Installation Guide for Cisco Configuration Assurance Solution–SP

Version 2.0

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number: OL-11353-01

Installation Guide for Cisco Configuration Assurance Solution–SP

CONTENTS

Preface

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number "DOC-DOCDVD=") from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non emergencies.

- Non emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco

service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Planning Your Installation

Cisco Configuration Assurance Solution–SP is a combination of integrated software programs:

- Cisco Audit and Analysis–SP—Performs systematic configuration audits of enterprise-class and service-provider-class networks, analyzing an up-to-date model of the production network to diagnose device misconfigurations, policy violations, inefficiencies, and security gaps. Hundreds of standard checks incorporate industry best practices. Users are notified about critical issues and comprehensive results are published to an integrated web-based report server.
- Cisco Report Server—Provides a web-based central repository for reports produced by the Cisco Audit and Analysis–SP engine.
- Cisco Virtual Network Data Server—Enables the creation of a high-fidelity network model based on configuration, topology, and traffic information.

The Cisco Configuration Assurance Solution–SP package contains multiple installation CDs for the software, models, documentation, and other components of this solution.

Installation Workflows

There are several possible workflows for installing Cisco CAS–SP, depending on your situation:

- First-Time Installation, page 1-2—use this workflow to install Cisco CAS–SP for the first time.

- Update Installation (Windows Only), page 1-3—use this workflow to update a previous version of Cisco CAS–SP to the current version.

First-Time Installation

You should perform a first-time installation only if no prior version of Cisco CAS–SP is installed.

Note Cisco recommends that you do the steps in the order listed in Table 1-1.

Table 1-1 First-Time Installation: Workflow

	Description	Reference
Step 1	Register your Cisco Solution product	Registering Your Cisco Solution Product, page 1-5
Step 2	Determine the host computers	Determining Installation Options, page 1-6
Step 3	Determine the licensing options	Product Licensing, page 1-7
Step 4	Verify system requirements	Cisco Audit and Analysis–SP: System Requirements, page 2-2 Cisco Virtual Network Data Server: System Requirements, page 3-1 Cisco Report Server: System Requirements, page 2-3
Step 5	Install Cisco Audit and Analysis–SP	*Windows:* • Installing Cisco Audit and Analysis–SP (Windows), page 4-1 *Linux:* • Installing Cisco Audit and Analysis–SP (Linux), page 4-3 • Setting Up Cisco Audit and Analysis–SP to Run Automation Tasks (Linux), page 4-5

Table 1-1 First-Time Installation: Workflow (continued)

	Description	Reference
Step 6	Install Cisco VNDS	Installing Cisco Virtual Network Data Server (Windows), page 5-1 Installing Cisco Virtual Network Data Server (Linux), page 6-1
Step 7	Install Cisco Report Server	Installing Cisco Report Server (Windows), page 7-1 Installing Cisco Report Server (Linux), page 7-4
Step 8	Add licenses for: • Cisco Audit and Analysis–SP • Cisco VNDS • Additional product modules (if any)[1]	Adding a License, page 9-3
Step 9	Configure node pack licenses (if any)	Configuring Node Pack Licenses and Notifications, page 9-5
Step 10	Update the Product Options list for additional product modules (if any)	Adding a Module to the Product Options List, page 9-6

1. If you have licenses for any additional product modules, you must add these licenses and add the modules to your Product Modules list.

Update Installation (Windows Only)

You should perform an update installation if you already have a previous version of Cisco CAS–SP installed.

Release 2.0 is backward-compatible with earlier releases. Most data from your existing installation can be migrated transparently to release 2.0, including:

- Network models
- Automation tasks

Cisco Report Server reports can be migrated by using a single menu operation.

Warning **When updating from an earlier Cisco Virtual Network Data Server release, you must configure the Oracle database by running the setup_accounts script (`@setup_accounts.sql`). This means that you must re-create the network database. Network models created by previous releases cannot be retained by this release.**

Note Cisco recommends that you perform the steps in the order listed in Table 1-2.

Table 1-2 Update Installation: Workflow

	Description	Reference
Step 1	Verify system requirements	Cisco Audit and Analysis–SP: System Requirements, page 2-2 Cisco Virtual Network Data Server: System Requirements, page 3-1 Cisco Report Server: System Requirements, page 2-3
Step 2	Install current release of Cisco Audit and Analysis–SP	*Windows:* • Installing Cisco Audit and Analysis–SP (Windows), page 4-1 *Linux:* • Installing Cisco Audit and Analysis–SP (Linux), page 4-3 • Setting Up Cisco Audit and Analysis–SP to Run Automation Tasks (Linux), page 4-5
Step 3	Install current release of Cisco VNDS	Installing Cisco Virtual Network Data Server (Windows), page 5-1 Installing Cisco Virtual Network Data Server (Linux), page 6-1
Step 4	Install current release of Cisco Report Server	Installing Cisco Report Server (Windows), page 7-1 Installing Cisco Report Server (Linux), page 7-4
Step 5	Refresh licenses	Upgrading a License, page 9-4

Table 1-2 Update Installation: Workflow (continued)

	Description	Reference
Step 6	Configure node pack licenses (if any)	Configuring Node Pack Licenses and Notifications, page 9-5
Step 7	(*Optional*) Migrate existing Cisco Report Server reports	Migrating Data from a Previous Installation, page 7-5
Step 8	(*optional*) Remove previous release of Cisco Audit and Analysis–SP	Uninstalling Cisco Audit and Analysis–SP (Windows), page 10-1 Uninstalling Cisco Audit and Analysis–SP (Linux), page 10-6
Step 9	(*optional*) Remove previous release of Cisco VNDS	Uninstalling Cisco VNDS (Windows), page 11-3 Uninstalling Cisco VNDS (Linux), page 11-8
Step 10	(*optional*) Remove previous release of Cisco Report Server	Uninstalling Cisco Report Server (Windows), page 12-1

Registering Your Cisco Solution Product

Before you can install Cisco CAS–SP, you must register your product with Cisco Systems, Inc. After you register your product, Cisco will send you a username, password, and group ID number. You will need this information when you install your product licenses (as described in the "Adding a License" section on page 9-3.)

Note By accessing or using the Cisco Systems, Inc. products in this package, you agree that your use of such products is governed by the terms and conditions of the Cisco Systems, Inc. Software License and any applicable supplemental license agreement.

To review the terms of the Software License before accessing or using the products, you can find a copy of the Cisco Software License in the Cisco Information Packet that accompanies the products below or online at:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

To obtain the license activation credentials, log on to one of the websites listed below and follow the registration instructions. The Product Authorization Key (PAK) attached to your Software License Claim Certificate is required for the registration process. After registering, retain your Claim Certificate for future reference.

Registration Information

Use this URL if you are a registered user of Cisco.com:

http://www.cisco.com/go/license

Use this URL if you are not a registered user of Cisco.com:

http://www.cisco.com/go/license/public

You should receive the activation credentials and additional installation instructions through e-mail within one hour of registration. If you experience problems with the registration websites or if you have additional questions, contact the Cisco Licensing department through e-mail at licensing@cisco.com, or open a service request over the telephone by using one of these numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

You can find a complete list of Cisco TAC contacts at this URL:

http://www.cisco.com/techsupport/contacts

Determining Installation Options

Cisco CAS–SPincludes three component programs:

- Cisco Audit and Analysis–SP (including the Service Provider (SP) module)
- Cisco Report Server
- Cisco Virtual Network Data Server

Before installing the component programs, select the computers where you want to install these programs. Each computer must meet the system requirements for the program of interest, as described in the System Requirements for Cisco Audit and Analysis–SP chapter.

Product Licensing

Both Cisco Audit and Analysis–SP and Cisco Virtual Network Data Server require a corresponding license to be installed and available. On startup, the program contacts a *License Server* and requests a license. The License Server is a daemon/process that runs on the host where a license is installed; it handles license requests from component programs.

Selecting the License Type

When you install a component program, the installer asks you to specify the licensing mode. The options are:

- Floating/Local ("*Floating: serve licenses from this computer*")—If you select this option, the program will request a license from a License Server running on the local computer.
- Floating/Remote ("*Floating: access licenses from remote server*")—If you select this option, the program will request a license from a License Server running on a remote computer. (The installer also prompts you for the hostname of the remote server.)

  Floating mode enables multiple users to share a license. The following section describes Floating mode in more detail.
- Standalone—If you select this option, the installed license is restricted to the local computer and the program can be run on that computer only. (In essence, the program acts as its own License Server.) Select this option only if you want to restrict the use of Cisco Audit and Analysis–SP to one computer.

Note Cisco Virtual Network Data Server does not support Standalone licensing.

Floating Mode

Floating mode enables users to use the same license on different hosts. On startup, the program communicates with the License Server automatically and "checks out" a license. When the program closes, it returns the license to the License Server. Then the license is available for another user to start the program and check out the license. In Floating mode, the license is not "node-locked," but can "float" to different computers.

Note Multiple users cannot share the same license concurrently. Multiple concurrent sessions require an equivalent number of program licenses.

Although the License Server(s) for Cisco Virtual Network Data Server must use Floating mode, these licenses are not shared among multiple users. Each program runs automatically and "consumes" its license continually. System administrators do not need a license to log in to and operate these programs.

Note the following requirements:

- You must add the corresponding license as described in the "Adding a License" section on page 9-3. Installing a program and specifying the licensing options does not install the license itself.
- If you specify Floating (remote) licensing for a program, the specified License Server must be accessible (via a TCP/IP network) to that program.
- You must use Floating mode for Cisco Audit and Analysis–SP if Cisco Virtual Network Data Server is also running on the same host. (Note, however, that Cisco does not recommend running these programs on the same host.)

Node Pack Licensing

Cisco Audit and Analysis–SP uses a *node pack licensing* system that determines the size of the network you can create and analyze. The number of nodes in a network determines the node pack licenses required to perform an analysis.

You can purchase two different types of licenses for the Cisco Configuration Assurance Solution–SP product:

- Cisco CAS–SP 2.0 (50 nodes without Cisco VNDS)
- Cisco CAS–SP 2.0 (100 nodes with Cisco VNDS)

If your network has more nodes than are specified in the product license, you must purchase additional node pack licenses. Node pack licenses are available with different values (300, 500, 1000, and so on). You must register any additional node pack licenses before you can create network models and run analyses.

You can combine multiple licenses to satisfy your requirements. For example, any of the following license combinations will enable you to analyze a 1000-node network:

- One 1000-node pack license
- Two 500-node pack licenses
- One 500-node pack license and two 300-node pack licenses

Note Node pack licenses are available for Cisco CAS–SP 2.0 (100 nodes with Cisco VNDS) only. If you have Cisco CAS–SP 2.0 (50 nodes without Cisco VNDS) and want to model networks with more than 50 nodes, you must upgrade to Cisco CAS–SP 2.0 (100 nodes with Cisco VNDS).

Licensing Scenarios: Examples

This section shows some examples of how you can install and configure licenses in your network.

In Table 1-3, all licenses are installed on one host (VNDS_client), which acts as the only License Server in the network. The local Cisco VNDS program uses Floating/Local mode, while the remote programs use Floating/Remote mode. This type of setup is recommended; because there is only one License Server, it is easier to manage your licenses and configure programs.

Table 1-3 Licensing Example 1

LOCAL HOST CONFIGURATION			LICENSING OPTION SETTINGS FOR INSTALLED PROGRAM	
Installed Program	**Host Name**	**Licenses Installed on Host**	**License Server**	**License Mode**
Cisco Audit and Analysis–SP	AA_client_1	—	VNDS_client	Floating / Remote
Cisco Audit and Analysis–SP	AA_client_2	—	VNDS_client	Floating / Remote
Cisco VNDS	VNDS_client *(License Server)*	Cisco VNDS Cisco Audit and Analysis –SP	(*local host*)	Floating / Local

In Table 1-4, the Cisco Audit and Analysis–SP program is installed on AA_client_1 and two other hosts. Each installation requests a license from AA_client_1. (Keep in mind that if only one license is installed on the host, only one Cisco Audit and Analysis–SP session can run at a time.) The two other programs are installed on separate hosts which also act as License Servers.

Table 1-4 Licensing Example 2

LOCAL HOST CONFIGURATION			LICENSING OPTION SETTINGS FOR INSTALLED PROGRAM	
Installed Program	**Host Name**	**Licenses Installed on Host**	**License Server**	**License Mode**
Cisco Audit and Analysis–SP	AA_client_1 *(License Server)*	Cisco Audit and Analysis–SP	(*local host*)	Floating / Local
Cisco Audit and Analysis–SP	AA_client_2	—	AA_client	Floating / Remote
Cisco Audit and Analysis–SP	AA_client_3	—	AA_client	Floating / Remote
Cisco VNDS	VNDS_client *(License Server)*	Cisco VNDS	(*local host*)	Floating / Local

In Table 1-5, the programs are installed on separate hosts with their respective licenses. Cisco Audit and Analysis–SP uses Standalone mode, while Cisco VNDS request licenses from local License Servers.

Table 1-5 Licensing Example 3

	LOCAL HOST CONFIGURATION		LICENSING OPTION SETTINGS FOR INSTALLED PROGRAM	
Installed Program	**Host Name**	**Licenses Installed on Host**	**License Server**	**License Mode**
Cisco Audit and Analysis–SP	AA_client_1	Cisco Audit and Analysis–SP	(*local host*)	Standalone
Cisco VNDS	VNDS_client *(License Server)*	Cisco VNDS	(*local host*)	Floating / Local

In Table 1-6, each program has its license installed on the same computer and uses Floating/Local mode.

Table 1-6 Licensing Example 4

	LOCAL HOST CONFIGURATION		LICENSING OPTION SETTINGS FOR INSTALLED PROGRAM	
Installed Program	**Host Name**	**Licenses Installed on Host**	**License Server**	**License Mode**
Cisco Audit and Analysis–SP	CAS_client (*License Server)*	Cisco Audit and Analysis–SP	(*local host*)	Floating / Local
Cisco VNDS		Cisco VNDS	(*local host*)	Floating / Local

System Requirements for Cisco Audit and Analysis–SP

Cisco recommends that, before you start to install Cisco CAS–SP, you verify that your computer hardware and software meet the requirements outlined in this chapter.

Cisco Configuration Assurance Solution–SP: Operating Environment

An implementation of Cisco CAS–SP consists of the following components:

- Cisco Audit and Analysis–SP
- Cisco Virtual Network Data Server and the back-end Oracle database
- Cisco Report Server

You can install these components on one multi-processor platform (as described in Single-Platform Implementation, page 2-4) or on multiple platforms.

Cisco Audit and Analysis–SP: System Requirements

Supported Platforms

Vendor [1]	OS	Processor
Microsoft	Windows Server 2003 Windows 2000 Server Windows 2000 Professional	3.0+ GHz Intel Pentium 4, M, or Xeon with 800-Mhz front-side bus
Red Hat	Red Hat Enterprise Linux 3 (v2.4 Linux kernel)[2] Red Hat Enterprise Linux 4 (v2.6 Linux kernel)	x86 or EM64T (Intel Pentium III, 4, Xeon, or compatible, 500 Mhz or better) x86 AMD or AMD64, 500 MHz or better

1. Cisco Audit and Analysis–SP is supported on the English-language version of each operating system.
2. libstdc++.so.6 is required with Red Hat Enterprise Linux 3. You can obtain this by installing gcc 3.4 or higher.

Required Patches

Vendor	OS	Patch Number/Name
Microsoft	Windows Server 2003	N/A
	Windows 2000 Server	Service Pack 1, 2, and 4 are supported, but not required
	Windows 2000 Professional	Service Pack 1, 2, and 4 are supported, but not required

To determine the service pack installed on your Windows system, run winver.exe:

Step 1 Select **Run** from the Windows **Start** menu.

Step 2 Type in the command `winver` and click **OK**. The *About Windows* window appears and shows the version and service pack level installed.

Other Requirements

Display	Colors: 256 (minimum) Resolution: 1024x768 (minimum)
Supporting Software	TCP/IP networking software is required.
Web Browser	To view web reports generated by Cisco CAS–SP, you must have Firefox 1.0.6 or higher, Internet Explorer 5.0 or higher, or a compatible browser that supports Style Sheets.

Cisco Report Server: System Requirements

Supported Platforms

Vendor[1] [2]	Series	Processor
Microsoft	Windows 2000 Server	intel Pentium III, 4 or compatible (500 MHz or better)
	Windows 2000 Professional	
	Windows XP Professional	
	Windows Server 2003	

1. Cisco Report Server is supported on the English-language version of Windows only.
2. Cisco Report Server is not supported on 64-bit editions of Windows operating systems.

Required System Patches

Vendor	OS	Patch Number/Name
Microsoft	Windows 2000 Professional	Service Packs 1, 2, and 4 are supported but not required.
	Windows XP Professional	Service Pack 1 is required; Service Pack 2 is supported but not required.

Windows System Configuration

RAM	System and Working File Space[1]
512MB (minimum) 1GB (recommended)	80GB (minimum) 20GB (recommended)

1. Disk space requirements are highly dependent on the volume of report information stored on the report server and aging and report deletion policies.

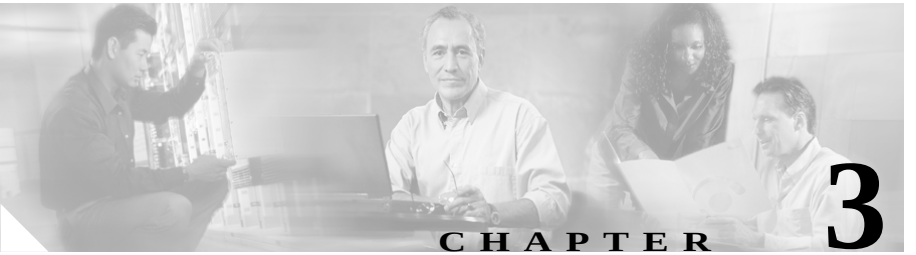
Browser Requirements

To view Cisco Report Server reports, you must use Internet Explorer 6.x or a compatible browser that supports Style Sheets.

Single-Platform Implementation

A single multi-processor platform might not deliver performance comparable to multiple platforms with equivalent total processors due to differences in the maximum front-side bus speed. However, if all components are to be installed on a single platform, the requirements are as follows.

RAM	Free Disk Space	Processor
7+ GB	200 GB	4-way 3.0+ GHz Intel Xeon or Pentium 4 with 800-MHz front-side bus



System Requirements for Cisco VNDS

This chapter describes the system requirements for the individual components in Cisco Virtual Network Data Server. Cisco recommends that, before you start to install Cisco CAS–SP, you verify that your computer hardware and software meet the requirements outlined in this chapter.

Cisco Virtual Network Data Server: System Requirements

Supported Platforms

Vendor[1] [2]	Series
Microsoft	Windows 2000 Server
	Windows 2000 Professional
	Windows XP Professional
	Windows Server 2003
Red Hat	Red Hat Enterprise Linux 3 (v2.4 Kernel)[3] Red Hat Enterprise Linux 4 (v2.6 Kernel)

1. Cisco VNDS is supported on the English-language version of each operating system.
2. Cisco VNDS is not supported on 64-bit editions of Windows or Linux operating systems, nor on Windows 2003 Web Edition.
3. libstdc++.so.6 is required with Red Hat Enterprise Linux 3. You can obtain this by installing gcc 3.4 or higher.

Required System Patches

Vendor	OS	Patch Number/Name
Microsoft	Windows 2000 Server	Service Pack 2 minimum
	Windows 2000 Professional	Service Pack 2 minimum
	Windows XP Professional	N/A
	Windows Server 2003	N/A

To determine the service pack installed on your Windows system, run `winver.exe`:

Step 1 Select **Run** from the Windows **Start** menu.

Step 2 Type in the command **`winver`** and click **OK**. The *About Windows* window appears and shows the version and service pack level installed.

Windows and Red Hat System Configuration

Cisco VNDS does not operate on machines with the Intel Itanium processor. To check the processor used by your Windows computer, right-click on the **My Computer** desktop icon and choose **Properties**.

	Processor[1]	RAM[2]	Disk	FSB[3]
Minimum	Intel Pentium D processor model 945 2x2MB Cache, 3.4 GHz	4 GB	80 GB	800 MHz
	Dual Processor, Dual Core Intel Xeon Model 5060, 2x2MB Cache,3.2 GHz	4 GB	80 GB	1066 MHz
Recommended	Intel Core2 Duo Processor Model E6700, 4MB Cache - 2.66GHz	6 GB	80GB	1066 MHz
	Dual Processor, Dual Core Intel Xeon Model 5160, 4MB Cache - 3.0 GHz	6 GB	160GB	1333 MHz

1. A dual-processor configuration is recommended if Cisco VNDS and the back-end Oracle database are to reside on the same platform.
2. Cisco VNDS performance will improve with more available memory as network size increases.
3. Front-Side Bus (FSB) speed affects the speed of data transfer to and from the Cisco VNDS database; faster bus speeds will improve Cisco VNDS performance.

Other Requirements

Cisco VNDS requires a dedicated Oracle database installation and dedicated database instance that cannot be shared with other applications. The preferred configuration includes a dedicated Oracle database installation local to the system on which Cisco VNDS is installed.

A shared Oracle instance where applications other than Cisco VNDS share/access the database or database instance are NOT supported. An Oracle database that is running on a system physically remote from or on a separate LAN from the Cisco VNDS system is NOT supported.

Software[1]	Platform	Supported Version	Required Database Character Set[2]
Oracle Database	Windows	• Oracle 9i Release 2 (version 9.2.0.1 or higher) • Oracle 10g Release 2 (version 10.2.0.1 or higher)	WE8MSWIN1252
	Red Hat	• Oracle 9i Release 2 (version 9.2.0.1 or higher) or • Oracle 10g Release 2 (version 10.2.0.1 or higher)	WE8ISO8859P1

1. Contact Oracle Corporation for information about Oracle 9i system requirements.
2. The supported national character set is: AL16UTF16. **For international customers:** The Virtual Network Data Server 4.0 product might not operate correctly when used with Oracle databases that have been configured with international, or Unicode (AL32UTF8), database character sets.

Installing Cisco Audit and Analysis–SP

This chapter contains the following procedures:

Installing Cisco Audit and Analysis–SP (Windows)

Note Before you install Cisco Audit and Analysis–SP, verify that you have a supported version of Windows installed as well as any required system patches. For more information, see Cisco Audit and Analysis–SP: System Requirements, page 2-2.

Use the following procedure to install Cisco Audit and Analysis–SP.

Installing Cisco Audit and Analysis–SP on Windows

Step 1 Log in as Administrator.

Step 2 Insert the Cisco CAS–SP, Audit and Analysis CD into your CD-ROM drive.

The installation program should start automatically. If it does not, double-click on the icon that represents the CD-ROM and click on the `setup.exe` icon.

Note If you are installing on Windows XP, you might see an error window that reads, "OPNET <*product_name*> has encountered a problem and needs to close." This error occurs because the installer caused an existing License Server process (op_license_server.exe) to terminate abnormally. This is a known issue; simply click **Don't Send** and proceed with the installation.

You will be prompted for a directory in which to install your software (typically `C:\Program Files\Cisco\CiscoCASSP2.0`).

Step 3 The software installer prompts you to specify the Cisco Report Server hostname and port.

If you have not yet installed Cisco Report Server, write down the port number because you will need this when you install the Cisco Report Server software (as described in Chapter 7, "Installing Cisco Report Server.").

If you have already installed Cisco Report Server, enter its host and port number now.

Step 4 When the software installer prompts you to specify the type of licensing system to install, the following might help you decide:

- *Standalone* is recommended if you are the only Cisco Audit and Analysis–SP user.
- *Floating: access licenses from remote server* is the correct choice if you already have a license server running on a remote machine and you want this installation to get its licenses from that machine.
- *Floating: serve licenses from this computer* is the correct choice if the current machine will be the license server.

Note If there is an existing installation of Cisco Audit and Analysis–SP on this computer, you can check how that release was licensed by running its License Manager. The first line of the license servers tree describes the licensing.

For more information about these options, see the "Product Licensing" section on page 1-7.

Step 5 Insert the Cisco CAS–SP, Models CD into your CD-ROM drive.

The installation program should start automatically. If it does not, double-click on the icon that represents the CD-ROM and click on the **setup.exe** icon.

Step 6 Insert the Cisco CAS–SP, Documentation CD into your CD-ROM drive.

The installation program should start automatically. If it does not, double-click on the icon that represents the CD-ROM and click on the **setup.exe** icon.

Note Installing does not install the license for this program. Before you can run the program, you must add the license as described in the Managing Licenses chapter.

Cisco Audit and Analysis–SP is now installed. Return to the installation workflow and continue with the next step.

Installing Cisco Audit and Analysis–SP (Linux)

Note Before you install Cisco Audit and Analysis–SP, verify that you have a supported version of Linux installed as well as any required system patches. For more information, see Cisco Audit and Analysis–SP: System Requirements, page 2-2.

Use the following procedure to install Cisco Audit and Analysis–SP.

Installing Cisco Audit and Analysis–SP (Linux)

Step 1 Log in as `root`.

Step 2 If you plan to use the Report Server, install it now. (See the *Report Server Installation Instructions* that come with the Report Server install package.)

Step 3 Insert Cisco CAS–SP, Audit and Analysis CD in your CD-ROM drive.

Step 4 Move to the `unix` directory on the CD, as follows:

```
mount /media/cdrom
cd /media/cdrom
```

```
cd unix
```

Step 5 Enter the command `./op_install.`

Step 6 When you are prompted to specify the type of licensing system to install, the following might help you decide:

- *Standalone* is recommended if you are the only Cisco Audit and Analysis–SP user.
- *Floating -- access licenses from remote server* is the correct choice if you already have a license server running on a remote machine and you want this installation to get its licenses from that machine.
- *Floating -- serve licenses from this computer* is the correct choice if the current machine will be the license server.

Step 7 At the end of the installation script for the Core software CD, the installer shows the following instruction: “To complete the installation process, follow these steps”. Note this information for use when configuring user accounts.

Step 8 When you see the prompt “End of installation script”, change directories to `/tmp` to allow the CD to be ejected.

Step 9 Eject the CD with the **`eject`** command.

Step 10 Insert the Cisco CAS–SP, Models CD into your CD-ROM drive and run the installer as described previously.

Step 11 Insert the Cisco CAS–SP, Documentation CD into your CD-ROM drive and run the installer as described previously.

Cisco Audit and Analysis–SP is now installed. Return to the installation workflow and continue with the next step.

Note These installers do not install the license for this program. Before you can run the program, you must add the license as described in the Managing Licenses chapter.

Note These installers do not automatically detect the default web browser you have installed on your Linux system. Search the known product issues (as described in Appendix D, "Known Issues") for details on how to configure Cisco Audit and Analysis–SP to use your preferred web browser.

Setting Up Cisco Audit and Analysis–SP to Run Automation Tasks (Linux)

When running on Linux, Cisco Audit and Analysis–SP requires an X display to run an automation task. If the task is launched while a user is logged on to the Linux host, Cisco Audit and Analysis–SP can use the X display of that user. If no one is logged on, however, Cisco Audit and Analysis–SP does not have access to a user display.

To run automation tasks even when no one is logged on, you must install and configure a virtual frame buffer on the host. To do this, perform the following procedures:

1. Installing a Virtual Frame Buffer on the Linux Host, page 4-5
2. Configuring Cisco Audit and Analysis–SP to use the Virtual Buffer Display, page 4-6

Installing a Virtual Frame Buffer on the Linux Host

Step 1 Download and install the xvfb software package. Using Red Hat distributions, the package name is usually "xvfb" and can be installed through the distribution's package manager. It may also be obtained from `http://www.xfree86.org` or `http://www.x.org`. You should download the version of xvfb that corresponds to your existing X server.

Step 2 Choose a screen that will be dedicated to **`Xvfb`**. (**NOTE—**The following steps assume that `screen 1` is chosen.)

Step 3 Create the file `/etc/init.d/xvfb` (with root execution permissions) that contains the following text:

```
#!/bin/sh
mode=$1
case "$mode" in
'start')

# start the X Virtual Framebuffer (Xvfb)
if [ -f /usr/X11R6/bin/Xvfb ]; then
echo "***Starting up the Virtual Frame Buffer on Screen 1***"
/usr/X11R6/bin/Xvfb :1 -screen 0 1152x900x8 &
fi
;;
*)

echo " Usage: "
echo " $0 start (start XVFB)"
echo " $0 stop (stop XVFB - not supported)"
exit 1
;;

esac
exit 0
-----
```

Step 4 Create a soft link to a file in the appropriate run-level directory. For example, to make **`Xvfb`** execute at run level 5, run the following command:

```
ln -s /etc/init.d/xvfb /etc/rc5.d/S75xvfb
```

Step 5 Reboot the Linux system.

Configuring Cisco Audit and Analysis–SP to use the Virtual Buffer Display

Step 1 If you have not already done so, perform Installing a Virtual Frame Buffer on the Linux Host, page 4-5.

Step 2 Start Cisco Audit and Analysis–SP.

Step 3 Select Automation > Configure/Run Automation Tasks.

Step 4 Click the "Display Settings..." button.

Step 5 Enter the display name for **`Xvfb`**. For example, if your host name is “my_local_host” and **`Xvfb`** is running on screen 1, you would enter the following string:

```
my_local_host:1
```

Step 6 Click **OK** in the Display Settings dialog box, then click **OK** in the Configure/Run Automation Tasks dialog box.

From this point forward, Sentinel will send its windows to xvfb. To view the "screen" at any time, you can run the following command:

```
xwd -display :1 -root -out image.xwd
```

To view the image dump, run the following command:

```
xwud -in image.xwd
```

Installing Cisco Virtual Network Data Server (Windows)

This chapter describes how to install the Cisco Virtual Network Data Server program on Windows.

System Requirements

Note The host for Cisco Virtual Network Data Server must meet minimum system requirements. If the host system does not meet minimum requirements, do not install Cisco VNDS. For more information, see Cisco Virtual Network Data Server: System Requirements, page 3-1.

If the host system does not have an Oracle database or an Oracle client installation, but meets all other requirements, install Oracle before installing Cisco Virtual Network Data Server as described in the Installation Workflows for your installation scenario.

Installation Workflows

This section covers the various installation scenarios you may encounter with Cisco VNDS on Windows. The procedures you must follow depend upon whether this is an initial installation or an update to an existing installation of the Cisco Virtual Network Data Server program. The procedures to follow also depend upon whether Cisco VNDS uses a local (same host) or a remote (different host) database.

Select the installation workflow appropriate for your circumstances. Follow the procedures in your workflow to install Cisco Virtual Network Data Server.

- Initial Cisco VNDS Installation (Windows/Local Oracle Database), page 5-2
- Initial Cisco VNDS Installation (Windows/Remote Oracle Database), page 5-3
- Update Cisco VNDS Installation (Windows), page 5-5

Note Cisco VNDS software is installed in HTTP mode by default. After successful installation and verification of the Cisco Virtual Network Data Server software, HTTPS may be configured. See the HTTPS Mode section of Release Notes for more information.

Initial Cisco VNDS Installation (Windows/Local Oracle Database)

If you are installing Cisco Virtual Network Data Server for the first time and will install Oracle on the same host, follow this workflow:

Step 1 Install the Oracle database on the Cisco VNDS host.

- Oracle9i users: see Installing the Oracle9i Database (Windows), page A-1.
- Oracle10g users: see Installing the Oracle10g Database (Windows), page A-7.

Step 2 Collect Oracle database information.

See the "Collecting Oracle Database Access Information (Windows)" procedure on page A-13.

Step 3 Install Oracle TopLink.

See the "Installing Oracle TopLink (Windows)" procedure on page A-14.

Note You must complete the previous steps before you install Virtual Network Data Server.

Step 4 Install the Cisco Virtual Network Data Server program.

See the "Installing Cisco VNDS (Windows)" procedure on page 5-6.

Step 5 Configure the Oracle database.

See the "Configuring the Oracle Database for Cisco VNDS (Windows)" procedure on page 5-17.

Step 6 Verify the Oracle configuration.

See the "Verifying the Oracle Configuration for Cisco VNDS (Windows)" procedure on page 5-21).

Step 7 Verify the Cisco VNDS software installation.

See the "Verifying the VNDS Software Installation (Windows)" procedure on page 5-23.

Initial Cisco VNDS Installation (Windows/Remote Oracle Database)

If you are installing Cisco Virtual Network Data Server for the first time and will install Oracle on a different host, follow this workflow:

Step 1 Install the Oracle database on the remote host.

For information about installing the Oracle database, see Appendix A, "Oracle Procedures (Windows)" or Appendix B, "Oracle Procedures (Linux)".

Step 2 Install the Oracle client on the Cisco VNDS host.

Note Install the version of the client that matches the version of the database that you installed in step 1.

- Oracle9i users: see Installing the Oracle9i Client (Windows), page A-5.
- Oracle10g users: see Installing the Oracle 10g Client (Windows), page A-10.

Step 3 Collect Oracle database information (use the procedure for the platform on which the remote database is installed):

- "Collecting Oracle Database Access Information (Windows)" procedure on page A-13
- "Collecting Oracle Database Access Information (Linux)" procedure on page B-3

Step 4 Install Oracle TopLink.

See the "Installing Oracle TopLink (Windows)" procedure on page A-14.

Note You must complete the previous steps before you install Virtual Network Data Server.

Step 5 Install the Cisco Virtual Network Data Server program.

See the "Installing Cisco VNDS (Windows)" procedure on page 5-6.

Step 6 Configure the Oracle database on the database host.

See the "Configuring the Oracle Database for Cisco VNDS (Windows)" procedure on page 5-17.

Step 7 Verify the Oracle configuration on the Cisco VNDS host.

See the "Verifying the Oracle Configuration for Cisco VNDS (Windows)" procedure on page 5-21.

Step 8 Verify the Cisco VNDS software installation.

See the "Verifying the VNDS Software Installation (Windows)" procedure on page 5-23.

Update Cisco VNDS Installation (Windows)

If you are updating a previous Cisco Virtual Network Data Server program installation, follow this workflow.

Warning **When updating from an earlier Cisco Virtual Network Data Server release, you must configure the Oracle database by running the setup_accounts script (`@setup_accounts.sql`). This means that you must re-create the network database. Network models created by previous releases cannot be retained by this release.**

Step 1 Collect Oracle database information.

See the "Collecting Oracle Database Access Information (Windows)" procedure on page A-13.

Note You must complete this step before you install Virtual Network Data Server.

Step 2 Install the Cisco Virtual Network Data Server program.

See the "Installing Cisco VNDS (Windows)" procedure on page 5-6.

Step 3 Configure the Oracle database on the database host.

See the "Configuring the Oracle Database for Cisco VNDS (Windows)" procedure on page 5-17.

Step 4 Verify the Oracle configuration on the Cisco VNDS host.

See the "Verifying the Oracle Configuration for Cisco VNDS (Windows)" procedure on page 5-21.

Step 5 Verify the Cisco VNDS software installation.

See the "Verifying the VNDS Software Installation (Windows)" procedure on page 5-23.

Note When updating from a previous Cisco VNDS installation, you can migrate configuration settings. Do not uninstall the previous installation until you migrate product configuration settings to the new installation. Make sure you read important notes on product migration in the Release Notes.

Installing Cisco VNDS (Windows)

Use the following procedure to install the Cisco Virtual Network Data Server program.

Installing Cisco VNDS (Windows)

Step 1 Log into the host as Administrator or as a user with full administrative privileges. If you are not logged in with the proper privileges, log off and then log on with an appropriate account.

Step 2 If the Cisco VNDS program is already installed on the host and you are updating to a new release, perform the following steps before continuing.

- **a.** Stop Cisco VNDS operation: Select **Services > Stop Services** from the Cisco Virtual Network Data Server Control Panel.
- **b.** Exit Cisco VNDS: Select **File > Exit** from the Control Panel menu bar.
- **c.** Open the Windows Task Manager, and select the Processes tab. If an op_monitor process is running, stop the process.
- **d.** Use a License Manager to see if your Cisco VNDS license is still held. If the license is still held by Cisco VNDS, use the License Manager to revoke the license.

Note Do not rename or uninstall the existing Cisco VNDS release. If Cisco VNDS 3.5 is already installed (as part of CAS, CAS-SP, NPS, or NPS-SP), you can migrate configuration settings to Cisco VNDS 4.0.

Step 3 Start the installer:

a. Insert the Cisco Virtual Network Data Server installation CD into the CD drive of the host. If the installer does not start automatically, use **Start > Run** to execute the `cvnds-2.0-win-K9.exe` program on the CD.

The installer displays an *Introduction* panel.

b. Click **Next**.

If an existing Cisco VNDS software installation is detected, a *Notice* dialog appears to remind you to stop services and exit Cisco VNDS. Click **Yes** to continue or **No** to cancel the installation.

Step 4 Determine your Oracle installation scenario in Table 5-1 on page 5-8 and follow instructions for that scenario.

Note Cisco VNDS can operate with either a local or remote Oracle database. If a database is present on the local host, you can use this database; you can also use a remote database on a different host. In either case, the installer displays a panel that requests database access information. If a local database is not found, but an Oracle client installation is detected, the installer displays a panel requesting access information about the remote database.

Table 5-1 Oracle Installation Scenarios

Scenario	Oracle Installation	Instructions
1	• An Oracle installation is not present on the host. • A message box indicates that Oracle cannot be found.	• Abort installation. Click OK to cancel the installation. • Install Oracle on the host before attempting to install Cisco VNDS.
2	• Oracle database installation is present on host. • If more than one Oracle installation is found on the host, the installer asks which Oracle you want to use. Select the radio button for the correct Oracle installation and click **Next**.	An installer panel appears and asks if you want Cisco VNDS to use the local database. • Select **Yes** to use the local database and continue with step 5. • Select **No** to use a remote database, and continue with step 6.
3	• Oracle client installation is present on the host. • If more than one Oracle installation is found on the host, the installer asks you which Oracle you want to use. Select the radio button for the correct Oracle installation and click **Next**.	• An installer panel appears stating that a local Oracle client is detected[1]. • if the Oracle installation is a Client, select the Client radio button. Click OK and continue with step 6. • If the Oracle installation is really a local database server, select the Server radio button. Enter the Database SID from Table A-1 on page A-14. Click OK and continue with step 5.

1. Depending upon how Oracle is installed and databases are created, what appears to be a Client installation may really be a Server.

Note If you are working with a local database, use step 5. If you are working with a remote database, use step 6.

Step 5 Specify values for the account Cisco VNDS will use to access the **local** Oracle database:

- Local Database TNS Service Name
- Local Database User Name

- Local Database Password
- Confirm Password

Note Select a user name that is dedicated for use by Cisco VNDS. *DO NOT use SYS or SYSTEM for the Local Database User Name.*

Fill in each field with the information collected in Table A-1 on page A-14 and click **Next**. Jump to step 7.

Step 6 Specify **remote** database access information.

a. The installer prompts you for the following database access information:

- Remote Database TNS Service Name
- Remote Database SID
- Remote Database Hostname
- Remote Oracle Home Directory
- Remote Oracle Oradata Parent Directory

Fill in each field with the information collected in Table A-1 on page A-14 and click **Next**.

The installer prompts you for additional remote database access information.

b. Specify values for the account Cisco VNDS will use to access the Oracle database.

- Remote Database User Name
- Remote Database Password
- Confirm Password

Note Select a username that is dedicated for use by Cisco VNDS. *DO NOT use SYS or SYSTEM for the Local Database User Name.*

c. Fill in each field with the information collected in Table A-1 on page A-14 and click **Next**.

Step 7 The installer prompts you for the location of Oracle Toplink files required by Cisco VNDS.

Note Note: Version 9.0.3.5 of Oracle Toplink is required.

a. If you have Toplink installed to the default path within your existing Oracle installation, the default path shown in this panel is the correct path. Locate the path on your system that contains the following Toplink files:
`tl_core.jar  tl_tools.jar  tl_x.jar`

b. Click **Choose** and browse to the directory of the required Oracle Toplink files. Click **Select** to complete your choice.

Step 8 Click **Next**. If the required files are not found at the selected path, an error dialog appears. Click one of the following:

- **OK** to try again to select a path.
- **Cancel** to cancel the installation.

Step 9 Specify the licensing scheme.

a. The installer prompts you for the type of licensing to use. The *`Select Licensing Type`* panel provides a choice between remote and local licensing:

– Access licenses from a remote server

– Serve licenses from a license server on this computer

Note Selecting the local option results in a license server being installed with the VNDS installation. This license server installed is the same version license server as is installed with other Cisco Solution programs.

Note The specified license server must have a valid VNDS license before you can run the software.

b. Choose the licensing type, then click **Next**.

– If you selected remote licensing, the installer displays the *Enter Server Name and Port* panel. Proceed to step c.

– If you selected local licensing the *Enter Port* panel displays. Jump to step d.

c. The installer prompts you for the server name and port.

- Type the hostname of the remote license server in the Server field.
- Type the port (`port_a`, `port_b`, or `port_c`) used by the remote license server in the Port field.
- Click **Next**.

The installer prompts you for an installation path. Proceed to step 10.

d. The installer prompts you for the port used by the local license server (`port_a`, `port_b`, or `port_c`).

Accept the default value. Click **Next** to proceed.

The installer prompts you for an installation path. Proceed to step 10.

Note If you are installing on Windows XP, you might see an error window that reads "OPNET <*product_name*> has encountered a problem and needs to close." This error occurs because the installer caused an existing license server process (`op_license_server.exe`) to terminate abnormally. This is a known issue; click **Don't Send** and proceed with the installation.

Note Write down the license settings you have chosen for future reference.

Step 10 Specify the VNDS installation directory.

a. Type an installation path in the panel's path field or use the file browser to select an installation path. The path you choose cannot contain embedded spaces.

Note The path you enter is the parent directory for the installation. The installer adds `\VNDServer\<version>_<build#>` to the path you choose.

b. Click **Next**.

The installer prompts you for the path to use for the VNDS temp directory.

Step 11 Specify the VNDS temporary directory.

a. Type a temp directory path in the panel's *path* field or use the file browser to select a path. The path you choose cannot contain embedded spaces.

Note The temp directory holds temporary working files for the product. The path you specify is the full path to this directory.

b. Click **Next**.

The installer prompts you for the path to use for the VNDS config file archive directory.

Step 12 Specify the VNDS config file archive directory.

a. Type an archive directory path in the panel's path field or use the file browser to select a path. The path you choose cannot contain embedded spaces.

Note The archive directory holds collected device configuration files that have been archived by the product. The path you specify is the full path to this directory.

b. Click **Next**.

The installer prompts you to configure server parameters.

Step 13 Specify server information for this instance of Cisco VNDS. The installer prompts you for the following information:

- Virtual Network Data Server Name
- Virtual Network Data Server ID (0-1022)
- Virtual Network Data Server Address

a. Type the primary IP address of the host in the *Cisco Configuration Assurance Solution-SP Address* field.

Note The primary IP address is required for all VNDS installations. To obtain the IP address, open a command window and run the **ipconfig** command.

b. Fill in additional fields if this instance of Cisco VNDS will participate in an *n*-tier hierarchy.

c. Click **Next**.

The installer displays the *Configure Cisco Configuration Assurance Solution-SP Client Connectivity* panel.

Step 14 Specify the VNDS Client Connectivity Port.

Type a port number or click **Next** to accept the default value.

Note The Client Connectivity port is the port on which the Live Update Service runs. If you enter a non-default port, VNDS clients might be unable to communicate with Cisco VNDS until you make a corresponding change in the client preferences.

The installer displays a panel for configuration of the web server.

Step 15 Specify web server connectivity information.

a. The installer prompts you for the following:

- HTTP Port
- HTTPS Port
- Keystore Directory

b. Fill in each field or click **Next** to accept default values.

The installer prompts you to set the Web Server Administrator password.

Note Write down the web server connectivity settings for future use.

Step 16 Specify the password for the administrator (*admin*) user account for the Cisco Configuration Assurance Solution–SP Web Console. The installer prompts you for the following information:

- Enter administrator password
- Confirm administrator password

Type a password into the password fields or click **Next** to accept the default (*cisco*).

Note Write down the *admin* password. You will need this password to log into the Cisco Virtual Network Data Server Web Console for the first time—the VNDS Web Server is installed in the local authentication mode by default. Once logged into the Web Console, the *admin* user can change the *admin* password, create user accounts, or change the authentication scheme.

The installer prompts you to configure email notification parameters.

Step 17 If you want to begin receiving email notification as soon as you start VNDS services, configure email notifications at this time. Otherwise, configure notifications when you are ready to begin automated operation (recommended) using the Notification panel in the Cisco Virtual Network Data Server Administrative Console.

a. Enter the sender, recipients, and subject prefix for VNDS email notifications or leave these fields blank if you want to configure email notifications post-installation.

b. Click **Next** to proceed.

The installer prompts you for email server settings.

c. Enter the SMTP Server, Port, User Name, and Password (if you want to configure email notifications post-installation, leave these fields blank).

d. Click **Next** to proceed.

An installation progress panel shows status messages as VNDS installation progresses. Installation normally finishes in several minutes.

– If an existing VNDS 3.5 installation is detected, the installer displays the *Migrate Cisco Configuration Assurance Solution-SP Product Configuration* panel. Proceed to Step 18.

Note The installer checks the version of the Oracle Toplink files that you chose in Step Step 7. If the wrong version files were selected, an error dialog box appears. Click OK to continue. Before operating Virtual Network Data Server, you must locate the correct version of the required Toplink files and copy them to the <install dir>\ext directory

– If you are installing on a host that does not have Cisco VNDS 3.5 software installed, the installer displays the *Web Services Note* panel when installation is complete. Jump to step 19.

Step 18 Migrate the configuration settings from the previous version of Cisco Virtual Network Data Server to the current version (*optional*).

To migrate previous settings, perform the following steps:

– Select **Yes** in the *Migrate Cisco Configuration Assurance Solution–SP Product Configuration* panel, then click **Next**.

A Confirm dialog box displays. It provides the path of the previous installation (from which it will migrate product configuration) and lists the actions that will be performed if you proceed.

– Click **Yes** to continue with migration. Click **No** to skip migration and proceed to step 19.

Progress dialog boxes display during product configuration. A Status dialog box displays when migration is complete. This dialog summarizes the actions performed and provides the location of migration logs. Click **OK** and proceed to step 19.

Note During migration, VNDS 3.5 device info file is copied to the 4.0 installation. However, it is not converted to the 4.0 format or imported into Cisco VNDS. See the *Release Notes* for important notes on updating.

To install without migrating previous settings, perform the following steps:

– Select **No** in the *Migrate Cisco Configuration Assurance Solution-SP Product Configuration* panel then click **Next**.

A Notice dialog displays.

– Click **OK** to proceed to step 19. Click **Previous** to go back to the *Migrate Cisco Configuration Assurance Solution-SP Product Configuration* panel.

Note If you chose not to migrate but want to preserve groups, you must export this information from the database before you configure the database for 4.0. You can migrate adapter resources and text files after installation is complete as long as you do not uninstall or delete files from the previous release installation directory. See the Administration chapter of the *Cisco Configuration Assurance Solution–SP User Guide* for instructions on how to run the migration tools.

Step 19 Read the *Web Services Note*.

Note VNDS software is installed in HTTP mode. You can optionally configure HTTPS after you have completed your installation workflow. See the HTTPS Mode section of the *Release Notes* for more information.

Step 20 Click **Next**.

The installer displays the *Install Complete* panel.

Step 21 Click **Done** to exit the installer.

Note Installation of VNDS software is now complete. Return to the workflow you are following and continue with the next step. Do not attempt to start Cisco VNDS or access the Web Console until you complete all steps in the installation workflow.

Note Refer to the *Cisco Configuration Assurance Solution–SP User Guide*, Administration chapter, Licensing Operations section for instructions on adding a license.

After you have installed VNDS software, see Configuring the Oracle Database for Cisco VNDS (Windows), page 5-17.

Configuring the Oracle Database for Cisco VNDS (Windows)

After you install the current version of Cisco Virtual Network Data Server, you must configure the Oracle database for use by Cisco VNDS. This involves running an SQL script named *setup_accounts.sql* that creates tablespaces for the database and a VNDS access account.

Warning **Do not modify the setup_accounts.sql script. This can cause the installation to fail or prevent Cisco Configuration Assurance Solution–SP from operating correctly.**

To configure the Oracle database, perform "Configuring the Oracle Database (Windows)" section on page 5-17.

Configuring the Oracle Database (Windows)

Step 1 If the Oracle database and Cisco VNDS are located on the same host system, open a command window and navigate to the Cisco Virtual Network Data Server installation directory by typing

```
cd <install path>\VNDServer\<release_number>_<build_number>
```

Stay in the command window on the host system for Cisco VNDS, and continue with step 2.

Step 2 Log into Oracle using the *system* account.

- For a local Oracle database installation enter the following command:

  ```
  sqlplus system/<system password>
  ```

- For a remote Oracle database, enter the following command:

  ```
  sqlplus system/<system password>@<DB TNS Service Name>
  ```

  For example, if the Database is remote with a TNS Service Name of *o92avnes* and the Oracle system password is *magic*, type:

  ```
  sqlplus system/magic@o92avnes
  ```

Step 3 Enter the following command at the ***SQL>*** prompt:

```
@setup_accounts.sql
```

A message banner displays to inform you how much free disk space is required on the disk that hosts the database.

Note If you do not have sufficient disk space available to run this script, free up sufficient disk space before proceeding. If you want to cancel the script, press Ctrl-C or close the command window.

Step 4 Click **Enter** to continue.

A message banner displays a notification about Device and Platform Info.

- For Oracle9i, proceed to step 5.
- For Oracle10g, jump to step 6.

Step 5 Click **Enter** to continue.

When you configure Oracle 9i, a message banner displays with a list of database parameters, database parameter settings, and whether the parameters meet recommended settings. A log of database analysis results is saved to `<install_dir>\analyzedb.<timestamp>.log`.

Note If all parameters meet recommended settings, no further action is required. If one or more parameters do not meet recommended settings, the installer recommends that you run the *dbparamchg.sql* script after this procedure is completed; this will improve data import performance with large networks and increase Oracle memory requirements.

Step 6 Click **Enter** to continue.

A database name displays.

Step 7 Verify the database instance name.

Note If the database is located on a Solaris or Linux system, the case (uppercase, lowercase) of the characters in the database instance name must be a case-sensitive match of the name of the database directory located under the `oradata` directory (e.g., `/uo1/app/oracle/oradata`) on the database host. Look in the `oradata` directory to ensure that, when you enter the database instance name, it is a case-sensitive match.

Step 8 Click **Enter** to continue.

The *setup_accounts* script prompts you for the database instance name.

Step 9 Enter the database instance name obtained in step 7.

The setup_accounts script prompts you for the user password.

Step 10 Enter the same database user account password that was entered during VNDS installation and written down in Table A-1 on page A-14.

A message displays to inform you that the VNDS user account and all data will be deleted by this script.

Step 11 Click **Enter** to continue.

The setup_accounts SQL script configures database storage for use by Cisco VNDS and sets up the user account. After the script finishes, the Oracle account information for Cisco VNDS is the user name and password from Table A-1 on page A-14. A log of script actions is saved to the following location:

`<install_dir>\setup_accounts.<timestamp>.log`

Note When you run this script for the first time, several SQL error messages appear. You can ignore these messages. The messages are the result of the script trying to remove VNDS table and user accounts that do not exist prior to this script being run for the first time.

Step 12 Type **quit** at the *SQL>* prompt to exit sqlplus.

If the setup_accounts script recommended changing your database settings during step 5, and you agree with the recommended changes, see Modifying Database Parameters (Windows), page 5-20 at this time.

If you do not need to change your database settings or choose not to change them, see Verifying the Oracle Configuration for Cisco VNDS (Windows), page 5-21 to verify that Oracle is configured correctly for use with Cisco VNDS.

Modifying Database Parameters (Windows)

Perform Modifying Database Parameters (Windows), page 5-20 on the Oracle 9i database host to modify database parameters. The database parameter changes improve VNDS performance when working with large networks and will increase Oracle memory requirements.

Do not modify database parameters for Oracle 10g unless instructed to do so by Cisco Technical support.

Note Work with your Database Administrator to run this script.

Modifying Database Parameters (Windows)

Step 1 Log into Oracle using the *system* account.

- For a local Oracle database installation:

  Type `sqlplus system/<system password>` in the command window.

- If the Oracle database is not on the same host system as Cisco VNDS, then perform the following steps:

  Type `sqlplus system/<system password>@<DB TNS Service Name>`

  For example, if the Database is remote with a TNS Service Name of *o92avnes* and the Oracle system password is *magic*, type:

  ```
  sqlplus system/magic@o92avnes
  ```

Step 2 Enter the following command at the *SQL>* prompt:

```
@dbparamchg.sql
```

A message shows the path to the Oracle spfile that contains the parameters for your database.

Step 3 Make a backup copy of the spfile at the path specified in the previous step.

Step 4 Press **Enter** as many times as needed to step through information messages produced by this script.

When the script is done, a list of the changed parameters and their new settings appears with a reminder to restart the Oracle DB service for the changes to take effect.

Step 5 Type `quit` at the *SQL>* prompt to exit sqlplus.

Step 6 Use the Windows Service Manager to stop and restart the Oracle database service.

a. From the desktop, select **Start > Settings > Control Panel > Administrative Tools > Services** to open the Windows Service Manager.

b. Select the service named **OracleService<DB SID>**.

c. Right-click on the service, and select **Stop** from the menu.

d. After the Service Control progress dialog completes, right-click on the service, and select **Start** from the menu to restart the service.

Step 7 If the Oracle database service fails to restart, restore the original spfile for the database and repeat step 6 to recover.

See "Verifying the Oracle Configuration for Cisco VNDS (Windows)" section on page 5-21 to verify that you can connect to the database through the VNDS account.

Verifying the Oracle Configuration for Cisco VNDS (Windows)

Perform the follow procedure on the VNDS host to verify that you can connect to the database through the VNDS account.

Verifying the Oracle Configuration (Windows)

Step 1 Open a command window.

Step 2 Navigate to the VNDS installation directory.

Step 3 Verify that you can log in into Oracle using the VNDS account.

- For a local Oracle database, enter the following command:

  ```
  sqlplus <user name>/<password>
  ```

  Use the user name and password from Table A-1 on page A-14.

- For a remote Oracle database, enter the following command:

```
sqlplus <user name>/<password>@<DB TNS Service Name>
```

Use the user name and password from Table A-1 on page A-14. For example, if the database is remote with a TNS Database Service Name of *o92avnes* and the VNDS username and password are *vnes* and *pwd* respectively, enter:

```
sqlplus vnes/pwd@o92avnes
```

Step 4 If Oracle configuration was not successful, error messages display indicating that login has been denied.

Reconfigure the Oracle database and verify again.

Step 5 If configuration of the Oracle account for Cisco VNDS was successful, an Oracle banner, and a *Connected To:* message appears.

Step 6 Type **quit** at the *SQL>* prompt to exit.

Step 7 Test the Oracle database configuration.

a. Enter the following command:

```
vnes.bat DBAUTOTEST
```

Tests run to verify that the VNDS account can perform needed operations in Oracle.

Output is written to the command window and a separate java window opens to display a summary of results.

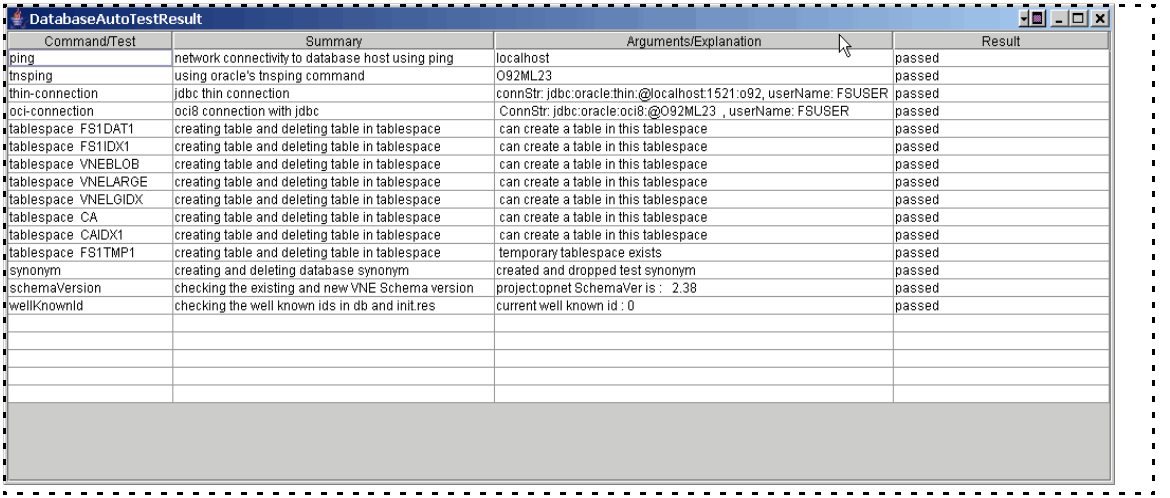
b. Review DBAUTOTEST results.

Note Do not proceed until all tests pass. Figure 5-1 on page 5-23 shows a successful result.

If any of the database tests fail, contact Cisco Technical Support (as described in "Obtaining Technical Assistance" section on page fm-xii).

When all database tests pass, continue with your installation roadmap.

Figure 5-1 Example of Successful DBAUTOTEST Results



DatabaseAutoTestResult

Command/Test	Summary	Arguments/Explanation	Result
ping	network connectivity to database host using ping	localhost	passed
tnsping	using oracle's tnsping command	O92ML23	passed
thin-connection	jdbc thin connection	connStr: jdbc:oracle:thin:@localhost:1521:o92, userName: FSUSER	passed
oci-connection	oci8 connection with jdbc	ConnStr: jdbc:oracle:oci8:@O92ML23 , userName: FSUSER	passed
tablespace FS1DAT1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace FS1IDX1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNEBLOB	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNELARGE	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNELGIDX	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace CA	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace CAIDX1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace FS1TMP1	creating table and deleting table in tablespace	temporary tablespace exists	passed
synonym	creating and deleting database synonym	created and dropped test synonym	passed
schemaVersion	checking the existing and new VNE Schema version	project:opnet SchemaVer is : 2.38	passed
wellKnownId	checking the well known ids in db and init.res	current well known id : 0	passed

VNDS program installation and database configuration are now complete. Proceed to Verifying the VNDS Software Installation (Windows), page 5-23 to verify the VNDS installation.

Verifying the VNDS Software Installation (Windows)

After the database has been configured and verified, perform the following procedure to verify that the VNDS software is installed correctly.

Verifying the VNDS Installation (Windows)

Step 1 Verify that the license server specified during installation has required licenses installed.

Note Do not proceed until you have verified that the appropriate licenses are available.

Step 2 Open the Cisco Configuration Assurance Solution–SP Control Panel from the Program Group shortcut as follows.

Start > Programs > Cisco Configuration Assurance Solution–SP 2.0 > Virtual Network Data Server

Within a minute, the Cisco Configuration Assurance Solution–SP Control Panel appears.

Step 3 Start VNDS services from the Control Panel by clicking the Start Services button on the tool bar.

A progress dialog appears, and within a few minutes, service start-up completes.

Step 4 Stop VNDS services from the Control Panel by clicking the Stop Services button on the tool bar.

A progress dialog box appears; services should stop within a few minutes.

Note If the Control Panel fails to open, services fail to start or stop, or error dialog boxes appear, there is a problem with the installation. Review Release Notes for known issues and workarounds; you can also search for troubleshooting information in the FAQ database at the Cisco Quick Support Center. Contact Cisco Technical Support for assistance if problems persist (for more information, see "Obtaining Technical Assistance" section on page fm-xii).

Step 5 Verify communication with the VNDS Web Server via HTTP.

a. Start the Cisco Virtual Network Data Server Web Service using the Windows services window.

b. Open a web browser and enter the URL for the VNDS Web Console.

```
<protocol>://<host>:<port>/vnes
```

For example, if the VNDS host is myhost.myco.com and the http port is 9190, enter the following:

```
http://myhost.myco.com:9190/vnes
```

c. Close the browser window.

Step 6 Click the Exit button on the Control Panel tool bar to exit from Cisco VNDS.

Step 7 Some VNDS services continue to run in the background. If you want to completely shut down Cisco VNDS, stop all services.

To stop all services, do the following:

a. Open a commend window and navigate to theVNDS install directory.

b. Enter the following command:

```
vnes.bat /svc_cmd stop ALL
```

Installing Cisco Virtual Network Data Server (Linux)

This chapter describes how to install the Cisco Virtual Network Data Server program on Linux.

System Requirements

Note The host for Cisco Virtual Network Data Server must meet minimum system requirements. If the host system does not meet minimum requirements, do not install Cisco VNDS. For more information, see Cisco Virtual Network Data Server: System Requirements, page 3-1.

If the host system does not have an Oracle database or an Oracle client installation, but meets all other requirements, install Oracle before installing Cisco VNDS as described in the "Installation Workflows: Overview" section.

Installation Workflows: Overview

This chapter covers the installation scenarios you might encounter with Cisco VNDS on Linux. The procedures you must follow depend upon whether VNDS uses a local or a remote database.

Select the installation workflow appropriate for your circumstances. Follow the procedures in your workflow to install Cisco VNDS.

- Initial VNDS Installation (Linux/Local Oracle Database), page 6-2
- Initial Cisco VNDS Installation (Linux/Remote Oracle Database), page 6-3

Note VNDS software is installed in HTTP mode by default. After successful installation and verification of the VNDS software, HTTPS may be configured. See the "HTTPS Mode" section of the *Release Notes* for more information.

Initial VNDS Installation (Linux/Local Oracle Database)

If you are installing Cisco VNDS for the first time and will install Oracle on the same host, follow this workflow.

Step 1 Install the Oracle database on the VNDS host.

For more information, see Oracle Installation Procedures, page B-1.

Step 2 Collect Oracle database information (see Collecting Oracle Database Access Information (Linux), page B-3).

Step 3 Install Oracle TopLink.

See the "Installing Oracle TopLink (Linux)" procedure on page B-4.

Note You must complete the previous steps before you install Virtual Network Data Server.

Step 4 Install the Cisco Virtual Network Data Server program (see Installing Cisco VNDS (Linux), page 6-4).

Step 5 Configure the Oracle database for VNDS (see Configuring the Oracle Database for Cisco VNDS (Linux), page 6-14).

Step 6 Verify the Oracle configuration for VNDS (see Verifying Oracle Configuration for Cisco VNDS (Linux), page 6-19).

Step 7 Verify the VNDS installation (see Verifying the VNDS Software Installation (Linux), page 6-21).

Initial Cisco VNDS Installation (Linux/Remote Oracle Database)

If you are installing Cisco VNDS for the first time and will install Oracle on a different host, follow this workflow:

Step 1 Install the Oracle database on the remote host.

For information about installing the Oracle database, see Appendix A, "Oracle Procedures (Windows)" or Appendix B, "Oracle Procedures (Linux)".

Step 2 Install the Oracle client on the host for Cisco VNDS.

Note Install the version of the client that matches the version of the database that you installed in step 1.

For more information, see Appendix B, "Oracle Procedures (Linux)."

Step 3 Collect Oracle database information (use the procedure for the platform on which the remote database is installed):

- "Collecting Oracle Database Access Information (Windows)" procedure on page A-13
- "Collecting Oracle Database Access Information (Linux)" procedure on page B-3

Step 4 Install Oracle TopLink.

See the "Installing Oracle TopLink (Linux)" procedure on page B-4.

Note You must complete the previous steps before you install Virtual Network Data Server.

Step 5 Install the Cisco Virtual Network Data Server program (see Installing Cisco VNDS (Linux), page 6-4).

Step 6 Configure the Oracle database on the remote host (see Configuring the Oracle Database for Cisco VNDS (Linux), page 6-14).

Step 7 Verify the Oracle configuration on the remote host (see Verifying Oracle Configuration for Cisco VNDS (Linux), page 6-19).

Step 8 Verify the VNDS installation (see Verifying the VNDS Software Installation (Linux), page 6-21).

Installing Cisco VNDS (Linux)

Perform the following procedures to install the Cisco Virtual Network Data Server program:

1. Performing Pre-Installation Checks for Cisco VNDS (Linux), page 6-4
2. Installing Cisco VNDS (Linux), page 6-5

Performing Pre-Installation Checks for Cisco VNDS (Linux)

Step 1 Make sure the Oracle database is up and running.

Enter the following command on the database host:

```
ps -aef | grep ora_
```

You should see a number of processes with the following naming convention:

```
ora_<process>_<sid>
```

If the Oracle database is not running, contact your database administrator to start the database.

Step 2 If Cisco VNDS is already installed on the host and you are updating to a new release, perform the following steps to make sure that all VNDS services are stopped.

a. Log into the VNDS host as **root** or a user with permission to run VNDS or switch users to one of these accounts. When switching users, use the following command:

```
su - <user_name>
```

b. Navigate to the VNDS installation directory.

c. Enter the following command to determine whether VNDS services are running:

```
ps -aef | grep wrapper
```

d. Stop any VNDS services that are running. Navigate to the VNDS installation directory and enter the following command:

```
vnes.sh -c stop ALL
```

Installing Cisco VNDS (Linux)

Step 1 Log into the VNDS host as **root** or switch users to **root**. To switch to `root`, open a command prompt window and enter the following command:

```
su - root
```

Step 2 Start the installer.

a. Insert the Cisco Virtual Network Data Server installation CD into the CD drive of the host, then execute the `cvnds-2.0-lin-K9.bin` program.

As an example, open a command window and navigate to the folder that corresponds to the CD drive (e.g., `/media/cdrecorder`), then enter `./cvnds-2.0-lin-K9.bin`.

The installer displays an *`Introduction`* panel.

b. Click **Next**.

The installer displays a *`Specify database type`* panel.

Step 3 Specify parameters that describe the Oracle installation that Cisco VNDS will use. The installer prompts you for the following:

- Choose whether the database is local or remote

- Choose whether you are using a 32 bit or 64 bit Oracle

Make your selections, then click **Next**.

The installer displays a *Specify an Oracle database* panel.

Step 4 Specify the Oracle database that Cisco VNDS will use. The installer prompts you for the following database access information:

- Database TNS Service Name
- Database SID
- Database Hostname
- Local Oracle Installation Dir
- Base Dir for Database

Fill in each field with the information collected in Table B-1 on page B-3 and click **Next**.

The installer displays the *Specify account information for the Oracle database* panel.

Step 5 Specify values for the account that Cisco VNDS will use to access the Oracle database.

- Database User Name
- Database Password
- Confirm Password

Fill in each field with the information collected in Table B-1 on page B-3 and click **Next**.

Note Select a user name that is dedicated for use by Cisco VNDS. DO NOT use SYS or SYSTEM for the Local Database User Name.

If you specified a remote database in Step 3, the installer displays the *Choose the Oracle version* panel. Proceed to Step 6.

If you specified a local database in Step 3, the installer prompts you for the location of the Oracle TopLink files. Jump to Step 7.

Step 6 Specify the Oracle version for the remote database. The choices are:

- Oracle9i

- Oracle10g

Choose the appropriate Oracle version, then press Next to continue. The installer prompts you for the location of the Oracle Toplink files.

Step 7 The installer prompts you for the location of Oracle Toplink files required by Cisco VNDS.

Note Note: Version 9.0.3.5 of Oracle Toplink is required.

a. If you have Toplink installed to the default path within your existing Oracle installation, the default path shown in this panel is the correct path. Locate the path on your system that contains the following Toplink files:
`tl_core.jar  tl_tools.jar  tl_x.jar`

b. Click **Choose** and browse to the directory of the required Oracle Toplink files. Click **Select** to complete your choice.

c. Click **Next**. If the required files are not found at the selected path, an error dialog appears. Click one of the following:

– **OK** to try again to select a path.

– **Cancel** to cancel the installation.

Step 8 Specify the licensing type (see Licensing Notes, page 6-13 for more information).

a. The installer prompts you for the type of licensing to use. The *`Select Licensing Type`* panel provides the following choices:

– Access licenses from a remote server

– Serve licenses from a new license server on this computer

– Serve licenses from an existing license server on this computer

b. Choose the licensing type, then click **Next**.

Note The specified license server must have a valid VNDS license before you can run the software.

If you selected remote licensing, the installer displays the *`Enter Server Name and Port`* panel. Proceed to step c.

If you selected local licensing, the installer displays the *`Enter Port`* panel. Jump to step d.

c. The installer prompts you for the server name and port.

- Type the hostname of the remote license server in the Server field.
- Type the port (`port_a`, `port_b`, or `port_c`) used by the remote license server in the Port field.
- Click **Next**.

The *Choose the Cisco Configuration Assurance Solution–SP Installation folder* panel displays. Proceed to Step 9.

Note Write down the license settings for future reference.

d. The installer prompts you for the port used by the local license server (port_a, port_b, or port_c)

Accept the default value. Press **Next** to proceed.

The installer displays the *Choose the Cisco Configuration Assurance Solution-SP Installation folder* panel. Proceed to Step 9.

Step 9 Specify the VNDS installation directory.

a. Type an installation path in the panel's path field or use the file browser to select an installation path. The path you choose cannot contain embedded spaces.

Note The path you enter is the parent directory for the installation. The installer adds `\VNEServer\<version>_<build#>` to the path you choose.

Note The installer suggests a default directory. Although you can override the default, Cisco strongly recommends that you install Cisco VNDS in its own, program-specific directory. Cisco also recommends that you do not install multiple Cisco Solution programs (such as Cisco VNDS and Cisco Audit and Analysis–SP) in the same directory.

b. Press **Next**.

The installer displays the *Enter File Ownership* panel.

Step 10 Specify user and group ownership for the VNDS installation directory. The installer prompts you for the following information:

- User ID
- Group ID

Note The user must be a member of the specified group. The user will be the owner of the VNDS installation directory. Any user that is a member of the specified group will have appropriate permission to run the VNDS software.

Type a valid user name and group name into the appropriate fields then press **Next**.

The installer displays the *Choose the Cisco Configuration Assurance Solution-SP temp folder* panel.

Step 11 Specify the VNDS temporary directory.

Type a temp directory path in the panel's path field or use the file browser to select a path. The path you choose cannot contain embedded spaces.

Note The temp directory holds temporary working files for the product. The path you specify is the full path to this directory.

Note Make sure that the specified directory has appropriate write permissions. The group specified in Step 10 must be able to write to this directory.

a. Press **Next**.

The installer displays the *Choose the Cisco Configuration Assurance Solution-SP config file folder* panel.

Step 12 Specify the VNDS config file archive directory.

a. Type an archive directory path in the panel's path field or use the file browser to select a path. The path you choose cannot contain embedded spaces.

Note The archive directory holds collected device configuration files that have been archived by the product. The path you specify is the full path to this directory.

Note Make sure that the specified directory has appropriate write permissions. The group specified in Step 10 must be able to write to this directory.

a. Press **Next**.

The installer displays the *Configure Cisco Configuration Assurance Solution-SP* panel.

Step 13 Specify server information for this instance of Cisco VNDS. The installer prompts you for the following information:

- Virtual Network Data Server Name
- Virtual Network Data Server ID (0-1022)
- Virtual Network Data Server Address

a. Type the primary IP address of the host in the **Cisco Configuration Assurance Solution-SP Address** field.

Note The primary IP address is required for all VNDS installations. To obtain the IP address, open a command window and run the **ifconfig** command.

b. Fill in additional fields if this instance of Cisco VNDS will participate in an n-tier hierarchy.

c. Press **Next**.

The installer displays the *Configure Cisco Configuration Assurance Solution-SP Client Connectivity* panel.

Step 14 Specify the VNDS Client Connectivity port.

Type a port number or press **Next** to accept the default value.

Note The Client Connectivity port is the port on which the Live Update Service runs. If you enter a non-default port, VNDS clients might be unable to communicate with this service until you make a corresponding change in the client preferences.

The installer displays the *Configure Web Server Connectivity* panel.

Step 15 Specify web server connectivity information.

The installer prompts you for the following:

- Virtual Network Data Server HTTP Port
- Virtual Network Data Server HTTPS Port
- Keystore Directory

a. Fill in each field or press **Next** to accept default values.

Note Write down the web server connectivity settings for future use.

The installer displays the *Set Web Server Administrator Password* panel.

Step 16 Specify the password for the administrator (*cisco*) user account for the VNDS Web Console. The installer prompts you for the following information:

- Enter administrator password
- Confirm administrator password

Type a password into the password fields or press **Next** to accept the default password (*cisco*).

Note Write down the *admin* password. You will need this password to log into the VNDS Web Console for the first time—VNDS Web Server is installed in the local authentication mode by default. Once logged into the Web Console, the *admin* user may change the *admin* password, create user accounts, or change the authentication scheme.

The installer prompts you to configure email notification parameters.

Step 17 If you want to begin receiving email notification from Cisco VNDS as soon as you start VNDS services, configure email notifications at this time. Otherwise, configure notifications when you are ready to begin automated operation (recommended) using the Notification panel in the VNDS Administrative Console.

a. Enter the sender, recipients, and subject prefix for VNDS email notifications or leave these fields blank if you want to configure email notifications post-installation.

b. Click **Next** to proceed.

The installer prompts you for email server settings.

c. Enter the SMTP Server, Port, User Name, and Password or leave these fields blank if you want to configure email notifications post-installation.

d. Click **Install**.

An installation progress panel shows status messages as VNDS installation progresses. Installation normally finishes in several minutes. When installation is complete, the *Web Services Note* panel displays.

Note The installer checks the version of the Oracle Toplink files that you chose in Step 7. If the wrong version files were selected, an error dialog box appears. Click OK to continue. Before operating Virtual Network Data Server, you must locate the correct version of the required Toplink files and copy them to the <*install dir*>/ext directory.

Step 18 Read the *Web Services Note*.

Note VNDS software is installed in HTTP mode. You can optionally configure HTTPS after you have completed your installation workflow. See the "HTTPS Mode" section of the *Release Notes* for more information.

Click **Next** to proceed.

The installer displays the *Install Complete* panel.

Step 19 Click **Done** to exit the installer.

Note Installation of VNDS software is now complete. Return to the workflow you are following and continue with the next step. Do not attempt to start Cisco VNDS or access the Web Console until you complete all steps in the installation workflow.

After you have installed VNDS software, see Configuring the Oracle Database for Cisco VNDS (Linux), page 6-14.

Licensing Notes

You must specify a licensing type for the VNDS software during installation. The installer provides the following options:

- Access licenses from a remote server—Selecting this option results in the VNDS software obtaining a license from a remote host.
- Serve licenses from a new license server on this computer—Selecting this option results in a license server being installed with the VNDS installation. The license server executable installed by Cisco Virtual Network Data Server version 4.0 is the same version license server that is included with programs in other Cisco Solution packages (such as the program included in the Cisco Configuration Assurance Solution) . To start the license server, enter the following from a command prompt:

  ```
  vnes.sh -l <license_server_host> -p <port> LS
  ```

  Note The license server program must be manually restarted when the server reboots.

- Serve licenses from an existing license server on this computer—Selecting this option configures Cisco VNDS to use a license server that is already installed on the host as part of an existing Cisco VNDS or Cisco Solution package. No license server is installed by the VNDS installer.

Note The specified license server must have a valid VNDS license before you can run the software. Check to see if the license server has a valid VNDS license before you attempt to run the VNDS software. Add a license, if needed. Refer to the *Cisco Configuration Assurance Solution–SP User Guide*, Administration chapter, Licensing Operations section for instructions on adding a license.

Configuring the Oracle Database for Cisco VNDS (Linux)

After VNDS software is installed, the Oracle database must be configured for use by VNDS. This involves running an SQL script named setup_accounts.sql that creates tablespaces for the database and a VNDS access account. This SQL script is run on the host system for the Oracle database.

Warning **Do not modify the setup_accounts.sql script. This can cause the installation to fail or prevent VNDS from operating correctly.**

See Configuring the Oracle Database (Linux), page 6-14 for instructions on configuring the Oracle database.

Configuring the Oracle Database (Linux)

Step 1 Log into the VNDS host as **`oracle`** or switch users to the **`oracle`** account. To switch to `oracle`, open a command prompt window and enter the following command:

```
su - oracle
```

Step 2 Copy the SQL scripts from the VNDS installation directory to a directory on the database host where the **`oracle`** user has execute permission. The SQL scripts have a file extension of `.sql`.

Step 3 Navigate to the directory that contains the SQL scripts.

Stay in the command window on the database host (as **oracle**) and continue with step 4.

Step 4 Log into Oracle using the **system** account.

- For a local Oracle database installation, type the following command in the command window:

  ```
  sqlplus system/<system password>
  ```

- For a remote Oracle database installation, type the following command in the command window:

  ```
  sqlplus system/<system password>@<DB TNS Service Name>
  ```

  For example, if the Database TNS Service Name is *o92avnes* and the account password is *magic*, type:

  ```
  sqlplus system/magic@o92avnes
  ```

Step 5 Enter the following command at the *SQL>* prompt:

```
@setup_accounts.sql
```

A message banner appears that states how much free disk space is required on the disk that hosts the database.

Note If you do not have sufficient disk space available to run this script, free up sufficient disk space before proceeding. If you want to cancel the script, press Ctrl-C or close the command window.

Step 6 Press **Enter** to continue.

A message banner displays a notification about Device and Platform Info.

- For Oracle9i, proceed to step 7.
- For Oracle10g, jump to step 8.

Note If you want to cancel the script, press Ctrl-C or close the command window.

Step 7 Press **Enter** to continue.

When configuring Oracle 9i, database parameters are analyzed and a message banner displays with a list of database parameters, database parameter settings, and whether the parameters meet recommended settings. A log of database analysis results is saved to `<install_dir>\analyzedb.<timestamp>.log`.

Note If all parameters meet recommended settings, no further action is required. If one or more parameters do not meet recommended settings, the installer recommends that you run the *dbparamchg.sql* script after you complete this procedure. This will improve data import performance with large networks and increase Oracle memory requirements.

Step 8 Press **Enter** to continue.

A database name appears. If more than one database is available, contact your database administrator to find out which database name to use with Cisco VNDS.

Step 9 Verify the database instance name.

Note If the database is located on a Solaris or Linux system, the database instance name must be a case-sensitive match of the name of the database directory located under the oradata directory (for example, `/uo1/app/oracle/oradata`) on the database host. Look in the `/oradata` directory to ensure that when you enter the database instance name it is a case-sensitive match.

Step 10 Press **Enter** to continue.

The *setup_accounts* script prompts you for the database instance name.

Step 11 Enter the database instance name obtained in step 9.

The *setup_accounts* script prompts you for the user password.

Step 12 Enter the same database user account password that was entered during VNDS installation and written down in Table B-1 on page B-3.

The script informs you that the VNDS user account and all data will be deleted by this script.

Step 13 Press **Enter** to continue.

The *setup_accounts* SQL script configures database storage for use by VNDS and sets up the user account. After the script finishes, the Oracle account information for Cisco VNDS is the user name and password from Table B-1 on page B-3. A log of script actions is saved to <*install_dir*>\setup_accounts.<*timestamp*>.log.

Note When you run this script for the first time, several SQL error messages appear. You can ignore these messages. The messages are the result of the script trying to remove VNDS table and user accounts that do not exist prior to this script being run for the first time.

Type **quit** at the *SQL>* prompt to exit sqlplus.

If the setup_accounts script recommended changing your database settings during step 7, and you agree with the recommended changes, see Modifying Database Parameters (Linux), page 6-17 at this time.

If you do not need to change your database settings or choose not to change them, see Verifying Oracle Configuration for Cisco VNDS (Linux), page 6-19 to verify that Oracle is configured correctly for use with Cisco VNDS.

Modifying Database Parameters (Linux)

Perform Modifying Database Parameters (Linux), page 6-18 on the Oracle 9i database host to modify database parameters. The database parameter changes improve VNDS performance when working with large networks and will increase Oracle memory requirements.

Do not modify database parameters for Oracle 10g unless instructed to do so by Cisco Technical support (see Obtaining Technical Assistance, page fm-xii).

Note Work with your Oracle Database Administrator to run this script.

Modifying Database Parameters (Linux)

Step 1 Log into the database host as **oracle** or switch users to the **oracle** account. To switch to oracle, open a command prompt window and enter the following command:

```
su - oracle
```

Step 2 Open a command window.

Step 3 Navigate to the VNDS installation directory or directory where you copied the VNDS SQL scripts.

Stay in the command window on the database host (as) and proceed with Step 4.

Step 4 Log into Oracle using the **system** account.

- For a local Oracle database installation, type the following command in the command window:

  ```
  sqlplus system/<system password>
  ```

- If the Oracle database is not on the same host system as Cisco VNDS, type the following command in the command window:

  ```
  sqlplus system/<system password>@<DB TNS Service Name>
  ```

  For example, if the Database TNS Service Name is *o92avnes* and the account password is *magic*, type:

  ```
  sqlplus system/magic@o92avnes
  ```

Step 5 Enter the following command at the *SQL>* prompt:

```
@dbparamchg.sql
```

A message is displayed that shows the path to the Oracle spfile that contains the parameters for your database.

Step 6 Make a backup copy of the spfile at the path specified in the previous step.

Step 7 Press **Enter** as many times as needed to step through information messages produced by this script.

When the script is done, a list of the changed parameters and their new settings appears with a reminder to restart the Oracle DB service for the changes to take effect.

Step 8 Type **quit** at the *SQL>* prompt to exit sqlplus.

Step 9 Stop and restart the Oracle database service.

Step 10 If the Oracle database service fails to restart, restore the original spfile for the database and repeat step 9 to recover.

See Verifying Oracle Configuration for Cisco VNDS (Linux), page 6-19 to verify that you can connect to the database through the VNDS account.

Verifying Oracle Configuration for Cisco VNDS (Linux)

Perform the following procedure on the database host to verify that Oracle is configured correctly for use with Cisco VNDS.

Verifying the Oracle Configuration (Linux)

Step 1 Log in to the database host as **`oracle`** or switch users to **`oracle`**. To switch to `oracle`, open a command prompt window and enter the following command:

```
su - oracle
```

Step 2 Open a command window.

Step 3 Verify that you can log into Oracle using the VNDS account.

- For a local Oracle database, enter the following command:

  `sqlplus <user name>/<password>`

  Use the user name and password from Table B-1 on page B-3.

- For a remote Oracle database, enter the following command:

  `sqlplus <user name>/<password>@<DB TNS Service Name>`

  Use the user name and password from Table B-1 on page B-3. For example, if the Database TNS Service Name is *o92avnes* and the VNDS username and password are *vnes* and *pwd* respectively, enter:

  `sqlplus vnes/pwd@o92avnes`

Step 4 If Oracle configuration was not successful, error messages notify you that login has been denied.

- Reconfigure the Oracle database and verify again.

Step 5 If configuration of the Oracle account for Cisco VNDS was successful, an Oracle banner, and a *Connected To:* message appears.

Step 6 Type **quit** at the *SQL>* prompt to exit.

Step 7 Test the Oracle database configuration.

a. Switch users to **root** or a user with permission to run Cisco VNDS. When switching users, open a command prompt window and enter the following command:

```
su - <user>
```

For example, you might enter **su - vnds_user**

b. Navigate to the VNDS installation directory.

Enter the following command:

```
vnes.sh DBAUTOTEST
```

Tests run to verify that the VNDS account can perform needed operations in Oracle.

Output is written to the command window and a separate java window opens to display a summary of results.

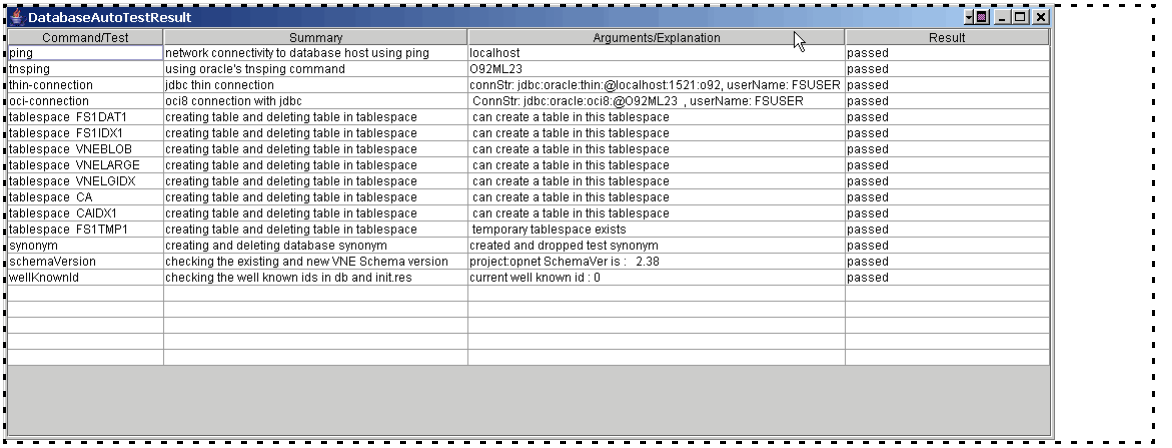
c. Review DBAUTOTEST results.

Note Do not proceed until all tests pass. Figure 6-1 shows a successful result.

– If any of the database tests fail, contact Cisco Technical Support for assistance and provide the DBAUTOTEST results (for more information, see Obtaining Technical Assistance, page fm-xii).

– When all database tests pass, continue with your installation workflow.

Figure 6-1 Example of Successful DBAUTOTEST Results



DatabaseAutoTestResult

Command/Test	Summary	Arguments/Explanation	Result
ping	network connectivity to database host using ping	localhost	passed
tnsping	using oracle's tnsping command	O92ML23	passed
thin-connection	jdbc thin connection	connStr: jdbc:oracle:thin:@localhost:1521:o92, userName: FSUSER	passed
oci-connection	oci8 connection with jdbc	ConnStr: jdbc:oracle:oci8:@O92ML23 , userName: FSUSER	passed
tablespace FS1DAT1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace FS1IDX1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNEBLOB	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNELARGE	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace VNELGIDX	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace CA	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace CAIDX1	creating table and deleting table in tablespace	can create a table in this tablespace	passed
tablespace FS1TMP1	creating table and deleting table in tablespace	temporary tablespace exists	passed
synonym	creating and deleting database synonym	created and dropped test synonym	passed
schemaVersion	checking the existing and new VNE Schema version	project:opnet SchemaVer is : 2.38	passed
wellKnownId	checking the well known ids in db and init.res	current well known id : 0	passed

VNDS installation and database configuration are now complete. Proceed to Verifying the VNDS Software Installation (Linux), page 6-21 to verify the VNDS installation.

Verifying the VNDS Software Installation (Linux)

After the database has been successfully configured for Cisco VNDS, perform the following procedure to verify that the VNDS software is installed correctly.

Verifying the VNDS Installation (Linux)

Step 1 Verify that the license server specified during installation has the required licenses installed.

Note Do not proceed until you have verified that the appropriate licenses are available.

Step 2 Log in to the VNDS host as a member of the VNDS group or switch to a user that is a member of the VNDS group. When switching users, open a command prompt window and enter the following command:

```
su - <user>
```

For example, you might enter **su - vnds_user**

Step 3 Open the *Cisco Virtual Network Data Server Control Panel* as follows:

a. Open a command window and navigate to the VNDS installation directory.

b. Enter the following command:

```
vnes.sh CP
```

Within a minute, the *Cisco Virtual Network Data Server Control Panel* appears.

Step 4 Start VNDS services from the Control Panel by clicking the Start Services button on the tool bar.

A progress dialog appears, and within a few minutes, service start-up completes.

Step 5 Stop VNDS services from the Control Panel by clicking the Stop Services button on the tool bar.

A progress dialog appear appears; services should stop within a few minutes.

Note If the Control Panel fails to open, services fail to start or stop, or error dialog boxes appear, there is a problem with the installation. Contact Cisco Technical Support for assistance if problems persist (for more information, see Obtaining Technical Assistance, page fm-xii).

Step 6 Verify communication with the VNDS Web Server via HTTP.

a. Start the VNDS Web Service by entering the following command:

```
vnes.sh -c start WS
```

Note You must start the Web Service manually before you can access the Web Console.

b. Open a web browser and enter the URL for the Cisco Virtual Network Data Server Web Console.

```
<protocol>://<host>:<port>/vnes
```

As an example, if the VNDS host is myhost.myco.com and the http port is 9190, enter:

```
http://myhost.myco.com:9190/vnes
```

The login page displays.

c. Close the browser window.

Step 7 Click the Exit button on the Control Panel tool bar to exit from Cisco VNDS.

Step 8 Some VNDS services continue to run in the background. If you want to completely shut down VNDS, stop all services (`vnes.sh -c stop ALL`).

Note If you manually stop the Web Service or shut down VNDS by stopping all services, you must manually start the Web Service before you can access the Web Console. See substep a. of Step 6.

Note Before using Virtual Network Data Server, you must change the default port that Cisco Configuration Assurance Solution's Audit and Analysis uses to connect to VNDS. Search the known product issues (as described in Appendix D, "Known Issues") for details on how to configure Audit and Analysis to successfully import from a Virtual Network Data Server running on Linux.

Installing Cisco Report Server

This chapter describes the following procedures:

Installing Cisco Report Server (Windows)

Note Functionality of Cisco Report Server is comparable between Cisco CAS and Cisco CAS-SP; *there is no functional reason to modify this installation* when upgrading to Cisco CAS-SP. However, if Cisco CAS is upgraded to Cisco CAS-SP and an existing Cisco Report Server *installed on the same host* is not upgraded, Cisco Report Server will not appear in the Windows Start menu as a component of Cisco CAS-SP; instead, it will appear as a peer-level program. If you choose to upgrade Cisco Report Server to the version provided with Cisco CAS-SP, it must be reconfigured "from scratch." In such case, reports can still be migrated.

Note You can install Cisco Report Server as either a service or an application. If you install it as a service, a user does not need to be logged on for Cisco Report Server to run, and Cisco Report Server starts and runs automatically when the host is rebooted. You can install Cisco Report Server as an application if the previous

requirements do not apply or for debugging purposes. However, you must decide which method of operation you want to use before installing the Cisco Report Server. You cannot change the method after installation.

Warning **When selecting or creating the installation directory for Cisco Report Server, make sure the directory name DOES NOT contain spaces.**

Step 1 Log in as Administrator before inserting the CD.

Step 2 Insert the installation CD into the CD-ROM drive.

Step 3 Use **Start > Run** and execute the installer. Enter the following installer name:

```
setup_CCASSP.exe
```

The Cisco Report Server installation wizard appears.

Step 4 The *Introduction* panel appears. Press **Next** to continue.

Step 5 The installer displays a panel to choose the installation path. Select a path and press **Next**.

Step 6 By default, Cisco Report Server uses port 9090 for HTTP traffic and 8443 for HTTPS traffic. Determine if these ports are free. If either default port is in use, you must select a different (unused) port in Step 7.

Step 7 The installer displays a panel to select the HTTP/HTTPS ports and Keystore directory used by Cisco Report Server. Specify the desired ports and path (or leave the default settings).

Note During the installation process, you are prompted to specify the Cisco Report Server ports for HTTP (default: 9090) and HTTPS (default: 8443), as well as the Keystore Directory (default: `<install_dir>\security`). Make a note of this information. You will need this information when installing or configuring applications that publish to the Cisco Report Server. The applications will refer to this port as the “Cisco Report Server port.”

After you set these fields, click **Next**.

Step 8 The installer prompts you for the password for logging in to the Cisco Report Server. Enter the desired password and click **Next**.

Step 9 The installer displays a panel asking whether you want to run Cisco Report Server as a Windows service.

- Set the checkbox to run Cisco Report Server as a Windows service.
- Clear the checkbox to run Cisco Report Server as an application.

Then click **Next** to continue.

Note If you run Cisco Report Server as an application, Program Group shortcuts are provided to start and stop Cisco Report Server.

Step 10 If you are installing Cisco Report Server to run as a Windows service, the installer displays a panel to ask whether you want to start the Cisco Report Server service after installation. Set the checkbox to start services after installation. Clear the checkbox to prevent the start of services after installation. Press Install to continue. An Installing Cisco Report Server panel appears.

Step 11 From the Install Complete window, click **Done**.

This concludes the Cisco Report Server installation. Look at the following procedures and perform them if needed:

- Migrating Data from a Previous Installation, page 7-5
- Configuring Cisco Report Server, page 7-6

When you are finished with all Cisco Report Server installation procedures, return to the installation workflow and continue with the next step.

If you plan to access the Cisco Report Server through a firewall, make sure to open the port specified in the installation process to HTTP traffic in the firewall configuration. Also, if the machine on which you are installing the Cisco Report Server has a sleep/power save mode, make sure you turn off this sleep/power save mode. Otherwise, the Cisco Report Server will suspend operations when the machine goes into sleep or power save mode.

Installing Cisco Report Server (Linux)

Warning **When selecting or creating the installation directory for Cisco Report Server, make sure the directory name DOES NOT contain spaces.**

Step 1 Log in as `root`.

Step 2 Insert an installation CD in your CD-ROM drive. (You can install the CDs in any order.)

Step 3 Move to the `unix` directory on the CD, which is typically `/mnt/cdrom/unix`.

Step 4 Enter the following command:

./ReportServer_Cisco_25APL2_273_linux.bin

Step 5 The installer displays a panel to choose the installation path. Select a path and press **Next**.

Step 6 By default, Cisco Report Server uses port 9090 for HTTP traffic and 8443 for HTTPS traffic. Determine if these ports are free. If either default port is in use, you must select a different (unused) port in Step 7.

Step 7 The installer displays a panel to select the HTTP/HTTPS ports and Keystore directory used by Cisco Report Server. Specify the desired ports and path (or leave the default settings).

Note During the installation process, you are prompted to specify the Cisco Report Server ports for HTTP (default: 9090) and HTTPS (default: 8443), as well as the Keystore Directory (default: `<install_dir>\security`). Make a note of this information. You will need this information when installing or configuring applications that publish to the Cisco Report Server. The applications will refer to this port as the "Cisco Report Server port."

After you set these fields, click **Next**.

Step 8 The installer prompts you for the password for logging in to the Cisco Report Server. Enter the desired password and click **Next**.

Step 9 From the Install Complete window, click **Done**.

This concludes the Cisco Report Server installation. Look at the following procedures and perform them if needed:

- Migrating Data from a Previous Installation, page 7-5
- Configuring Cisco Report Server, page 7-6

When you are finished with all Cisco Report Server installation procedures, return to the installation workflow and continue with the next step.

Migrating Data from a Previous Installation

If you want to retain information from previous versions of Cisco Report Server, you can migrate the previous data after installing the new version of Cisco Report Server. Use the following procedure to migrate the old data.

Warning **Migration of reports from previous versions of Cisco Report Server is supported. However, you must not uninstall the previous version of Cisco Report Server prior to performing the migration (described in the "Migrating Data from a Previous Installation" section on page 7-5). Doing so results in the loss of data from the previous version.**

Note Migration does not move old user data to the new installation. You must manually recreate user data.

Migrating Data from a Previous Cisco Report Server Version

Step 1 Install the newest version of Cisco Report Server.

Step 2 Log in to the new version of Cisco Report Server as an administrator.

Note To log in to Cisco Report Server for the first time, you can use one of three preconfigured accounts: *admin* (password specified during installation), *test1* (password: *test1*), or *test2* (password: *test2*).

Step 3 Navigate to Settings > Migration.

Step 4 Enter the name of the directory for the previous Cisco Report Server version in the space provided. For example:
`C:\Cisco\Cisco Configuration Assurance Solution-SP 1.0\ReportServer\2.0.1.`

Step 5 Click the Verify button. The migration tool will check to see if the entry is a valid directory. If the specified directory is not found or does not have any reports, you will see a warning message and no migration is performed.

Step 6 Select the checkbox to "Import Custom Folders and Filters", if desired. This checkbox will cause the migration tool to import all previously created custom folders and filters. Not checking this box will not impact the migration of any reports, however.

Step 7 Click Import to complete the migration or Cancel to quit.

Configuring Cisco Report Server

After you install Cisco Report Server, you must configure the administrative settings. For instructions on how to perform the following tasks, see the corresponding sections in the Cisco Report Server Administration chapter of the Cisco Report Server *User Guide*:

- To log in for the first time, see the "Logging in to Cisco Report Server" section.
- To set up user accounts and passwords, see the "User Administration" section.
- To set up secure communications for Cisco Report Server, see the "Secure Web Portal" section.
- (*Optional*) To change the activation period for the Cisco Report Server cleanup operation, see the "Setting the Activation Period" section.
- (*Optional*) To change the maximum age limit for reports on the Cisco Report Server, see the "Setting the Maximum Age Limit of Published Reports" section.

Installing the OTL Service (Windows)

Perform the following procedure to install the OTL service on Windows.

Note The OTL feature is supported on Windows hosts only.

Note The OTL service can communicate with one and only one instance of Audit and Analysis. This means that, if you have multiple instances of Audit and Analysis or Audit and Analysis–SP installed on the same host, and you want to use OTL with more than one instance, you must install one OTL service for each instance.

Installing the OTL Service

Step 1 Load the Cisco CAS–SP, Audit and Analysis installation CD into the CD-ROM drive, or download the installer executable on the same host where Cisco Audit and Analysis–SP. is installed.

Step 2 If you want to install the OTL service in a directory that does not yet exist, create that directory now.

Step 3 Navigate to the directory containing the OTL installer.

Step 4 Double-click on the file called Setup.

The InstallShield Wizard opens.

Step 5 Click the Next button to continue with installation.

Step 6 Specify the following information, as prompted by the OTL installer:

- The directory where you want to install OTL
- The HTTP port you want the OTL server to use

Note Be sure to use a unique http port on which Cisco Audit and Analysis–SP will listen for network events. There must be no other applications listening on this port. Make sure this is the same port that Cisco VNDS will use to contact OTL.

Note To change the HTTP port setting at any time after installation, edit the setting in the file `<release_dir>\sys\configs\global_prefs\op_task_launcher.ef`.

Step 7 Click Finish to close the installer when the installation finishes.

Note To run OTL, you must make additional configuration steps in other programs. For more information, see the following section of the product documentation:
Cisco Audit and Analysis–SP User Guide > OPNET Task Launcher

Managing Licenses

To start a Cisco Solutions program such as Cisco Audit and Analysis–SP or Cisco Virtual Network Data Server, you must have a valid license for that program installed on the local or a remote computer.

This chapter describes the following operations:

- Adding a License, page 9-3—Perform this workflow if you have purchased an initial or additional license and want to add it.
- Upgrading a License, page 9-4—Perform this workflow if you have already added a Restricted license and want to upgrade it to an Unrestricted license.
- Deregistering a License, page 9-7—Perform this workflow if you need to deregister a license.

Note Licenses (that is, the License Manager) must reside on a host that is accessible to the component program at startup. This can be the local host where the component program is installed or a remote host. For more information about licensing options, see the "Product Licensing" section on page 1-7.

Using the License Manager

You can see which licenses and license servers are installed on your network by using the License Manager. You can also perform license operations from the License Manager using the following procedure.

Step 1 Start the License Manager for the installed program. On a Windows host, for example, you might see the following shortcut:

Start > Programs > Cisco Audit and Analysis–SP 2.0 > License Manager

Step 2 In the License Manager, select the license(s) or license server you want to act on, then click on the correct operation button on the right.

Note The License Manager might show some child windows that prompt you for additional information, such as which product modules to use. You do not need to specify these options to use the License Manager; generally you can click **OK** to accept the default settings and close the child window.

License Names

License names in the License Manager differ from the Cisco component names. The following table shows the component names and the license names that appear for each component.

Table 9-1 Cisco Product Component Names and License Names

Cisco Component Name	License Name
Audit and Analysis	SP Sentinel
Virtual Network Data Server	VNE Server

Adding a License

Table 9-2 shows the workflow for adding your licenses.

Table 9-2 Adding a License: Workflow

	Description	Reference
Step 1	Obtain a username and password (if you have not done so already)	Obtaining a Username and Password, page 9-3
Step 2	Add program license(s) using one of the following methods for each license:	
	• Express method	Adding a License (Express Method), page 9-8
	• Browser method (if Express method does not work)	Adding a License (Browser Method), page 9-9
	Contact Cisco Technical Support (if Express and Browser methods do not work)	Technical Support for Licensing Operations, page 9-14
	Note You must repeat the Add License procedure for every computer on which you want to add a license. In this case, you must do the add-license operation twice—once for each computer.	

Obtaining a Username and Password

To add a license, you must have a valid username, password, and group ID. To obtain this information, you must register your Cisco CAS–SP product with Cisco Systems, Inc. Instructions for doing this are listed on the Software License Claim Certificate that is included in your product installation package. For more information, see the "Registering Your Cisco Solution Product" section on page 1-5.

After your registration is confirmed, Cisco will send you an email with a username, password, and Group ID number. You will need this information when you add the component licenses as described in the following sections.

After you obtain a username and password, you can add your licenses as described in the "Adding a Component License (Express Method)" procedure on page 9-8 or the "Adding a Component License (Browser Method)" procedure on page 9-9.

Upgrading a License

Table 9-3 shows the workflow for upgrading your licenses. For information about different grades of licenses, see the "Product Licensing" section on page 1-7.

Table 9-3 Upgrading a License: Workflow

	Description	Reference
Step 1	Obtain an Upgrade authorization from Cisco Systems, Inc.	Getting an Upgrade Authorization from Cisco Systems, Inc., page 9-5
Step 2	Deregister the original (Restricted) license using one of the following methods:	
	• Express method	Deregistering a License (Express Method), page 9-11
	• Browser method (if Express method does not work)	Deregistering a License (Browser Method), page 9-12
	• Contact Cisco Technical Support (if Express and Browser methods do not work)	Technical Support for Licensing Operations, page 9-14
Step 3	Add the upgraded (Unrestricted) version of the original license using one of the following methods:	
	• Express method	Adding a License (Express Method), page 9-8
	• Browser method	Adding a License (Browser Method), page 9-9
	• Contact Cisco Technical Support (if Express and Browser methods do not work)	Technical Support for Licensing Operations, page 9-14
Note	You must perform both procedures—that is, deregister the Restricted license and add the Unrestricted license—before you can use Unrestricted licensing mode. Also, keep in mind that after you deregister your current (Restricted) license, you will be unable to use the software until you register the updated (Unrestricted) license.	

Getting an Upgrade Authorization from Cisco Systems, Inc.

Before you can upgrade a Cisco Solution license, you must obtain an authorization from Cisco Systems, Inc. To obtain an authorization, do the following:

Step 1 Go to the following URL:

http://www.opnet.com/support/cisco_qsp.html

Step 2 Follow the **My PAKS** link to see the Product Authorization Keys you have added already. Note the PAK of the product that you want to upgrade from Restricted to Unrestricted.

Step 3 Go to one of the URLs listed in the"Registration Information" section on page 1-6.

Step 4 Follow the instructions on the Cisco licensing page. You must submit the Product Authorization Key for both the new license and the original license that you want to upgrade.

After you submit the requested information, Cisco Systems will email you an authorization to proceed with the upgrade (go to Step 2 of Upgrading a License, page 9-4).

Configuring Node Pack Licenses and Notifications

You should purchase node pack licenses based on the size of your network; you must also register the licenses before you can create network models and run analyses. (For more information, see Node Pack Licensing, page 1-8.)

Before you create and analyze networks in Cisco Audit and Analysis–SP, you must configure the node pack licenses and notifications.

Configuring Warnings and Notifications

There are various warning messages to inform you of licensing requirements. Warning messages display when your network size

- *approaches* the maximum number of nodes

- *reaches* the maximum number of nodes
- *exceeds* the maximum number of nodes

To define notifications, choose License > Notification Settings.
Cisco Audit and Analysis–SP can send warnings and notifications to one or more of the following: e-mail/pager, automation log, Remedy trouble ticket. Defining notifications is especially useful when analyses are automated.

Configuring the "Node Pack Configuration" Preference

Cisco Audit and Analysis–SP cannot create or analyze a network when the number of nodes exceeds the number of nodes defined by the node pack license configuration. You must set the Node Packet Configuration preference to specify the number of nodes in your network. This preference has the following properties:

- **Name:** Node Pack Configuration
- **Description:** Specifies the node pack license obtained at startup and optional notifications. Valid values are 100_node, 300_node, 500_node, 1000_node, 2500_node, and 5000_node. You can select multiple node licenses to combine the values. For example, select 100_node and 300_node to analyze a 400-node network.
- **Tag:** node_pack_configuration
- **Type:** string
- **Default:** " " (A network with up to 50 nodes can be analyzed if no node pack license is selected.)

Adding a Module to the Product Options List

After you add a license for a product module, you must update your Product Options list so that the program requests the module license on startup.

Adding a Module to the Product Options List

Step 1 Start the program to which the product module applies.

Step 2 In the main program window, choose License > Product Modules.

Step 3 In the Select Product Modules, select the checkbox for the module you have added. Then click OK.

Step 4 For the change to take effect, you must exit and restart the program.

Deregistering a License

Table 9-4 shows the workflow for deregistering licenses.

Table 9-4 Deregistering a License: Workflow

	Description	Reference
Step 1	Deregister a program license(s) using one of the following methods for each license:	
	• Express method	Deregistering a License (Express Method), page 9-11
	• Browser method (if Express method does not work)	Deregistering a License (Browser Method), page 9-12
	Contact Cisco Technical Support (if Express and Browser methods do not work)	Technical Support for Licensing Operations, page 9-14

Refreshing a License

After installing an update to the Cisco Configuration Assurance Solution–SP software, you must refresh your licenses by contacting Cisco Systems as described in the "Technical Support for Licensing Operations" section on page 9-14.

License Operations

Adding a License (Express Method)

The following procedure is the quickest and easiest way to add a license. This method requires that your computer be able to communicate directly with the Cisco Solutions license-registration server over the Internet, either directly or using a proxy server.

Note The Express method can fail due to firewall restrictions, socket or proxy errors, or transaction time-outs. If you cannot add the license using this method, try the Browser method (as described in Adding a License (Browser Method), page 9-9).

Adding a Component License (Express Method)

Step 1 Start the License Manager for the installed program. On a Windows host, for example, you might see the following shortcut:

Start > Programs > Cisco Audit and Analysis–SP 2.0 > License Manager

Step 2 In the License Manager, click on the green dot that represents the license server on the computer where you want to add the license. (The license server computer might not be the same as your local computer.)

Click on the **Add License** button on the right side of the box.

Step 3 When prompted to select the transaction method, click **Express**. This method is easiest and fastest.

Step 4 Enter the **Username**, **Password**, and **Group ID** that you received when you registered your product with Cisco Systems, Inc. (as described in the "Obtaining a Username and Password" section on page 9-3).

Step 5 If the computer uses a proxy server, click on **Specify Proxy** button and fill in the information.

Step 6 The next screen shows a list of available licenses. To select one license, click on it. To select multiple licenses, control-click or drag on the licenses.

Note Select only the licenses you want to add to the computer of the license server you have selected. (If you also want to add other licenses to a different computer, you must repeat this procedure for that computer.)

Step 7 After you select the licenses you want to add, click on the **Add License** button at the bottom. A progress window might appear while the license is added to your computer. A window should then appear and say that the license operation succeeded.

Step 8 When the operation is complete, the *Select Product Modules* box might appear. This allows you to select the modules you want to use. (In most cases, you should select all available modules.)

Step 9 To start using the program, exit the License Manager and start the program.

Adding a License (Browser Method)

Before using the Browser method, try the Express method. With the Express method, there is no need to exchange codes and you can add many licenses to your computer in one operation. Use this procedure if the Express method fails or you prefer to use the Browser method.

Note If you still cannot add your licenses using this method, see the "Technical Support for Licensing Operations" section on page 9-14.

Adding a Component License (Browser Method)

Step 1 Start the License Manager for the installed program. On a Windows host, for example, you might see the following shortcut:

Start > Programs > Cisco Audit and Analysis–SP 2.0 > License Manager

Step 2 *License Manager:* Click on the green dot that represents the license server on the computer where you want to add the license. (The license server computer might not be the same as your local computer.)

Click **Add License** on the right side of the window.

Step 3 *License Manager:* When prompted, click **Browser**. The following events should now occur:

- The License Manager launches your Web browser and points it to the Cisco Solutions Quick Support Page.
- The License Manager shows a transaction code and a hostname.

Step 4 *Web browser:* Enter the **Username** and **Password** that you received when you registered your product with Cisco Systems, Inc. (as described in the "Obtaining a Username and Password" section on page 9-3).

If your browser fails to launch, start it manually and navigate to the following URL:

http://www.opnet.com/support/cisco_qsp.html

Then follow the **My Licenses** link in the browser window.

Step 5 *Web browser:* Click **Perform license operations**, then select **Add License (add_permits)** and click **Next**. Back in the License Manager, a dialog box containing a Transaction Code and Hostname field should appear.

Step 6 *Web browser:* Copy the Transaction Code and Hostname from the License Manager into the corresponding fields in the browser. You can either copy/paste the text or type it manually.

Note Make sure there are no extra spaces before or after the code or hostname.

Step 7 *Web browser:* Click **Next**.

Step 8 *Web browser:* When the *Select the starting license number* page appears, select the lowest license ID that you want to add to your computer. If you want to add only one license, select that license.

Step 9 *Web browser:* When the *Select the ending license number* page appears, select the highest license ID that you want to add to your computer. If you want to add only one license, select that license. The confirmation page appears.

Step 10 *Web browser:* When the License Registration Confirmation page appears, check that the information is correct, then click **Get Approval Code**. The approval code appears.

Step 11 *License Manager:* Click **Next** and enter the approval code that appears in the web browser.

Note This code can be very long, so make sure you copy the entire approval code.

Step 12 *License Manager:* After you enter the approval code, click **Next**.

Step 13 *License Manager:* If the *Select Product Modules* license window appears, click **OK**. Then click **File > Exit** to close the License Manager.

Step 14 To start using the program, exit the License Manager and start the program.

Deregistering a License (Express Method)

The following procedure is the quickest and easiest way to deregister a license. This method requires that your computer be able to communicate directly with the Cisco Solutions license-registration server over the Internet, either directly or using a proxy server.

Note The Express method can fail due to firewall restrictions, socket or proxy errors, or transaction time-outs. If you cannot deregister the license using this method, try the Browser method (as described in the "Deregistering a License (Browser Method)" section on page 9-12).

Deregistering a Component License (Express Method)

Step 1 Start the License Manager for the installed program. On a Windows host, for example, you might see the following shortcut:

Start > Programs > Cisco Audit and Analysis–SP 2.0 > License Manager

Step 2 In the License Manager, expand the license file by clicking on the **+** sign next to the **License file** folder icon. Make sure the license you want to deregister is available (green).

Note If a license is represented by a "white page" icon, that license is currently in use. If you want to deregister a license that is in use, quit the component that is using it, then choose **File > Refresh Server Information** in the License Manager.

Step 3 Select the license you want to deregister by clicking on it. To select one license, click on it. To select multiple licenses, control-click or drag on the licenses.

Step 4 Click **Deregister License** on the right side of the License Manager window.

Step 5 When prompted to select the transaction method, click **Express**. This method is easiest and fastest.

Step 6 When the *Authentication* window appears, enter your **Username**, **Password**, and **Group ID** in the appropriate fields.

Step 7 If the computer uses a proxy server, click **Specify Proxy**; when the *Specify proxy server information* window appears, fill in the requested information and click **OK**.

Step 8 Click **OK** in the *Authentication* window.

- A progress window might appear while the license is deregistered from your computer.
- A window should then appear to indicate that the operation succeeded.

Deregistering a License (Browser Method)

Before using the Browser method, try the Express method. With the Express method, there is no need to exchange codes and you can add many licenses to your computer in one operation. Use this procedure if the Express method fails or you prefer to use the Browser method.

Note If you still cannot deregister your licenses using this method, see the "Technical Support for Licensing Operations" section on page 9-14.

Deregistering a Component License (Browser Method)

Step 1 Start the License Manager for the installed program. On a Windows host, for example, you might see the following shortcut:

Start > Programs > Cisco Audit and Analysis–SP 2.0 > License Manager

Step 2 *License Manager:* Expand the appropriate license file by clicking on the **+** sign next to the **License file** folder icon. Make sure the license you want to deregister is available (green).

Note If a license is represented by a "white page" icon, that license is currently in use. If you want to deregister a license that is in use, quit the component that is using it, then choose **File > Refresh Server Information** in the License Manager.

Step 3 *License Manager:* Select the license you want to deregister by clicking on it. To select one license, click on it. To select multiple licenses, control-click or drag on the licenses.

Step 4 *License Manager:* Click **Deregister License**.

Step 5 *License Manager:* When prompted, click on the **Browser** button.

Step 6 The License Manager launches your Web browser and points it to the Cisco Quick Support page. If your browser fails to launch, start it manually and navigate to the following URL:

http://www.opnet.com/support/cisco_qsp.html

Step 7 *Web browser:* Log in with your Cisco Solution username and password. Then click on **My Licenses**.

Step 8 *Web browser:* Follow the **Perform license operations** link, then select **Deregister License (delete_permits)** and click **Next**.

Back in the License Manager, a dialog box containing a Transaction Code and Hostname field should appear.

Step 9 *Web browser:* Copy the **Transaction Code** and **Hostname** from the License Manager into the browser window, then click **Next**. You can either paste the text or type it manually.

Note Make sure there are no extra spaces before or after the text you enter.

Step 10 *Web browser:* When the *Select the starting license number* page appears, select the lowest license ID that you want to deregister from your computer. If you want to deregister only one license, select that license.

Step 11 *Web browser:* When the *Select the ending license number* page appears, select the highest license ID that you want to deregister from your computer. If you want to deregister only one license, select that license.

Step 12 *Web browser:* When the License Registration Confirmation page appears, check that the information is correct, then click **Get Approval Code**. The approval code appears.

Step 13 *License Manager:* Click **Next** and enter the approval code that appears in the browser.

Note This code can be very long, so make sure you copy the entire approval code.

Step 14 *License Manager:* Click **Next**. The confirmation code appears.

Step 15 *Web browser:* Enter the confirmation code that appears in the License Manager, then click **Next**.

The confirmation code is saved in the Session Log, which is available from the Help menu in the Cisco Solution software.

Step 16 *License Manager:* click **Done**. The license is deregistered and you can now add it to another computer.

Technical Support for Licensing Operations

If you cannot manage your licenses using the Express or Browser methods, or if you have additional questions or problems regarding your licenses, you can do the following:

- Go to the Cisco Solutions Quick Support Page:

http://www.opnet.com/support/cisco_qsp.html

- Contact Cisco Systems as described in the "Obtaining Technical Assistance" section on page fm-xii

CHAPTER 10

Uninstalling Cisco Audit and Analysis–SP

Use the procedures in this chapter to Cisco Audit and Analysis–SP.

Uninstalling Cisco Audit and Analysis–SP (Windows)

This section contains the following procedures:

Uninstalling Cisco Audit and Analysis–SP (Windows/Standard)

This is the recommended procedure for uninstalling Cisco Audit and Analysis–SP.

Warning **Do not use this procedure if two different releases of Cisco CAS–SP exist on the machine and you are removing the older release. Instead, use the "Uninstalling Cisco Audit and Analysis–SP (Windows/Advanced)" procedure on page 10-3.**

Uninstalling Cisco Audit and Analysis–SP (Standard)

Step 1 If this machine has licenses installed on it and there are no other versions of the program using the licenses, deregister the licenses. Use either the "Deregistering a Component License (Express Method)" procedure on page 9-11 or the "Deregistering a Component License (Browser Method)" section on page 9-13.

Step 2 Open the Windows Control Panel from the Start menu:

Start > Settings > Control Panel

Step 3 In the Windows Control Panel, double-click **Add/Remove Programs**.

Step 4 Scroll down the list of installed programs, select the entry for the program you want to remove, and click **Remove**. Repeat for the corresponding documentation and model library. Example names:

- Cisco Configuration Assurance Solution–SP 2.0 - Service Provider Module
- Cisco Configuration Assurance Solution–SP Documentation 2.0
- Model Library for Cisco Configuration Assurance Solution–SP 2.0

If you cannot uninstall Cisco Audit and Analysis–SP by using the Add/Remove Programs control panel, use the "Uninstalling Cisco Audit and Analysis–SP (Windows/Advanced)" procedure on page 10-3 to ensure that all of the Cisco Audit and Analysis–SP files have been removed.

Step 5 If this machine is running a local license server from the Cisco Audit and Analysis–SP installation, use the Windows Services Manager to stop the OPNET License Server service.

In Add/Remove Programs, select and remove "OPNET License Server 12.0.A".

Uninstalling Cisco Audit and Analysis–SP (Windows/Advanced)

You should do this procedure ONLY if you could not uninstall Cisco Audit and Analysis–SP using the "Uninstalling Cisco Audit and Analysis–SP (Windows/Standard)" procedure on page 10-1.

Uninstalling Cisco Audit and Analysis–SP (Advanced)

Step 1 If this machine has licenses installed on it and there are no other versions of the program using the licenses, deregister the licenses. Use either the "Deregistering a Component License (Express Method)" procedure on page 9-11 or the "Deregistering a Component License (Browser Method)" procedure on page 9-13.

Warning **Do not deregister the Cisco Audit and Analysis–SP license if you will continue to use a later release of Cisco Audit and Analysis–SP.**

Step 2 Remove the installation directory of the release you are uninstalling. Typical paths:

- `C:\Program Files\Cisco\CiscoCASSP2.0`

Step 3 If you had licenses installed on this machine, delete the `C:\OPNET_license` directory. Be sure you have already deregistered the licenses (as described in Step 1) before deleting the directory.

Warning **Do not delete the license directory if it contains licenses being used by other versions of Cisco or OPNET software.**

Step 4 There are shortcuts under the **Start > Programs** menu. You can remove these using the Advanced Taskbar properties.

a. Right-click on the Windows task bar.

b. Select **Properties**. The *Taskbar Properties* dialog box appears.

c. Choose the **Advanced** tab.

d. Click the **Advanced** button under Customize Start Menu. Windows Explorer opens.

e. Go up the tree to **All Users > Start Menu**, then delete the directories relating to the Cisco CAS–SP software being removed.

Step 5 Cisco Audit and Analysis–SP creates two directories in your user's home directory (`op_admin` and `op_models`).

These directories can be deleted if you no longer wish to keep your custom models and projects.

Warning **Do not delete these directories if your computer contains other versions of Cisco or OPNET software.**

Step 6 Remove the InstallShield bookkeeping files.

a. Make sure that you can view hidden system files on your PC. This procedure varies on different versions of Windows; ask your system administrator if you do not know how to do this.

b. Open the following directory:

```
C:\Program Files\InstallShield Installation Information\
```

c. You will see some directories with long names consisting of numbers and letters surrounded by { } (these are called GUID names). CTRL-F to find files and look for the following:

Files named: *.ini

Containing text: OPNET, Cisco, or similar

d. Determine which directories apply to the release you are uninstalling, using one or more of the following methods:

– Look in the *.ini files to see if there is a release number.

– Look at the date timestamp of the *.ini files to see if they match the installation date of the release you are removing.

– Open the `\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\` registry tree (as described in Step 7), match the registry keys to the GUID name of the *.ini file's directory, and check the release number in the registry.

Make a note of the GUID names of directories that contain matching *.ini files.

e. Remove the directories that contain *.ini files for the correct release from the InstallShield Installation directory.

   If these directories are not deleted along with the Cisco Solution software, future Cisco Solution installations might fail.

Warning **DO NOT delete the entire InstallShield Installation Information directory, because other software you have installed may have information installed here. Be sure to delete only those directories relating to Cisco CAS–SP software.**

Step 7 Remove Registry entries.

Warning **Be very careful when you edit the system registry. Incorrect changes to the registry can cause your Windows system to become unstable. You might want to create a backup before editing the registry.**

a. Start regedit: From the Windows Start menu, choose **Run**, then enter `regedit` and click **OK**.

b. Open the registry tree to `\\HKEY_LOCAL_MACHINE\SOFTWARE\`

c. Delete the registry key for the software being removed. Example registry keys:

```
OPNET Technologies\Cisco Configuration Assurance Solution-SP 2.0
- Service Provider Module\OPNET\12.0.A
```

d. Open the registry tree to `\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\`

e. Match the registry keys with the GUID names you recorded in Step 6d and delete them from the registry.

f. Quit regedit.

You have now removed the current release of Cisco Audit and Analysis–SP entirely from your system.

Uninstalling Cisco Audit and Analysis–SP (Linux)

Perform the following procedure to remove the Application Analysis software from your computer.

Step 1 Open a command window.

Step 2 Enter the following command:

```
rm -rf <install_dir>
```

where *<install_dir>* is the directory where Application Analysis is installed. For example, suppose Cisco Audit and Analysis–SP is installed in the following directory:

```
/usr/CiscoCAS-SP/2.0
```

In this case, you would enter:

```
rm -rf /usr/CiscoCAS-SP/2.0
```

Warning **When you enter this command, take care that you specify the exact directory where Cisco Audit and Analysis–SP is installed. If you enter the wrong path—the parent directory, for example—you might delete other software by accident.**

Uninstalling Cisco Virtual Network Data Server

Use the procedures in this chapter to uninstall Cisco VNDS:

Removing VNDS Database Contents (Optional)

If you want to completely remove the tablespace files and user account for Cisco VNDS 4.0 from a local database, perform Removing Cisco VNDS Database Contents, page 11-2. You do not need to perform this procedure if you are updating the Cisco VNDS installation.

Warning **Perform this procedure only if you are permanently removing Cisco VNDS from a system AND want to remove database contents as well as the product installation.**

Note If you choose to perform this procedure, you must do it before you remove the Cisco VNDS installation.

Removing Cisco VNDS Database Contents

Step 1 Log into the Cisco VNDS host using an account with administrator and ORA_DBA privileges.

Step 2 Stop services and exit the Control Panel.

Step 3 Open a command window and use the **cd** command to set the working directory to the Cisco VNDS installation directory. An example installation directory might be:

- Windows: `C:\Cisco\VNDServer\4.0.2_<build_number>`
- Linux: `/opt/cisco/VNDServer/4.0.2_<build_number>`

Step 4 Stop all VNDS background services/daemons by entering the following command:

- Windows: **vnes.bat /svc_cmd stop ALL**
- Linux: **vnes.sh -c stop ALL**

Step 5 Type: **sqlplus system/<*password*>**

A *Connected to:* Oracle banner message appears if you succeed in logging into Oracle.

Step 6 To get a list of database instance names, type: **select name from v$database;**

A list (probably just one item) of database names known to Oracle appears. If more than one name appears, work with your DBA to identify which one is used for Cisco VNDS.

Step 7 While still in sqlplus, type: **@drop_accounts.sql <*dbname*>**

where the **<*dbname*>** is the one identified in the previous step.

- Progress messages appear as the user account and tablespace files are deleted.
- When done, the database instance still exists, but the tables and account used by Cisco VNDS no longer exist.

Note ALL network project data written to the database by Cisco VNDS is deleted by this procedure.

Uninstalling Cisco VNDS (Windows)

This section includes the procedures described in the following table.

Procedure	Description
Uninstalling Cisco VNDS on Windows (Standard), page 11-3	Procedure for uninstalling Cisco VNDS 4.0.
Removing All VNDS Elements (Advanced), page 11-5	Procedure for removing residual elements of the VNDS 4.0 installation (such as top-level Windows Registry keys and Program Group shortcuts). Perform this procedure ONLY if you need to completely remove everything installed or generated by Cisco VNDS 4.0.
Removing Prior Cisco VNDS Release After Software Update, page 11-7	Procedure for removing VNDS 3.5 following successful installation of Cisco VNDS 4.0 and migration of product configuration.

Use the "Uninstalling Cisco VNDS on Windows (Standard)" procedure on page 11-3 to uninstall the current release. If you wish to completely remove all traces of the current release from a machine, first perform "Uninstalling Cisco VNDS on Windows (Standard)" procedure on page 11-3 then continue on to "Removing All VNDS Elements (Advanced)" procedure on page 11-5.

To uninstall VNDS 1.1 after you update to the current release, perform "Removing Prior Cisco VNDS Release After Software Update" procedure on page 11-7.

Uninstalling Cisco VNDS on Windows (Standard)

Perform the following procedure to remove the VNDS 4.0 software from your computer.

Step 1 Log into the Cisco VNDS host using an account with administrator privileges.

Step 2 Stop services and exit the Control Panel.

Step 3 Open a command window and use the `cd` command to set the working directory to the Cisco VNDS installation directory. An example installation directory might be:

`C:\Cisco\VNDServer\4.0.2_<build_number>`

Step 4 Stop all VNDS background services by entering the following command:

Windows: `vnes.bat /svc_cmd stop ALL`

Step 5 Open the Windows Control Panel from the Start menu:

Start > Settings > Control Panel

Step 6 In the Windows Control Panel, double-click **Add/Remove Programs**.

Step 7 Scroll down the list of installed programs, select the entry for Cisco Virtual Network Data Server 4.0, and click **Remove**.

The Windows uninstaller removes the following items:

- Windows services
- Desktop shortcut
- Most Windows Registry entries
- Most Program Group shortcut entries
- Most of the installation directory

Step 8 Delete the remnants of the corresponding installation directory. For example, the installation directory might be:

`C:\Cisco\VNDServer\4.0.2_<build_number>`

After you complete this procedure, the following remain:

- top-level Windows Registry entry for the release
- top-level Program Group shortcut for the release
- VND Server temporary directory
- VND Server archive directory
- Jre directory

Removing All VNDS Elements (Advanced)

If you wish to completely remove all traces of Cisco Virtual Network Data Server 4.0 from a machine, first perform "Uninstalling Cisco VNDS on Windows (Standard)" procedure on page 11-3 then use the "Removing All VNDS Elements (Advanced)" procedure on page 11-5 to remove residual components of the installation.

Note Perform this procedure ONLY if you need to completely remove everything installed or generated by Cisco Virtual Network Data Server 4.0.

Removing All Cisco VNDS Elements

Step 1 Perform "Uninstalling Cisco VNDS on Windows (Standard)" procedure on page 11-3 if you have not already done so.

Step 2 Log into the VND Server host using an account with administrator privileges.

Step 3 Delete the temporary directory. Typical temporary directory:

```
C:\op_admin\temp\vne
```

Note If you have another VNDS release that you want to keep and it uses the same parent directory, skip this step.

Step 4 Delete the archive directory. Typical archive directory:

```
C:\op_admin\archive
```

Note If you have another VNDS release that you want to keep and it uses the same archive directory, skip this step.

Step 5 Delete the `Java Jre` directory (if it remains). This directory is located under the parent install directory. Typical Jre directory:

```
C:\Cisco\Jre
```

Note If you have another VNDS release that you want to keep and it is installed to the same parent directory (for example C:\Cisco), skip this step. Otherwise, you'll remove the Jre used by a release you want to keep.

Step 6 Delete the top-level Program Group shortcut for the release. All users have a shortcut. Delete the `Cisco Virtual Network Data Server 2.0` shortcut from:

```
C:\Documents and Settings\All Users\Start Menu\Programs
```

Step 7 Start regedit: From the Windows Start menu, choose **Run**; then enter **`regedit`** and click **OK**.

Warning **Be very careful when you edit the system registry. Incorrect changes to the registry can cause your Windows system to become unstable. You might want to create a backup before editing the registry.**

Step 8 In the Windows Registry Editor, find and select the registry key for the software being removed. Example registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OPNET Technologies\
Cisco VND Server 4.0.2
```

Step 9 Select **Delete** from the menu to delete the entry.

Step 10 Verify that the uninstaller entry in the Registry has been removed. Remove the entry if it still exists in the Registry at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall
```

Example entry:

```
Cisco Virtual Network Data Server 2.0
```

Step 11 Verify that any services installed by Virtual Network Data Server are gone. Remove the following services if they still exist in the Registry at the following location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

`-OPNETVNES`*`xxx`*

`-OPNETVnes`*`xxx`*

Where *xxx* is AdapterServer, BootstrapService, etc.

Step 12 Exit the Windows Registry Editor.

At this point, Cisco Virtual Network Data Server is completely removed from your system.

Removing Prior Cisco VNDS Release After Software Update

Perform this procedure if you wish to remove Cisco Virtual Network Data Server 3.5 after you have installed Cisco VNDS 4.0 and migrated your product configuration.

If you want to remove Cisco VNDS 3.5 completely from a machine that has not been updated to the current release, Refer to the Installation Guide for Cisco Configuration Assurance Solution 1.1 or Network Planning Solution 1.1.

Note Do not run the Windows uninstaller for a previous VNDS release after you have updated to the current software release. Doing so may impact the current release.

Removing a Prior VNDS Release After Update

Step 1 Delete the VNDS 3.5 install directory. Typical default install directory:

`C:\Cisco\CiscoCAS\VNEServer\3.5.2_<build_number>`

`C:\Cisco\CiscoNPSSPM1.1\VNEServer\3.5.2_1107<`*`build_number`*`>`

Step 2 Delete the following VNDS Program Group shortcuts from the Program Group menu for the appropriate Cisco solution bundle (Cisco Configuration Assurance Solution, Cisco Network Planning Solution, etc.):

- `Virtual Network Data Server`
- `Open Virtual Network Data Server File Log Viewer`

Example Program Group menus for Cisco solution bundles:

`C:\Documents and Settings\All Users\Start Menu\Programs\Cisco Configuration Assurance Solution 1.1`

`C:\Documents and Settings\All Users\Start Menu\Programs\Cisco Network Planning Solution 1.1 - SPM`

Step 3 If the Program Group menu for the appropriate Cisco solution bundle is now empty, delete the menu.

Warning **Be very careful when you edit the system registry. Incorrect changes to the registry can cause your Windows system to become unstable. You might want to create a backup before editing the registry.**

Step 4 In the Windows Registry Editor, find and select the registry key for the software being removed. Example registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OPNET Technologies\
Cisco Configuration Assurance Solution-SP 1.1\OPNET VNE Server 3.5.2.
```

Step 5 Select **Delete** from the menu to delete the entry.

Step 6 Remove the uninstaller entry in the Registry at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall
```

Example entry names:

```
Cisco Configuration Assurance Solution-SP 1.1 Virtual Network Data
Server
```

```
Cisco Configuration Assurance Solution-SP 1.1 - Service Provider
Module - Virtual Network Data Server
```

Step 7 Exit the Windows Registry Editor.

Uninstalling Cisco VNDS (Linux)

Perform the following procedure to remove the VNDS software from your computer.

Step 1 Stop services and exit the Control Panel.

Step 2 Open a command window and use the `cd` command to set the working directory to the VNDS installation directory. An example installation directory might be:

```
/opt/cisco/VNDServer/4.0.2_<build_number>
```

Step 3 Enter the following command:

```
./vnes.sh -c stop ALL
```

Step 4 Close the window or `cd` up one level.

Step 5 Enter the following command:

```
rm -rf <vnds_install>
```

where <*install_path*> is the VNDS installation directory.

Step 6 At this point, there are still some daemon scripts remaining in the /etc directory. Removing these scripts is optional. To remove these scripts, open a command window and enter the following commands:

```
cd /etc/init.d

run "rm OPNET*"

run "rm tomcat.sh"

run "rm vnetomcat.sh"
```

Uninstalling a License Server

This section describes how to uninstall a license server from the Cisco VNDS host.

Note In previous versions of Cisco VNDS, a license server that was installed with the software was uninstalled with the Cisco VNDS software. If you installed a local license server with Cisco VNDS 3.5, refer to the *Installation Guide* for the previous release.

If you installed a local license server with Cisco VNDS 4.0, use the following procedure to remove it.

Uninstalling License Server (Windows)

Warning **Do not uninstall the license server until another license server can be set up elsewhere. You must deregister licenses and move them to the new license server then redirect all impacted solution components to the new license server before you uninstall the old license server.**

Step 1 Deregister all active licenses for the license server. Use the **"Deregistering a License" procedure on page 9-7**.

Step 2 Open the Windows Control Panel from the Start menu:

Start > Settings > Control Panel

Step 3 In the Windows Control Panel, double-click **Add/Remove Programs**.

Step 4 Scroll down the list of installed programs, select the entry for OPNET License Server 12.0, and click **Remove**.

Step 5 (Optional) Remove the license directory (for example, C:\OPNET_license dir).

Warning **Be very careful when you edit the system registry. Incorrect changes to the registry can cause your Windows system to become unstable. You might want to create a backup before editing the registry.**

Step 6 (Optional) Verify that the registry key has been removed. In the Windows Registry Editor, find and select the registry key for the software being removed. Example registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OPNET Technologies\
OPNET License Server 12.0\12.0.A
```

If the entry exists, select **Delete** from the menu to remove it.

Uninstalling License Server (Linux)

Warning **Do not uninstall the license server until another license server can be set up elsewhere. You must deregister licenses and move them to the new license server then redirect all impacted solution components to the new license server before you uninstall the old license server.**

Step 1 Deregister all active licenses for the license server.

Step 2 Open a command window and use the cd command to set the working directory to the license server installation directory (for example, `/usr/bin/OPNET/12.0.A/`).

Step 3 Enter the following command to delete the contents of the license server installation directory:

```
rm -rf *
```

Step 4 Remove the startup folder by entering the following command:

```
rm /etc/rc3.d/S99opnet_lic_server
```

Step 5 (*Optional*) Remove the license directory.

Uninstalling Cisco Report Server

This chapter contains the following sections:

Uninstalling Cisco Report Server (Windows)

Step 1 Open the Windows Control Panel from the Start menu:

Start > Settings > Control Panel

Step 2 In the Windows Control Panel, double-click **Add/Remove Programs**.

Step 3 Scroll down the list of installed programs, select the entry for the Cisco Report Server release you want to remove, and click **Remove**. For example, you might see the following entry:

Cisco Configuration Assurance Solution–SP 2.0 - Cisco Report Server

Step 4 Delete the corresponding install directory. Thus, if your version of Report Server is installed in `C:\Cisco\ReportServer\2.5.2`, delete the `2.5.2` directory.

Note When you uninstall a previous release of Cisco Report Server, the Cisco Report Server service registered to the current release will be stopped. Use the Windows Service Manager to re-start the Cisco Report Server service.

Uninstalling Cisco Report Server (Linux)

Step 1 Log in as `root`.

Step 2 Open a command prompt window.

Step 3 Move to the parent directory of the Report Server installation. Thus, if you installed Report Server in `/opt/cisco`, enter the following command:

```
cd /opt/cisco
```

Step 4 Enter the following command:

```
./ReportServer/2.5.2/UninstallerData/Uninstall_Cisco_Report_Server_2.0
```

Note You must enter this command from the parent directory and specify the path name to the `UninstallerData` directory.

Step 5 Delete the ReportServer directory by entering the following command:

```
rm -rf ReportServer
```

Caution The following step will delete all the generated security keys for Report Server. Perform the following step ONLY if there are no other programs (such as Cisco Virtual Network Data Server) that are using the `Security` directory.

Step 6 Delete the Security directory by entering the following command:

```
rm -rf Security
```

Oracle Procedures (Windows)

This appendix includes a series of procedures for installing Oracle software for use with Cisco Virtual Network Data Server. For information about when to perform each procedure, see the "Installation Workflows" section on page 5-2.

Note The instructions in this appendix are included for the convenience of Cisco CAS–SP users. For detailed information about using Oracle products, consult the Oracle product documentation or Oracle technical support.

Oracle9i Installation Procedures

Installing the Oracle9i Database (Windows)

Warning **Use caution when installing Oracle for use with VNDS. Recovery is difficult if Oracle is incorrectly installed.**

You can install the Oracle database on the same host as VNDS or on a different host. Install the database on the appropriate host using Installing the Oracle 9i Database on Windows, page A-2.

Installing the Oracle 9i Database on Windows

Step 1 Log into the host as Administrator or as a user with full administrative privileges. If you are not logged in with the proper privileges, log off and log on with an appropriate account.

Step 2 Insert the Oracle installation CD into the CD drive of the host for the database. If the installer does not start automatically, use **Start > Run** to execute Oracle's *setup.exe* program.

The installer displays a *Welcome* panel.

Step 3 Press **Next** to proceed to the *File Locations* panel.

The installer prompts you for an installation path in the *File Locations* panel. Oracle (9.2.0.1.0) requires about 2.8 GB of disk space.

Step 4 Enter an installation path that resides on a disk with adequate free space. Press **Next** to proceed.

The installer prompts you for the Oracle product to install in the *Available Products* panel.

Step 5 Select the *Oracle9i Database* product. Press **Next** to proceed.

The installer prompts you for the type of installation in the *Installation Types* panel.

Step 6 Select a *Personal*, *Standard*, or *Enterprise* edition installation. Any of these editions can be used with VNDS. The Enterprise edition is recommended for best scalability and performance.

Step 7 Press **Next** to proceed.

The installer prompts you for the type of database in the *Database Configuration* panel.

Step 8 Select **General Purpose**. Press **Next** to proceed.

The installer prompts you for the port number for the Oracle MTS Recovery Service.

Step 9 Leave the default port number (2030) unchanged. Press **Next** to proceed.

The installer prompts you for a global database name (GDN) in the *Database Identification* panel.

VNDS will work with any valid GDN and SID that Oracle accepts.

Answer with a GDN constructed according to the following rules:

Global Database Name = `o92a<name>.<domain>.com`

An example: `o92avnes.opnet.com`

Note If the first portion of the GDN exceeds 8 characters, the Oracle installer will block installation.

The installer prompts you for a system ID (SID). Some examples follow:

- o92a
- o92avnes
- vnesDB

Step 10 Enter the SID you want to use. After entering a GDN and SID, press **Next** to continue to the *Database File Location* panel.

The installer prompts you for the Database File Location.

Step 11 Keep the default location and press **Next** to proceed.

The installer prompts you for the Database Character Set.

Note To view the list of supported Oracle database and national character sets for use with VNDS, refer to Cisco Virtual Network Data Server: System Requirements, page 3-1. Choose a supported character set and press **Next** to proceed with file installation.

The Oracle installer takes up to 30 minutes to copy files to the installation directories. Oracle9i has three installation CDs. The installer prompts you to insert a new CD in the CD drive when it is ready to copy files from the next CD.

During this time, *Install, Configuration Tools and Database Creation* panels appear.

Step 12 Press **Next** or **OK** to proceed through these panels.

Note A window titled HTTP Server may launch at this point. You can close this window.

An installation *Summary* panel appears.

Step 13 Press **Install** to proceed.

The Database Configuration Assistant prompts you for new passwords for the SYS and SYSTEM accounts.

Step 14 Enter the passwords that you want to use for these accounts, and press **OK** when done.

Step 15 When installation is complete, an *End of Installation* panel appears. Press **Exit** to close the Oracle installer.

Note You do not need to create a user account for VNDS at this time. This is done after VNDS installation.

Step 16 Record the Oracle GDN, SID, install path and database hostname in Table A-1 on page A-14.

Installation logs are located here:

`C:\Program Files\Oracle\Inventory\logs\installActions.log`

If you run the Oracle installer again, the install actions log is renamed with an embedded date-stamped name such as: `installActions2002-01-24_xxx`.

Oracle9i (9.2.0.1.0) installation is now complete.

After VNDS is installed, a final configuration step is required to finish Oracle setup for VNDS. This step is described in "Configuring the Oracle Database for Cisco VNDS (Windows)" section on page 5-17, but is not performed until after installation of VNDS.

Proceed at this time to "Oracle9i Installation Procedures" section on page A-1 and then to "Installing Cisco VNDS (Windows)" section on page 5-6.

Note About Oracle Services

After Oracle installation, several Windows services are created. VNDS only requires the Oracle services shown below. These Windows services should be configured to automatically start when the PC is booted. All other Oracle services may be configured for a manual start and stopped unless specifically needed for other uses. The following services are required for VNDS to run:

- `OracleOraHome92TNSListener`

- `OracleService<DB SID>`

Installing the Oracle9i Client (Windows)

Warning **Use caution when installing Oracle for use with VNDS. Recovery is difficult if Oracle is incorrectly installed.**

If the Oracle database is installed on a different machine that the VNDS software, you must install the Oracle client on the VNDS host. The Oracle client is required by VNDS to communicate with an Oracle database located on another host. Perform "Installing the Oracle 9i Client on Windows" section on page A-5 to install the Oracle 9i client.

Installing the Oracle 9i Client on Windows

Step 1 Log into the host as Administrator or as a user with full administrative privileges. If you are not logged in with the proper privileges, log off and log on with an appropriate account.

Step 2 Insert the Oracle installation CD into the CD drive of the host for VNDS. If the installer does not start automatically, use **Start > Run** to execute Oracle's `setup.exe` program.

The installer displays a `Welcome` panel.

Step 3 Press **Next** to proceed to the *`File Locations`* panel.

The installer prompts you for an installation path in the *`File Locations`* panel. Oracle Client (9.2.0.1.0) requires about 200 MB of disk space.

Step 4 Enter an installation path that resides on a disk with adequate free space. Press **Next** to proceed.

The installer prompts you for the Oracle product to install.

Step 5 Select the **Oracle9i Client** product. Press **Next** to proceed.

The installer prompts you for the type of installation in the *`Installation Types`* panel.

Step 6 Select **Runtime**. Press Next to proceed to the *`Summary`* panel.

An installation *`Summary`* panel appears.

Step 7 Press **Install** at this panel to begin Oracle installation. The Oracle installer takes up to 30 minutes to copy files to the installation directories.

Note The final installation tasks involve setting up Net services using the Net Configuration Assistant.

Step 8 Press **Next** at the *Configuration Tools* panel.

The installer prompts you for whether you want to use a directory service at the *Net Configuration Assistant* panel.

Step 9 Select **No**, and press **Next**.

The installer prompts you for the version of Oracle used by the database at the *Database Version* panel.

Step 10 Select **Oracle 8i or later database**, and press **Next**.

The installer prompts you for a database service name at the *Service Name* panel.

Step 11 Enter the Global Database Name used during Oracle database installation on the database host. This name should be the same as the Database TNS Service Name collected in Table A-1 on page A-14. Press **Next**.

The installer prompts you for the communication protocol to use at the *Select Protocols* panel.

Step 12 Select the appropriate protocol to use (e.g. TCP), and press **Next**.

The installer prompts you for the database host name.

Step 13 Enter the hostname as an IP address or a fully qualified domain name, and press **Next**.

The installer prompts you for whether you want to test the database connection.

Step 14 Answer **Yes**, and press **Next**.

The installer displays the test status in a test result panel.

Step 15 Press **Next**.

Note Investigate and resolve any problems if the connection test fails.

The installer prompts you for whether or not you want to configure another service name.

Step 16 Answer **No**, and press **Next**.

A *Configuration Complete* panel appears.

Step 17 Press **Next**.

Another completion panel appears.

Step 18 Press **Finish**.

The installer displays an *End of Installation* panel.

Step 19 Press **Exit** to close the Oracle installer.

Installation logs are located here:

`C:\Program Files\Oracle\Inventory\logs\installActions.log`

If you run the Oracle installer again, the install actions log is renamed with an embedded date-stamped name such as: `installActions2002-01-24_xxx`.

Proceed at this time to Oracle9i Installation Procedures, page A-1, and then to Installing Cisco VNDS (Windows), page 5-6.

Oracle10g Installation Procedures

Installing the Oracle10g Database (Windows)

Warning **Use caution when installing Oracle for use with** VNDS**. Recovery is difficult if Oracle is incorrectly installed.**

You can install the Oracle database on the same host as VNDS or on a different host. Install the database on the appropriate host using Installing the Oracle 10g Database (Windows), page A-8.

Note Oracle10g requires a static IP address on the database host machine. If the database host has a dynamically assigned IP address, install the Microsoft Loopback Adapter before you install Oracle10g.

Installing the Oracle 10g Database (Windows)

Step 1 Log into the host as Administrator or as a user with full administrative privileges. If you are not logged in with the proper privileges, log off and log on with an appropriate account.

Step 2 Insert the Oracle installation CD into the CD drive of the host for the database. If the installer does not start automatically, use **Start > Run** to execute Oracle's `setup.exe` program.

The installer displays an *`Installation Method`* panel.

Step 3 Select Basic Installation in the *Installation Method* panel and enter values for Basic Installation configuration.

a. Enter an installation path into the **Oracle Home Location** field. Make sure that it resides on a disk with adequate free space.

Oracle (10.2.0.1.0) requires about 2.8 GB of space.

b. Select the **Installation Type**.

Select a **Personal**, **Standard**, or **Enterprise** edition installation. Any of these editions can be used with VNDS. The Enterprise edition is recommended for best scalability and performance.

c. Make sure that **Create Starter Database** is selected.

d. Specify the **Global Database Name (GDN)**.

VNDS will work with any valid GDN that Oracle accepts.

Enter a GDN constructed according to the following rules:

Global Database Name = *<database_name>.<database_domain>* where *<database_domain>* is optional.

Some examples:

`o10gvnes`

`vnes`

`vnes.opnet.com`

e. Type the password that will be used for the SYS, SYSTEM, SYSMAN, and DBSNMP accounts into the Database Password and Confirm Password fields.

f. Press **Next** to proceed.

Step 4 A progress dialog displays while Oracle runs system verification checks.

The *Product-Specific Prerequisite Checks* panel displays.

Step 5 Review the results of the prerequisite checks and resolve errors and warnings before proceeding.

Step 6 Press **Next** to proceed.

A Summary panel displays.

Step 7 Press **Install** to proceed with installation.

An Install panel displays progress.

Next a Configuration Assistants panel displays progress.

A *Database Configuration Assistant* dialog notifies you when database creation is complete.

Step 8 Record the Oracle GDN, SID, install path and database hostname in Table A-1 on page A-14.

You do not need to do any account or password management at this time. Creation of the VNDS account is done after VNDS installation.

Step 9 Press **OK** in the *Database Configuration Assistant* dialog to continue.

When configuration is complete, an *End of Installation* panel displays.

Step 10 Press **Exit** to close the Oracle installer.

Note A web browser with the Oracle Enterprise Manager may open. You can close this window.

Installation logs are located here:

```
C:\Program Files\Oracle\Inventory\logs\installActions.log
```

If you run the Oracle installer again, the install actions log is renamed with an embedded datestamped name such as: `installActions<date_time>.log`.

Oracle10g (10.2.0.1.0) installation is now complete.

After VNDS is installed, a final configuration step is required to finish Oracle setup for VNDS. This step is described at "Configuring the Oracle Database for Cisco VNDS (Windows)" section on page 5-17, but is not performed until after installation of VNDS.

Proceed at this time to Oracle9i Installation Procedures, page A-1 and then to Installing Cisco VNDS (Windows), page 5-6.

Installing the Oracle10g Client (Windows)

Warning **Use caution when installing Oracle for use with VNDS. Recovery is difficult if Oracle is incorrectly installed.**

If the Oracle database is installed on a different machine that the VNDS software, you must install the Oracle client on the VNDS host. The Oracle client is required by VNDS to communicate with an Oracle database located on another host. Perform Installing the Oracle 10g Client (Windows), page A-10 to install the Oracle 10g client.

Installing the Oracle 10g Client (Windows)

Step 1 Log into the host as Administrator or as a user with full administrative privileges. If you are not logged in with the proper privileges, log off and log on with an appropriate account.

Step 2 Insert the Oracle installation CD into the CD drive of the host for VNDS. If the installer does not start automatically, use **Start > Run** to execute Oracle's `setup.exe` program.

The installer displays a *`Welcome`* panel.

Step 3 Press **Next** to proceed to the *`Installation Type`* panel.

The installer prompts you for the type of client installation.

Step 4 Select Runtime then press **Next**.

The installer displays the *`Specify Home Details`* panel.

Step 5 Specify the Path.

Oracle Runtime Client (10.2.0.1.0) requires about 213 MB of disk space.

Note Do not modify the Name field in the Specify Home Details panel. Use the value that the Oracle installer provides.

Step 6 Enter an installation path that resides on a disk with adequate free space. Press **Next** to proceed.

The Oracle installer performs prerequisite checks then displays the results in the *Product-Specific Prerequisite Checks* panel.

Step 7 Press **Next** to proceed.

The *Summary* panel displays.

Step 8 Press **Install** at this panel to begin Oracle installation. The Oracle installer takes several minutes to copy files to the installation directories.

The *Install* panel displays progress then the *Configuration Assistants* panel displays.

After a moment, the *Oracle Net Configuration Assistant: Welcome* dialog displays.

Step 9 Press **Next**.

The *Oracle Net Configuration Assistant: Done* dialog displays.

Step 10 Press **Finish**.

Step 11 The *End of Installation* panel displays.

Step 12 Press **Exit**.

Note The final installation tasks involve setting up Net services using the Oracle Net Configuration Assistant.

Step 13 Select **Programs > Oracle - Oracle - OraClient10g_home1 > Configuration and Migration Tools > Net Configuration Assistant** from the Windows Start menu.

The Oracle Net Configuration Assistant opens and prompts you to choose the configuration you would like to do at the *Welcome* panel.

Step 14 Select Local Net Service Name configuration and press **Next**.

The Oracle Net Configuration Assistant opens and prompts you to specify an action at the *Net Service Name Configuration* panel.

Step 15 Select Add then press **Next**.

The Oracle Net Configuration Assistant prompts you for a database service name at the Net *Service Name Configuration, Service Name* panel.

Step 16 Enter the Global Database Name used during Oracle database installation on the database host. This name should be the same as the Database TNS Service Name collected in Table A-1 on page A-14. Press **Next**.

The Oracle Net Configuration Assistant prompts you for the communication protocol to use at the *Net Service Name Configuration, Select Protocols* panel.

Step 17 Select the appropriate protocol to use (e.g. TCP), and press **Next**.

The Oracle Net Configuration Assistant prompts you for the database host name and TCP/IP port number.

Step 18 Enter the hostname as an IP address or a fully qualified domain name, and press **Next**.

The Oracle Net Configuration Assistant prompts you for whether you want to test the database connection.

Step 19 Answer **Yes**, and press **Next**.

The test status displays.

Note Investigate and resolve any problems if the connection test fails. If the test did not succeed, make sure that the username and password is valid for the VNDS account that has been configured on the remote database. Change the login, if required, and retest.

Step 20 Press **Next**.

The Oracle Net Configuration Assistant prompts you for a net service name.

Step 21 Leave the Net Service Name set to the global database name for the remote database and press **Next**.

The Oracle Net Configuration Assistant prompts you for whether or not you want to configure another service name.

Step 22 Answer **No**, and press **Next**.

A *Net Service Name Configuration* panel displays.

Step 23 Press **Next**.

The *Welcome* panel displays.

Step 24 Press **Finish** to close the Oracle Net Configuration Assistant.

Step 25 Verify that a tnsnames.ora file has been created for the database client.

Look in `<oracle_home>\client_1\NETWORK\ADMIN` directory (for example, *`C:\oracle\product\10.2.0\client_1\NETWORK\ADMIN`*).

Installation logs are located here:

`C:\Program Files\Oracle\Inventory\logs\installActions.log`

If you run the Oracle installer again, the install actions log is renamed with an embedded date-stamped name such as: `installActions<date_time>.log`.

Now proceed to the following procedures.

For VNDS on Windows:

a. Oracle9i Installation Procedures, page A-1

b. Installing Cisco VNDS (Windows), page 5-6.

For VNDS on Linux:

a. Collecting Oracle Database Access Information (Linux), page B-3

b. Installing Cisco VNDS (Linux), page 6-4.

Collecting Oracle Database Access Information (Windows)

The VNDS installer prompts for database access information. Before beginning installation, collect the database access information listed in Table A-1 on page A-14. The database administrator can supply the database access information that you need. Print out the installation instructions and write down the database access information in the Table A-1 on page A-14 for reference during installation. Continue with Installing Cisco VNDS (Windows), page 5-6.

The Database Account User Name in Table A-1 on page A-14 is the account used by VNDS to access network data stored in the database. This account is created after VNDS is installed using the user name and password entered during VNDS installation.

Warning **DO NOT use SYS or SYSTEM for the Database Account User Name.**

Table A-1 Database Access Information Worksheet

Access Item	Value	Description
Database TNS Service Name (alias for Database GDN)	•	The TNS Net Service name used for the local or remote database. Refer to Locating a Database Net Service Name in tnsnames.ora (Windows), page A-16 in the Appendix for instructions on locating the service name.
Database SID	•	The database SID.
Database hostname	•	The IP address or fully qualified domain name for the database host. ***Only needed for remote databases.***
Oracle Home (installation) directory	•	The Oracle installation directory on the database host. ***Only needed for remote databases.***
Oracle Oradata Parent directory	•	The parent directory to the Oracle oradata directory on the database host. ***Only needed for remote databases.***
Database account user name	•	User name of the account used to access the database. DO NOT use the Oracle SYS or SYSTEM accounts.
Database account password	•	Password for the account used to access the database.

Installing Oracle TopLink (Windows)

The Cisco VNDS program requires access to an installation of Oracle 9i Application Server Toplink that is patched to release 9.0.3.5. This section describes how to install Toplink 9.0.3.5 on your system. Install Toplink on the same system as Cisco Virtual Network Data Server.

Note VND Server requires access to Oracle TopLink 9.0.3.5. This is true regardless of the version of Oracle used for the VNDS database.

Note You must perform the following procedure before you install Cisco Virtual Network Data Server.

Installing Toplink 9.0.3.5 (Windows)

Step 1 Download or copy the required Oracle Toplink components into a working directory:

- Oracle Toplink 9.0.3.0 (A99417-01.zip)
- Oracle Toplink 9.0.3.5 patch (p3188702_9031_GENERIC.zip)

Step 2 Create a working directory on your system. Copy the downloaded Oracle Toplink 9.0.3.0 and 9.0.3.5 zip files to this directory.

Step 3 Unzip the Oracle Toplink 9.0.3.0 archive, A99417-01.zip, into the working directory.

Step 4 Execute the Toplink 9.0.3.0 installer, toplink903-windows.exe:

a. At the introduction panel, click Next. The installer prompts you for the installation folder.

Note If you already have an Oracle installation on this system, the default Toplink installation folder will be in your Oracle installation. Cisco recommends that you use this folder. Write down the installation folder you choose; you will need it later during installation of Cisco Virtual Network Data Server.

b. Select an install folder and click **Next**. In the remaining panels, the installer prompts you for:

- Shortcut Location (select your preference)
- Toplink Features (select **Full Install**)
- Viewing Release Notes (select your preference)

c. Work through the remaining installer panels and enter the preferences in Step b. Click **Done** in the *Install of TopLink Complete* panel to exit the installer.

Step 5 Do the following steps to install the Toplink 9.0.3.5 patch.

a. Open a window to the working directory that contains the Toplink patch, p3188702_9031_GENERIC.zip.

b. Unzip the Oracle Toplink patch archive, p3188702_9031_GENERIC.zip, into the Toplink installation directory. For example, if you installed Toplink to C:\oracle\ora92\toplink, select this path as the extraction path for the archive.

c. If you are prompted to confirm file overwrite, select "Yes to All".

d. Close the archive application (WinZip or similar application) when done.

e. Verify that the Toplink installation has the files required by Cisco Virtual Network Data Server. The following files should exist in the `<toplink install>\core\lib` directory:

- tl_core.jar
- tl_tools.jar
- tl_x.jar

At this point, Toplink 9.0.3.5 is installed on your system and ready for access during Cisco Virtual Network Data Server installation. Proceed to the next step of the installation workflow (as described in Installation Workflows, page 5-2).

Locating a Database Net Service Name in tnsnames.ora (Windows)

VNDS uses a database's Oracle Net service name for connection to the database. This is true whether VNDS uses a local or remote database. The database service name is located in the `tnsnames.ora` file. This file is located in the `<oracle`

install dir>\ora92\network\Admin for Oracle9i and at <*oracle install dir*>\product\10.2.0\db_1\NETWORK\ADMIN directory for Oracle10g. A sample file is shown below.

In this sample file, there are three entries. The O92AML14.OPNET.COM entry (highlighted) represents the database service name. Each entry has a <*net service name*> = () structure. The text string preceding the "=" is the service name. In this example, you use O92AML14.OPNET.COM as the service name for VNDS installation.

Note that this file has entries for other Oracle Net services and may contain entries for more than one database. If the Oracle installation you are using supports other products, contact the database administrator for the service name you should use.

```
# TNSNAMES.ORA Network Configuration File:
D:\oracle\ora92\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

O92AML14.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = mlpc14)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = o92aml14)
    )
  )

EXTPROC_CONNECTION_DATA.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
    )
    (CONNECT_DATA =
      (SID = PLSExtProc)
      (PRESENTATION = RO)
    )
  )

INST1_HTTP.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = mlpc14)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = SHARED)
      (SERVICE_NAME = o92aml14)
      (PRESENTATION = http://admin)
```

)
)

Oracle Procedures (Linux)

This appendix includes a set of procedures for installing Oracle software for use with Cisco Virtual Network Data Server. For information about when to perform each procedure, see the "Installation Workflows: Overview" section on page 6-2.

Note The instructions in this appendix are included for the convenience of Cisco CAS–SP users. For detailed information about using Oracle products, consult the Oracle product documentation or Oracle technical support.

Oracle Installation Procedures

The procedures for installing Oracle on Linux can vary, depending on the versions of Oracle and Linux as well as platform-specific parameters. Installing Oracle might also require changes in kernel settings, updating system patches, and other system administration tasks. Work with your Database Administrator and refer to the Oracle Installation Guide and other relevant Oracle documentation to complete the installation.

Note Check the `/etc/oratab` file and verify that the database instance you are using can be started by Oracle scripts. The oratab entry for the database instance name you are using should end in ":Y". If it does not, work with your database administrator to change this setting to allow database startup.

Configuring the Environment for the *oracle* Account (Linux)

Step 1 Verify/configure the environment for the *oracle* account.

a. Open `/oracle/.bash_profile` with a text editor of your choice.

Note If you are using another shell, examine the appropriate file.

b. Confirm that it has the following entries. Manually add the entries, if needed.

```
ORACLE_HOME=<oracle_home>
ORACLE_SID=<dbSID>
PATH=$ORACLE_HOME/bin:$PATH
export PATH
export ORACLE_HOME ORACLE_SID
```

where <*dbSID*> is the database SID (for example, `o92ml23`)
and <*oracle_home*> is the Oracle installation directory (for example, `/u01/app/oracle/product/9.2.0`)

Configuring Permissions for Oracle Directories (Linux)

Step 1 Assign read and execute permissions for all users to the bin, lib and jdbc directories in `$ORACLE_HOME`.

a. Log in as *oracle*.

b. Use the following commands to modify directory permissions.

```
chmod 755 $ORACLE_HOME/bin
chmod 755 $ORACLE_HOME/lib
chmod 755 $ORACLE_HOME/jdbc
```

Collecting Oracle Database Access Information (Linux)

The VNDS installer prompts for database access information. Before beginning installation, collect the database access information listed in Table B-1. The database administrator can supply the database access information that you need. Print out the installation instructions and write down the database access information in the Table B-1 for reference during installation. Continue with installing Cisco VNDS.

The Database Account User Name in Table B-1 is the account used by VNDS to access network data stored in the database. This account is created after VNDS is installed using the user name and password entered during VNDS installation.

Warning **DO NOT use SYS or SYSTEM for the Database Account User Name.**

Table B-1 Database Access Information Worksheet

Access Item	Value	Description
Database TNS Service Name (alias for Database GDN)		The TNS Net Service name used for the local or remote database. Refer to Locating a Database Net Service Name in tnsnames.ora (Linux), page B-6 in the Appendix for instructions on locating the service name.
Database SID		The database SID.
Database hostname		The IP address or fully qualified domain name for the database host.
Oracle Home (installation) directory		The Oracle installation directory on the database host.
Oracle Oradata Parent directory		The parent directory to the Oracle oradata directory on the database host.

Table B-1 Database Access Information Worksheet (continued)

Access Item	Value	Description
Database account user name		User name of the account used to access the database. DO NOT use the Oracle SYS or SYSTEM accounts.
Database account password		Password for the account used to access the database.

Installing Oracle TopLink (Linux)

The VNDS program requires access to an installation of Oracle 9i Application Server Toplink that is patched to release 9.0.3.5. This section describes how to install Toplink 9.0.3.5 on your system. Install Toplink on the same system as Cisco Virtual Network Data Server.

Note VND Server requires access to Oracle TopLink 9.0.3.5. This is true regardless of the version of Oracle used for the VNDS database.

Note You must perform the following procedure before you install Cisco Virtual Network Data Server.

Installing Toplink 9.0.3.5 (Linux)

Step 1 Log into your system using the account used to operate Cisco VNDS.

Step 2 Download or copy the required Oracle Toplink components into a working directory:

- Oracle Toplink 9.0.3.0 (A99417-01.zip)
- Oracle Toplink 9.0.3.5 patch (p3188702_9031_GENERIC.zip)

Step 3 Create a working directory on your system. Copy the downloaded Oracle Toplink 9.0.3.0 and 9.0.3.5 zip files to this directory.

Step 4 Unzip the Oracle Toplink 9.0.3.0 archive into the working directory. To do this, enter the following command:

```
unzip -d <working_dir> <zip_file>
```

Step 5 Use the gzip command to expand the GZ file. To do this, enter the following command:

```
gunzip toplink903-unix.tar.gz
```

Step 6 Use the tar command to expand the TAR file. To do this, enter the following command:

```
tar -xvf toplink903-unix.tar
```

This command creates a toplink directory under the working directory.

Step 7 Do the following steps to install the Toplink 9.0.3.5 patch.

a. Open a window to the working directory that contains the Toplink patch, p3188702_9031_GENERIC.zip.

b. Unzip the Oracle Toplink patch archive, p3188702_9031_GENERIC.zip, into the Toplink installation directory. To do this, enter the following command:

```
unzip -d <working dir>/toplink p3188702_9031_GENERIC.zip
```

For example, if you installed Toplink to `/uo1/app/oracle/9.2.0/toplink`, select this path as the extraction path for the archive.

c. If you are prompted to confirm file overwrite, select [A] for "Yes to All".

d. Verify that the Toplink installation has the files required by Cisco Virtual Network Data Server. The following files should exist in the `<toplink install>/core/lib` directory:

- tl_core.jar
- tl_tools.jar
- tl_x.jar

At this point, Toplink 9.0.3.5 is installed on your system and ready for access during Cisco Virtual Network Data Server installation. Proceed to the next step of the installation workflow (as described in Installation Workflows, page 5-2).

Locating a Database Net Service Name in tnsnames.ora (Linux)

VNDS uses a database's Oracle Net service name for connection to the database. This is true whether VNDS uses a local or remote database. The database service name is located in the *tnsnames.ora* file. This file is located in the following directory:

Oracle 9i: *<oracle install dir>/oracle/product/9.2.0/network/Admin*

Oracle10g: *<oracle install dir>/oracle/product/10.2.0/NETWORK/ADMIN*

In the following example file, there are three entries. The O92AML14.OPNET.COM entry (highlighted) represents the database service name. Each entry has a *<net service name> = ()* structure. The text string preceding the "=" is the service name. In this example, you use O92AML14.OPNET.COM as the service name for VNDS installation.

Note that this file has entries for other Oracle Net services and may contain entries for more than one database. If the Oracle installation you are using supports other products, contact the database administrator for the service name you should use.

```
# TNSNAMES.ORA Network Configuration File:
/uo1/app/oracle/product/10.2.0/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.

O92AML14.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = mlpc14)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = o92aml14)
    )
  )

EXTPROC_CONNECTION_DATA.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
    )
    (CONNECT_DATA =
      (SID = PLSExtProc)
      (PRESENTATION = RO)
    )
  )
```

```
INST1_HTTP.OPNET.COM =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = mlpc14)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = SHARED)
      (SERVICE_NAME = o92aml14)
      (PRESENTATION = http://admin)
    )
  )
```

Errata

This appendix contains miscellaneous information that was unavailable when the Cisco CAS–SP documentation was published.

Additional Requirements for the “Cisco WAN Manager” Adapter

The Cisco WAN Manager adapter includes a CWM Database Reader option. To use this option, you must perform the following procedure.

For more information about the Cisco WAN Manager adapter, see the following section of the Cisco Virtual Network Data Server documentation:

VNE Server User Guide > Importing Device and Configuration and Topology > Cisco WAN Manager Import

Installing Additional Libraries to Allow Communication with the Cisco WAN Manager Database

Step 1 Obtain and install the IBM Informix JDBC Driver libraries.

For information about purchasing the IBM Informix JDBC Driver, go to:

http://www.ibm.com/software/data/informix/tools/jdbc

For information about downloading an evaluation or trial version of the IBM Informix JDBC Driver, go to :

http://www.ibm.com/software/data/informix/downloads.html

Note You must install IBM Informix JDBC Driver version 2.21.JC4 or later.

Step 2 After you obtain and successfully install the IBM Informix JDBC driver, you must copy or link all files located in

`<Informix_JDBC_Driver_Install_Directory>/lib`

to the following directory:

`<Cisco_VNDS_Install_Directory>/ext`

Note All files in the `<Informix_JDBC_Driver_Install_Directory>/lib` directory should have a prefix of "`ifx`" and a suffix of "`.jar`".

Step 3 Restart Cisco VNDS services.

Known Issues

We highly recommend that you check, after installation and on a regular basis, for software updates and maintenance information of any software, documentation, model, or other components on http://www.cisco.com/techsupport.

You can search for additional online information regarding known product issues and workarounds on the Cisco Quick Support page at OPNET Technologies (http://www.opnet.com/support/cisco_qsp.html).

A

C

D

F

H

I

L

O

P

R

S

T

U

V

W