Cisco Virtual Network Data Server Readme

For Cisco Network Planning Solution 2.1 and
Cisco Network Planning Solution–Service Provider 2.1

Release 2.1

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

Customer Order Number:
Text Part Number: OL-14537-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Virtual Network Data Server *Readme*
Copyright © 2007 Cisco Systems, Inc. All rights reserved.

Cisco Virtual Network Data Server 2.1 Readme

This document summarizes the differences between Cisco Virtual Network Data Server (Cisco Virtual Network Data Server) Release 2.1 and Release 2.0.1. Release 2.1 is a full release that replaces existing 2.0 installations. If you are updating to Release 2.1, you should review this document.

Contents

Release 2.1 Description 1

Installing Cisco Virtual Network Data Server 2.1 2

Cisco Virtual Network Data Server 2.1 Release Notes 3

Updating Cisco Virtual Network Data Server 3

License File Format Change 4

Embedded Data Storage Server 5

New Features and Enhancements 6

Device Info File 28

Schedules 28

Importing into Cisco Analysis Software 28

Restrictions and Limitations 29

Documentation Addendum 39

Device and Platform Info Auto Discovery 39

Alcatel 5620 SAM-O Network Import 64

Publishing to Secure Cisco Report Server 75

Format of Device Info File 77

Resolved Problems 79

Known Issues 81

Release 2.1 Description

Release 2.1 provides enhancements to the existing capabilities of Cisco Virtual Network Data Server. It also implements suggestions and fixes to software problems reported in earlier releases.The following sections highlight the changes to Cisco Virtual Network Data Server that were introduced in Release 2.1.

Installing Cisco Virtual Network Data Server 2.1

For detailed instructions on how to install the Release 2.1 software, refer to the instructions in the *Installation Guide for Cisco Virtual Network Data Server.* You can view an online version of this document at Cisco.com:

http://www.cisco.com/en/US/products/ps6363/prod_installation_guides_list.html

WARNING—If you are using Release 1.1 software or earlier, you must update to Release 2.0 before you update to Release 2.1. For details on updating from Release 1.1, see the *Installation Guide for Cisco Virtual Network Data Server* for Release 2.0 at the above URL.

Note—A software patch is available to correct the following problems in Release 2.1 of Cisco Virtual Network Data Server.

Model import from Cisco Virtual Network Data Server into Design and Analysis is slow: Depending on the size and composition of a network, importing a network model from Cisco Virtual Network Data Server into Design and Analysis may take longer than it did in the previous release.

Cisco Virtual Network Data Server services shutdown on database multikey error: Cisco Virtual Network Data Server installations that use the Ascii Generic Data Import adapter may experience service shutdown problems when you import XML data files. When this happens, the Cisco Virtual Network Data Server services are stopped and the Event Viewer shows emergency messages and the following error message: “ERROR: updating existing nwk_multikey...” This problem occurs when the device sysNames in the Ascii data files do not use the same case as the names in the network model.

If you encounter either of these problems when using the software, contact the Cisco Technical Assistance Center to obtain the software patch.

Cisco Virtual Network Data Server 2.1 Release Notes

Cisco Virtual Network Data Server 2.1 is a software update to the 2.0.2 release. This release contains new features and enhancements to existing capabilities. This release also implements suggestions and fixes many software problems reported in earlier releases.

These release notes cover the following topics:

- Updating Cisco Virtual Network Data Server on page 3
- License File Format Change on page 4
- Embedded Data Storage Server on page 5
- New Features and Enhancements on page 6
- Device Info File on page 28
- Schedules on page 28
- Importing into Cisco Analysis Software on page 28
- Restrictions and Limitations on page 29
- Documentation Addendum on page 39
- Format of Device Info File on page 77

Updating Cisco Virtual Network Data Server

The contents of the Cisco Virtual Network Data Server database cannot be retained during a software update. This means that you must recreate the network database after you successfully update the software. Certain data can be exported from the database to text files prior to the software update and then imported after the software update is complete. The specific data that can be exported include: Device and Platform Info, interface utilization data, and group information.

WARNING—The network topology and configuration data in the Cisco Virtual Network Data Server database cannot be retained during a software upgrade. You must recreate the network topology and configuration after you upgrade.

The Cisco Virtual Network Data Server 2.1 installer offers to migrate product configuration if it detects a supported release.
Cisco Virtual Network Data Server 2.1 supports migration of product configuration from the following software releases:

- Cisco Virtual Network Data Server 2.0.1
- Cisco Virtual Network Data Server 2.0.2

See Migration of Product Configuration on page 31 for known issues relating to migration.

Note—If you currently have 2.0 installed and you want to migrate product configuration when you update to 2.1 you must apply the 2.0.1 patch before you install 2.1.

License File Format Change

Cisco Virtual Network Data Server 2.1 includes the Cisco 2.1 license server. The format of the license file has been changed to hold additional information about each license. This change has the following effects:

- The 2.1 license server automatically converts pre-2.1 license files to the new format when it reads them. A 2.1 license server can serve licenses to any release of Cisco software.
- After a pre-2.1 license file has been converted, pre-2.1 license servers cannot use it and should be replaced with 2.1 license servers.

If you need to run a mix of 2.1 and pre-2.1 applications, install a 2.1 license server (using the “Floating—serve licenses from this computer” option) and configure the applications to contact it.

Embedded Data Storage Server

As of the Cisco Virtual Network Data Server 2.0.2 release, Cisco Virtual Network Data Server software includes a Data Storage Server (PostgreSQL).

This section provides top-level information on the following topics:

- Initial Installation on page 5
- Software Update on page 6

Note—If you are updating Cisco Virtual Network Data Server software and you want to continue to use an existing Oracle installation for Cisco Virtual Network Data Server data storage, you may do so. Note, however that Cisco Virtual Network Data Server requires a dedicated Oracle database installation and dedicated database instance that is not shared with other applications. Use Cisco Virtual Network Data Server's embedded Data Storage Server if your Oracle installation does not meet these requirements.

Initial Installation

When you install Cisco Virtual Network Data Server 2.0.2 or later on a host for the first time, PostgreSQL 8.2.3 is installed and the Cisco Virtual Network Data Server software is configured to use it. The installer creates a local operating system user account (named *dssowner*) on the Cisco Virtual Network Data Server host. The *dssowner* account owns the Data Storage Server service.

WARNING—Do not delete the *dssowner* account. This account is required in order to run Cisco Virtual Network Data Server's Data Storage Server.

In addition, the installer creates two PostgreSQL accounts:

- *dssadmin*—The Administrator user for PostgreSQL
- *dssuser*—The account that Cisco Virtual Network Data Server uses to access PostgreSQL

Software Update

This section discusses the actions the installer takes with respect to the Data Storage Server during a software update:

- If you update from Cisco Virtual Network Data Server 2.0.1, the installer installs the Data Storage Server and configures it for use by Cisco Virtual Network Data Server 2.1.
- If you update from Cisco Virtual Network Data Server 2.0.2, the Data Storage Server should already be installed on the host. The installer checks for the existence of a Cisco Virtual Network Data Server Data Storage Server installation. If the installer does not detect an Cisco-installed version of PostgreSQL 8.2.3, it is installed with the Cisco Virtual Network Data Server software.

WARNING—Data stored in the database is deleted when the database (PostgreSQL or Oracle) is configured for the new version of Cisco Virtual Network Data Server. Review Updating Cisco Virtual Network Data Server on page 3 for important information regarding software upgrades.

New Features and Enhancements

New features and enhancements in this release include:

- Integration of Management Console into the Web Console on page 7
- Group-Based Network Browser on page 8
- Enhancements to Device and Platform Info Auto Configuration Adapter on page 8
- Enhanced Vendor Support on page 13
- Enhancements to Device IP Route Import Adapter on page 13
- Enhanced Messaging for Invalid CLI Data Files on page 18
- Validation Reports on page 20
- Link and Connection Inference Troubleshooting on page 26
- Enhancements to Notification on page 26
- New and Renamed Adapters on page 27

Integration of Management Console into the Web Console

The most significant changes to the Cisco Virtual Network Data Server User Interface are the integration of Cisco Virtual Network Data Server Management Console functions into the Web Console and removal of the Management Console window.

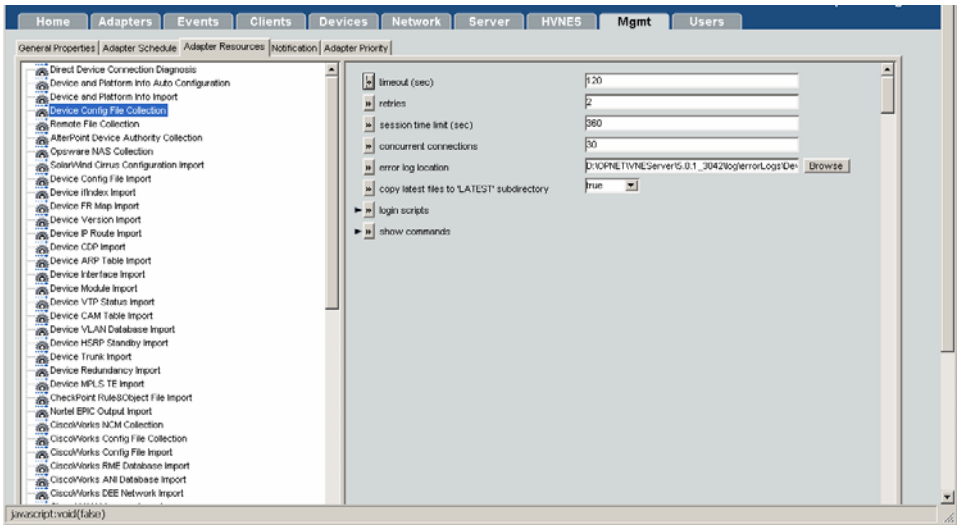
The administrative functions that were previously performed using the Management Console are now performed using the Cisco Virtual Network Data Server Web Console. This restricts Cisco Virtual Network Data Server administrative functions to users that have Cisco Virtual Network Data Server user accounts with administrative privileges.

The Web Console Management (Mgmt) page (Figure 1) contains tabbed panels that correspond to the tabbed panels that were included in the Management Console in previous releases of Cisco Virtual Network Data Server:

- General Properties—Contains the properties formerly contained in the Project Properties, Merge Rules, Device Info File, and Database Properties tabs of the Management Console.
- Adapter Schedule
- Adapter Resources
- Notification
- Adapter Priority

Note—The **Mgmt** page displays in the Web Console only when the user account has administrative privileges for Cisco Virtual Network Data Server.

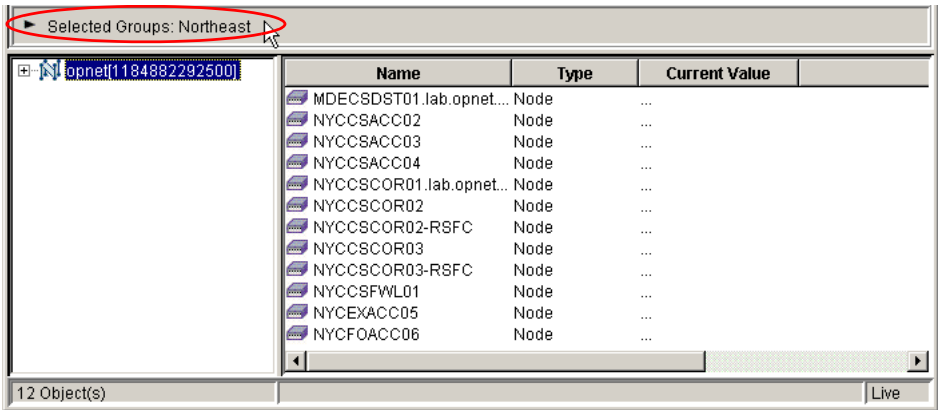
Figure 1 Web Console Management (Mgmt) Page



Group-Based Network Browser

In this release, you can use the Network Browser to examine nodes by group as shown in Figure 2.

Figure 2 Viewing Specified Groups in Network Browser



By default, all nodes contained in the project are displayed in the Network Browser. Use Procedure 1 to configure the Network Browser to display only the nodes that are members of the selected groups.

Procedure 1 Examine Nodes by Group

1. Open the Group Selection Panel at the top of the Network Browser, as shown in Figure 3.

   Figure 3 Open Group Selection Panel

2. Move the groups you want to view in the Network Browser from the Available Groups list to the Selected Groups list.

3. Click the Update button.

4. Close the Group Selection Panel.

End of Procedure 1

Enhancements to Device and Platform Info Auto Configuration Adapter

The Device and Platform Info Auto Configuration adapter has been enhanced to provide faster, more accurate results. It also provides additional information about its actions and results in the adapter statistics and reports.

The Device and Platform Info Auto Configuration adapter assists the user by determining the Login Script and Vendor Type and setting the appropriate values in Device and Platform Info. Login Script and Vendor Type are required if you want to collect CLI data directly from devices using the Device Config File Collection adapter.

Certain fields must be provided in the device entry before running the Device and Platform Info Auto Configuration adapter:

- Device Name
- Access Address
- Username
- Password and/or Privileged Password
- Access Method—Can be determined by the Direct Device Connection Diagnosis adapter.
- Community String (and other fields if using SNMPv3)

The Device and Platform Info Auto Configuration adapter can then determine the appropriate Login Script and Vendor Type that should be used for each of the devices it is configured to examine. (By default the adapter examines only the devices that are Active in the Device and Platform Info.)

The Device and Platform Info Auto Configuration adapter has been enhanced in the following areas:

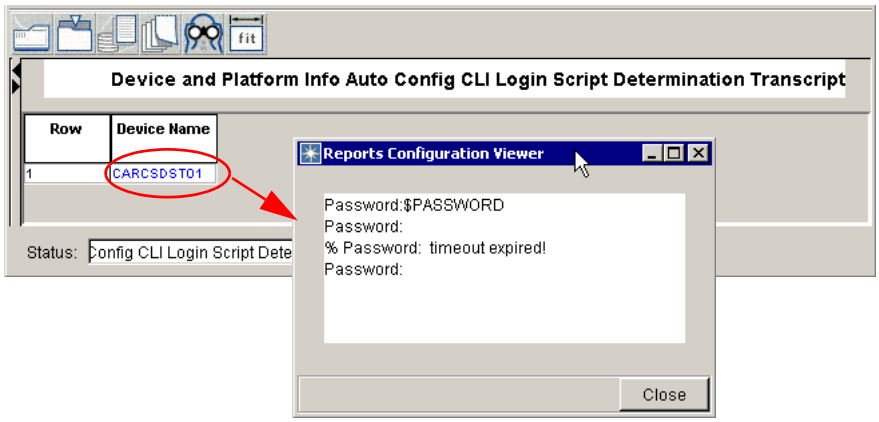
- Login Script Determination on page 9
- Vendor Type Determination on page 10
- New Reports on page 11

Login Script Determination

The Device and Platform Info Auto Configuration adapter can generate a transcript of the commands sent to the device and the device responses when the adapter is determining the appropriate Login Script for the device. By default, the adapter will generate a transcript only in the event of failure. You can optionally configure the adapter to generate transcripts for both successful and failed logins.

The Device and Platform Info Auto Config CLI Login Script Determination Transcript report provides access to the login transcripts that the adapter generates. See Figure 4 for an example of the Device and Platform Info Auto Config CLI Login Script Determination Transcript report.

Figure 4 Device and Platform Info Auto Config CLI Login Script Determination Transcript Report



Click on the name of a file (shown in blue text in the “Device Name” column) to open and examine the login transcript in a file viewer. The transcript in Figure 4 provides an example of a login that failed due to incorrect password.

Note—In the transcripts, $PASSWORD and $ENABLE_PASSWORD are symbolic values that refer to the password and privileged password, respectively, from the device entry in the Device and Platform Info.

Note—Using the default adapter settings, the Device and Platform Info Auto Config CLI Login Script Determination Transcript report will only have entries for devices for which the CLI login was unsuccessful and for which the Login Script could not be determined. When Login Script determination succeeds for all devices, this report is empty.

Vendor Type Determination

In release 2.1, the Device and Platform Info Auto Configuration adapter can assist in determining the Vendor Type using the following methods:

- SNMP
- CLI

In the default configuration, the adapter first attempts to determine Vendor Type by contacting the device via SNMP and obtaining the specific MIB objects. If the adapter fails to connect or determine Vendor Type using SNMP, it attempts to connect to the device via CLI. The CLI method is not attempted unless the SNMP method fails. SNMP vendor determination is preferred since it is more categorical than the CLI method.

Note—If none of the devices in your network are reachable via SNMP, you can disable vendor determination via SNMP to minimize the adapter runtime.

When the adapter attempts to determine a device's Vendor Type using CLI, it can generate a transcript of the commands sent to the device and the device responses. By default, transcripts of the CLI commands and device responses are created only when vendor determination using the CLI method fails. You can optionally configure the adapter to generate transcripts for both successful and failed CLI vendor determination.

The Device and Platform Info Auto Config CLI Vendor Determination Transcript report provides access to the vendor determination transcripts that the adapter generates.

Note—Using the default settings, the Device and Platform Info Auto Config CLI Vendor Determination Transcript report will only have entries for devices for which Vendor Type determination: a.) failed via SNMP, and b.) failed via CLI. When Vendor Type determination succeeds for all devices—either via SNMP or CLI—this report is empty.

New Reports

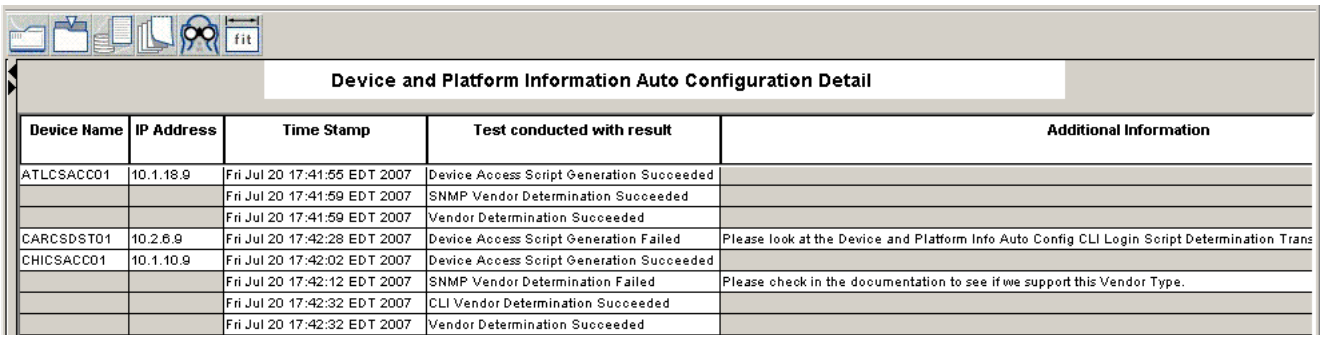
The following reports provide summary-level and detailed information about the Device and Platform Info Auto Configuration adapter actions and results:

- Device and Platform Info Auto Config CLI Login Script Determination Transcript—Provides access to transcripts of the CLI commands and device responses obtained when the adapter attempts to determine Login Script. By default, the adapter is configured to generate transcripts for failed sessions. If you want transcripts of the successes as well as failures, enable the Generate Successful Login Script Transcripts attribute for this adapter. See Login Script Determination on page 9 for additional information on Login Transcripts and an example report.
- Device and Platform Info Auto Config CLI Vendor Determination Transcript—Provides access to transcripts of the CLI commands and device responses obtained when the adapter attempts to determine the Vendor Type using CLI. By default, the adapter is configured to generate transcripts

for failed sessions. If you want transcripts of the successes as well as failures, enable the Generate Successful Vendor Type Transcripts attribute for this adapter. See Vendor Type Determination on page 10 for additional information on Vendor Type determination.

- Device and Platform Info Auto Configuration Detail—Provides a summary of the adapter actions and results for all devices examined. This report includes results (both successes and failures) for all attempts the adapter makes to determine Login Script and Vendor Type for the devices examined. See Figure 5 for an example report.
- Device and Platform Info Auto Configuration Error—The format of this report is similar to the Device and Platform Info Auto Configuration Detail report, however this report lists only the devices for which Login Script and/or Vendor Type could not be determined. See Figure 6 for an example report.

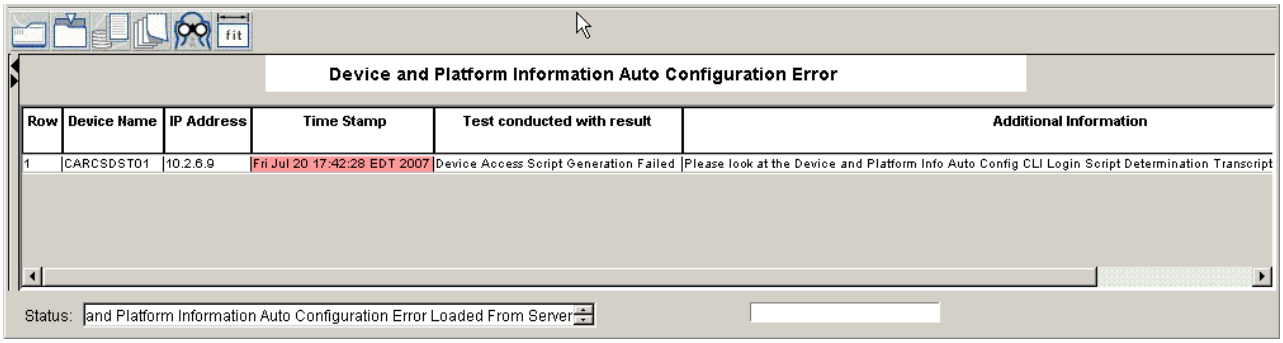
Figure 5 Device and Platform Info Auto Configuration Detail Report



Device and Platform Information Auto Configuration Detail

Device Name	IP Address	Time Stamp	Test conducted with result	Additional Information
ATLCSACC01	10.1.18.9	Fri Jul 20 17:41:55 EDT 2007	Device Access Script Generation Succeeded	
		Fri Jul 20 17:41:59 EDT 2007	SNMP Vendor Determination Succeeded	
		Fri Jul 20 17:41:59 EDT 2007	Vendor Determination Succeeded	
CARCSDST01	10.2.6.9	Fri Jul 20 17:42:28 EDT 2007	Device Access Script Generation Failed	Please look at the Device and Platform Info Auto Config CLI Login Script Determination Trans
CHICSACC01	10.1.10.9	Fri Jul 20 17:42:02 EDT 2007	Device Access Script Generation Succeeded	
		Fri Jul 20 17:42:12 EDT 2007	SNMP Vendor Determination Failed	Please check in the documentation to see if we support this Vendor Type.
		Fri Jul 20 17:42:32 EDT 2007	CLI Vendor Determination Succeeded	
		Fri Jul 20 17:42:32 EDT 2007	Vendor Determination Succeeded	

Figure 6 Device and Platform Info Auto Configuration Error Report



Device and Platform Information Auto Configuration Error

Row	Device Name	IP Address	Time Stamp	Test conducted with result	Additional Information
1	CARCSDST01	10.2.6.9	Fri Jul 20 17:42:28 EDT 2007	Device Access Script Generation Failed	Please look at the Device and Platform Info Auto Config CLI Login Script Determination Transcript

Status: and Platform Information Auto Configuration Error Loaded From Server

Enhanced Vendor Support

This release provides new or enhanced support for the following Vendor Types:

- Cisco Systems (IOS XR)
  - IOS XR-based devices
- Juniper Netscreen
  - ScreenOS-based devices

In addition, this release adds support for the collection and import of IP Route information for the following Vendor Types:

- CiscoPIX
- Nortel Contivity
- Nortel Networks
- Nortel Networks (Passport 8000)
- CheckPointNokia

Note—The collection of IP Route (by the Device Config File Collection adapter) is disabled by default for performance reasons unless the IP Route information is required in order to correctly represent the device configuration for that Vendor Type. See Enabling and Configuring Collection of IP Route on page 14 for instructions on how to enable and configure collection of IP Route.

For related information, see Enhancements to Device IP Route Import Adapter on page 13.

Enhancements to Device IP Route Import Adapter

The Device IP Route Import adapter has been enhanced to import the IP Routing tables for new Vendor Types that have been added to the Device Config File Collection adapter in this release and for Vendor Types that have been enhanced to include IP Route support.

This adapter has also been enhanced to import protocol-specific and vrf-specific versions of IP Routing tables collected from Cisco Systems (IOS), Juniper (JUNOS), Juniper ERX (JUNOSe), and Foundry Networks. The Device IP Route Import adapter can import the output of a protocol-specific or vrf-specific ip route command as along as it conforms to a supported format for the Vendor Type.

The following table lists the supported command output.

Table 1 Device IP Route Import—Enhanced Support

Vendor Type	Supported Command Output
Cisco Systems	show ip route show ip route <protocol> show ip route bgp {param} show ip route vrf <vrf> show ip route vrf <vrf> <protocol> {param} where <protocol> is: (bgp|dhcp|egp|eigrp|igrp|isis|mobile|odr|ospf|rip|vrf|connected|static)
Juniper	show route show route protocol (bgp|direct|esis|isis|ldp|local|ospf|rip|rsvp|static) Note: vrf information (such as green.inet.0) is parsed from the output
Juniper ERX	show ip route show ip route <protocol> where <protocol> is: (access|access-internal|bgp|bgp-internal|dvmrp|isis|ldp|local|mbgp|ospf|other|rip|rsvp|static|static-rpf)
Foundry Networks	show (ip route|vrf) Note: the vrf name is not parsed from the output

If you want to collect and import protocol-specific or vrf-specific IP Route information you must:

- Enable collection of IP Route for the appropriate Vendor Type in the Device Config File Collection adapter resources and configure it to send the desired show command(s). See Enabling and Configuring Collection of IP Route on page 14.
- Add the Device IP Route Import adapter to your schedule. See Adding IP Route to Existing Event-Based Schedule on page 15.

Enabling and Configuring Collection of IP Route

Procedure 2 provides instructions for configuring the Device Config File Collection adapter for collection of IP Route.

Procedure 2 Configure Collection of IP Route

1. Open the Mgmt page of the Web Console.
2. Select the Adapter Resources tab.
3. Expand Device Config File Collection > IP Route.

4 Expand the Vendor Type that you want to modify.

5 Check the active checkbox, if it is not already checked.

6 Expand show ip route.

7 Type the name of the command(s) you want the Device Config File Collection adapter to send into the send command text field.

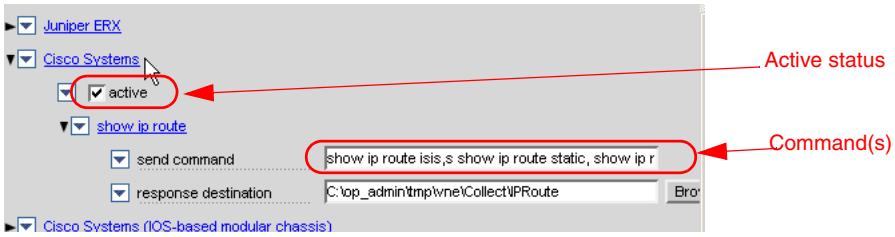
Note—You can enter multiple commands. Separate commands using a comma.

8 Click the OK button at the bottom of the Mgmt page to save your changes.

End of Procedure 2

Figure 7 shows an example of the Cisco Systems vendor type configured to collect show ip route isis, show ip route static, and show ip route bgp.

Figure 7 Example of Configured Collection of IP Route



Note—When multiple commands are configured, the output is written to a single command output file that is imported when the Device IP Route Import adapter runs.

Adding IP Route to Existing Event-Based Schedule

Procedure 3 provides instructions for inserting the Device IP Route Import adapter into an existing event-based schedule.

Procedure 3 Add Device IP Route Import to Existing Event-Based Schedule

1 Determine to which chain you will add Device IP Route Import (for example, “Default Chain”).

2 Use the Schedule Visualizer to visualize the currently configured adapter chain and determine at what point in the chain you want to insert Device IP Route. (Refer to the Cisco Virtual Network Data Server online documentation for instructions on opening the Schedule Visualizer.)

3 Determine where in the chain you will insert Device IP Route Import. Note the name of the adapter that you want to trigger Device IP Route and the name of the adapter that you want Device IP Route to trigger. That is, the adapter that will immediately precede Device IP Route Import and the adapter that will follow it, respectively.

4 Open the Mgmt page of the Web Console.

5 Select the Adapter Schedule tab.

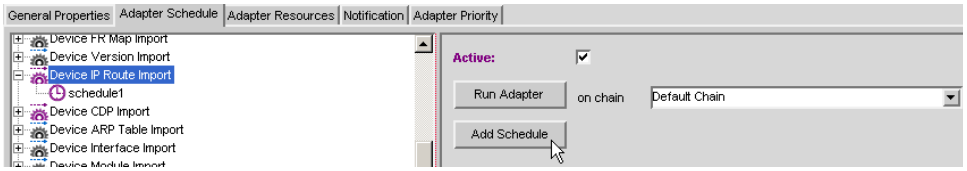
6 Select the adapter that you want to trigger Device IP Route Import in the left pane of the Adapter Schedule tab.

7 Verify that the Active checkbox is checked.

8 Select Device IP Route Import in the left pane of the Adapter Schedule tab.

9 Check the Active checkbox, as shown in Figure 8

Figure 8 Active Status of Device IP Route Import



10 Click the Add Schedule button.

11 Enter a name, such as schedule1, in the New Schedule text field.

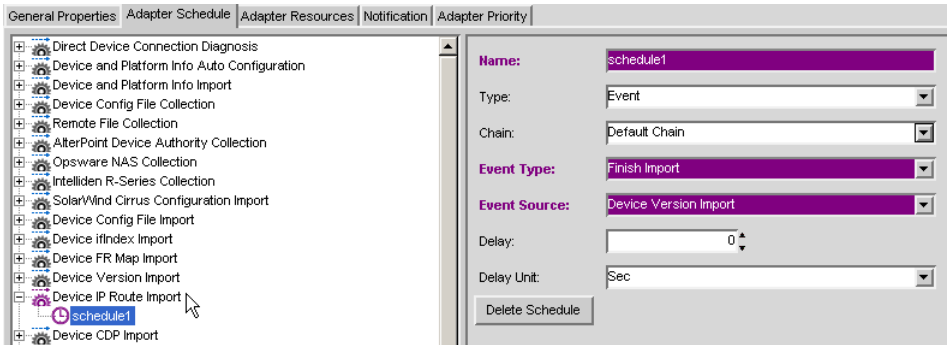
12 Select the name of the chain in which the schedule will participate from the Chain menu.

13 Select Finish Import from the Event Type menu.

14 Select the adapter that you want to trigger Device IP Route Import from the Event Source menu.

Figure 9 shows a Device IP Route Import schedule in which it is triggered by Finish Import of Device Version Import.

Figure 9 Example Schedule for Device IP Route Import



15 Set the Delay and Delay Unit attributes, if you want the Device IP Route Import adapter to wait before it runs.

16 Click the OK button at the bottom of the Mgmt page to save your changes.

17 Select the adapter that you want Device IP Route to trigger in the left pane of the Adapter Schedule tab.

18 Verify that the Active checkbox is checked.

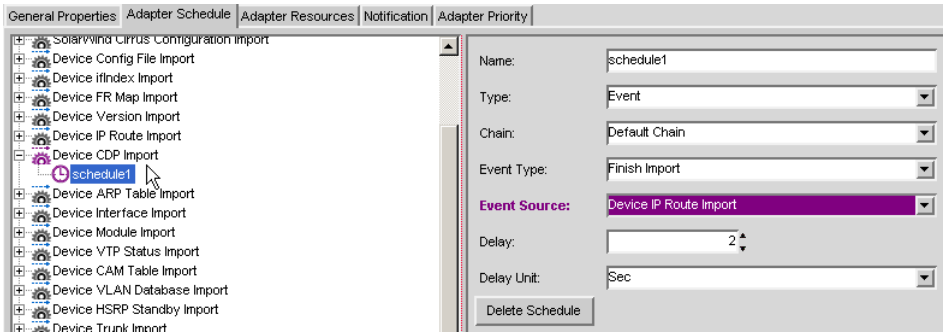
19 Expand the adapter in the left pane of the Adapter Schedule tab and select a schedule. Unless you have created or renamed schedules, select schedule1.

20 Verify that the Event Type is set to Finish Import.

21 Select Device IP Route from the Event Source menu.

Figure 10 shows a Device CDP Import schedule in which it is triggered by Finish Import of Device IP Route Import.

Figure 10 Example Schedule for Device CDP Import



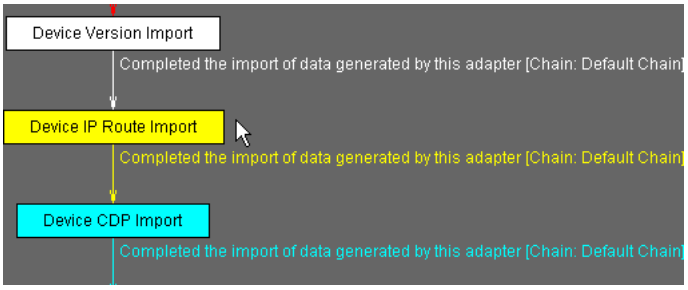
22 Set the Delay and Delay Unit attributes, if you want the adapter to wait before it runs.

23 Click the OK button at the bottom of the Mgmt page to save your changes.

24 Use the Schedule Visualizer to verify your schedule.

Figure 11 shows the portion of the Schedule Visualizer window that illustrates that Device Version Import, Device IP Route Import, and Device CDP Import are scheduled to run one after the other. Device IP Route is triggered when Device Version Import finishes importing data and Device CDP Import is triggered when Device IP Route Import finishes importing data. The adapters are configured to run in a chain named Default Chain.

Figure 11 Example of Event-Based Schedule in Schedule Visualizer



25 Restart Cisco Virtual Network Data Server services for the changes to take effect.

End of Procedure 3

Enhanced Messaging for Invalid CLI Data Files

In previous releases of Cisco Virtual Network Data Server, CLI Data Import adapters (Device Config File Import, Device Interface Import, etc.) marked files as “invalid” when a command output file could not be processed. In this release, when a file cannot be processed by the CLI Data Import adapter the reason is provided. Invalid files will be marked using the following categories:

- “Empty” File—The file contains only white space after the initial prompt. This typically indicates that the device supports the command, however it does not have any information to supply in response to that command. For an example, see Figure 12 on page 19.
- “No Useful Info” File—The file is not empty, however it does not contain any useful information. For an example, see Figure 13 on page 19.
- “Command Failed” File—The device responded with an error message indicating that the command is unsupported by that device. For an example, see Figure 14 on page 19. When this occurs, investigate to determine if the device supports a different form of the command. If it does, you can create a Vendor Type (or modify an existing Vendor Type) in the Device Config File Collection adapter and use a form of the command that the device supports.
- “Specific Error” File—The device responded with an error message. An example of a specific error is when a device responds that CDP is not enabled in response to a CLI command that requests the cdp configuration. For an example, see Figure 15 on page 20.
- “Failed to Parse” File—The CLI Data Import adapter was unable to identify the contents of the file. This may indicate that the file is for a vendor or device type that is not supported in the current version of Cisco Virtual Network Data Server or that the output from a supported vendor/device type is in a *format* that is not supported by the current version of Cisco Virtual Network Data Server. When this occurs you can request that

the file format be supported in a future version of Cisco Virtual Network Data Server by contacting the Cisco Technical Assistance Center and providing the following: the device vendor, model, and operating system and the file that the import adapter failed to parse.

Figure 12 Example of an "Empty" File

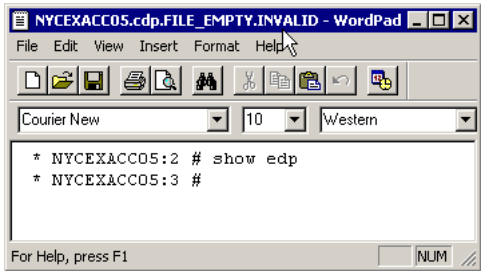


Figure 13 Example of a "No Useful Info" File

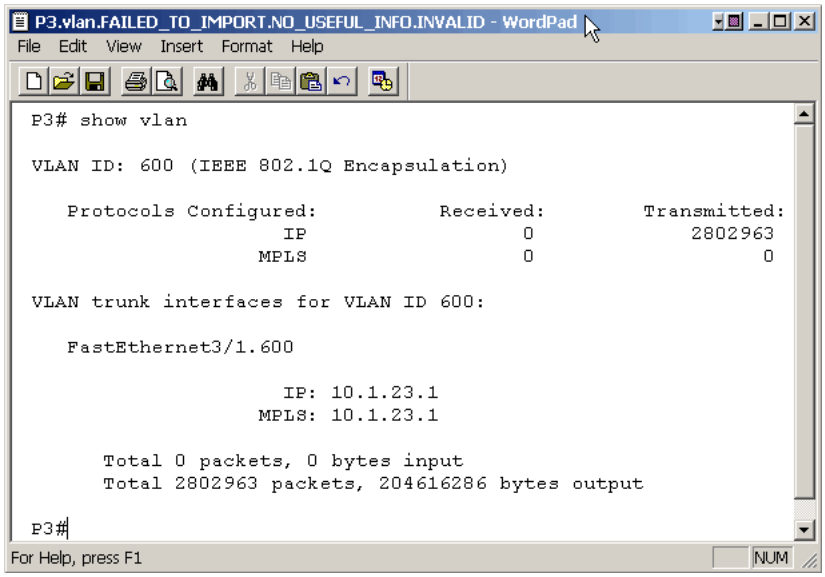


Figure 14 Example of a "Command Failed" File

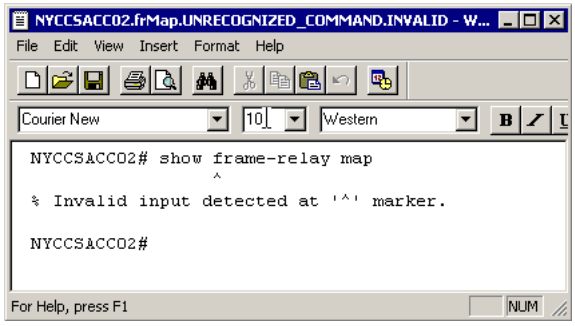
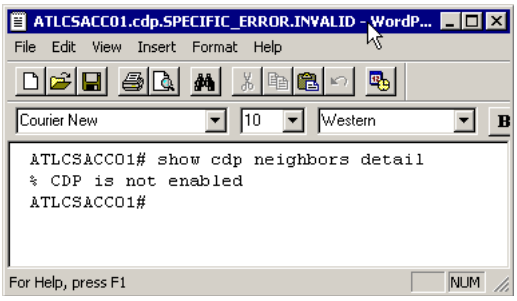


Figure 15 Example of a "Specific Error" File



The Invalid Files report presents a summary of all of the files that could not be processed by the CLI Data Import adapters. For more information and an example report, see Invalid Files on page 21.

Validation Reports

Validation reports are provided to assist in determining which CLI data contribute to device data in the Cisco Virtual Network Data Server database and to assist in determining when data may be missing, resulting in an incorrect or incomplete topology.

The following validation reports are provided in this release:

- Neighbors Not Found in Model on page 20
- Invalid Files on page 21
- Device File Archive Imports on page 21
- Unsupported Command Logs on page 23
- Device Collection Configuration Discrepancies on page 24

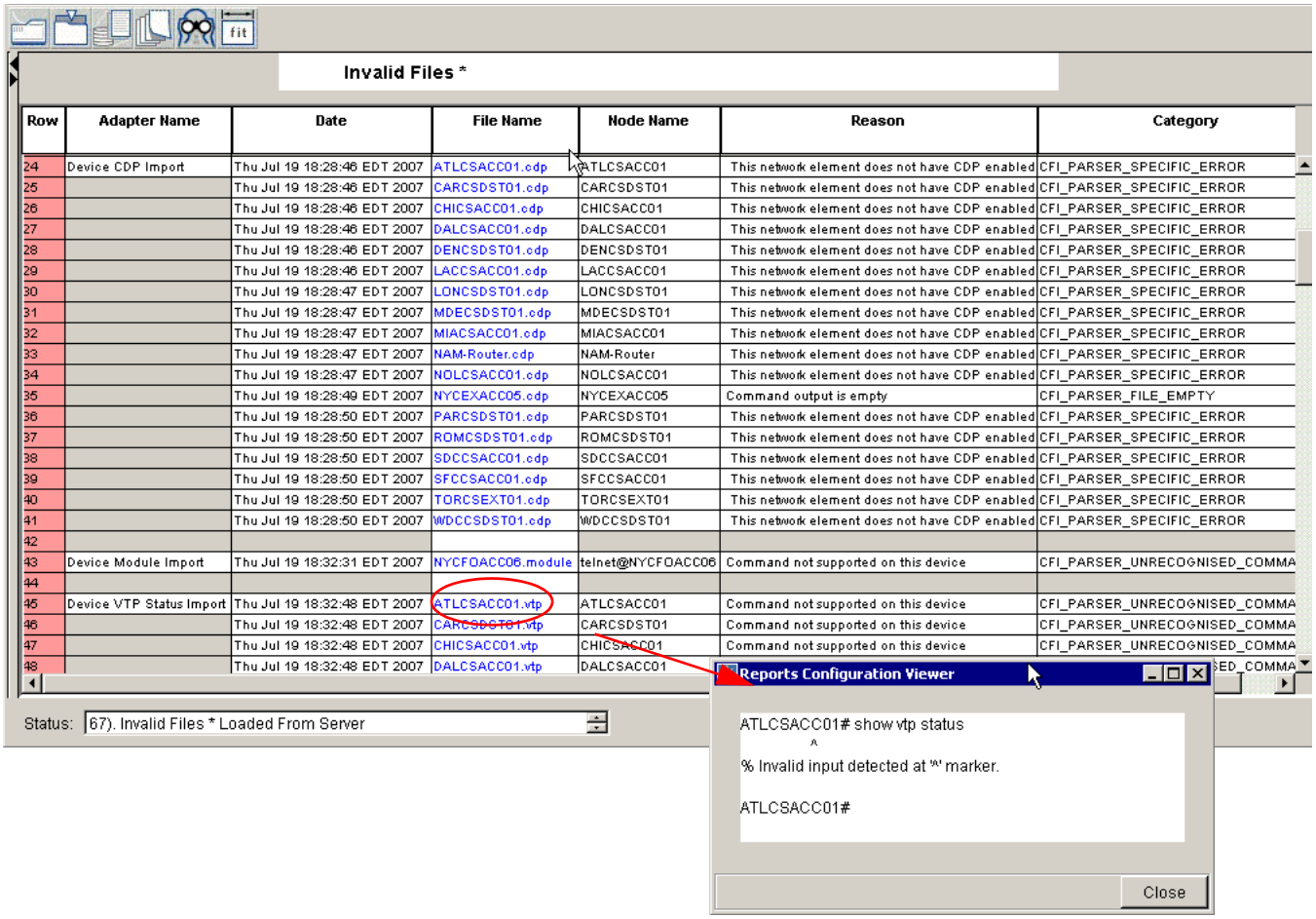
Neighbors Not Found in Model

The Neighbors Not Found in Model Report provides a list of devices that are referenced as neighbor nodes in the neighbor discovery protocol (CDP, EDP, etc.) configuration of one or more devices in the Cisco Virtual Network Data Server database. When a neighbor device is missing, it may indicate that the network data is incomplete and/or the topology inferred by Cisco Virtual Network Data Server will not be fully connected.

Invalid Files

The Invalid Files report provides a list of the invalid files for each CLI Data Import adapter for the most recent import cycle and the reason why the file was deemed invalid. Figure 16 shows an Invalid Files report. Click on the name of a file (shown in blue text in the “File Name” column) to open and examine that file in a file viewer.

Figure 16 Invalid Files Report



Invalid Files *

Row	Adapter Name	Date	File Name	Node Name	Reason	Category
24	Device CDP Import	Thu Jul 19 18:28:46 EDT 2007	ATLCSACC01.cdp	ATLCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
25		Thu Jul 19 18:28:46 EDT 2007	CARCSDST01.cdp	CARCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
26		Thu Jul 19 18:28:46 EDT 2007	CHICSACC01.cdp	CHICSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
27		Thu Jul 19 18:28:46 EDT 2007	DALCSACC01.cdp	DALCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
28		Thu Jul 19 18:28:46 EDT 2007	DENCSDST01.cdp	DENCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
29		Thu Jul 19 18:28:46 EDT 2007	LACCSACC01.cdp	LACCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
30		Thu Jul 19 18:28:47 EDT 2007	LONCSDST01.cdp	LONCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
31		Thu Jul 19 18:28:47 EDT 2007	MDECSDST01.cdp	MDECSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
32		Thu Jul 19 18:28:47 EDT 2007	MIACSACC01.cdp	MIACSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
33		Thu Jul 19 18:28:47 EDT 2007	NAM-Router.cdp	NAM-Router	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
34		Thu Jul 19 18:28:47 EDT 2007	NOLCSACC01.cdp	NOLCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
35		Thu Jul 19 18:28:49 EDT 2007	NYCEXACC05.cdp	NYCEXACC05	Command output is empty	CFI_PARSER_FILE_EMPTY
36		Thu Jul 19 18:28:50 EDT 2007	PARCSDST01.cdp	PARCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
37		Thu Jul 19 18:28:50 EDT 2007	ROMCSDST01.cdp	ROMCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
38		Thu Jul 19 18:28:50 EDT 2007	SDCCSACC01.cdp	SDCCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
39		Thu Jul 19 18:28:50 EDT 2007	SFCCSACC01.cdp	SFCCSACC01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
40		Thu Jul 19 18:28:50 EDT 2007	TORCSEXT01.cdp	TORCSEXT01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
41		Thu Jul 19 18:28:50 EDT 2007	WDCCSDST01.cdp	WDCCSDST01	This network element does not have CDP enabled	CFI_PARSER_SPECIFIC_ERROR
42						
43	Device Module Import	Thu Jul 19 18:32:31 EDT 2007	NYCFOACC06.module	telnet@NYCFOACC06	Command not supported on this device	CFI_PARSER_UNRECOGNISED_COMMA
44						
45	Device VTP Status Import	Thu Jul 19 18:32:48 EDT 2007	ATLCSACC01.vtp	ATLCSACC01	Command not supported on this device	CFI_PARSER_UNRECOGNISED_COMMA
46		Thu Jul 19 18:32:48 EDT 2007	CARCSDST01.vtp	CARCSDST01	Command not supported on this device	CFI_PARSER_UNRECOGNISED_COMMA
47		Thu Jul 19 18:32:48 EDT 2007	CHICSACC01.vtp	CHICSACC01	Command not supported on this device	CFI_PARSER_UNRECOGNISED_COMMA
48		Thu Jul 19 18:32:48 EDT 2007	DALCSACC01.vtp	DALCSACC01		ED_COMMA

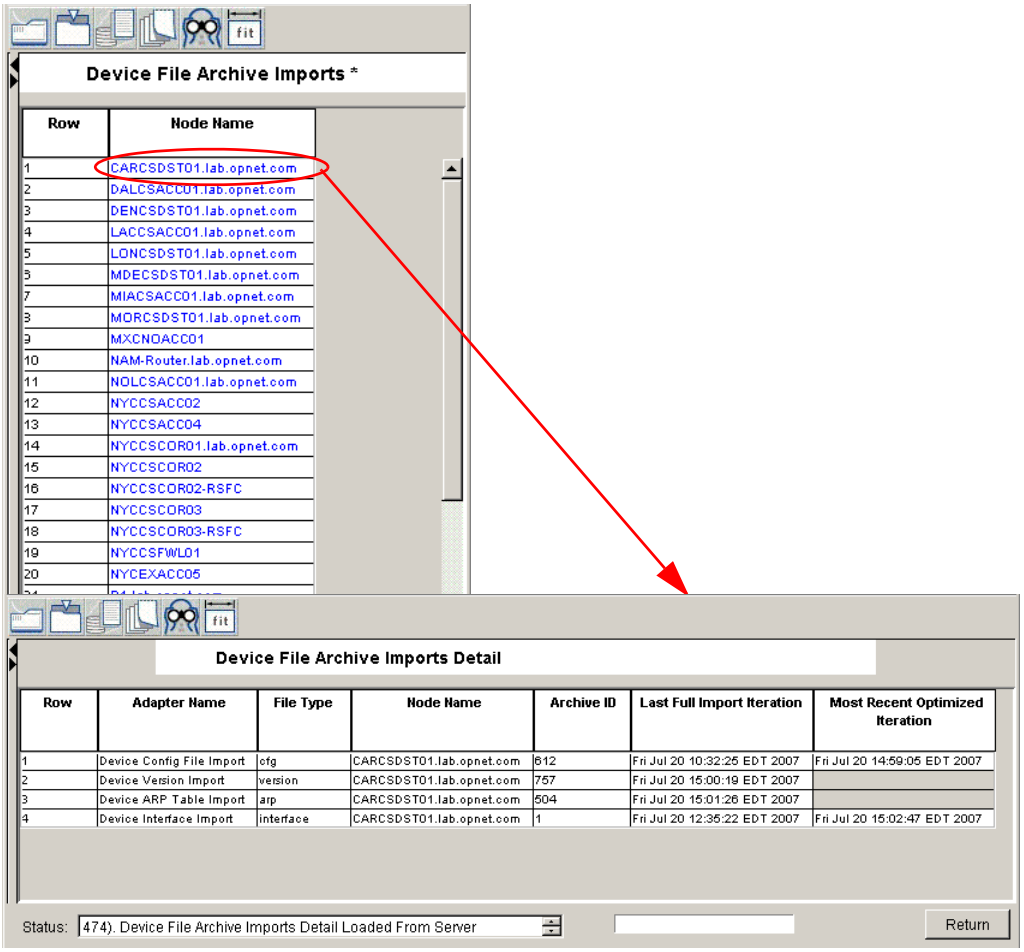
Status: 67). Invalid Files * Loaded From Server

See Enhanced Messaging for Invalid CLI Data Files on page 18 for related information about invalid files.

Device File Archive Imports

The Device File Archive Imports report provides access to a list of the CLI data files that were successfully imported and contribute to the network data for each device in the Cisco Virtual Network Data Server database. When you open the report you are presented with a list of devices. When you click on a node name (shown in blue text in the “Node Name” column), you open a detailed version of the report that provides information about the imported CLI data for this device. Figure 17 provides an example of the Device File Archive Imports report.

Figure 17 Device File Archive Imports



The Device File Archive Imports indicates the following:

- If and when a certain type of data was imported for this device.
  - CLI data types that are not listed in the Device File Archive Imports Detail report are not contributing to the device data in Cisco Virtual Network Data Server.
- The age of device data.
  - In other words the last time data was imported for this node and when it last refreshed. For each CLI data type, this can be deduced from the Last Full Import Iteration or the Most Recent Optimized Iteration column, whichever is later. For the entire device, this can be deduced from the Last Full Import Iteration or the Most Recent Optimized Iteration column across the entire report, whichever is later.

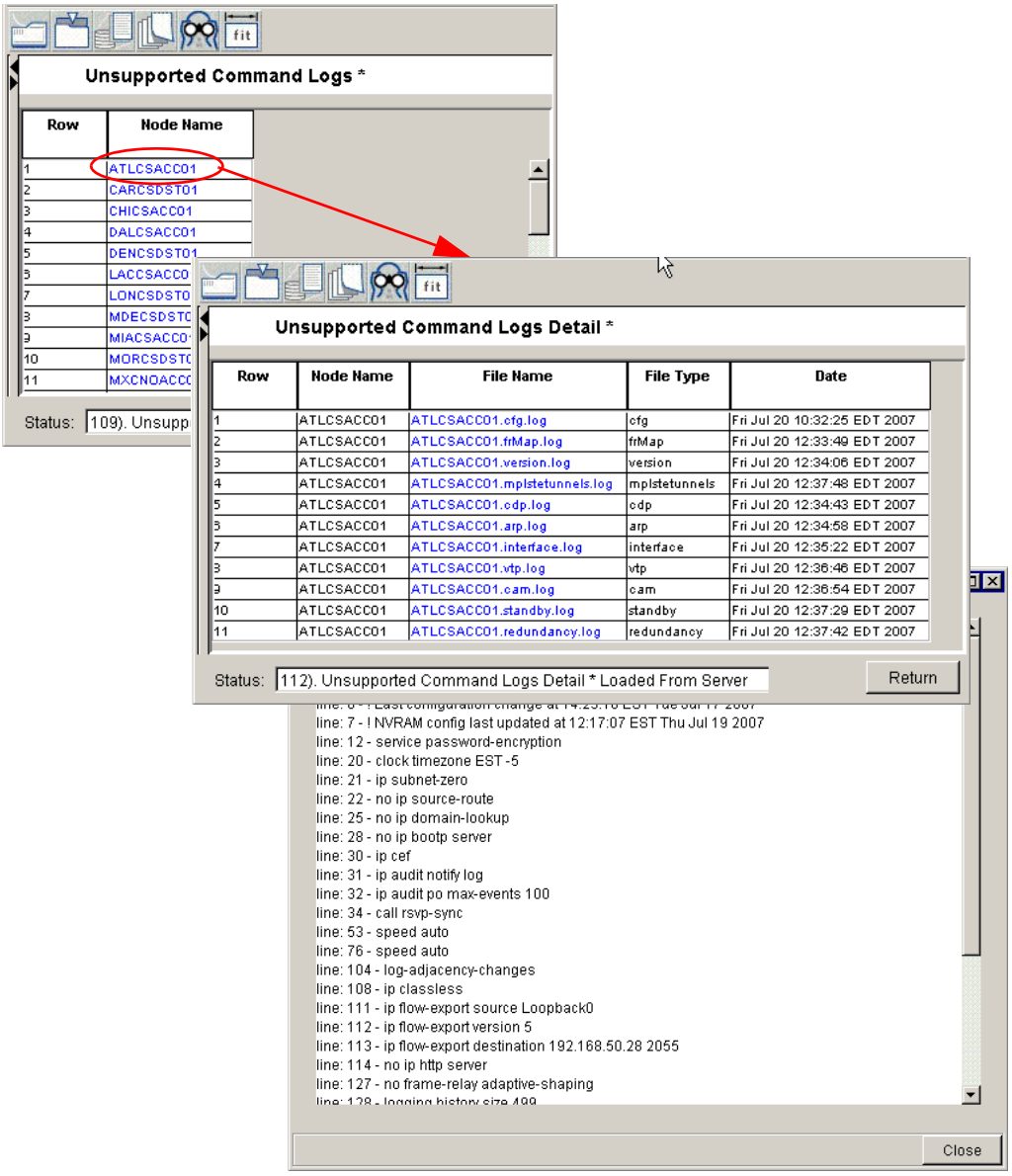
Unsupported Command Logs

The Unsupported Command Logs report provides access to the commands that were ignored by the CLI Data Import adapter when it imported a CLI data file (.cfg, .interface, .cdp, etc.). Figure 18 provides an example of the Unsupported Command Logs report.

Note—The information in the file viewer is a list of the lines from the input file that do **not** contribute to the data in the Cisco Virtual Network Data Server database.

Note—If there are commands in the unsupported commands log file that you believe would be useful to import and represent in the Cisco Virtual Network Data Server database, you can request that it be supported in a future version of Cisco Virtual Network Data Server by contacting the Cisco Technical Assistance Center and providing the following: the device vendor, model, and operating system, the specific command that was ignored and an example file containing the command output.

Figure 18 Unsupported Command Logs Report



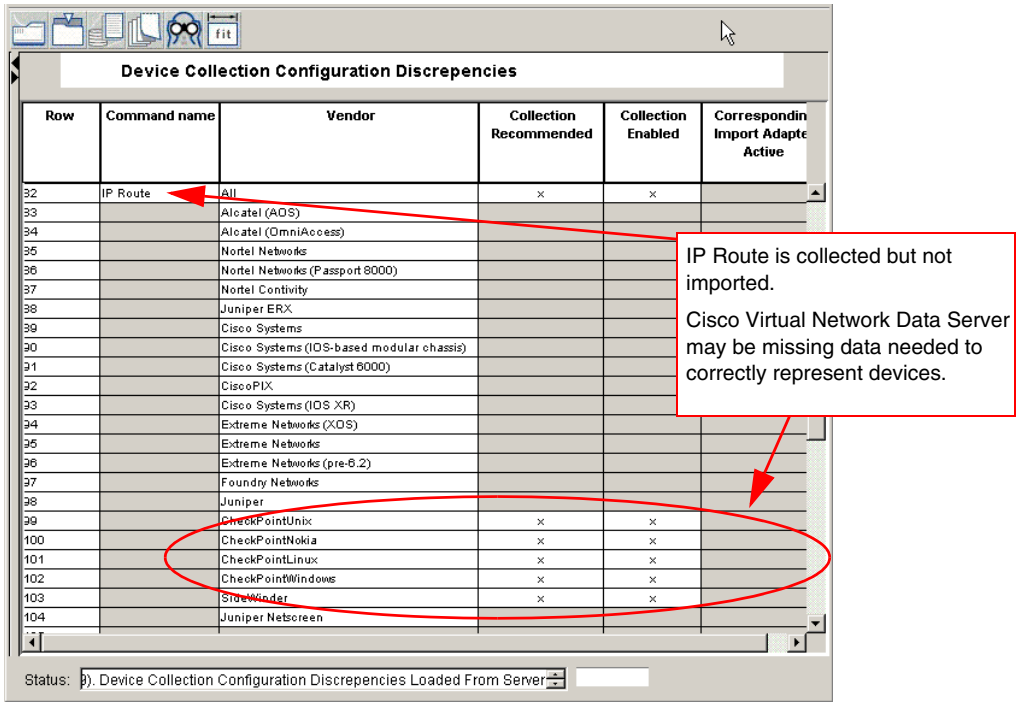
Device Collection Configuration Discrepancies

The Device Collection Configuration Discrepancies report can be used to determine if

- data for a Vendor Type is not being collected
- data for a Vendor Type is collected but not imported

An example report is shown in Figure 19.

Figure 19 Device Collection Configuration Discrepancies Report



The “Collection Recommended” column is checked when collection is enabled by default for a Vendor Type in the Adapter Resources for Device Config File Collection adapter.

The “Collection Enabled” column indicates whether collection is currently enabled for that Vendor Type.

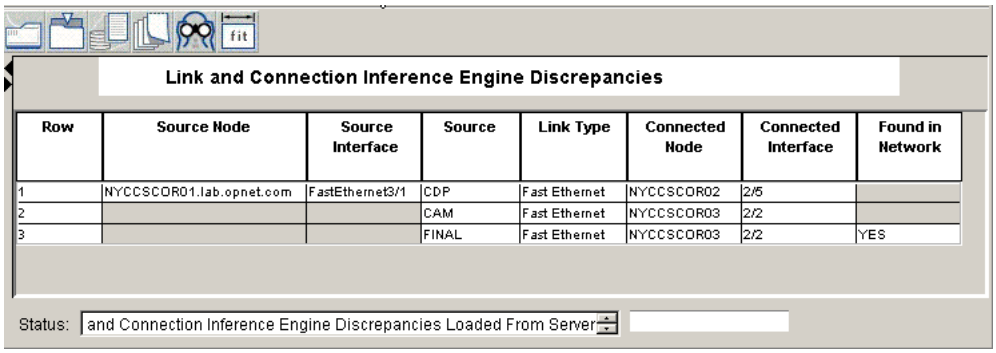
The “Corresponding Import Adapter Active” column indicates whether the CLI Data import adapter for that data type is currently active in the adapter schedule.

If collection of a CLI data type is recommended for a particular Vendor Type but it is not currently enabled, Cisco Virtual Network Data Server may be missing data that is needed to correctly represent devices of that Vendor Type. If collection is enabled, but the corresponding import adapter is not active, data is being collected but not imported. Again, Cisco Virtual Network Data Server may be missing data.

Link and Connection Inference Troubleshooting

The Link and Connection Inference Engine Discrepancies report provides troubleshooting assistance by identifying discrepancies between inference engines. Figure 20 shows an example report.

Figure 20 Link and Connection Inference Engine Discrepancies Report



Link and Connection Inference Engine Discrepancies

Row	Source Node	Source Interface	Source	Link Type	Connected Node	Connected Interface	Found in Network
1	NYCCSCOR01.lab.opnet.com	FastEthernet3/1	CDP	Fast Ethernet	NYCCSCOR02	2/5	
2			CAM	Fast Ethernet	NYCCSCOR03	2/2	
3			FINAL	Fast Ethernet	NYCCSCOR03	2/2	YES

Status: and Connection Inference Engine Discrepancies Loaded From Server

An entry is created in this report when

- Two or more inference engines infer different endpoints for a given source interface
- A link inferred by one or more inference engines is not found in the Cisco Virtual Network Data Server database

The “Source” column lists each inference engine that inferred a link from the source interface as well as the final choice that was made by Link and Connection Inference. The “Found in Network” column indicates whether the link is present in the Cisco Virtual Network Data Server database after the links inferred by Link and Connection Inference are imported into the database.

Enhancements to Notification

The Notification function includes the following enhancements:

- Rollup of messages—Limits the number of e-mails sent by Cisco Virtual Network Data Server by permitting configuration of maximum number of e-mails within a given time frame
- Test email function—Performs a basic SMTP test
- Test Notification System function—Performs a test of the Notification system using the last saved configuration
- Logging

New and Renamed Adapters

The following have been added in this release:

- Device and Platform Info Auto Discovery. See Device and Platform Info Auto Discovery on page 39.
- Intelliden R-Series Collection
- SolarWinds Cirrus Configuration Import
- Alcatel 5620 SAM-O Network Import. See Alcatel 5620 SAM-O Network Import on page 64.
- Symantec AntiVirus Gateway Import
- CA eHealth Service Import
- CA eHealth CoS Utilization Import
- CoS MIB-Based Utilization Import
- SolarWinds Orion Network Inventory Status and Utilization Import
- Metrics Maintenance Service

The CA eHealth Point-to-Point Latency Import adapter has been renamed as CA eHealth IP SLA Import.

Device Info File

The device info file format has not changed in this release. It is identical to the file format used in Cisco Virtual Network Data Server 2.0, 2.01, and 2.0.2. See Format of Device Info File on page 77 for updated documentation.

Schedules

Custom and manual schedules are deprecated in this release.

Importing into Cisco Analysis Software

This section describes preferences that you may need to create or modify in Cisco analysis software when you import from Cisco Virtual Network Data Server.

Note—These are changes that you will make in the Preferences for the Cisco analysis software. Unless otherwise noted, make changes using **Edit >Preferences** in the Cisco analysis software.

Cisco Virtual Network Data Server on Linux Set the “VNE Server Port” preference for the Cisco analysis software client to 3001 when importing from Cisco Virtual Network Data Server running on a Linux platform.

Cisco Virtual Network Data Server Installed with Non-Default Client Connectivity Port The software is installed to the Live Update Service (LUS) on a specified port. Since software clients connect to Cisco Virtual Network Data Server using the LUS, the LUS port is also called the client connectivity port. The default value for Cisco Virtual Network Data Server’s Client Connectivity Port is 3100. If a user-defined (non-default) value was specified for Cisco Virtual Network Data Server’s Client Connectivity Port during Cisco Virtual Network Data Server installation, you must make a corresponding change to the value of the “VNE Server LUS Port” preference for any Cisco analysis software client that you want to connect to that Cisco Virtual Network Data Server.

Restrictions and Limitations

This section describes restrictions and limitations of this Cisco Virtual Network Data Server release:

- Version of DirectX on page 29
- Virus Scanning, Backup Services, and Windows Updates on page 29
- VMware on page 31
- Installation Restrictions on page 31
- Migration of Product Configuration on page 31
- Service Startup on page 34
- Launch of Control Panel on page 36
- User Interface Operation on page 36
- User Interface Look and Feel on page 37
- Licensing on page 37
- Web Console on page 37
- Linux on page 38

Version of DirectX

Versions of DirectX older than 9.0.c are known to interfere with the correct operation of the Cisco Virtual Network Data Server installer and Cisco Virtual Network Data Server software. Select Start > Run > dxdiag to determine the version of DirectX installed. If your DirectX version is older than 9.0c, upgrade your version.

Virus Scanning, Backup Services, and Windows Updates

Note—We strongly recommend that you perform activities such as virus scanning of Cisco Virtual Network Data Server directories, backup of the Cisco Virtual Network Data Server host and database host (if you use a remote database), and Windows updates when Cisco Virtual Network Data Server services are stopped rather than attempting these activities during normal Cisco Virtual Network Data Server operation.

Virus scanning, backup services, and Windows updates can interfere with and/or significantly slowdown Cisco Virtual Network Data Server operation as described in the following sections.

- Virus Scanning on page 30

- Backup Services on page 30
- Windows Updates on page 30

Virus Scanning

On-access virus scanning of the Cisco Virtual Network Data Server directories (including the database data directory) negatively impacts performance and can interfere with correct operation of the Cisco Virtual Network Data Server software. Exclude the Cisco Virtual Network Data Server directories (both the directory where the software is installed and the database data directory) from being scanned if on-access virus scanning is enabled on the Cisco Virtual Network Data Server host. (For PostgreSQL installed on a Windows host, the data directory is <dss_rootdir>\DSS\PostgreSQL\8.2\data.) If the database is on a remote host, you must also make sure that the database data directory is excluded from on-access scanning on that host.

Virus scanning of Cisco Virtual Network Data Server directories may be performed on a regular basis, however scanning of directories where Cisco Virtual Network Data Server software writes and manipulates files should NOT be performed during normal Cisco Virtual Network Data Server operation. Instead, conduct virus scanning of Cisco Virtual Network Data Server software and database data directories at a time when the Cisco Virtual Network Data Server services are stopped.

Backup Services

Backup services running on the Cisco Virtual Network Data Server host that lock files in the database directory and/or other directories to which Cisco Virtual Network Data Server reads and writes (for example, the temporary directory and log directory) interfere with Cisco Virtual Network Data Server operation. Do not run backup services on the Cisco Virtual Network Data Server host during normal Cisco Virtual Network Data Server operation as this can interfere with correct operation.

Windows Updates

We do not recommend that you configure Windows Automatic Updates to automatically install updates on the Cisco Virtual Network Data Server host or database host (if you have a remote database). Instead, we recommend that you configure Windows Automatic Updates to download updates (but not to install the updates automatically) and that you install the updates and reboot, if necessary, when Cisco Virtual Network Data Server services are stopped for the following reasons.

- Many OS updates require that the system be rebooted. If a system reboot occurs on the Cisco Virtual Network Data Server host or database host at a time when Cisco Virtual Network Data Server is either collecting or importing data the adapter or service operation is halted and cannot be resumed. As a result, the Cisco Virtual Network Data Server data may be stale or only partially updated at the time of the reboot and reflect incorrect network data and/or topology.

- Some Windows updates have been known to interfere with correct Cisco Virtual Network Data Server operation. When you are cognizant of when OS updates occur you are better equipped to troubleshoot and resolve any issues that might arise as the result of an update.

VMware

Deployment of Cisco Virtual Network Data Server on VMware requires static allocation of resources to meet minimum system requirements for a Cisco Virtual Network Data Server installation. See the System Requirements for additional information.

WARNING—Even with static allocation of resources, you may experience significant and unpredictable performance degradation if you choose to run Cisco Virtual Network Data Server on VMware.

Installation Restrictions

This release has the following installation restrictions:

- You must run the installer as an administrative user.
- The installation path for Cisco Virtual Network Data Server, and the paths chosen for the temporary directory and the archive directory cannot contain embedded spaces.
- Cisco Report Server and Cisco Virtual Network Data Server should not be installed to the same parent directory on the same host.
- (Windows) The installation directory specified for the Data Storage Server must be a local NTFS-formatted drive.
- (Windows) The “Secondary Logon” or “RunAs Service” Windows service must be started when you run the installer. This service can be stopped after successful installation.
- The installer must be able to create a local (non-domain) operating system account on the Cisco Virtual Network Data Server host in order to successfully install and run the Data Storage Server.
- If you are running the installer on a remote system and using remote desktop to access the host, you must be connected using console mode.

Migration of Product Configuration

This section describes known issues relating to migration of Cisco Virtual Network Data Server product configuration—including adapter resource migration—when migrating from Cisco Virtual Network Data Server 2.0.1 or 2.0.2 to Cisco Virtual Network Data Server 2.1.

- Authentication and User Accounts on page 32
- Notification Settings on page 32

- Custom Schedules on page 32
- AlterPoint Device Authority Collection on page 33
- CiscoWorks NCM Collection/Opsware NAS Collection on page 33
- Intelliden R-Series Collection on page 33
- Remote File Collection on page 34
- CLI Data Import Adapters (Device Config File Import and Others) on page 34
- CA eHealth IP SLA Import (CA eHealth Point-to-Point Latency Import) on page 34
- External Adapter on page 34

Authentication and User Accounts

Cisco Virtual Network Data Server software is installed with local authentication configured by default and one local administrative user (*admin*) configured. The installer permits you to enter the password for this *admin* account. Neither local user accounts nor authentication scheme migrate to the new release.

WARNING—Before you configure remote authentication, make sure that at least one local Cisco Virtual Network Data Server user account with the “admin” role has a matching user account on the remote authentication server. (The usernames must match.)

Notification Settings

Notification settings do not migrate. The installer permits you to enter email server settings, however after the upgrade you will need to configure your selected Notifications since they will be set to the defaults for the new release.

Custom Schedules

Custom schedules are no longer supported. Adapter and Service schedules of type custom are deleted during migration. After you migrate, configure a schedule from the supported schedule types.

AlterPoint Device Authority Collection

Some properties for cloned servers are not handled properly during migration. If you have created additional servers in the adapter resources for the AlterPoint Device Authority Collection adapter, perform the following steps after you upgrade:

1) Manually copy the include and exclude text files from your old installation directory to the new installation directory

2) Correct the path for the “collect device and folders from file” and “exclude device and folders from file” properties to point to the new installation directory

CiscoWorks NCM Collection/Opsware NAS Collection

Some properties for cloned servers are not handled properly during migration. If you have created additional servers in the adapter resources for the CiscoWorks NCM Collection or Opsware NAS Collection adapter, perform the following steps after you upgrade:

1) Manually copy include and exclude text files from your old installation directory to the new installation directory

2) Correct the path for the “collect device and groups from file” and “exclude device and groups from file” properties to point to the new installation directory

3) Correct group paths (group export filename, nodes to group export filename, subgroup export filename) to point to the new installation directory

Intelliden R-Series Collection

Some properties for cloned servers are not handled properly during migration. If you have created additional servers in the adapter resources for the Intelliden R-Series Collection adapter, perform the following steps after you upgrade:

1) Manually copy include and exclude sub-realms text files from your old installation directory to the new installation directory

2) Correct the path for the “include Sub-Realms from file” and “exclude Sub-Realms from file” properties in the Realm Setup> Dynamic - Get Realm List from Server> Explicit Sub-Realm List (Optional) property tree to point to the new installation directory

Remote File Collection

All settings migrate from the previous installation to the new installation for this adapter. If the previous and new installation use different temporary directory (tempdir) paths, then files obtained by this adapter may no longer be in tempdir directories from which they can be imported. Review “Storage” property paths and reconfigure as needed so that files collected by this adapter go into input directories for adapters that use them. An example of this situation is when Remote File Collection is used to collect files for Device Config File Import.

CLI Data Import Adapters (Device Config File Import and Others)

The “input file directory” property does not migrate from the old installation and is reset to the new installation's tempdir. If the previous and new installation use different tempdir paths, then any external tools that deposit config files in the input directory will need to be reconfigured to copy files to the new location. Alternatively, you can manually configure the “input file directory” properties for the CLI Data Import adapters to point to the tempdir used in the old installation.

CA eHealth IP SLA Import (CA eHealth Point-to-Point Latency Import)

The adapter resources for the CA eHealth Point-to-Point Latency Import adapter (renamed CA eHealth IP SLA Import in this release) are not migrated. If you use this adapter, you must manually configure the adapter resources after you upgrade.

External Adapter

The stdout and stderr logfile paths for each command migrate. Review the settings and reconfigure these log file paths to the new installation's log directory or some location outside the installation where you wish to keep these logs.

Service Startup

The following sections describe known issues relating to Cisco Virtual Network Data Server service startup:

- General Service Startup Issues on page 35
- Services Fail to Start Following Installation (Windows) on page 35
- Service Startup Following Reboot (Linux) on page 35

General Service Startup Issues

Database Service Cisco Virtual Network Data Server services are dependent upon the database service. If the database service has not started, Cisco Virtual Network Data Server services will fail to start. When Cisco Virtual Network Data Server is configured to use the Data Storage Server (PostgreSQL):

- Ensure that the port on which the PostgreSQL listens (default is 5432) is not in use by another application
- Ensure that the OS user account that owns the PostgreSQL service (*dssowner*) has not been deleted.

Licensing Ensure that the license server that the Cisco Virtual Network Data Server software is configured to use is up and reachable from the Cisco Virtual Network Data Server host. Check to make sure that the license server has a license available for use by Cisco Virtual Network Data Server.

Services Fail to Start Following Installation (Windows)

When installing Cisco Virtual Network Data Server on a Windows platform you may encounter a known issue with Microsoft Windows that will prevent Cisco Virtual Network Data Server services from starting. If services fail to start, try to start the web service manually. Locate the Cisco VNDS Web Service in the Windows Services window, right-click on it, and select Start from the right-click menu.

You have encountered the Microsoft Windows problem if the following message displays: “Could not start Cisco VNDS Web Service service on Local Computer. Error 1053: The service did not respond to the start or control request in a timely fashion.”

The solution is to reboot the PC. Cisco Virtual Network Data Server services should start normally after the system reboots.

Service Startup Following Reboot (Linux)

This section describes steps you can perform if you encounter a situation on a Linux host where Cisco Virtual Network Data Server services fail to restart following system reboot or appear to be in a suspended state while restarting.

Cisco Virtual Network Data Server services are dependent on the database services and cannot start if the database has not yet started. In addition, the license server service must be running in order to grant Cisco Virtual Network Data Server a license.

Local Database For a **local database**, ensure that

- the database has its startup script in run levels 3 and 5

- start order of the database is before the Cisco Virtual Network Data Server Services
- the database has its shutdown scripts in run levels 0 and 6
- shutdown order of the database is after the Cisco Virtual Network Data Server services

---

Note—Please use “runuser” instead of “su” for the database startup scripts as “su” might cause an interactive prompt which will cause the database service to wait for input during bootup.

Remote Database For a **remote database**, ensure that the remote database has started before (re)booting the Cisco Virtual Network Data Server host. If the database has started and you still see Cisco Virtual Network Data Server services fail to start, reboot into run level 1 and examine /var/log/messages to see if it is waiting for input at an interactive dialog.

Local License Server For a **local license server**, ensure that

- the license server has its startup script in run levels 3 and 5
- start order of the license server is before the Cisco Virtual Network Data Server Services

Remote License Server For a **remote License Server**, ensure that the remote License Server has started before (re)booting the Cisco Virtual Network Data Server host. If the database has started and you still see Cisco Virtual Network Data Server services fail to start, reboot into run level 1 and examine /var/log/messages to see if it is waiting for input at an interactive dialog.

Launch of Control Panel

See Version of DirectX on page 29.

User Interface Operation

See the following:

- Version of DirectX on page 29
- Web Console on page 37

User Interface Look and Feel

If you are running Cisco Virtual Network Data Server on Windows XP and have a white menu bar in the application window, change the theme from Windows XP to Windows Classic. You can change the theme in the Display panel by opening the Windows OS **Control Panel > Display**.

Licensing

Cisco Virtual Network Data Server has the following restrictions and limitations with respect to product licensing.

- Standalone licensing is not supported by Cisco Virtual Network Data Server.
- Loanable licenses are not supported by Cisco Virtual Network Data Server.
- Only one local license server may be installed on the Cisco Virtual Network Data Server host.
- The Cisco licensing software deployed with Cisco Virtual Network Data Server does not include the License Manager user interface. Instead, a command line utility, LS_UTIL, is provided.
- The Cisco Virtual Network Data Server command line licensing utility (LS_UTIL) cannot revoke a license managed by a remote license server.

Web Console

This section describes known issues relating to Cisco Virtual Network Data Server's Web Console. The following topics are covered:

- Internet Explorer Memory Usage on page 37
- Authentication on page 37
- Initialization of Events Summary on page 38
- Tabbed Browsers on page 38
- Web Console/Web Service Startup (Linux) on page 38

Internet Explorer Memory Usage

Internet Explorer may consume excessive memory when used to view Cisco Virtual Network Data Server's Web Console over an extended period of time (for example, overnight.) To work around this situation, close the browser window and then reopen it.

Authentication

TACACS+ authentication does not function properly with the Dialways 3.x server. To work around this issue, use RADIUS authentication with the Dialways server or select another TACACS+ server.

Initialization of Events Summary

The Home page of the Cisco Virtual Network Data Server Web Console displays summary information including summary counts of event log messages. The first time the Web Console Home page is opened the Events summary displays zero events. Refresh the page to initialize the Events summary.

Tabbed Browsers

When you are using a tabbed browser, the Mgmt page of the Web Console may display duplicates of the tabbed panels within the page (for example, Adapter Resources may display multiple times). Refresh the page to remove the duplicates.

Web Console/Web Service Startup (Linux)

You must manually start the Cisco VNDS Web Service after the initial installation of Cisco Virtual Network Data Server on Linux. You will not be able to access the Web Console until you do so. Start the web service using the following command: `vnes.sh -c start WS`.

Linux

The following sections describes known issues when Cisco Virtual Network Data Server runs on Linux:

- Adapter Support on Linux on page 38
- Web Console/Web Service Startup (Linux) on page 38
- Service Startup Following Reboot (Linux) on page 35

Also see Importing into Cisco Analysis Software on page 28 for information relating to Cisco Virtual Network Data Server on Linux.

Adapter Support on Linux

Some adapters require installation of client software on the Cisco Virtual Network Data Server host. If the required client software is not supported for the Cisco Virtual Network Data Server host operating system, the adapter cannot be implemented. The following adapters are not supported when Cisco Virtual Network Data Server runs on Linux:

- InfoVista Network Utilization Import
- NetScout nGenius Import

Documentation Addendum

This addendum contains documentation for the following topics:

- Device and Platform Info Auto Discovery
- Alcatel 5620 SAM-O Network Import on page 64
- Publishing to Secure Cisco Report Server on page 75

Device and Platform Info Auto Discovery

The Device and Platform Info Auto Discovery adapter provides a way to create device entries in the Device and Platform Info table by discovering IPv4 network devices. This adapter assists in preparation for
Cisco Virtual Network Data Server's direct collection adapters and is most useful if you have SNMP access to network devices and permission to access devices via SNMP.

Key Concept—This adapter discovers network devices and adds corresponding entries to the Device and Platform Info table. It does not import data into the Cisco Virtual Network Data Server database.

The Device and Platform Info Auto Discovery adapter is not intended to be run on a regular basis as part of your event chain. It is provided as a way to create an initial set of entries in the Device and Platform Info table.

WARNING—This adapter adds traffic to the network and places a load on network devices during the discovery process. Use care when determining when you should run this adapter in order to avoid impacting network performance and coordinate with network administrators to ensure that this adapter's actions are not interpreted as a security threat/intrusion.

This following topics are covered in the sections that follow:

- Adapter Operation on page 40
- Requirements on page 44
- Workflow on page 44
- Configuration Properties for Device and Platform Info Auto Discovery on page 54
- Tips for Optimizing SNMP Discovery on page 59
- Reports on page 60

- Troubleshooting on page 62
- Related Adapters on page 63

For more information on Cisco Virtual Network Data Server's direct collection adapters refer to the Cisco Virtual Network Data Server online documentation for the following adapters:

- Device Config File Collection
- Device MIB Configuration Import
- Device MIB MPLS TE Import
- MIB-Based Interface Utilization Import

Adapter Operation

This section describes the auto discovery process for each of the adapter's discovery engines and describes the device entries created in the Device and Platform Info table. Topics covered include:

- SNMP Discovery
- ICMP Ping Discovery on page 42
- Device Entries Created in Device and Platform Info Table on page 43

SNMP Discovery

The SNMP Discovery engine supports SNMP v1 and v2c. The discovery process starts at a one or more user-specified IP addresses. This starting point is called a discovery seed. The SNMP Discovery engine attempts to access the discovery seed(s) via SNMP using a list of user-specified community strings. The adapter tries each community string until one succeeds or the list is exhausted. If none of the community strings succeed, the adapter determines that the device is not SNMP-capable and moves on to the next IP address.

Upon successful SNMP access, the discovery engine queries MIB values to learn IP addresses. It then attempts to access each of the learned IP addresses that fall within the discovery range. In this way, discovery of the network expands from the discovery seed(s) based on IP addresses learned from each device that it successfully accesses. In the default configuration, the adapter will run an unbounded discovery. This means that it will attempt to discover every

IP address it learns during the discovery process. An unbounded discovery process can expand to devices outside of your network domain and/or management control and/or attempt to access devices that are not SNMP-enabled thus increasing the amount of time it takes to complete the discovery.

Note—We strongly recommend that you configure a discovery range to optimize adapter runtime. See Configure Discovery Range on page 50 for more information.

The final step in the SNMP discovery process is creation of entries in the Device and Platform Info table. Once a device is discovered via SNMP and passes the capability and vendor filters, the engine creates a corresponding device entry in the Device and Platform Info table. When an entry is added to Device and Platform Info, the community string that succeeded during the SNMP discovery process is filled in for the device in the device entry. See Filters for Device and Platform Info Entries to learn more about filters that are applied to determine whether a device entry is created.

See the following for more information about SNMP discovery and firewalls:

- Discovering Through Firewalls
- Discovering Firewalls

Filters for Device and Platform Info Entries When the SNMP Discovery engine successfully accesses a device, it not only queries to learn IP addresses from the device, it also queries MIB values to learn the device capability and vendor for that device. The discovery engine uses the capability and vendor information to determine if an entry should be added to the Device and Platform Info table for that device. By default, entries are created only for devices with router or switch capability.

Discovering Through Firewalls If you want the discovery process to discover devices that are located on either side of a firewall you will need to configure an access list for the Cisco Virtual Network Data Server host and open a port (default SNMP port is 161) to permit SNMP traffic between Cisco Virtual Network Data Server and devices on the other side of the firewall. You may also specify a seed device on either side of the firewall to speed discovery.

Note—The Device and Platform Info Auto Discovery adapter will be unable to discover a device if a firewall separates it from the Cisco Virtual Network Data Server host and bi-directional SNMP traffic between the devices and Cisco Virtual Network Data Server is not permitted through the firewall.

Discovering Firewalls A firewall may not be SNMP-enabled for security reasons. If this is the case, the Device and Platform Info Auto Discovery adapter will be unable to discover it. If you want to collect CLI data from a firewall using the Device Config File Collection adapter, you can manually add an entry to the Device and Platform Info table.

In the event that a firewall is SNMP-enabled and you want Cisco Virtual Network Data Server to discover it, you will likely need to configure the firewall to permit SNMP access from the Cisco Virtual Network Data Server host.

ICMP Ping Discovery

The ICMP Ping Discovery engine determines if specified seed devices can be accessed across the network. When the ICMP Ping Discovery engine runs, it attempts to ping the seed device(s). If a device does not respond to the ping, the operation is tried again, up to the configured number of retries. The engine adds an entry in the Device and Platform Info table for each device that responds. This engine does not learn IP addresses or any other information from a discovered device, therefore so the range of ICMP Ping Discovery is determined by the seed devices. When using this engine, carefully define the seeds so that this engine only attempts to ping devices that are supported by Cisco Virtual Network Data Server's direct collection adapters. If you do not, it can potentially create a large number of entries in the Device and Platform Info table (for devices such as servers, load balancers, and workstations) that are not useful for collection.

Note—If network devices are not SNMP-enabled or you do not have permission/access to devices via SNMP, the ICMP Ping Discovery engine can be used to create entries in the Device and Platform Info Table for subsequent CLI collection. However, it may be more fruitful for you to explore the use of a different method of creating device entries. See the Device and Platform Info chapter in the Cisco Virtual Network Data Server online documentation to learn about other methods of creating device entries in the Device and Platform Info table.

Device Entries Created in Device and Platform Info Table

The amount of information included in a device entry created by this adapter will vary depending on which discovery engine discovered the device. Table 2.1-1 describes the fields populated in a device entry by each discovery engine. For more information on the Device and Platform Info table—including a description of other methods for creating device entries in the Device and Platform Info table—see the Device and Platform Info chapter of the Cisco Virtual Network Data Server online documentation.

Note—When the adapter successfully discovers a device using the SNMP Discovery engine, the corresponding device entry created contains enough information for SNMP collection. Additional fields are required in order to successfully collect CLI data from a device using the Device Config File Collection adapter. See Related Adapters on page 63 to learn about Cisco Virtual Network Data Server adapters that assist in supplying fields required for Device Config File Collection.

Table 2.1-1 Device Entry Fields Populated by Engine

Device Entry Field/Attribute	SNMP Discovery Engine	ICMP Ping Discovery Engine
Device Name	X (sysName)	X (IP Address)
Active flag	enabled	enabled
Access Address	X[1]	X
Merge ID	X	
Read Community String	X (successful community string guessing)	X (“public”)
Collect MIB flag	enabled	
System Name	X	

1. The adapter chooses the device loopback address when populating this field. The access address may be outside of the discovery range if the device has at least one IP address in the discovery range.

Note—The SNMP engine may discover a device through more than one IP address, however it will only create one entry in Device and Platform Info Table. When determining which of the IP addresses to use as the Access Address for the device entry, it chooses the loopback.

Requirements

This section describes requirements for discovery engines supported by this adapter.

The following are required in order to discover network devices using the SNMP Discovery engine:

- SNMPv1 or SNMPv2c must be enabled on all network devices that you want to discover (read-only level is adequate)
- Cisco Virtual Network Data Server must have access to network devices on via SNMP (default SNMP port is 161)
- You must provide the set of SNMP read-only community strings defined for the network domain of interest
- You must provide the IP address of at least one router or switch in each separately connected component that you want to discover
- You must have permission to poll devices on your network via SNMP

If you want to use the ICMP Ping Discovery engine, the Cisco Virtual Network Data Server host must have ICMP access to devices.

Workflow

1) Review Requirements
2) Gather Information
3) Configure Seed(s)
4) Specify Community Strings
5) Test Discovery of Seed(s)
6) (Optional) Configure Discovery Range
7) Discover Network

See Related Adapters on page 63.

Gather Information

Gather the following information for the SNMP Discovery engine:

- Community string(s)—Obtain community strings for all devices that you want to discover. You will enter these values into a Community Strings file used during the discovery process.

  For more information, see Specify Community Strings on page 48.

- IP Address(es)—Obtain the IP address of at least one device in each separately connected segment of your network. You will use this information to specify seed(s) for the SNMP discovery process.

  For more information, see Configure Seed(s) on page 45.

- IP address ranges/subnets—Determine address ranges and/or subnets that are actively used in your network. This information can be used to limit the range of the discovery and speed the discovery process.

  For more information, see Configure Discovery Range on page 50.

For the ICMP Ping Discovery engine you must gather IP subnets/addresses for routers and switches in your network that you want to ping.

Configure Seed(s)

When identifying a seed for the SNMP discovery process, a centrally located device that is connected to other parts of the network via high-speed access is a good choice. For this reason, a router or switch in the core of your network is a good candidate, particularly for a large network.

The discovery seed(s) can be configured in a user-created text file (called the Seed File), using active entries in the Device and Platform Info table, or both. The Advanced Options> Discovery Seed property determines where the adapter obtains the discovery seed(s). In the default configuration, this adapter obtains the discovery seed(s) from the Seed File.

Note—If using ICMP Ping Discovery engine, use care to limit the seed devices to network devices—such as routers and switches—that are supported by Cisco Virtual Network Data Server's direct collection adapters. Do not include IP addresses for servers, hosts, etc. as this can result in a large number of unusable entries in the Device and Platform Info table.

Follow Procedure 1 to configure discovery seed(s) using a Seed File.

Procedure 1 Specify Discovery Seed Using Seed File

1. Select the Adapter Resources tab of the Mgmt page in the Web Console.

2 Select Device and Platform Auto Discovery in the left pane.

3 Click the Edit button for the Seed file property.

➥ The file opens in a text editor.

4 Add entries to the Seed File. See Format of Seed File/Include File/Exclude File on page 47.

5 Click Ok in the Edit File window to save changes and close the text editor.

6 Expand Advanced Options> Discovery Seed.

7 Verify that the Use seed file option is checked.

8 Click OK at the bottom of the Mgmt page to save changes.

End of Procedure 1

Follow Procedure 2 to configure discovery seed using active entries in the Device and Platform Info table.

Procedure 2 Specify Discovery Seed Using Active Device and Platform Info Entries

1 Open the Device and Platform Info window from the Control Panel.

2 Add a device entry for each seed device.

Make sure each entry has the Active flag checked and contains the following fields.

- Device Name
- Access Address

3 Select the Adapter Resources tab of the Mgmt page in the Web Console.

4 Select Device and Platform Info Auto Discovery in the left pane.

5 Expand Advanced Options> Discovery Seed.

6 Verify that the Include active Device and Platform Info Entries option is checked.

7 Click OK at the bottom of the Mgmt page to save changes.

End of Procedure 2

Format of Seed File/Include File/Exclude File

Use the following guidelines when creating the Seed File/Include File/Exclude File:

- Start each comment line with #
- Include one entry per line
- An entry may be an IP address, range of IP addresses, or subnet
  - — a subnet entry in the Seed File can have a mask value of 16-32
  - — a subnet entry in the Include or Exclude File can have a mask value of 0-32

Note—When a subnet is specified in the Seed File, the SNMP Discovery engine enumerates the addresses in the subnet. Address enumeration is limited to Class B networks. Therefore, you can specify a subnet with a mask value of 16-32. A Seed File entry that defines a subnet with a mask value of 0-15 is invalid and the engine skips the entry when it reads the file.

Figure 1 shows an example of a Seed File.

Figure 1 Seed File

```
## connected component in your network.

## Format :
## IP Addresses and Subnets should be defined in a single line
## To specify an IP Address
## xxx.xxx.xxx.xxx, e.g.:- 192.168.1.1
## To specify a Subnet
## xxx.xxx.xxx.xxx/yy, e.g. :- this discovers all IP Addresses from 192.168.1.1
192.168.1.255
## 192.168.1.1/24
## If providing a subnet as a seed, we only enumerate a subnet as large as /16.

## Additionally, you can also specify ranges of IP Address
## xxx.xxx.xxx.xxx-xxx, e.g.:- 192.168.1.1-5 discovers all IP Addresses from
192.168.1.1 to 192.168.1.5

## By default, we do not include any IP Address/subnet to be discovered and th
has to be provided
## by the user.

10.3.1.1
```

Figure 2 provides an example of an Include File.

Figure 2 Include File

```
## This is a file that contains a combination of IP Address and Subnets that
determines
## whether an IP Address that is being discovered should be discovered.
## If an IP Address is discovered and is included in the includeList, then it will
be discovered.

## Format :
## IP Addresses and Subnets should be defined in a single line
## To specify an IP Address to be included
## xxx.xxx.xxx.xxx, e.g.:- 192.168.1.1
## To specify a Subnet to be included
## xxx.xxx.xxx.xxx/yy, e.g. :- this includes all IP Addresses from 192.168.1.1 to
192.168.1.255
## 192.168.1.1/24

## Additionally, you can also specify ranges of IP Address to be included
## xxx.xxx.xxx.xxx-xxx, e.g.:- 192.168.1.1-5 includes all IP Addresses from
192.168.1.1 to 192.168.1.5

10.3.1.1/24
```

Figure 3 provides an example of an Exclude File.

Figure 3 Exclude File

```
## This is a file that contains a combination of IP Address and Subnets not to
## be auto discovered. If any new IP Addresses to be discovered matches any
## IP address in the below list, then it will not be discovered.

## Format :
## IP Addresses and Subnets should be defined in a single line
## To specify an IP Address to be excluded
## xxx.xxx.xxx.xxx, e.g.:- 192.168.1.1
## To specify a Subnet to be excluded
## xxx.xxx.xxx.xxx/yy, e.g. :- this excludes all IP Addresses from 192.168.1.1 to
192.168.1.255
## 192.168.1.1/24
## Additionally, you can also specify ranges of IP Address to be excluded
## xxx.xxx.xxx.xxx-xxx, e.g.:- 192.168.1.1-5 excludes all IP Addresses from
192.168.1.1 to 192.168.1.5

## By default, we only exclude the loop back addresses
127.0.0.0/8
```

Specify Community Strings

In order for the SNMP Discovery engine to discover devices you must provide community strings for your network devices. Make sure you include the community strings for all of the devices in your network that you want to discover and include “public” if applicable. Provide the most complete set of read community strings to yield the most complete discovery results.

To speed the initial stages of the discovery process you should list the most-used community strings first. The order of appearance in the community strings file is the order in which the engine tries the community strings for the seed device(s). As the discovery process progresses, it learns which community strings are most successful and tries them first.

Use the following guidelines when creating a community strings file:

- Comment lines start with #
- Include one entry per line

Follow Procedure 3 to specify community strings.

Procedure 3 Specify Community Strings

1. Select the Adapter Resources tab of the Mgmt page in the Web Console.
2. Select Device and Platform Auto Discovery in the left pane.
3. Expand SNMP Discovery engine.
4. Click the Edit button for the community strings property.

   ➥ The file opens in a text editor.
5. Add entries to the file.
6. Click Ok in the Edit File window to save changes and close the text editor.
7. Click OK at the bottom of the Mgmt page to save changes.

End of Procedure 3

Figure 4 shows an example community strings file with four valid entries.

Figure 4 Community Strings File

```
## This is a file that contains a list of community strings to be tried when
## accessing a device using SNMP. This is only used in Auto Discovery.

## Format :
## Each community string must be specified in a single line
## public
## foo
## bar

stringone
stringtwo
stringthree
public
```

Test Discovery of Seed(s)

Before you attempt to discover an entire subnet or network using the SNMP Discovery engine, test to ensure that you can successfully access the discovery seed(s).

You can limit SNMP discovery to a single device or small number of devices by configuring the adapter to limit the discovery using an Include File and then specifying the same IP address(es) in the Seed File and in the Include File. Follow Procedure 4 to limit discovery using an Include File and specify only the discovery seed(s) in the Include File. If you have created other entries in the Include File that you want to retain, you can comment them out until you confirm that you can successfully discover the seed(s) and then uncomment these entries when you are ready to discover additional IP addresses and/or subnets.

When the adapter completes, you should have an entry in the Device and Platform Info table for each specified discovery seed.

See Troubleshooting on page 62 for assistance if you encounter issues.

Configure Discovery Range

Note—In the default configuration, the adapter discovery is unbounded. For best results, limit the discovery to the SNMP-enabled devices in the network domain of interest over which you have access and management control and access and from which you want to collect data using
Cisco Virtual Network Data Server's direct collection adapters.

You can configure a discovery range to minimize the work performed by the adapter and optimize runtime. The discovery process can be bounded using an Include File, Exclude File, or both. The adapter will not attempt to discover a device using an IP address that is implicitly excluded (outside of the discovery range as defined by the Include File) or one that is explicitly excluded through the use of an Exclude File. When creating an Include or Exclude File, you can specify an individual IP address, range of IP addresses, or subnet.

The following properties control whether an IP address learned during SNMP discovery is contacted during the discovery process:

- Limit discovery using Include File—Controls whether the discovery process is bounded by a user-configured range of IP addresses/subnets specified in an Include File. By default this property is unchecked meaning that the discovery process is unbounded.
- Limit discovery using Exclude File—Controls whether the discovery process explicitly excludes user-configured IP addresses/subnets specified in an Exclude File. By default this is checked and loopback addresses (127.0.0.0/8) are excluded (to preclude discovery of the Cisco Virtual Network Data Server host and speed the discovery process).

Note—When the Limit discovery using Include File property is unchecked, the discovery process is unbounded. This is the default configuration.

When the Limit discovery using Include File property is checked, as the SNMP Discovery engine learns an IP address during the discovery process it determines if the address is within the discovery range (as specified by the Include File). If the IP address is not within the discovery range, the SNMP Discovery engine makes not attempt to access the address and adds the address to the list of skipped IP addresses. Similarly, When the Limit discovery using Exclude File property is checked, the SNMP Discovery engine determines if the address is excluded from discovery (as specified by the Exclude File) and acts accordingly. The Device and Platform Info Auto Discovery Skipped IP Addresses report provides a list of addresses skipped by the discovery process during the most recent run of the adapter. See Reports on page 60 for an example.

Follow Procedure 4 to limit discovery using an Include or Exclude File.

Procedure 4 Configure Discovery Range Using Include File and/or Exclude File

1. Select the Adapter Resources tab of the Mgmt page in the Web Console.
2. Select Device and Platform Auto Discovery in the left pane.
3. Check the checkbox for the Limit discovery using Include File or Limit discovery using Exclude File property, as appropriate.

   Note—If you want to limit the discovery using an Include or Exclude File you must check the appropriate checkbox. An Include or Exclude File is not read unless the corresponding checkbox is checked.
4. Click the Edit button for the file that corresponds to your selection in step 3 (“Include subnets or IP addresses” or “Exclude subnets or IP addresses”).

   ➥ The file opens in a text editor.

5. Add entries to the file. See Format of Seed File/Include File/Exclude File on page 47.

6. Click Ok in the Edit File window to save changes and close the text editor.

7. Click OK at the bottom of the Mgmt page to save changes.

End of Procedure 4

Discover Network

The discovery process takes time, particularly for large networks. See Tips for Optimizing SNMP Discovery on page 59 for general tips on optimizing SNMP discovery of your network.

See Troubleshooting on page 62 for assistance if you encounter issues.

As the adapter runs, event messages are written to the event log as the discovery process progresses. The Device and Platform Info Auto Discovery Errors report summarizes errors encountered by the adapter. See Reports on page 60 for an example.

The adapter periodically writes entries to the Device and Platform Info table according to the configured update frequency (default is 5 minutes). It will run until the discovery process is complete or the total discovery time limit is reached (default of 300 minutes).

If you want to stop the auto discovery process you can stop Cisco Virtual Network Data Server services, however this halts the discovery process. Device entries that have not been written to the Device and Platform Info table are discarded.

Figure 5 provides an example of the adapter statistics written by this adapter. A device may have multiple capabilities, therefore the addresses exhibiting different capabilities may not be equal to the number of IP addresses configured for SNMP.

Figure 5 Device and Platform Info Auto Discovery Adapter Statistics

```
File

Device and Platform Info Auto Discovery
        Start Time: 09/27/2007 12:20:53
        Stop Time: 09/27/2007 12:21:41

        Duration: (hh:mm:ss) 0:00:48

        ==================================================
        General Summary Statistics
        ==================================================
        IP Addresses queried: 8


        ==================================================
        SNMP Discovery Engine Statistics
        ==================================================
        IP Addresses configured for SNMP: 8
        IP Addresses not configured for SNMP: 0
        IP Addresses exhibiting Router capability: 3
        IP Addresses exhibiting Switch capability: 7
        IP Addresses exhibiting Server capability: 4
        IP Addresses exhibiting Host capability: 4


        ==================================================
        Detailed SNMP Statistics
        ==================================================
        Total SNMP v1 Devices: 0
        Total SNMP v2c Devices: 8
        Total SNMP v3 Devices: 0
```

See Reports on page 60 to learn about reports that provide information about errors encountered and devices discovered during the discovery process.

Figure 6 provides an example of entries created by the SNMP Discovery engine. See Device Entries Created in Device and Platform Info Table on page 43 for a description of the fields populated by each engine.

Figure 6 Entries Created by SNMP Discovery Engine

Device Name	Active	Access Address	Merge ID	Username	Password	Privileged ...	Read Com...	Vendor Ty...	Login Script
NYCCSACC02	☑	10.3.1.8	NYCCSACC02_10.3.1.8	none	none	none	*******	Unknown	Unknown
NYCCSACC03	☑	10.3.1.7	NYCCSACC03_10.3.1.7	none	none	none	*******	Unknown	Unknown
NYCCSCOR01.lab....	☑	10.1.128.3	NYCCSCOR01.lab.opnet.com_...	none	none	none	*******	Unknown	Unknown
NYCCSCOR02	☑	10.3.1.2	NYCCSCOR02_10.3.1.2	none	none	none	*******	Unknown	Unknown
NYCCSCOR02-RS...	☑	10.3.1.3	NYCCSCOR02-RSFC_10.3.1.3	none	none	none	*******	Unknown	Unknown
NYCCSCOR03	☑	10.3.1.4	NYCCSCOR03_10.3.1.4	none	none	none	*******	Unknown	Unknown
NYCCSCOR03-RS...	☑	10.3.1.5	NYCCSCOR03-RSFC_10.3.1.5	none	none	none	*******	Unknown	Unknown

Continue to Related Adapters on page 63 if you are preparing to run the Device Config File Collection adapter.

Configuration Properties for Device and Platform Info Auto Discovery

This section cover the following topics:

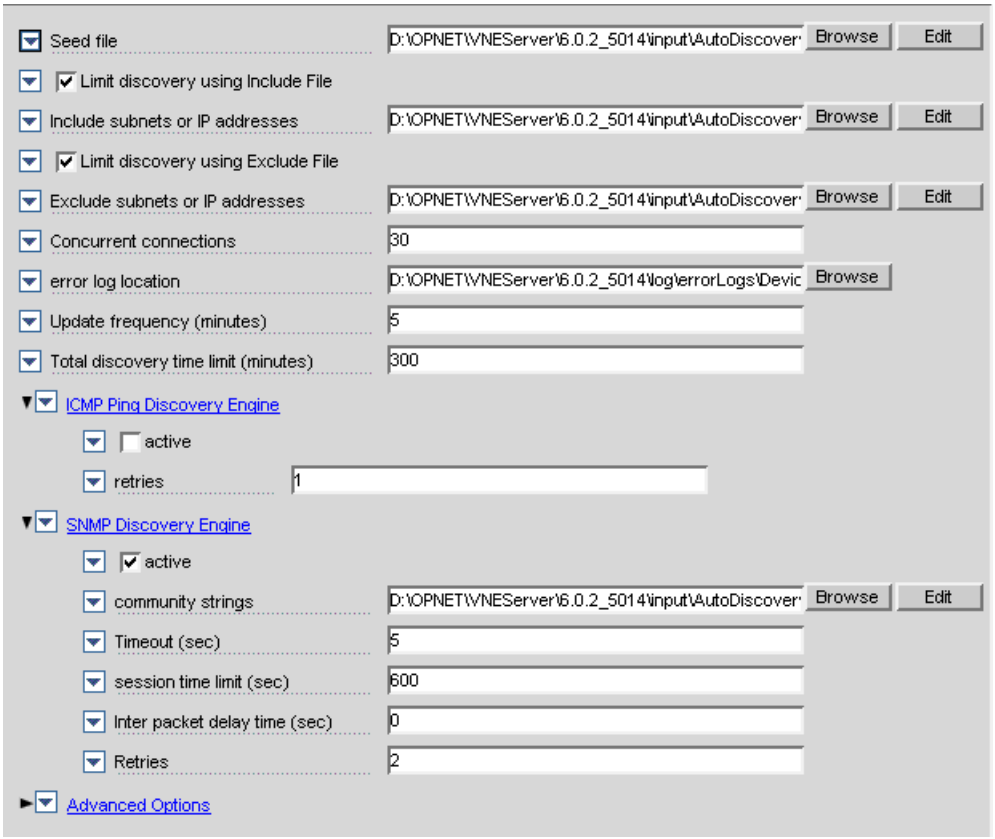
- General Properties
- Advanced Properties on page 57

General Properties

The general configuration properties for this adapter are illustrated in Figure 7 and listed in Table 2.

Note—Figure 7 shows the adapter configured to run the SNMP Discovery engine and to limit discovery using an Include File (recommended).

Figure 7 Device and Platform Info Auto Discovery General Properties



The following table lists general properties for the Device and Platform Info Auto Discovery adapter.

Table 2 Device and Platform Info Auto Discovery General Properties

Adapter Property	Description
Seed file	Points to a text file that can be used to specify the seed device(s) for the discovery process. Advanced Options> Discovery Seed property controls where discovery engines obtain the seed(s). For more information, see Configure Seed(s) on page 45.
Limit discovery using Include File Include subnets or IP addresses Limit discovery using Exclude File Exclude subnets or IP addresses	Control which subnets/IP addresses are contacted by the adapter during the discovery process. When the Limit discovery using Include file is unchecked, the discovery process is unbounded. This is the default setting. When the Limit discovery using Include File option is checked, the Include File defines boundaries (IP addresses/subnets) for the discovery process. If an IP address/subnet is not listed in the Include File, it is implicitly excluded. When the Limit discovery using Exclude File option is unchecked, no IP addresses are explicitly excluded from the discovery process. When the Limit discovery using Exclude File option is checked, the Exclude File defines IP addresses/subnets that are explicitly excluded from the discovery process. Exclusion takes precedence over inclusion. For more information, see Configure Discovery Range on page 50.
Concurrent connections	Specifies the maximum number of parallel threads that the adapter can spawn. The default value is 30.
error log location	Specifies the directory in which the error logs generated by this adapter are stored.
Update frequency (minutes)	Controls how often the adapter updates the Device and Platform Info table. The default is 5 minutes.
Total discovery time limit (minutes)	Controls the total time allotted to run this adapter. If this limit is reached, the adapter will write entries to the Device and Platform Info table and halt. The default is 300 minutes.
ICMP Ping Discovery Engine	
active	Controls whether the adapter uses ICMP ping to discover devices. In the default configuration, this discovery engine is not active. For more information, see Adapter Operation on page 40.

Table 2 Device and Platform Info Auto Discovery General Properties (Continued)

Adapter Property	Description
retries	The number of ICMP packets that will be sent to the device. The default is 1.
SNMP Discovery Engine	
active	Controls whether the adapter uses SNMP to discover devices. In the default configuration, the SNMP Discovery engine is active. For more information, see Adapter Operation on page 40.
community strings	Specifies a file containing read community strings for network devices that you want to discover via SNMP.
Timeout (sec)[1]	Specifies the time limit for a device to respond to an SNMP login request once it has been determined to be SNMP accessible. The default is 5 seconds. You may need to increase this timeout if devices are slow to respond or network access to devices is slow. We recommend that you contact the Cisco Technical Assistance Center before you adjust this value.
session time limit (sec)	The maximum amount of time the discovery engine will spend on a device before giving up on it. The default value is 600 seconds.
Inter packet delay time (sec)	Do not modify. Contact the Cisco Technical Assistance Center with questions. The default is 0 seconds.
Retries[1]	The number of times SNMP login is attempted for a device once it has been determined to be SNMP accessible. The default is 2. We recommend that you contact the Cisco Technical Assistance Center before you adjust this value.
Advanced Options	See Table 3.
End of Table 2	

1. When the SNMP Discovery engine makes the initial attempt to determine if it can access an IP address, the timeout is 1 second per community string. No retries are attempted. Once a device has been successfully accessed via SNMP and the discovery engine begins to query MIB tables, these user-configurable timeout and retries go into effect.

Advanced Properties

The advanced options for this adapter are shown in Figure 8 and described in Table 3.

Figure 8 Device and Platform Info Auto Discovery Advanced Options

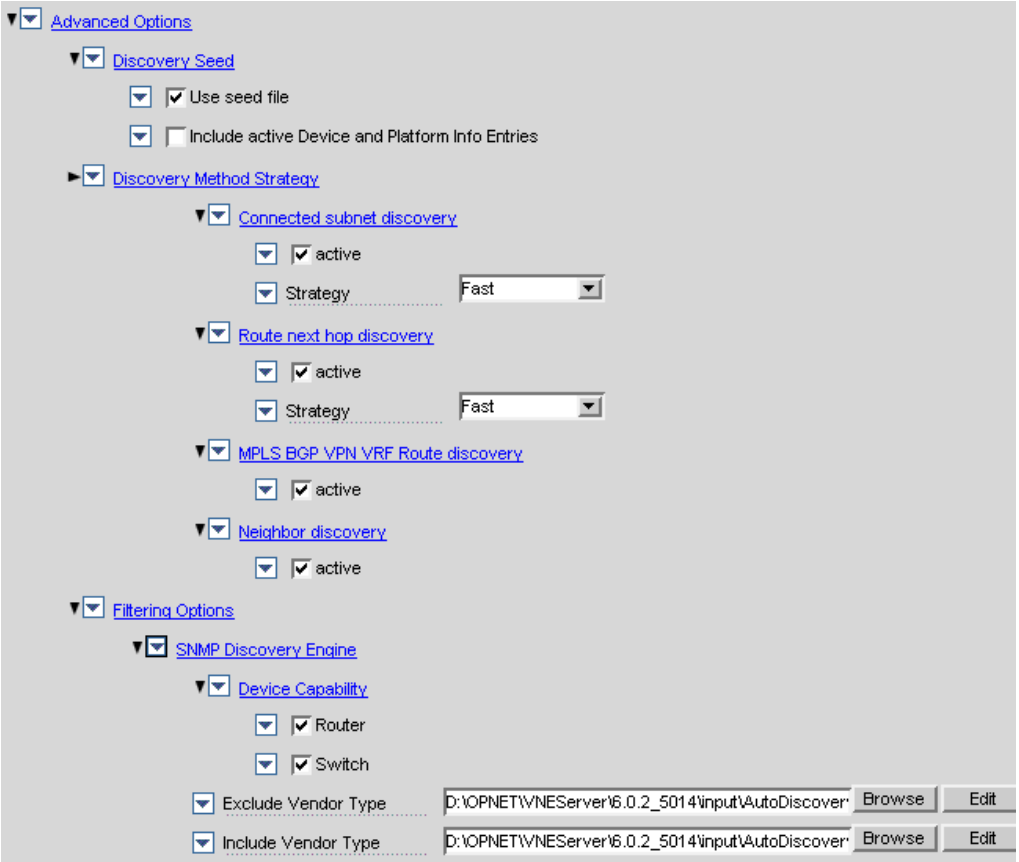


Table 3 Device and Platform Info Auto Discovery Advanced Options

Adapter Property	Description
Advanced Options	
Discovery Seed	Determines where the adapter obtains the seed(s) for the discovery process. The options are: • Use seed file • Include active Device and Platform Info Entries By default, the adapter uses the seed file.
Discovery Method Strategy> SNMP Discovery Engine	
Connected subnet discovery	active—Controls whether the engine examines the IpNetToMedia and ipAddrTable MIB tables to learn IP addresses/subnets to which the device is connected during the discovery process. By default this is active. Strategy—the strategy may be set to Fast or Exhaustive. The default is Fast. When set to Fast the discovery engine attempts to discover all IP addresses listed in the IpNetToMedia table. When the Exhaustive strategy is configured, the engine also enumerates IP subnets for configured interfaces on the device (learned from the ipAddrTable) and attempts to discover all IP addresses in connected subnets. Note: Setting the strategy to Exhaustive may increase the amount of time it takes for the discovery process however the increase is not expected to be significant.
Route next hop discovery	active—Controls whether the engine examines the ipRouteTable MIB Table to learn IP addresses from a discovered device's IP routing table. By default this is active. Disabling Route next hop discovery may yield incomplete discovery. Strategy—the strategy may be set to Fast or Exhaustive. The default is Fast. When strategy is set to Fast the discovery engine attempts to discover each IP address that is listed as a next hop in the IP routing table. When the Exhaustive strategy is configured, not only does the engine attempt to discover the next hop address, but also the remote destination subnet for each entry in the IP routing table. Note: Setting the strategy to Exhaustive will significantly increase the amount of time it takes for the discovery process. Warning: Querying a network device IP routing table will yield the most complete results for the discovery, however it can cause high CPU utilization.

Table 3 Device and Platform Info Auto Discovery Advanced Options (Continued)

Adapter Property	Description
MPLS BGP VPN VRF Route discovery active	active—Controls whether the adapter examines the mplsVpnVrfRoute MIB Table to learn IP addresses. By default this is active.
Neighbor discovery active	active—Controls whether the adapter examines the a vendor-specific MIB table that lists neighbor devices learned through Cisco Discovery Protocol (CDP) for Cisco device or Extreme Discovery Protocol (EDP) for Extreme devices. By default this is active.
Filtering Options> SNMP Discovery Engine	
Device Capability	Controls whether an entry is added to the Device and Platform Info table based on device capability of the device. In the default configuration Router and Switch are both selected.
Exclude Vendor Type Include Vendor Type	Specify file(s) containing sysObjectIDs that can be used to control whether an entry is added to the Device and Platform Info table based on the device vendor. Exclusion takes precedence over inclusion.
End of Table 3	

Tips for Optimizing SNMP Discovery

This section contains general tips for optimizing SNMP discovery of your network:

- Supply all community strings. Verify that the community strings file contains all of the community strings for your network.
- Make sure that discovery seed(s) are SNMP enabled and can be accessed from the Cisco Virtual Network Data Server host.
- If you run the SNMP Discovery engine's *Route next hop discovery*, run it with the fast strategy configured to minimize runtime.
- If you choose not run *Route next hop discovery,* run the *Connected subnet discovery* with the exhaustive strategy configured.
- Consider limiting discovery.
  - The SNMP discovery process takes longer when attempting to access IP addresses that are not active, and/or devices that are not SNMP-enabled or are outside of your management control. If you are running an unbounded discovery, consider limiting the discovery. If you have configured a discovery range, examine the Include and Exclude Files to ensure that the discovery is limited to network devices under your

management control and excludes devices such as servers and workstations. Depending on how your network is addressed, you may be able to create entries in the Include File to represent only active IP address ranges.

— Depending on the size of your network, rather than attempting to discover your entire network in one run, consider running the adapter multiple times to discover different components of your network and incrementally build entries in your Device and Platform Info table.

Reports

The following reports provide information about this Device and Platform Auto Discovery adapter:

- Device and Platform Info Auto Discovery Error Report—Lists errors encountered during the discovery process. Figure 9 provides an example of an SNMP access failure. In this example, a seed device could not be accessed because the correct community string for that device was not specified in the community string file.
- Device and Platform Info Auto Discovery Skipped IP Addresses Report—Provides a list of IP addresses learned through the SNMP discovery process but not accessed by the SNMP discovery engine due to boundaries placed on the discovery process through the use of an Include or Exclude File. See Figure 10 for an example report.
- Device and Platform Info Auto Discovery Neighbor Report—Contains the complete list of IP addresses learned from each device during the SNMP Discovery process. See Figure 11 for an example report.
- Device and Platform Info Auto Discovery Capability Report—Shows a list of devices discovered by the SNMP discovery engine and the corresponding device capability and indicates if a device was filtered (no device entry created in the Device and Platform Info Table) based on device capability. Devices that do not have router and/or switch capability are filtered because they are not supported by Cisco Virtual Network Data Server's direct collection adapters. (Note: This report will not have entries for devices that are skipped because their IP addresses are outside of the discovery range). Figure 12 provides an example. From this example, you can see that the adapter created device entries for all of the devices listed in this report except for the last, which it filtered based on device capability.

Figure 9 Device and Platform Info Auto Discovery Error Report

Device and Platform Info Auto Discovery Error

Row	Device Name	IP Address	Time Stamp	Error Type	
1	10.3.1.1	10.3.1.1	Thu Sep 27 12:34:40 EDT 2007	SNMP Request timed out or the authentication parameters set are incorrect	Please check if th

Figure 10 Device and Platform Info Auto Discovery Skipped IP Addresses Report

Device and Platform Info Auto Discovery Skipped IP Addresses

Row	Device Name	IP Address	Time Stamp	Comments
1	10.0.3.200	10.0.3.200	Tue Sep 25 15:16:16 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
2	10.0.3.3	10.0.3.3	Tue Sep 25 15:16:16 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
3	10.1.128.21	10.1.128.21	Tue Sep 25 15:15:57 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
4	10.1.128.22	10.1.128.22	Tue Sep 25 15:15:57 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
5	10.1.128.3	10.1.128.3	Tue Sep 25 15:15:57 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
6	10.2.12.1	10.2.12.1	Tue Sep 25 15:15:57 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
7	10.2.12.2	10.2.12.2	Tue Sep 25 15:15:57 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
8	10.3.10.1	10.3.10.1	Tue Sep 25 15:15:58 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
9			Tue Sep 25 15:16:16 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
10	10.3.10.10	10.3.10.10	Tue Sep 25 15:15:58 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
11			Tue Sep 25 15:16:16 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
12	10.3.10.5	10.3.10.5	Tue Sep 25 15:15:58 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
13			Tue Sep 25 15:16:16 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
14	10.3.10.9	10.3.10.9	Tue Sep 25 15:15:58 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.
15	10.3.2.1	10.3.2.1	Tue Sep 25 15:15:58 EDT 2007	Please update your include/exclude list if you think this IP Address should be discovered.

Figure 11 Device and Platform Info Auto Discovery Neighbor Report

Device and Platform Info Auto Discovery Neighbor

Row	System Name	Time Stamp	IP Address	Neighbor Name	Neighbor IP Address	Discovery Engine	Data Source
1	NYCCSACC02	Tue Sep 25 15:16:08 EDT 2007	10.3.1.8	10.3.1.1	10.3.1.1	SNMP Discovery Engine	ipNetToMediaTable
2			10.3.1.8	10.3.1.2	10.3.1.2	SNMP Discovery Engine	cdpTable
3			10.3.1.8	10.3.1.4	10.3.1.4	SNMP Discovery Engine	cdpTable
4			10.3.1.8	10.3.1.8	10.3.1.8	SNMP Discovery Engine	ipNetToMediaTable
5			10.3.1.8	172.18.0.110	172.18.0.110	SNMP Discovery Engine	ipNetToMediaTable
6			10.3.1.8	172.18.0.164	172.18.0.164	SNMP Discovery Engine	ipNetToMediaTable
7			10.3.1.8	192.168.12.185	192.168.12.185	SNMP Discovery Engine	ipNetToMediaTable
8			10.3.1.8	192.168.50.25	192.168.50.25	SNMP Discovery Engine	ipNetToMediaTable
9			10.3.1.8	192.168.50.26	192.168.50.26	SNMP Discovery Engine	ipNetToMediaTable
10			10.3.1.8	192.168.50.29	192.168.50.29	SNMP Discovery Engine	ipNetToMediaTable
11	NYCCSACC03		10.3.1.7	10.3.1.1	10.3.1.1	SNMP Discovery Engine	ipNetToMediaTable
12			10.3.1.7	10.3.1.2	10.3.1.2	SNMP Discovery Engine	cdpTable
13			10.3.1.7	10.3.1.4	10.3.1.4	SNMP Discovery Engine	cdpTable
14			10.3.1.7	10.3.1.7	10.3.1.7	SNMP Discovery Engine	ipNetToMediaTable
15			10.3.1.7	172.18.0.110	172.18.0.110	SNMP Discovery Engine	ipNetToMediaTable
16			10.3.1.7	172.18.0.164	172.18.0.164	SNMP Discovery Engine	ipNetToMediaTable
17			10.3.1.7	192.168.12.185	192.168.12.185	SNMP Discovery Engine	ipNetToMediaTable
18			10.3.1.7	192.168.50.26	192.168.50.26	SNMP Discovery Engine	ipNetToMediaTable
19			10.3.1.7	192.168.50.29	192.168.50.29	SNMP Discovery Engine	ipNetToMediaTable
20	NYCCSCOR01.lab.opnet.com	Tue Sep 25 15:15:57 EDT 2007	10.3.1.1	10.1.128.21	10.1.128.21	SNMP Discovery Engine	ipNetToMediaTable and ipRoute

Figure 12 Device and Platform Info Auto Discovery Capability Report

Device and Platform Info Auto Discovery Capability

Row	Device Name	Time Stamp	IP Address	Capability	Comments
1	NYCCSACC02	Thu Sep 27 12:21:21 EDT 2007	10.3.1.8	Switch-	
2	NYCCSACC03	Thu Sep 27 12:21:20 EDT 2007	10.3.1.7	Switch-	
3	NYCCSCOR01.lab.opnet.com	Thu Sep 27 12:21:13 EDT 2007	10.3.1.1	Switch-Router-Host-Server	
4	NYCCSCOR02	Thu Sep 27 12:21:23 EDT 2007	10.3.1.2	Switch-	
5	NYCCSCOR02-RSFC	Thu Sep 27 12:21:22 EDT 2007	10.3.1.3	Switch-Router-Host-Server	
6	NYCCSCOR03	Thu Sep 27 12:21:40 EDT 2007	10.3.1.4	Switch-	
7	NYCCSCOR03-RSFC	Thu Sep 27 12:21:22 EDT 2007	10.3.1.5	Switch-Router-Host-Server	
8	nam-blade	Thu Sep 27 12:21:17 EDT 2007	10.3.1.10	Host-Server	Device was filtered based on its capability

Troubleshooting

This section contains troubleshooting tips for the Device and Platform Info Auto Discovery adapter.

If the adapter does not discover any devices

- Ensure that discovery seed(s) are configured
- Verify that discovery seed(s) can be accessed via SNMP
  - — Ensure that SNMP is enabled on undiscovered device(s)
  - — Ensure that SNMP (default SNMP port is 161) is not blocked between Cisco Virtual Network Data Server and the device(s)
  - — Verify that community string(s) for undiscovered device(s) is present in community strings file
  - — Check SNMP timeouts to ensure they are not too low for the network
  - — Use a MIB browser to determine if undiscovered devices can be accessed via SNMP

If the adapter does not discover a specific device or set of devices that is known to exist

- Verify that device(s) can be accessed via SNMP
  - — Ensure that SNMP is enabled on undiscovered device(s)
  - — Ensure that SNMP (default SNMP port is 161) is not blocked between Cisco Virtual Network Data Server and the device(s)
  - — Verify that community string(s) for undiscovered device(s) is present in community strings file
  - — Check SNMP timeouts to ensure they are not too low for the network
  - — Use the MIB browser packaged with Cisco Virtual Network Data Server (vnes.bat mib_browser) to determine if undiscovered devices can be accessed via SNMP
- Check to see if IP address is being skipped
  - — Ensure that the IP address for undiscovered devices are within the discovery range as specified by the Include and Exclude Files.

If adapter does not create any entries in Device and Platform Info table

- SNMP discovery may not have discovered any routers or switches
- Filtering (device capability or vendor) may be misconfigured

Related Adapters

After you discover your network using the Device and Platform Info Auto Discovery adapter you have created device entries in the Device and Platform Info table. The amount of information supplied in each device entry depends on the discovery engine that created the entry. (See Device Entries Created in Device and Platform Info Table on page 43 for details.)

If you are preparing to run the Device Config File Collection adapter, run the following adapters in the order shown to provide additional information in the device entries that is required for successful CLI collection:

- Direct Device Connection Diagnosis—Tests reachability via telnet/SSH and sets Access Method for entries in Device and Platform Info table. In default adapter configuration, the Active and Collect Config flags must be checked if you want this adapter to run telnet/ssh tests and set the Access Method for the device entry. Alternatively you can run the adapter in Custom mode and configure it to set the Collect Config flag and Access Method based on whether the device is reachable. See the Cisco Virtual Network Data Server online documentation for more information on configuring this adapter.
- Device and Platform Info Auto Configuration—Sets Login Script and Vendor Type for entries in Device and Platform Info table. You must provide username, password, and/or privileged password (as needed) in each device entry prior to running the Device and Platform Info Auto Configuration adapter in order for the adapter to determine Login Script and Vendor. You can provide this information by editing the Device and Platform Info table directly or if you have a common credentials, you may specify this in the user credentials file for this adapter. See the Cisco Virtual Network Data Server online documentation for more information on configuring this adapter.

Alcatel 5620 SAM-O Network Import

The Alcatel 5620 Service Aware Manager (SAM) is a suite of management applications for managing IP, Ethernet, and MPLS-based data networking services. Cisco Virtual Network Data Server interfaces with the Alcatel 5620 SAM via the SAM open interface (SAM-O). SAM-O provides an XML interface for applications to interact with the Alcatel 5620 SAM.
Cisco Virtual Network Data Server uses SOAP to send XML request to the Alcatel 5620 SAM and receive the XML reply.

Cisco Virtual Network Data Server integrates with the Alcatel 5620 SAM v5.0, build R1.

The Alcatel 5620 SAM-O Network Import adapter obtains device data from the Alcatel 5620 SAM by interfacing with the SAM-O through SOAP requests. Cisco Virtual Network Data Server obtains data from SAM-O in XML format. The adapter does not obtain device config files. Therefore when importing from Cisco Virtual Network Data Server into Cisco analysis software, configs are not available for devices whose device data is provided by this adapter.

Key Concept—This adapter collects and imports device and interface configuration data and physical link information from the Alcatel 5620 SAM-O network management system. The collected data is in XML format.

The Alcatel 5620 SAM-O Network Import adapter collects and imports data for the following device types:

- Alcatel 7450 Ethernet Service Switch (ESS)
- Alcatel 7550 and Alcatel 7710 Service Router (SR)

The Alcatel 5620 SAM provides the following data:

- device information including node-level routing protocol configuration
- interface information including interface-level routing protocol configuration
- physical links

Adapter Operation

The adapter operates by sending a series of XML/SOAP requests to the Alcatel 5620 SAM through SAM-O, then parsing the SOAP responses. It executes a series of queries to obtain a list of devices and groups managed in the Alcatel 5620 SAM and then it requests data for specified devices or groups (as defined by the device filter configured for the adapter). The adapter logs both the

requests it sends to the SAM-O service and the responses. Then the adapter processes the SAM responses and produces a
Cisco Virtual Network Data Server XML file for each device and one containing physical links. These Cisco Virtual Network Data Server XML files are then imported by VNE-XML import.

The adapter supports the following modes of operation:

- live—Adapter accesses SAM server via SAM-O and initiates export of device and link data.
- local files—Adapter imports data previously collected from SAM-O server. This mode is intended to support troubleshooting operations only and/or to import the most recently collected files in the event that you needed to delete one or more devices that were populated with data from this adapter. This mode is not intended to support the import of files exported from Alcatel 5620 SAM by a method other than live connection to the SAM-O server by this adapter.

This following topics are covered in the sections that follow:

- Requirements on page 65
- Workflow on page 65
- Configuration Properties for Alcatel 5620 SAM-O Network Import on page 70
- Troubleshooting on page 73
- Related Adapters on page 74

Requirements

This section lists requirements for the Alcatel 5620 SAM-O Network Import adapter:

- The SAM server must have a SAM-O license
- The SAM-O module must be reachable from
Cisco Virtual Network Data Server via HTTP (default port is 8080)
- You must provide an account that Cisco Virtual Network Data Server can use to log into the Alcatel 5620 SAM. The account must have an OSS management role that permits reading the Alcatel 5620 SAM data through SAM-O.

Workflow

1) Review Requirements on page 65

2) Gather Information on page 66

3) Verify Login to Alcatel 5620 SAM on page 66

4) Configure Required Properties on page 66

5) Configure Collection of Chosen Devices on page RN-69

See Related Adapters on page 74.

Gather Information

You will need the following information:

- hostname or IP address of the target Alcatel 5620 SAM
- username and password to log into Alcatel 5620 SAM (see Requirements on page 65 for the permission level required for this account)
- port on which Alcatel 5620 SAM runs on the target server (or should this be "port on which Alcatel 5620 SAM-O service runs on the target server"

Verify Login to Alcatel 5620 SAM

Verify the username and password permit you to login to the Alcatel 5620 SAM. You can do this by logging into an Alcatel 5620 SAM client user interface installed on any host (does not need to be installed on Cisco Virtual Network Data Server host.)

Configure Required Properties

Follow Procedure 5 to configure required properties for this adapter. See Configuration Properties for Alcatel 5620 SAM-O Network Import on page 70 for a description of adapter properties.

Procedure 5 Configure Required Properties for Alcatel 5620 SAM-O Network Import

1. Open the Cisco Virtual Network Data Server Web Console > Mgmt page and select the Adapter Resources tab.
2. Expand the Alcatel 5620 SAM-O Network Import folder.
3. Set the sourceList > live > active property to "true."
4. Configure the following:
   - sourceList > live > hostName
   - sourceList > live > port
   - sourceList > live > user
   - sourceList > live > password
   - sourceList > live > clientID

5 Click the **OK** button to save your changes.

End of Procedure 5

Test Adapter

Follow Procedure 6 to verify correct adapter operation by collecting data for a single device.

Note—See Troubleshooting on page 73 for assistance if you encounter issues.

Procedure 6 Test Collection For a Single Device

1 Configure required properties (Procedure 5).

2 Obtain the siteID for a device that is managed in the Alcatel 5620 SAM. Make sure the device you select is one of the device types that the adapter collects from Alcatel 5620 SAM.

3 Open the Cisco Virtual Network Data Server Web Console > Mgmt page and select the Adapter Resources tab.

4 Expand the Alcatel 5620 SAM-O Network Import folder.

5 Set the sourceList > live > SAM5620-Devices > Filter Devices? property to “true.”

6 Set the sourceList > live > SAM5620-Devices > Device Filter > Filter Type to “Include.”

7 Type the siteID you obtained in step 2 into the text field for the following property:

sourceList > live > SAM5620-Devices > Device Filter > siteIDs(comma’,’ delimited).

8 Click the OK button to save your changes.

9 Run the adapter.

10 View the event log messages while the adapter is running and examine adapter statistics when it completes.

11 Confirm that data was collected for the device and imported into Cisco Virtual Network Data Server.

End of Procedure 6

When the adapter successfully contacts the Alcatel SAM-O service and obtains data for one device, adapter statistics look similar to Figure 13.

Figure 13 Adapter Statistics

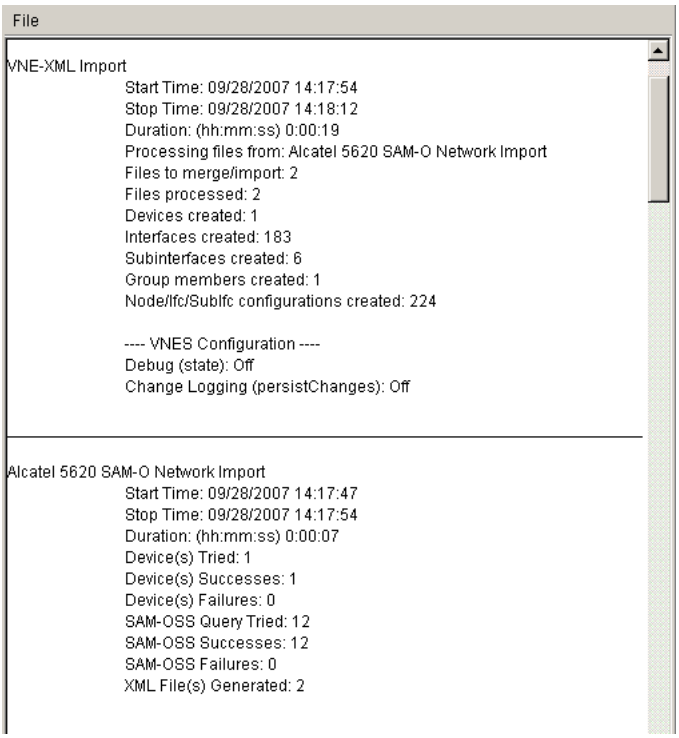
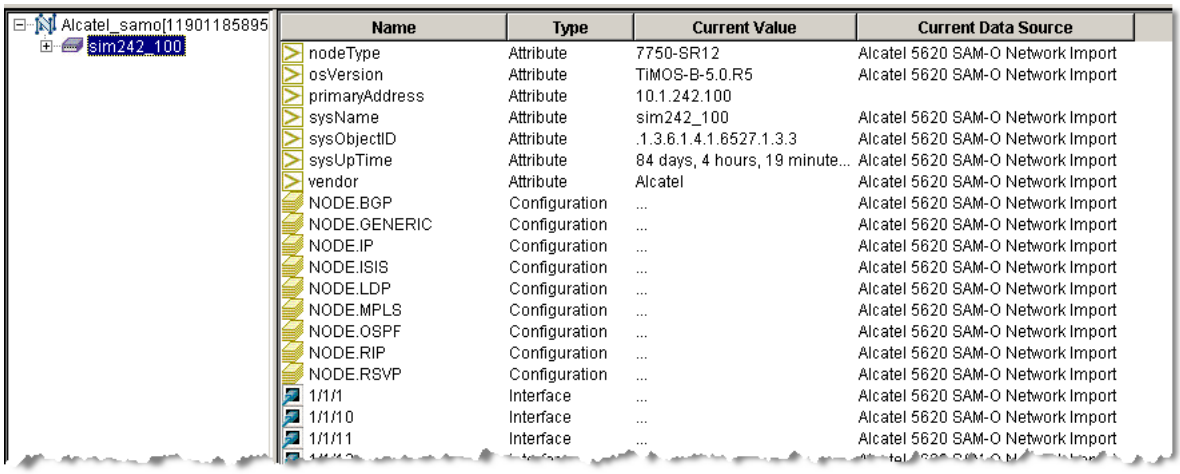


Figure 14 provides an illustration of device data imported by the Alcatel 5620 SAM-O Network Import adapter.

Note—The Alcatel 5620 SAM data may contain one or more non-loopback logical ports that do not have a physical port assigned to it. An interface like this is not a functioning port in the Alcatel 5620 SAM and is not modeled in Cisco software. When Cisco Virtual Network Data Server encounters this type of interface during import, it skips it and writes a message to the event log.

Figure 14 Device Data Imported by Alcatel 5620 SAM-O Network Import Adapter



Name	Type	Current Value	Current Data Source
nodeType	Attribute	7750-SR12	Alcatel 5620 SAM-O Network Import
osVersion	Attribute	TiMOS-B-5.0.R5	Alcatel 5620 SAM-O Network Import
primaryAddress	Attribute	10.1.242.100	
sysName	Attribute	sim242_100	Alcatel 5620 SAM-O Network Import
sysObjectID	Attribute	.1.3.6.1.4.1.6527.1.3.3	Alcatel 5620 SAM-O Network Import
sysUpTime	Attribute	84 days, 4 hours, 19 minute...	Alcatel 5620 SAM-O Network Import
vendor	Attribute	Alcatel	Alcatel 5620 SAM-O Network Import
NODE.BGP	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.GENERIC	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.IP	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.ISIS	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.LDP	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.MPLS	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.OSPF	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.RIP	Configuration	...	Alcatel 5620 SAM-O Network Import
NODE.RSVP	Configuration	...	Alcatel 5620 SAM-O Network Import
1/1/1	Interface	...	Alcatel 5620 SAM-O Network Import
1/1/10	Interface	...	Alcatel 5620 SAM-O Network Import
1/1/11	Interface	...	Alcatel 5620 SAM-O Network Import

Configure Collection of Chosen Devices

You can configure Cisco Virtual Network Data Server's Alcatel 5620 SAM-O Network Import adapter to retrieve data for all of the managed devices in the target Alcatel 5620 SAM or you can create a device filter whereby you include or exclude one or more device and/or group.

The Alcatel 5620 SAM assigns a unique identifier called a siteID to each managed device. Additionally, devices in Alcatel 5620 SAM may be organized into groups. If you want to specify the devices for which Cisco Virtual Network Data Server will retrieve data, you must examine the devices that are managed in the Alcatel 5620 SAM and decide which of the devices you wish to include in the Cisco Virtual Network Data Server collection.

Note—To include or exclude a group of devices, you must first create that group in the target Alcatel 5620 SAM. See Configuration Properties for Device and Platform Info Auto Discovery on page 54 for a description of adapter properties.

When importing data from Alcatel 5620 SAM you can configure the Alcatel 5620 SAM-O Network Import adapter to include or exclude devices based on siteID and/or group name. If you configure the device filter to include device siteIDs and group names, the adapter collects and imports device data for the specified devices and all devices that are members of the specified group(s). Similarly, if you configure the device filter to exclude device siteIDs and group names, all will be excluded from collection and import.

Note—Only one device filter may be configured per Alcatel 5620 SAM server.

Configuration Properties for Alcatel 5620 SAM-O Network Import

The following are covered in this section:

- General properties
- Live properties
- Local files properties

The configuration properties for this adapter are illustrated in Figure 15, Figure 16, and Figure 17. They are listed in Table 4.

Figure 15 Alcatel 5620 SAM-O Network Import—General Properties

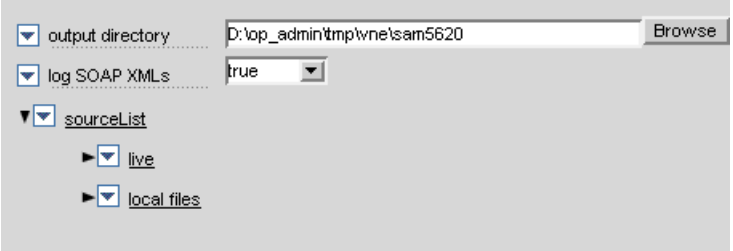


Figure 16 Alcatel 5620 SAM-O Network Import Properties—Live Server

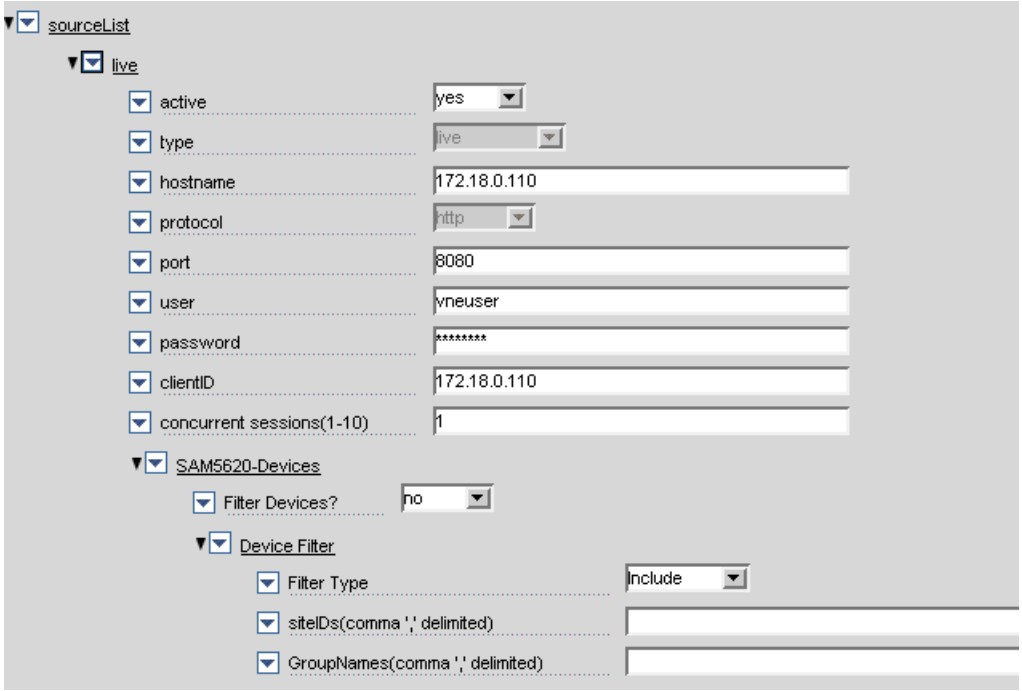


Figure 17 Alcatel 5620 SAM-O Network Import Properties—Local Files

Table 4 Alcatel 5620 SAM-O Network Import Properties

Adapter Property	Description
output directory	Points to the directory on the Cisco Virtual Network Data Server host where this adapter writes output. The default is <tempdir>\sam5620. Output can include the raw data retrieved from the 5620 SAM server(s) (requests and responses between the adapter and SAM) as well as the adapter-generated XML files that are ready for import.
log SOAP XMLs	Controls whether the adapter stores each request to and response from 5620 SAM server(s). These files are very useful for troubleshooting. Files are stored in \log folder in the output directory. A separate folder is created for each Alcatel 5620 SAM server that the adapter contacts and general requests and responses are stored at this level. Within each Alcatel 5620 SAM server folder, requests and responses are stored separately by SiteID for each device. Options are true or false. By default this is true.
sourceList> live	
active	Controls whether data is collected from this source.
type	Displays the source type—live. This property is display only and may not be modified.
hostname	(REQUIRED) Specifies the hostname or IP address of the Alcatel 5620 SAM server.
protocol	Specifies the protocol that Cisco Virtual Network Data Server uses to connect to the Alcatel 5620 SAM server. In this release, the adapter only supports HTTP, therefore this property is read only and may not be modified.
port	(REQUIRED) Specifies the port on which Cisco Virtual Network Data Server connects to the Alcatel 5620 SAM-O service. The default is 8080.
user password	(REQUIRED) User account and password for Cisco Virtual Network Data Server to log into the Alcatel 5620 SAM server.
clientID	(REQUIRED) Identifier included in Cisco Virtual Network Data Server SOAP requests sent to the SAM-O service. Identifies the client requesting the data from SAM. Must be a unique text string. W recommend that you use the IP address of the Cisco Virtual Network Data Server host.

Table 4 Alcatel 5620 SAM-O Network Import Properties (Continued)

Adapter Property	Description
concurrent sessions(1-10)	Controls the number of concurrent SOAP requests that the adapter sends to the Alcatel 5620 SAM server. The default is 1. Increasing this value can speed adapter runtime. WARNING: The maximum concurrent SOAP requests for the Alcatel 5620 SAM is 10. However, since the SAM will likely have clients other than Cisco Virtual Network Data Server, we do not recommend setting this to a value greater than 5.
sourceList> live> SAM5620-Devices	
Filter Devices? Device Filter	Controls whether the adapter requests device data for all devices OF THE SUPPORTED TYPES from the Alcatel 5620 SAM server. The options are “yes” or “no.” The default is “no” which means that the adapter requests data for all devices managed in the SAM server. When the Filter Devices property is set to “yes” the Device Filter property tree determines the device(s) for which the adapter requests data. Note: Only one device filter may be specified. Filter Type—Include or Exclude. siteIDs(comma ’,’ delimited)—Identifies one or more devices in the Alcatel 5620 SAM. The values specified here must exactly match the siteIDs used to identify the devices in the Alcatel 5620 SAM. Specify multiple devices by separating them with a comma. If a siteID does not exist in the SAM, the adapter writes a message to the event log. GroupNames(comma ‘,’ delimited)—Identifies one or more groups. The values specified here must exactly match the GroupNames used in the Alcatel 5620 SAM. Specify multiple groups by separating them with a comma. If a groupID does not exist in the SAM, the adapter writes a message to the event log.
sourceList> local files	
active	Controls whether data is imported from this source. For more information about importing local files, see Adapter Operation on page 64.

Table 4 Alcatel 5620 SAM-O Network Import Properties (Continued)

Adapter Property	Description
type	Displays the source type—local files. This property is display only and may not be modified.
Input Directory	Points to the location of input files for the adapter to import. The default is <tempdir>\sam5620\log
Filename Filter	Controls which files are imported. When the adapter logs SOAP XML files during a live connection to the Alcatel 5620 SAM, both the adapter requests and SAM-O responses are stored. The filename filter is applied to the stored files so that only the SAM-O responses are imported.
End of Table 4	

Troubleshooting

This section contains tips for troubleshooting the Alcatel 5620 SAM-O Network Import adapter. Event log messages are the best source of information for troubleshooting this adapter.

If the adapter did not successfully connect to the Alcatel 5620 SAM-O service, you will see a Failed SOAP XML ping message in the event log. Examine the detailed data in the event log message to determine the cause:

- Server hostname may be incorrect
  - Error msg: Failed SOAP_XML_PING SAM 5620 server: http://<host>:8080//xmlapi/invoke, failure reason: Exception in sending/parsing SOAP request: java.net.UnknownHostException: <host>
  - To confirm that this is the issue, open a command window and try to ping the host. The manual ping should also fail.
- Server port may be incorrect
  - Error msg: Failed SOAP_XML_PING SAM 5620 server: http://<host>:8081//xmlapi/invoke, failure reason: Exception in sending/parsing SOAP request: java.net.ConnectException: Connection refused: connect
- Username/password may be incorrect
  - Error msg: Failed SOAP_XML_PING SAM 5620 server: http://<host>:8080//xmlapi/invoke, failure reason: SOAP fault response: SOAP Fault - Fault code: SOAP:Client, Fault string: Login failure., requestId: null
  - To confirm that this is the issue: Use Alcatel 5620 SAM client GUI to login using username/password

- User account may not have needed privileges to obtain data from the Alcatel 5620 SAM server
  - Error msg: Failed SOAP_XML_PING SAM 5620 server: http://<host>:8080//xmlapi/invoke, failure reason: SOAP fault response: SOAP Fault - Fault code: SOAP:Client, Fault string: Users require OSS Management privileges to use SAM-O, requestId: null

If the adapter did not retrieve any device data

- Verify that there are devices managed in the Alcatel 5620 SAM server
- If the Device Filter is enabled, check the filter settings.
  - If the Filter Type is “Include” either no siteIDs/groupNames were specified or the specified values do not exist on the Alcatel 5620 SAM server
  - If the Filter Type is “Exclude” the excluded siteIDs/GroupNames match all devices managed in the Alcatel 5620 SAM server

Related Adapters

The Alcatel 5620 SAM-O Network Import adapter imports MPLS configuration data from the Alcatel 5620 SAM. You will not find MPLS LSPs in Cisco Virtual Network Data Server database until you run Link and Connection Inference. Run Link and Connection Inference with the MPLS engine enabled in order to infer MPLS connections in Cisco Virtual Network Data Server.

Publishing to Secure Cisco Report Server

A secure Cisco Report Server is one that has been configured to run HTTPS. In order for a Cisco Virtual Network Data Server to publish reports to a secure Cisco Report Server, the Cisco Report Server public certificate must be present in the Cisco Virtual Network Data Server trust store. Follow Procedure 7 to prepare a Cisco Virtual Network Data Server to publish reports to a secure Cisco Report Server.

Note—You must perform Procedure 7 for each Cisco Virtual Network Data Server that publishes to the secure Cisco Report Server and you must repeat the procedure if the Cisco Report Server public certificate changes.

Procedure 7 Prepare Cisco Virtual Network Data Server to Publish to Secure Cisco Report Server

1 Export the public certificate from the Cisco Report Server to a file.

1.1 Open a command prompt on the Cisco Report Server host and change directories to the following directory:
<Cisco Report Server_install_dir>\jakarta\bin\scripts

1.2 Export the Cisco Report Server public certificate.

Run the appropriate command based on certificate type:

- If Cisco Report Server uses a self signed certificate then use the following command: https_setup.bat /format rfc /export_cert servercert
- If Cisco Report Server uses a CA signed certificate then use the following command: https_setup.bat /format rfc /export_cert cacert

➥ The certificate exports to a file in the Cisco Report Server security directory. The command output provides the location of the file.

2 Copy the Cisco Report Server public certificate file (*.der) generated in step 1 from the Cisco Report Server host to the security directory for the Cisco Virtual Network Data Server software on the Cisco Virtual Network Data Server host. The default location of the security directory is: <install_dir>\security. For example, C:\Cisco\security.

3 Import the Cisco Report Server public certificate file to the Cisco Virtual Network Data Server trust store.

3.1 Open a command prompt on the Cisco Virtual Network Data Server host and navigate to the Cisco Virtual Network Data Server release directory. For example, C:\Cisco\VNDServer\<version_build>.

3.2 Import the Cisco Report Server public certificate.

Run the appropriate command based on the Cisco Report Server certificate type:

- If Cisco Report Server uses a self signed certificate then use the following command: vnes.bat /keytool “import -alias rscert -file <cert>”
  where <cert> is the full path and filename of the Cisco Report Server public certificate that you copied to the Cisco Virtual Network Data Server host in step 2.

  Example:

  vnes.bat /keytool “import -alias rscert -file C:\Cisco\security\rscert.der”

- If Cisco Report Server uses a CA signed certificate then use the following command: vnes.bat /keytool importcacert

End of Procedure 7

Format of Device Info File

This appendix describes the format and required fields for the device info file. The device info file is a text file that you can import into Cisco Virtual Network Data Server to create device entries in the Device and Platform Info table.

Note—See the online documentation for instructions on generating a starter file that contains required header information and column headers.

Header The following header information must be present at the top of the file:
// VNE Server VERSION 4.0

Delimiter Valid field delimiters are tab, comma, and semicolon.

Fields Except for the `isActive` field, the fields match the display order in the Device and Platform Info window. The `isActive` field displays under the heading **Active** in the Device and Platform Info window (immediately to the right of the device name).

Each entry in the device info file must contain mandatory fields in order for the device entry to be imported into the Device and Platform Info table. Mandatory fields are shown in bold text in the following list.

Note—When importing the device info file, Cisco Virtual Network Data Server skips an entry if it does not contain all mandatory fields or if it is considered to be a duplicate (based on nodeName or hostAddress).

- **deviceId**—(hidden field) Set this to 0 for each new device entry that you are adding to the Device and Platform Info table so that Cisco Virtual Network Data Server generates a unique deviceId when it imports the entry. Use caution when you are updating existing entries in the Device and Platform Info table through file import. Each device entry in the Device and Platform Info table has a unique deviceId. When you export the Device and Platform Info table to a file, Cisco Virtual Network Data Server writes existing device entries—each with an assigned deviceId—to a text file. You must retain these assigned deviceIds.

WARNING—DO NOT modify the deviceId for an existing device entry.

- **userId**—(hidden field) set this to 1 for all devices
- **nodeName**—hostname of the device. This must be unique for each entry.
- **hostAddress**—network address used to access the device. This must be unique for each entry.

- **mergeID**— unique string or “none”
- **userName**—username used to login to the device or “none”
- **password**—password used to login to the device or “none”
- **privilegedPassword**—password for privileged exec mode or “none”
- **commString**—SNMP community string or “none”
- **vendorType**— device vendor or vendor subtype defined in adapter resources for the Device Config File Collection adapter or “unknown”
- **loginScript**—login script defined in adapter resources for the Device Config File Collection adapter or “unknown”
- **isActive**—(TRUE | FALSE) globally activates a device
- **isActiveDCFC**—(TRUE | FALSE) activates a device for Device Config File Collection (isActive must be set for this flag to be read)
- **isActiveDMCI**—(TRUE | FALSE) activates a device for Device MIB Configuration Import (isActive must be set for this flag to be read)
- **isActiveMIUI**—(TRUE | FALSE) activates a device for MIB Interface Utilization Import (isActive must be set for this flag to be read)
- **accessMethod**—0 (Unknown), 1 (TELNET), 2 (SSHv1), or 3 (SSHv2). The integer mapping for the accessMethod field changed to this scheme in Release 4.0.
- sysName—System Name by which the device is known in the Cisco Virtual Network Data Server database. Leave this field blank when you create new device entries. Do not modify values for exported device entries.
- v3userName—SNMPv3 User Name
- contextID—SNMPv3 Context ID
- contextName—SNMPv3 Context Name
- v3AuthProt—SNMPv3 Authentication Protocol
- v3SecurityLevel—SNMPv3 Security Level
- v3AuthPassword—SNMPv3 Authentication Password
- v3PrivProt—SNMPv3 Privacy Protocol
- v3PrivPassword—SNMPv3 Privacy Password
- comments

Resolved Problems

Release 2.1 includes enhancements that address the following software problem reports (SPRs) from previous releases:

Table 1 SPRs Fixed in Cisco Virtual Network Data Server Release 2.1

SPR ID	Problem Description
105063	Device Config File Import adapter does not import legitimate Juniper Config file.
103330	CAM inference does not pick up link between router and switch.
103081	Running Link and Connection Inference after the ASCII Import adapter turns links created by linkInfo.txt into clouds.
102664	Device Version Import adapter does not bring in system uptime information for Cisco Wireless Access Points.
102524	New attribute needed for the Cisco processor board ID.
102227	Need to apply fix for SPR 102177 to all other Cisco IOS-XR lexers.
102066	Ciscoworks CMF access does not get correct access.
101833	On Juniper devices, Cisco VNDS ignores a “down” interface that comes “up” and vice-versa.
101750	Link inference infers bogus ethernet clouds for Juniper aggregate ethernet interfaces.
101547	The error message generated when the Netflow Import adapter fails to connect to a server is wrong.
101545	CDP engine creates links between tunnel interfaces.
101338	Passport 8k configs are not parsed if they are missing the “cli prompt” command.
101035	XML-Import times increasing after each cycle.
100555	Device and Platform Info Auto Configuration adapter generates wrong User_pwd_Priv script.
100047	Cisco VNDS merges PIX ACL entries incorrectly.
99368	The Device and Platform Info adapter shows empty table when the Web Console is used.
99351	Import Adapters should be able to distinguish empty files from invalid files.
99307	Link Inference containment engine does not work for dual Cisco FWSM with the same sysName

Table 1 SPRs Fixed in Cisco Virtual Network Data Server

SPR ID	Problem Description
104624	[Cisco IOS XR] OSPF interface information not populated if the 'address-family' command is present in the config file.
103743	ifType is not set on Cisco FWSM created by CFI.
102177	Cisco IOS-XR skips BGP data when preceded by line that starts with “! # devicename”
101239	[Cisco IOS-XR] Need to support new format for the command used to create static routes.
100896	DCFI (IOS-XR): Interfaces falsely detected as not participating in ISIS routing.
100476	Alterpoint adapter collected files that used the wrong prompt for devices running CatOS.
100282	Cisco NCM Collection Report does not display due to case mismatch between requesting string and filename. [Linux]
99560	Opsware NAS adapter ignores some devices in a group—they are collected if specified separately in “Collect from devices.”
102075	CiscoWorks RME adapter gets wrong userField data for CWALIAS.
100819	Opsware adapter cannot collect from groups that have spaces in their group name.
99879	Cannot see the Devices table through Web GUI.
100506	Cisco “ip route” entries that include “#” for comments are skipped
103323	Operational priority is not parsed from show standby output of cisco routers.
100201	Cisco VNDS collection does not collect from Juniper NetScreen devices.
End of Table 1	

Known Issues

This release contains the known issues listed in Table 2.

Table 2 Known Issues in Cisco Virtual Network Data Server Release 2.1

SPR ID	Problem Description
105903	Unable to run the product on Solaris machines that do not have libgcc.
101346	Adapter Collection report reaches maximum java memory setting.
101912	Database aging does not delete empty Service Configs.
103264	The Network Browser is slow to refresh node information when you select all columns under “preferences.”
103774	[Web GUI-Mgmt Console-Adapter Resources] Some copy/paste operations should not be able to write to certain folders.
103881	Devices with a large number of interfaces or subinterfaces may cause an out-of-memory exception and fail to import.
104029	The Cisco VNDS Export Service should honor traffic priorities for its exports—even if a filter other than “All” is used to import from Cisco VNDS.
106474	Link Inference generates an out of memory exception when running against a large data set (over 10 000).
107737	XML-Import generates “duplicate key violates unique constraint”' error message.
107942	Importing from Cisco VNDS via LUS is significantly slower than importing from Cisco VNDS via Corba.
End of Table 2	