



Installation Guide for Cisco Unified Videoconferencing Manager Release 7.1

February 2010

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

Text Part Number: OL-21618-01

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

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

Installation Guide for Cisco Unified Videoconferencing Manager Release 7.1
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Installing Cisco Unified Videoconferencing Manager	1-1
About Prerequisites for Installing of Cisco Unified Videoconferencing Manager	1-1
Minimum System Requirements	1-1
Downloading the Server Operating System	1-2
LDAP Server Types	1-2
Supported Devices	1-2
SNMP Service	1-2
Port Requirements	1-3
How to Install Cisco Unified Videoconferencing Manager	1-4
Installing Cisco Unified Videoconferencing Manager	1-4
Installing Cisco Unified Videoconferencing Desktop	1-5
How to Perform Post-installation Procedures	1-8
Confirming Installation	1-8
Verifying the Cisco Unified Videoconferencing Manager Services Are Installed	1-8
Logging in for the First Time	1-9
Obtaining a License	1-9
Changing Server Name and Web Port	1-9
Updating the Cisco Unified Videoconferencing Desktop License	1-10
Uninstalling Cisco Unified Videoconferencing Manager	1-11

CHAPTER 2

Backing up and Restoring Cisco Unified Videoconferencing Manager Data	2-1
How to Back up Cisco Unified Videoconferencing Manager Data	2-1
What is Backup up?	2-2
Backing up Cisco Unified Videoconferencing Manager Data	2-3
How to Restore Cisco Unified Videoconferencing Manager Data	2-3
About Restore Procedure	2-3
Restoring Cisco Unified Videoconferencing Manager Data	2-4



CHAPTER 1

Installing Cisco Unified Videoconferencing Manager

- [About Prerequisites for Installing of Cisco Unified Videoconferencing Manager, page 1-1](#)
- [How to Install Cisco Unified Videoconferencing Manager, page 1-4](#)
- [How to Perform Post-installation Procedures, page 1-9](#)
- [Updating the Cisco Unified Videoconferencing Desktop License, page 1-11](#)
- [Uninstalling Cisco Unified Videoconferencing Manager, page 1-12](#)

About Prerequisites for Installing of Cisco Unified Videoconferencing Manager

Read this section before installing Cisco Unified Videoconferencing Manager.

- [Minimum System Requirements, page 1-1](#)
- [Downloading the Server Operating System, page 1-2](#)
- [LDAP Server Types, page 1-2](#)
- [Supported Devices, page 1-2](#)
- [SNMP Service, page 1-2](#)
- [Port Requirements, page 1-3](#)

Minimum System Requirements

You must install Cisco Unified Videoconferencing Manager on one of the following Cisco MCS server models:

- Cisco MCS 7825 Series
 - MCS-7825-H2
 - MCS-7825-I2
 - MCS-7825-H3
 - MCS-7825-I3

- Cisco MCS 7835 Series
 - MCS-7835-H2
 - MCS-7835-I2
- Cisco MCS 7845 Series
 - MCS-7845-H2
 - MCS-7845-I2

Downloading the Server Operating System

The Cisco MCS server operating system is shipped with the Cisco Unified Videoconferencing Manager software.

For information about downloading the Media Convergence Server operating system software updates from Cisco.com, refer to the Release Notes for Cisco Unified Videoconferencing Manager Release 7.1.

LDAP Server Types

Cisco Unified Videoconferencing Manager supports Microsoft Active Directory 2000 and 2003, and IBM Lotus Domino Server.

Supported Devices

Cisco Unified Videoconferencing Manager supports the following devices:

- Cisco IOS H.323 Gatekeeper
- Cisco Unified Communications Manager
- Microsoft LCS 2005 SP1
- Microsoft OCS 2007 and OCS 2007 R2
- Broadsoft IPCentrix
- Cisco Unified Videoconferencing 3500 MCU version 5.6
- Cisco Unified Videoconferencing 3500 Gateway versions 5.6
- Cisco Unified Videoconferencing 5000 MCU versions 7.0 and 7.1
- Cisco Unified Videoconferencing Desktop version 7.1
- Sony endpoints: PCS 1, PCS 11, PCS 1600, TL30, TL50, G50, and G70

SNMP Service

Install the Microsoft Windows SNMP service for Cisco Unified Videoconferencing Manager.

Port Requirements

Table 1 shows the required ports for Cisco Unified Videoconferencing Manager. Make sure all required ports are available.

Table 1 Required Ports

Protocol	Ports	Type	Direction	Purpose	Destination
Cisco Unified Videoconferencing Manager Server Ports					
HTTP	80	TCP	In from Web	Web UI access and Web Service access	Cisco Unified Videoconferencing Manager
HTTPS	443	TCP	In from Web (HTTPS)	Web UI access and Web Service Security access	Cisco Unified Videoconferencing Manager
XML	3336	TCP	In from Desktop	Cisco Unified Videoconferencing Manager's version of MCU Call Control XML API	Cisco Unified Videoconferencing Manager
XML	3339	TCP	Local connection	CUVCM XML API with B2B	Cisco Unified Videoconferencing Manager
XML	3271	TCP	Local connection	Resource Manager connects to the XML API interface of the internal gatekeeper	Cisco Unified Videoconferencing Manager
Internal gatekeeper HTTP	8011	TCP	In from Web	Web UI access. Disabled by default.	Cisco Unified Videoconferencing Manager
Database connection	3306	TCP	Local database connection	If the internal database is installed, the application communicates with the database using port 3306.	Cisco Unified Videoconferencing Manager
Data synchronization	3344	TCP/UDP	Info from another CUVCM	Synchronization of object data between two CUVCM, only used in redundancy deployments.	Another CUVCM
LDAP	389	TCP	Between CUVCM and LDAP Servers	LDAP servers communication	LDAP servers
LDAP	636	LDAP over SSL	CUVCM and Directory Servers	Connection to Directory Server with Security	Active Directory Servers
NTLM	445	TCP/UDP	Between CUVCM and Directory Servers	Connection to Active Directory Server for SSO	Active Directory Servers
SNMP	161	UDP	In from Resource Manager and Network Manager	Configuration/Status	Cisco Unified Videoconferencing Manager
SMTP	25	TCP	Out to SMTP server	Connect SMTP server for sending email notifications	SMTP server
SIP Signaling	5060/5061	TCP/UDP	Info from SIP entries	SIP signaling between B2B and SIP entries	Other SIP entries
FTP	21	TCP	In from Network Manager	Log retrieval	Cisco Unified Videoconferencing Manager

Table 1 Required Ports (continued)

Protocol	Ports	Type	Direction	Purpose	Destination
TCP/TLS	3340	TCP/ TLS	Info from CUVC Desktop	XML Connection to CUVC Desktop	CUVC Desktop
MCU Ports					
HTTP	80	TCP	In from Web	Web UI access	MCU
XML	3336	TCP	In from Resource Manager	MCU Call Control XML API	MCU
XML	3337	TCP	In from another MCU or Desktop	MCU Cascade XML API	MCU
SNMP	161	UDP	In from Resource Manager and Network Manager	Configuration/Status	MCU
Telnet	23	TCP	In from Network Manager	Log retrieval and advanced commands	MCU
Gateway Ports					
HTTP	80	TCP	In from Web	Web UI access	Gateway
SNMP	161	UDP	In from Resource Manager and Network Manager	Configuration/Status	Gateway
Telnet	23	TCP	In from Network Manager	Log retrieval and advanced commands	Gateway

How to Install Cisco Unified Videoconferencing Manager

During the Cisco Unified Videoconferencing Manager installation procedure you install Resource Manager and Network Manager components. You install the Desktop component of Cisco Unified Videoconferencing Manager separately.

- [Installing Cisco Unified Videoconferencing Manager, page 1-4](#)
- [Installing Cisco Unified Videoconferencing Desktop, page 1-6](#)

Installing Cisco Unified Videoconferencing Manager

Before you Begin

Verify that the account you use while performing this installation procedure is an administrator account, either a local administrator or the domain account that has administrator privileges on the local computer.

Procedure

-
- Step 1** Click the `Cisco_Unified_Videoconferencing_Manager` installer to start the installation wizard.
- Step 2** Click **Next** in the Introduction window.

- Step 3** Read and accept the license agreement in the License Agreement window, and then click **Next**.
- Step 4** Leave the default option in the Installation Type window, and then click **Next**.
- Step 5** Select a user provisioning option in the User Provisioning window. There are three available options:
- No integration with Directory Server
 - Directory Server
 - Directory Server with Single Sign On (SSO) enabled.

You must enable SSO to work with the Cisco Unified Videoconferencing Manager Resource Manager Outlook Client.

- Step 6** Click **Next**.



Note

Using SSO, a user who is logged into the organization domain and then tries to access the Cisco Unified Videoconferencing Manager Web login window, is authenticated (transparently) according to ADS domain account and password credentials when that user enters the Cisco Unified Videoconferencing Manager Web login window. As long as the user employs ADS, he/she will not be requested to enter a user name and password.

For more information about Microsoft Active Directory Server, see <http://support.microsoft.com/default.aspx?scid=kb;en-us:Q258063>.

If the URL contains dots (for example, “server.mycompany.com”), add the URL as a trusted site in your local Internet Explorer to enable SSO to work on your local machine.

- Step 7** Select the directory in which you want to install the application in the Directory Selection window, and then click **Next**.
- Step 8** Enter the host name URL and Web server port number used by the application in the Server Information window.
- Make sure that the Web server port is not in use by another application, and then click **Next**.
- Step 9** Select MySQL installation.
- Step 10** Click **Next**.
- Step 11** If you choose to create a new database, choose a folder where you want to install MySQL.
- Step 12** Click **Next**.
- Step 13** Enter the database name, user login ID, and password in the CUVCM RM Database Information window.
- Step 14** Click **Next**.
- Step 15** Enter mail server information in the Outgoing Mail Server Information window. To confirm that the email server is functioning, enter an email address. If the email server is functioning correctly, you receive a test email.



Note

If SMTP server fields are left blank, email messages are not sent.

- Step 16** Create an administrator account for accessing the application in the Account Login Information window. With this account, you can access Cisco Unified Videoconferencing Manager.
- Step 17** Review the installation summary in the Pre-installation Summary window, and then click **Install** to proceed with the installation.

**Note**

Do not interrupt the installation. After starting the Cisco Unified Videoconferencing Manager service allow several minutes for server initialization before logging in to the web-user interface.

Installing Cisco Unified Videoconferencing Desktop

During the installation you perform a basic Desktop configuration by defining which servers Desktop uses. Follow recommendations in this section to configure Desktop correctly:

- For deployments of more than 100 users in which streaming or recording is heavily used or for deployments in which port 80 is used for streaming, Cisco recommends that you perform one of the following:
 - install the streaming and recording servers together on a server different from the Desktop server
 - install the streaming and recording servers separately on two servers different from the Desktop server
- The Streaming Server is always installed under C:\Program Files, even if other components of Cisco Unified Videoconferencing Desktop Server are installed at a different location.
- The default Desktop web server port is 80. If other applications are using port 80, the installer prompts you to choose another port.

If you wish to use port 80 in such cases, access the Services panel on your computer and disable the IIS Administration, HTTP SSL and World Wide Web Publishing services. You can do this before installing the Desktop server software or when you receive the "ip address/ port is in use" error during installation.

After disabling these services, installation completes normally and Desktop clients can connect to the Desktop server using port 80.

- If you wish to use the HTTPS protocol for security, configure the Desktop web server port to 443 after installation is complete.
- The Cisco Unified Videoconferencing Desktop License Key is required for the installation and operation of the Cisco Unified Videoconferencing Desktop Server and is not included in this package. For more information about obtaining the serial key, refer to the License Fulfillment Instructions for Cisco Unified Videoconferencing Manager at http://www.cisco.com/en/US/products/ps7088/prod_installation_guides_list.html.
- A Cisco Unified Videoconferencing Desktop Recording Key is required to activate the recording and playback functionality within this product. You can choose to install recording without a license key, in which case it is installed in evaluation mode. Only one recording is allowed at a time, and the recording duration is limited to five minutes.

**Note**

Do not install the Desktop Client on the Cisco Unified Videoconferencing Desktop Server.

Before You Begin

- Add the hostname of the Cisco Unified Videoconferencing Desktop Server to the DNS.
- Obtain a Desktop License key and an optional recording serial key. See License Fullfillment Instructions at http://www.cisco.com/en/US/products/ps7088/prod_installation_guides_list.html

Procedure

- Step 1** Insert the product CD-ROM.
- Step 2** Click **Install Cisco Unified Videoconferencing Desktop Server** in the CD menu
-or-
Double-click the setup.exe file in the Windows folder on the product CD-ROM to launch the installer.
- Step 3** Select the installation language in the Choose Setup Language window, and then click **OK**.
- Step 4** Click **Next** in the Welcome window.
- Step 5** Read the agreement in the License Agreement window, click **I accept the terms in the license agreement**, and then click **Next**.
- Step 6** Enter information for software registration in the Customer Information window, select the user access option for Desktop, and then click **Next**.
- Step 7** Enter the Desktop key number in the Cisco Unified Videoconferencing Desktop Key window, and click **Next**.
- Step 8** Define which Desktop components to install on this server and specify the installation location in the Custom Setup window, and then click **Next**.



Note The default directory for Cisco Unified Videoconferencing Streaming Server installation is C:\Program Files\Darwin Streaming Server.
For a single server installation, install both components.

- Step 9** Configure the Desktop Network Interface and Desktop web server port in the Cisco Unified Videoconferencing Desktop Network Configuration window, and click **Next**.
- Step 10** Configure server settings in the Configure Servers window:
- a. Enter the IP address of your gatekeeper in the Gatekeeper IP address field.
 - b. Enter the NIC IP address of the server in the IP address field under Use Cisco Unified Videoconferencing Manager for moderation.

Alternatively, click **Do not enable moderation** to work without a meeting control server in a multiple Cisco Unified Videoconferencing 3545 MCU deployment. If you use Cisco Unified Videoconferencing Manager as your meeting control server, enter the Cisco Unified Videoconferencing Manager IP address in the IP address of Cisco IOS H.323 Gatekeeper field so that Desktop uses the Cisco Unified Videoconferencing Manager internal gatekeeper.



Note You must use the specific IP addresses, not loopback addresses.

- Step 11** Select a server to manage streaming in the Configure Streaming window:
- a. When your deployment includes multiple Desktop servers, you must define which one of your Desktop servers is enabled for streaming.

Select **This Cisco Unified Videoconferencing Desktop will be used to manage streaming services** to define the Desktop server that you are currently configuring as the Desktop server that is enabled for streaming.



Note Cisco recommends that you select only one Desktop server to be a streaming server.

If you install the Cisco Unified Videoconferencing Streaming Server on a separate server, enter the IP address of that server in the Darwin Streaming Server IP address field.

- b. When your deployment includes multiple Desktop servers, and you do *not* want to define the Desktop server that you are currently configuring as the Desktop server that is enabled for streaming, select **Use an alternative Cisco Unified Videoconferencing Desktop to manage streaming services**.

Enter the Fully Qualified Domain Name (FQDN) of the Desktop server that *is* enabled for streaming in the Server URL field.

- c. Click **Disable streaming for this Cisco Unified Videoconferencing Desktop** to disable streaming for the Desktop server that you are currently configuring.

- Step 12** Specify the hostname of the server that clients should use to connect to the Desktop in the Cisco Unified Videoconferencing Desktop Hostname Configuration window.



Note Make sure that you specify the hostname that clients can resolve.

- Step 13** Specify the storage location for recorded meetings. You can change the location of recorded meetings by clicking "Browse". You can also change the maximum amount of disk space to allocate for recorded meetings by entering the value in the text box. The default size for recorded meetings is 8192 MB.

- Step 14** Click **Install** in the Ready to Install the Program window.

- Step 15** Click **Finish**.

- Step 16** After installation is completed, verify that the Desktop server is operational:

- a. Access the Desktop Server Administration interface by connecting to the following URL:
http://<SERVERFQDN:PORT>/cuvvm/admin
- b. Sign-in using the default user name (admin) and password (admin).
- c. Open the Status tab of the Desktop Server Administration interface, and verify that all four types of servers are connected.

The light next to each link indicates whether or not the connection to the target server or registration with the Gatekeeper is successful. When the light is red, a tooltip containing error details is available. Click the red light to view further error information.

- Step 17** Remove the product CD-ROM.
-

How to Perform Post-installation Procedures

- [Confirming Installation, page 1-9](#)
- [Verifying the Cisco Unified Videoconferencing Manager Services Are Installed, page 1-9](#)
- [Signing-In for the First Time, page 1-10](#)
- [Obtaining a License, page 1-10](#)
- [Changing Server Name and Web Port, page 1-10](#)

Confirming Installation

Procedure

- Step 1** Wait two to three minutes for server initialization.
- Step 2** Go to <http://host-URL:port-number>.
- Step 3** Verify that the Resource Manager login window appears.
- Step 4** Verify that you can sign-in to the web interface using the administrator account specified in the installation process.
-

Verifying the Cisco Unified Videoconferencing Manager Services Are Installed

Cisco Unified Videoconferencing Manager is installed as a Windows Service on your server.



Tip

Cisco Unified Videoconferencing Manager automatically starts when you start the server.

Procedure

- Step 1** Navigate to **Start > Settings > Control Panel > Administrative Tools > Services** and find the list of Cisco Unified Videoconferencing Manager related services.
- Step 2** Verify that the following services are installed:
- Cisco Unified Videoconferencing Manager—The service that Resource Manager and Network Manager run on. This is started automatically.
 - Cisco SipServer—The service for the SIP User agent included with Resource Manager for SIP call control. This is started automatically.
 - Cisco Unified Videoconferencing Desktop - Apache Tomcat - Apache Tomcat Server. This is started automatically.
 - Cisco Unified Videoconferencing Desktop - Conference Server 7.11.000 - Multipoint Control Unit. This is started automatically.
 - Cisco Unified Videoconferencing H.323 Gatekeeper Watchdog - Restarts the Cisco Unified Videoconferencing H.323 Gatekeeper on system failure. This is started automatically.

You can turn off this service in H.323-only deployments. Access the `vcs-core.properties` file located by default under

`C:\Program Files\Cisco\Unified Videoconferencing Manager\CUVCMRM\jboss\bin`

and make the following change:

```
vnex.vcms.core.sip.serverAddress=
```

- Cisco Unified MeetingPlace H.323 Gatekeeper - The service that the internal gatekeeper runs on. This is started automatically.

Signing-In for the First Time

Procedure

-
- Step 1** Access either the Resource Manager or the Network Manager login window from the Start menu of the local server.
- Step 2** Sign-in to Resource Manager for the first time.
The User Provisioning window opens.
- Step 3** (Optional) Enable directory integration to synchronize user records from a Directory Server.
-

Related Topics

For further information, see the Configuration Guide for Cisco Unified Videoconferencing Manager at http://www.cisco.com/en/US/products/ps7088/products_installation_and_configuration_guides_list.html.

Obtaining a License

At the end of the installation process, a temporary license is automatically installed. This license is valid for 30 days. To obtain an Cisco Unified Videoconferencing Manager license, perform a procedure described in the License Fulfillment Instructions for Cisco Unified Videoconferencing Manager at http://www.cisco.com/en/US/products/ps7088/prod_installation_guides_list.html.

Changing Server Name and Web Port

Procedure

-
- Step 1** After installation, navigate to
`\JBOSS_DIR\server\default\deploy\jbossweb-tomcat55.sar\server.xml`
and modify the entry in bold in the example:

```
<Connector port="80" address="{jboss.bind.address}"
  maxThreads="250" strategy="ms"
    maxHttpHeaderSize="8192"
  emptySessionPath="true"
  enableLookups="false" redirectPort="8443"
    acceptCount="100"
  connectionTimeout="20000"
    disableUploadTimeout="true"/>
```

Step 2 Navigate to the \JBOSS_DIR\bin\wcs-config.xml file and modify the following entry:

```
<host-url>http://server_URL:port_number</host-url>
```

JBOSS_DIR is the default JBOSS home directory path.

The default path is C:\Program Files\Cisco\Unified Videoconferencing Manager\CUVCMRM\jboss.

Updating the Cisco Unified Videoconferencing Desktop License

You need to update the Cisco Unified Videoconferencing Desktop Server license in these cases:

- If you upgrade the Cisco Unified Videoconferencing Desktop Server by adding the recording feature or increasing the number of simultaneous recordings which requires a new or updated recording serial key
- If you upgrade Cisco Unified Videoconferencing Solution by adding Cisco Unified Videoconferencing 3500 MCUs and required additional ports on the Cisco Unified Videoconferencing Desktop Server

Before You Begin

Obtain a Cisco Unified Videoconferencing Desktop License Key and an optional Cisco Unified Videoconferencing Desktop Recording Key.

Procedure

- Step 1** Click **Start > Settings > Control Panel**.
- Step 2** Double-click **Add or Remove Programs**.
- Step 3** From the list of programs, choose **Desktop**, and then **Change**.
The Setup Wizard opens.
- Step 4** In the Welcome screen click **Next**.
- Step 5** In the Program Maintenance screen, choose **Modify**, and click **Next**.
- Step 6** In the Custom Setup screen, click **Next**.
- Step 7** In the Cisco Unified Videoconferencing Desktop Key window, enter updated keys, and then click **Next**.
- Step 8** Follow on-screen instructions to complete installation configuration.
-

Uninstalling Cisco Unified Videoconferencing Manager

Procedure

Step 1 Select **Start > Programs > Cisco > Cisco Unified Videoconferencing Manager > Uninstall Cisco Unified Videoconferencing Manager**

–or–

Step 2 Select **Control Panel > Add/Remove Programs > Cisco Unified Videoconferencing Manager > Uninstall Program.**



CHAPTER 2

Backing up and Restoring Cisco Unified Videoconferencing Manager Data

You can restore the Cisco Unified Videoconferencing Manager database and configuration files from a backup copy. You should back up your database and configuration files on a regular basis.

You can only backup and restore database and configuration files within the same Cisco Unified Videoconferencing Manager release number. Do not attempt to back up the database and configuration files from an old Cisco Unified Videoconferencing Manager version and restore these files to a newer version.

There are many reasons for performing system backups on a regular basis, such as:

- Hardware failure
- Software failure
- Data corruption
- User mistakes
- Before any software upgrade

To restore Cisco Unified Videoconferencing Manager data, stop the Cisco Unified Videoconferencing Manager service before restoring the database, configuration files, branding and sound files. Restart the Cisco Unified Videoconferencing Manager service after restoration is complete.

You perform the backup and restore procedures using the Cisco Unified Videoconferencing Manager Backup and Restore tool.

- [How to Back up Cisco Unified Videoconferencing Manager Data, page 2-1](#)
- [How to Restore Cisco Unified Videoconferencing Manager Data, page 2-3](#)

How to Back up Cisco Unified Videoconferencing Manager Data

- [What is Backed up?, page 2-2](#)
- [Backing up Cisco Unified Videoconferencing Manager Data, page 2-3](#)

What is Backed up?

During backup the following data is saved and backed up:

- Property files—Local text files which are used by the Cisco Unified Videoconferencing Manager application.
- Database—Stores all the configuration information and the scheduling information.

Table 1 shows what property files are backed up during the backup procedure.

Table 1 Property Files

Location	File name
Cisco Unified Videoconferencing Manager-related property files	
%Cisco Unified Videoconferencing Manager% <i>\i</i> CM\jboss\bin	authentication.properties
	ivrslidemsg.properties
	vcs-advanced.properties
	vcs-core.properties
	vnex.properties
	aivr-call-state-machine.xml
	ha.xml
	mdap-context.xml
	pre-start-call-state-machine.xml
	trap-config.xml
	vcs-cdr-conf.xml
	vcs-config.xml
	vcs-config-dest.xml
vivr-call-state-machine.xml	
%Cisco Unified Videoconferencing Manager% <i>\i</i> CM\jboss\server\default\conf	jndi.properties
	log4j.xml
	login-config.xml
%Cisco Unified Videoconferencing Manager% <i>\i</i> CM\jboss\server\default\deploy	mysql-ds.xml
B2BUA-related property files	
%Cisco Unified Videoconferencing Manager% <i>\i</i> CM\sipserver\conf	service.ini
	SIPConfig.xml
	UpdatedSIPConfig.xml

The Cisco Unified Videoconferencing Manager Backup and Restore tool supports both types of databases used by Cisco Unified Videoconferencing Manager:

- Internal—MySQL
- External—MS SQL

Backing up Cisco Unified Videoconferencing Manager Data

Procedure

- Step 1** Select **Start > Programs > Cisco > Cisco Unified Videoconferencing Manager > Launch Backup and Restore Tool**.
- Step 2** Select **Backup Configuration**, and then click **Next**.
- Step 3** Select the type of files you want to back up.
- Step 4** Specify the path to the location where you want to place the backup file.
- Step 5** If necessary, modify the backup file name.

By default the file name format is Backup_Database_Props. After the backup process is completed, the current date (YYYYMMDD) and time (1421) stamps are automatically added to the file name. For example, Backup_Database_Props_20091215_1421.zip.

- Step 6** Click **Next**.
- Step 7** Click **Start**.
- The backup process begins. Upon completion the success message is displayed.
- Step 8** For the MS SQL database backup, share a folder on the MS SQL server so that it is accessible with read permission. The share name and the actual name of this folder must be the same. Then click the link to verify that the folder is accessible.
- Step 9** Click **OK**. The backup procedure is completed.
-

How to Restore Cisco Unified Videoconferencing Manager Data

- [About Restore Procedure, page 2-3](#)
- [Restoring Cisco Unified Videoconferencing Manager Data, page 2-4](#)

About Restore Procedure

The database restore procedure may be risky due to possible network or database issues. In case such issues occur and the restore procedure cannot be completed, the current database is destroyed. The Cisco Unified Videoconferencing Manager Backup and Restore tool reduces the risk by using a safe restore workflow:

The Cisco Unified Videoconferencing Manager Backup and Restore tool creates a new database instance with a temporary name for restore data. If the restore procedure is executed successfully, the Cisco Unified Videoconferencing Manager Backup and Restore tool renames and stores the current database and renames the newly created database instance. If the restore procedure fails, an administrator can still use the current database which was not deleted.

Restoring Cisco Unified Videoconferencing Manager Data

Procedure

- Step 1** Select **Start > Programs > Cisco > Cisco Unified Videoconferencing Manager > Launch Backup and Restore Tool**.
- Step 2** Select **Restore Configuration**, and then click **Next**.
- Step 3** Select the backup file which you want to use, and then click **Next**.
- Step 4** Click **Start**.
- The restore process begins. Upon completion the success message is displayed.
- Step 5** For the MS SQL database restore:
- Enter admin login name and admin password.
 - Share a folder on the MS SQL server so that it is accessible with write permission.
- Step 6** Click **OK**.
-