Release Notes for Cisco Digital Media System 4.1

DMS	Cisco Digital Media System 4.1 (DMS) helps organizations of any size to:

- Create, manage and deliver desktop video content (whether live or on-demand) over an IP network to any general or targeted audience.
- Filter questions (received in real time from audience members at a live event) for display in a Q&A.
- Synchronize presentation slides with video streams.
- Create, manage and deliver digital signage content (including video, audio, text, multimedia, and web pages) over an IP network to any general or targeted audience.
- Communicate with targeted customers, investors, press, and analysts.
- Deliver critical information and training to employees, suppliers, and partners.
- Deliver educational content to students.

This Document	This document contains release note information for the hardware *and* software components of DMS 4.1. In addition, it contains ID numbers, headlines, and descriptions for each known problem, and contains a list of resolved problems. If you have a Cisco.com user account and obtained this document from Cisco.com, you can click any ID number to see the corresponding release note enclosure in the Bug Toolkit. The release note enclosure describes symptoms, conditions, and workarounds. This document contains these sections:

This document might be updated at any time; the most recent revision is always available on Cisco.com.

⚠
Caution   To maintain security in your network, DMS 4.1 component appliances (meaning, your DMM appliances and your Video Portal appliances) use digital certificates to communicate amongst themselves. These certificates use the DNS-routable hostname for an appliance to identify it uniquely. When you use AAI to set up any DMS component appliance and AAI prompts you to enter the fully-qualified domain name (FQDN) for that appliance, you must enter its DNS-routable hostname. **If you mistakenly enter an IP address, your DMS component appliances will be unable to communicate with each other.** In addition, you must use AAI to configure each of your DMS component appliances so that it points correctly to the DNS server for your network, and you must configure that DNS server so that it correctly associates the IP addresses that your DMS component appliances use with the FQDNs that their digital certificates use. DMS component appliances will not work correctly without a DNS server.

⚠
Caution   When you use AAI to set up your DMS 4.1 component appliances, AAI prompts you to enter an instance name for your Video Portal. **You must not use "Cisco" as the instance name**. We reserve and use the Cisco name for other purposes; all deployments will fail if you try to use it as the instance name.

What's New In DMS 4.1

DMS 4.1 includes new components, new features, and changed features.

Digital Signage

- Digital Media Designer (DMD) is a powerful drag-and-drop user interface that you can use to design presentations for digital signage, create presentation templates, and manage playlists.
- Cisco Digital Media Player 4305Gs (DMPs) are the replacement for DMP 4300Gs, providing 2 GB of storage capacity instead of 1 GB.
- DMP firmware enhancements deliver:
    - Improved security for device ports and for centralized management.
    - Upgraded format support for Adobe Shockwave Flash files.
- Enhanced RS-232 support for the commands to remotely configure and control certain display models manufactured by NEC and DMTech.
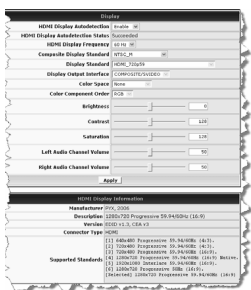
Desktop Video

- Synchronize slides with video streams, whether live or on-demand.
- Receive, display, and create an archive of questions from live event audience members.
- Use Active Directory (requires Windows Server 2003 or Windows 2000 Server) to authenticate administrator and user logins.
- Customize your Video Portal user interface in new, more versatile ways.

Documentation Errata

Online-only documents for DMS on Cisco.com are updated, expanded, and corrected whenever necessary. This section describes errors and omissions in the *printed* user documentation for DMS 4.1 components.

78-18249-02—Quick Start Guide for Cisco Digital Media Player 4305G:

- Section 3 of this quick start guide should mention that DMP 4305G support for DHCP in this release does not extend to the client FQDN extension that Microsoft DHCP servers provide.

- Nomenclature changes occurred in the user interfaces for DMPDM and DMM-DSM after the first 1,000 copies of this quick start guide went to press. As a result, some procedures in the first printing of this guide are not correct on pages 21, 22, 25, and 26. See the corrections in this table:

Page	Nomenclature That Changed	Corrected Nomenclature (in boldface type)
21		Select **Schedules > Immediate Deployment**.
22		In the Settings area, click **DMP Display Attributes**.

Page	Nomenclature That Changed	Corrected Nomenclature (in boldface type)
25	⚠ **Caution** To stop untrusted DMM appliances from being able to seize control of your DMPs, you must configure your network firewall to restrict which devices you will permit to send inbound traffic to your DMP over TCP port 7777. If you do not know how to work with access control lists, see the manufacturer documentation for your firewall. **Step 1** Specify in DMPDM which one DMM appliance to trust. **a.** Select **Settings > DMM**. **b.** In the **Timeout (Seconds)** field, enter the maximum number of seconds that your DMP should wait for a response from the trusted DMM appliance. (This is the appliance that serves DMM-DSM.) **c.** In the **DMM Host** field, enter the routable IP address or DNS-resolvable hostname of the trustworthy DMM appliance. **25**	• Select **Settings > Centralized Management**. • In the **DMM-DSM Server Timeout (in seconds)** field, enter the maximum number of seconds that your DMP should wait for a response from the trusted DMM appliance. (this is the appliance that serves DMM-DSM.) • In the **DMM Appliance IP Address** field, enter the routable IP address or DNS-resolvable hostname of the trustworthy DMM appliance.
26	The DMM Host field might already be populated with the correct IP address for your DMM appliance if you used DMM-DSM to autodiscover your new DMP. **d.** To confirm your selections and to implement them until you change them or until you restart your DMP, click **Apply**. **e.** To make these configuration changes persist even after you restart your DMP, do the following: – Select **Administration > Save Configuration**. – On the Save Configuration page, click **Save**. ✎ **Note** DMM-DSM and your DMP communicate over TCP port 7777 when centralized management is enabled. **Step 2** Throughout your digital signage network, confirm that your centrally managed DMPs all share: • Identical user credentials for their DMP Web Account. • Identical user credentials for their DMP Service Account. To learn how to make these credentials identical, see the "Logging in to DMPDM and Changing its Passwords" section on page 13. **26**	The **DMM Appliance IP Address** field might already be populated with the correct IP address for your DMM appliance if you used DMM-DSM to autodiscover your new DMP.

Video Portal Concurrent Sessions

Table 1 describes the maximum number of concurrent Video Portal user sessions that can start within a 1-minute period. These connection threshold values assume that users will receive all data directly from the Video Portal, rather than receiving essential files from a content delivery network where you prepositioned them.

Table 1   Video Portal Capacity

This Video Portal appliance chassis type:	Supports this many concurrent user sessions:
MCS-7825-H3	500 per minute
MCS-7835-H2	1,000 per minute

Options for Upgrading

To understand the requirements and procedures to upgrade, see *Upgrade Guide to Release 4.1 for Cisco Digital Media System* on Cisco.com.

DMS Component	Upgrade Path
Cisco Digital Media Manager (DMM) appliances	**Note** You must perform this upgrade if you upgrade your Video Portal appliances. The two upgrades are interdependent. You can upgrade from DMM 4.0 to DMM 4.1. After the upgrade is finished, you will have these software components installed: • Appliance Administration Interface 4.1 for DMM appliances. • Cisco Digital Media Manager 4.1, including the: – Administration Module. – Desktop Video Module, which includes its separately-licensed Live Event Module 1.0. – Digital Signage Module, which includes the new Digital Media Designer user interface.

DMS Component	Upgrade Path
Cisco Video Portal appliances	**Note** You must perform this upgrade if you upgrade your DMM appliances. The two upgrades are interdependent. You can upgrade from Video Portal 4.0 to Video Portal 4.1. After the upgrade is finished, you will have these software components installed: • Appliance Administration Interface for Video Portal appliances. • Cisco Video Portal 4.1. • Cisco Video Portal Reports 4.1.

Cisco Digital Media Players	**Note** Unless your DMPs use firmware release 2.43.x, you will not be able to create or deploy any presentations or playlists for digital signage.
	
	Firmware Release 2.43
	
	You can upgrade the firmware on a DMP 4300G from release 2.42.x to release 2.43. After the upgrade is finished, you will have version 1.1 of the Digital Media Player Device Manager software installed. Your DMP 4300 is then identical to a DMP 4305G except that the DMP 4305G has 2 GB of storage space while your DMP 4300G still has only 1 GB.
	
	Firmware Release 2.43.1
	
	Firmware release 2.43.1 (which is suitable for both the DMP 4300G and the DMP 4305G) resolves two known defects, CSCsk25551 and CSCsk44959.
	
	• The fix for CSCsk25551 adds support in Cisco Digital Media Player Device Manager 1.1.1 (DMPDM) for the use of relative file paths in the "Local Storage Playback" field. In previous DMPDM releases, you were required to enter absolute paths for this purpose. Now you can use relative paths and absolute paths interchangeably when you specify the names and locations of files that you have stored on SD cards. For example:
	
	  – Absolute Path:
	    `/tmp/ftproot/usb_1/...`
	
	  – Relative Path:
	    `usb_1/...`
	
	• The fix for CSCsk44959 causes DMPs to support program map table (PMT) packets with sizes greater than 188 bytes. Encoders sometimes produce unusually large PMT packets for a transport stream that should contain data in support of multiple languages.
	
	If you are not already familiar with PMT Packets: To distinguish among, demultiplex, and synchronize the many different types of program data that they might contain, all of the constituent "elementary streams" within a multiplexed MPEG transport stream start with a structured prefix. This prefix is known as the packet ID (PID). The PID, in turn, combines four program-specific information (PSI) tables, one of which is the program map table (PMT). PMTs contain metadata and other important information about the programs in streams.

Client System Requirements

Ensure that Java Runtime Engine (JRE) 1.6.0 or later is installed on your PC. Also confirm that it is configured to use English as its language, and that it is working correctly. The JRE 1.6.0 release is part of Java Version 6.

- To learn exactly which JRE release you are using and to confirm that it is working correctly, go to http://java.com/en/download/help/testvm.xml.

- To understand the Java release naming conventions, which have changed over time, see http://java.sun.com/javase/namechange.html.

- To obtain the required JRE, go to http://javasoft.com, click **Java SE**, then download the latest JRE version.

- Apple maintains and distributes its own implementations of Java software for Mac OS users. To learn if Apple has made available any JRE that is based on JRE 1.6.0, see http://www.apple.com/java. Alternatively, registered Apple Developer Connection (http://connect.apple.com/) members might find that Apple has released a preview version of a compatible JRE. We make no claims about the suitability of such software for any purpose and recommend that you test all software thoroughly before you rely on it.

Table 2 describes all other client system requirements to use the software user interfaces for DMM-DSM and DMPDM.

Table 2   Additional Requirements to Use DMM-DSM or DMPDM

In this operating system	You must use this browser version (or a later version):
Windows	One of these: • Internet Explorer 6.0 • Internet Explorer 7.0 • Firefox 2.0
Linux	Firefox 2.0
Mac OS X	Firefox 2.0

Table 3 describes all other client system requirements to use the software user interfaces for DMM-VPM and Video Portal.

Table 3   Additional Requirements to Use DMM-VPM or Video Portal

To use this video type:	In this operating system:	You must use this browser version (or a later version):	And you must use these browser plug-ins:
Flash Video	Windows	One of these: • Internet Explorer 6.0 • Internet Explorer 7.0 • Firefox 2.0	Flash 9
	Linux	Firefox 2.0	
	Mac OS X	Firefox 2.0	

Table 3 Additional Requirements to Use DMM-VPM or Video Portal (continued)

To use this video type:	In this operating system:	You must use this browser version (or a later version):	And you must use these browser plug-ins:
Windows Media	Windows	One of these: • Internet Explorer 6.0 • Internet Explorer 7.0 • Firefox 2.0	Flash 9 and one of these: • Windows Media 10 • Windows Media 11
QuickTime	Windows	One of these: • Internet Explorer 6.0 • Internet Explorer 7.0 • Firefox 2.0	Flash 9 and one of these: • QuickTime 7.0.x • QuickTime 7.1.x (except 7.1.6) • QuickTime 7.2.x

Table 4 describes all other client system requirements to use the software user interface for Video Portal Reports 4.1.

Table 4 Requirements to Use Video Portal Reports

In this operating system:	You must use this browser version and plug-in (or a later version):
Windows	• Internet Explorer 6.0, with Adobe SVG Plug-in 3.0 • Internet Explorer 7.0, with Adobe SVG Plug-in 3.0 • Firefox 2.o or later
Mac OS X	Firefox 2.0

Low Memory Causes DMPs to Restart Automatically

Rather than crashing when they run low on memory, DMPs are designed to restart automatically, which clears their memory and causes downtime of much less than 1 minute — as opposed to the lengthy downtime that a hard crash would cause. In the rare cases when DMPs do run out of memory and restart automatically, SWF files are almost always responsible. The known scenarios when this can occur are as follows:

- The file size is greater than 500KB for your SWF file. Larger SWF files do work correctly in most cases, but we recommend as a best practice that you should always strive to use the smallest possible SWF files. Smaller files are far less likely to be burdensome to your DMPs.

- Your SWF file uses bitmapped image files outside itself that have a very large file size, either individually or collectively. Any bitmapped image files that you use in the production of a SWF file should be small files. If a bitmapped file has a large file size, it is important for you to understand that merely reducing the height and width of its placeholder on your canvas in Adobe Flash (or any similar authoring tool that you might use to develop a SWF file) will not reduce the actual file size.

- The web page that you are showing uses too many embedded SWF files.

Known Problems

This section describes known problems in DMS 4.1.

✎
Note To learn more about a known problem, use the Cisco Software Bug Toolkit at
http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. (You will be prompted to log into Cisco.com.)

Table 5   *Known Problems*

Problem ID	Description	Workaround
Appliance Administration Interface (AAI)		
CSCsk75779	You must not use underscores in the appliance name when you enter it in AAI. Worldwide DNS standards do not support any use of special characters in DNS-resolvable device names.	To work around this problem, use the characters in device names that the DNS standard support. The supported characters are letters, numerals, and hyphens.
Cisco Digital Media Player (4300G and 4305G)		
CSCsk07794	Sometimes no SWFs are shown after the sequence in a playlist uses a URL between two SWF objects. This behavior is caused by defects in the Adobe Flash browser plugin.	To work around this problem, use a sequence in your playlists that our tests have shown should succeed: • URL, SWF, URL, SWF. • URL, URL, SWF, URL, SWF. • SWF, SWF converted from PowerPoint slides, URL, SWF. • SWF, SWF converted from PowerPoint slides, SWF, URL, SWF. • SWF converted from PowerPoint slides, SWF, URL, SWF, SWF, URL, SWF. • SWF converted from PowerPoint slides, URL, SWF, SWF, SWF, URL, SWF. • SWF converted from PowerPoint slides, URL, SWF converted from PowerPoint slides, SWF, SWF, SWF, URL, SWF.
CSCsh65471 CSCsj97431 CSCsj61448 CSCsj90458 CSCsj93576	DMPs are designed to restart automatically when their memory runs low, so that they will not hang or crash instead.	To work around this problem, do either of the following. • Choose content to show on your DMP that does not cause it to run out of memory frequently. • If your DMPs restart as often as once a day, schedule the DMM-DSM system task called Reboot to recur every night in a deployment to the affected DMP groups. See the "Using Advanced Tasks" section of the DMM user guide on Cisco.com.
CSCsj32062	The time stamp is always wrong in Syslog messages from a DMP 4300G or a DMP 4305G because they do not have internal clocks.	There is no workaround.

Table 5 *Known Problems (continued)*

Problem ID	Description	Workaround
CSCsj02878	Video files do not play if their file names contain any spaces.	To work around this problem, remove the spaces from all file names before you upload video files to your media library.
CSCsh27238	This release supports the Windows version of Apache web server, not Microsoft IIS.	To work around this problem, install and use Apache. If IIS is installed, uninstall it.
CSCsh88615	This release does not support the linear pulse code modulation (LPCM) audio codec. Use of this audio codec might cause your DMP to crash when you play MPEG-2 files	To work around this problem, do not encode audio with LPCM. If your existing files use LPCM, recreate them without it or transcode them so that they do not use it.
CSCsk22719	All services are brought down when firmware upgrade is started.	To work around this problem, schedule your firmware upgrades to start outside your normal business hours.
CSCsk33009	If you use a static IP address on a DMP instead of using DHCP, DMPDM does not prevent the entry of invalid IP address values that make a DMP unreachable. IP addresses are valid only when they use four octets (4 bytes), but DMPDM allows you to enter and save address values that use only three octets (3 bytes).	To work around this problem, press the Reset button on the DMP chassis. The DMP will require a DHCP server, as before.
CSCsk24406	DMPs crash when their browser screen rotates 180 or 270 degree while video is playing.	To work around this problem, do not rotate the browser while you are simultaneously playing a video.
CSCsk33862	DMM-DSM does not show any error message if you try to use firmware for a DMP 4305G when you upgrade a DMP 4300G.	There is no workaround.
CSCsh06492	IE6 prompts twice, IE7 prompts five times for login after password change.	There is no workaround.

Table 5   ***Known Problems (continued)***

Problem ID	Description	Workaround
CSCsk22380	You cannot upgrade DMP firmware if the TAC Troubleshooting Access option is set to Off in DMPDM.	To work around this problem in DMPDM, enable the TAC Troubleshooting Access feature. Alternatively, do the following in DMM-DSM: 1. Select **Digital Media Players > Advanced Tasks**. 2. Click **System Tasks** in the list of defined tasks, then click **Add New Application**. 3. Enter a name and description, then select **Set** from the Request Type list and enter exactly this in the Request field: `init.startService_shell=yes&` `mib.save=1&mng.exit=1`. 4. From the Request Type list, select **Set**, then click **Submit**. 5. Select **Schedules > Immediate Deployment**. 6. In the **DMP Groups** object selector, click the name of a DMP group to see its member DMPs in the DMP List table. 7. In the DMP List table, select the check box for each DMP that should receive the firmware deployment. 8. From the Actions list, select the name that you entered in Step 3, then click **Go**. To restore DMP security after the file transfer and the firmware upgrade are finished, repeat the procedure but enter exactly this in the Request field: `init.startService_shell=no&mib.save=1&mng.e` `xit=1`.

Table 5 Known Problems (continued)

Problem ID	Description	Workaround
Cisco Digital Media Manager for Digital Signage (DMM-DSM)		
CSCsh67156	The user interfaces for Java applets in DMM-DSM (meaning, Digital Media Designer and the features to schedule signage deployments) are not visible to you or your selections in them have no effect unless you use a supported Java Runtime Engine (JRE) version and your Java language settings are configured for US-English. If your PC uses any JRE version older than 1.5 (for DMS 4.0.x) or 1.6.0 (for DMS 4.1.x) or is configured to use any Java language other than US-English, it is likely that you will have problems when you try to see or use the scheduling features in DMM-DSM. Even if you can see the user interface for scheduling, your selections in it might not take effect. It is equally likely that problems of the same kind will interfere with your use of Digital Media Designer in DMS 4.1.x. To learn exactly which JRE release you are using and to confirm that it is working correctly, go to http://java.com/en/download/help/testvm.xml. To obtain the required JRE, go to http://javasoft.com, click **Java SE**, then download the required JRE version. To understand the Java release naming conventions, which have changed over time, see http://java.sun.com/javase/namechange.html.	To work around this problem, use a supported JRE version and configure your Java language setting to be US-English. **If you use Windows:** To confirm that you use the required JRE version or a later one, choose **Start > Settings > Control Panel > Java**, click the **General** tab, then click **About**. To confirm that your Java language is US-English, complete whichever procedure here applies to your Windows version: http://www.java.com/en/download/help/locale.xml. If this problem affects you even though you use the correct Java version, try the following: 1. Select **Start > Run**. 2. Enter **inetcpl.cpl**, then press **Enter**. 3. Click the **Advanced** tab. 4. In the Browsing area, find the check box that is named "Enable third-party browser extensions (requires restart)." 5. If the check box is selected, deselect it. 6. Click **OK**, restart your PC, then try again to open the DMM-DSM scheduler. **If you use Mac OS:** Apple maintains and distributes its own implementations of Java software for Mac OS users. To learn if Apple has made available any JRE that is based on JRE 1.6.0, see http://www.apple.com/java. Alternatively, registered Apple Developer Connection (http://connect.apple.com/) members might find that Apple has released a preview version of a compatible JRE. We make no claims about the suitability of such software for any purpose and recommend that you test all software thoroughly before you rely on it.
CSCsk47709	Playlist synchronization relationships are missing in Digital Media Designer when you reopen saved designs.	To work around this problem, restore the relationship between the two playlists, then save your work again.
CSCsk45701	In Digital Media Designer, you might simultaneously lose all of your work in a newly saved design *and* overwrite a design that you saved previously. This happens after you select File > Save As to save your work in a design for the first time, then select a saved design to be overwritten. The old design is overwritten and its replacement does not contain any objects or actions that you included in the old design *or* the new design.	To work around this problem the first time that you save your work in a new design, do either of the following: • Select **File > Save**, then enter a unique name. • Select **File > Save As**, then enter a unique name.

Table 5   ***Known Problems (continued)***

Problem ID	Description	Workaround
CSCsk45232	Any DMM-DSM user can start and use Digital Media Designer regardless of his or her user role. However, authorization is required to deploy anything from DMD to your DMPs.	There is no workaround.
CSCsk41444	Although we do not support playlist synchronization for more than two playlists per synchronization action, Digital Media Designer allows it.	To work around this problem, never use synchronization actions in DMD that synchronize more than two playlists per action.
CSCsk49449	If their frame delay rate is zero, animated GIF images play too fast in DMD and use 100 percent of CPU capacity on the client system PC where Digital Media Designer is running. (The underlying cause is a known problem in the JRE.) However, your DMPs play these files correctly. It is commonplace for GIF animations to use zero as their frame delay rate.	To work around this problem, explicitly enter a frame delay rate greater than zero for each animated GIF file that you use.
CSCsj33561	After you deploy a firmware upgrade to one or more of your DMPs, DMM-DSM shows the incorrect, old firmware version number for one of the successfully upgraded DMPs. This happens when the total number of DMPs that you have upgraded is exactly the same as the total number of licenses that you have purchased to manage DMPs centrally. There is no effect on the performance or capabilities of your digital signage environment.	There is no workaround.
CSCsk53087	If you double-click any unsaved deployment job on the timeline at Schedules > Future Deployment, DMM-DSM opens a popup window that shows an HTTP status code 500 message.	To work around this problem, close the popup window, click **Save**, then try again to double-click the deployment job on the timeline.
CSCsk55107	The end date is extended by 2 months for a recurring scheduled job if you configure it to end within the hour preceding midnight on the last day of any month.	To work around this problem, do not schedule any job to end at any time from 23:00 to 23:59 on the last day of any month.
Cisco Digital Media Encoders		
CSCsk53344	DMEs (1000 and 2000) stop capturing video after 30 hours when you use Save As. This problem does not affect live encoding, which can run for 5 days.	To work around this problem, restart the encoder
CSCsk35671	Volume is low when you play live video through your Video Portal.	To work around this problem, do ether of the following: • Use Niagara SCX to increase the volume. • Add an amplifier.
CSCsk66835	The default audio input is set to Virtual Cable 1 when you use the AVI, Flash, and Real codecs.	To work around this problem, make sure to set the audio interface to Osprey if you use the SCX or web interfaces.

Table 5 **Known Problems (continued)**

Problem ID	Description	Workaround
CSCsk53361	Niagara SCX defaults to the C: drive when it saves video to a file. The C drive fills up quickly because it has too little free space.	To work around this problem when you use the Niagara SCX option to save video to a file, change the default location to D:\AVFiles\Out\.
CSCsk66837	You cannot set the IP Address or gateway from the LCD when an octet in the address uses only one or two digits.	To work around this problem, use DHCP to set the IP address and gateway values automatically or connect a keyboard, mouse, and VGA monitor to the encoder so that you can configure its network settings.
CSCsk66843	The AVI codec does not encode correctly at full resolution.	To work around this problem, use a lower resolution when you use the AVI encoding format.
Cisco Video Portal 4.1		
CSCsk16652	Video Portal does not indicate when replication has not occurred. LDAP users cannot login. Video Portal errors say that user names and passwords are invalid.	To work around this problem, perform the replication again on both your DMM appliance and your Video Portal appliance.
CSCsk35671	Program search does not work with titles that have line breaks. User can find the content, but when you select it, you cannot go to it	There is no workaround.
CSCsk28257	Video Portal client systems with low memory might hang while viewing events (live or VoD) that include more than 100 synchronized slides. (Each such slide requires approximately 2 MB of memory.)	To work around this problem, increase memory on the client system.
CSCsk24494	The interstitials on your Video Portal show nothing even though you populated them with JPEG files in DMM-VPM.	To work around this problem if you upload JPEG files in DMM-VPM so that you can use them as interstitials on your Video Portal, the files must use .JPG (**not** .JPEG) as their filename extension.
CSCsk35948	The displayed sizes are sometimes wrong for downloadable files on your Video Portal. This happens after administrators use kilobytes as the measurement unit when they upload files to DMM-VPM. Your Video Portal displays file sizes to you in bytes and sometimes cannot parse file sizes correctly when the measurement units differ.	To work around this problem in DMM-VPM, enter file sizes in bytes, not in kilobytes.
Cisco Digital Media Manager for Desktop Video (DMM-VPM)		
CSCsj59549	The Start Encoder button disappears for a DME after you use ad-hoc streaming controls to start it. You are therefore prevented from scheduling any new events for it.	To work around this problem, use the ad-hoc streaming controls to stop the encoder before you try to schedule a new event.
CSCsj29463	You do not see a video preview when you click the View Live Video link. The preview is missing if the encoder IP address changes and is rediscovered, because the link still uses the old IP address for the encoder.	To work around this problem, change your pull configurations so that they use the new IP address.

Table 5   Known Problems (continued)

Problem ID	Description	Workaround
CSCsk20220	DMM-VPM does not warn you that it will not allow you to upload any file with a file size greater than 2 GB.	To work around this problem, upload files that are smaller than 2 GB apiece.
CSCsk18817	When your DME2000 is running two or more encoding sessions simultaneously, the Encoder Dashboard can only stop one encoding session.	There is no workaround.
CSCsk69784	Slide deployments fail if the Deployment Root Directory location uses backslashes. This happens because the improper use of backslashes prevents DMM-VPM from creating the required /slides subdirectory automatically on your deployment server.	To work around this problem, do either of the following: • Use forward slashes when you enter a value to define the root directory for deployments. • Log in to your deployment server, then manually create the **/slide** subdirectory under the **/support** directory.

Resolved Problems

This section describes problems from earlier releases that are solved (or are not problems) in DMS 4.1.

Table 6   Resolved Problems

Cisco Digital Media Player (4300G)

CSCsi31782

When you play MPEG-1 or MPEG-2 video files that are stored locally (on the SD card or on a USB flash memory drive), playback stops approximately 5 to 10 seconds before the file actually ends.

CSCsh29814

You might think that the Reset button on a DMP 4300G chassis should restore the factory-default settings, but that is not its purpose. Its purpose is to reset (restart) the device.

CSCsh49548

Zoning application cannot play 3 GB MPEG2 video file.

CSCsh57008

DMP cannot play video in web server port other than 80 for zoning application.

CSCsh40935

Failover SD playback sometimes MPEG2 pauses in zoning application.

CSCsh43126

Templates sometimes do not work well with analog inputs: SVideo/NTSC_M.

CSCsh27216

Upgrade firmware status not updated automatically using IE.

CSCsh29806

Sometimes DMP has sound only, without video, from UDP multicast MPEG1 video file.

CSCsh24149

Zoning application sometimes does not play Flash from SD card.

Table 6 **Resolved Problems (continued)**

Cisco Digital Media Manager for Digital Signage (DMM-DSM)

CSCsh72512

If you deliver an empty playlist from DMM-DSM to a DMP, the DMP restarts repeatedly.

CSCsh67169

Delete and recreate ACNS channel with the same name causes HTTP 500.

CSCsh42045

Tiny content selection box in zoning application GUI.

CSCsh70312

DMM-DSM in ACNS multichannel environment, stop and start command in race condition and sometimes cause DMP to stop playing.

CSCsh67472

DMM-DSM Scheduler applet slows after you configure multiple tasks.

Cisco Digital Media Manager for Desktop Video (DMM-VPM)

CSCsi86193

DMM users do not see scheduled live events on the Encoder Dashboard page in DMM-VPM. Audience members cannot see scheduled live events on their Video Portal. (Digital signage is not affected.) On a DMS appliance or a Video Portal Appliance that was already configured, an administrator used AAI to change the time zone setting. However, the administrator did not then restart the appliance, even though a restart is required.

CSCsg85672

DMM-VPM sometimes shows the wrong duration for Flash Video (FLV) files.

CSCsf27269

Uploading two video types at the same time causes both of the fields to be populated with the same file name.

CSCsf25251

The system cannot play videos using RealPlayer and Windows Media Player when the interstitial sequence contains zero interstitials.

CSCsf12812

The video player pauses at the end of the playback.

CSCsf16913

When playing Real video on an Apple Macintosh using the Safari browser, the video never loads.

CSCsf25461

It is possible to schedule a transcoding job in the past.

CSCsg44766

The DMM Video Portal Preview popup window does not open in the display.

CSCsg45129

The dashboard shows status for only a single transcoding job at a time.

CSCsg56309

Automatic duration calculation for Flash/FLV does not work for files bigger than 150 MB.

CSCsh70123

HTTP Status error when creating more than 21 users.

Table 6   Resolved Problems (continued)

Cisco Video Portal 4.0

CSCsg92460

The Video Information link disappears for an FLV video after you view it at full-screen size, then return it to its normal size.

Related Documentation

To see all user documentation for DMS products, go to http://www.cisco.com/web/psa/products/tsd_products_support_troubleshoot_and_alerts.html?c=268438145&sc=280889186.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html