Using Network Data Collector

The Network Data Collector tool is made up of eight processes, each available in the Network Data Collector drawer. The processes are performed in the order shown below. Once one process is successfully completed, the next process will automatically begin.

1. Net Audit Settings
2. Device Import/Discovery
3. Device Selection
4. Access Verification
5. Interface/Ports Selection (VoIP audit only)
6. Data Collection
7. Data Collection Status
8. Data Packaging

The Net Audit Process

The following shows an overview of the Net Audit process performed using the Network Data Collector Tool.

Step 1 Set up the audit.

Step 2 Import and/or add devices.

Step 3 Select devices to be tested for telnet access capability.

Step 4 Run selected devices through telnet access verification test.

Step 5 From the devices that passed access verification, select the ones to include in the data collection.

Step 6 Start or schedule data collection.

Step 7 Start data packaging.

Step 8 Upload files to CCO.

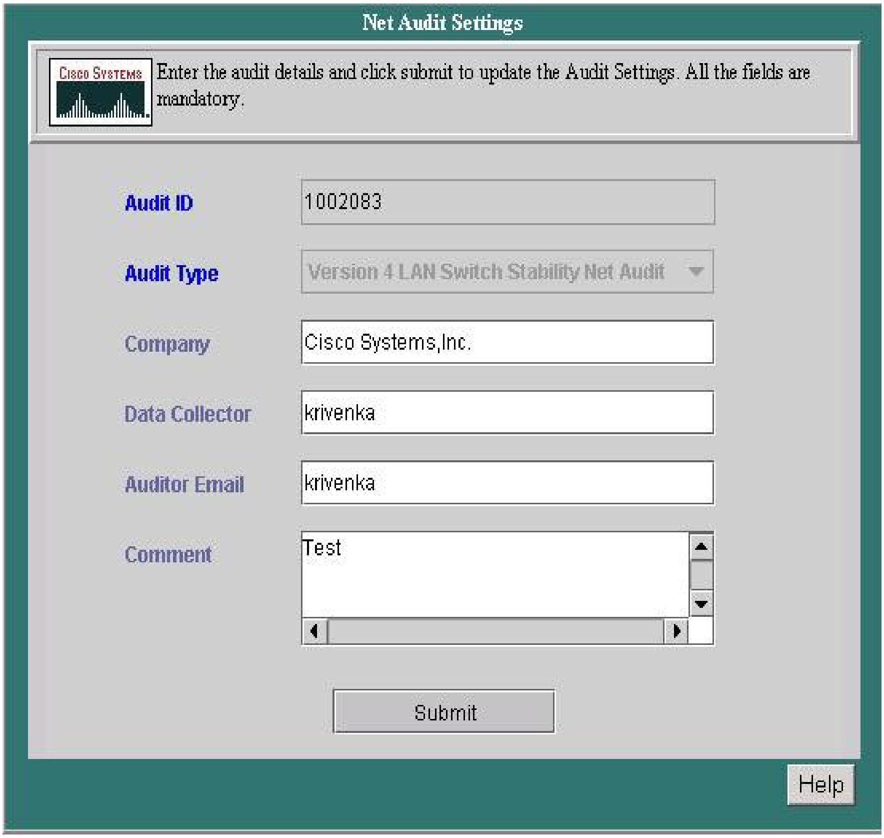
Setting Up An Audit

The initialization phase of setting up an audit is done here. The following information can be entered on this screen:

- Company
- Data Collector
- Auditor Email
- Comments

Procedure

Step 1 Select **Network Data Collector >Net Audit Settings**. The Net Audit Settings dialog box appears.



Net Audit Settings

Enter the audit details and click submit to update the Audit Settings. All the fields are mandatory.

Audit ID	1002083
Audit Type	Version 4 LAN Switch Stability Net Audit
Company	Cisco Systems,Inc.
Data Collector	krivenka
Auditor Email	krivenka
Comment	Test

Step 2 Enter the name of the company the audit is being peformed for in the **Company** field.

Step 3 Enter the name of the company contact person in the **Audit Engineer** field.

Step 4 Enter the email address of the audit engineer in the **Auditor Email** field.

Step 5 Enter any information deemed pertinent in regards to the audit being performed in the **Comment** field.

Step 6 Click **Submit**.

Important

- The Company, Audit Engineer, Auditor Email, and Comments fields are all mandatory.
- Symbols are not accepted in the Company or Audit Engineer fields.

Importing Devices

Select the Import method to choose which devices to include in the Net Audit. The methods available include Discovery and Network Management System import.

Discovery Methods

Use this option to specify the device discovery method for your network. Choose from CDP, Pingsweep Starting IP Address, or Pingsweep IP Address Range. An Advanced Settings link containing the following Resource Management Essentials (RME) tools is also available from within each method:

- Exclude Filters
- Include Filters
- Community
- Advanced Features
  - Set the total bandwidth
  - Set the maximum "% Bandwidth Usage" of total bandwidth
  - SNMP timeout rate
  - Number of SNMP retries
  - Ping timout rate
  - Number of Ping retries

Note Click the **Help** button in any of the above tools to learn more about that tool and how to use it.

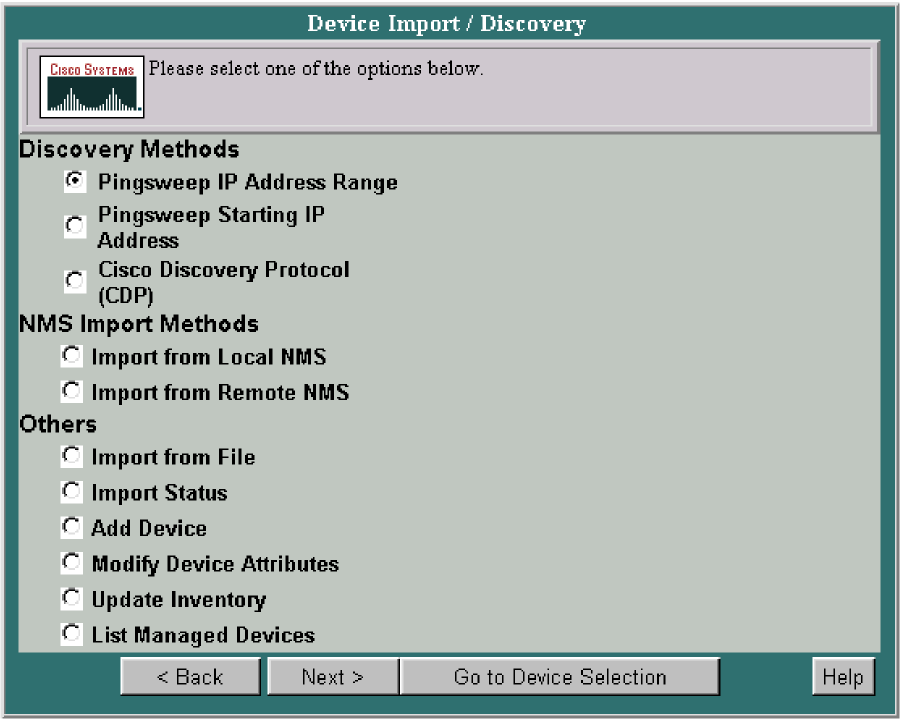
CDP

Discovers only CDP (Cisco Discovery Protocol) enabled Cisco devices. This method takes the least time to complete and is most useful in networks made up entirely of Cisco devices. Products acquired by Cisco do not support CDP. CDP is found in IOS 10.0 and later, and is not supported by WAN switches.

Devices running CDP periodically send out CDP hello messages that are picked up by other CDP-enabled devices and formulate a table of connected devices.

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.



Device Import / Discovery

Please select one of the options below.

Discovery Methods

● Pingsweep IP Address Range

○ Pingsweep Starting IP Address

○ Cisco Discovery Protocol (CDP)

NMS Import Methods

○ Import from Local NMS

○ Import from Remote NMS

Others

○ Import from File

○ Import Status

○ Add Device

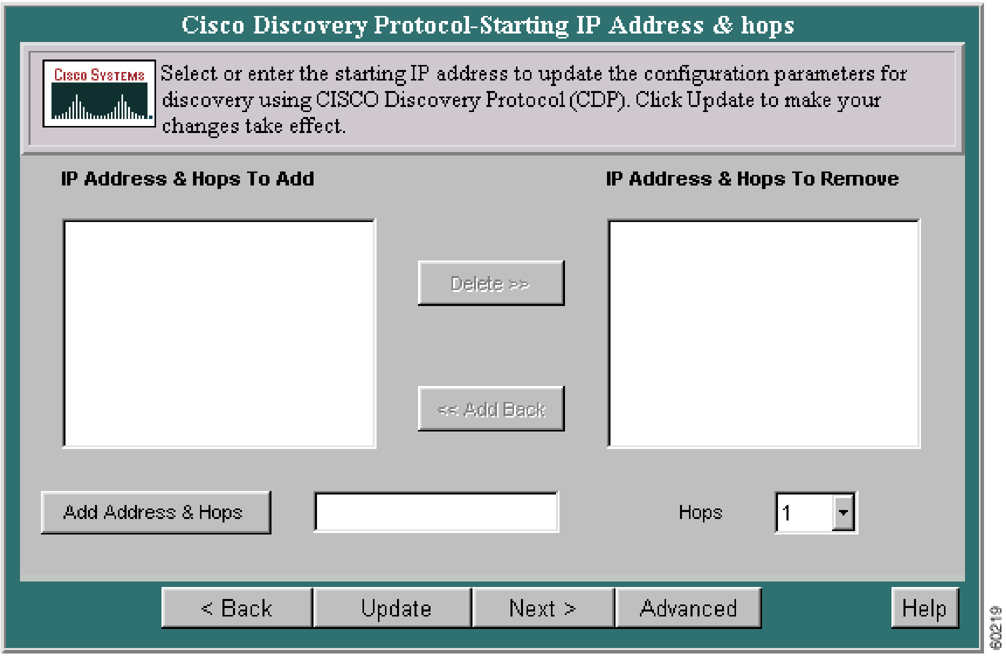
○ Modify Device Attributes

○ Update Inventory

○ List Managed Devices

Step 2 Click the radio button next to **Cisco Discovery Protocol (CDP)**.

Step 3 Click **Next**. The Cisco Discovery Protocol-Starting IP Address & Hops screen appears.



Cisco Discovery Protocol-Starting IP Address & hops

Select or enter the starting IP address to update the configuration parameters for discovery using CISCO Discovery Protocol (CDP). Click Update to make your changes take effect.

Hops: 1

Step 4 To delete an entry from the IP Address & Hops To Add window, select it, then click **Delete**. The entry is moved to the IP Address & Hops To Remove window.

Step 5 To return a deleted entry to the IP Address & Hops To Add window, select it, then click **Add Back.**

Step 6 To add a new IP address, enter the address in the Add Address & Hops window.

Step 7 Select the number of hops to be run from the Hops pull-down menu.

Step 8 Click **Update**. The new entries appear in the IP Address and Hops window.

Note Click on **Advanced** to display the Advanced Settings window.

Pingsweep Starting IP

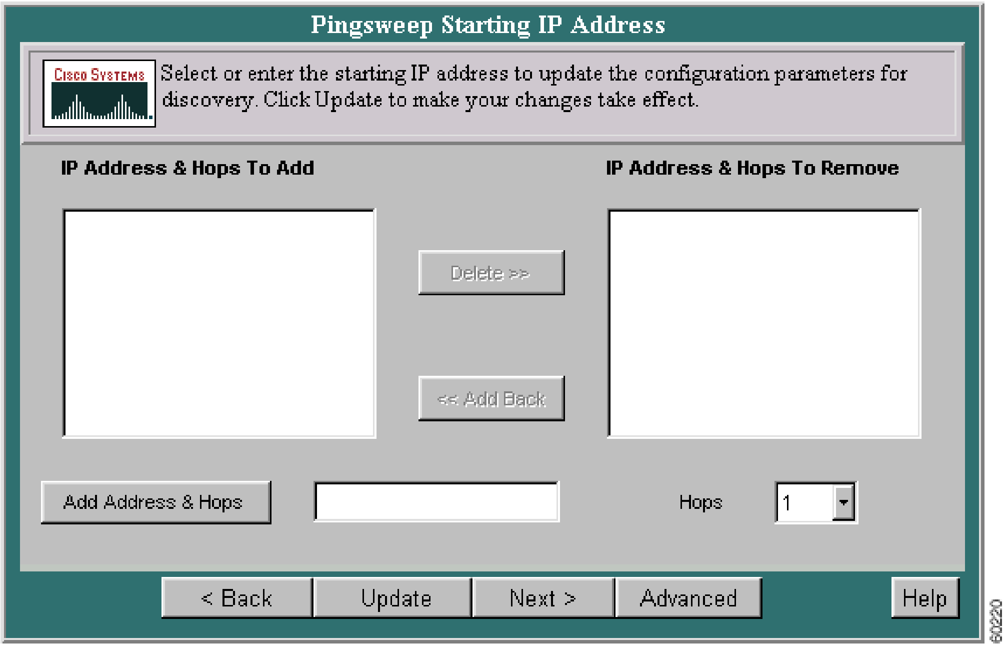
Discovers all SNMP-enabled Cisco devices in your network. This method takes the longest time to complete but is the most comprehensive. In this method, device discovery finds all devices connected to the device whose IP address is given. The process is repeated recursively until all devices are reached.

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Pingsweep Starting IP Address**.

Step 3 Click **Next**. The Pingsweep Starting IP Address screen appears.



Pingsweep Starting IP Address

Select or enter the starting IP address to update the configuration parameters for discovery. Click Update to make your changes take effect.

Hops: 1

Step 4 To delete an entry from the IP Address & Hops To Add window, select it, then click **Delete**. The entry is moved to the IP Address & Hops To Remove window.

Step 5 To return a deleted entry to the IP Address & Hops To Add window, select it, then click **Add Back.**

Step 6 To add a new IP address, enter the address in the Add Address & Hops window.

Step 7 Select the number of hops to be run from the Hops pull-down menu.

Step 8 Click **Update**. The new entries appear in the IP Address and Hops window.

Note Click on **Advanced** to display the Advanced Settings window.

Pingsweep IP Address Range

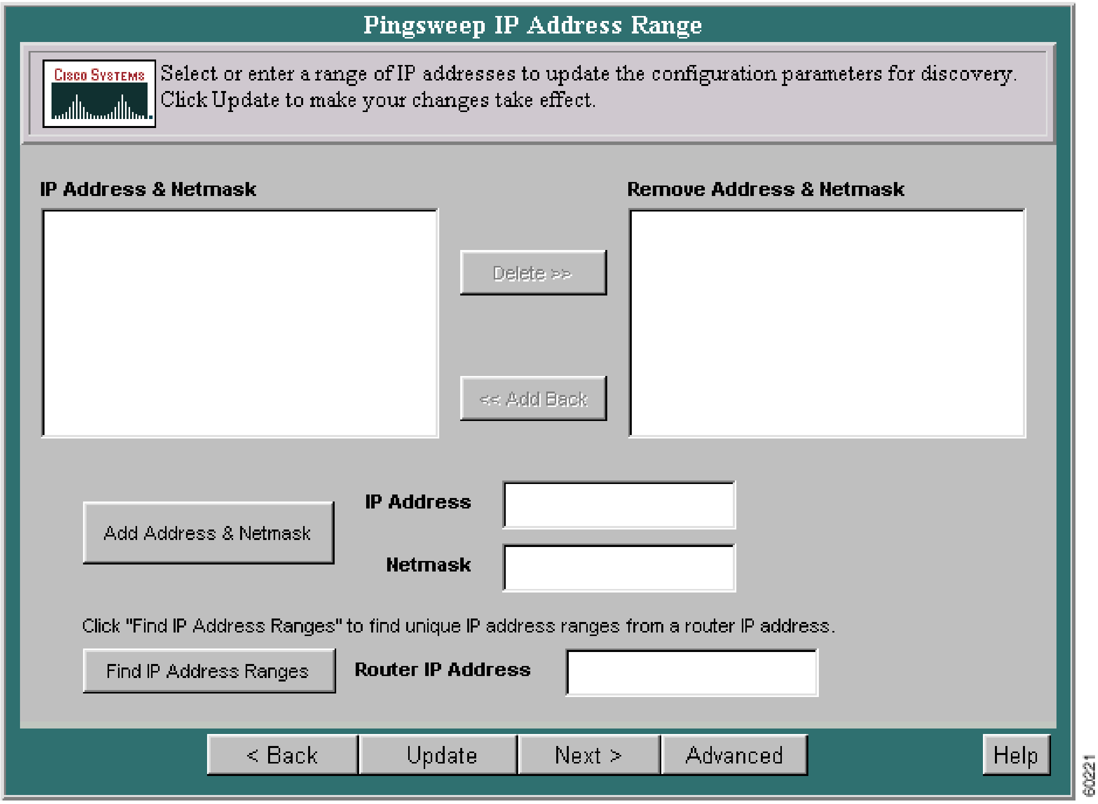
Discovers a specific range of SNMP-enabled Cisco devices in your network. This method takes more time to complete than the CDP method but less time than the Pingsweep Starting IP Address method. This method is useful if you know the unique IP subnets in the network. In this method, device discovery finds all the devices within a range of user-supplied IP addresses. It also provides the ability to find unique IP address ranges from a single device and perform device discovery using the address ranges.

Procedure

Step 1 Select **Network Data Collector > Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Pingsweep IP Address Range**.

Step 3 Click **Next**. The Pingsweep IP Address Range screen appears.



Pingsweep IP Address Range

Select or enter a range of IP addresses to update the configuration parameters for discovery.
Click Update to make your changes take effect.

Click "Find IP Address Ranges" to find unique IP address ranges from a router IP address.

Step 4 To delete an entry from the IP Address & Netmask window, select it, then click **Delete**. The entry is moved to the IP Address & Netmask To Remove window.

Step 5 To return a deleted entry to the IP Address & Netmask window, select it, then click **Add Back.**

Step 6 To add a new IP address and netmask, enter the address in the Add Address & Netmask window and click **Add Address & Netmask**.

Step 7 If you do not know the unique IP address ranges, enter the main router IP address in the Router IP Address window and click **Find IP Address Ranges**. The IP address ranges will be found.

Step 8 Click **Update**. The new entries appear in the IP Address and Netmask window.

Note Click on **Advanced** to display the Advanced Settings window.

NMS Import Methods

The NMS Import module will allow the device list to be imported from an existing Network Management System (NMS). Select to import from either a Local NMS or a Remote NMS.

Import from Local NMS

Local NMS Import gets the list of devices being managed by the specified local NMS and makes them available to RME applications.

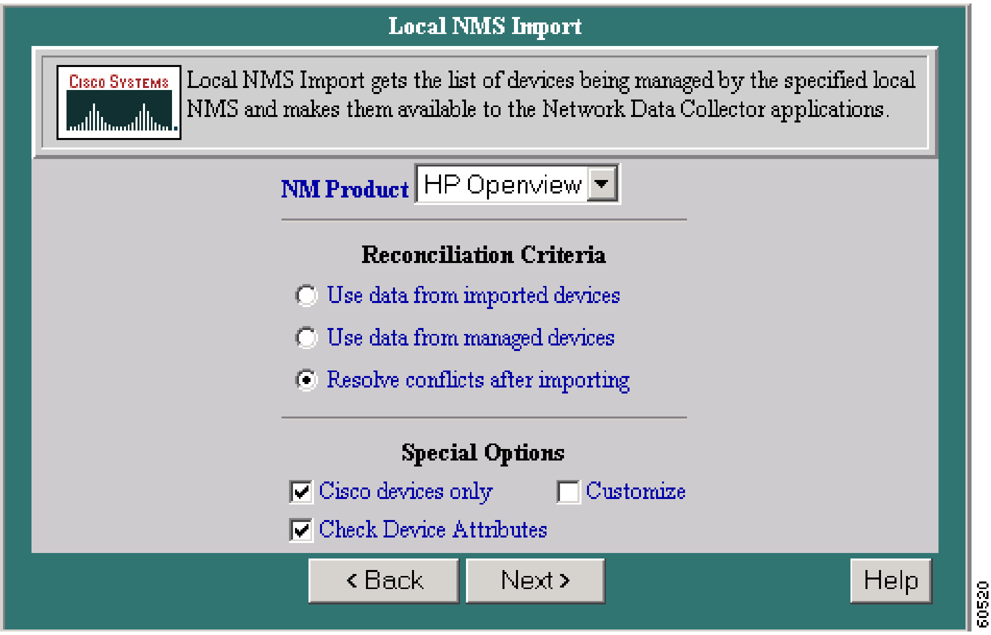
You can populate your RME server with device inventory data by importing the data from a supported network management system database residing on the local host.

Procedure

Step 1 Select **Network Data Collector > Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Import from Local NMS**.

Step 3 Click **Next**. The Local NMS Import screen appears.



Local NMS Import

Local NMS Import gets the list of devices being managed by the specified local NMS and makes them available to the Network Data Collector applications.

NM Product: HP Openview

Reconciliation Criteria

○ Use data from imported devices

○ Use data from managed devices

● Resolve conflicts after importing

Special Options

☑ Cisco devices only □ Customize

☑ Check Device Attributes

Step 4 Select the database you are importing from the NM Product drop-down list box. Only applicable products appear.

Step 5 Click a radio button in the Reconciliation Criteria list. This specifies the conflict resolution method to apply if there is a conflict between a device you try to import and a managed device with the same hostname and domain name.

Step 6 Select **Cisco Devices Only** or **Customize** or both under Special Options, then click **Next**. To change default import options, click **Customize**.

- If you select **Cisco Devices Only**, device filtering is performed only for CiscoWorks and HP OpenView. Note that if you performed a "quick sync" in CiscoWorks, device filtering will not work. (Devices are filtered based on the SNMP variable "sysObjectId.")

- If you select **Customize**, the Import Options dialog box appears. Enter the import options that apply to your NMS database.
- If you installed the NMS at a user-specified location (instead of the default), click **Customize** and enter the Source location.
- If you select **Check Device Attributes** and RME is installed, device attribute information is verified after the import.

Step 7 Click **Finish**. The Add/Import Status Summary displays the number of devices that are managed, alias, pending, conflicting, suspended, and not responding.

- You can click any of these statuses to view the devices in that state.
- If you select **Check Device Attributes** and RME is installed, the number of device attribute errors is also shown. Click this field to view details.
- Click **Update** to display the most recent information.

Import from Remote NMS

Remote NMS Import gets the list of devices being managed by the specified remote NMS and makes them available to RME applications.

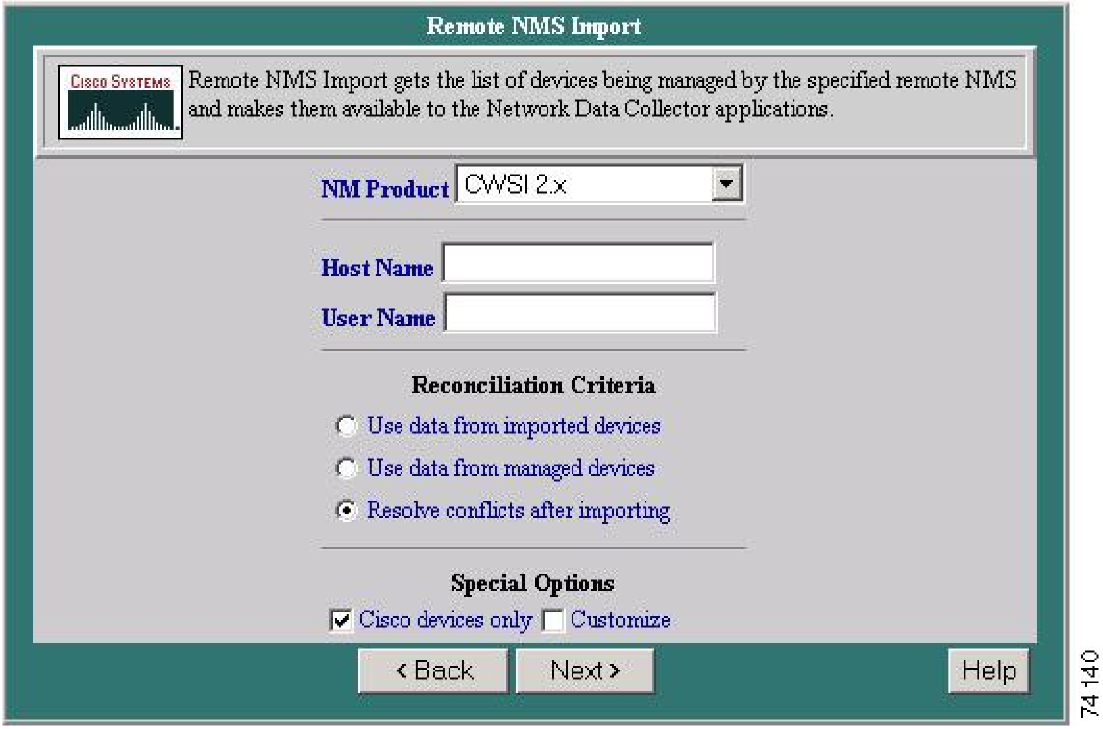
You can populate your RME server with device inventory data by importing the data from a supported network management system database residing on a remote host. Device import supports the following NMS databases.

Procedure

Step 1 Select **Network Data Collector > Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Import from Remote NMS**.

Step 3 Click **Next**. The Remote NMS Import dialog box appears.



Remote NMS Import

Remote NMS Import gets the list of devices being managed by the specified remote NMS and makes them available to the Network Data Collector applications.

NM Product: CWSI 2.x

Host Name:

User Name:

Reconciliation Criteria

○ Use data from imported devices

○ Use data from managed devices

● Resolve conflicts after importing

Special Options

☑ Cisco devices only □ Customize

Step 4 In the Host Name field, enter the network name of the host on which the remote NMS resides. In the User Name field, enter the name of the remote user.

Step 5 Click a radio button from the Reconciliation Criteria list. This specifies the conflict resolution method to apply if there is a conflict between a device you try to import and a managed device with the same host and domain names.

Step 6 Select **Cisco Devices Only** or **Customize** or both from Special Options, then click **Next**. If you are importing non-Cisco devices or you want to enter device information, click **Customize**.

- If you select **Cisco Devices Only**, devices are filtered based on the SNMP variable "sysObjectId." (Devices are not filtered on CWSI.)

- If you select **Customize** or **CWSI**, the Import Options dialog box appears. Enter the import options that apply to your NMS database.
- If you installed the NMS at a user-specified location (instead of the default), click **Customize** and enter the Source location.
- If you select **Check Device Attributes** and RME is installed, device attribute information is verified after the import.

Step 7 Click **Finish**. The Add/Import Status Summary displays the number of devices that are managed, alias, pending, conflicting, suspended, and not responding.

- You can click any of these statuses to view the devices in that state.
- If you selected **Check Device Attributes** and RME is installed, the number of device attribute errors is also shown. Click this field to view details.
- Click **Update** to display the most recent information.

Others

Import a device from a file, check the status of an import, add a device, modify a device, update inventory, or list managed devices.

Import from File

You can add multiple devices to Network Data Collector from a data source other than a supported NMS. Instead of adding each device individually using the online dialog box, you can perform a bulk device import from two kinds of files:

- Comma separated values (CSV) file, or
- Device integration file (DIF)

CSV files are the recommended way to import devices. They are generally easier to create, and they provide most, but not all, of the DIF functionality. If you cannot import device information from a CSV file, you can try importing from a DIF.

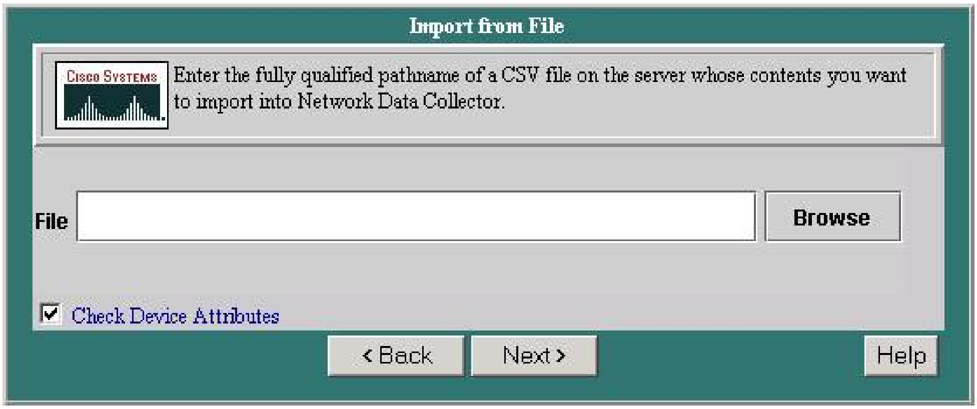
To validate device addresses before importing from a file, run the checkaddr.pl utility from the command line (from <your installation folder>/bin/checkaddr.pl).

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Import from File**.

Step 3 Click **Next**. The Import from File screen appears.



Import from File

Enter the fully qualified pathname of a CSV file on the server whose contents you want to import into Network Data Collector.

File

☑ Check Device Attributes

74138

Step 4 Enter the fully qualified pathname of a CSV file on the server whose contents you want to import.

Step 5 Click **Next** to add the file.

Input Status

The Add/Import Status Summary dialog box appears when you open it directly from the navigation tree and automatically when you add or import devices into Network Data Collector. Use the Add/Import Status Summary dialog box to:

- View a summary of the add or import progress
- List managed devices
- List and handle unmanaged devices

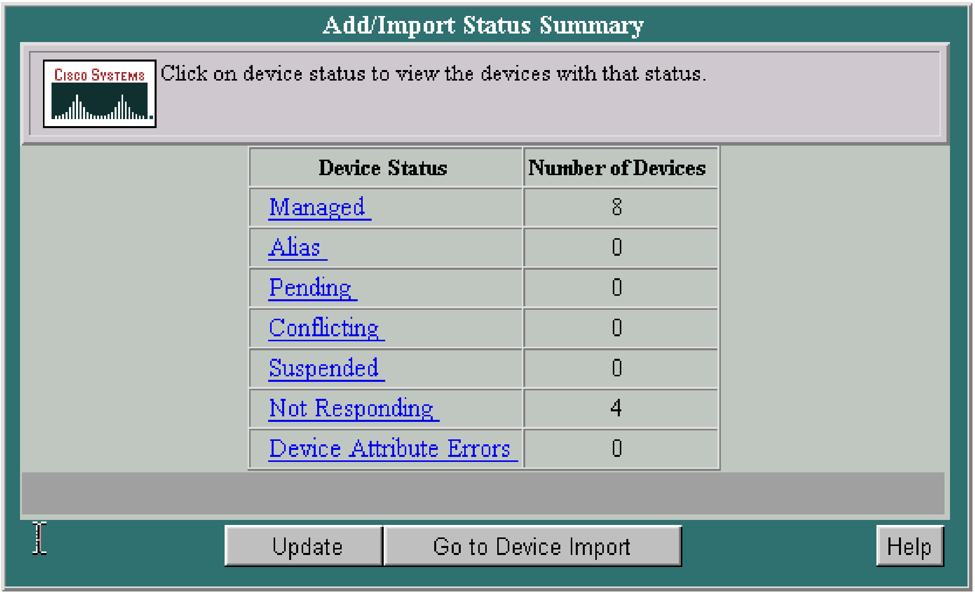
The Add/Import Status Summary displays device states of managed, alias, pending, conflicting, suspended, not responding, as well the number device attribute errors (if any). The pending count shows 0 when all devices have been added or imported.

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Import Status**.

Step 3 Click **Next**. The Add/Import Status Summary screen appears.



Add/Import Status Summary

Click on device status to view the devices with that status.

Device Status	Number of Devices
Managed	8
Alias	0
Pending	0
Conflicting	0
Suspended	0
Not Responding	4
Device Attribute Errors	0

Step 4 Click **Update** to refresh the display during the operation. You can continue to update the display until the pending count goes to 0.

Step 5 To display a read-only list of managed devices, click **Managed**.

Add Device

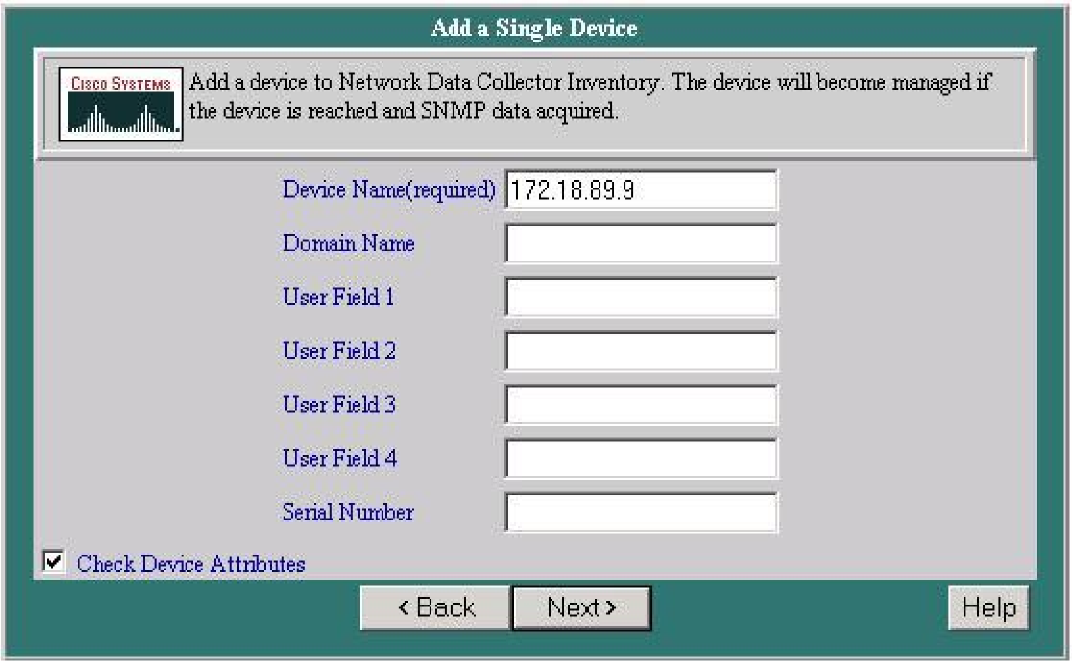
Add devices individually to the Network Data Collector inventory by specifying basic device information for each device. The device will become managed if the device is reached and SNMP data acquired. If you use this option to add a device that duplicates an already managed device (same device and domain names), RME discards any preexisting device data and polls the device for new data.

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Add Device**.

Step 3 Click **Next**. The Add a Single Device dialog box appears.



Add a Single Device

Add a device to Network Data Collector Inventory. The device will become managed if the device is reached and SNMP data acquired.

Device Name(required)	172.18.89.9
Domain Name	
User Field 1	
User Field 2	
User Field 3	
User Field 4	
Serial Number	

☑ Check Device Attributes

Step 4 Enter the device access, user, and serial number information:

- Device name
- Domain Name
- User fields 1 through 4
- Serial number

Step 5 Select **Check Device Attributes** if RME is installed and you want verify device attribute information after the device is added.

Step 6 Click **Next**. The Enter Login Authentican Information dialog box appears.

Step 7 Enter the login authentication information for Telnet login mode:

- Read-write community strings
- TACACs and local usernames and passwords
- Telnet password

Step 8 Click **Next**. The Enter Enable Authentican Information dialog box appears.

Step 9 Enter the enable authentication information for Telnet enable mode:

- Enable TACACs username and password
- Enable and enable secret passwords

Step 10 Click **Finish**. The Single Device Add dialog box shows that the device has been added to the Pending list. After adding a device, you can click **Add Another** to add another device.

Step 11 Click **View Status** to display the Add/Import Status Summary of the number of devices that are managed, alias, pending, conflicting, suspended, and not responding:

- You can click any of these statuses to view the devices in that state.
- If you selected **Check Device Attributes** and RME is installed, the number of device attribute errors is also shown. Click this field to view details.

Step 12 Click **Update** to display the most recent information.

Modify Device Attributes

Add, change, and delete the following attributes for one or more managed devices:

- SNMP read and write community strings
- Telnet passwords
- TACACS usernames and passwords
- Enable TACACs use names and passwords
- Enable and enable secret passwords
- Local usernames and passwords
- User fields
- Device serial numbers. You must select a single device to change device serial numbers.

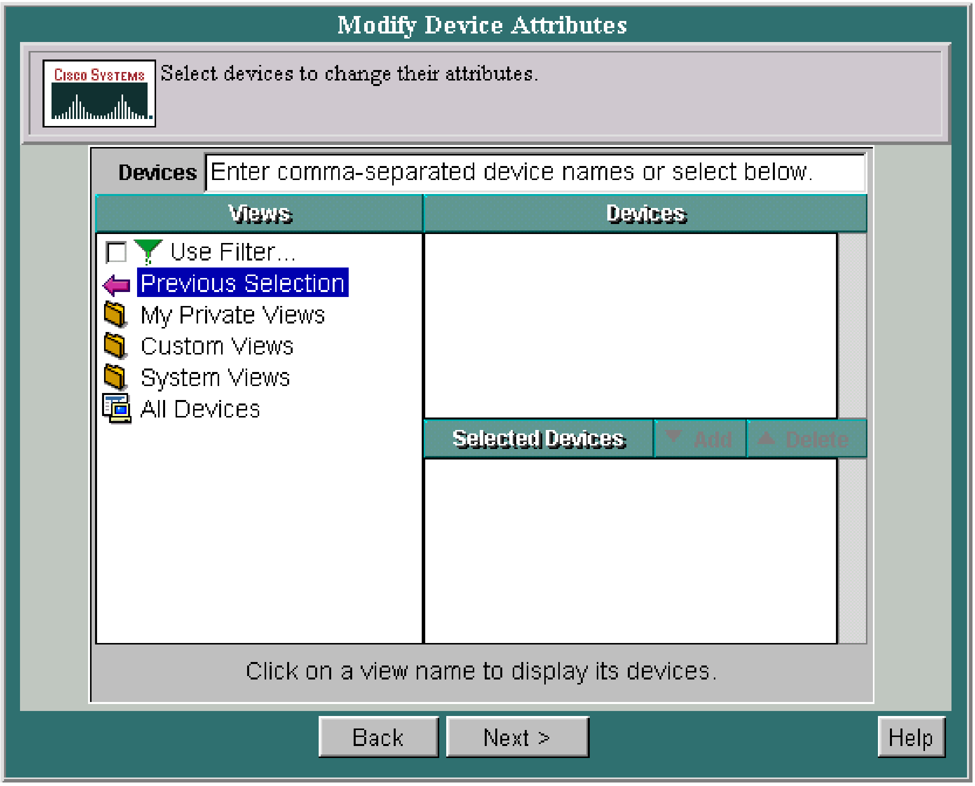
Except for device serial numbers, any changes are applied to all selected devices.

Procedure

Step 1 Select **Network Data Collector > Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Modify Device Attributes**.

Step 3 Click **Next**.The Modify Device Attributes screen appears.



Modify Device Attributes

Select devices to change their attributes.

Devices: Enter comma-separated device names or select below.

Click on a view name to display its devices.

Step 4 Select the devices whose device information you want to edit, then click **Next**. The Change dialog box displays the following options:

- All
- Read-Write Community Strings
- Telnet Login Mode User Names and Passwords
- Telnet Enable Mode User Names and Passwords
- User Fields

- Device Serial Numbers

Select one or more options, then click **Next**. A dialog box appears for each option you select (selecting **All** displays each dialog box). The dialog box fields are blank; they do not display the current information.

Step 5 Edit the dialog box:

- To retain a value, leave the field blank.
- To change a value, enter new information. If you are changing a password, you must also enter the user ID.
- To delete a value, click **Delete** next to the field. The **Delete** checkbox overrides any text entered in the field. If you are deleting a password, you must also enter the username.

Caution Make sure you verify your entries before you click **Next** in any dialog box. If you change device attributes, you *cannot undo* the change, except by reediting.

Step 6 When you finish:

- Click **Next** to apply the changes and go to the next dialog box.
- Click **Finish** to apply the changes and exit the final dialog box.
- Click **Back** to close the dialog box without changing any information.

Update Inventory

Run inventory collection as a one-time event for specific devices. To collect inventory at regular intervals (hourly, daily, or weekly), use the Start/Stop Data Collection procedure. Both procedures update your inventory database and show changes in all associated inventory reports.

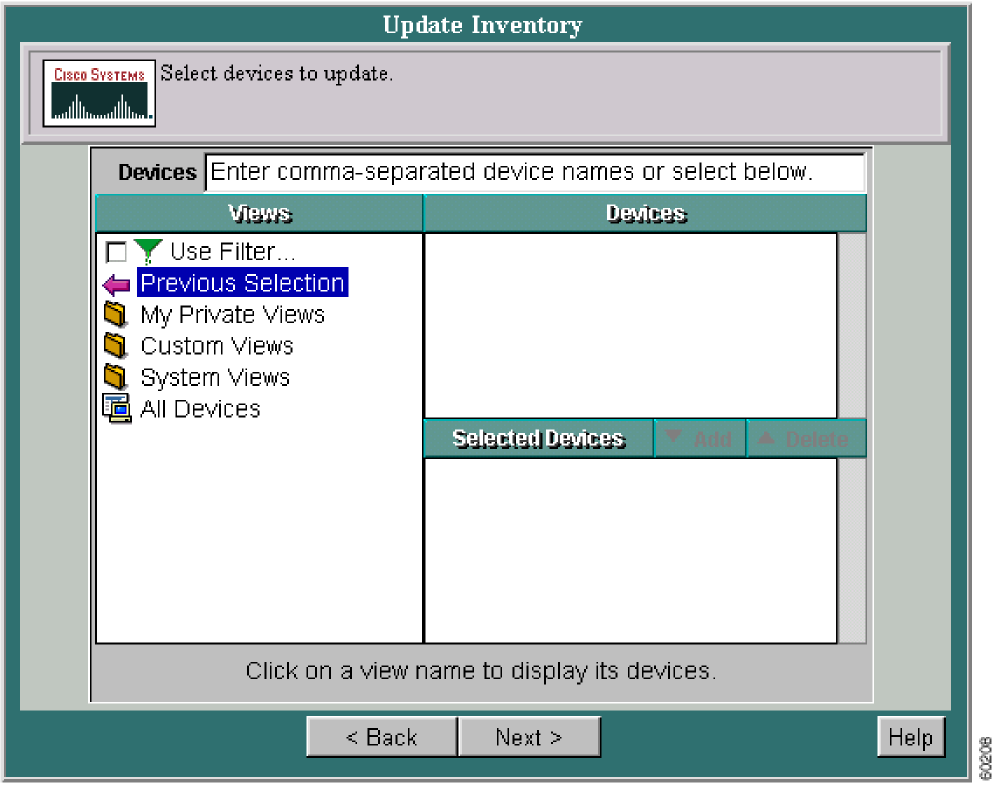
For inventory collection to work, your devices must have accurate read community strings entered.

Procedure

Step 1 Select **Network Data Collector** > **Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **Update Inventory**.

Step 3 Click **Next**. The Update Inventory dialog box appears.



Select devices to update.

Enter comma-separated device names or select below.

Click on a view name to display its devices.

Step 4 Select the devices you want polled for new information, then click **Finish**.

The Update Inventory dialog box displays inventory collection status. The status field shows that the IcServer:

- Is running
- Has processed a device
- Is ready

Step 5 If the IcServer is running, click **Update**. Continue to click **Update** until the IcServer is ready, indicating that inventory collection is complete.

List Managed Devices

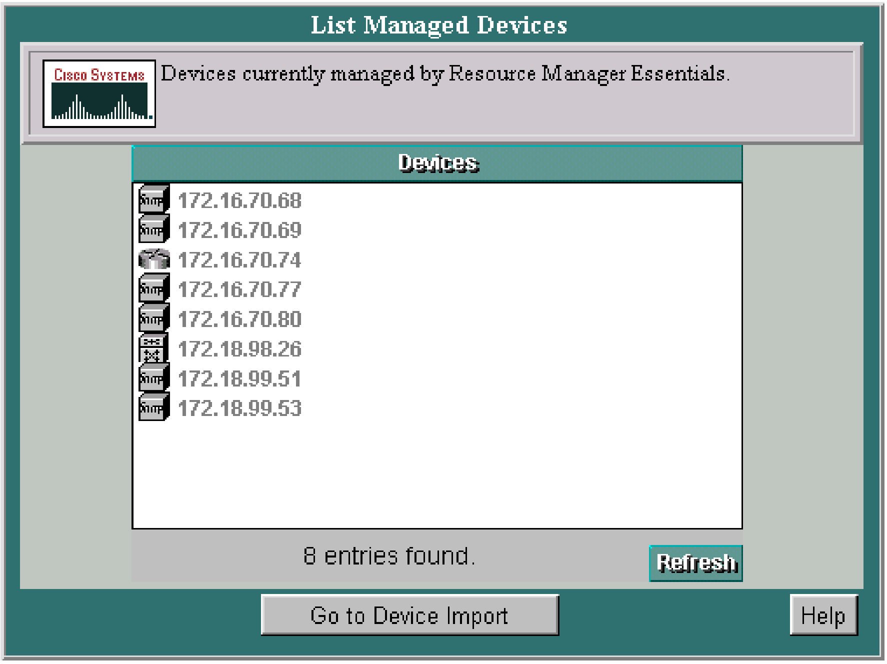
Display a read-only list showing all currently managed devices.

Procedure

Step 1 Select **Network Data Collector > Device Import/Discovery**. The Device Import/Discovery dialog box appears.

Step 2 Click the radio button next to **List Managed Devices**.

Step 3 Click **Next**. The List Managed Devices screen appears.



List Managed Devices

Devices currently managed by Resource Manager Essentials.

Devices

172.16.70.68
172.16.70.69
172.16.70.74
172.16.70.77
172.16.70.80
172.18.98.26
172.18.99.51
172.18.99.53

8 entries found.

60209

Step 4 The List Managed Devices dialog box displays the names of the managed devices.

Step 5 To refresh the list, click **Refresh**.

Step 6 Click **Go to Device Import** to return to the Device Import/Discovery dialog box.

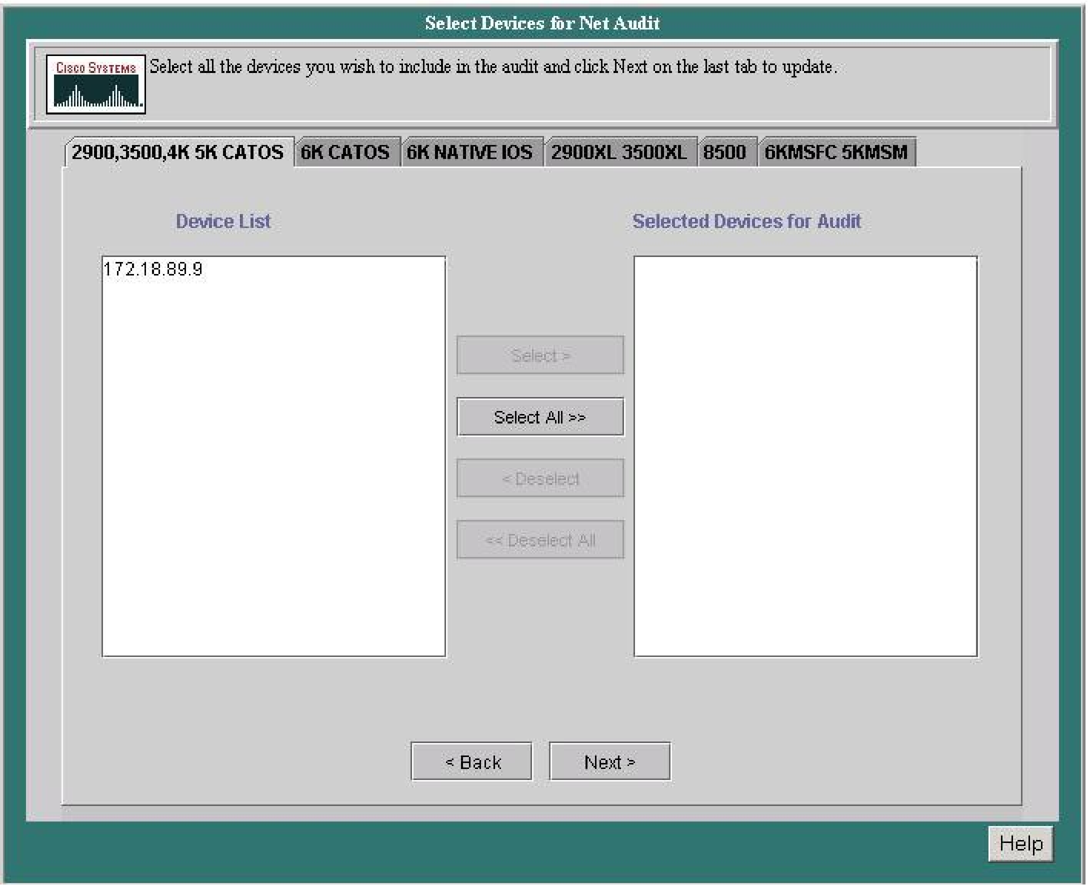
Selecting Devices

All eligible routers and/or switches added or imported in the Device Import & Discovery section will appear in their respective Switch List or Router List screen. Select one or more of each to include in the audit. The devices selected be will tested using the Access Verifier as explained in the Starting/Stopping Telnet Access Verification section. Devices on the Switch List and Router List screens will appear in one of the following two columns:

- Device List: Devices available to be audited, but have not yet been selected to be included in the audit.
- Devices for Audit: Devices that have been selected to be included in the audit.

Procedure

Step 1 Select **Network Data Collector > Device Selection**. The Select Devices for Net Audit dialog box opens with the Router List tab selected (if a Switch is being audited, a Switch List tab will appear instead. If a VoIP audit, both tabs will appear).


Select Devices for Net Audit

Select all the devices you wish to include in the audit and click Next on the last tab to update.

Device List

172.18.89.9

Selected Devices for Audit

Step 2 Highlight the device (or devices) in the Device List window to be included in the audit.

Step 3 Click **Select**. The highlighted router(s) will be moved to the Selected Devices for Audit window (or click on **Select All** to move all devices to the Selected Devices for Audit window).

Step 4 To unselect a device, highlight the device in the Selected Devices for Audit window and click on **Deselect** to return it to the Device List window (or **Deselect All** to return all devices).

Step 5 Click on **Next** to proceed to Access Verification (or the Switch List window if a VoIP audit is being run. Repeat stpes 4 through 6 and click **Next** again to advance to Access Verification).

Access Verification

Access verification tests for access problems before data collection begins. All devices chosen from the Select Devices for Audit page will be tested using the Telnet Access Verifier. Data collection fails if the maximal failure rate is exceeded while collecting data.

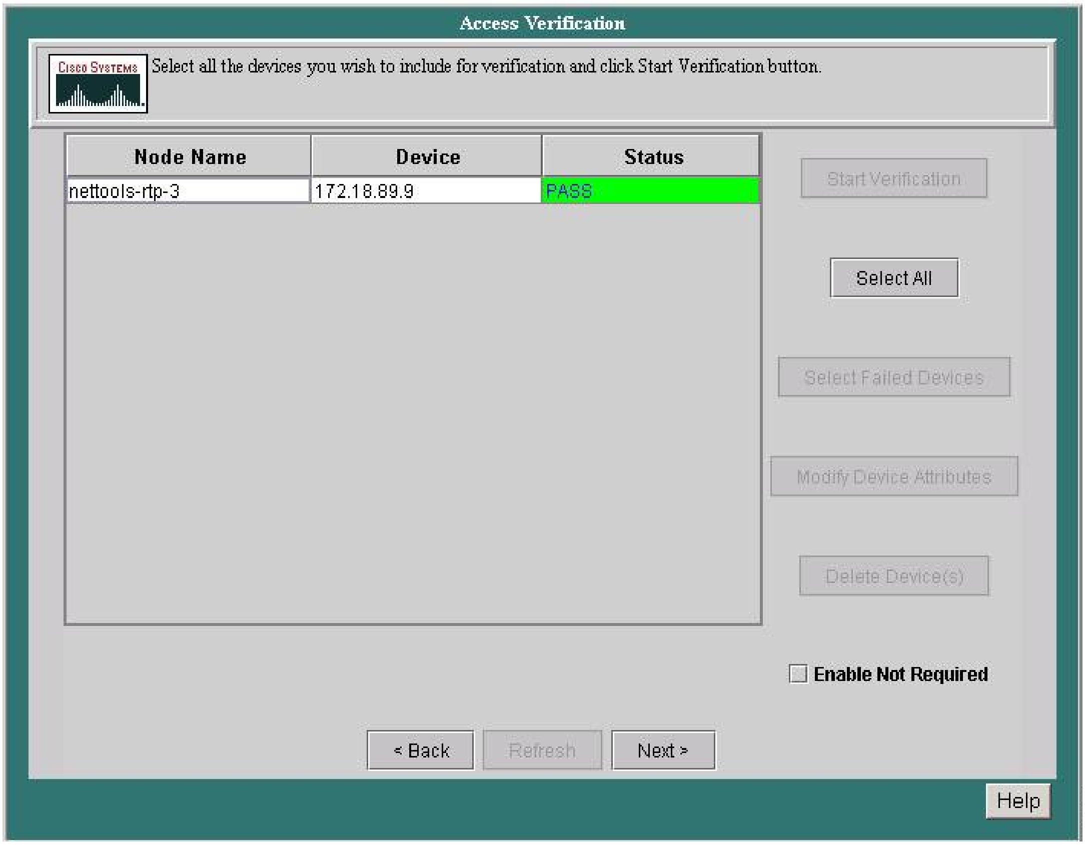
If an error or failure is detected, it must be fixed before the audit can be performed. Depending on the type of error, it may be necessary to return to the Device Import & Discovery page. From this page, use the Modify Device Attributes feature to make the necessary changes. You can add, change, and delete the following attributes for one or more managed devices:

- SNMP read and write community strings
- Telnet passwords
- TACACS usernames and passwords
- Enable TACACs use names and passwords

Note If a device is failing access verification due to a problem in the device (crashes or goes down), then it can be removed from the audit by selecting it and pressing **Delete Device**.

Procedure

Step 1 Select **Network Data Collector > Access Verification**. The Access Verification dialog box appears.



Access Verification

Select all the devices you wish to include for verification and click Start Verification button.

Node Name	Device	Status
nettools-rtp-3	172.18.89.9	PASS

□ Enable Not Required

74134

Step 2 Select the device(s) in the Node Name column to run through the telnet access verification process. Use the **Ctrl** or **Shift** keys to select multiple devices, or click on **Select All** to choose all the devices listed.

Note Click in the Enable Not Required check box (if activated) if you want to make all commands for all devices require no enable passwords.

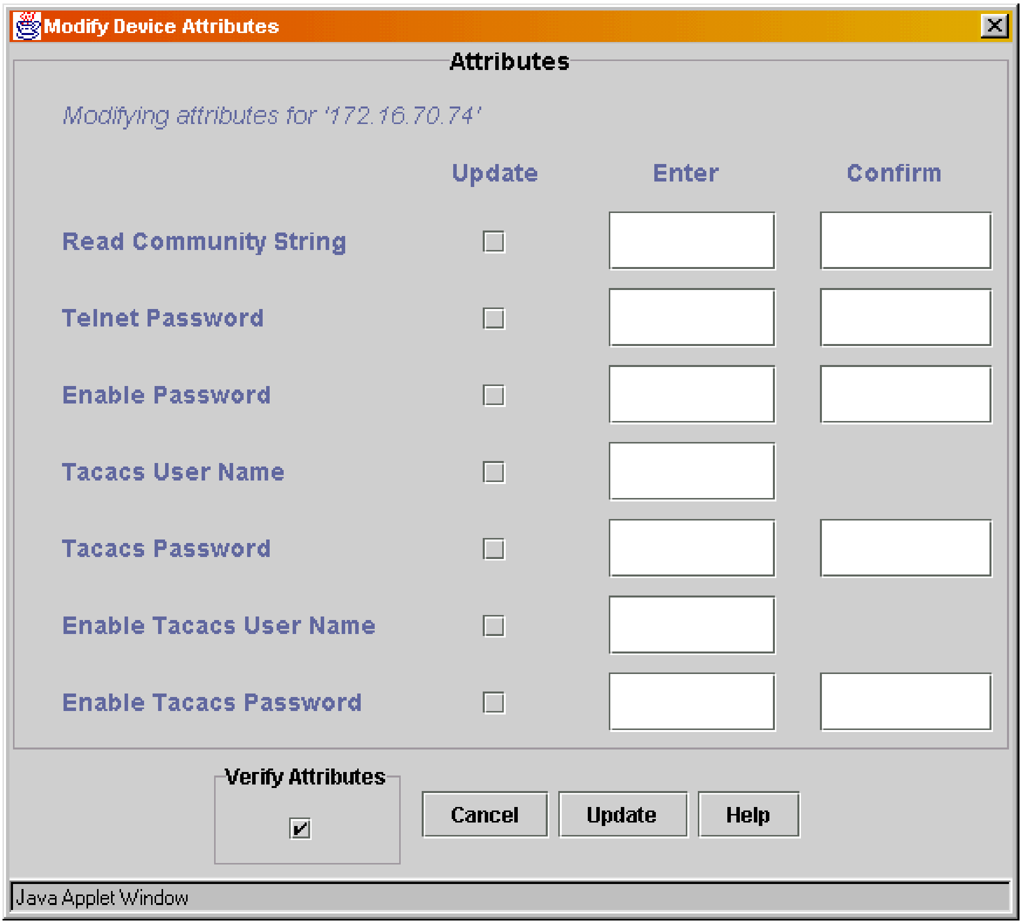
If this option is activated, then some of the commands on one or more devices in the current audit require enable password for successful data collection to take place, i.e., an enable password will have to be entered to complete the data collection. If this option is greyed out, then there are no commands that require enable password. The Enable Not Required tool will allow an audit to take place without the enable password being revealed.

Step 3 Click **Start Verification**. Once the telnet access verification process is complete, the result of the test will appear in the Status column next to each device. If no errors were detected, click **Finished**.

Any errors detected during the telnet access verification process must be fixed before the audit can be completed. Do the following to fix an error, or to simply change the attribute of a particular device:

Step 1 Click **Select Failed Devices** to list all devices that failed. If this button is not lit up, then no errors were detected.

Step 2 Click **Modify Device Attributes**. The Modify Device Attributes dialog box appears.



Modify Device Attributes

Attributes

Modifying attributes for '172.16.70.74'

	Update	Enter	Confirm
Read Community String	□		
Telnet Password	□		
Enable Password	□		
Tacacs User Name	□		
Tacacs Password	□		
Enable Tacacs User Name	□		
Enable Tacacs Password	□		

Verify Attributes ☑

Java Applet Window

Step 3 Make the change in the **Enter** column to the right of the desired topic. Re-enter the change in the **Confirm** column (for verification purposes) if required.

Step 4 Click in the checkbox next to the attribute changed. Only attributes checkmarked will be updated.

Step 5 Click in the **Verify Attributes** checkbox to have the new attributes verified immediately. Leave unchecked if you only wish to update an attribute.

Note To update a null value for an attribute into the database, check the **Verify Attributes** box and do not enter any text.

Step 6 Click **Update** to return to Access Verification. Verification will automatically begin if the **Verify Attributes** checkbox was checked.

Step 7 If the **Verify Attributes** checkbox was not checked (see step 4), highlight the device(s) to re-test in the Node Name column and click **Start Verification**.

Step 8 Click **Finished** once device(s) pass verification.

Note You can also use the Modify Device Attributes tool located in **Device Import/ Discovery**. Select **Network Data Collector > Device Import /Discovery > Modify Device Attributes** and make the appropriate changes.

Selecting Interface/Ports

Note This section is only applicable for a Voice Over IP audit.

The interfaces and ports of all routers and/or switches that passed the telnet access verification test will appear in their respective Router Interface Selection or Switch Port Selection screen. Select one or more of each to add to the device list for data collection. Interfaces/ports on the Router Interface Selection and Switch Port Selection screens will appear in one of two columns. The left column lists all devices that passed the telnet access verification test and are elegible for data collection; the right column shows the devices actually selected for data collection. Both columns are split into the following two fields:

- Device: the device ID of the specific router/switch
- Interface: the type of interface of the specific router/switch

Procedure

Step 1 Select **Network Data Collector > Interface/Ports Selection.** The Router Interface Selection dialog box appears.

Step 2 Highlight the interface (interfaces) in the left column to be included in the audit.

Step 3 Click on **Select**. The highlighted interface(es) will be moved to the right column (or click on **Select All** to move all intefaces to the right column at once).

Note Highlight an interface listed in the right column and click on **Deselect** to return it to the left column, or click on **Deselect All** to return all interfaces to the left column.

Step 4 Click on **Next** to proceed to the Switch Port Selection window.

Step 5 Highlight the port (or ports) in the the left column to be included in the audit.

Step 6 Click on **Select**. The highlighted port(s) will be moved to the right column (or click on **Select All** to move all ports to the right column at once).

Note Highlight a port listed in the right column and click on **Deselect** to return it to the left column, or click on **Deselect All** to return all ports to the left column.

Step 7 Click **Next** to proceed to start or schedule the data collection.

Starting/Scheduling Data Collection

Start the data collection immediately or use the scheduler to set a time within in the next five years to begin data collection. You can stop data collection or change the schedule at any time. When scheduling a data collection, the following parameters can be set:

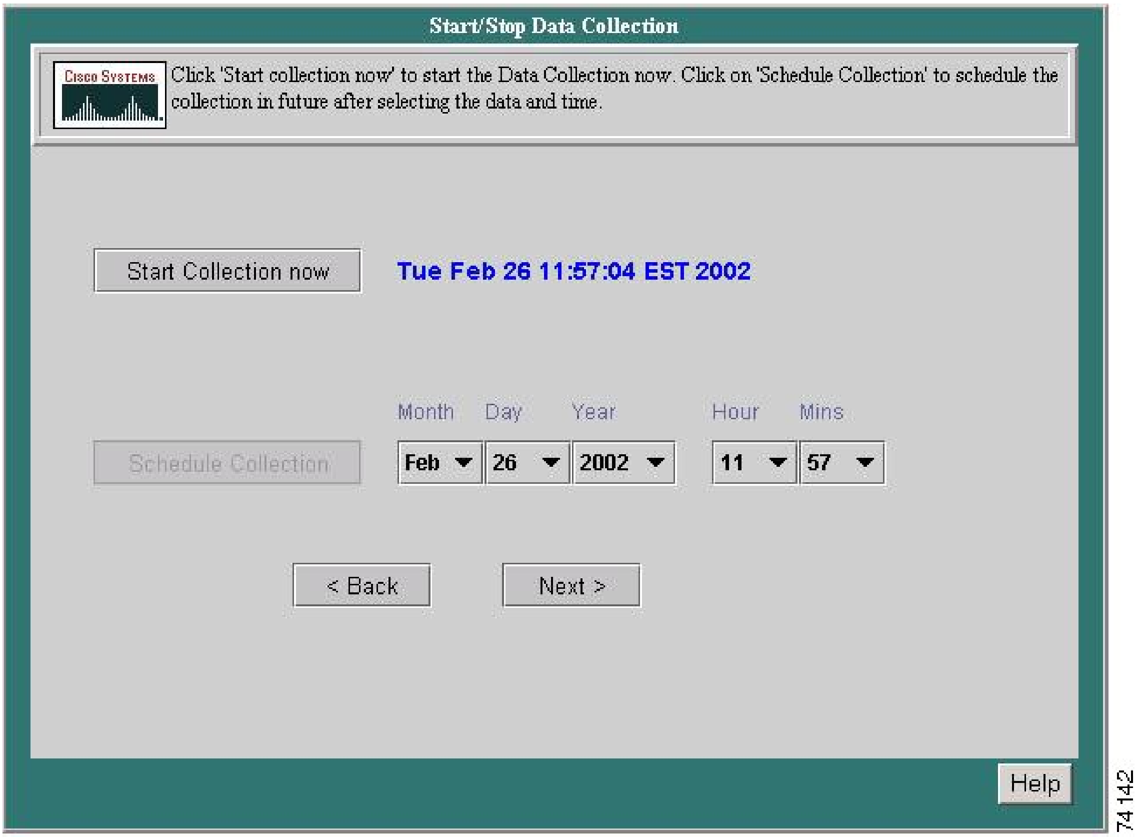
- Month
- Day
- Year
- Hour

- Minute

Procedures

Starting a Data Collection:

Step 1 Select **Network Data Collector** > **Data Collection**. The Start/Stop Data Collection dialog box appears.



Start/Stop Data Collection

Click 'Start collection now' to start the Data Collection now. Click on 'Schedule Collection' to schedule the collection in future after selecting the data and time.

Tue Feb 26 11:57:04 EST 2002

Month: Feb
Day: 26
Year: 2002
Hour: 11
Mins: 57

Step 2 Click **Start Collection**.

Note Once a data collection has started, it can be halted by clicking **Stop Collection**.

Scheduling a Data Collection:

Step 1 Select **Network Data Collector > Data Collection**. The Data Collection dialog box appears.

Step 2 Select **Schedule Collection**.

Step 3 Select the month to begin the data collection from the **Month** pull-down menu.

Step 4 Select the day to begin the data collection from the **Day** pull-down menu.

Step 5 Select the year to begin the data collection from the **Year** pull-down menu.

Step 6 Select the hour to begin the data collection from the **Hour** pull-down menu

Step 7 Select the minute to begin the data collection from the **Minute** pull-down menu.

Note Once **Schedule Collection** has been selected, the Change Schedule option becomes active. Click on it to change any of the previously selected settings.

Step 8 Click **Next**.

Note Once a data collection has started, it can be halted by clicking **Stop Collection**.

Data Collection Status

The Data Collection Status screen allows you to monitor the status of the current data collection process. The information displayed on this page reflects cumulative data for all routers and switches from the beginning of the collection up to the time the Data Collection Status screen was accessed. The Net Audit Success Rate is used to determine the success/failure of the audit. The success rate must be 80% or higher for the audit to pass.

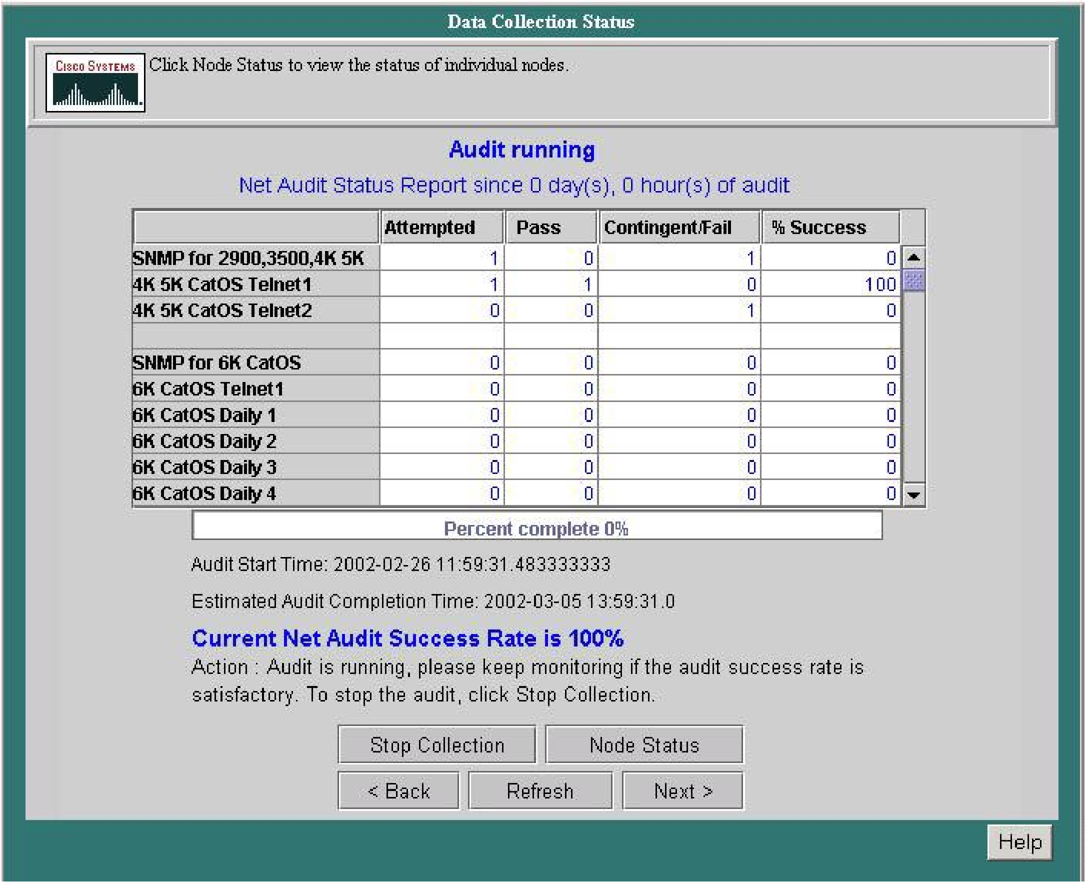
The node status can be in one of three states:

- Passed: Indicates a node that has passed all telnet iterations and achieves 80% or greater SNMP accessibility.
- Failed: Defined as a node that will be excluded from an audit. A node will be excluded if any telnet iterations fails or SNMP percentage can not achieve at least 80% for the seven day polling period.
- Contingent: Defined as a node that is in danger of failing. All telnet iterations have passed, but SNMP accessibility is under 80%. If SNMP reaches 80% or higher by the end of the audit, the node will be upgraded to "Passed".

The **% Success** number indicates the ratio of nodes tested to nodes passed.

Procedures

Step 1 Select **Network Data Collector > Data Collection Status.** The Data Collection Status screen appears.



Click Node Status to view the status of individual nodes.

Audit running

Net Audit Status Report since 0 day(s), 0 hour(s) of audit

	Attempted	Pass	Contingent/Fail	% Success
SNMP for 2900,3500,4K 5K	1	0	1	0
4K 5K CatOS Telnet1	1	1	0	100
4K 5K CatOS Telnet2	0	0	1	0
SNMP for 6K CatOS	0	0	0	0
6K CatOS Telnet1	0	0	0	0
6K CatOS Daily 1	0	0	0	0
6K CatOS Daily 2	0	0	0	0
6K CatOS Daily 3	0	0	0	0
6K CatOS Daily 4	0	0	0	0

Percent complete 0%

Audit Start Time: 2002-02-26 11:59:31.483333333

Estimated Audit Completion Time: 2002-03-05 13:59:31.0

Current Net Audit Success Rate is 100%

Action : Audit is running, please keep monitoring if the audit success rate is satisfactory. To stop the audit, click Stop Collection.

74137

Step 2 Select **Stop Collection** to end the current data collection process if needed.

Step 3 Click **Node Status** to advance to the Node Status screen. A more detailed breakdown of the current data collection process can be viewed there.

Step 4 Click **Next** to advance to Data Packaging.

Note Click **Refresh** to update the information on the Data Collection Status screen.

Node Status Report

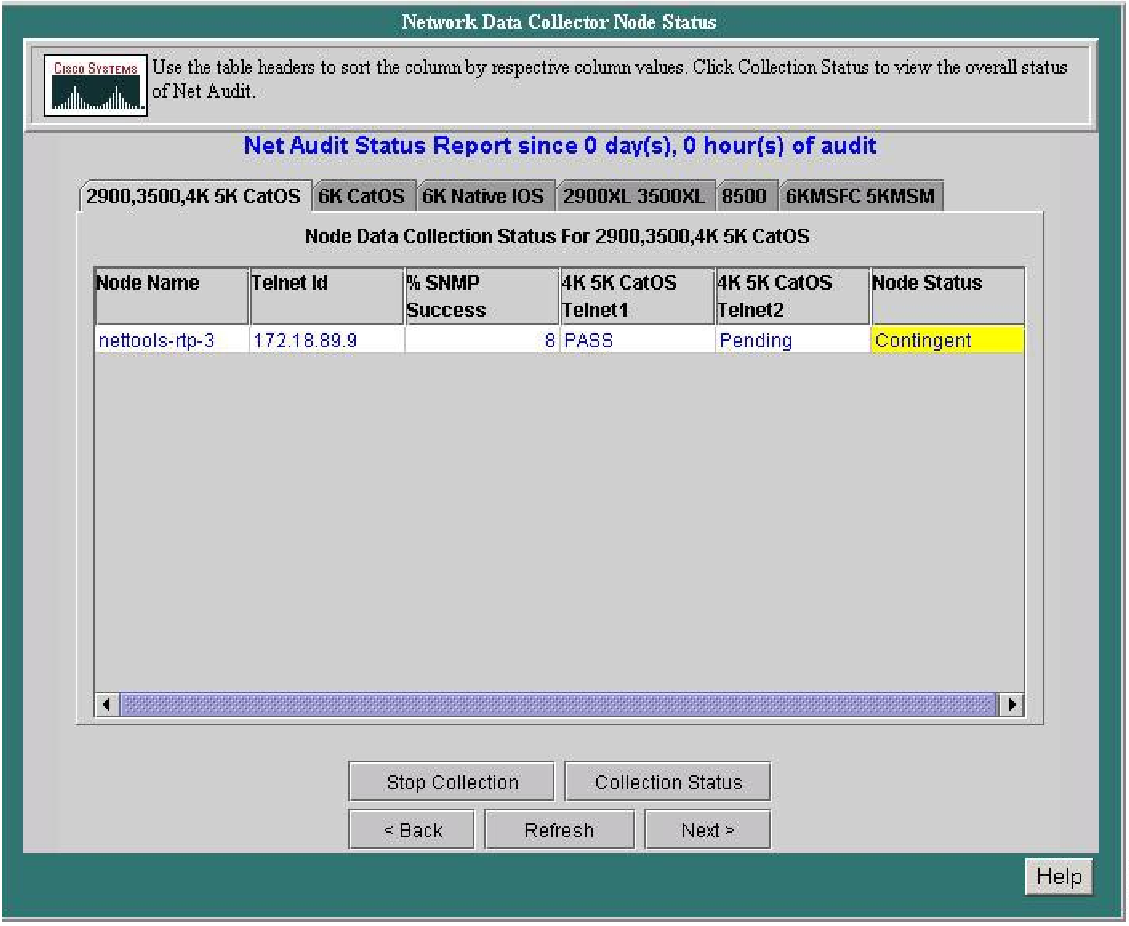
The Node Status Report screen displays a breakdown of the information listed on the Data Collection Status screen. The information displayed on this page reflects data for specific routers and switches from the beginning of the collection up to the time the Data Collection Status screen was accessed. Information for the routers and switches in the current data collection are displayed in separate windows.

If a node is not at an 80% SNMP success and unable to reach 80% or higher by the end of the audit, it will shown as failed without explanation.

Procedures

Step 1 Select **Network Data Collector > Data Collection Status**. The Data Collection Status screen appears .

Step 2 Click **Node Status**. The Network Data Collector Node Status screen appears.



Network Data Collector Node Status

Use the table headers to sort the column by respective column values. Click Collection Status to view the overall status of Net Audit.

Net Audit Status Report since 0 day(s), 0 hour(s) of audit

Node Data Collection Status For 2900,3500,4K 5K CatOS

Node Name	Telnet Id	% SNMP Success	4K 5K CatOS Telnet1	4K 5K CatOS Telnet2	Node Status
nettools-rtp-3	172.18.89.9	8	PASS	Pending	Contingent

Note If a VoIP audit is being run, Router Status and Switch Status tabs will also appear.

Step 3 Click **Collection Status** to return to the Data Collection Status screen (or **Stop Collection** to end the current collection process).

Note Click **Refresh** to updated the information on the Node Status report.

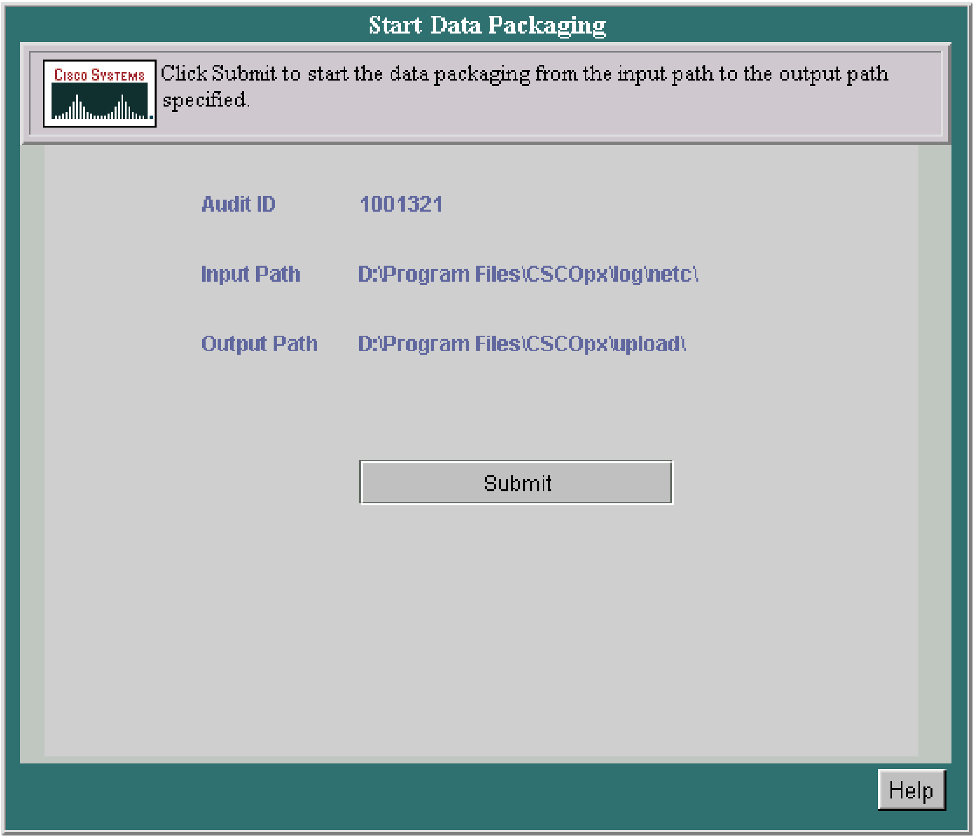
Data Packaging

The output path is automatically set to the location on your local computer where the compressed and packaged files created during the data upload are to be stored. These files can then be sent via an encrypted link back to a location at Cisco.

Data packaging can be performed before, during or after an audit. If started prior to an audit (so just to keep packaged data), all files and sub directories will be packaged. During an audit, data packaging can be performed even if iteration fails or the poller crashes.The audit must be running to do this, however.

Procedure

Step 1 Select **Network Data Collector** > **Data Packaging.** The Start Data Packaging dialog box appears.



Start Data Packaging

Click Submit to start the data packaging from the input path to the output path specified.

Audit ID 1001321

Input Path D:\Program Files\CSCOpx\log\netc\

Output Path D:\Program Files\CSCOpx\upload\

Step 2 Verify all settings and click **Submit**.

Sending Files to CCO

Once the compressed and packaged files are stored on your local computer, you'll need to upload them to a CCO server. To upload the files to CCO, do the following:

Step 1 Open an anonymous FTP session to nettools-upload.cisco.com.

Step 2 Change directory to /incoming/netcollector.

Step 3 Set transfer mode to binary.

Step 4 Select the compressed and packaged file from where it is stored on the local computer (Network Data Collector server).

Step 5 Initiate the FTP (put the files onto CCO).

Step 6 Close the connection after FTP is done.

The above upload procedure can also be performed using the following commandline format:

```
C:\>ftp nettools-upload.cisco.com
ftp>username: anonymous
ftp>password: <email_id>@domainname.com

ftp>cd /incoming/netcollector
ftp>bin
ftp>lcd c:\progra~1\cscopx\upload
ftp>put A1000.out
ftp>bye
C:\>
```

FTP Upload

FTP Upload allows you to upload the collected data to Cisco. The data will be uploaded from *<NETCHOME>/upload to Cisco*.

Before performing this step, however, you should package the data using the **Network Data Collector --> Data Packaging** tool.

If you need to configure the FTP with proxy details, go to **Network Data Collector -> Advanced Settings -> Audit Details --> FTP Settings** to make any changes.

Procedures

Step 1 Select **Network Data Collector > Start FTP Upload**. The FTP Upload dialog box appears.

Step 2 Click **Start Upload** to immediately start uploading the collected data to Cisco.

Note Once the FTP process has started, it can be halted by clicking Stop Upload.

Advanced Settings Folder

Network Data Collector also comes with an Advanced Settings folder, which contains a collection of useful links from RME and CiscoWorks 2000 utilities. The folder contains the following sub-folders:

- Discovery
- Inventory
- Audit Details
- Process Management
- Administration
- Troubleshooting

The following table shows the tools found in the above sub-folders.

Discovery	Inventory	Adudit Details	Process Management	Administration
• Exclude Filters • Include Filters • Community • Advanced Discovery Settings • Start or Stop Discovery • Discovery Status • View Discovered Devices.	• Reports folder • List All Devices • List Managed Devices • Delete Devices • Delete Device Status • Export to File • Update Inventory	• Sample SeedFile • Show Commands List • Show MIBs List • Supported Devices List • Manual Device Classification • FTP Settings	• Start Process • Stop Process • Process Status • Process Failures	• Permissions Report • Who is Logged On • Modify My Profile • Add Users • Modify/Delete Users • Log File Status • Package Options

Trouble-shooting
• Traceroute • Ping • NSLookup • Management Station to Device • Collect Server Info • Self Test

Click the **Help** button while in any of the above tools to learn more about that tool and how to use it.

Exporting Device Information to a File

You can export your device and device access information to an output file in a predefined directory in either comma separated values (CSV) or data integration file (DIF) format. This file lets you view information before importing it into your own spreadsheet or database. You can also change the information from within the file, then import the data to Network Data Collector in either file format.

Procedure

Step 1 Select **Network Data Collector > Advanced Settings > Inventory > Export to File**. The Export to File dialog box appears.

Step 2 Enter the full pathname of the file to which you want to write the data.

Caution For security reasons, the file will be saved to $PX_DATADIR/inventory.

Step 3 Select the output version (version 1.0 or version 2.0).

Note If a field is empty, null, or not in the database, it will be stored as follows:

- In a version 1.0 file, the field is stored as empty
- In a version 2.0 file, the field is stored as !{[NOVALUE]}!

Step 4 Click **Next**. A confirmation message appears. If the file already exists, you will be asked to confirm overwriting the file.