



Using Virtual Network Computing Version 4.1

Virtual Network Computing (VNC) allows a system administrator to use a server to install applications or perform configuration tasks on a remote server while the user of the remote server views the tasks that occur. In this way, VNC operates similar to Microsoft Terminal Services.

Contents

- [Before You Begin, page 1](#)
- [Installing and Configuring VNC, page 2](#)
- [Starting a Remote Server from the Master Server, page 4](#)
- [Using the Master Server to Perform Tasks on the Remote Server, page 4](#)
- [Troubleshooting, page 5](#)
- [Obtaining Documentation, page 6](#)
- [Documentation Feedback, page 7](#)
- [Cisco Product Security Overview, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 10](#)

Before You Begin

Review the following information before you install VNC:

About VNC Terminology

In this document, *master server* refers to the server where the user initiates, performs, and manages tasks; the *remote server* receives the software or configuration information from the master server.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

About Compatible Operating System Versions

Make sure that you have installed Cisco-provided operating system version 2000.4.2 on all servers that will use VNC. For information on upgrading the operating system, refer to the documentation for the version of the Cisco CallManager upgrade that runs in the cluster.

About Security Risks

Be aware that using VNC poses a security risk by making the cluster vulnerable to attacks.

Installing VNC opens a network port, which may make the server vulnerable to attacks. A network scanner will show port 5900 "VNC => Remote Control Software" and allow an attacker to access the server.

During the VNC installation, enter a complex alphanumeric password for VNC. VNC limits the password to eight characters.

To minimize security risks, set the VNC service to Manual startup and start it only during remote management. This action ensures that users must enter a Windows user name/password that the server can authenticate before starting the service.

If you no longer plan to use Terminal Services for remote management, disable Terminal Services.

About Upgrading VNC

When you upgrade the operating system or run an operating system patch on the server, make sure that you review the operating system readme document for information on upgrading VNC. Cisco provides the VNC upgrade files in the operating system upgrade and/or operating system support patch, although Cisco does not automatically install these files on the server.

About Older Versions of VNC

Before you install VNC 4.1, uninstall any previous version of VNC that exists on the server. To uninstall VNC, choose **Start > Programs > Settings > Add/Remove Programs**.

About CPU Utilization

VNC may use a large percentage of CPU when you move the mouse and particularly when you move entire windows on the desktop. To minimize CPU utilization, limit unnecessary movements on the desktop, particularly while the server is in production.

Installing and Configuring VNC

Perform the following procedure to install and configure VNC Version 4.1 on all servers that will use VNC.

Procedure

- Step 1** Using Windows Explorer, browse to the following folder:
C:\utils\VNC
- Step 2** In the VNC folder, double-click **vnc-4.1_1-x86_win32.exe**.
The Welcome window displays.
- Step 3** Click **Next**.
- Step 4** To accept the software license agreement, click **I accept the agreement**; then, click **Next**.

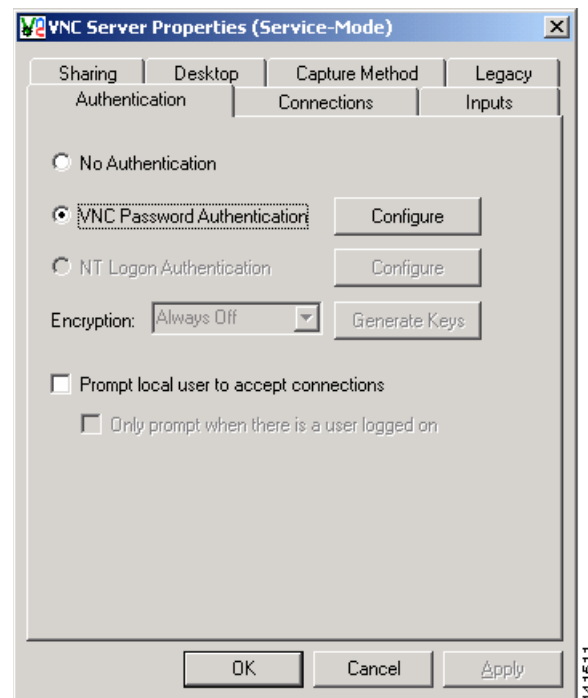
- Step 5** In the Select Destination Directory, accept the default location or choose another folder where you want to install VNC; then, click **Next**.
- Step 6** In the Select Components window, click **Next**.
- Step 7** In the Select Start Menu Folder window, accept the default folder name or choose another folder where you want the setup program to create the program shortcuts; then, click **Next**.
- Step 8** In the Select Additional Tasks window, check the **Register VNC Server as a system service** check box and the **Start the VNC Server System service** check box. If you want to create additional icons, check the check box next to the icons that you want to create; then, click **Next**.

The Ready to Install window displays.

- Step 9** Click **Install**.

The VNC Server Properties window displays, as show in [Figure 1](#).

Figure 1 VNC Server Properties Window



- Step 10** In the Authentication pane, choose the VNC Password Authentication radio button, and click **Configure** to enter a password in the Password and Confirm Password fields.
- You can enter a password of up to eight characters. You will use this password to open a VNC session between servers.
- Step 11** In the Password window, click **OK**.
- Step 12** Click the **Connections** tab; then, uncheck the **Serve Java viewer via HTTP on port: 5800** check box.
- Step 13** In the VNC Server Properties window, click **OK**.
- Step 14** To continue the setup, click **Next**.
- Step 15** Click **Finish**.

Starting a Remote Server from the Master Server

To start a remote server via VNC, perform the following procedure:

Procedure

-
- Step 1** From the master server, map a drive to the remote server by using the server name (not the IP address).
 - Step 2** Right-click **My Computer** and choose **Manage**.
 - Step 3** Choose **Action > Connect to another computer....**
The Select Computer dialog box displays.
 - Step 4** In the Name field, enter the name of the server to which you want to connect; then, click **OK**.
 - Step 5** In the Computer Management window, double-click **Services and Applications**.
 - Step 6** If an Internet Services Manager dialog displays, click **Yes**.
 - Step 7** Click **Services**.
 - Step 8** Right-click **VNC Server Version 4**; then, choose **Start**.
-

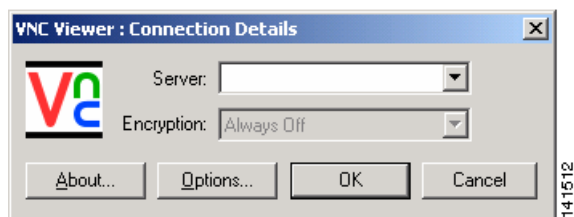
Using the Master Server to Perform Tasks on the Remote Server

Perform the following procedure to complete installation or configuration tasks via VNC:

Procedure

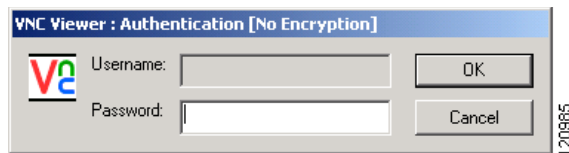
-
- Step 1** On the master server, choose **Start > Programs > RealVNC > VNC Viewer 4 > Run VNC Viewer**.
The Connection Details dialog box displays, as shown in [Figure 2](#).

Figure 2 Connection Details dialog box



- Step 2** In the Server field, enter the IP address of the remote server on which you want to install the software or perform a configuration task.
- Step 3** Click **OK**.
The VNC Authentication dialog box displays, as shown in [Figure 3](#).

Figure 3 VNC Authentication Dialog Box



Step 4 In the Password field, enter the password that you specified in [Step 10](#) in the “[Installing and Configuring VNC](#)” section on page 2.

Step 5 Click **OK**.

The desktop of the remote server displays.

Step 6 From the master server, install software or perform configuration tasks on the remote server.



Caution

Make sure that you insert installation CD-ROMs into the CD-ROM drive of the remote server or download the files from the web onto the remote server.



Note

When you are using a remote terminal over VNC to install Cisco CallManager on an IBM server, the procedure may seem to stall or hang during the installation. On the remote terminal, if you move (drag) the VNC window or refresh the screen by choosing **Request screen refresh** from the VNC application window menu (the menu that displays when you click the VNC icon in the left corner of the window title bar), the procedure will continue.

Step 7 Stop the **VNC Server** service.

Step 8 Perform the procedures in the “[Starting a Remote Server from the Master Server](#)” section on page 4 and in the “[Using the Master Server to Perform Tasks on the Remote Server](#)” section on page 4 for each remote server on which you want to perform installation or configuration tasks.

Troubleshooting

If you run VNC to install/upgrade Cisco CallManager on IBM xSeries servers, the installation may appear to hang when the server is copying the files during the installation. Move the mouse to continue the installation.

When VNC is used, some servers exhibit high CPU utilization. The server response may be slower than usual.

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 nonemergencies.

- Nonemergencies—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://cisoiq.texterity.com/cisoiq/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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CDDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

