Cisco TelePresence Content Server Release 7.0 Quick Start Guide

November 2015

This document contains information about installing and configuring the Cisco TelePresence Content Server Release 7.0. See these sections:

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

Product Overview

The Cisco TelePresence Content Server, allows you to share knowledge and enhance communication by recording video conferences. You can access live and on-demand presentations anywhere, anytime. In addition, you can distribute live or recorded content to any computer, or download to your favorite portable media device.

This release introduces the fourth-generation Content Server hardware that runs Cisco Content Server Release 7.0 software. The fourth-generation Content Server is based on the Cisco UCS C220 M4 server. (For more information, see the *Cisco UCS C220 Server Installation and Service Guide* on Cisco.com.)

Figure 1 and Figure 2 show the Content Server front and rear panels, and Table 1 describes the server features.

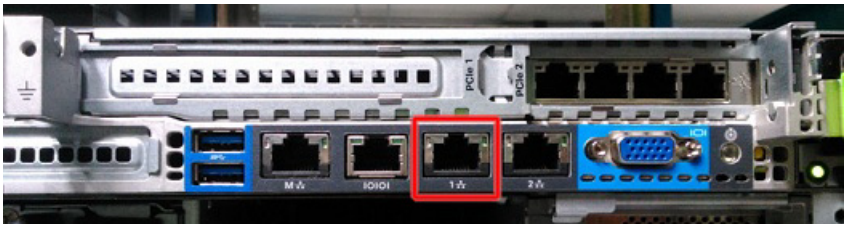
Figure 1 Content Server Front Panel

1	Power button/Power status LED	**6**	Power supply status LED
2	Identification button/LED	**7**	Network link activity LED
3	System status LED	**8**	Asset tag (serial number)
4	Fan status LED	**9**	KVM[1] connector—**Use this port for initial configuration**
5	Temperature status LED	**10**	Hard drives (two), hot-swappable (2.5-inch drives installed in slots 1 and 2; slots 3 to 8 are empty)

1. KVM = keyboard, video, and mouse

Figure 2 Content Server Rear Panel: USB Port

Figure 3 Content Server Rear Panel: Lom Port



1	Power supplies (two)	**6**	1-Gb Ethernet dedicated management port (also see Figure 4)
2	Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane)	**7**	Dual 1-Gb Ethernet ports: LAN1 (Arrow 7, left pointer)—**Use this port to connect the Content Server to the network** (also see Figure 4) LAN2 (Arrow 7, right pointer)—**Not used**
3	Standard-profile PCIe slot on riser (full-height, half-length, x16 lane)	**8**	USB ports (two)
4	VGA video connector	**9**	Identification button/LED
5	Serial port (RJ-45 connector)—**Not used**		–

Table 1 Content Server Features

Chassis	One rack-unit (1RU) chassis. 1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)
Processors	Two Intel Xeon E5-2665 processors.
Memory	Four 8-Gb DDR3[1] low-voltage DIMMs provide a total of 32 GB of memory.
Baseboard management	Integrated Emulex Pilot-3 baseboard management controller (BMC), running Cisco Integrated Management Controller (CIMC) firmware. IPMI 2.0 compliant for management and control. One 10/100/1000 Ethernet out-of-band management interface. CLI and web GUI management tool for automated, lights-out management. Depending on your CIMC settings, the CIMC can be accessed through the 1-Gb Ethernet dedicated management port or the dual 1-Gb Ethernet LOM ports.

Table 1 Content Server Features (continued)

Network and management I/O	The appliance provides these rear-panel connectors: One 1-Gb Ethernet dedicated management port. Two 1-Gb Base-T Ethernet ports. One RS-232 serial port (RJ-45 connector). One 15-pin VGA connector. Two USB 2.0 connectors. One front-panel KVM connector used with the included KVM cable that provides two USB, one VGA, and one serial connector.
Front-panel locator LED	One indicator light to help direct administrators to specific appliances in a data center environment.
Power	Up to two power supplies, 650 W each. Redundant as 1+1. (Hot-pluggable when in a redundant configuration.)
Cooling	Five hot-pluggable fan modules for front-to-rear cooling.
PCIe I/O	Two Generation 3 PCIe[2] expansion slots on risers, occupied by a RAID[3] card (LSI MegaRAID SAS9266-8i with SuperCap power module RAID backup unit, configured for RAID 5) and a NIC[4] card (Broadcom 5709 quad port 1-Gb Ethernet). **Note** The Content Server does not support a dual NIC configuration.
Storage	Drives are installed into front-panel drive bays that provide hot-pluggable access. Small Form Factor—The appliance can hold up to eight 2.5 in x .55 in (63.5 mm x 14mm) SAS[5] or SATA[6] hard drives or solid state drives. The appliance ships with two drives installed. Hard disk option: 2.5-inch, 600 GB SAS hard drive that operates at 10,000 RPM.
Disk Management (RAID)	LSI MegaRAID 9266-8i (RAID 1).
RAID Backup	There is an LSI battery backup unit for the LSI MegaRAID card.
Video	Resolution up to 1600 x1200, 16 bpp at 60 Hz. Up to 256 MB of video memory.

1. DDR3 = double data rate, type 3
2. PCIe = peripheral component interconnect express
3. RAID = redundant array of independent disks
4. NIC = network interface card
5. SAS = serial attached SCSI
6. SATA = serial advanced technology attachment

Technical Specifications

Environmental specifications and regulatory standards compliance for the Content Server are in the product data sheet at this URL:

http://www.cisco.com/en/US/products/ps11347/products_data_sheets_list.html

Hardware Supported

Fourth Generation (M4 hardware)

- **UCS C220 M4**
- **Intel(R) Xeon(R) CPU E5-2680 v3 @2.50GHz 24 cores**
- **64 GB RAM**

Note This hardware specification is for TCS 7.0 Appliance on M4 hardware. TCS 7.0 Appliance is not supported on third generation hardware.

TCS 7.0 VM is supported on third-generation, fourth-generation and third party hardware.

Hardware and Software Limitations

These are the software and hardware limitations:

- For TCS 7.0, there is no on-box streaming server as Windows Server 2012 doesn't support Windows Media Streaming server.For live streaming, TCS needs to be configured with external streaming server.
- TCS 7.0 software cannot be installed on first, second or third generation Content Server hardware. If you attempt to run the 7.0 installer it will fail.
- For TCS 7.0, fourth-generation Content Servers in a cluster must all be the same hardware version. You cannot mix older (first, second or third generation) servers in a cluster with fourth-generation Content Servers.
- The USB media kit is used only for a fourth-generation Content Server software reimage. You cannot use the USB drive to upgrade the software on first, second or third generation server hardware.

Installing the Content Server

Review these sections for installation information:

- Site Requirements and Safety Information, page 5
- Shipping Carton Contents, page 6
- Rack Mounting, page 6

Site Requirements and Safety Information

Select and prepare an installation site that meets the requirements that are described in the *Cisco UCS C220 Server Installation and Service Guide* on Cisco.com.

For specific compliance and safety information, see the *Regulatory Compliance and Safety Information for the Cisco UCS C-Series Servers* on Cisco.com.

Shipping Carton Contents

When you receive the server, verify the contents of the shipping carton to ensure that you have all items necessary for installation. Save the packing material in case you need to repack the server. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

The contents of the shipping carton include these items:

- Content Server
- USB media kit (used only for a software reimage)
- Rail kit
- Serial cable
- Ethernet cable
- Cable kit power
- Accessory kit
- Printed card with URLs for product documentation and RoHS information for China

Rack Mounting

For Content Server rack mounting procedures, see the "Installing the Server" chapter of the *Cisco UCS C220 Server Installation and Service Guide*.

Completing the Initial Configuration

You need these items to complete the Content Server initial configuration:

- USB keyboard, mouse, and VGA monitor.
- Windows Server 2012 product activation key—see the product activation key label on the Content Server chassis.
- IP address, subnet mask, and gateway for:
  - Content Server.
  - Cisco Integrated Management Controller (CIMC) Configuration Utility.

These are the initial configuration tasks:

Task 1: Connect and power on the Content Server and configure CIMC

Follow these steps:

Step 1 Attach a supplied power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet. Wait for approximately two minutes to let the server boot in standby power mode during the first bootup. You can verify power status by looking at the Power Status LED (Figure 1):

- Off—There is no AC power present in the server
- Amber—The server is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.
- Green—The server is in main power mode. Power is supplied to all server components.

Step 2 Use the supplied KVM cable to connect a USB keyboard, mouse, and a VGA monitor to the KVM connector on the Content Server front panel (Figure 1).

Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you do so, the first VGA connector is disabled.

Step 3 Press the **Power** button to boot the server. During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility.

Step 4 Enter these settings in the CIMC Configuration Utility:

a. NIC Properties NIC mode: **Dedicated**

b. NIC Redundancy: **None**

c. IPv4 (Basic): *CIMP ip-address*, *subnet-mask*, *gateway ip-address*

Note The Content Server does not support dual NIC configuration.

Step 5 Press **F10** to save your settings and restart the Content Server.

Task 2: Set the local administrator password

Follow these steps:

Step 1 Log in to the Content Server Windows Server Manager by using the default password, **Cisco123**.

Step 2 Go to **Start > Control Panel > User Accounts > Change your Windows password > Change your password**.

Step 3 In the Change your password window, enter the current password (**Cisco123**), the new password, and confirm the new password.

Step 4 Click **Change password**.

Step 5 Click **OK**.

Task 3: Enter the Windows Server 2012 activation key

The Windows Server 2012 Physical Key is on the printed label on the Content Server top near the front. You should have an Internet connection to access the Windows Server 2012 online activation service. Follow these steps:

Step 1 Connect the Content Server to your network. Use an Ethernet cable to connect from your LAN to the LAN1 network port, marked with blue in Figure 4, on the rear panel. Use the connector marked with red for your CIMC management connection.

Figure 4 Network Connections

Step 2 Log in to the Content Server Windows Server Manager by using the password that you set in Task 2: Set the local administrator password.

Step 3 Go to **Start > Administrative Tools > Server Manager**. In the Server Manager window, click **Activate Windows**. Enter the **Physical Key** (located on the Content Server chassis label). Click **Next**.

If the Content Server is not connected to the Internet, you can follow the on-screen instructions to activate Windows Server 2012 by using your phone.

Step 4 When the product key is verified and activated, click **Close**.

Task 4: Configure a static IP address

By default, the server automatically acquires an IP address assigned by a DHCP server in your network. We recommend that you change the IP address from DHCP to static. Follow these steps:

Step 1 Go to **Start > Control Panel > Network and Internet**.

Step 2 From the Network and Sharing Center, click **View network status and tasks**.

Step 3 In the Connect or disconnect section, click **Local Connection**.

Step 4 Choose **IPv4** from the list. In the IPv4 Properties window, click the **Use the following IP address** radio button. Enter the Content Server *IPv4 address*, *subnet-mask*, and *default-gateway*. Click **OK**.

Task 5: Set the date and time

You should set the Content Server date and time to ensure that the conference creation date and time displays correctly in the Conference lists. Follow these steps:

Step 1 Log in to the Content Server by using the Administrator password that you set in Task 2: Set the local administrator password.

Step 2 In the Server Manager window, click the time and date box in the lower right corner to open the settings window. Or, go to **Start > Control Panel > Clock, Language, and Region > Set the time and date**.

Step 3 Click **Change date and time settings**.

Step 4 Update the date, time, and time zone. Click **OK**.

Task 6: Enable Remote Desktop Connection

Beginning with Cisco Content Server Release 7.0, all Windows Server 2012 administration and configuration is accomplished by using Windows Remote Desktop Connection to access the server administration interface. Follow these steps to enable remote desktop on the Content Server:

Step 1 Log in to the Content Server by using the Administrator password that you set in Task 2: Set the local administrator password.

Step 2 Go to **Start > Control Panel > System Security > System > Remote Settings**.

Step 3 From the System Properties window Remote tab, select and click a radio button to enable Remote Desktop on the Content Server. Click **OK**.

Step 4 Restart the Content Server. Go to **Start > Log Off > Restart**.

You can now disconnect the KVM cable from the Content Server and continue configuring the server by accessing the Content Server user interface and by using Windows Remote Desktop Connection.

Task 7: Configure SQL Settings

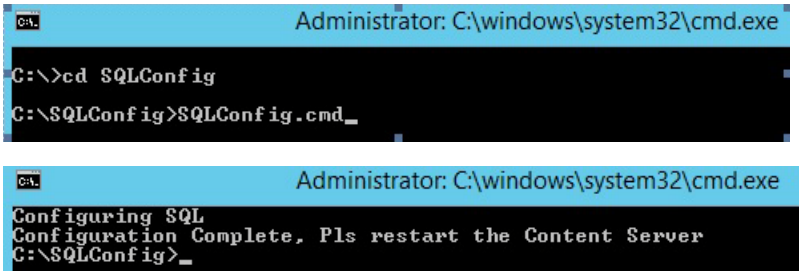
Step 1 Remote log in to the Content Server by using the Administrator password.

Step 2 Launch the **Command Prompt.**

Step 3 On the command prompt, type "**cd c:\SQLConfig"** to change the current directory to c:\SQLConfig

Step 4 Type SQLConfig.cmd to run the script. See the image, given below:

Figure 5 SQL Configuration



Step 5 Restart the Content Server. Go to **Start > Log Off > Restart**.

Task 8: Install a security certificate

The Content Server is shipped with a self-signed certificate, which is valid for ten years. Because self-signed certificates are not from a trusted Certificate Authority, when users log in, most browsers will display a message that the identity of the site could not be verified.

You can add the server to the Trusted sites list in Internet Explorer, or add an exception in Firefox to avoid error messages at log in. However, we recommend 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, which eliminates the need to add the server to the list of Trusted sites. The certificate should be generated against the Windows machine name or the DNS entry associated with the server IP address.

Follow these steps to install a purchased security certificate on the server default website:

Step 1 On your computer, go to **Start > All Programs > Accessories > Remote Desktop Connection**.

Step 2 In the Remote Desktop Connection dialog box, enter the IP address that you configured in Task 4: Configure a static IP address.

Step 3 Click **Connect**. Log in with the administrator password that you set in Task 2: Set the local administrator password. The Server Manager user interface appears.

Step 4 Go to **Start > Internet Information Services (IIS) Manager**.

Step 5 Under Connections, click the Content Server Windows 2012 server “machine_name (local computer)”.

Step 6 Click **Server certificates** in the machine_name Home window.

Step 7 Under Actions, click **Import** to import a new certificate.

Step 8 Follow the instructions in the Web Server Certificate Wizard to replace the current certificate with the purchased certificate.

For more information, see the Internet Information Services help.

You can also install the certificate for the Windows Media Administration website to avoid security warnings when administrators log in to that site. When you have installed the certificate on the website, the purchased certificate is then used instead of the self-signed certificate.

If the security certificate expires, (regardless of whether the server uses the purchased security certificate or the original self-signed certificate), browsers will display additional warnings. You can generate a new certificate request by using the IIS Web Server Certificate Wizard. After this request another self-signed certificate may be created by 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 certificate because this will prevent any log in attempts.

Task 9: Configure the H.323/SIP registration settings

Step 1 On your computer, open a browser and enter the Content Server IP address the you configured in Task 4: Configure a static IP address.

Step 2 Log in to the Content Server web interface by using the password that you configured in Task 2: Set the local administrator password.

Step 3 In the Content Server web interface, go to **Management > Configuration > Site settings**.

Step 4 Enter the **System name** that is used by the Cisco TelePresence Management Suite to identify the Content Server.

(Optional) Select the **Show in browser title** check box to display the System name in the browser title bar when using the web interface.

Step 5 If you are using an H.323 gatekeeper, in the Gatekeeper settings section:

a. Select **Gatekeeper enabled** and enter the Gatekeeper 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 the H.323 and E.164 gateway prefixes as needed.

Step 6 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 IP address or DNS name.

Step 7 Click **Save**. The **Registration status** is updated. (You might need to refresh the page.)

Step 8 Go to **Recording setup > Recording aliases**.

Step 9 Click **Edit** for the default Recording aliases. For each alias 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 *Live<serial_number>* and the default on-demand recording alias is *OnDemand<serial_number>*.

See the online help for an explanation of recording aliases. SIP URIs must be unique in their network and valid for their SIP registrar.

Task 10: Make a test recording

You can make a test recording by dialing out. The recording is stored and then transcoded. When the process is complete, the recording appears in the **View Recordings** tab.

Follow these steps:

Step 1 In the Content Server web interface, go to **Management > Recordings > Create recording**.

Step 2 Select a recording alias.

Step 3 For **Dial number**, enter the endpoint address that you want to call. 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 from the endpoint or by clicking on the thumbnail followed by **Edit recording** and **End call**.

You can make a test call by dialing in. The recording is stored and then transcoded. When the process is complete, the recording appears in the **View Recordings** tab.

Follow these steps:

Step 1 In the Content Server web interface, go to **Management > 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 addresses that you noted.

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 from the endpoint or by clicking on the thumbnail followed by **Edit recording** and **End call**.

Additional 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 this release on Cisco.com.

Changing the API password

We recommend that you change the default API password. For information about the default API settings, see the *Cisco TelePresence Content Server API Guide* on Cisco.com.

1. In the Content Server web interface, log in with the administrator password.
2. Go to the **Management > Configuration > Site settings**.
3. In the API section, enter a new password in the **Password** and **Password confirm** fields.
4. Click **Save**.

Setting up your authentication method

The default authentication option in the **Management** tab, **Configuration > Site settings** is Local. We recommend that you change the default authentication method to LDAP/Active Directory mode 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. In the **Management** tab go to **Configuration > Groups and users**.

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, you can enable guest access in the User properties section of **Site settings**. Users that are not logged in are 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 enable multicast streaming you should configure a Media server 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, you should create a media server for each of those applications.

Selecting the default media server configurations

You can make the media server configurations that you created the system defaults in **Site settings**. The server configurations will display as the defaults when you create a Template or when editing a recording output in the Manage outputs page.

Reviewing and configuring templates

The server is preconfigured with a number of default templates that you can edit, or you can create new templates by using the Media server configurations. In the **Management** tab, go **Recording setup > Templates**.

Configuration categories

You can assign Recordings 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 server is preconfigured 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 or 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 server IP address is called, the Default Recording alias is used. You can set the Default Recording alias 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* and all TMS documentation for this release on Cisco.com.

Backing up

We recommend that you back up the server regularly and also before system upgrades. For more information on backup, see the *Cisco TelePresence Content Server Administration and User Guide* for this release on Cisco.com.

Using a Networked Attached Storage device (NAS)

The default location for media files is drive E:. You can change this location to store files on a Network Attached Storage (NAS) device. Using an NAS device ensures that the recording capacity is not limited by the disk space on the server. For more information about NAS, see the *Cisco TelePresence Content Server Administration and User Guide* for this 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 system requirements, set up and management of a Content Server cluster, see the *Cisco TelePresence Content Server Administration and User Guide* for this release on Cisco.com.

Troubleshooting and Technical Support

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 issues. 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 for an explanation of how individual features and settings work. Also, see the *Cisco TelePresence Content Server Administration and User Guide* for this release on Cisco.com.

When contacting Cisco for support, make sure that you have this information:

- The serial number and product model number of the server
- 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

Related Documentation

- Cisco TelePresence Content Server Documentation

  http://www.cisco.com/en/US/products/ps11347/tsd_products_support_series_home.html
- Cisco UCS C220 Documentation

  http://www.cisco.com/en/US/products/ps10493/tsd_products_support_series_home.html
- Cisco Capture Transform Share Documentation

  http://www.cisco.com/en/US/products/ps12130/products_installation_and_configuration_guides_list.html

Information About Accessibility and Cisco Products

For information about the accessibility of this product, contact the Cisco accessibility team at accessibility@cisco.com.

Providing Documentation Feedback

To provide feedback on this document, or to report an error or omission, you can use the online, Embedded Feedback form that appears on the left side of the screen. You can also send feedback to mxe-doc@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.
