Cisco TelePresence Content Server Release 5.2 and 5.3 Quick Start Guide

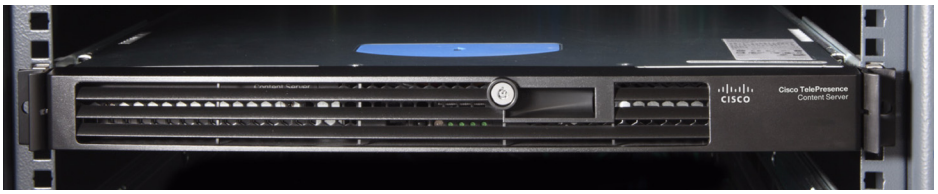
Revised: February 2012

This document contains information about getting your Content Server installed and initially configured:

About the Cisco TelePresence Content Server

The Cisco TelePresence Content Server (Content Server) provides you with a quick and easy way to record video calls and conferences, edit them, and watch them later. You can also stream calls and recordings while they take place.

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



Package Contents

The following items are included with the Content Server. Verify that you have these items before you install the unit:

- Power cable
- Ethernet cable
- Serial cable
- Rack mounting kit. The rack mounting kit contains the following:
  - Outer rail slide assembly (2)
  - Inner rail slide (2)
  - Rail safety stop (one each on inner slides)
  - Outer slide scale screws (8 #8-32 x 1/2”) *
  - Inner slide scale screws (8 #6-32 x 1/4”)
  - Rack screws (2 #8-32 x 3/4”)

Note This kit includes two sets of 8-32 x 1/2” screws. One set of eight has a larger screw head size than the other: use the set that best fits the rack in which the rail kit is being installed.

Connecting the Content Server

Note Before installing the Content Server, you must read the safety information at this location:

http://www.cisco.com/go/telepresence/safety

Installation Site Preparations

Ensure that the following conditions are satisfied:

- There is at least 10 cm (4 inches) behind the unit’s rear panel and 10 cm (4 inches) in front of the front panel.
- The room in which you install the unit has an ambient temperature between 0 ºC and 35 ºC (32 ºF and 95 ºF) and between 10% and 90% non-condensing relative humidity.

- You use a grounded AC power outlet for the unit.
- You turn off all peripheral devices connected to the unit.
- You turn off the unit by pressing the power button on the front of the chassis; then unplug the AC power cord(s) from the chassis or wall outlet.
- You disconnect all peripheral cables and all telecommunications lines connected to I/O connectors or ports on the back of the chassis.
- You provide electrostatic discharge (ESD) protection by wearing an anti-static wrist strap attached to a chassis ground - any unpainted metal surface - when handling components.
- You have the following tools:
  - Phillips (cross head) screwdriver (#1 bit and #2 bit).
  - Anti-static wrist strap and conductive foam pad (recommended).

Also take these precautions:

- Do not place heavy objects directly on top of the unit.
- Do not place hot objects directly on top, or directly beneath the unit.

Task 1: Rack Mounting (Optional)

Cisco recommends that the unit is mounted in the rack using the supplied rack mounting kit. If necessary, using the key, unlock and remove the black grill.

Removing the inner rail from the rail assembly

Step 1 Extend the inner rail until it locks.

Step 2 Depress the spring safety lock to release the inner rail.

Step 3 Remove the inner rail from the rail assembly.

Installing the outer rail slides to the rack posts

The rail flanges mount to the inside of each post. Attach the outer rail slides to the rack posts using two #8-32 x 1/2” screws at the front posts, and two #8-32 x 1/2” screws at the rear posts.

Attaching the inner rails to the server chassis sidewalls

Step 1 Insert the inner rails over the server chassis sidewall studs.

Step 2 Slide the inner rails toward the front of the server chassis so that it “locks” into place.

Step 3 Secure the inner rails with one #6-32 x 1/4” screw for each rail.

Installing the server chassis into the rack

Step 1 Align the inner rails (attached to the server chassis) with the outer rail assemblies (attached to the rack). The inner slides must be positioned all the way forward in the rails to ensure proper installation of the server.

Step 2 Engage the matching rails, and slide the server chassis into the rack until the two safety stops lock into position.

Step 3 Depress the two safety locks (one on each side).

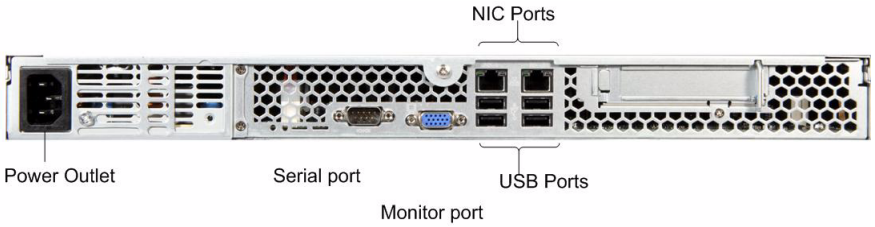
Step 4 Slide the server chassis all the way into the rack.

Step 5 Screw on the rack handles with the screws provided.

Step 6 Use the rack screws (#8-32 x 3/4") to secure the chassis and rack handles into the rack.

Task 2: Connecting Power

Step 1 Connect a LAN cable from the NIC 1 connector on the back panel to your network. (The NIC2 connector must not be used.)



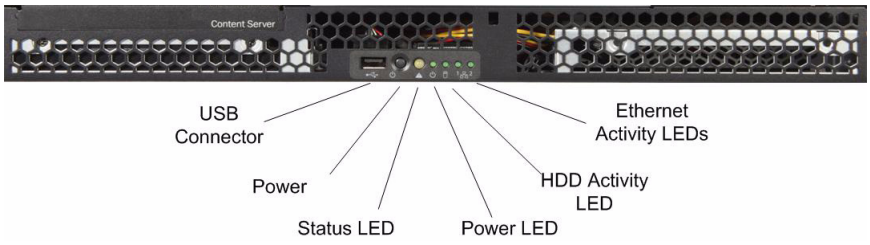
Step 2 Connect the AC power cable.

Step 3 Connect the supplied serial cable from the serial port on the back of the unit to the serial port on a PC.

Step 4 Press the power button on the front panel to turn the unit on.

Step 5 Wait until the system power indicator LED on the front panel lights up.

Step 6 If required, replace the front grill.



Task 3: Initial Configuration

Setting the local administrator password

You must set the local administrator password on first installation.

You can do this by using a terminal emulator program on a PC connected to the unit's serial port.

Step 1 Start a terminal emulator program on the PC by going to **All Programs > Accessories > Communications > HyperTerminal**. (If HyperTerminal is not installed, download a terminal emulator program from the Internet—for example, puTTY.)

Step 2 Open a new connection and enter a name for the connection.

Step 3 Configure the connection to use the PC's serial port as follows:

a. Set **Baud rate** to *115200* bps.

b. Set **Data bits** to *8*.

c. Set **Parity** to *None*.

d. Set **Stop bits** to *1*.

e. Set **Flow control** (hardware and software) to *None*.

Step 4 Press **Enter.**

Step 5 Press **Enter** again to display the main menu.

Step 6 Enter the new administrative password at the prompt. Confirm the password.

Step 7 Continue the terminal emulator session to set a static IP address, subnet mask and default gateway.

Note See the online help for more information.

Setting a static IP address, subnet mask, and default gateway

By default, the unit automatically acquires an IP address assigned by a DHCP server in your network. Cisco recommends that you change the IP address from DHCP to Static.

Step 1 Make sure that the unit is not recording or transcoding. Press **Esc** to check the recording/transcoding status**,** and to display the version, and IP address. If the status is displayed as recording or transcoding, calls and transcodes in progress should be terminated before moving on to Step 2.

Step 2 Use the Up or Down arrows to navigate to **IP settings > Address type** and press **Enter** to select. Use the Up or Down arrows to select *Static* and press **Enter**.

Step 3 Go to **IP settings > IP Address**.

Step 4 The cursor sits below the first digit showing which digit you can edit. For each digit in turn, press **Enter** to edit the digit and the cursor will flash. Use the Up or Down arrows to display the correct number and press **Enter** to set the digit. Press the Up arrow to move to the next digit, or the Down arrow to move to the previous digit.

Step 5 When all the digits have been set, press **Enter** to finish editing and select **Y**. Press **Enter** to confirm the changes.

Step 6 Go to **IP settings > Subnet mask**. Repeat steps 9 and 10.

Step 7 If you require a default gateway, go to **IP settings > Default gateway** and set its **IP address** using steps 9 and 10.

Step 8 Go to **IP settings > DNS (Preferred)** and set the **DNS Server IP address** using steps 9 and 10.

Step 9 Go to **IP settings > DNS (Alternate)** and set the **DNS Server IP address** using steps 9 and 10.

Step 10 Close the terminal emulator session and disconnect the serial cable.

Note Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for the unit's operation and restart.

Step 11 Restart the unit.

Note You must restart the unit after changing its IP address. Failure to do so may cause issue for unit operation.

Setting the date and time

You can do this by using the Content Server web interface:

Step 1 In Internet Explorer enter the IP address of the Content Server that you set to access the Content Server web interface.

Step 2 Log in with the local administrator account that you set.

Step 3 Go to the **Management** tab. Then go to **Configuration > Windows server**. The web interface for Windows Server administration opens.

Step 4 Go to **Maintenance > Date/Time**.

Step 5 Update the date, time and time zone and then click **OK**. This ensures that the creation date and time of conferences is displayed correctly in the Conference lists. Additionally, troubleshooting is easier when the logs reflect the correct time.

Step 6 Close the web interface for Windows Server administration.

Configuring H.323/SIP registration settings

Step 1 In the Content Server web interface, go to **Management settings > Site settings** and enter the **System name**. (This is used by the Cisco TelePresence Management Suite to identify the Content Server.) You can also display the System name in the browser's title bar when using the web interface by selecting **Show in browser title.**

Step 2 If you are using an H.323 gatekeeper, in the Gatekeeper settings section:

a. Select **Gatekeeper enabled** and enter the Gatekeeper's IP address or DNS name.

b. Enter the **H.323 ID** and **E.164 alias**, as needed.

c. For **Registration**, select either *Terminal* or *Gateway.*

d. If you select gateway mode, enter H.323 and E.164 gateway prefixes as needed.

Step 3 If you are using a SIP registrar, in the SIP settings section:

a. Select **SIP enabled** and enter the **SIP address (URI)** and **SIP display name**.

b. For **Server address**, enter the SIP registrar's IP address or DNS name.

Step 4 Click **Save**. The **Registration status** is updated. (You may need to refresh the page.)

Step 5 Go to **Recording setup > Recording aliases**.

Step 6 Click **Edit** for the default Recording aliases in turn. For each one set the following:

- If you are using an H.323 gatekeeper, enter the **H.323 ID** and the **E.164 alias**. Click **Save**.
- If you are using a SIP registrar, enter the **SIP address (URI)** and **SIP display name**. Click **Save**.

Caution Make sure that all E.164 aliases and H.323 IDs are unique in your network and valid for your gatekeeper. The H.323 ID of the default live recording alias is set to Live<serial_number> and is OnDemand<serial_number> for the default on-demand recording alias. See the online help for an explanation of recording aliases. SIP URIs must be unique in their network and valid for their SIP registrar.

Making a test recording by dialing out

Step 1 Go to the **Management** tab. Then go to **Recordings > Create recording.**

Step 2 Select the recording alias that you want to use.

Step 3 For **Dial number**, enter the address of the endpoint that you want to call and click **Place call**.

Step 4 Go to the **View Recordings** tab. You should see a thumbnail with a red recording dot for the recording in progress.

Step 5 End the call either from the endpoint or by clicking on the thumbnail first, then clicking **Edit recording** and finally clicking the **End call** button.

The recording is stored and then transcoded. When the process is complete, you will see the resulting recording in **View Recording > Recorded**. Click **Play** to watch the recording. See the online help for more information.

Making a test recording by dialing in

Make a test call from an endpoint by calling the dialing address of one of the default Recording aliases.

Step 1 Go to **Management** tab. Then go to **Recording setup > Recording aliases**.

Step 2 Note the H.323 ID, E.164 alias or SIP address (URI) for the Recording alias that you want to use.

Step 3 From an endpoint, dial one of the dialing addresses that you noted, as appropriate.

Step 4 Go to the **View Recordings** tab. You should see a thumbnail with a red recording dot for the recording in progress.

Step 5 End the call either from the endpoint or by clicking on the thumbnail first, then clicking **Edit recording** and finally clicking the **End call** button.

The recording is stored and then transcoded. When the process is complete, you will see the resulting recording in **View Recordings > Recorded**. Click **Play** to watch the recording. See the online help for more information.

Installing a security certificate

The Content Server has implemented SSL (Secure Sockets Layer) protocol for sending user authentication information (username and password) in a secure way at user log in. The SSL implementation means that the web-based user interface needs to establish its credentials with the user's browser through an electronic document known as a security certificate.

Each unit is shipped with a self-signed certificate, which is valid for a year. Because self-signed certificates are not from a trusted Certificate Authority, when users try to log in to the unit, most browsers will display a message that the identity of the site could not be verified.

You can add the unit to the Trusted sites list in Internet Explorer or add an exception in Firefox to avoid seeing error messages at log in. However, Cisco recommends purchasing a security certificate from a certificate issuing authority that has a trusted relationship back to a root authority, such as VeriSign or Comodo. These credentials are most likely to be trusted by browsers, removing the need to add the unit to the list of Trusted sites. This certificate needs to be generated against the Windows machine name or the DNS entry associated with the IP address that the unit is using.

To install your purchased security certificate on the unit's default web site:

Step 1 Log in to the unit using Remote Desktop and go to **Start > Administrative tools > Internet Information Services (IIS) Manager**.

Step 2 Under Internet Information Services, expand '<machine_name> (local computer)' and then 'Web Sites'.

Step 3 Right-click **Default web site**, and select **Properties**.

Step 4 In the **Directory Security** tab, click **Server certificate** in the Secure communications section.

Step 5 Follow the instructions in the Web Server Certificate Wizard to replace the current certificate with your purchased one. For more information, see the Internet Information Services help.

You can also install it for the Windows Media Administration web site and the Windows Server Administration web site to avoid getting security warnings when administrators log in to those sites.

When you have installed your certificate on the web sites, this certificate is then used instead of the self-signed one.

If the security certificate expires, (regardless of whether the unit uses your purchased security certificate or the original self-signed certificate), browsers will display another warning in addition to any previous warning related to self-signed certificates. A new certificate request can be generated using the IIS Web Server Certificate Wizard. After this request is generated, another self-signed certificate may be created using a third party tool, or this request can be forwarded to a certificate issuing authority. Do NOT remove the expired certificate until you have installed a new one because this will prevent any logon attempts.

Further Content Server Setup

For more information about any of the tasks below, see the online help or the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com.

Changing the API password

Cisco recommends that you change the API password from the default.

Step 1 Log in with the local administrator account that you set.

Step 2 Go to the **Management** tab. Then go to **Configuration > Site settings**.

Step 3 In the API section, change the Password and Password confirm fields.

Step 4 Click **Save**.

Setting up your authentication method

The default authentication option in the **Management** tab, **Configuration > Site settings** is Local. Cisco recommends that you change to using LDAP/Active Directory or Domain mode. See the online help for more information about when to use each mode.

Adding groups and users

Set up groups and users and their roles according to whether they are viewers, creators or site managers. The method for this depends on the Authentication mode that you have set.

Adding guest user access (if required)

Recording access can be restricted to authenticated users—that is, those who have logged in. If you want to allow unauthenticated users to view conferences, set guest access in the User properties section of **Site settings**. Users who have not logged in will then be able to view conferences that have **Allow access to all users** selected in the conference permissions. RSS feeds are only available if guest access is enabled.

Configuring media server configurations

If you want to use an external streaming server or set up multicast streaming, configure a Media server configuration for live streaming, on demand streaming or both. In the **Management** tab, go to **Recording Setup > Media servers**.

If you want to automatically upload media to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer, or iTunes U, create a Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U Media server configuration.

Selecting the default media server configurations

Make the media server configurations that you created the system defaults in **Site settings**. They will be displayed as the defaults when you create a Template or when editing a recording's outputs in the Manage outputs page.

Reviewing and configuring templates

The unit is delivered with a number of default templates that you can edit, or you can create new ones using the Media server configurations that you configured, as needed. In the **Management** tab, go **Recording setup > Templates**.

Configuration categories

Recordings can be assigned a display category to help users find them. For example, the marketing department can have a category for use with all marketing recordings. In the **Management** tab, go to **Recording setup > Categories**.

Configuring recording aliases

The unit is delivered with a number of default Recording aliases. Each Recording alias has an H.323 ID, E.164 alias and/or SIP URI that can be dialed to record a call/conference. In the **Management** tab, go to **Recording setup > Recording aliases**.

Selecting the recording alias system default

When the system H.323 ID, E.164 alias, SIP URI or unit's IP address is called, the Default Recording alias is used. This is set in the System defaults section of **Site settings**.

Configuring TMS to use the Content Server

The Cisco TelePresence Management Suite (TMS) can be used to record scheduled one-off or recurrent conferences. See the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com for more information. Also, see the documentation for the TMS.

Additional Considerations

Backing up

Cisco recommends that you back up the unit regularly and also before you upgrade it. For more information on backup, see the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com.

Using a Networked Attached Storage device (NAS)

The default location for media files is drive E:. You can change this to store files on a Network Attached Storage device (NAS), so that the recording capacity is not limited by the disk space on the unit. For more information about NAS, see the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com.

Clustering Content Servers

Up to ten Content Servers can be clustered to increase the total call capacity and improve redundancy and resilience. For more information about the main features, system requirements, setup and management of a Content Server cluster, see the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com.

Troubleshooting and Technical Support Information

Using the server logs to help solve a problem

You can use the server logs to produce debugging information to assist customer support in solving an issue if one arises. From the **Management** tab, go to **Diagnostics > Server logs** to access the Content Server logs.

Getting more help

If you experience any problems when configuring or using the Content Server, consult the online help (available within the UI of your unit) for an explanation of how its individual features and settings work. Also, see the *Cisco TelePresence Content Server Administration and User Guide* for your release on Cisco.com.

When contacting Cisco for support, make sure that you have the following information ready:

- The serial number and product model number of the unit
- The software build number, which can be found on the product user interface
- Your contact email address or telephone number
- A full description of the problem

Technical Specifications

Power requirements

Table 1 Content Server Ratings

Rating	Value
Normal voltage	115V to 230V 50/60 Hz
Current rating	9A Maximum
Supply voltage range	100 to 240V 50/60 Hz

Over-current protection

Ensure that the supply to this unit is protected by a branch circuit protector rated by a maximum of 20A.

Caution Over-current devices must meet applicable national and local electrical safety codes and be approved for the intended application.

Operating environment

The unit must only be used within the following environmental conditions:

Table 2 Content Server Ratings

Environment	Temperature	Humidity
Operating environment	0°C to 35°C	10% to 95% (non-condensing)
Non-operating environment	-10°C to 60°C	10% to 95% (non-condensing)
Optimum operating environment	21°C to 23°C	45% to 50% (non condensing)

Anti-static precautions

When servicing or removing components or connection, first attach an anti-static wrist strap to an appropriate earth point.

Disclaimers and notices

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.

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.

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