Upgrade Guide to Release 4.1 for Cisco Digital Media System

Warning **Before you start to upgrade your Cisco Digital Media System (DMS) environment, it is important that you read this brief document carefully. It contains crucial information and detailed checklists that can help you to ensure a successful upgrade and avoid potentially serious problems.**

This guide explains how to upgrade your DMS appliances and Digital Media Player endpoints from the DMS 4.0 release so that they use software from the 4.1 release—with updates to *Cisco Digital Media Manager* (DMM) software, *Cisco Video Portal* and *Video Portal Reports* software, *Digital Media Player Device Manager* (DMPDM) software, and the *Appliance Administration Interface* (AAI) command shell.

This upgrade is suitable for customers who purchased:

- Media Convergence Server appliances that use H1 or H2 chassis and on which DMS 4.0 software is installed, licensed, and working correctly. (If your appliances use DMS 3.4 or DMS 3.5, you must upgrade them to DMS 4.0 before you can use this upgrade.)
- Cisco Digital Media Player 4300G endpoints.

For late-breaking information about DMS 4.1 and to understand the known and resolved problems in this release, see *Release Notes for Cisco Digital Media System 4.1* on Cisco.com.

This guide contains these sections:

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

Upgrading Your Video Portal Appliances

⚠

Caution   Cisco does not support any deployment of, or storage of, content files on Cisco Video Portal appliances. If you deployed any files to your Video Portal 4.0 appliance despite our warnings that you should not, this upgrade **will delete all of these files automatically**. You will not be able to retrieve them or use them after they are deleted.

If you have not kept any other copies of files that you deployed to a Video Portal appliance, we recommend that you download and save local copies of these files before you upgrade. You can do this from one or more HTTP URLs that show directory listings in your browser, like this:

```
Icon  Name                                          Last modified    Size  Description

[DIR] Parent Directory                                               -
[IMG] 000000000000000000000000000001_                27-Sep-2007 18:52   20K
[   ] 000000000000000000000000000002_                27-Sep-2007 18:53  5.4M
[   ] 000000000000000000000000000003_                27-Sep-2007 18:53  4.2M
[   ] 000000000000000000000000000003_                27-Sep-2007 18:53  5.5M
[   ] 000000000000000000000000000004_                27-Sep-2007 18:52  253K
[IMG] 000000000000000000000000000006_                27-Sep-2007 18:53   26K
[TXT] 000000000000000000000000000010_                27-Sep-2007 17:38  437
```

There is one URL apiece for each media type that your Video Portal supports. To learn in this case what the HTTP URLs are on your Video Portal appliance that will show directory listings like this one to you, do the following:

1. In DMM-VPM, select **Setup > Deployment Locations**.
2. Copy the URLs that you see in the Root URL Path field for each media type that your Video Portal supports.
3. Show in your browser the directory listing for one media type that your Video Portal supports, which you deployed to your Video Portal appliance:

   a. To use the browser field where you enter URLs, press **Ctrl-L**.
   b. To paste the corresponding URL into the browser field, press **Ctrl-V**.
   c. To load the directory listing in your browser, press **Enter**.

4. Download each file that you should save, then edit each filename to delete its numeric prefix.

If you have not kept any other copies of these files, cannot use the directory listings method to download them, and cannot afford to lose them, we strongly urge you to call Cisco TAC **before you start** to install this upgrade.

Remember: You will not be able to retrieve your files after they are deleted.

To prevent any future upgrades from deleting the files again, do the following:

1. Select and prepare a dedicated storage server to host your content files.
2. Complete the Video Portal appliance upgrade process that the following checklist describes.
3. In DMM-VPM, reconfigure the Video Portal deployment locations as the DMM user guide describes.
4. In DMM-VPM, redeploy your content files to your dedicated storage server.

✎

Note   Wherever this guide tells you in AAI to move between menus, find options, or make selections:

- To navigate through a list of options and to highlight one option, press the **Up** and **Down** arrow keys.
- To select or deselect a highlighted option, press **Spacebar**.
- To save your changes and activate them, press **Enter**.

🔍

Tip   Do not use underscores or any other special characters in hostnames. DNS standards do not support these characters. Use only letters, numerals, and hyphens.

Use the following checklist to track your progress as you upgrade your Video Portal appliances. If you do not have any Video Portal appliances, you can skip this checklist.

✓	Task
☐	**1. Obtain the upgrade ISO image.** **a.** Log in to your Cisco.com account, then go to http://www.cisco.com/cgi-bin/tablebuild.pl/dms. **Note** After May 5, 2008, go to http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281723656. **b.** Download **CVP-UPG-40to41_4.1.0.35.iso**.
☐	**2.** (**Optional**) To verify the upgrade image after you download it, confirm that its MD5 hash value is **7C6FFECB89F9032F6CF3F53233EEF0B3**. **Tip** To obtain a GNU utility called md5sum, which you can use to check the MD5 hash value of any file, go to http://www.gnu.org/directory/textutils.html. Cisco does not support the md5sum utility. You can use any other utility for this purpose that you prefer. Alternatively, see http://directory.fsf.org/coreutils.html.
☐	**3. Burn the upgrade image on a CD-ROM disc as an ISO or CD image and not as a file.** For more information, see the manufacturer documentation for your CD-ROM writer. If you are not sure that you burned the disc as a CD image, insert it into any PC, then browse the files on the disc. If any filename uses the .ENC extension, it is likely that you burned the disc correctly. If you see exactly the same .ISO file that you downloaded, you did not burn the disc correctly and must try again to burn it.
☐	**4. Install the upgrade on your Video Portal appliance.** **a.** Insert the CD into the chassis CD-ROM drive. **b.** Use the attached keyboard[1] to log in to the Appliance Administration Interface (AAI) as **admin**. **c.** In AAI, select **APPLIANCE_CONTROL**, then press **Enter**. **d.** In AAI, select **SOFTWARE_UPDATE**, then press **Enter** two times. **e.** Follow the on-screen instructions to update the software on your Video Portal appliance. **Tip** AAI shows a status code at the end of every stage in the upgrade process. The numeral 0 signifies success and any other number signifies an error. At the end of the upgrade process, you can expect to see a message that says, "The upgrade was successful. You will now be logged out for the changes to reflect on the AAI." **f.** To complete the appliance upgrade process, press **Enter**. It is not necessary to restart your Video Portal appliance now, but you should restart it after the upgrade is finished for your DMM appliance. See DMM 4.1 Upgrade Checklist, page 7.

1. Alternatively, to log in securely from a remote system, rather than the actual appliance (for example, if a keyboard or monitor are not attached to it), point an SSH client to the IP address that your Video Portal appliance uses. PuTTY is a popular SSH client that you might use, but there are many others.

Upgrading Your DMM Appliances

This section includes these topics:

Understanding DMM 4.1 Compatibility with Cisco Digital Media Players

You must upgrade any DMPs that use any earlier firmware revision than 2.43. Otherwise, your DMPs will not be compatible with the new Digital Media Designer (DMD) features in DMM-DSM 4.1.

- On a DMP 4300G, the required firmware revision is 2.43.x.
- On a DMP 4305G, the required firmware revision is 2.43.x.

If you want to see in DMM-DSM what firmware version is running on your DMPs, deploy to any of your DMP groups the system task called Version. See the "Using Advanced Tasks" section of Chapter 3 in *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com.

Before you upgrade any DMP firmware for compatibility with this DMS release, you must upgrade your DMM appliance as described in DMM 4.1 Upgrade Checklist, page 7.

When you upgrade DMM, all of the playlists and zoning applications that you created in DMM-DSM 4.0 will be converted automatically for compatibility with DMD.

Note
- **We do not support downgrades from DMP firmware version 2.43 to version 2.42.**
- All files that you have saved to the internal SD flash memory card will be deleted permanently when you upgrade from DMP firmware version 2.42 to version 2.43. Your files are deleted because the two firmware versions use different file systems and the internal SD flash memory card must be reformatted.
- Any "custom" digital signage applications that you developed outside of DMM-DSM 4.0 for DMP firmware version 2.42 are not compatible with DMM-DSM 4.1 and will not be converted automatically for compatibility with DMM-DSM 4.1 during this upgrade process. For example, if you developed a custom digital signage application for DMM-DSM 4.0 that relies on the Cisco Digital Signage JavaScript APIs (no matter which JavaScript development environment you used), that application will not be compatible with this release. Nor will it be compatible with DMP firmware 2.43.x.
- We recommend that, before you decide to upgrade, you consider which of your existing DMM-DSM 4.0 applications will be converted automatically and which will not be converted.
- We further recommend that the most effective method to convert any custom application for digital signage from DMM-DSM 4.0 to DMM-DSM 4.1 is to recreate it in Digital Media Designer, which is an integral part of DMM-DSM 4.1. Starting in DMM-DSM 4.1, DMD is the preferred method for creating, editing, and managing your playlists and presentations for digital signage.
- Custom JavaScript applications are complex and, as in any programming or scripting language, many different methods and styles might lead to the same result. For this reason, Cisco TAC cannot provide development or migration support for custom JavaScript applications.

Java Runtime Engine (JRE) 1.6 must be installed on each PC in your organization where any DMM-DSM user will design or deploy presentations for digital signage. In addition, each of those PCs must use an operating system and browser that DMS supports. We recommend that you reach out to the DMM-DSM users (creative staff, for example) and desktop support staff in your organization and help them to understand these requirements.

There are many possible error messages that PCs might display if the wrong JRE is installed, or if there is no installed JRE. In some cases, the error message is "java.lang.UnsupportedClassVersionError: Bad version number in .class file." Alternatively, affected PCs might display a prompt to save the authoring_tool.jnlp file.

Tip

- To learn about the supported platforms and browsers, see *Release Notes for Cisco Digital Media System 4.1* on Cisco.com.

- To learn more about the requirement to use JRE 1.6, see the "Before You Start to Use Digital Media Designer" checklist in Chapter 3 of *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com.

- To test for the presence of JRE 1.6 on a PC, log it in to DMM-DSM, select **Help > Downloads**, then click **Check Java Plugin**.

Understanding DMM 4.1 Compatibility with Cisco Digital Media Encoders

- On a DME 1000, the required software revision is 5.2.184. For upgrade instructions, see *Upgrade Guide to Release 5.2.184.0 for Cisco Digital Media Encoder 1000*, available on Cisco.com.

- On a DME 2000, the required software revision is 5.2.180. For upgrade instructions, see *Upgrade Guide to Release 5.2.180.0 for Cisco Digital Media Encoder 2000*, available on Cisco.com.

You must upgrade any DMEs that use any earlier software revision than is specified here. Otherwise, your DMEs will not support the new question and answer features or the new slide synchronization features for live events. To obtain these upgrades, email your request to dms-softwarekeys@cisco.com.

DMM 4.1 Upgrade Checklist

🔍

Tip   Do not use underscores or any other special characters in hostnames. DNS standards do not support these characters. Use only letters, numerals, and hyphens.

Use the following checklist to track your progress as you upgrade your DMM appliance.

✓	Task
☐	**1. Back up the settings, configurations, and video metadata for your DMM appliance.** **a.** Use the attached keyboard[1] to log in to the Appliance Administration Interface (AAI) as **admin**. **b.** Select **DMM_CONTROL**, then press **Enter**. **c.** Select **BACKUP_DMM**, then press **Enter**. **d.** Do one of the following: • To back up to a USB drive that is connected to your DMM appliance, select **USB**, then press **Enter**. • To back up to your Video Portal appliance, select **VIDEO_PORTAL**, then press **Enter**. (The Video Portal appliance that you use, if you have more than one, is whichever one you selected in DMM-VPM as the location for deployments.) Assuming that your network is fast, the backup is finished in less than 30 seconds. A message says, "Done."
☐	**2. Obtain the upgrade ISO image.** **a.** Log in to your Cisco.com account, then go to http://www.cisco.com/cgi-bin/tablebuild.pl/dms. **Note** After May 5, 2008, go to http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281723656. **b.** Download **DMS-UPG-40to41-4.1.0.40.iso**.
☐	**3.** (**Optional**) To verify the upgrade image after you download it, confirm that its MD5 hash value is **9865defdb018f90cc7e8d30a46affbb11**. **Tip** To obtain a GNU utility called md5sum, which you can use to check the MD5 hash value of any file, go to http://www.gnu.org/directory/textutils.html. Cisco does not support the md5sum utility. You can use any other utility for this purpose that you prefer. Alternatively, see http://directory.fsf.org/coreutils.html.
☐	**4. Burn the upgrade image on a CD-ROM disc as an ISO or CD image and not as a file.** For more information, see the manufacturer documentation for your CD-ROM writer.
☐	**5. Install the upgrade on your DMM appliance.** **a.** Insert the CD into the chassis CD-ROM drive. **b.** Use the attached keyboard[1] to log in to the Appliance Administration Interface (AAI) as **admin**. **c.** In AAI, select **APPLIANCE_CONTROL**, then press **Enter**. **d.** In AAI, select **SOFTWARE_UPDATE**, then press **Enter** two times. **e.** Follow the on-screen instructions to update the software on your DMM appliance. **Tip** AAI shows a status code at the end of every stage in the upgrade process. The numeral 0 signifies success and any other number signifies an error. At the end of the upgrade process, you can expect to see a message that says, "The upgrade was successful. You will now be logged out for the changes to reflect on the AAI." **f.** To complete the appliance upgrade process, press **Enter**. It is not necessary to restart your appliance.

✓	Task
☐	6. **Check the DMM release number.** In your browser, log in to DMM (http://*<DMM_IP_address>*:8080), then check its splash screen to see if the DMM release version is 4.1. If the version *is not* 4.1, contact Cisco TAC.

☐	7. **Check the license for each DMM module that you have purchased.**
	
	  a. In DMM, select **Administrator Module** from the untitled list in the top far-right of any page.
	
	  b. Click **View Current License**, then read the page carefully to confirm that your DMM licenses support all of the DMM software modules (such as DMM-VPM and DMM-DSM) that you have purchased.
	
	  If you see that your license entitlements are incomplete, contact Cisco TAC. If the support engineer asks that you send Cisco a copy of the Tomcat logfile, see the "Obtaining or Transferring a Copy of the System Log" topic in Chapter 5 of *Appliance Administration Guide for Cisco Digital Media System 4.1* on Cisco.com.

☐	8. **If you use DMM-VPM, make sure that its deployment values are correct.** If you do not use any desktop video features, you can skip this task.
	
	  a. Select **Video Portal Module** from the untitled list at the top far-right of any page, then select **Setup > Deployment Locations**.
	
	  b. In the areas that represent the possible deployment types (Flash Video, Windows Media Video, MPEG4/H.264, and Support), verify or enter the values for the types that you will use. Any missing or incorrect values will cause your Video Portal deployments to fail.
	
	    • **Connection type**—The protocol or method for file transfer (the options are FTP, SFTP, and SCP).
	
	    • **Host address**—The DNS-resolvable hostname or IP address of the remote server where you will deploy files of the relevant filetype.
	
	    • **Login name**—A user account name that has the required privileges to access the remote server.
	
	    • **Login password**—The assigned password for the login name that you specified. If you select the SFTP option for deployments to your Video Portal appliance (even though **we do not support such deployments** and despite our warnings that you should **never deploy content to a Video Portal** appliance), the password that you enter must be exactly the same as your Video Portal admin password.
	
	    • **Root file directory**—The value of the relative directory path to files that you will deploy. For example, if the root directory on the server is configured to be /data/ftproot and the absolute path for the deployment site ends with /data/ftproot/vp/flash, then the relative value to enter here would be /vp/flash.
	
	    • **Root URL Path**—The absolute URL, where the Video Portal will host and reference your files.
	
	  c. Scroll to the bottom of the page, then click **Save Deployment Locations**.

☐	⚠
	Caution The selections that you make here must all be perfectly identical to the selections that you make when you configure the supported media types on your Video Portal appliance.
	
	9. **If you use DMM-VPM, specify the formats that your Video Portal should support.** If you do not use any desktop video features, you can skip this task.
	
	  a. Select **Video Portal Module** from the untitled list at the top far-right of any page.
	
	  b. Select **Setup > Video Portal**, then select the relevant check boxes in the "Supported Media Formats" area.
	
	  c. Click **Save Portal Parameters**.

✓	Task
☐	**10.** **If you use DMM-DSM, make sure that its external deployment server locations are correct.** If you do not use any digital signage features, you can skip this task.

a. Select **Digital Signage Module** from the untitled list at the top far-right of any page.

b. Select **Settings > External Deployment Locations**, then verify or enter the values for your external deployment servers.

To see and use the Settings tab, you must be logged in an administrator.

- **External Publishing Server List**—Click a server to highlight it, so that you can edit or delete it. DMM-DSM automatically shows the Change External Publishing Server pane for the corresponding server, where you can edit its settings.
    - -- **Add New External Publishing Server ( )**—Shows the Add New External Publishing Server pane, where you can define the settings to use a new server.
    - -- **Delete External Publishing Server ( )**—Deletes the server that you highlighted.
- {**Add New** | **Change**} **External Publishing Server**—Add or edit attributes of the external servers that you use for deployments.
    - -- **Host**—The routable IP address or resolvable DNS hostname of the external deployment (FTP) server. You must enter this value.
    - -- **Port**—The port number to use. You can use any port number, but the default is 21.
    - -- **Server Type**—FTP.
    - -- **Remote Directory**—Corresponding to the same server directory structure that you reference when you enter an HTTP Mapping value (see the item below this one), enter the root-level deployment directory to use on your external publishing server when your communications protocol is ftp. For example, you might enter only a forward slash (*/*).
    - -- **HTTP Mapping**—Corresponding to the same server directory structure that you reference when you enter a Remote Directory value (see the item above this one), enter the root-level deployment directory to use on your external publishing server when your communications protocol is http. For example, you might enter **/ftproot**.
    - -- **HTTP Port**—Enter the port number to use on the external deployment server. You can use any port number. If you do not enter a port number, the default is to use port 80.
    - -- **User Name**—Enter the FTP username. It is acceptable to use the name *anonymous*.
    - -- **Password** | **Confirm Password**—You must enter the FTP password, then reenter it.

c. Click **Save**.

✓	Task
☐	**11. If you use DMM-DSM, make sure that Digital Media Designer (DMD) converted your preexisting digital signage designs correctly.** If you do not use any digital signage features, you can skip this task. **a.** Complete the "Before You Start to Use Digital Media Designer" checklist in *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com. **b.** Select **Digital Signage Module** from the untitled list at the top far-right of any page. **c.** Select the **Designs** tab, then click **Start Digital Media Designer**. **d.** When prompted, select the option to use Java Web Start. **e.** When DMD opens, select **File > Open**. **f.** Under the Presentations tab, select one of your preexisting designs that was converted, then click **OK**. To learn how to use DMD to correct any errors that might have occurred during the automated design conversion, see the "Developing Presentations, Templates, and Playlists for Signage" section in *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com. **g.** To save your work in DMD, select **File > Save**. **h.** To exit DMD, select **File > Exit**.
☐	**12. If you use DMM-DSM, make sure that your preexisting inventory of DMPs is intact.** If you do not use any digital signage features, you can skip this task. **a.** Select **Digital Signage Module** from the untitled list at the top far-right of any page. **b.** Select **Digital Media Players > DMP Manager**. When you make selections anywhere on the DMP Manager page, it is updated automatically to show the options and features that are relevant to your selection. Device inventory management options and features are complex. To understand inventory management, see the "Managing and Grouping DMPs" section in *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com.
☐	**13. If you use DMM-DSM, make sure that your DMPs are working.** If you do not use any digital signage features, you can skip this task. **a.** Select **Digital Signage Module** from the untitled list at the top far-right of any page. **b.** Select **Digital Media Players > Network Status**.

1. Alternatively, to log in securely from a remote system, rather than the actual appliance (for example, if a keyboard or monitor are not attached to it), point an SSH client to the IP address that your DMM appliance uses. PuTTY is a popular SSH client that you might use, but there are many others.

After You Upgrade Your DMM Appliance

After you upgrade your DMM appliance, if you have been using a licensed copy of DMM-DSM, you must also complete some additional tasks to update your digital signage network.

✎

Note Because you upgraded the software on your DMM appliance, all of the zoning applications, full-screen Flash applications, multicast applications, and playlist applications that you saved in DMM-DSM 4.0 have been converted automatically to DMD presentations so that you can continue to use them in DMM-DSM 4.1. Although the old formats were resolution-independent, your converted presentations have been set at 1,366 pixels wide by 768 pixels high. You can modify these dimensions in DMD.

Use the following checklist to track your progress as you update your digital signage network.

✓	Task
☐	**1.** **If you changed the administrative username or password on _any_ of your DMPs, you must restore the factory-default values on every DMP in your network.** This task applies to you only if some of your DMPs use different administrative usernames or passwords than the rest of your DMPs use. In this case, they must all be made to use the factory default username, **admin**, and the factory default password, **default**. If your DMPs already all use the factory-default username and password for administrative access, you can skip this task. **a.** In DMM-DSM, select **Digital Media Players > Advanced Tasks**. **b.** In the list of application types, click **System Tasks**. **c.** In the title bar for the Applications area, click **Add New Application**. **d.** In the Name field, enter **DMP_Admin_Factory_Default**. **e.** In the Description field, enter a meaningful description. **f.** In the Request field, enter `mibifc.user=admin&mibifc.password=default&mib.save=1&mng.exit=1`. **g.** From the Request Type list, select **Set**, then click **Submit**. **h.** Select **Schedules > Immediate Deployment**. The root level of your digital signage network is selected by default, representing all of your DMPs. This is the correct selection. **i.** From the Actions list, select **DMP_Admin_Factory_Default**, then click **Go**.

✓	Task
☐	⚠ **Caution** **Make sure that your DMPs never lose power while they are burning their firmware during an upgrade. If they lose power during this critical period, they will be severely damaged.**

Tip   We recommend that you send the DMP firmware for an upgrade job to your ACNS servers (and deploy the upgrade as a scheduled job, not an immediate job). However, if you must deploy the upgrade directly to your DMPs, we recommend that you never upgrade any more than 20 DMPs at any one time. We further recommend that all upgrades should occur outside the normal business hours for your organization.

2. **Upgrade the firmware on your DMPs so that they support DMD and use improved security measures.** Until you complete this task, your centrally managed DMPs will not be able to play any presentations, including those that DMM-DSM converted automatically from your old zoning applications, old playlists, and all similar methods that the DMS 4.0 release supported.

   a. Log in to your Cisco.com account, then go to http://www.cisco.com/cgi-bin/tablebuild.pl/dms.

Note   After May 5, 2008, go to http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281723656.

   b. Download the **rootfs-2.43FCS_4300.fwimg** firmware file.

   c. (**Optional**) To verify the firmware file after you download it, confirm that its MD5 hash value is *C65E9381FE44109112755F5E7636F4C4*.

   d. In DMM-DSM, select **Media > Media Library** and, in the title bar for the Media Files area, click **Add New Content**.

   e. For the source, click **File**.

   f. Click **Browse**, select the firmware image that you downloaded, then press **Enter**.

   g. Verify that the selected file type is **Firmware**, then click **Submit**.

      Do not click any button or move away from this page in your browser until the upload is finished. After it is finished, the page refreshes automatically. You should see that a description of the firmware file has been added in the table that the page shows. If you want to confirm that the upload succeeded and the firmware file was not corrupted or truncated while it was uploading, compare its filesize in the Size column to the size of the source file on your PC.

   h. Select **Digital Media Players > Advanced Tasks**, then click **DMP Firmware Upgrade**.

   i. In the title bar for the Applications area, click **Add New Application**.

   j. In the Name field, enter **DMP_Firmware_2.43_Upgrade**.

   k. In the Media Categories tree, select the category that contains the firmware.

   l. In the Available Content table, click the firmware file to highlight it, then click **Submit**.

   m. Select **Schedules > Immediate Deployment**.

Tip   We recommend that you upgrade just one DMP initially, or upgrade just a small group of DMPs, then test the result before you send the firmware to every DMP.

   n. In the **DMP Groups** object selector, click the name of a DMP group to see its member DMPs in the DMP List table.

   o. In the DMP List table, select the check box for each DMP that should receive the deployment.

   p. From the Actions list, select **DMP_Firmware_2.43_Upgrade**, then click **Go**.

Note   DMP firmware upgrades take approximately 30 minutes to complete. If you want to check the current status of an upgrade, deploy to the relevant DMP groups the system task called Upgrade Status. See the "Using Advanced Tasks" section of Chapter 3 in *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com.

✓	Task
☐	**3.** **Unify the user credentials for all of your DMPs.** **a.** In DMM-DSM, select **Digital Media Players > Advanced Tasks**. **b.** In the list of application types, click **System Tasks**. **c.** In the title bar for the Applications area, click **Add New Application**. **d.** In the Name field, enter **DMP_Admin_New_Credentials**. **e.** In the Description field, enter a meaningful description. **f.** In the Request field, enter `mibifc.user=NEW_USER_NAME&mibifc.password=NEW_USER_PASSWORD&mib.save=1` `&mng.reboot=1`, where: • NEW_USER_NAME is a new login name for the DMP administrator. • NEW_USER_PASSWORD is a new password for the DMP administrator. We recommend that you use a strong password. **g.** From the Request Type list, select **Set**, then click **Submit**. **h.** Select **Schedules > Immediate Deployment**. **i.** In the **DMP Groups** object selector, click the name of a DMP group to see its member DMPs in the DMP List table. **j.** In the DMP List table, select the check box for each DMP that should receive the deployment. **k.** From the Actions list, select **DMP_Admin_New_Credentials**, then click **Go**.
☐	**4.** In DMM-DSM, select **Settings > Server Settings**, update the entries in the Name field and the User Password field to match the new values that you configured in Task 3, then click **Save**.

✓	Task

☐	⚠️
	Caution Before you use a file transfer application to deploy the assets from a new or updated presentation to any of your DMPs, you *must first* run the "Stop All Applications" system task on each affected DMP. To do so, click the **Schedules** tab, select the DMP group that will use the presentation, select **Stop All Applications** from the Actions list, then click **Go**.
	
	5. **If you use DMM-DSM, redeploy any assets that were deleted during the upgrade.** If you previously saved any assets for digital signage on the SD memory card inside a DMP, the upgrade process deleted those assets when it reformatted the SD memory card.
	
	  a. Select **Digital Signage Module** from the untitled list at the top far-right of any page.
	
	  b. Select **Digital Media Players > Advanced Tasks**.
	
	  c. From the Application Types list, select **File Transfer to DMP or Server**.
	
	  d. Click 📄 **Add New Application**.
	
	    The page is refreshed. To understand the options and features of this advanced task and learn how to use it, look for the "File Transfer to DMP or Server" row in the "Understanding and Using Advanced Tasks" table in Chapter 3 of *User Guide for Cisco Digital Media Manager 4.1* on Cisco.com.
	
	  e. To save your selections, click **Submit**.
	
	  f. Select **Schedules > Immediate Deployment**.
	
	  g. In the **DMP Groups** object selector, click the name of a DMP group to see its member DMPs in the DMP List table.
	
	  h. In the DMP List table, select the check box for each DMP that should receive the deployment.
	
	  i. Select from the **Actions** list the name of the presentation that you want to deploy. It will be under the Digital Media Designer heading.
	
	  j. Click **Go**.

☐	**6.** In DMM-DSM, select **Schedules > Future Deployment**, then click **Publish**. This step is essential if you use Cisco ACNS for content distribution in your digital signage network.

Related DMS 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.

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