



Using Cisco Unified CallManager Upgrade Utility 4.3(1)

The Cisco Unified CallManager Upgrade Utility, a nonintrusive tool, detects the health of the servers in the Cisco Unified CallManager cluster before you perform an upgrade to Cisco Unified CallManager.

This version of Cisco Unified CallManager Upgrade Utility replaces previous versions of Cisco Unified CallManager Upgrade Utility, Release 3.3(5), Release 4.0(2a), Release 4.1(2), Release 4.1(3), Release 4.2(1), Release 4.2(2), and Release 4.2(3). Cisco Unified CallManager Upgrade Utility 4.3(1) adds support for multiple version upgrades. Use Cisco Unified CallManager Upgrade Utility, version 4.3(1) or later, to detect the health of your servers before you upgrade to Cisco CallManager Release 3.3(5), 4.0(2a), 4.1(2), 4.1(3), 4.2(1), 4.2(2a), 4.2(3), 4.3(1), 5.0, and 5.1.



Caution

This utility identifies problems that could cause the Cisco Unified CallManager upgrade to fail. This utility does not correct the problem(s); you must perform the corrective action for the problem that the utility identifies.

Cisco strongly recommends that all servers in the cluster pass the validation before you upgrade any servers.

Contents

This document contains the following topics:

- [Related Documentation, page 2](#)
- [Before You Begin, page 3](#)
- [Understanding How the Utility Works, page 3](#)
- [Installing the Utility, page 6](#)
- [Running the Utility, page 7](#)
- [Interpreting the Results, page 7](#)
- [Obtaining the Log File, page 8](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Conventions

Consider the following documentation conventions as you review this upgrade document.

Blue Text—To quickly navigate to a section or URL, click text that appears in blue.



Note

Reader, take note. Notes contain helpful suggestions or references to material not covered in the publication.



Caution

Reader, be careful. You may do something that could result in equipment damage or loss of data.



Timesaver

Reader, this tip saves you time as you perform the procedure.

Related Documentation

Use the following documentation in conjunction with this document. Click the URLs in [Table 1](#) to navigate to the appropriate documentation.

Table 1 Quick Reference for URLs

Related Documentation and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation (not readme documentation)	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco Unified CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco Unified CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco Unified Communications Applications Backup and Restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Service releases and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml Note The operating system and SQL Server support patches post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco Unified CallManager software page.
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Before You Begin

Before you run the utility, Cisco strongly recommends that you perform the following tasks.

- Back up your Cisco Unified CallManager servers. To obtain the backup utility documentation, go to <http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm>.
- Review the “Understanding How the Utility Works” section on page 3.
- Verify that your server login account has Administrative privileges to run the utility.

Understanding How the Utility Works

Before you perform an upgrade to a Cisco Unified CallManager version, download and run the latest version of Cisco Unified CallManager Upgrade Utility, a nonintrusive tool that detects the health of the servers in the Cisco Unified CallManager cluster without changing the state of the system.

To verify that the server meets the minimum requirement for the Cisco Unified CallManager version to which you are upgrading, refer to the *Cisco Unified CallManager Compatibility Matrix*. To obtain the most recent version of this document, go to

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm



Caution

Your server login account must have Administrative privileges to run the utility. You may log in to the server by using the Administrator username and password.

Before you begin the upgrade on the publisher database server, you must run the utility on all servers in the cluster. If any server fails the validation process, investigate and correct the problem(s) before you begin the upgrade on the publisher database server. After you correct the problem(s), run the utility again before you upgrade.

You can run the utility on only one server at a time.

Cisco strongly recommends that you run this utility during a scheduled, maintenance window.

The utility runs the validation modules that display in [Table 2](#). The utility runs some validation modules only on publisher servers, some validation modules only on subscriber servers, and some modules on both publisher and subscriber servers. As soon as the utility identifies a problem with a module, the utility begins checking the next module. After the utility performs the entire validation process, review the validation list in the Summary window for modules that fail the validation or for modules that provide warnings.

Table 2 Validation Checks That the Utility Performs

Module	Applicable Server	Additional Information
The utility performs the following validations for servers that are running Cisco CallManager Release 3.1 or 3.2.		
Backup File Integrity Validation	This check occurs on the publisher database server only.	<p>The Upgrade Utility verifies the following items:</p> <ul style="list-style-type: none"> • The existence of the chosen MCS.sti file <p>If the file does not exist after you click Select, an error message displays.</p> <ul style="list-style-type: none"> • The backup file size • The backup utility version that is used to create the file <p>If you do not want the utility to validate the backup file, click the Skip button; a dialog box prompts you to skip the backup file validation.</p> <p>If you do not choose a backup file for the utility to validate, the utility assigns a Skipped status to the module.</p>
OS Flag Files Validation	This check occurs on the publisher database and subscriber servers.	The utility verifies that the Stirnw.flg and Stisys.inf files exist.
Database Location Setting Validation	This check occurs on the publisher database and subscriber servers.	The utility performs a check of your Cisco Unified CallManager registry (specifically, dbconnection0) to verify that the registry points to the proper database.
Resource Validation	This check occurs on the publisher database and subscriber servers.	This utility verifies that the system has enough physical memory.
The utility performs the following validations for servers that are running Cisco CallManager Release 3.3, 4.0, 4.1, or 4.2		
Software Version Validation	This check occurs on the publisher database and subscriber servers.	<p>The utility validates the Cisco-provided operating system/related service releases and SQL Server/related service releases.</p> <p>For information on minimum software requirements, refer to the <i>Cisco Unified CallManager Compatibility Matrix</i>. To obtain the most recent version of this document, see Table 1.</p> <p>The Upgrade Utility checks only for software applications that this document lists. If you run other applications in the cluster or other applications on the servers, verify that compatibility exists between Cisco Unified CallManager and the application before you upgrade. Failing to do so may cause applications to not work as expected.</p>
Database Location Setting Validation	This check occurs on the publisher database and subscriber servers.	The utility performs a check of your Cisco Unified CallManager registry (specifically, dbconnection0) to verify that the registry points to the proper database.
DC Directory HealthCheck Validation	This check occurs on the publisher database and subscriber servers.	The utility validates whether Cisco Unified CallManager is integrated with DC Directory. This utility validates the DC Directory connection and the DC Directory configuration containers.

Table 2 **Validation Checks That the Utility Performs (continued)**

Module	Applicable Server	Additional Information
Security Settings Validation	This check occurs on the publisher database and subscriber servers.	<p>The utility validates the following policies and accounts:</p> <ul style="list-style-type: none"> • Password policies, including Enforce Password History, Minimum Password Age, and Minimum Password Length Verify that these policies are set to default. • Account lockout policies Verify that these policies are set to default. • Local system accounts for all Administrator accounts Verify that the local system accounts for all Administrator accounts are set to Never Expire. <p>Note The utility validates the settings of the publisher database server even when it is running on the subscriber server.</p>
Cisco Unified CallManager Database Replication Validation	This check occurs on the publisher database server.	<p>The publisher database server upgrade requires that all call-processing processes that the server handles fail over to the configured subscriber servers. Database replication must exist prior to the upgrade, so failover occurs.</p> <p>This utility verifies the database replication status for all subscriber servers in the cluster. This utility validates that the database contains the latest information about the system. Validation results include Running, Idle, Failed, or Succeeded.</p>
Hostname Resolution Validation	This check occurs on the subscriber database server only.	The utility validates that the server hostname resolves to a valid IP address.
Password Validation	This check occurs on the subscriber database server only	The utility performs a check on each subscriber database server to verify that the Administrator password on the subscriber database servers matches the Administrator password on the publisher database server.
Domain Validation	This check occurs on the publisher database and subscriber servers.	The utility verifies that the system is not part of a domain.
Resource Validation	This check occurs on the publisher database and subscriber servers.	This utility verifies that the system has enough physical memory.

Installing the Utility

**Caution**

If you choose to do so, you can use Virtual Network Computing (VNC) to install and run this utility. To obtain the most recent version of this document, go to http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm.

Do not use Integrated Lights Out (ILO) or Terminal Services to install or run this utility; Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote management and configuration tasks.

Perform the following procedure to install the utility:

Procedure

Step 1 Click <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.

Step 2 Click **CallManager Utilities**.

Step 3 Download the Upgrade Utility file to your hard drive.

**Tip**

For this utility, Cisco uses the file format, CCMUpgdAsstInstall_<utility version>.exe.

Step 4 Remember the location where you save the downloaded file.

Step 5 To begin the installation, double-click the download file.

**Note**

If Cisco Security Agent (CSA) is enabled, a prompt asks you if you are installing software. To continue the installation, click **Yes to All**.

The Preparing to Install window displays.

Step 6 The Welcome window displays; click **Next**.

The license agreement displays.

Step 7 Review the license agreement, click the **I accept the terms in the license agreement** radio button to accept the terms, and click **Next** to proceed with the installation.

Step 8 Verify the customer information. Click **Next**.

The Ready to Install window displays. Click **Install**.

Step 9 When the InstallShield Wizard Complete window displays, click **Finish**.

Running the Utility



Tip

You can run the utility on only one server at a time.

Running this utility takes approximately 1 to 60 (or more) minutes for the publisher database server. The time that it takes on the publisher database server depends on the size of the backup file.

The utility takes approximately 1 to 5 minutes for each subscriber server.

To run the utility, perform the following procedure.

Procedure

-
- Step 1** Choose **Start > Programs > Cisco Systems, Inc > CallManager Upgrade Utility**.
- Step 2** The Welcome window displays. Review the information in the window and click **Next**.
- Step 3** The Choose a Cisco Unified CallManager Version displays. Choose the Cisco Unified CallManager version to which you are interested in upgrading and click **Next**.
- Step 4** The Upgrade Utility Confirmation window displays with a list of checks that the utility performs. Review the information in the window and click **Next**.
- During the validation process, the Cisco Unified CallManager Upgrade Utility Status windows displays. An “x” indicates that the validation failed; a check indicates that the validation succeeded; an arrow indicates the validation task that the utility currently performs.
- Step 5** In the Upgrade Utility Summary window, the validation results display. To interpret the results, see the [“Interpreting the Results” section on page 7](#).



Caution

Clicking **Finish** closes the window. Review the results before you click Finish. If you close the window, you can obtain the results from the log file; see the [“Obtaining the Log File” section on page 8](#).

- Step 6** After you fix the problems that the utility identifies, run the utility again on every server in the cluster before you begin the upgrade.
-

Interpreting the Results

The validation results display in the Upgrade Utility Summary window. At the top of the window, a report summarizes the results for all modules and displays which modules failed, which modules produced warnings, and which modules passed. A link to the folder that contains all log files, including the Upgrade Utility Summary report, displays also.

To identify a problem with the failed validation module, review the following information that displays in the Summary window:

- The first link points to the log file that specifies the error or warning.

Click the first link and search for the error or warning; for example, ERR: <message> or WARN: <message>.

- The second link points to the corrective action file that describes the log file error message and recommends the corrective action.

To open the corrective action file, click the second link. Search the corrective action file for the error message that is noted in the log file. Review the description and corrective action.

**Caution**

After you correct all problems that the utility identifies, Cisco strongly recommends that you run the utility again on every server in the cluster before you begin the upgrade.

Obtaining the Log File

You can obtain the results from the utility in the following directory:

C:\Program Files\Common Files\Cisco\Log\UPGRADEASST<date> (for example, UPGRADEASST-05-15-2003_13.47.58)

To access the log file, click the **Summary** file.

**Tip**

A link to the log file displays in the Summary window for every failed validation module. To access the log file, click the link in the Summary window.

The Summary.html file, which is the Upgrade Utility Summary report, provides the exact same information that displays in the Upgrade Utility Summary window.

Each time that you run the utility, the utility creates a new log folder and new set of log files. The utility does not remove the log files, even if you uninstall the utility. You erase the log files when you reimaged the server or manually delete the files.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wl/export/crypto/tool/stqrg.html>. If you require further assistance please contact us by sending email to export@cisco.com

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key 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.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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/en/US/support/index.html>

Access to all tools on the Cisco Support 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

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
- 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>
- *Internet Protocol Journal* is a quarterly journal published by Cisco 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, 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 where networking professionals 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>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- 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>

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Copyright © 2006. Cisco Systems, Inc. All rights reserved.

