CHAPTER 7

Maintaining the Content Server

This chapter includes the following Content Server maintenance procedures:

Note These procedures contain steps that you must perform on devices that are external to the Content Server. If you need more information about devices that are not Cisco products, consult the documentation for those devices. If you need information about Windows Servers that is not provided here, consult the Microsoft documentation.

Backing Up the Content Server

To ensure that you do not lose data, you should back up the Content Server regularly. You should also back up the Content Server before you upgrade or install a security update. Follow the procedures as described here to prevent issues with future upgrades:

Note If your media files are located on a Network Attached Storage device (NAS) or on an external media server, this backup procedure does not back up those files. Ensure that you back up the media on external devices at the same time as the Content Server. If you restore from backup, you must restore the media backup taken at the same time as your Content Server backup; otherwise, you might not be able to play some recordings.

Before Backing Up

You can back up Content Server files to a USB drive or to a network drive.

When performing a manual or scheduled backup, if you use a USB hard drive, you must connect the drive to a USB port on the Content Server. Then log into the Content Server using Windows Remote Desktop Connection to make sure that the USB hard drive appears under My Computer.

Also, make sure that you have enough room on the USB hard drive or network drive for all the files that you want to back up. Check the size of the data for backup by logging in to the Content Server using Windows Remote Desktop Connection. Open My Computer to calculate the amount of C: drive and E: drive space is used.

Performing a Manual Backup

To perform a manual, on-demand backup, follow these steps:

Step 1 Open the backup and restore wizard in one of these ways:

- Log in to Content Server web interface in Internet Explorer. From the **Management** tab, go to **Configuration > Windows server**. In the dialog box that appears, log in with the local administrator password. Then go to **Maintenance > Backup**.

Note Internet Explorer security settings might prevent the necessary Active X scripts from running. With certain browser security settings, you will not be able to access the web interface for Windows Server administration or some of its tools. To overcome this issue, add the URL of the Content Server to the trusted sites in your browser. In Internet Explorer, go to **Tools > Internet Options**. Click the **Security** tab. Click **Trusted sites** and then **Sites**. Add the Content Server URL.

- Log in to the Content Server through Windows Remote Desktop. Go to **Start > All Programs > Accessories > System Tools > Backup**.

Step 2 In the Welcome to the Backup or Restore Wizard dialog box, click **Next**.

Step 3 Click **Back up files and settings**. Click **Next**.

Step 4 In the What to Back Up dialog, click **Let me choose what to back up**. Click **Next**.

Step 5 In the Items to Back Up dialog, expand **My Computer**. Check **Local Disk (C:)**, **Local Disk (E:)**, and **System State**. Click **Next**.

Step 6 In the Backup Type, Destination, and Name dialog, browse to the USB drive or network location that you want to back up to (see the "Before Backing Up" section on page 7-2 for more information). Type a name for the backup. Click **Next**.

Step 7 In the Completing the Backup or Restore Wizard dialog, verify the summary of your choices. Click **Finish**. The backup process takes approximately 10 minutes per 5 GB of data. Progress is displayed, and a detailed report is provided when the backup is complete.

Configuring a Scheduled Backup

To set up a scheduled backup, follow these steps:

Step 1 Open the backup and restore wizard in one of these ways:

- Log in to Content Server web interface in Internet Explorer. From the **Management** tab, go to **Configuration > Windows server**. In the dialog box that appears, log in with the local administrator password. Then go to **Maintenance > Backup**. In the Welcome to the Backup or Restore Wizard dialog box, click **Advanced Mode**.

Note Internet Explorer security settings might prevent the necessary Active X scripts from running. With certain browser security settings, you will not be able to access the web interface for Windows Server administration or some of its tools. To overcome this issue, add the URL of the Content Server to the trusted sites in your browser. In Internet Explorer, go to **Tools > Internet Options**. Click the **Security** tab. Click **Trusted sites** and then **Sites**. Add the Content Server URL.

- Log in to the Content Server through Windows Remote Desktop. Go to **Start > All Programs > Accessories > System Tools > Backup**. In the Welcome dialog box, click **Advanced Mode**.

Step 2 Click the **Schedule Job** tab. Then click **Add Job**. In the next dialog box, click **Next**.

Step 3 In the What to Back Up dialog, click **Let me choose what to back up**. Click **Next**.

Step 4 In the Items to Back Up dialog, expand **My Computer**. Check **Local Disk (C:)**, **Local Disk (E:)**, and **System State**. Click **Next**.

Step 5 In the Backup Type, Destination, and Name dialog, browse to the USB drive or network location that you want to back up to (see the "Before Backing Up" section on page 7-2 for more information). Type a name for the backup. Click **Next**.

Step 6 In the Type of Backup dialog, choose the type of backup from the drop-down list. Then click **Next**.

Step 7 In the How to Back Up dialog, check **Verify data after backup**. Click **Next**.

Step 8 In the Backup Options dialog, click **Append this backup to the existing backups**. Click **Next**.

Step 9 In the When to Backup dialog, click **Later**. Enter a name for the backup. Then click **Set Schedule**. Enter your desired schedule. Click **OK**.

Step 10 Enter an account that has administrative privileges on the Content Server (this could be the local administrator account, or if the Content Server is on a domain, a domain administrator account). Enter the administrator account password and confirm. Click **OK**.

Step 11 In the Completing the Backup or Restore Wizard dialog, verify the summary of your choices. Click **Finish**. The backup process is now scheduled to run according to the schedule you set.

Restoring Files

Note If your media files are located on a Network Attached Storage device (NAS) or on an external media server, this procedure does not restore those files. You must have a media backup that was taken at the same time as the Content Server backup, and you must also restore this media backup; otherwise, you might not be able to play some recordings.

Before Restoring

Make sure that you are using a backup that was taken from the same Content Server that you are restoring. If you want to restore to a different Content Server, contact your Cisco reseller.

Restoring from a Backup

To restore the Content Server from a backup, follow these steps:

Step 1 End any recording calls that are in progress.

Step 2 Log in to the Content Server using Windows Remote Desktop Connection.

Step 3 Uninstall the Content Server software:

a. Go to **Start > Control Panel > Add or Remove Programs**.

b. Click **Cisco TelePresence Content Server**. Click **Change**.

c. Select the **Remove** option. Click **Next**.

d. Click **Microsoft SQL Server 2005**. Click **Remove**.

e. In Component selection, select **TCS database engine**. Click **Next**.

f. Select **Microsoft SQL Server VSSWriter**. Click **Remove**.

g. Select **Microsoft SQL Server Setup Support Files**. Click **Remove**.

Step 4 Browse to C:\Windows\Security and look for files called edb*.log. (There is edb.log and at least one more file often called edbtmp.log or edb0000*.log.) Do not delete edb.log, but delete the other files. Not removing these files could result in issues with future upgrades after a restore.

Step 5 Go to **Start > Programs > Accessories > System Tools > Backup** to start the Backup and Restore Wizard.

Step 6 Click **Restore files and settings**. Click **Next**.

Step 7 In the What to Restore dialog, check **Local Disk (C:)**, **Local Disk (E:)** and **System State**. Click **Next**.

Step 8 In the Completing the Backup or Restore Wizard dialog, click **Advanced**.

Step 9 From Where to Restore, leave **Original location** (the default setting). Click **Next** and **OK** to acknowledge the warning.

Step 10 In the How to Restore, select **Replace existing files**. Click **Next**.

Step 11 Leave the default options in Advanced Restore Options. Click **Next**.

Step 12 Verify your choices. Click **Finish**. The restoring process starts, and progress is displayed. When the process is complete, you can display a detailed report by clicking **Report**.

Step 13 Restart the Content Server after the restoring process is successfully completed.

Upgrading the Content Server

We strongly recommend that you check regularly for upgrades to the Content Server software on Cisco.com. To upgrade the Content Server, read the release notes for the software that you are upgrading to. Then follow the upgrade procedure as described here:

- Downloading Content Server Software Releases, page 7-5
- Upgrading the Content Server Software, page 7-5

Note You need a release key to upgrade to another major release train (for example, from release 4.x to 5.x). However, if you upgrade to another release in the same release train, you do not need a release key (for example, from release 5.0 to 5.1). Release keys are available from Cisco.com, and you need your Content Server serial number to get the correct key.

Downloading Content Server Software Releases

Step 1 Log in to the Content Server web interface in the site manager role. From the **Management** tab, go to **Diagnostics > Server overview**.

Step 2 Note the software version that is currently installed.

Step 3 Go to the software download page for the Content Server on Cisco.com. Check for the more recent releases of software.

Step 4 Download the desired installer to a directory on your computer.

Upgrading the Content Server Software

Step 1 Verify that there are no active recording calls or active transcoding sessions.

Step 2 Log in to the Content Server using Windows Remote Desktop Connection.

Step 3 Back up your Content Server (see the Backing Up the Content Server, page 7-1 for more information). Turn off any anti-virus programs.

Step 4 Transfer the installer that you downloaded in Step 4 above to the Content Server. Do not run the installer from a mapped or network drive.

Step 5 If you want, verify the MD5 hash (checksum) of the file.

The unique MD5 file that is provided with the installer can be used to verify that a file has not become corrupted as a result of a faulty file transfer, a disk error, or tampering. With the provided MD5, any MD5 program can be used for verifying the installer.

Step 6 Double-click the executable to run it. Follow the on-screen instructions.

Step 7 If prompted, restart the Content Server. Otherwise, terminate your Windows Remote Desktop Connection session by logging off. Do not choose Shutdown because doing so shuts down the Content Server.

Shutting Down and Restarting the Content Server

You can shut down and restart the Content Engine service by restarting the Content Server. In the web interface for Windows Server administration, go to **Maintenance > Shutdown > Restart**. Before a shutdown and restart, you must first assign shutdown permission to the domain user on the Content Server that you want to shut down and restart. See the Resolved Caveats section in the *Release Notes for Cisco TelePresence Content Server Release 5.3.x* on Cisco.com for more information (CSCuf16163).

You can also use a serial cable to connect a PC to the Content Server serial port to shut down and restart the server. Cisco recommends that you end all calls on the Content Server before you shut down.

Note If calls are in progress when the shutdown occurs, the recorded calls appear in the recordings list but might be unusable. They can be deleted in the normal way.

To restart the Content Server, do the following:

Step 1 Connect the supplied serial cable from the serial port on the back of the Content Server to the serial port on a PC.

Step 2 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 3 Open a new connection. Enter a name for the connection.

Step 4 Configure the connection to use the PC serial port as follows:

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

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

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

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

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

Step 5 Click **OK**.

Step 6 Press **Enter** to display the main menu.

Step 7 Make sure that the Content Server is not recording or transcoding. Then press **Esc** to display Content Server version, IP address, and recording/transcoding status.

Step 8 Use the up or down arrows to navigate to **Commands** and press **Enter** to select.

Step 9 Use the up or down arrows to navigate to **Restart** and press **Enter** to select.

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

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

To shut down the Content Server using a PC connected to the serial port, do the following:

Step 1 1. Follow steps 1-8 in the previous section.

Step 2 2. Use the up or down arrows to navigate to **Shutdown** and press **Enter**.

Step 3 3. Close the terminal emulator session and disconnect the serial cable.

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

Table 7-1 Terminal Emulator Session Keys

Key	Description
Enter key	Enters Edit mode, confirms an entry.
Esc key	Returns to the previous menu, exits Edit mode without saving.
Up and down arrow keys	Moves between menu items, moves between values in a numerical address and modifies numerical values.

Restoring the Content Server Defaults

You can restore the Content Server to its default settings, partially or fully, usinga PC connected to the Content Server serial port:

- A partial restore (using **ConfigRestore**) deletes all user-created recording aliases, media server configurations, call configurations, and templates. **ConfigRestore** restores the default configuration for the current software release, but does not affect the recordings stored on the server.
- A full restore (using **FullRestore**) deletes all recordings, media files and logs, in addition to deleting all user-created recording aliases, media server configurations, call configurations and templates. **FullRestore** restores the default configuration for the current release. If the data location has been changed to an external storage location (NAS), it also changes the default storage location back to the Content Server. Media files on the NAS are not deleted.

Caution Restoring to defaults (either a partial or full restore) must not be interrupted. Logs of the restore are available in E:\logs\SetupUtility directory.

Important notes:

- Restoring to defaults cleans up the Content Server's database and/or media. It does not revert the Content Server back to the state it was in when delivered (that is, the restore does not affect the operating system in any way).
- A partial restore (**ConfigRestore**) is not available for Content Servers in a cluster.
- A full restore (using **FullRestore**) run on a Content Server which has been clustered will revert that Content Server to a standalone Content Server with the default configuration files for the current software release, and no media. However, the cluster database will still report that this Content Server is part of a cluster: Cisco recommends removing a clustered Content Server from the cluster by running the TCS Wizard before restoring it to its default settings.

To restore default settings, do the following:

Step 1 Connect the supplied serial cable from the serial port on the back of the Content Server to the serial port on a PC.

Step 2 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 3 Open a new connection. Enter a name for the connection.

Step 4 Configure the connection to use the PC 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 5 Click **OK**.

Step 6 Press **Enter** to display the main menu.

Step 7 Ensure that the Content Server is not recording or transcoding. Then press **Esc** to display Content Server version, IP address, and recording/transcoding status.

Step 8 Use the up or down arrows to navigate to **Commands** and press **Enter** to select.

Step 9 Use the up or down arrows to navigate to either **FullRestore** or **ConfigRestore** (see "Important Notes" above for more information). Press **Enter**.

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

Caution Do not leave a terminal emulator session open after it is no longer in use. An open session may cause issues for system operation and restart.

For terminal emulator session keys, see Table 7-1.

Securing the Content Server

Antivirus Protection

Antivirus protection may be used on the Content Server.

If you use antivirus software on the Content Server, we recommend that you do not scan the **E:** volume or the **C:\program files\Tandberg** directory where the data files are located.

Microsoft Security Patches

Microsoft security patches may be applied to the Content Server.

We recommend that you download and install the patches during normal maintenance windows. You can manually install recommended patches from the Microsoft web site or use Windows Update.

Content Server security bulletins inform you of patches either that we recommend highly or that we do not recommend applying because they have been known to cause instability in the Content Server application. These bulletins will be published if aspects of Microsoft patches are critical to performance or security of the Content Server.

Access the latest Content Server security bulletin at http://www.cisco.com/en/US/products/ps11347/prod_bulletins_list.html.

Joining the Content Server to a Domain

The Content Server can be joined to a Microsoft Active Directory Domain in the same way as any Windows Server 2003 server. Domain group policies may be applied to the Content Server.

The Content Server must be joined to a domain to configure external storage or a cluster of Content Servers.

Do not apply any policy that:

- Changes the Administrator account name. If the Administrator account name is changed, the Serial Port/LCD panel password reset tool will not work.
- Restricts the guest group. This will disable the IIS user account. The IIS user account is necessary to provide the web user interface for the Content Server.

Caution Other group policies might restrict services required for the Content Server to function. We recommended that you test the Content Server after each new group policy is applied before making the Content Server available to users in the production environment.