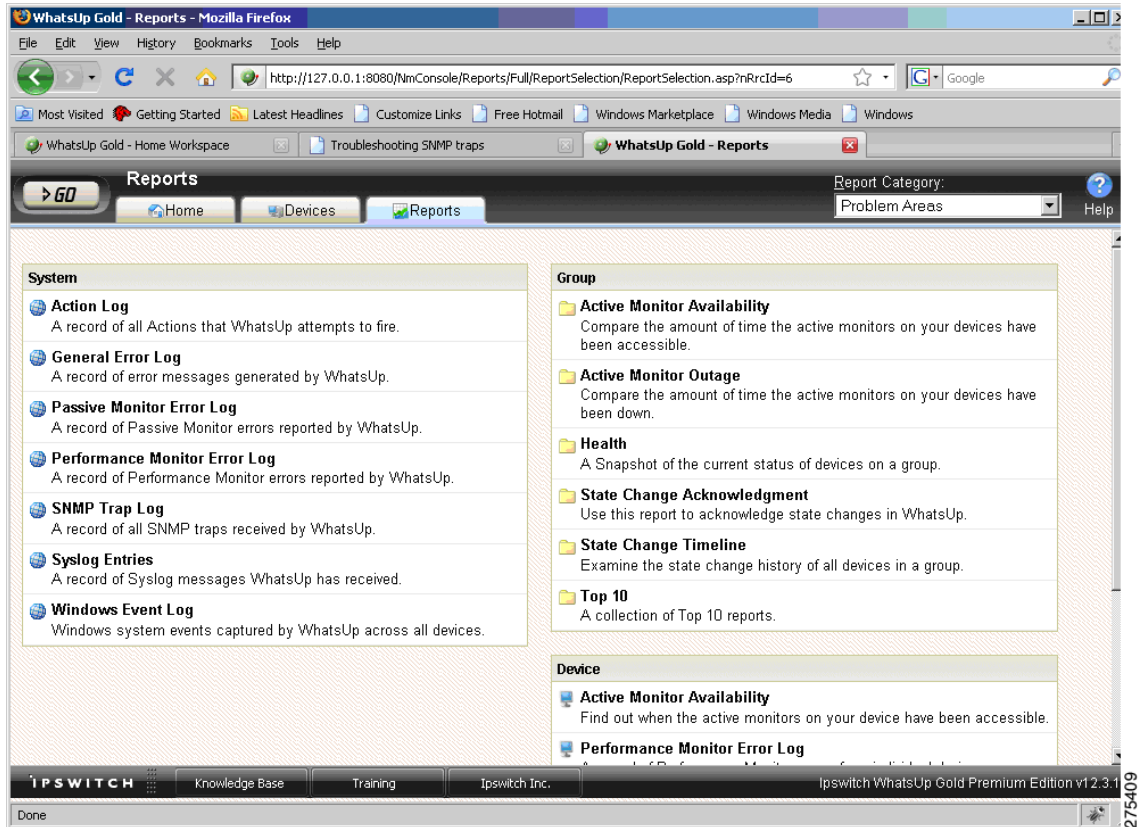
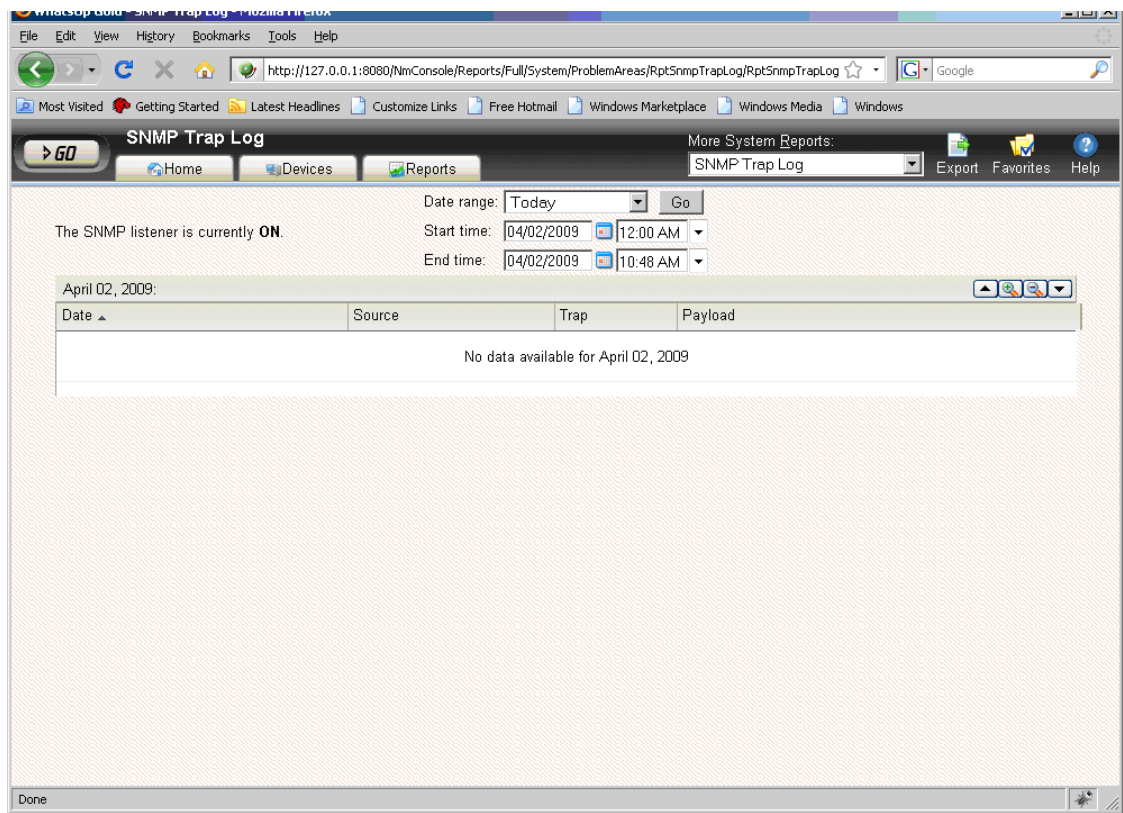


図 2-31 は SNMP トラップのログを示したものです。

図 2-31 SNMP トラップログのペイン



## HP OpenView Network Node Manager

HP OpenView Network Node Manager (NNM) 7.53 は、ネットワーク トポロジの作成、デバイスの管理、およびデバイス ヘルスのモニタリングを自動的に行うための管理ツールです。ASA は、この HP NNM のデバイス トポロジに組み込まれ、SNMP バージョン 3 に基づいてデバイスの統計情報や SNMP トラップをやり取りします。



(注) NNM 8.x に関する未解決の警告の一覧については、Cisco ASA 5500 シリーズのリリースノートを参照してください。

この項では、次のトピックについて取り上げます。

- [NNM のインストール\(2-31 ページ\)](#)
- [NNM の起動\(2-31 ページ\)](#)
- [MIB のロード\(2-32 ページ\)](#)
- [現在のマップへのネットワークの追加\(2-33 ページ\)](#)
- [特定の SNMP バージョン 3 パラメータの設定\(2-36 ページ\)](#)
- [グローバルな SNMP バージョン 3 クレデンシャルの設定\(2-37 ページ\)](#)

- ノード情報の表示(2-38 ページ)
- NNM MIB ブラウザの設定(2-39 ページ)
- HP OpenView NNM Web アプリケーションの使用方法(2-44 ページ)

## NNM のインストール

NNM 7.53 は Windows 2003 Server プラットフォーム上でテスト済みです。トライアルバージョン、およびインストールに必要な手順は、次の URL から入手できます。

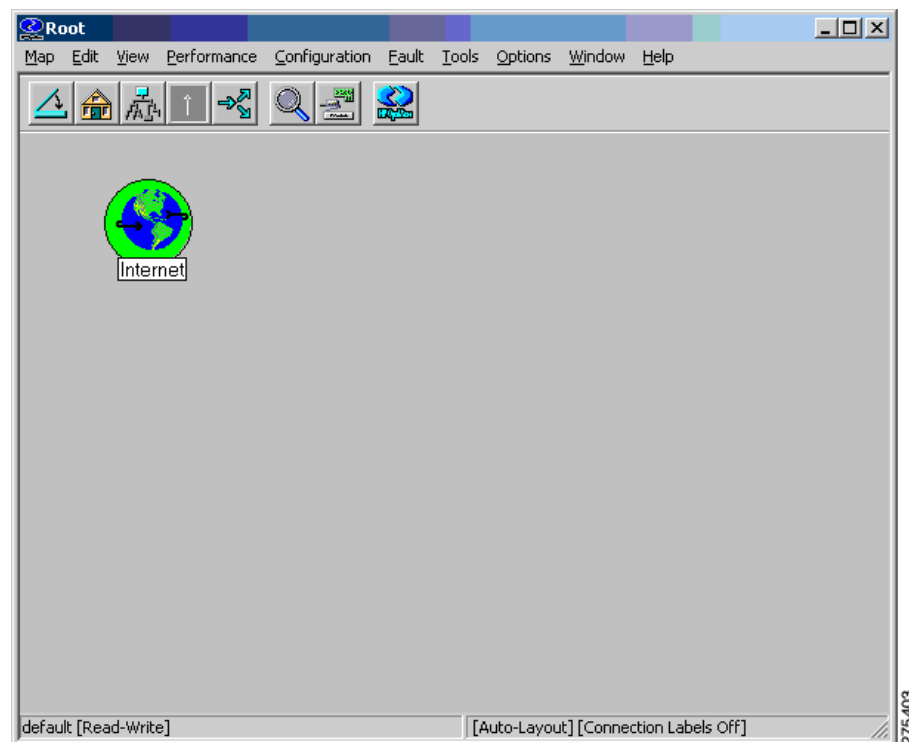
[https://h10078.www1.hp.com/cda/hpms/display/main/hpms\\_content.jsp?zn=bto&cp=1-11-15-119^1155\\_4000\\_100\\_\\_](https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119^1155_4000_100__)

## NNM の起動

NNM を起動する手順は次のとおりです。

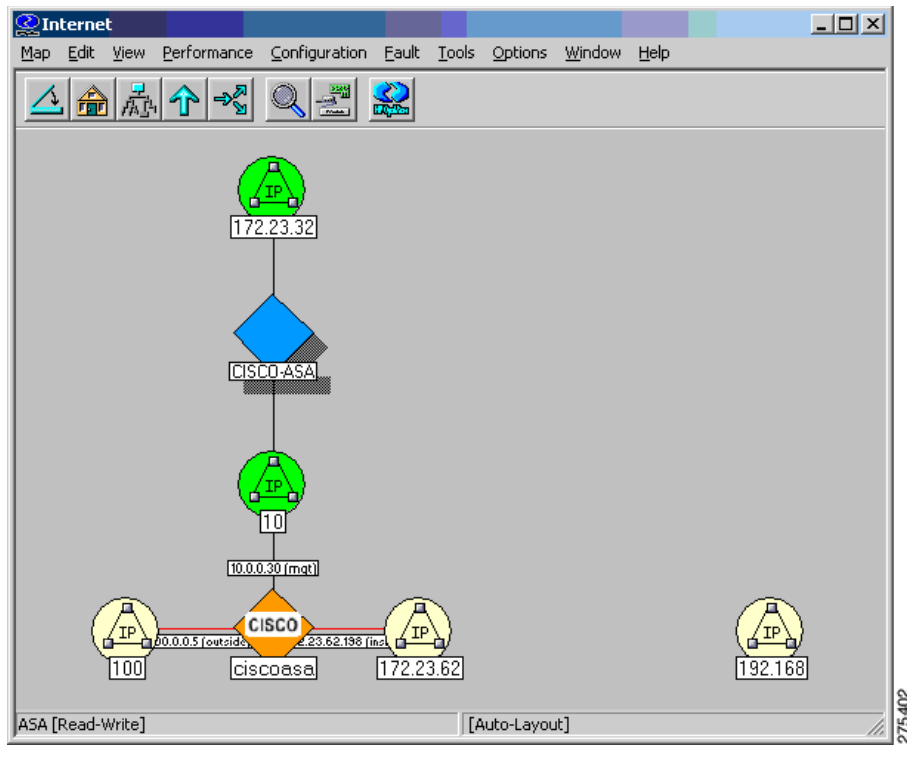
- ステップ 1 NNM サーバのコマンドプロンプトから、次のいずれかを実行します。
- [Start] > [Programs] > [HP OpenView] > [Network Node Manager Admin] > [Network Node Manager] を選択します。
  - C:\Program Files\HP OpenView\bin にある **ovw.exe** ファイルをダブルクリックします。
- [Root] ウィンドウが開き、[Internet map] アイコンが表示されます(図 2-32 を参照)。

図 2-32 NNM コンソールの [Root] ウィンドウ



- ステップ 2 [Internet map] アイコンをダブルクリックします。  
 [Internet] ウィンドウが開き、ネットワーク ノードが表示されます(図 2-33 を参照)。

図 2-33 ネットワーク ノードが表示された NNM コンソールの [Internet] ウィンドウ



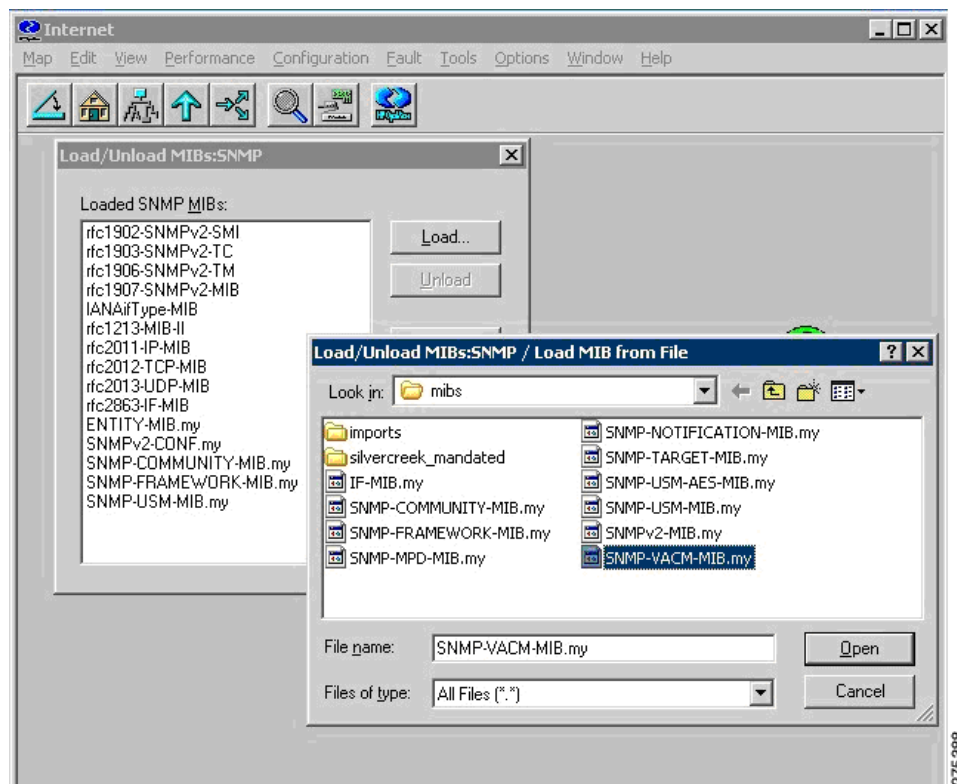
## MIB のロード

MIB をロードする手順は次のとおりです。

- ステップ 1 NNM のメインウィンドウで、[Options] > [Load/Unload MIBs: SNMP] を選択します。  
 現在ロードされている MIB がリスト表示されます。
- ステップ 2 [Load] をクリックし、さらにロードする MIB をサーバファイルシステムから選択します  
 (図 2-34 を参照)。



図 2-34 [Load/Unload MIBs: SNMP] ダイアログボックス

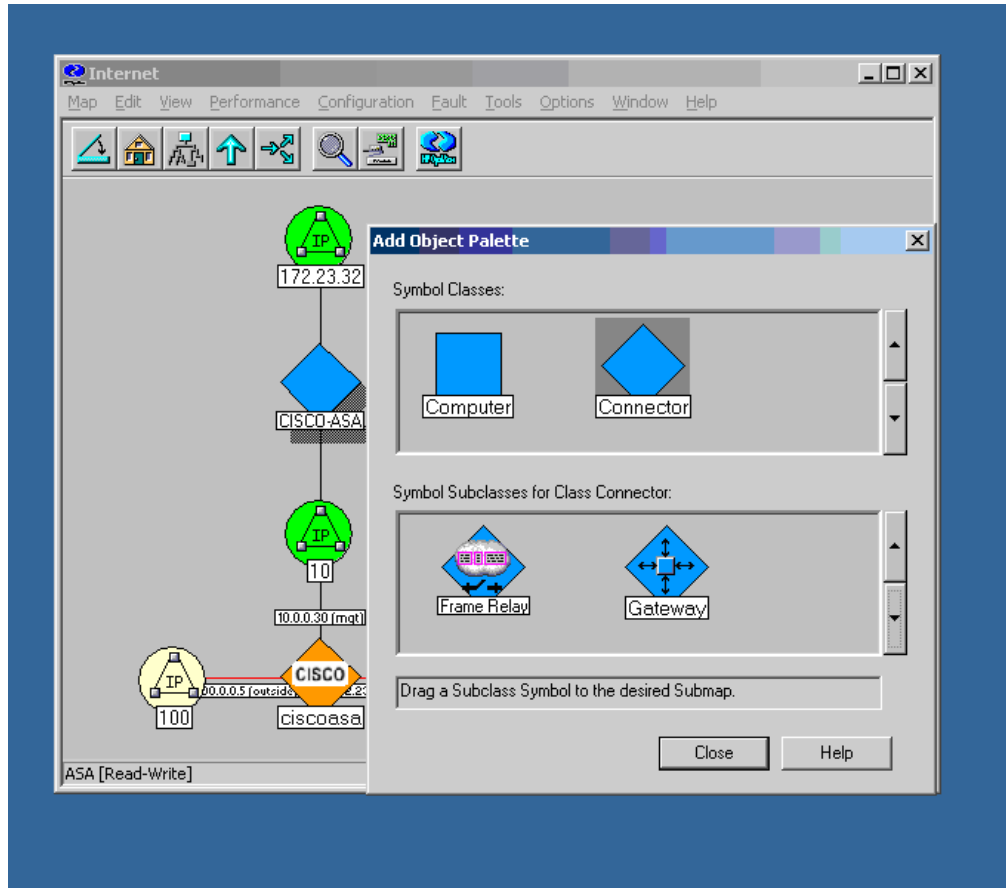


## 現在のマップへのネットワークの追加

現在のマップにネットワークを追加する手順は次のとおりです。

- ステップ 1 追加するネットワークの中からトラフィック量の多いデバイスを少なくとも 1 つ選び、その IP アドレスおよびホスト名を特定します。
- ステップ 2 インターネットレベル サブマップ内で、[Edit] > [Add Objects] を選択します。  
[Add Object Palette] ダイアログボックスが表示されます(図 2-35 を参照)。

図 2-35 [Add Object Palette] ダイアログボックス

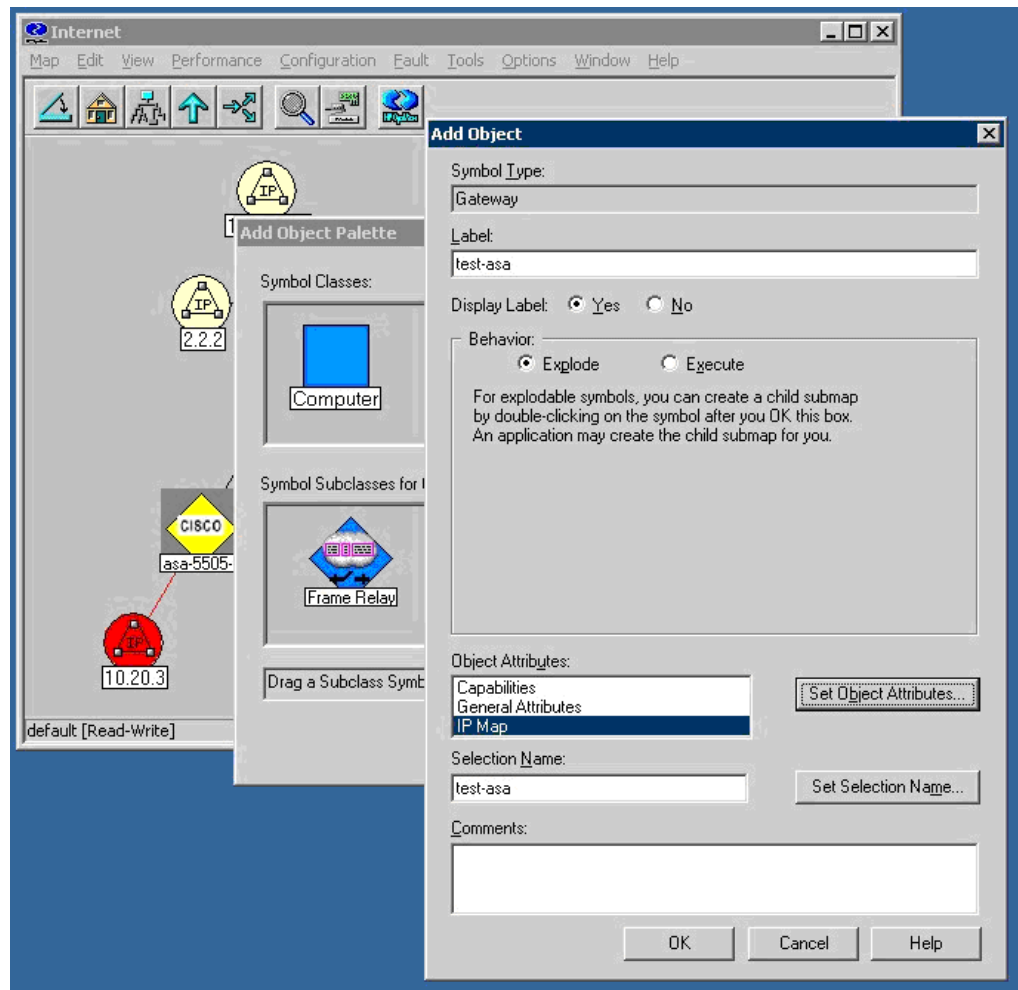


275-406

ステップ 3 [Connector] シンボル クラス アイコンをクリックし、[Gateway] シンボル サブクラス アイコンをインターネットレベルサブマップ上にドラッグします。探索を開始する際に使用しているデバイスのタイプにかかわらず、このゲートウェイ コネクタを選択してください。

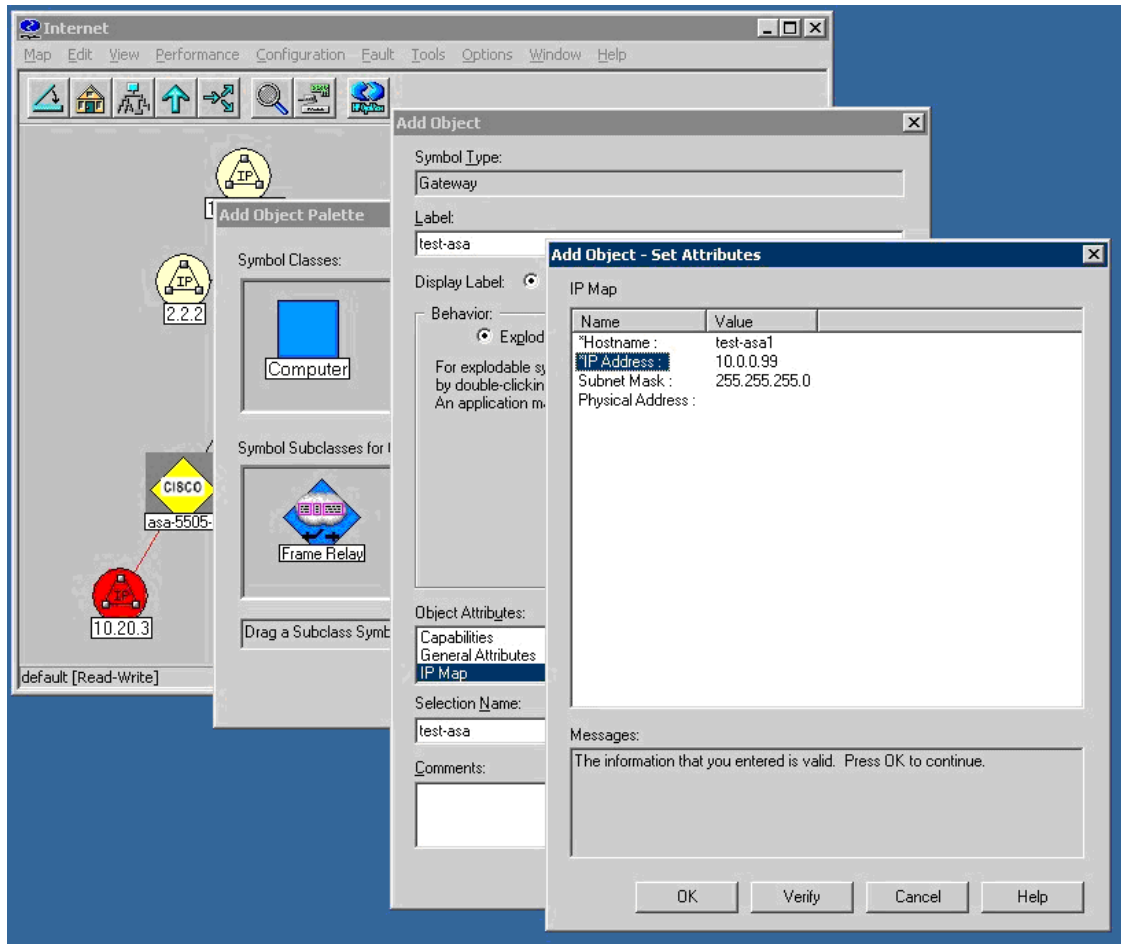
[Add Object] ダイアログボックスが表示されます(図 2-36 を参照)。

図 2-36 [Add Object] ダイアログボックス



- ステップ 4 [IP Map] をダブルクリックします。  
[Add Object – Set Attributes] ダイアログボックスが表示されます(図 2-37 を参照)。

図 2-37 [Add Object - Set Attributes] ダイアログボックス



- ステップ 5** 管理ドメインに追加するネットワーク内の SNMP 対応デバイスの IP アドレスおよびホスト名を入力し、[Verify] をクリックします。
- ステップ 6** NNM により、設定内容がチェックされた後で、記号の選択内容が変更されます。必要であればその位置も修正されます。この時点で、そのデバイスは NNM によって管理されるよう設定され、インターネット マップ上に表示されます。

## 特定の SNMP バージョン 3 パラメータの設定

特定の SNMP ノードに対してクレデンシャルを設定する手順は次のとおりです。

- ステップ 1** C:\Program Files\HP Open View\bin にある **xnmsnmpconf.exe** ファイルをダブルクリックします。
- ステップ 2** NNM のメインウィンドウで、[Options] > [SNMP Configuration] を選択します。  
設定ペインが表示されます。

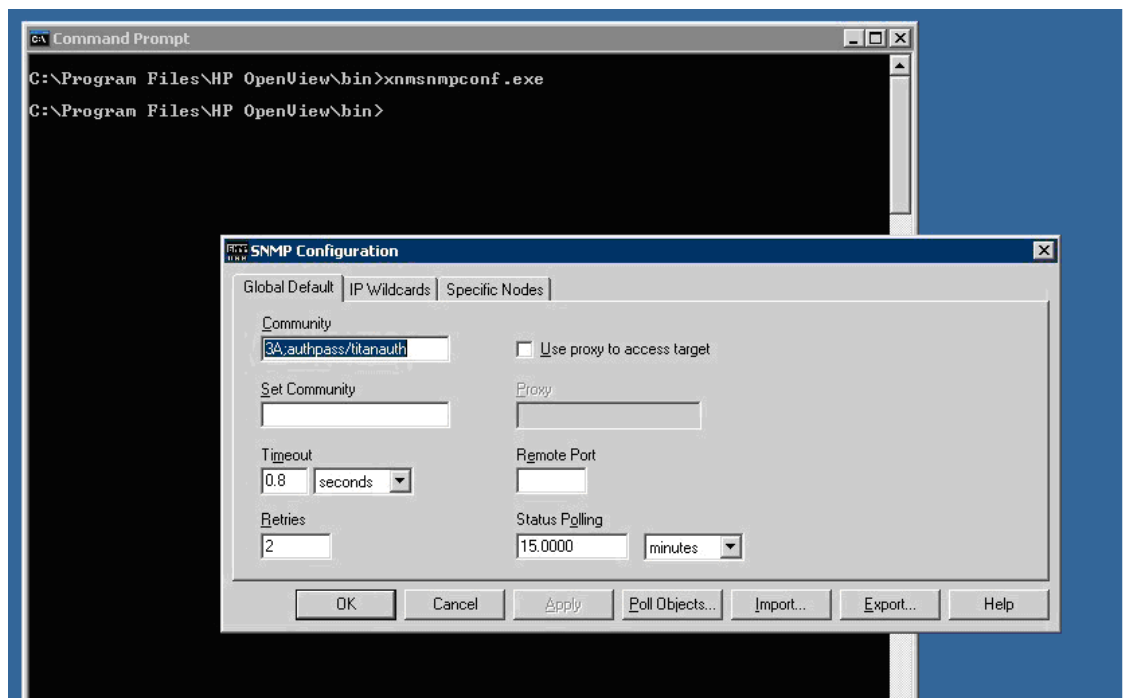


(注) SNMP バージョン 3 クレデンシャルを設定する場合は、オーバーロードされた SNMP ストリングを使用する必要があります。詳細については、「[NNM MIB ブラウザの設定](#)」セクション(2-39 ページ)のステップ 2 を参照してください。

## グローバルな SNMP バージョン 3 クレデンシャルの設定

グローバルな SNMP バージョン 3 クレデンシャルを設定する場合は、[グローバル設定] セクションで、デフォルトの通信に使用する SNMPv3 ユーザおよびパスワードを入力します(図 2-38 を参照)。コミュニティストリングの形式については、「[NNM MIB ブラウザの設定](#)」セクション(2-39 ページ)のステップ 2 を参照してください。

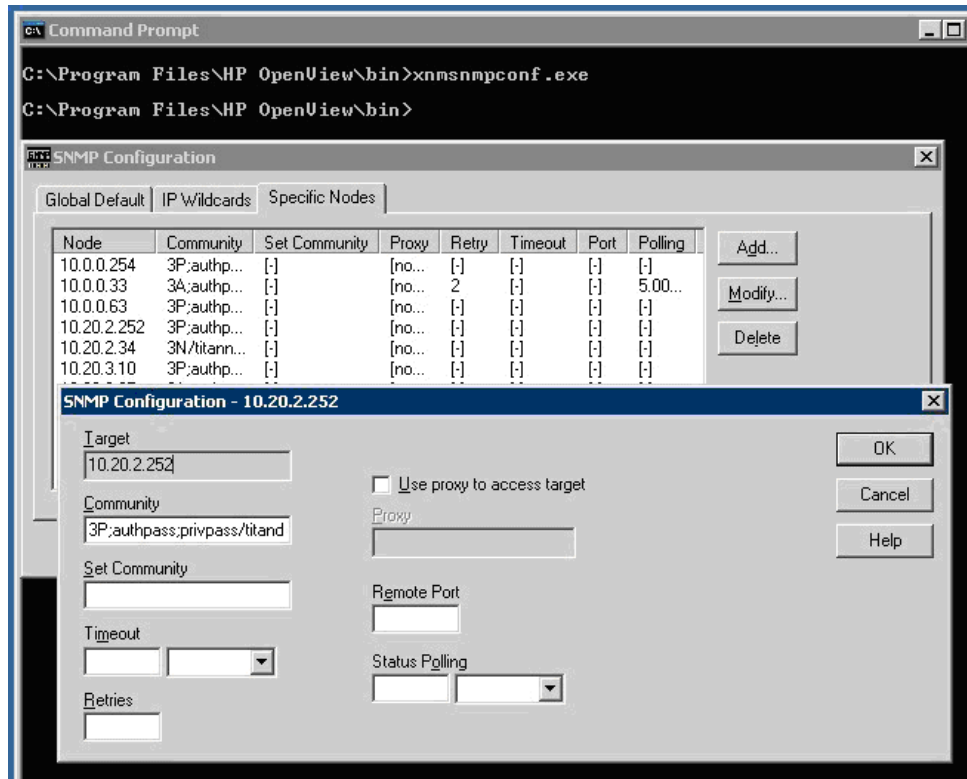
図 2-38 SNMP の設定



## 特定の SNMP バージョン 3 クレデンシャルの設定

特定の SNMP バージョン 3 クレデンシャルを設定する場合は、[Specific Nodes] タブ (図 2-39 を参照) をクリックして、個々の SNMP ノードに対する SNMP バージョン 3 ユーザおよびパスワードを入力します。

図 2-39 [SNMP Configuration] ダイアログボックス

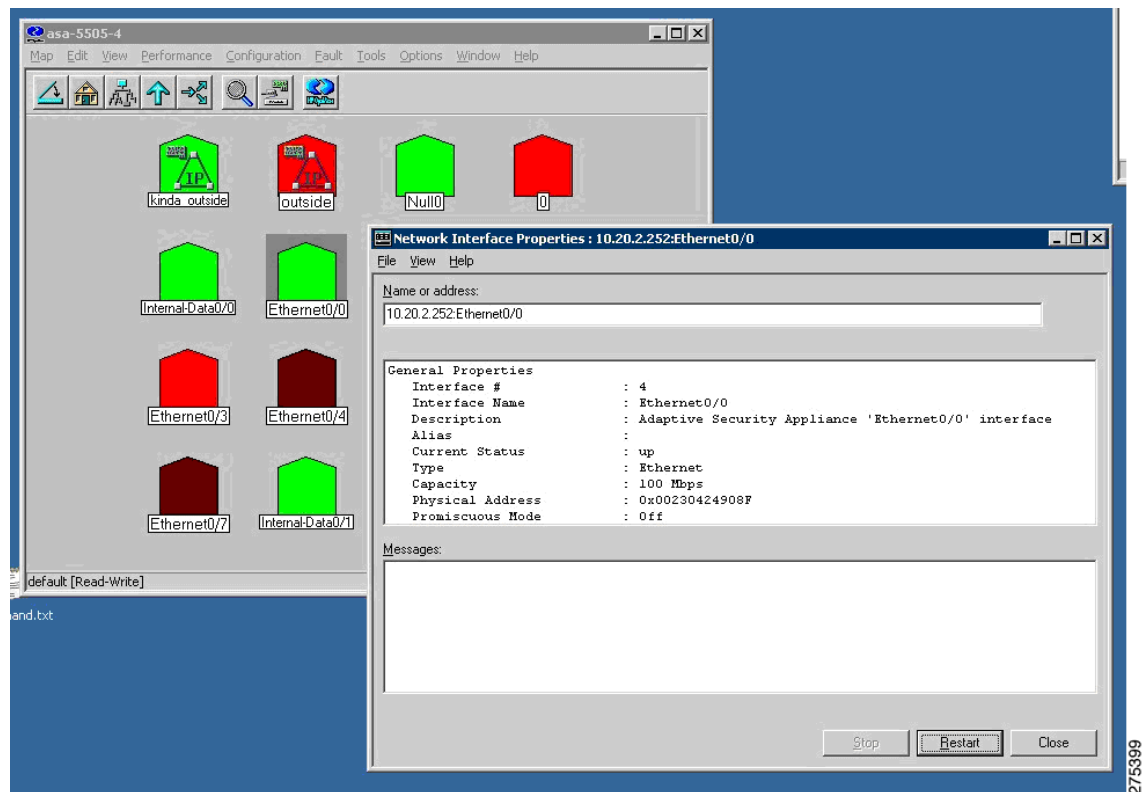


## ノード情報の表示

ノード情報を表示する手順は次のとおりです。

- ステップ 1 インターネット マップから特定のノードへドリルダウンし、使用可能なインターフェイスをすべて表示します。
- ステップ 2 さらにインターフェイス情報を表示する場合は、いずれかのインターフェイスを右クリックし、[Interface Properties] または [Interface Status] を選択します。  
[Network Interface Properties] ダイアログボックスが表示されます (図 2-40 を参照)。

図 2-40 [Network Interface Properties] ダイアログボックス



## NNM MIB ブラウザの設定

NNM MIB ブラウザを設定する手順は次のとおりです。

- ステップ 1 NNM サーバのコマンドプロンプトから、C:\Program Files\HP OpenView\bin にある xnmbrowser.exe を実行して MIB ブラウザを起動します。
- ステップ 2 SNMP ホストの IP アドレスおよびコミュニティ スtring を入力します。SNMP バージョン 3 接続の場合、コミュニティ スtring には、オーバーロードされたコミュニティ スtring の構文が使用されます。

次に示すのは、オーバーロードされたコミュニティ スtring に使用される構文の例です。

```
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
```



(注) デフォルトの認証方式は MD5、デフォルトの暗号化方式は DES です。

この項では、次のトピックについて取り上げます。

- [SNMP バージョン 3 の No-auth/No-priv 接続の設定 \(2-40 ページ\)](#)
- [SNMP バージョン 3 の MD5 Auth/No-priv 接続の設定 \(2-40 ページ\)](#)
- [SNMP バージョン 3 の SHA Auth/No-priv 接続の設定 \(2-40 ページ\)](#)
- [SNMP バージョン 3 の MD5 Auth/Priv 接続の設定 \(2-41 ページ\)](#)
- [SNMP バージョン 3 の SHA Auth/Priv 接続の設定 \(2-41 ページ\)](#)
- [MIB の参照 \(2-41 ページ\)](#)
- [MIB ブラウザのパケット トレースの実行 \(2-42 ページ\)](#)
- [NNM SNMP バージョン 3 トラップ ビューアの使用法 \(2-43 ページ\)](#)

## SNMP バージョン 3 の No-auth/No-priv 接続の設定

SNMP バージョン 3 の No-auth/No-priv 接続を設定する手順は次のとおりです。

- ステップ 1 UUT グループを設定するため、`snmp-server group asanoauth v3 noauth` コマンドを入力します。
- ステップ 2 UUT ユーザを設定するため、`snmp-server user titannoauth asanoauth v3` コマンドを入力します。
- ステップ 3 コミュニティ名として、`3N/titannoauth` と入力します。

## SNMP バージョン 3 の MD5 Auth/No-priv 接続の設定

SNMP バージョン 3 の MD5 Auth/No-priv 接続を設定する手順は次のとおりです。

- ステップ 1 UUT グループを設定するため、`snmp-server group asaauth v3 auth` コマンドを入力します。
- ステップ 2 UUT ユーザを設定するため、`snmp-server user titanauth asaauth v3 auth md5 authpass` コマンドを入力します。
- ステップ 3 コミュニティ名として、`3A:authpass/titanauth` と入力します。

## SNMP バージョン 3 の SHA Auth/No-priv 接続の設定

SNMP バージョン 3 の SHA Auth/No-priv 接続を設定する手順は次のとおりです。

- ステップ 1 UUT グループを設定するため、`snmp-server group asaauth v3 auth` コマンドを入力します。
- ステップ 2 UUT ユーザを設定するため、`snmp-server user titanshaauth asaauth v3 auth sha authpass` コマンドを入力します。
- ステップ 3 コミュニティ名として、`3A:SHA^authpass/titanshaauth` と入力します。



## SNMPバージョン3のMD5 Auth/Priv 接続の設定

SNMPバージョン3のMD5 Auth/Priv 接続を設定する手順は次のとおりです。

- 
- ステップ 1 UUT グループを設定するため、**snmp-server group asapriv v3 priv** コマンドを入力します。
  - ステップ 2 UUT ユーザを設定するため、**snmp-server user titandes asapriv v3 auth md5 authpass priv des privpass** コマンドを入力します。
  - ステップ 3 コミュニティ名として、次のいずれかを入力します。
    - **3P:authpass:privpass/titandes**
    - **3P:MD5^authpass:DES^privpass/titandes**
- 

## SNMPバージョン3のSHA Auth/Priv 接続の設定

SNMPバージョン3のSHA Auth/Priv 接続を設定する手順は次のとおりです。

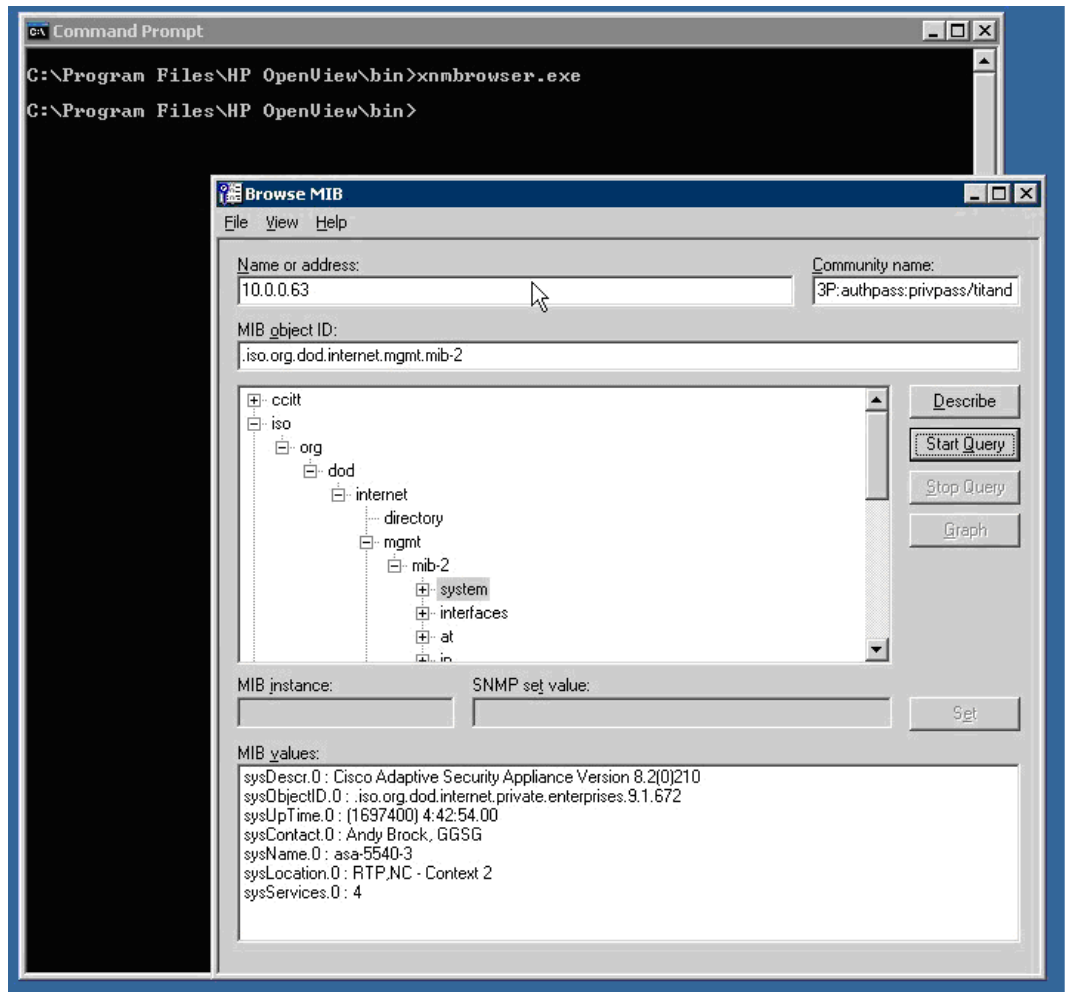
- 
- ステップ 1 UUT グループを設定するため、**snmp-server group asapriv v3 priv** コマンドを入力します。
  - ステップ 2 UUT ユーザを設定するため、**snmp-server user titanshades asapriv v3 auth sha authpass priv des privpass** コマンドを入力します。
  - ステップ 3 コミュニティ名として、**3P:SHA^authpass:DES^privpass/titanshades** と入力します。
- 

## MIB の参照

MIB を参照する手順は次のとおりです。

- 
- ステップ 1 目的の OID (.iso.org.dod.internet.mgmt.mib-2.system) までドリルダウンし、**system** オブジェクトを選択します。
  - ステップ 2 [Start Query] をクリックして、[MIB Values] フィールドに DUT の説明を入力します(図 2-41 を参照)。
-

図 2-41 [Browse MIB] ダイアログボックス

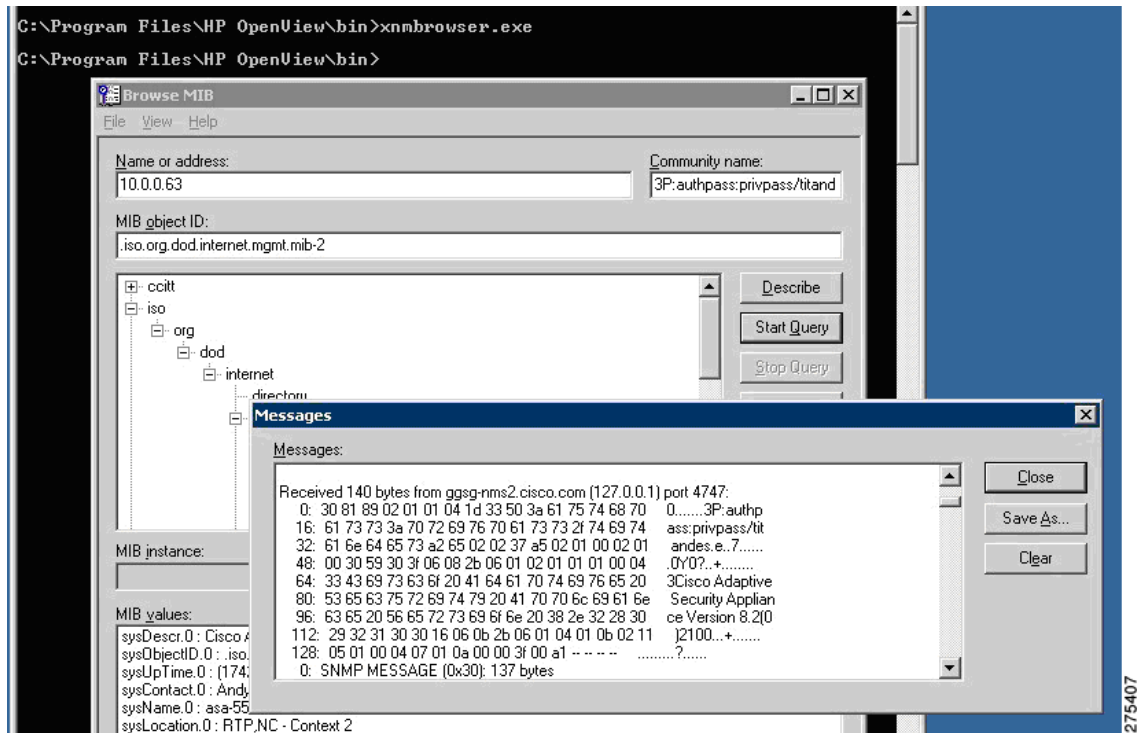


## MIB ブラウザの packets トレースの実行

MIB ブラウザの packets トレースを実行する場合は、[MIB Browser] ダイアログボックスで、[View] > [SNMP Packet Trace] を選択します。

[Messages] ダイアログボックス (図 2-42 を参照) が開き、MIB ブラウザと SNMP エージェントとの間で行われる SNMP 通信の packets の内容が表示されます。この情報は、デバッグを実行する際に有用です。

図 2-42 [Messages] ダイアログボックスでのパケット トレース



## NNM SNMP バージョン 3 トラップ ビューアの使用方法

NNM SNMP バージョン 3 トラップ ビューアを使用する場合の操作手順は次のとおりです。

- ステップ 1 SNMP エージェント上のユーザの SNMP バージョン 3 クレデンシャルが、NNM にキャッシュされていることを確認します。
- ステップ 2 MIB ブラウザを使用して SNMP エージェントに照会する場合は、次のようなコミュニティストリングを入力します。

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



(注) オーバーロードされたコミュニティストリングの中で **KEEP** パラメータを使用することにより、ユーザの資格情報を NNM コンフィギュレーション ファイル内に保存することができます。SNMP エージェントから NNM へセキュアな SNMP バージョン 3 トラップおよび inform 要求を送信し、かつ認証を必ず実行するためには、この操作は必須です。このコンフィギュレーション ファイルにはユーザ情報が保持されています。ファイルの保存場所は C:\etc\sconflmgr\mgr.cnf です。このファイルの内容は直接修正できます。手順については、NNM SPI SNMP Version 7.53 のマニュアルを参照してください。

また、次の例のように、**snmpget** コマンドを使用することもできます。

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

ステップ 3 SNMP エージェントを使用してトラップを送信する場合は、ASA で次のコマンドを入力します。

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



(注) コマンドの構文は、ASA のプラットフォームによって若干異なります。この例の中で設定されたユーザは、「[NNM MIB ブラウザの設定](#)」セクション(2-39 ページ)でコミュニティストリングを使用して定義したユーザと同じです。

NNM traprcv ユーティリティは、リモート SNMP エンティティから送信される SNMP トラップメッセージの受信、および SNMP inform 要求への応答を行うためのコマンドラインツールです。このユーティリティは、通知をリッスンするため SNMP トラップポート(udp/162)にバインドされています。そのため、root として実行する必要があります。また受信した通知に関しては標準的な出力メッセージを出力します。traprcv ユーティリティでは、SNMP バージョン 1 トラップ、SNMP バージョン 2c トラップ、SNMP バージョン 2c inform 要求、SNMP バージョン 3 トラップ、および SNMP バージョン 3 inform 要求を受信できます。詳細については、NNM SPI SNMP Version 7.53 のマニュアルを参照してください。

ステップ 4 traprcv ユーティリティを実行し、SNMP エージェント上でトラップが送達されるのを待機します。このユーティリティの実行ファイルは、C:\Program Files\HP OpenView\snmpv3\utils\traprcv.exe です(図 2-43 を参照)。

図 2-43 SNMP トラップレシーバ

```
C:\Program Files\HP OpenView\snmpv3\utils>traprcv
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)
```

## HP OpenView NNM Web アプリケーションの使用方法

NNM Web アプリケーションを起動する手順は次のとおりです。

ステップ 1 Web ブラウザから、次の URL にアクセスします。

<http://<NNM サーバの IP アドレス>:7510/topology/home>

ステップ 2 SNMP ノードを表示するため、ドロップダウンメニューから [Internet View] を選択します(図 2-44 を参照)。

[Internet View] ウィンドウが表示されます(図 2-45 を参照)。

図 2-44 [NNM Home Base] ウィンドウ

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  
 ops from the selected device.

Node Status Summary Alarm Browser About

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

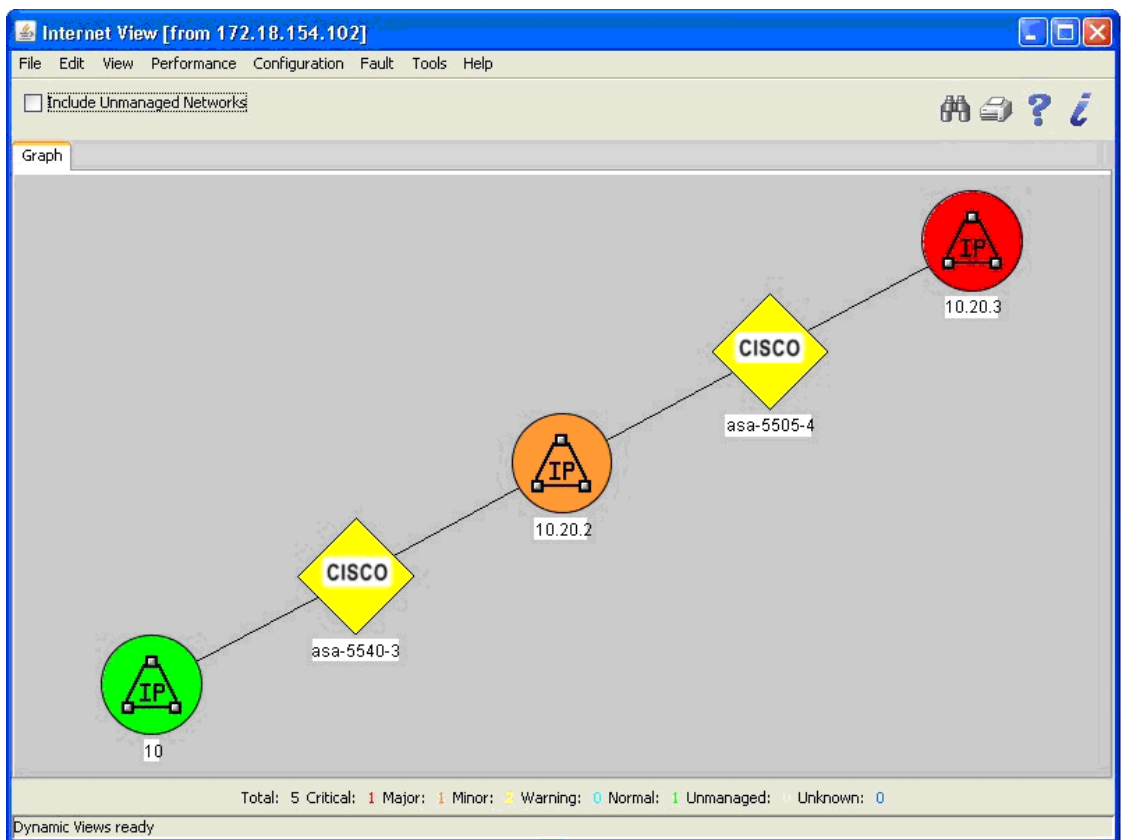
Critical	: 0 (0%)
Major	: 0 (0%)
Minor	: 2 (40%)
Warning	: 0 (0%)
Normal	: 3 (60%)
Unknown	: 0 (0%)
Total	: 5

Dynamic Views ready

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

ステップ 3 ノードのプロパティを表示するため、選択したノードをダブルクリックします。ブラウザ ウィンドウが開き、ノード情報が表示されます。

図 2-45 [Internet View] ウィンドウ



## CiscoWorks

CiscoWorks LAN Management Solution (LMS) は、Cisco ネットワークの設定、管理、モニタリング、およびトラブルシューティングの作業を簡素化するための強力な管理ツールスイートです。詳細については、次の URL を参照してください。

<http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html>

この項では、次のトピックについて取り上げます。

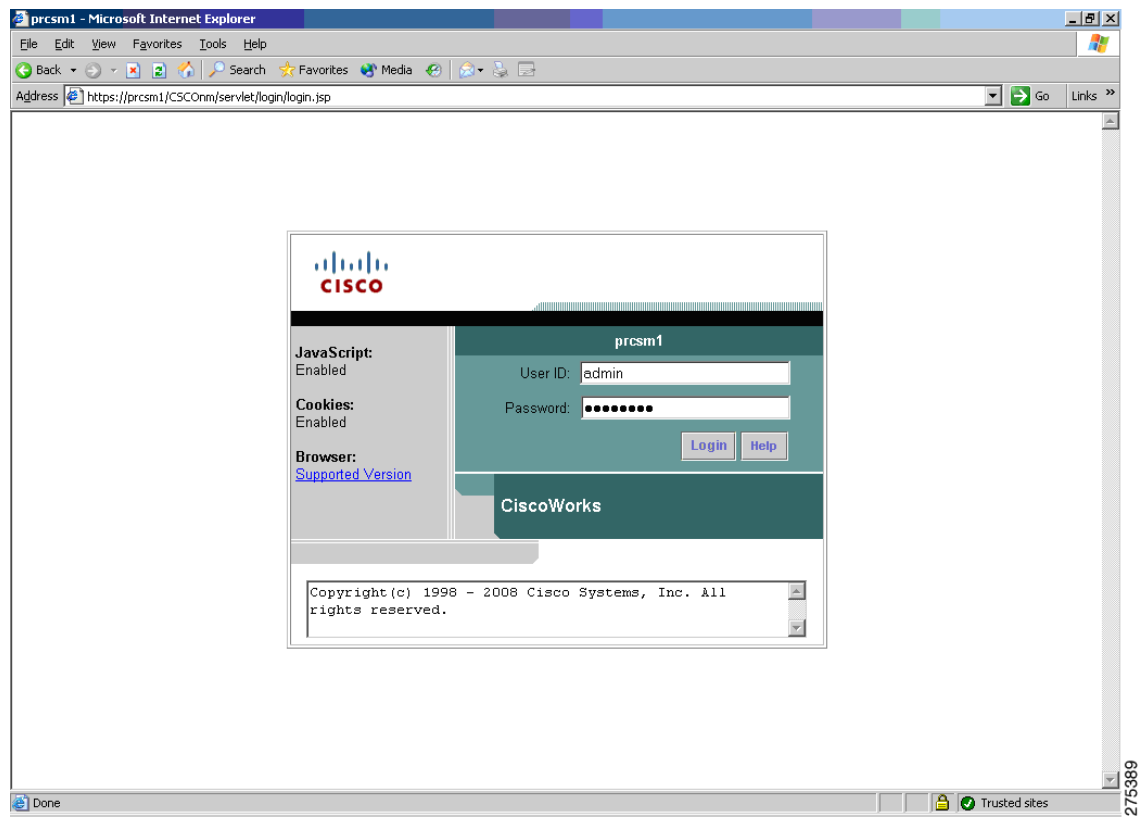
- [CiscoWorks の起動 \(2-47 ページ\)](#)
- [CiscoWorks LMS Portal の概要 \(2-48 ページ\)](#)
- [Device Center の使用方法 \(2-48 ページ\)](#)
- [SNMP ウォークの実行 \(2-49 ページ\)](#)
- [Management Station to Device ツールの使用方法 \(2-54 ページ\)](#)

## CiscoWorks の起動

Windows 2003 サーバ上で CiscoWorks を起動する手順は次のとおりです。

[Start] > [All Programs] > [CiscoWorks] > [CiscoWorks] を選択します。図 2-46 は、ログインページを示したものです。

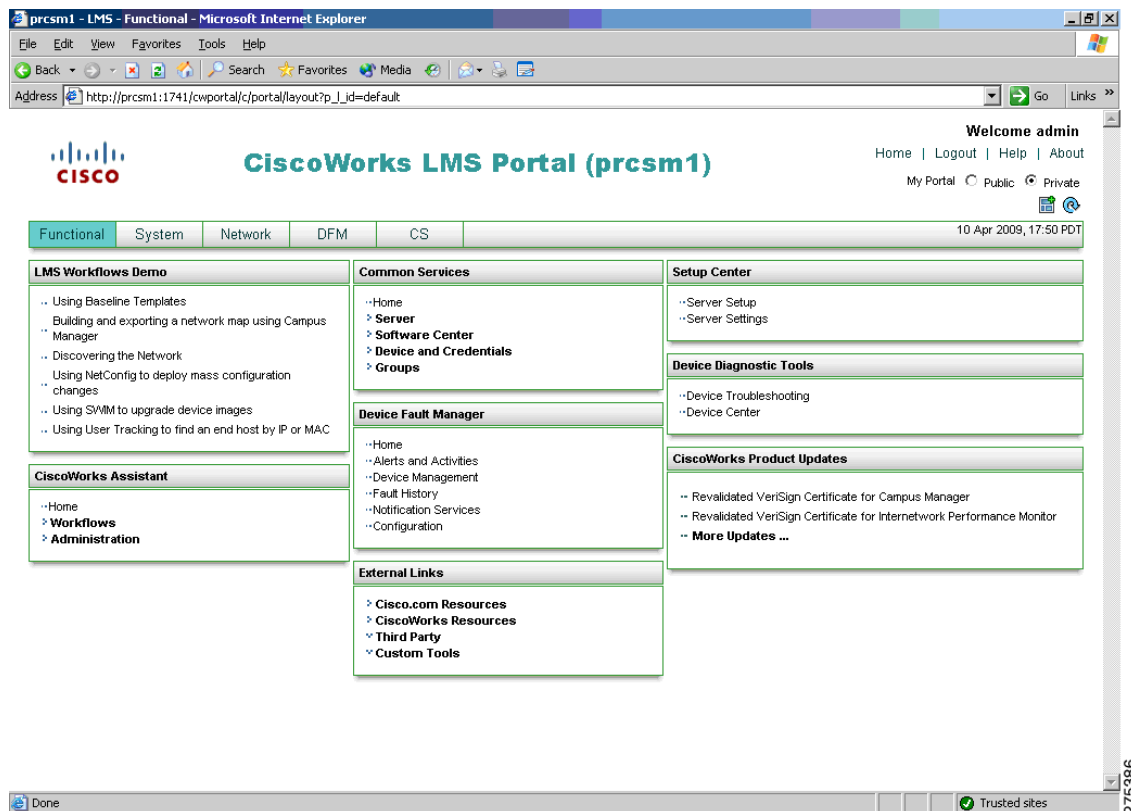
図 2-46 ログインページ



## CiscoWorks LMS Portal の概要

CiscoWorks LMS Portal は、LMS アプリケーションの起動時に表示される最初のページです (図 2-47 を参照)。このページは、アプリケーションの中で頻繁に使用する機能へのインターフェイスであり、それらの使用開始画面としての役割を持っています。

図 2-47 [CiscoWorks LMS Portal] ページ



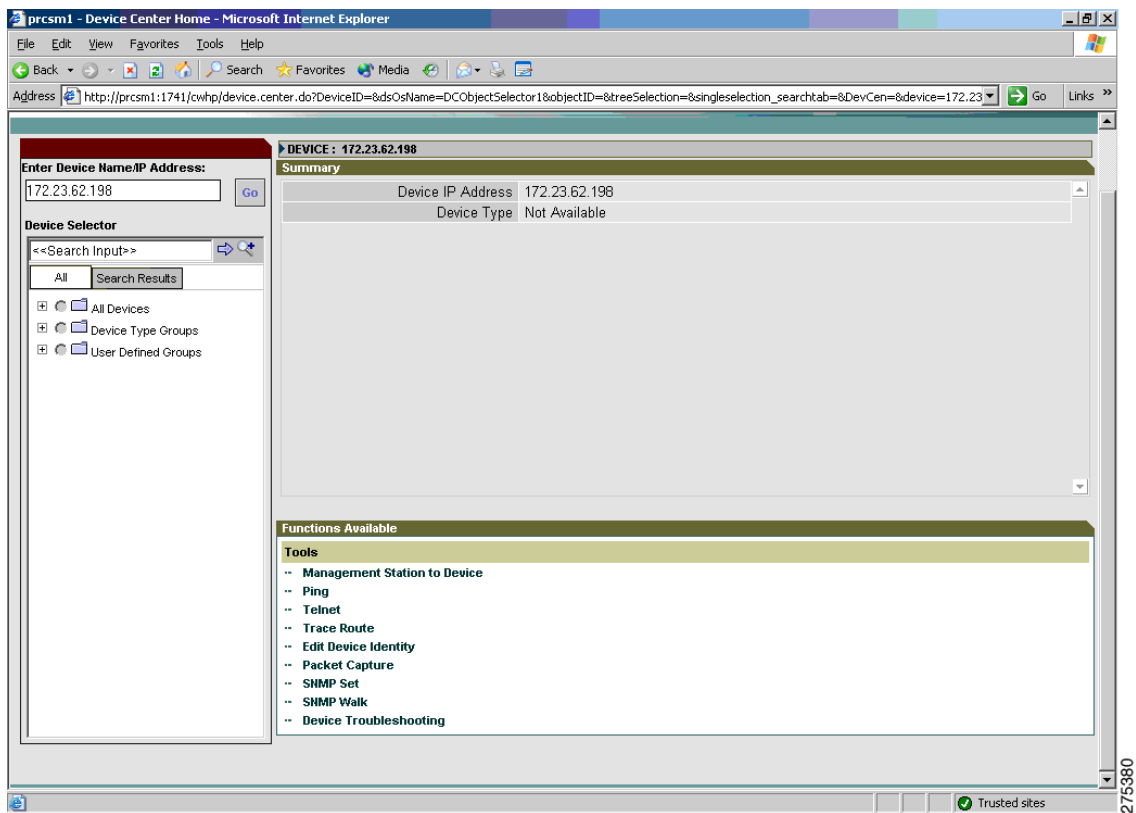
## Device Center の使用方法

デバイスを管理する手順は次のとおりです。

- ステップ 1 [Device Diagnostic Tools] > [Device Center] を選択します (図 2-48 を参照)。  
[Device Center Home] ページが開き、左側ペインに [Device Selector]、右側ペインに Device Center のサマリー情報が表示されます。
- ステップ 2 [Device Selector] ペインで、IP アドレスまたはデバイス名を入力するか、あるいはリストからデバイスを選択して、[Go] をクリックします。



図 2-48 [Device Center Home] ウィンドウ

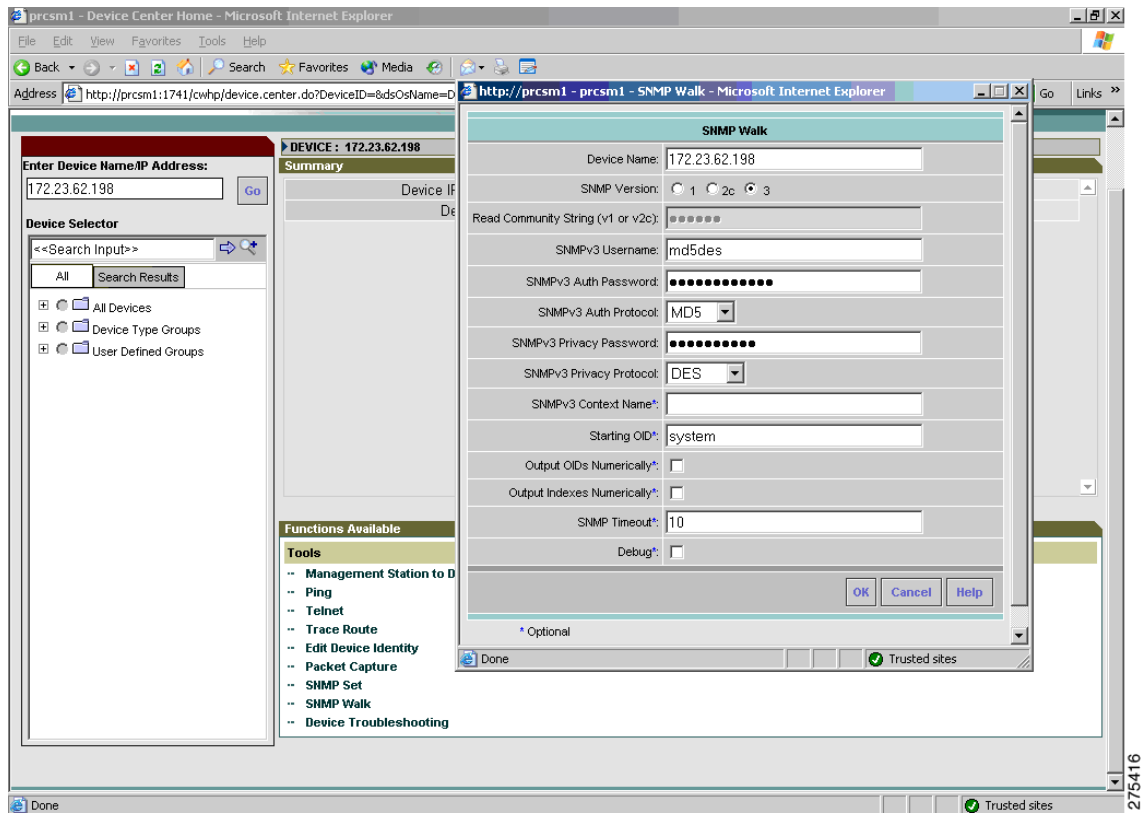


## SNMP ウォークの実行

SNMP ウォークを実行する手順は次のとおりです。

- ステップ 1 [Functions Available] ペインで、[SNMP Walk] リンクをクリックします。  
[SNMP Walk] ダイアログボックスが表示されます(図 2-49 を参照)。

図 2-49 [SNMP Walk] ダイアログボックス



ステップ 2 次の中から、使用する SNMP のバージョンを選択します。

- SNMP バージョン 3(セキュリティ レベルが NoAuthNoPriv および AuthNoPriv)の場合
  - a. SNMPv3 ユーザ名を入力します。
  - b. SNMPv3 認証パスワードを入力します。
  - c. ドロップダウンリストから SNMP v3 認証プロトコル(MD5 または SHA)を選択します。
  - d. SNMP コンテキスト名を入力します。



(注) ASA ではコンテキストがサポートされていません。そのため、[SNMP Context Name] は空欄にしておく必要があります。

- SNMP バージョン 3(セキュリティ レベルが AuthPriv)の場合
  - a. SNMPv3 ユーザ名を入力します。
  - b. SNMPv3 認証パスワードを入力します。
  - c. SNMP v3 認証プロトコルを指定します。MD5 と SHA のどちらかを選択します。
  - d. プライバシー パスワードを入力します。
  - e. ドロップダウンリストからプライバシー プロトコルを選択します。DES、トリプル DES、AES128、AES192、AES256 のいずれかを選択できます。
  - f. SNMP コンテキスト名を入力します。



(注) ASA ではコンテキストがサポートされていません。そのため、[SNMP Context Name] は空欄にしておく必要があります。

- g. (任意)開始 OID を入力します。このフィールドを空にした場合は 1 から開始されます。
- h. SNMP タイムアウト時間を入力します。デフォルト値は 10 秒です。
- i. (任意)出力される OID を数値として表示する場合は、[Output OIDs Numerically] チェックボックスをオンにします。
- j. デフォルトの場合、出力ウィンドウには対応する OID 名が表示されます。
- k. (任意)出力されるインデックスを数値として出力する場合は、[Output Indexes Numerically] チェックボックスをオンにします。
- l. (任意)デバッグオプションを有効にする場合は、[Debug] チェックボックスをオンにします。これらのフィールドに入力する文字列はすべて、大文字と小文字が区別されます。
- m. [OK] をクリックすると、入力したパラメータに基づく結果を取得できます。
- n. ウォークが完了したら、その結果をテキスト ファイルとして保存します(図 2-50 を参照)。



(注) 完全なウォークを実行すると、完了するまでに時間がかかる場合があります。

図 2-50 SNMP ウォークの結果例

The screenshot shows the CiscoWorks Device Center interface. The main window displays the 'SNMP Walk Results' for device 172.23.62.198. The results are as follows:

```

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 : discpasa
sysLocation.0 = STRING : sjc
sysServices.0 = INTEGER : 4
  
```

The interface also shows a 'Functions Available' section with the following tools:

- Management Station to Device
- Ping
- Telnet
- Trace Route
- Edit Device Identity
- Packet Capture
- SNMP Set
- SNMP Walk
- Device Troubleshooting

SNMPバージョン3のread/writeユーザ名およびパスワードと、SNMPバージョン1および2cのread/writeコミュニティストリングはどちらも、大文字と小文字が区別されます。Device and Credential Repository (DCR)にあるデバイスクレデンシャル(SNMPバージョン1、2c、および3)が使用可能であれば、それらが [SNMP Walk] ダイアログボックスに表示されます。使用可能でない場合は、各 SNMP バージョンに対するデフォルト値が表示されます。

Network Operator/Help Desk アクセス権限で SNMP ウォーク機能を使用すると、デバイスクレデンシャルのフェッチは失敗し、SNMPバージョン1、2c、および3に対応するread/writeコミュニティストリングの各フィールドにはデフォルト値が設定されます。

図 2-49 は、サポートされているプライバシープロトコルのリストを示したものです。SNMPバージョン1、2c、および3のクレデンシャルは、手動で入力する必要があります(図 2-52 を参照)。

図 2-51 [SNMP Walk] ダイアログボックス

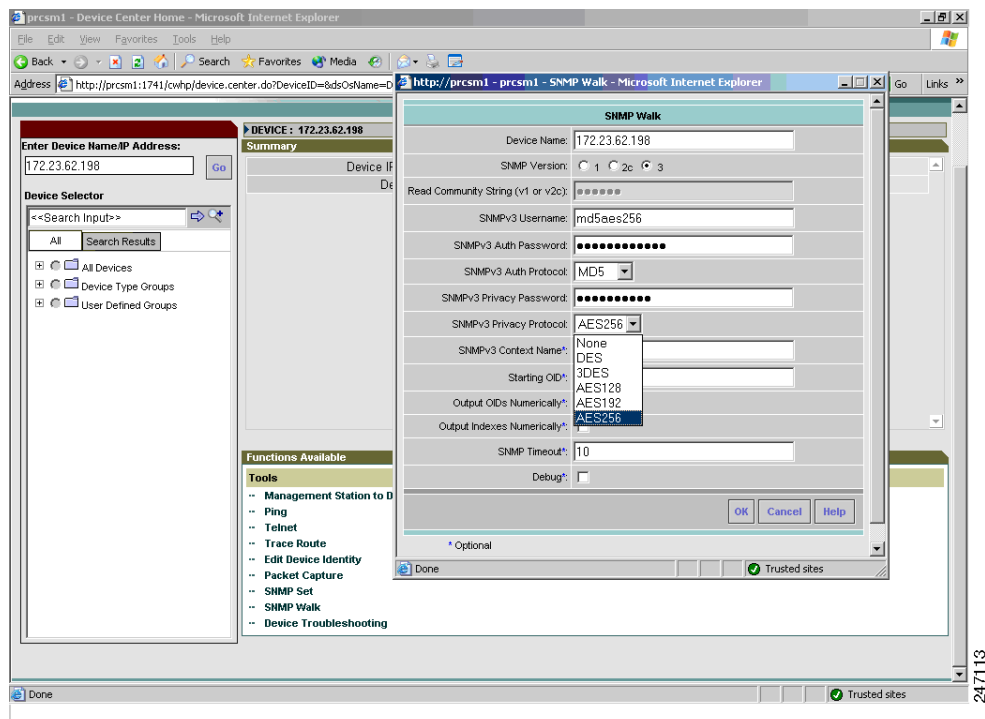


図 2-52 SNMP バージョン3 のパラメータ

SNMP Walk

Device Name: 172.23.62.198

SNMP Version:  1  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

\* Optional

Done Trusted sites

図 2-53 は、MD5 認証および AES256 暗号化アルゴリズムの設定に関する SNMP ウォークの結果を示したものです。

図 2-53 [SNMP Walk Results] ダイアログボックス

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 : 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

Close

## Management Station to Device ツールの使用方法

管理対象外のデバイスや応答のないデバイスに関するトラブルシューティングを行う場合、デバイスの接続をプロトコルごとにチェックすることがあります。Management Station to Device ツールを使用すると、レイヤ 4 (アプリケーション) の接続の問題点を診断することが可能です。

レイヤ 4 のテストは、ネットワーク デバイスの管理に欠くことのできない次のようなサービス要素を対象とします。

- デバッグ ツールおよび測定ツール (UDP および TCP)
- Web サーバ (HTTP)
- ファイル転送 (TFTP)
- 端末 (Telnet)
- 読み取り/書き込みアクセス (SNMP)

Management Station to Device ツールによるチェックの対象となるのは、プロトコルの接続のみです。対応するプロトコルのクレデンシャルは、テストや検証の対象にはなりません。IP アドレスではなくホスト名を入力すると、アドレスを特定するため名前検索が実行されます。アドレスが特定できないと、このタスクは失敗します。

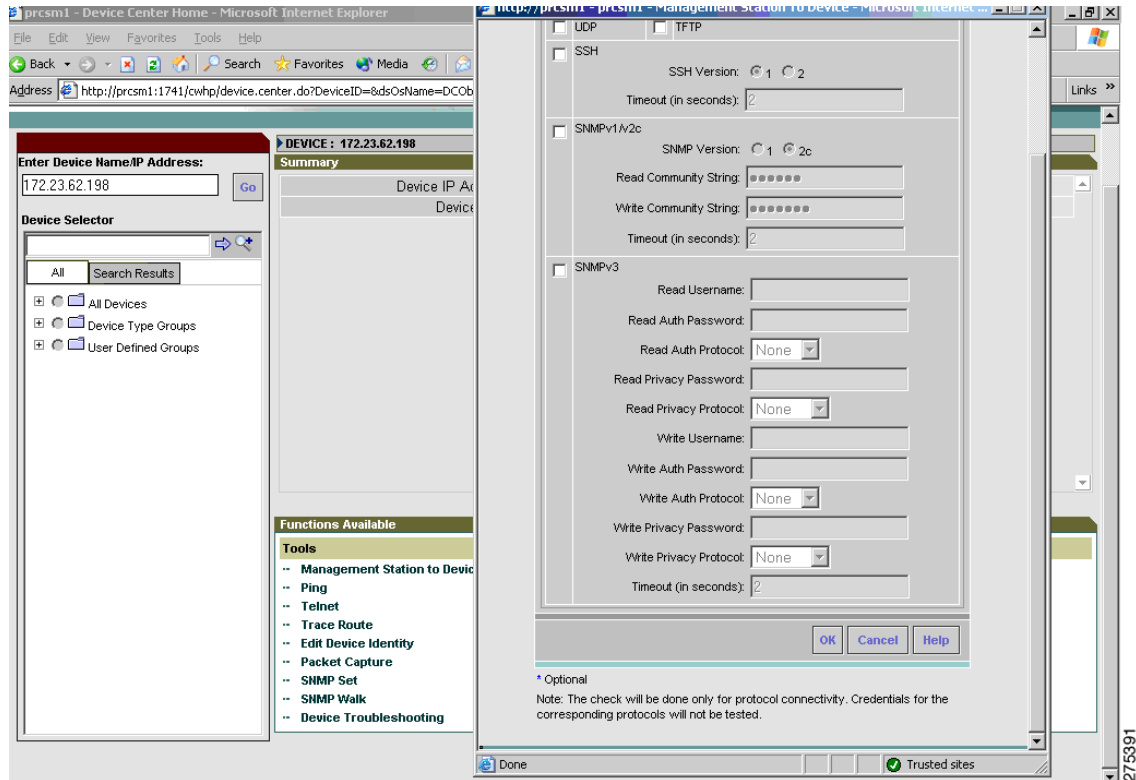
このツールを使用すると、SNMP 読み取りテスト (SNMPR) を行う場合に、宛先デバイスに SNMP の get 要求を送信することができます。また、SNMP 書き込みテスト (SNMPW) を行う場合には、宛先デバイスに SNMP の set 要求を送信することもできます。このプロトコルは、SNMP バージョン 1、2c、および 3 に対してサポートされています。

Network Operator/Help Desk アクセス権限で Management Station to Device ツールを起動すると、デバイス クレデンシャルのフェッチは失敗し、SNMP バージョン 1、2c、および 3 に対応する read/write コミュニティ ストリングの各フィールドにはデフォルト値が設定されます。SNMP バージョン 1、2c、および 3 のクレデンシャルは、手動で入力する必要があります。

Management Station to Device ツールを起動する手順は次のとおりです。

- 
- ステップ 1 [Device Diagnostic Tools] > [Device Center] を選択します。
  - ステップ 2 チェックの対象となるデバイスの名前または IP アドレス、完全修飾ドメイン名、またはホスト名を [Device Selector] フィールドに入力するか、またはチェックの対象となるデバイスをリストから選択し、[Go] をクリックします。  
[Summary] ペインおよび [Functions Available] ペインが表示されます。
  - ステップ 3 [Functions Available] ペインで [Management Station to Device] をクリックします。  
[Management Station to Device] ダイアログボックスが表示されます (図 2-54 を参照)。

図 2-54 [Management Station to Device] ダイアログボックス



ステップ 4 次の中から、対象とする接続アプリケーションを選択します。これらのフィールドに入力する文字列はすべて、大文字と小文字が区別されます。

- SNMP v3(セキュリティ レベルが NoAuthNoPriv)を選択した場合は、次の情報を入力します。
  - read ユーザ名。
  - write ユーザ名。
  - タイムアウト(秒単位)。デフォルト値は 2 秒です。
- SNMP v3(セキュリティ レベルが AuthNoPriv)を選択した場合は、次の情報を入力します。
  - read ユーザ名。
  - read 認証パスワード。
  - read 認証プロトコル。ドロップダウン リストから MD5 と SHA のどちらかを選択します。
  - write ユーザ名。
  - write 認証パスワード。
  - write 認証プロトコル。ドロップダウン リストから MD5 または SHA を選択します。
  - タイムアウト(秒単位)。デフォルト値は 2 秒です。
- SNMP v3(セキュリティ レベルが AuthPriv)を選択した場合は、次の情報を入力します。
  - read ユーザ名。
  - read 認証パスワード。
  - read 認証プロトコル。ドロップダウン リストから MD5 または SHA を選択します。
  - read プライバシー パスワード。

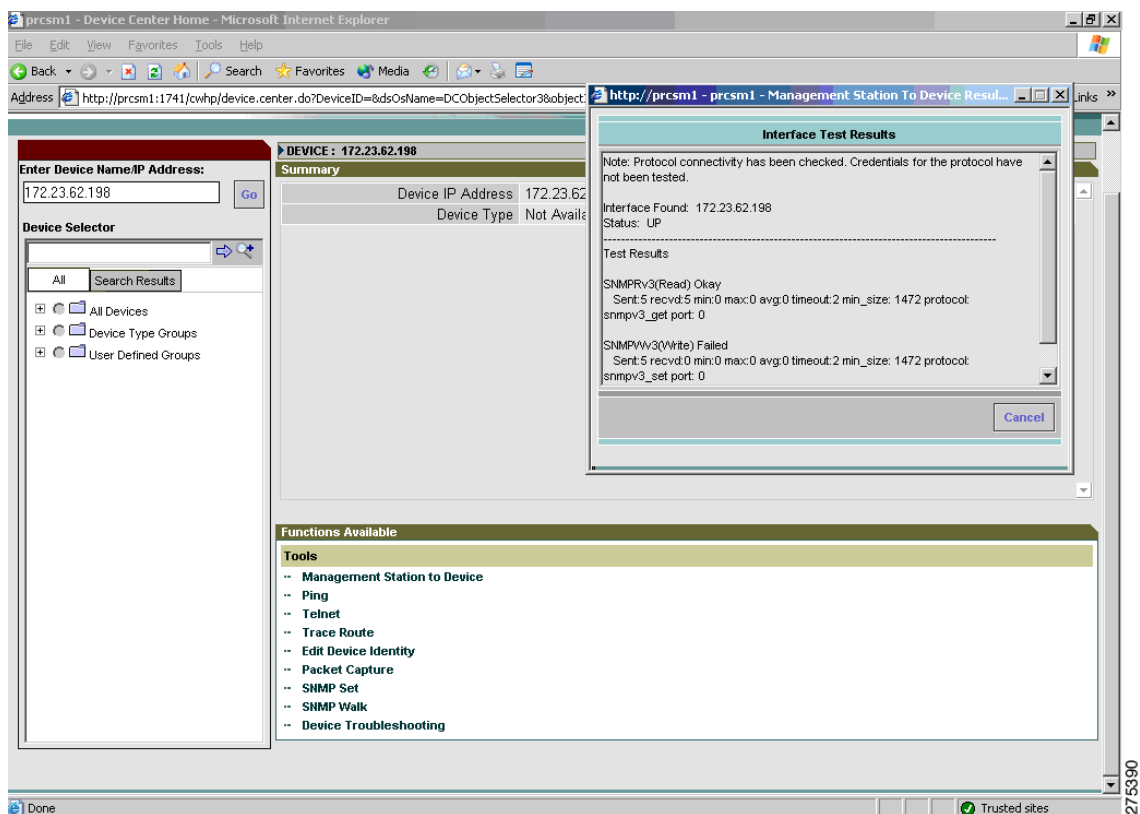
- read プライバシー プロトコル。ドロップダウン リストからプライバシー プロトコルを選択します。DES、トリプル DES、AES128、AES192、AES256 のいずれかを選択できます。
- write ユーザ名。
- write 認証パスワード。
- write 認証プロトコル。ドロップダウン リストから MD5 または SHA を選択します。
- write プライバシー パスワード。
- write プライバシー プロトコル。ドロップダウン リストからプライバシー プロトコルを選択します。DES、トリプル DES、AES128、AES192、AES256 のいずれかを選択できます。
- タイムアウト(秒単位)。デフォルト値は 2 秒です。

[Interface Test Results] ダイアログボックスに結果が表示されます(図 2-55 を参照)。**[Interface Details Results]** ダイアログボックスには、テスト済みのインターフェイスおよびテスト結果がオブションごとに表示されます。



(注) SNMP バージョン 3 の read/write ユーザ名およびパスワードと、SNMP バージョン 1 および 2c の read/write コミュニティ スtring はどちらも、大文字と小文字が区別されます。

図 2-55 [Management Station Device Results] ダイアログボックス







---

## A

### ASA の設定

SNMP バージョン 3 1-2

---

## C

### CiscoWorks 2-46

Device Center の使用 2-48

LMS ポータル 2-48

Management Station to Device ツールの使用 2-54

SNMP ウォークの実行 2-49

起動 2-47

---

## H

### HP OpenView

MIB の参照 2-41

MIB のロード 2-32

MIB ブラウザのパケット トレースの実行 2-42

NNM MIB ブラウザの設定 2-39

NNM SNMP バージョン 3 トラップ ビューアの使用 2-43

NNM Web アプリケーションの使用 2-44

NNM のインストール 2-31

NNM の起動 2-31

SNMP バージョン 3 の MD5 Auth/No-priv 接続の設定 2-40

SNMP バージョン 3 の MD5 Auth/Priv 接続の設定 2-41

SNMP バージョン 3 の No-auth/No-priv 接続の設定 2-40

SNMP バージョン 3 の SHA Auth/No-priv 接続の設定 2-40

SNMP バージョン 3 の SHA Auth/Priv 接続の設定 2-41

グローバルな SNMP バージョン 3 クレデンシャルの設定 2-37

現在のマップへのネットワークの追加 2-33

特定の SNMP バージョン 3 クレデンシャルの設定 2-38

特定の SNMP バージョン 3 パラメータの設定 2-36

ノード情報の表示 2-38

HP OpenView Network Node Manager 2-30

---

## I

### Ipswitch WhatsUp Gold 2-17

SNMP MIB または OID のウォーク 2-23

SNMP エージェントの新規追加 2-18

SNMP トラップの設定 2-27

SNMP バージョン 3 クレデンシャルの追加 2-19

Web インターフェイスの起動 2-22

アプリケーションの起動 2-18

---

## N

### Net-SNMP 2-1

MIB のポーリング 2-1

トラップの送信 2-2

NNM traprcv ユーティリティ 2-44

---

## S

### SilverCreek

MIB のテスト 2-12

MIB のロードと削除 2-7

MIB ブラウザへのアクセス [2-13](#)  
 SNMP バージョン 3 エージェントのセットアップ [2-5](#)  
 アプリケーションの起動 [2-3](#)  
 通知トラップ メッセージの受信 [2-15](#)  
 テストスイートの実行 [2-8](#)  
 デバッグの有効化 [2-10](#)  
 パフォーマンスのテスト [2-16](#)  
 SilverCreek, SNMP テストスイート [2-3](#)  
 SNMP コマンド [1-2](#)  
 SNMP の設定例 [1-2](#)  
 SNMP バージョン 3 の概要 [1-1](#)  
 snmptrap コマンドの出力 [2-3](#)  
 snmptrapd コマンド [2-2](#)  
 snmpwalk コマンドの出力 [2-2](#)

---

## か

### 概要

SNMP バージョン 3 [1-1](#)

---

## さ

サードパーティ製ツール [2-1](#)  
 HP OpenView Network Node Manager [2-30](#)  
 Ipswitch WhatsUp Gold [2-17](#)  
 SilverCreek [2-3](#)

---

## そ

その他のツールに関する資料 [i-v](#)

---

## つ

### ツール

ネットワーク管理 [1-1](#)

---

## ね

ネットワーク トポロジ [1-2](#)  
 ネットワーク管理ツール [1-1](#)  
 CiscoWorks [2-46](#)