Upgrade Guide for Cisco Digital Media Suite Release 5.2.3

Revised: July 27, 2011
OL-25176-01

Warning **Before you upgrade your Cisco Digital Media Suite (Cisco DMS) environment, read this document carefully. It contains important information that can help you avoid potentially serious problems during the upgrade process.**

This guide explains how to upgrade Cisco Digital Media Suite from version 5.2.2 to 5.2.3. See the "Hardware Compatibility" section on page 5, for information about the hardware supported by this upgrade.

If you are running any release that predates 5.2.2, you must upgrade to 5.2.2 first, and then upgrade to 5.2.3.

You must have a valid Cisco DMS 5.2 license to use this upgrade.

Table of Contents

- Before You Upgrade to Cisco DMS 5.2.3! page 2
- Hardware Compatibility, page 5
- Before You Begin, page 5
- Upgrade Your Cisco DMS Appliances, page 7
- Key Changes in Cisco DMS 5.2.3, page 20
- Learn More About..., page 21

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

Before You Upgrade to Cisco DMS 5.2.3!

Some user experience factors and deployment considerations are changed in Cisco DMS 5.2.3 because this release includes improved and expanded user authentication features.

- LDAP Syntax, page 2
- Browser Redirect, page 2
- Network Design, page 3
- Digital Certificates, page 3
- Firewall Ports, page 4
- User Authentication in Federation Mode (Single Sign-on), page 4

LDAP Syntax

This release is more strict than any prior release in its enforcement of proper LDAP syntax. Now, when you specify the administrator DN, you must use proper syntax, which conforms exactly to LDIF grammar.

- Proper syntax: `CN=admin1,OU=Administrators,DC=example,DC=com`
- Poor syntax: `EXAMPLE\admin1`

OTHERWISE

When you use poor syntax here for the first time while your DMM appliance runs Cisco DMS 5.2.3, we show you, the administrator, this error message: “Invalid username or password.”

But if you used and validated poor syntax in this way before ***upgrading*** to Cisco DMS 5.2.3, we do not repeat the validation process. Therefore—*even though we do not show an error message to anyone*—**LDAP users simply cannot log in**.

FURTHERMORE

LDAP validation also fails now whenever any expression includes a space immediately to either side of:

- Any “**=**” sign.
- Any “**objectClass**” attribute.

Browser Redirect

We redirect all login attempts from your Show and Share server to your DMM server. This browser redirect occurs by design and is integral to every user authentication transaction.

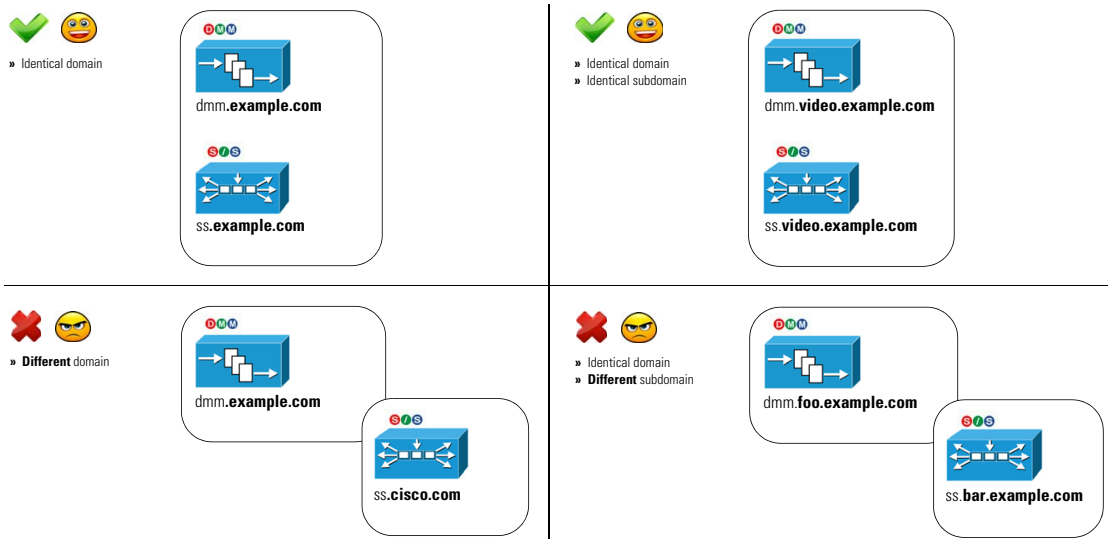
Network Design

Cisco DMS 5.2.3 imposes a new network design restriction.

The restriction is essential to support and maintain encrypted session cookies that cross-authenticate your Cisco DMS servers. As of this release, the FQDNs for your DMM appliance and your Show and Share appliance must share the same Internet domain—and subdomain, where applicable.

OTHERWISE

Show and Share login attempts all fail.



Digital Certificates

We recommend for Cisco DMS 5.2.3 that you stop all use of self-signed digital certificates.

Although we do not *force* you to buy and install third-party identity certificates, your failure to do so will affect all users of Show and Share in your network.

When you continue to use self-signed certificates despite this guidance, a browser message disrupts login authentication for Show and Share users by claiming that your login server is not trusted. This occurs with any and every supported method for user authentication—*embedded*, *LDAP*, and *federation*.

Firewall Ports

In Cisco DMS 5.2.3, you must open any firewall ports that affect traffic between your servers.

The most urgent use case is, for example, when your DMM server runs on a fully secured network segment but your Show and Share server is available to a wider population. *Even so, this guidance applies to every deployment.*

Otherwise, a browser message disrupts login authentication for Show and Share users by claiming that your login server is not trusted.

Note Additional errors and failures might occur at the same time.

These TCP ports must be open.

20	**21**	**22**	**80**	**389**	**443**	**514**	**554**	**636**	**694**	**695**
1935	**5432**	**7849**	**7850**	**8443**	**9161**	**9999**	**30865**	**45001**	**46001**	**61616**

User Authentication in Federation Mode (Single Sign-on)

When you migrate Cisco DMS user authentication services from LDAP mode to Federation mode—*assuming that you ever do*—**PAY URGENTLY CLOSE ATTENTION to the selection state of these two check boxes:**

- "Save LDAP Users"
- "Save Groups and Policies"

When you migrate from LDAP to Federation mode while these check boxes are both CHECKED, we *keep and continue to use* all user role assignment records for Show and Share. In addition, we *keep and continue to use* all records that associate individual users with the videos (and other assets) they published to Show and Share.

When you migrate from LDAP to Federation mode while these check boxes are both CLEARED, we *delete* all user role assignment records for Show and Share. In addition, we *delete* all records that associate individual users with the videos (and other assets) they published to Show and Share.

Hardware Compatibility

Cisco DMS 5.2.3 is supported on the following hardware platforms:

- SNS-SVR-C210EN-K9
- SNS-SVR-C200WG-K9
- DMM-SVR-C210-K9
- MCS-7835-H3
- Wave-574

Table 1 shows supported upgrade paths to Cisco DMS 5.2.3 based on hardware platform.

If you are performing a fresh install of Cisco DMS, you must use the recovery disc that was supplied with your appliance to install the base software and then continue along the upgrade path noted in Table 1.

Table 1 Upgrade path based on hardware platform.

Hardware Platform	Supported Upgrade Path
DMM-SVR-C210-K9, SNS-SVR-C210EN-K9, and SNS-SVR-C200WG-K9	5.2.2 to 5.2.3
MCS-7835-H3 (DMM and Show and Share) and Wave-574 (Show and Share)	5.2 to 5.2.1 to 5.2.2 to 5.2.3

The Cisco DMS 5.2.3 release is not supported on the following hardware platforms:

- MCS-7835-H1 or MCS-7835-H2
- MCS-7825-H2 or MCS-7825-H3

Before You Begin

Before you upgrade your Cisco DMS appliances, do the following:

1. Back Up Your Appliances, page 5
2. Obtain the Update Media, page 6
3. Connect a Terminal to Your Appliances, page 6

Back Up Your Appliances

We recommend backing up your appliances before performing the upgrade. To back up your appliances, refer to the *Administration Guide for Cisco Digital Media Suite 5.2.x Appliances* on Cisco.com:

http://www.cisco.com/en/US/partner/docs/video/digital_media_systems/5_x/5_2/dms/aai/administration/guide/dms_appliance_admin.html

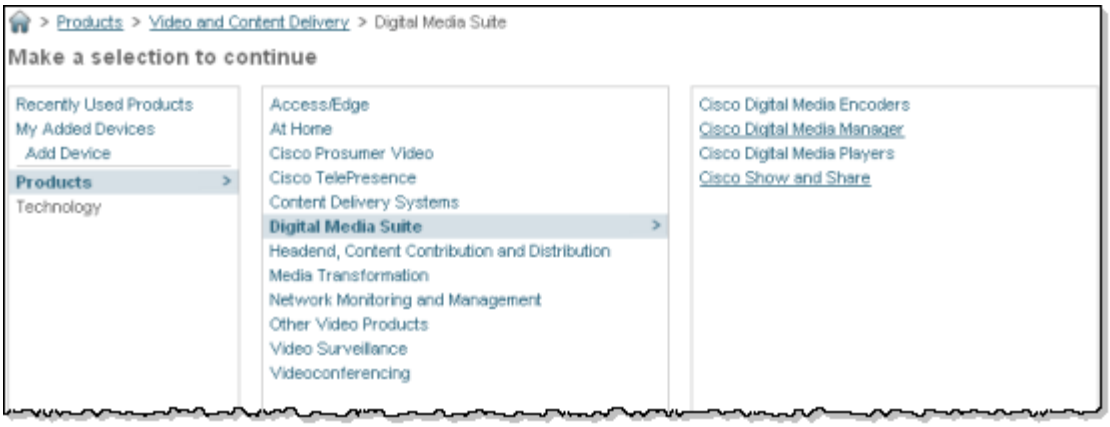
Obtain the Update Media

Download the update from Cisco.com.

Step 1 Point your browser to the Cisco software center:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Choose **Products > Video and Content Delivery > Digital Media Suite**.



Step 3 Download the following files:

- Cisco Show and Share: *sns522to523.iso*
- Cisco Digital Media Manager: *dmm522to523.iso*
- Digital Media Players:
  - Cisco DMP 4310G: *5.2.3_FCS_4310.fwimg*
  - Cisco DMP 4400: *5.2.3_FCS_4400.fwimg*
  - Cisco DMP 4305: *5.2.3_FCS_4305.fwimg*

Step 4 Create DVDs from the Cisco Digital Media Manager and Cisco Show and Share .iso files. Refer to your DVD burning software for information about how to create a DVD from an .iso file. We recommend burning the DVD at 1x speed.

Connect a Terminal to Your Appliances

You must attach a monitor and keyboard to each Cisco DMM and Cisco Show and Share appliance that you upgrade.

Do not attempt to upgrade using a remote SSH session—your upgrade will fail. The upgrade process reboots the appliance several times, causing remote sessions to be dropped. Your input is required after the reboot, but you cannot reestablish a remote session until the entire upgrade process is completed.

Upgrade Your Cisco DMS Appliances

Perform the following tasks to upgrade your Cisco DMS 5.2.2 installation to Cisco DMS 5.2.3. If you are using Cisco DMPs, upgrade your Cisco DMP software before upgrading your Cisco DMM software.

Note All components of your Cisco DMS installation must be upgraded to the same version for proper operation.

—	Task	Reference
Step 1	Upgrade your Cisco Digital Media Players, if any.	Upgrade Your DMPs, page 7
Step 2	Upgrade your Cisco DMM appliance software.	Upgrade Cisco Digital Media Manager, page 17
Step 3	Upgrade your Cisco Show and Share appliance software.	Upgrade Cisco Show and Share, page 19
Step 4	Verify the upgrade.	Verify the System Upgrade, page 20

Upgrade Your DMPs

To upgrade your DMPs, complete the following steps in the order shown:

1. Force DMPs From Their 'Initial' State, As Needed, page 7
2. Stop All Applications on DMPs, page 11.
3. Upgrade the Firmware and Root File System on DMP Endpoints, page 13.

Force DMPs From Their 'Initial' State, As Needed

Timesaver Complete this procedure if you have reapplied our factory-default settings to one or more of your DMPs. Otherwise, if you **have not** restored DMP factory defaults, you can skip this procedure.

Caution If this procedure applies to you and you do not complete it now, you will have to complete a more difficult and time-consuming procedure instead, after you finish all other tasks to upgrade Cisco DMS.

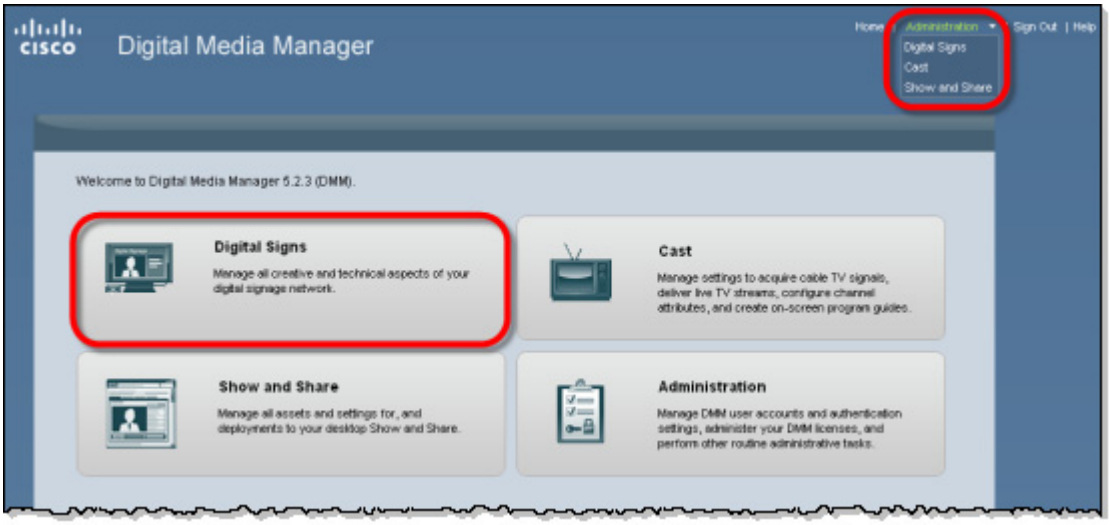
Before the *Cisco Digital Signs* software on your DMM appliance can manage these DMPs centrally, you must complete either this simple procedure now or the more complex procedure later.

A DMP returns to its "initial" state when you reset it to use factory-default settings. In its initial state, a DMP lacks an internal database file that supports centralized management. This procedure shows you how to force it from this initial state.

Tip If you collect these DMPs together in a DMP group, you can target them all simultaneously.

Procedure

Step 1 Choose **Digital Signage** from the global navigation or click **Digital Signage** on the dashboard.

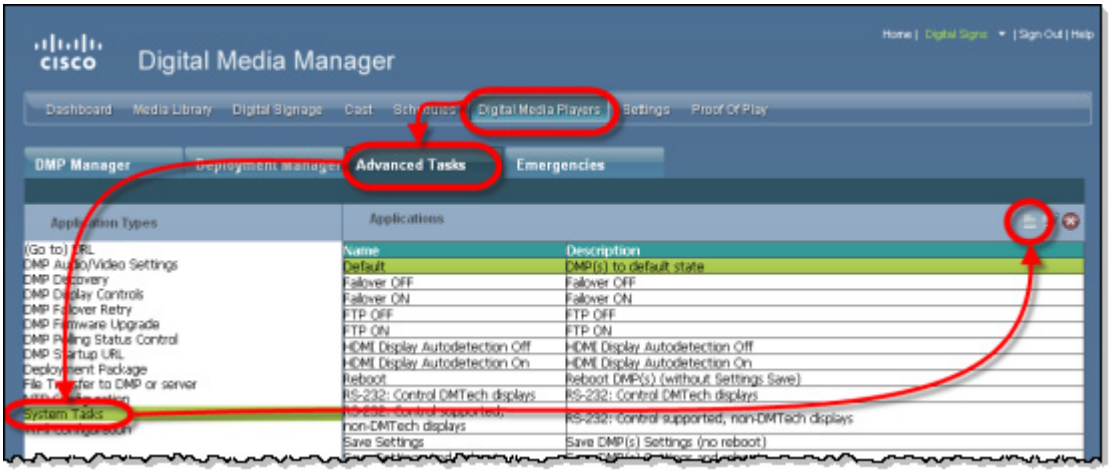


Step 2 Choose **Digital Media Players > Advanced Tasks**.

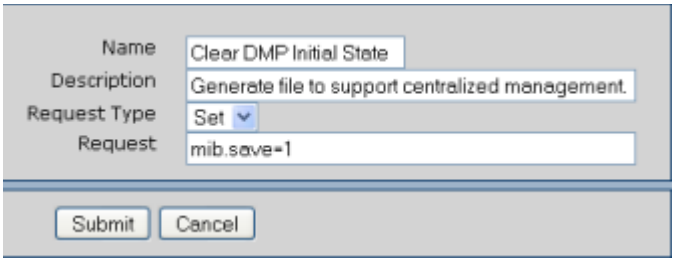
Step 3 Create the advanced task:

a. Click **System Tasks**.

b. Click **Add New Application**.



Step 4 Define and save the new system task:



a. Enter a unique name in the Name field. For example, *Clear DMP Initial State*.

b. Enter a short description in the Description field. For example, *Generate file to support centralized management*.

c. Choose **Set** from the Request Type list.

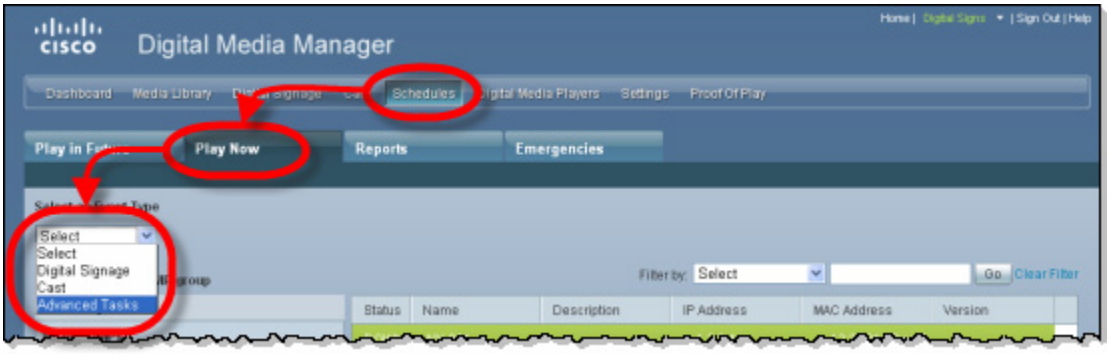
d. Enter **mib.save=1** in the Request field.

e. Click **Submit**.

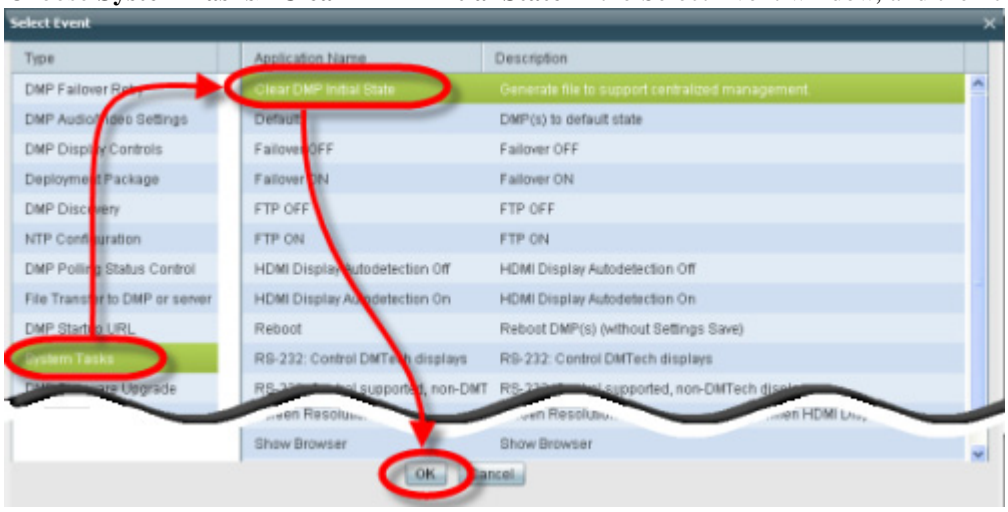
Step 5 Schedule an event to send the task to DMPs that are in the initial state.

a. Choose **Schedules > Play Now**.

b. Choose **Advanced Tasks** from the Select an Event Type list, and then click **Select Advanced Task**



c. Choose **System Tasks> Clear DMP Initial State** in the Select Event window, and then click **OK**.



d. Click the name of a group in the DMP Groups area to see a list of its member DMPs.

e. Click the name of each DMP in the list that should receive the deployment.

f. Click **Submit**, and then click **OK** when the Success message displays.

Step 6 Stop. You have completed this procedure.

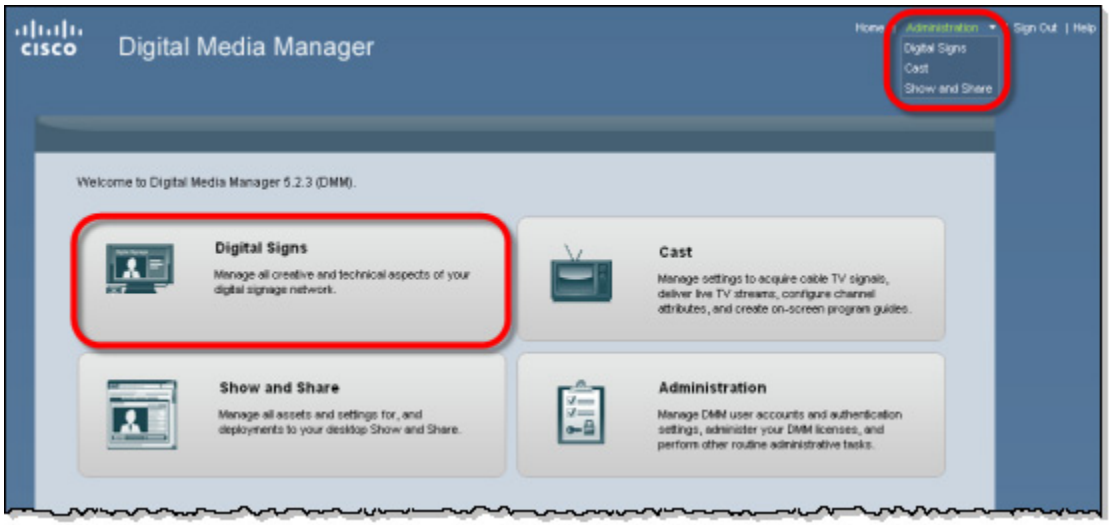
Stop All Applications on DMPs

Before you upgrade DMPs, you must stop all applications by using the DMP Startup URL advanced task.

Note Use the DMP Startup URL advanced task to clear the DMP startup URL and restart the DMP. **Do not use** the Stop All Applications system task.

Procedure

Step 1 Choose **Digital Signage** from the global navigation or click **Digital Signage** on the dashboard.

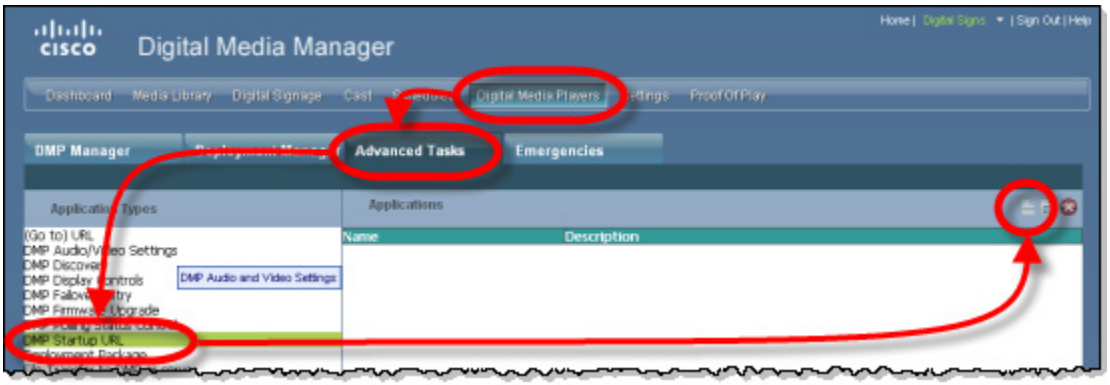


Step 2 Choose **Digital Media Players > Advanced Tasks**.

Step 3 Create the advanced task.

a. Click **DMP Startup URL**.

b. Click **Add New Application**.



c. Enter **Startup URL Empty & Reboot** in the Name and Description fields.

d. Leave empty the Video URL and Browser URL fields.

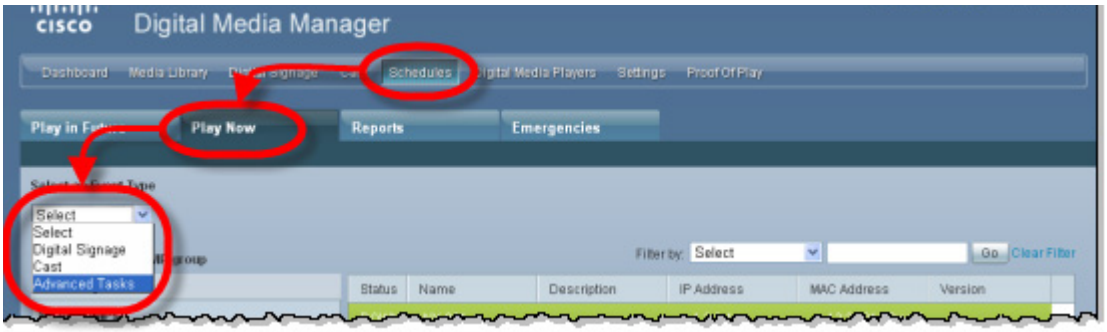
e. Check the **Reboot Necessary** check box.

f. Click **Submit**.

Step 4 Schedule an event to send the task to the DMP.

a. Choose **Schedules > Play Now**.

b. Choose **Advanced Tasks** from the Select an Event Type list, and then click **Select Advanced Task**.



c. Choose **DMP Startup URL > Startup URL Empty & Reboot** in the Select Event window, and then click **OK**.

d. Click the name of a group in the DMP Groups area to see a list of its member DMPs.

e. Click the name of each DMP in the list that should receive the deployment.

f. Click **Submit**, and then click **OK** when the Success message displays.

Step 5 Stop. You have completed this procedure.

Upgrade the Firmware and Root File System on DMP Endpoints

Note It takes approximately 30 minutes to upgrade the firmware and root file system on a DMP. However, while the upgrade is in progress on a DMP 4400G, its behavior might be confusing. It:

1. Shows these three messages in this order:
   -  Burn: *NN%*
   -  Verify: *NN%*
   -  Internal Upgrade Completed.

     (Where *NN* is a percentage value that climbs from 1 to 99.)
2. Restarts after approximately 1 minute.
3. Shows the same three messages as before, in exactly the same sequence.
4. Restarts a second time after approximately 29 minutes.

This occurs because the 4400G must install a small amount of data and restart before it can accept its new firmware and file system.

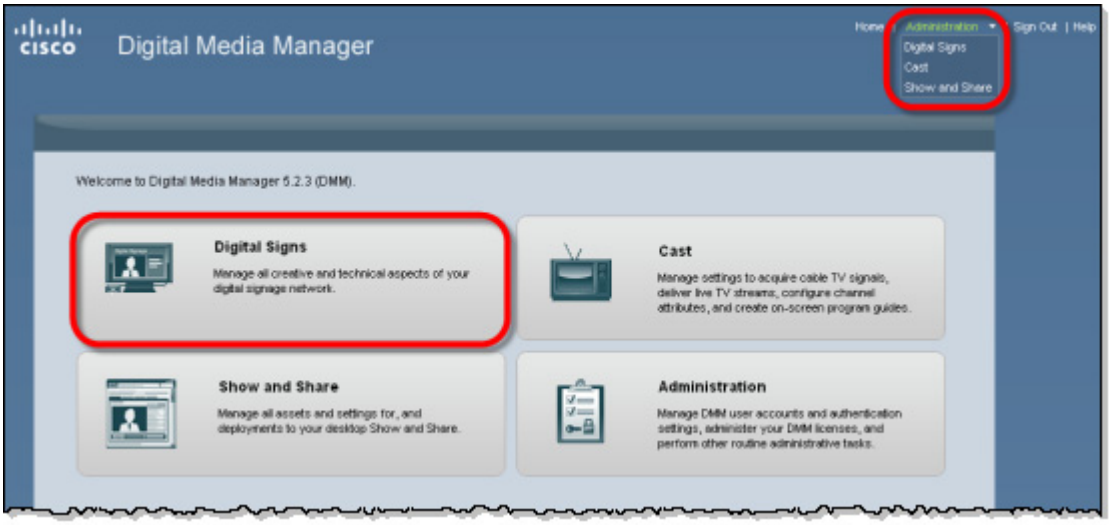
Before You Begin

- If you use ACNS, we recommend that you send DMP firmware files to your ACNS servers and deploy the upgrades as a future event—not an immediate event.
- If you deploy the upgrade directly to your DMPs, we recommend that you upgrade just one DMP initially or upgrade just a small group of DMPs and test the result before you send the firmware to multiple DMPs.
- We recommend that you do not upgrade any more than 5 DMPs at a time and that all upgrades occur outside normal business hours for your organization.

Warning **Make sure that the DMPs do not lose power while they are burning their firmware during an upgrade. If they lose power during this critical period, they will be severely damaged.**

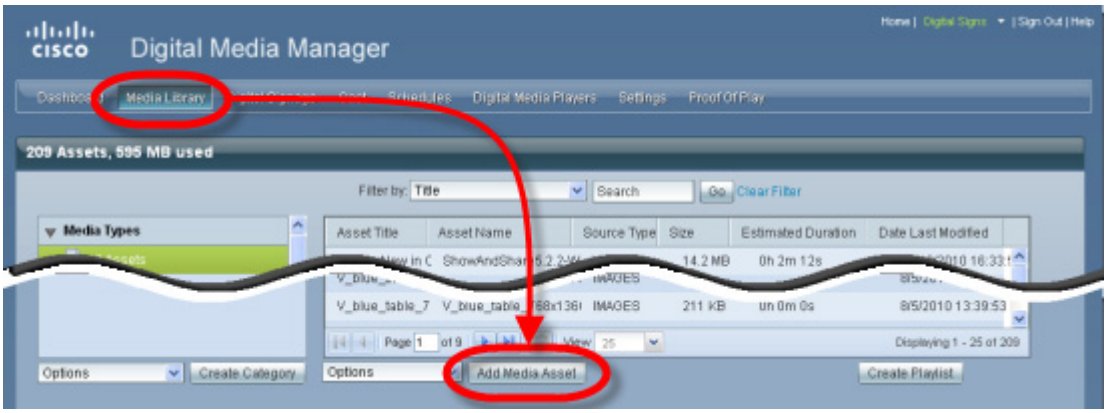
Procedure

Step 1 Choose **Digital Signage** from the global navigation or click **Digital Signage** on the dashboard.



Step 2 Add the firmware image to your media library as an asset. See Obtain the Update Media, page 6, for a list of the DMP firmware images.

a. Choose **Media Library**, and then click **Add Media Asset**.



b. For the source, click **Local File**.

c. Click **Browse**, choose the firmware image from the software upgrade disc or your local file system, and then click **Open**.

d. Enter a meaningful description in the Title field.

e. Uncheck the **Is Kernel Upgrade?** check box.

f. Verify that the file type is **Firmware**, and then click **Save**.

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.

Note You must upload the firmware to the Cisco DMM. Do not link to the firmware using a URL

Step 3 (**Optional**) To verify that the upload succeeded, compare its file size in the Size column to the size of the source file.

Step 4 Create an advanced task for the upgrade.

a. Choose **Digital Media Players > Advanced Tasks**, and then click **DMP Firmware Upgrade**.

b. Click **Add New Application** in the title bar for the Applications area.

c. Enter **DMP_Firmware_Upgrade** in the Name field.

d. Choose from the Media Categories tree the category that contains the firmware.

e. Click the firmware file to highlight it in the Available Content table, and then click **Submit**.

f. Click **Go**.

Step 5 Schedule an event to upgrade the DMPs.

—	To schedule an immediate event ...	To schedule a future event...
a.	Choose **Schedules > Play Now**	Choose **Schedules > Play in Future.**
b.	Choose **Advanced Tasks** from the Select an Event Type list, and then click **Select Advanced Tasks**.	Click **Add an Event**.
c.	Choose **System Tasks > DMP_Firmware_Upgrade** from the Select an Event Type list, and then, click **OK**.	Click **DMP Groups**, and then choose the groups.
d.	Click the name of a DMP group in the DMP Groups object selector to see its member DMPs in the DMP List table.	Click **Digital Signage**, and then choose the presentation or playlist.
e.	Click the name of each DMP in the DMP List table that should receive the deployment.	Specify the date, time, and frequency.
f.	Click **Submit**.	Click **Save**.
g.	Click **OK** when the Success message displays.	Click **Save All** to save the schedule.
h.	—	Click **Publish All** to publish the schedule.

Tip To check the status of an upgrade, deploy to the relevant DMP groups the system task called Upgrade Status.

What to Do Next

After updating your Cisco DMPs, proceed to Upgrade Cisco Digital Media Manager, page 17.

Upgrade Cisco Digital Media Manager

The Cisco Digital Media Manager upgrade can take an hour or more to complete. Make sure you have ample time in your maintenance window to complete the upgrade. During the upgrade, users cannot access the Cisco DMM web interface.

Procedure

Step 1 Insert the upgrade disc into the Cisco DMM appliance disc drive.

Step 2 Log in as **admin** to the Appliance Administration Interface (AAI).

Step 3 In AAI, choose **APPLIANCE_CONTROL > SOFTWARE_UPDATE**.

The system prompts you to insert the update disc.

Step 4 Verify that you have inserted the upgrade disc and press **Enter**.

The appliance reboots. A dialog asks you to confirm that you want to upgrade the appliance.

Step 5 Choose **Yes** to confirm that you want to upgrade the system.

The upgrade process begins.

The Select a default locale menu appears.

Step 6 Use the arrow or number keys to select the default locale and press **Enter**.

Select a default locale that matches the language that the majority of your existing content is or will be in. The default locale causes the content to be indexed according to the language rules (for example, ignoring the word “the” in English or the words “el” or “la” in Spanish).

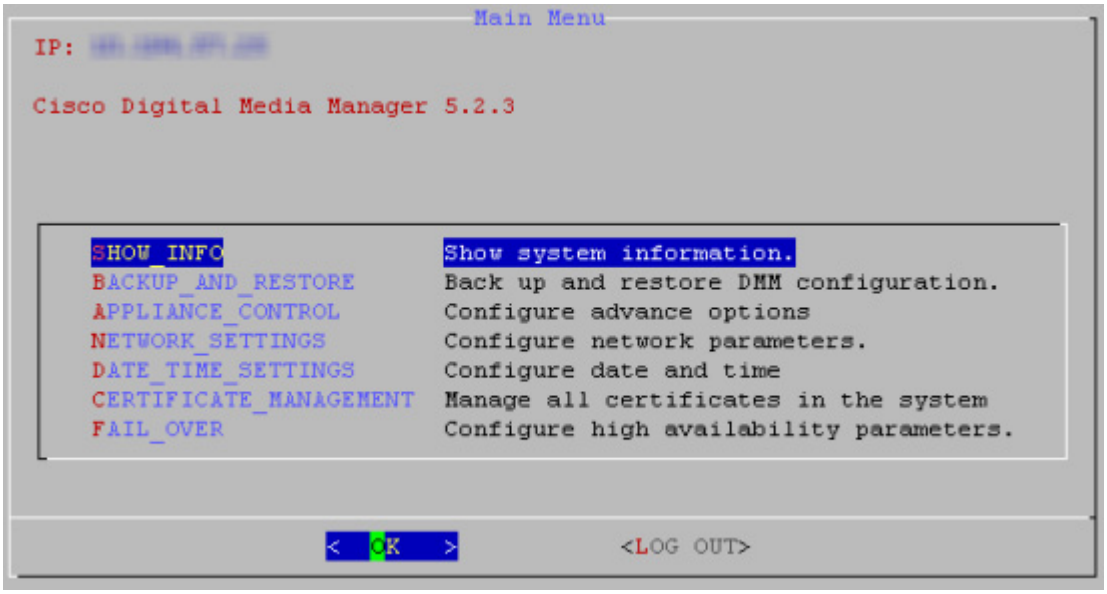
The appliance reboots and again asks you if you want to upgrade the system.

Step 7 Choose **Yes**.

The system installs the 5.2.3 update. If you are prompted to type “yes” to bypass a pause, you can type yes or ignore it; the upgrade will continue automatically after the designated time. After the update is complete, the system reboots and runs post-installation tasks

The upgrade is complete when the AAI login prompt appears.

Step 8 To verify the update, log back into the AAI interface as **admin**. The Main Menu shows the installed software version.



What to Do Next

If you are using Cisco Show and Share, proceed to Upgrade Cisco Show and Share, page 19.

Upgrade Cisco Show and Share

The Cisco Show and Share upgrade can take an hour or more to complete. Make sure you have ample time in your maintenance window to complete the upgrade. During the upgrade, users cannot access the Cisco Show and Share web interface.

Procedure

Step 1 Insert the upgrade disc into the Cisco Show and Share appliance disc drive.

Step 2 Log in as **admin** to the Appliance Administration Interface (AAI).

Step 3 Choose **APPLIANCE_CONTROL > SOFTWARE_UPDATE**.

The system prompts you to insert the update disc.

Step 4 Verify that you have inserted the upgrade disc and press **Enter**.

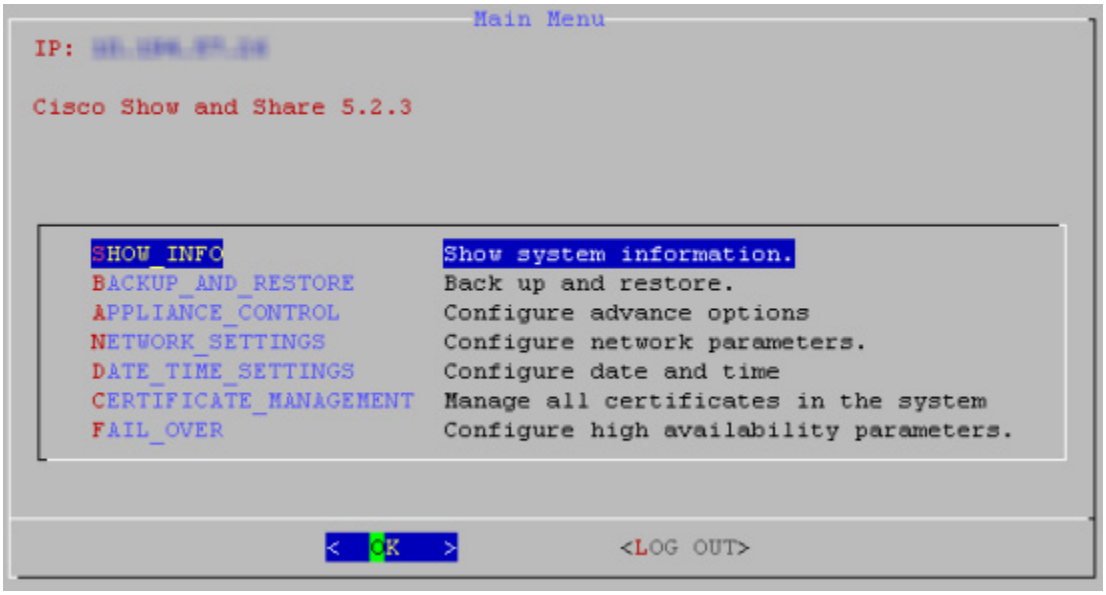
The appliance reboots. A dialog asks you to confirm that you want to upgrade the appliance.

Step 5 Choose **Yes** to confirm that you want to upgrade the system.

The system installs the 5.2.3 update. The system installs the 5.2.3 update. If you are prompted to type "yes" to bypass a pause, you type yes or ignore the prompt; the upgrade will continue automatically after the designated time.

The upgrade is complete when the AAI login prompt appears.

Step 6 To verify the update, log back into the AAI interface as **admin**. The Main Menu shows the installed software version.



What to Do Next

- Verify the System Upgrade, page 20

Verify the System Upgrade

Use this procedure to log into Cisco DMM and Cisco Show and Share for the first time after you upgrade and to verify that the appliances are communicating correctly.

Procedure

Step 1 Point your browser to the Cisco DMM appliance. For example, `http://dmm.example.com:8080`.

Step 2 Log in as **superuser**.

Step 3 When the splash screen appears, confirm that it refers to Digital Media Manager 5.2.3.

Step 4 Point your browser to your Cisco Show and Share server. For example, `http://showandshare.example.com`.

Step 5 Verify that Cisco Show and Share loads.

If Cisco Show and Share does not load, re-pair the devices (see the *Administration Guide for Cisco Digital Media Suite 5.2.x Appliances* on Cisco.com for more information).

Step 6 Stop. You have completed this procedure.

Key Changes in Cisco DMS 5.2.3

LDAP Syntax Enforcement

This DMS-Admin release is more strict than any prior release in its enforcement of proper LDAP syntax. Now, when you specify the "administrator DN" at Administration > Security > Authentication, you must use syntax that conforms exactly to LDIF grammar.

- Proper syntax: `CN=admin1,OU=Administrators,DC=example,DC=com`
- Poor syntax: `EXAMPLE\admin1`

Otherwise, you will observer one of two possible results.

- First-time LDAP configuration—When your DMM appliance already runs DMS 5.2.3 before you ever use poor LDAP syntax here, we show you, the administrator, this error message: "Invalid username or password."
- Upgraded LDAP configuration—When you use and validate poor LDAP syntax here in any earlier DMS-Admin release, before ***upgrading*** to Cisco DMS 5.2.3, we do not repeat the validation process. Therefore—*even though we do not show an error message to anyone, including you*—**LDAP users simply cannot log in.**

In either case, you must correct your LDAP syntax.

Note An LDAP expression must never include a space immediately to either side of a "=" sign. Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

Tip For information about what else is new or changed in this release, see the *Release Notes* on Cisco.com: http://www.cisco.com/en/US/docs/video/digital_media_systems/5_x/5_2/dms/release/notes/dms52rn.html

Learn More About...

To Learn About	Go To
Cisco DMS Components	
Cisco DMS products and technologies	http://cisco.com/go/dms
Cisco DMS technical documentation	http://cisco.com/go/dms/docroadmap
Cisco DMS APIs and SDK	http://cisco.com/go/dms/sdk
Cisco DMS MIB	http://cisco.com/go/dms/mib
Cisco DMS Services	
Cisco Academy of Digital Signage	http://cisco.com/go/dms/ads
Cisco Digital Media Creative Services	http://cisco.com/go/dmcs
Cisco Connected Sports	
Cisco StadiumVision	http://cisco.com/web/strategy/sports/connected_sports.html
Cisco	
Service contracts	http://cisco.com/go/cscc
Standard warranties	http://cisco.com/go/warranty [1]
Technical support	http://cisco.com/go/support
Technical documentation	http://cisco.com/go/techdocs
Product security	http://cisco.com/go/psirt
Sales	http://cisco.com/go/ordering
Obtain Documentation or Submit a Service Request	
For information on obtaining documentation, submitting a service request, and gathering additional information, 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 Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.	

1. Then, for the device that *this guide* describes, click **Cisco 90-Day Limited Hardware Warranty Terms**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2002–2011 Cisco Systems, Inc. All rights reserved.