Upgrade Guide for Cisco Digital Media Suite Release 5.2

Revised: June 24, 2010
OL-15763-03

Warning **Before you upgrade your Cisco Digital Media Suite (Cisco DMS) environment, read this document carefully. It contains crucial information that can help you to ensure a successful upgrade and avoid potentially serious problems.**

Tip This information is updated as needed. Its newest and best revision is on Cisco.com.

You can help us to improve.

Please submit review comments from the feedback form that accompanies this communication on Cisco.com.

Table of Contents

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

About This Guide

This guide explains how to upgrade your Cisco DMS appliances and Cisco Digital Media Player endpoints from Cisco DMS 5.1.*x* to 5.2.

Note See the *Release Notes for Cisco Digital Media Suite 5.2.x* to learn about:

- System requirements
- Caveats
- Product name changes
- New and changed features

CAUTION!
Regarding Cisco DMS Downgrades

Caution **Never upgrade software in your production network until you validate it in your test environment.**

We advise that you back up all records, reports, data, configuration settings, digital assets, and so on before you begin any upgrade. Although your routine creation of such backups is a best practice with any software for any platform, *it is especially important in our case*. Cisco DMS includes multiple hardware platforms, whose reciprocal compatibility requires—among other things—that they all run contemporaneous software releases. Otherwise, their features are not aligned and their data exchanges cannot succeed.

The products that constitute Cisco DMS 5.2.1 support software downgrades to Cisco DMS 5.2.0 but not to any earlier release. The only downgrading method that we support is reinstallation of product software from the Cisco DMS 5.2.0 release—and only if you are licensed to run it—on Cisco equipment that we certify is compatible with the Cisco DMS 5.2.0 release.

If you roll back to software from Cisco DMS 5.2.0, you can restore only the settings that you saved in backups from the Cisco DMS 5.2.0 release.

- All of your Cisco DMS products must run software and firmware from the same, one release.
- Do not run Cisco DMS 5.2.1 and Cisco DMS 5.2.0 simultaneously in your network.
- After a downgrade, you will lose any settings or data that you saved within Cisco DMS 5.2.1.
- After a downgrade, you will lose all bug fixes that Cisco DMS 5.2.1 introduced.
- After a downgrade, you will lose all security enhancements that Cisco DMS 5.2.1 introduced.
- After a downgrade, you will lose all new features and capabilities that Cisco DMS 5.2.1 introduced.
- Downgraded DMPs will lose their static IP address settings, reverting to DHCP.
- You must erase any assets that remain in local storage on downgraded DMPs.
- RSS settings and content from Cisco DMS 5.2.1 will not work in Cisco DMS 5.2.0.

Cisco DMS devices in your production network must all run contemporaneous software. Whenever they do otherwise, you must upgrade or reinstall their software.

Prerequisites for Upgrading

Prerequisites for Upgrade Workflow Tasks to Complete in AAI

Attach a monitor and keyboard to each appliance that you will upgrade. **You must be present with the appliance to insert its upgrade CD or DVD.**

Warning **Do not use an SSH client to complete any upgrade workflow tasks remotely. Otherwise, upgrade fails and your appliance stops responding to SSH and ping.**

Tip Later, after the upgrade is finished, you can log in securely from a remote system by pointing an SSH client (such as PuTTY for Windows or Terminal for Mac OS X) to the fully-qualified domain name that your appliance uses. **Do not point to the appliance IP address.**

Prerequisites for All Other Upgrade Workflow Tasks

See the DMM browser requirements in *Release Notes for Cisco Digital Media Suite 5.2.x*.

Restrictions for Upgrading

We support upgrade to Cisco DMS 5.2 on some Cisco DMS products but not others.

Supported Upgrade Migration Paths

If your devices use any earlier Cisco DMS release than 5.1, you must upgrade to 5.1 before you can upgrade to 5.2. We support only these migration paths:

- **5.0.0 > 5.0.2 > 5.1 > 5.2**
- **5.0.2 > 5.1 > 5.2**
- **5.0.3 > 5.0.2 > 5.1 > 5.2**
- **5.1 > 5.2**

For information about upgrading earlier releases, see the *Upgrade Guide for Cisco Digital Media System* for your release on Cisco.com.

Restrictions

User Authentication

- In DMS-Admin, we do not automatically migrate Microsoft Active Directory attribute-mapping for LDAP-based user authentication services. Part of the upgrade process is to recreate this information.

Digital Media Players

- We do not support Cisco DMS 5.2 on DMP 4300G endpoints. See http://cisco.com/en/US/prod/collateral/video/ps9339/ps6681/Prod_EoL_C51-451180.html
- We no longer support HTTP connections to DMPs. Instead, we require that you use HTTPS.
- We do not retain the Web account username that is configured on DMPs. Instead, we change it to **admin** in every case. In addition, we enforce password security for all users. See http://cisco.com/en/US/docs/video/digital_media_systems/dmp/getting/started/guide/5_2_x/dmp5_2_x.html.
- Cisco TAC cannot provide development or migration support for custom JavaScript applications that you might have developed for digital signage in any earlier release. Custom JavaScript applications are complex and many different methods and styles might lead to the same result.

Show and Share

- We do not automatically migrate live-event video from Video Portal. You must migrate it manually to *Show and Share*.
- We do not migrate on-demand video from Video Portal unless it is already published. You must migrate VoD drafts manually to *Show and Share*.
- We do not migrate user role assignments from Video Portal. You must reassign them in *Show and Share Administration*.
- We no longer support Secure Copy Protocol (SCP), which Video Portal supported. Instead, use SFTP.
- We do not migrate interstitials or programs from Video Portal. Show and Share does not use them.
- Although we do not migrate deployment records (pending or completed), we mark every migrated asset as deployed after we register it on your *Show and Share* appliance.
- We do not migrate any data from Video Portal Reports. However, you can use its export feature to save a local copy of this data before you upgrade your Video Portal appliance.

Supported Upgrades

This section identifies the particular device models and particular software versions that we support for upgrades to Cisco DMS 5.2.

Appliances

- Cisco Media Convergence Server (MCS) appliances on which DMS 5.1 software is installed, licensed, and working correctly.

	Media Convergence Server Chassis			
Appliance Software	**7825-H2**	**7825-H3**	**7835-H1**	**7835-H2**
Cisco Digital Media Manager 5.1	N	N	Y	Y
Cisco Video Portal 5.1 (500 users)	Y	Y	N	N
Cisco Video Portal 5.1 (1,000 users)	N	N	Y	Y

DMPs

- Cisco Digital Media Player 4305G and 4400G endpoints that use firmware version 5.1.

About the Upgrade Process

The upgrade process to Cisco DMS 5.2 results in updates to these software components:

- *Cisco Digital Media Manager* (DMM) software, including:
  - *Cisco Digital Signs* and its *Digital Media Designer* tool.
  - *Cisco Cast*.
  - *DMS-Admin* and its *SNMP Notifications* module.
  - *Cisco Hinter* software versions for Microsoft Windows and Linux.
- *Cisco Show and Share* software, including:
  - *Cisco Show and Share Administration* and its *Live Events* module.
  - *Cisco Show and Share Reports*.
- *Cisco Digital Media Player Device Manager* (DMPDM).
- The *Appliance Administration Interface* (AAI) command shell.

The upgrade process requires that you complete the following tasks in the order shown, as needed for your deployment:

—	Task	Reference
Step 1	Prepare for the upgrade. **a.** Learn about requirements, prerequisites, and changes in this release. **b.** Obtain upgrade CDs, new DMS 5.2 licenses (if you have purchased features for this release that you were not licensed to use previously), and DMP firmware.	• *Release Notes for Cisco DMS 5.2.x on Cisco.com* • Prerequisites for Upgrading, page 3 • Restrictions for Upgrading, page 3 • Prepare to Upgrade, page 12
Step 2	Save local copies of any assets that you stored on your Video Portal appliance. They will be deleted otherwise.	Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance, page 16
Step 3	Upgrade your DMPs. **a.** Stop all applications on DMPs. **b.** Upgrade the kernel on DMP 4305G endpoints only. **c.** Upgrade the firmware and root file system on all DMPs.	Upgrade Your DMPs, page 19
Step 4	Upgrade your Digital Media Manager appliance. **Warning** **Have you upgraded your DMPs?** • Make note of or save a copy of your LDAP attribute-mapping definitions, if you use Active Directory to authenticate users. • Back up the appliance. • Install DMM 5.2 software. • Verify licenses and configuration. • Recreate your LDAP attribute-mapping definitions, if you use Active Directory to authenticate users. • For Cisco ACNS deployments, provision assets. • Resubmit presentations and playlists to DMPs.	Upgrade Digital Media Manager Appliances, page 31
Step 5	Upgrade your *Show and Share* appliance. • Back up the appliance. • Install *Show and Share* 5.2 software. • Reassign user roles in *Show and Share*. They are not migrated from Video Portal.	Upgrade Video Portal Appliances to Run Show and Share, page 36
Step 6	Pair your appliances.	Pair Your Cisco DMS 5.2 Appliances, page 39

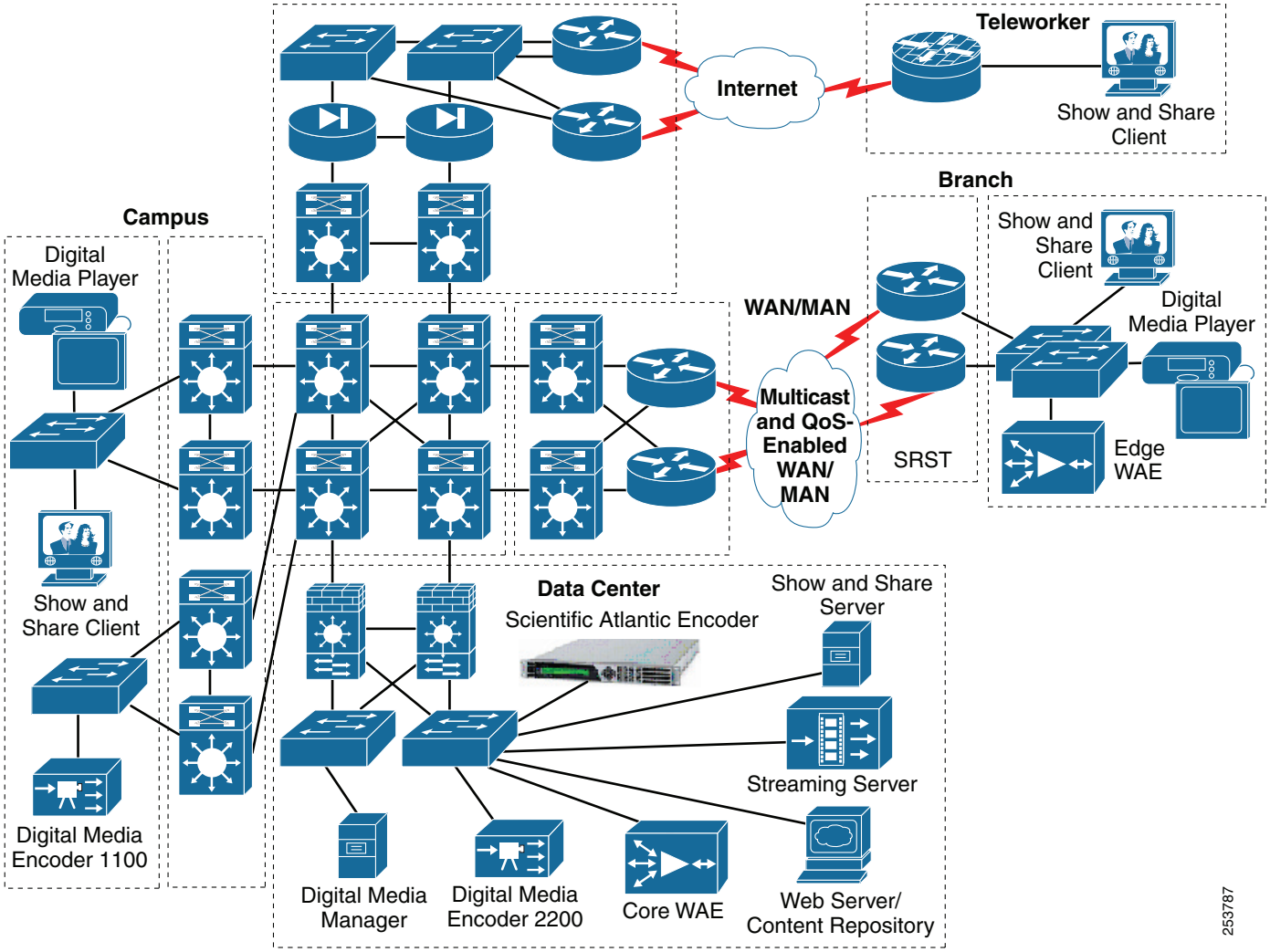
PIN Architecture Considerations

Figure 1 on page 8 illustrates the Cisco-validated *places in the network* (PIN) architecture for Cisco DMS 5.2.*x*.

Note We intend that your Cisco DMS server appliances should share one physical location. Failing this, they should at least operate together within one network segment.

- We do not support any deployment whose network design inserts a firewall between your Cisco DMS server appliances.
- We recommend that you run Cisco DMS server appliances in your data center.

Figure 1 Places in the Network Architecture Design



PIN Design Considerations for a Data Center

The data center is home to the computational power, storage, and applications necessary to support an enterprise business. All content is sourced from, or passes through, the data center. It is central to IT architecture. The data center holds the core Cisco DMS components and is the central point of content distribution.

You can store VoD assets in the data center and distribute them through a content delivery network. Storage requirements can become substantial as video content moves more toward high definition. Direct attached storage or SANs can be used to provide capacity and redundancy benefits.

For more information, see *Design Zone for the Data Center* at http://cisco.com/go/designzone.

PIN Design Considerations for a Campus

Multicast enablement is one of the primary design considerations for a campus network. Digital Signs and Cast use multicast to deliver live video to DMP endpoints. DMPs support IGMPv3.

Tip We recommend that you use *source-specific multicast* (SSM) whenever possible. With SSM, multicast clients must specify the multicast source explicitly. SSM does not use rendezvous points.

As needed, you can use technologies such as VRF-Lite to segment or virtualize video traffic within a campus network.

For more information, see *Design Zone for Campus* at http://cisco.com/go/designzone.

PIN Design Considerations for Branch Locations

You can design branch locations with any number of WAN connections. You achieve the greatest network availability, however, when you combine multiple WAN connections with redundant Cisco Integrated Services Routers (ISRs). Dual links and ISRs facilitate your use of additional optimization services, such as *performance routing* (PfR).

Beyond this, you can integrate content distribution and optimization services by running Cisco WAAS or Cisco ACNS on Cisco WAE network modules.

- Single-Tier Branch Architecture, page 9
- Dual-Tier Branch Architecture, page 10

Single-Tier Branch Architecture

Figure 2 on page 10 illustrates a single-tier branch.

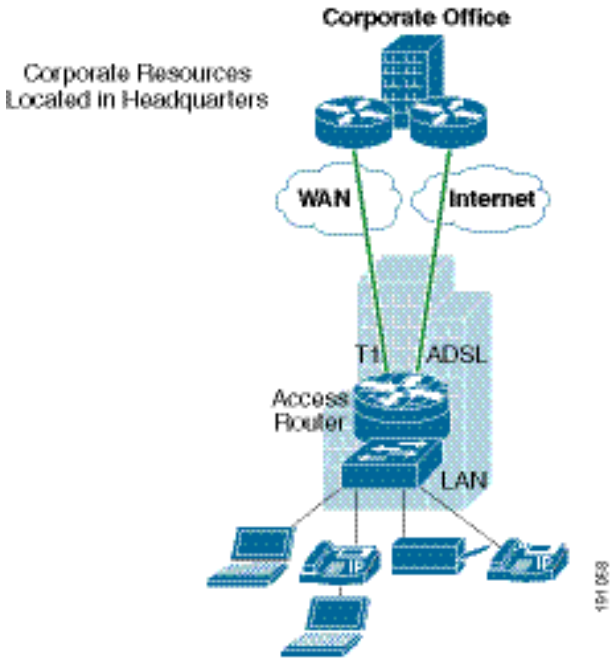
We recommend a single-tier branch architecture for smaller enterprise branches. This profile is optimal for a branch with a small user base and little or no need for platform redundancy. It consists of an ISR as the access router, incorporating an Integrated EtherSwitch network module for LAN and WAN connectivity. High availability is achieved through a T1 link with an ADSL backup.

With this profile, smaller branches can provide multiple services from a single platform. Furthermore, use of this cost-effective profile leaves you with only one device to manage on-site at a branch location.

However, network resiliency and capacity planning are not robust in this profile. Any a single-platform solution introduces a common point of failure. Without redundancy, any network bottleneck or outage can affect users.

This design also limits user capacity to the number of LAN ports that your ISR platforms can support. To accomodate and plan ahead for future headcount at a branch location, we recommend that you use an external desktop switch or other router platform to obtain additional slot capacity.

Figure 2 Single Tier Branch Architecture



Dual-Tier Branch Architecture

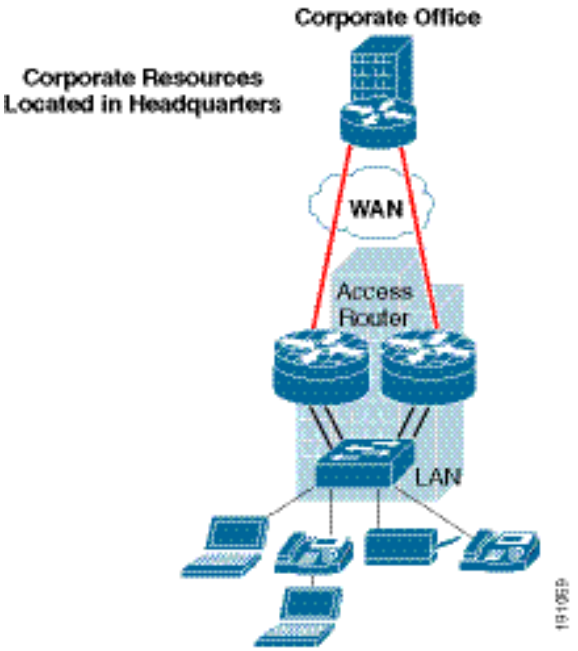
Figure 3 on page 11 illustrates a dual-tier branch.

We modeled this profile on legacy branch networks that continue to run. It adds advanced services to a branch network without imposing a massive upgrade or a complete network redesign.

This profile connects two ISR access routers to an external switch. Dual WAN links and hardware redundancy support greater availability than the single-tier branch profile supports. Yet, this increased capacity comes with new equipment costs and a more complex branch topology to manage.

Typically, most enterprise branch networks are dual-tier.

Figure 3 Dual Tier Branch Architecture



For more information about the branch design, see the Design Zone for Branch at the following URL: http://www.cisco.com/go/designzone.

PIN Design Considerations for a WAN or MAN

Your WAN constrains which Cisco DMS services are available to your branch locations.

- To transmit live video to branch-site DMPs for playback via Cisco Digital Signs or Cisco Cast, your WAN must be high speed multicast-enabled.
- You can transmit live video to Cisco Show and Share clients over a lower speed, non-multicast WAN.

It is essential that you configure *quality-of service* (QoS) on the WAN to ensure the delivery of any critical content. Cisco DMS depends upon a QoS-enabled WAN to guarantee delivery of live streaming video that satisfied baseline requirements for latency, jitter, and loss.

For more information, see *Design Zone for MAN/WAN* at http://cisco.com/go/designzone.

How to Upgrade

To upgrade to Cisco DMS 5.2, complete the following procedures in the order shown, as needed for your deployment:

1. Prepare to Upgrade, page 12
2. Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance, page 16
3. Export Any Important Records from Video Portal Reports, page 17
4. Prepare to Migrate Content Categories, page 18

5. Upgrade Your DMPs, page 19
6. Upgrade Digital Media Manager Appliances, page 31
7. Install DMS 5.2 Licenses, page 36
8. Upgrade Video Portal Appliances to Run Show and Share, page 36
9. Pair Your Cisco DMS 5.2 Appliances, page 39
10. After Your Appliances are Paired, page 40
11. Configure Show and Share 5.2, page 49

Prepare to Upgrade

To prepare to upgrade, complete the following procedures, as needed for your deployment:

- Obtain Cisco DMS 5.2 Licenses, page 12
- Obtain the CDs or DVDs to Upgrade Cisco DMS Appliances, page 14
- Obtain the Files to Upgrade DMPs, page 15

Obtain Cisco DMS 5.2 Licenses

The upgrade process migrates Cisco DMS 5.1 licenses automatically. If you purchased additional Cisco DMS 5.2 features, use this procedure to obtain the licenses.

If you did not purchase new licenses or do not plan to install new licenses immediately after upgrade, proceed to "Obtain the CDs or DVDs to Upgrade Cisco DMS Appliances" section on page 14.

Before You Begin

- Obtain the Sales Order (SO) numbers that Cisco used when you originally purchased the Cisco DMS software modules and DMP license packs that are to be upgraded.

Procedure

Step 1 Send an email message to dms-softwarekeys@cisco.com that includes the following information:

- Cisco sales order number for your DMM purchase.
- Ten-character DMM server appliance serial number.
- Your email address, to which we will email the license.
- Name of your organization and your department.
- Software modules with respective Cisco sales order number:

If you recently purchased Digital Media Manager, any or all of these:

- SNMP Notifications module
- *Cisco Digital Signs* module
- Digital Media Player license packs for DMM in increments of 10, 100, or 1000
- *Cisco Cast* module

If you recently purchased Show and Share, at least the first of these:

- *Cisco Show and Share* (with, implicitly, *Cisco Show and Share Reports*)
- Live Event Module

Step 2 Save a copy of each Cisco DMS 5.2 license that you receive by email from Cisco.

Step 3 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Obtain the CDs or DVDs to Upgrade Cisco DMS Appliances" section on page 14.

Obtain the CDs or DVDs to Upgrade Cisco DMS Appliances

Procedure

Step 1 Do one of the following to obtain upgrade CDs or DVDs for this Cisco DMS release:

- If you have a valid SAS contract for an earlier Cisco DMS release, which entitles you to upgrade at no additional cost, go to http://www.cisco.com/upgrade to use the Product Upgrade Tool. Enter your SAS contract number and place an order for the CDs or DVDs that you are entitled to receive. Cisco will process your order and ship the upgrade discs to you.
- **If you do not have** a valid SAS contract for an earlier Cisco DMS release, you must pay to upgrade to this release. Cisco will process your order and ship the upgrade discs to you:

Software License Upgrades	Part Numbers
Upgrade Cisco DMS	
Digital Media Mgr V5.1-V5.2 Perptl. SW Lic. Update	DMM51-U52-K9
Upgrade Cisco Show and Share	
Show and Share V5-V5.2 Perptl SW Lic. Update for Video Portal 500	DV-WKGP-U52-K9
Show and Share V5-V5.2 Perptl SW Lic. Update for Video Portal 1000	DV-ENT-U52-K9
Upgrade Cisco Digital Media Players	
Digital Media Player V5-V5.2 Perptl. SW Update	DMP-SW52-U-K9

Step 2 (**Optional**) Purchase any additional licenses, including those for features that you did not use previously.

Software License Add-Ons	Part Numbers
SNMP Notifications Module for Cisco DMS	
DMM SNMP Module V5.2 Perptl. SW Lic., Spare	DMM-SNMP52-K9=
Cisco Show and Share	
DMM Show and Share Module V5.2 Perptl. SW Lic., Spare	DMM-DVM52-K9=
DMM Show and Share Live Event Module V5.2 Pptl. SW Lic., Spare	DMM-LEM52-K9=
Show and Share Feature License for Up To 10 Authors, Spare	DVAUTHOR-FL-10=
Show and Share Feature License for Up To 50 Authors, Spare	DVAUTHOR-FL-50=
Show and Share Feature License for Up To 500 Authors, Spare	DVAUTHOR-FL-500=
Show and Share Feature License for Up To 1000 Authors, Spare	DVAUTHOR-FL-1000=
Cisco Digital Signs	
DMM Digital Signs Module V5.2 Perptl. SW Lic., Spare	DMM-SIGNSM52-K9=
DMM License for Distributed Proof of Play, 1 collector,Spare	DMM-DIST-POP52=

Software License Add-Ons (continued)	**Part Numbers**
Cisco Cast	
DMM Cast Module V5.2 Perptl. SW Lic., Spare	DMM-CAST52-K9=
Centralized Management of Cisco Digital Media Players	
DMM Feature License for Up to 10 DMPs	DMP-FL-10=
DMM Feature License for Up to 50 DMPs	DMP-FL-50=
DMM Feature License for Up to 500 DMPs	DMP-FL-500=
DMM Feature License for Up to 1000 DMPs	DMP-FL-1000=

Step 3 Locate the appliance upgrade installation utilities that you will use:

Digital Media Manager 5.2	**Show and Share 5.2**
The filename is **DMS-5.2.0.25.iso**.	The filename is **SS-5.2.0.20.iso**.

Step 4 Stop. You have completed this procedure.

What to Do Next

Proceed to one of the following sections:

- If you use *Cisco Digital Signs* or *Cisco Cast*, proceed to the "Obtain the Files to Upgrade DMPs" section on page 15.
- If you use *Cisco Show and Share*, proceed to the "Upgrade Digital Media Manager Appliances" section on page 31.

Obtain the Files to Upgrade DMPs

If you do not use *Cisco Digital Signs* or *Cisco Cast*, proceed to the "Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance" section on page 16.

Procedure

Step 1 Do one of the following to obtain upgrade CDs or DVDs for this Cisco DMS release:

- If you have a valid SAS contract for an earlier Cisco DMS release, which entitles you to upgrade at no additional cost, go to http://www.cisco.com/upgrade to use the Product Upgrade Tool. Enter your SAS contract number and place an order for the CDsor DVDs that you are entitled to receive. Cisco will process your order and ship the discs to you.
- Pay to upgrade to this release. Cisco will process your order and ship the upgrade discs to you.

Step 2 Locate the firmware and kernel files to upgrade each DMP model type that you use:

DMP 4305G	DMP 4400G
• The firmware filename is **5.2.0_FCS_4305.fwimg**. • The kernel filename is **DMPkernel_A2_4305.tivella**.	• The firmware filename is **5.2.0_FCS_4400.fwimg**.

Step 3 Stop. You have completed this procedure.

Note **Do not install these files now.** Instead. you will install them at a later stage in the upgrade process.

What to Do Next

- Proceed to the "Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance" section on page 16.

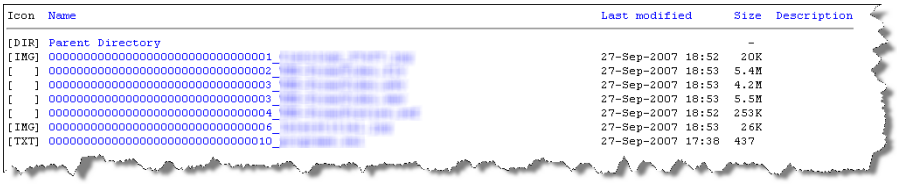
Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance

Caution We did not support storage of content files on Video Portal appliances in Cisco DMS 5.1.*x* and earlier releases. Therefore, if you deployed any files to your appliance in any earlier release, this upgrade **will delete all of these files automatically**.

Unless you complete this procedure, you will not be able to retrieve or use them after they are deleted.

Have you kept any other copies of files that you stored on a Cisco Video Portal appliance, which you will now upgrade to run *Show and Share*? If not, 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, as shown in Figure 4. Note that there was one URL for each media type that your Video Portal supported.

Figure 4 Example of HTTP URLs



Use this procedure to learn which HTTP URLs on your 5.1.*x* appliance will show directory listings.

Procedure

Step 1 Choose **Video Portal** from the 5.1.*x* global navigation.

Step 2 Choose **Setup > Deployment Locations**.

Step 3 Copy the URLs from the Root URL Path field for each media type that your Cisco Video Portal has supported.

Step 4 Load in your browser the directory listing for one media type.

a. Press **Ctrl-L** to use the browser field where you enter URLs.

b. Press **Ctrl-V** to paste the corresponding URL into the browser field.

c. Press **Enter** to load the directory listing in your browser.

Step 5 Download each file that you should save.

Step 6 Edit each filename to delete its numeric prefix.

Caution We recommend that you to call Cisco TAC **before** you install this upgrade, if you:

- Have not kept any other copies of these files.
- Cannot use the directory listings method to download them.
- Cannot afford to lose them.

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

Step 7 To prevent any future upgrades from deleting the files, we recommend that you do the following:

a. Choose and prepare a dedicated storage server to host your content files.

b. Complete the Cisco Video Portal appliance upgrade process in the "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.

c. Reconfigure the file storage locations in *Show and Share Administration*, as described in *User Guide for Cisco Show and Share Administration 5.2.x*.

d. Use *Show and Share Administration* to store your content files on a dedicated storage server.

Step 8 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Export Any Important Records from Video Portal Reports" section on page 17

Export Any Important Records from Video Portal Reports

We do not migrate any records or data from Video Portal Reports when you upgrade. To save a local copy of this information, you must export it.

Before You Begin

- Video Portal Reports uses scalable vector graphics in its charting. For browser requirements to use Video Portal Reports, see *Release Notes for Cisco Digital Media System 5.1.x* on Cisco.com.

Procedure

Step 1 To see a report, point your browser to **http://**<*video_portal_IP_address*>**:8080/CvpMetrics/**.

Step 2 If user authentication is enabled and Video Portal Reports prompts you to log in, enter your login credentials and log in.

Tip Does an error message tell you, "You entered an invalid username or password, or your password has expired. Please try again."? If so, we recommend that you contact the administrator for your LDAP server. Your Video Portal Reports user account might be derived from an LDAP user account that forces you to use a unique and dynamically generated password each time that you log in.

Step 3 Click the link that loads a particular type of report.

Step 4 Enter or choose the range of dates that the report should describe.

Step 5 Use the "Export" feature to save this information in a local file.

Step 6 Repeat as needed.

Step 7 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Prepare to Migrate Content Categories" section on page 18

Prepare to Migrate Content Categories

Ordinarily, we migrate all of your defined content categories automatically from Video Portal to *Show and Share*. However, a "corner case" might block this migration.

Procedure

Step 1 Check that at least one video on your Video Portal uses viewership permissions.

Step 2 If not even one video on your Video Portal has any permissions defined that specify who can view it:

a. Upload a video.

b. Assign viewership permissions for it.

c. Save your work.

Step 3 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Upgrade Your DMPs" section on page 19

Upgrade Your DMPs

Caution **Because Cisco DMS 5.2 secures all communication between DMPs and your DMM appliance, you must upgrade your DMPs before you upgrade your DMM appliance.** Otherwise, you cannot upgrade your DMPs at all and are prevented from managing them centrally.

Until you upgrade the firmware and kernel versions for your DMPs to 5.2, they are not compatible with all features of Digital Signs 5.2. After you upgrade your DMPs, the older version of DMM is prevented temporarily from managing them. However, as soon as you upgrade a DMM appliance to 5.2, its device inventory describes the same DMPs that you managed centrally in DMM-DSM 5.1.

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

1. Force DMPs From Their 'Initial' State, As Needed, page 19
2. Stop All Applications on DMPs, page 22.
3. Upgrade the Kernel on DMP 4305G Endpoints Only, page 24.
4. Upgrade the Firmware and Root File System on All DMP Endpoints (4305G and 4400G), page 27.
5. Restart Your DMM Appliance, page 31.

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 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. Therefore, you should force any such DMPs out of their initial state now.

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

Procedure

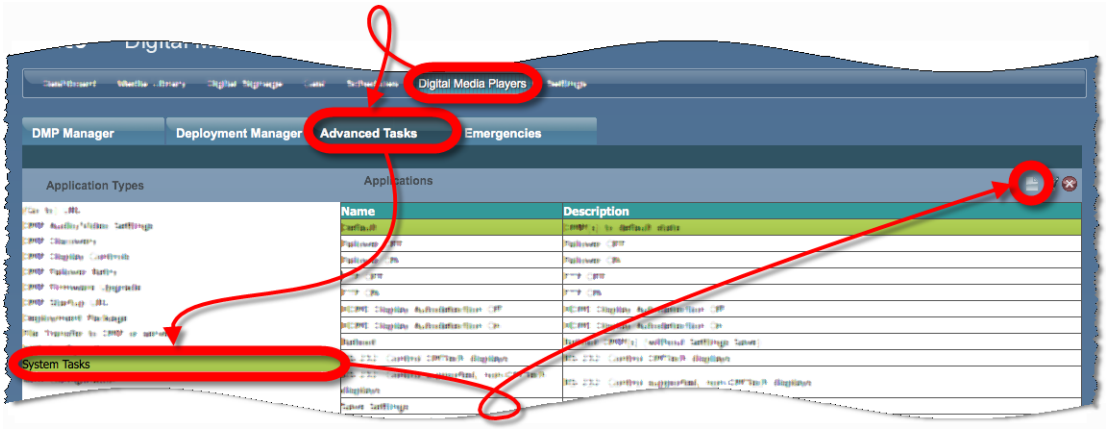
Step 1 Choose **Digital Signage** from the global navigation or click **Digital Signage** on the dashboard.

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.

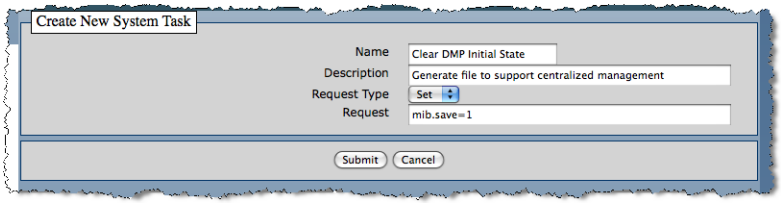
a. Enter a unique name in the Name field. For example, *Clear DMP Initial State*.

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**.

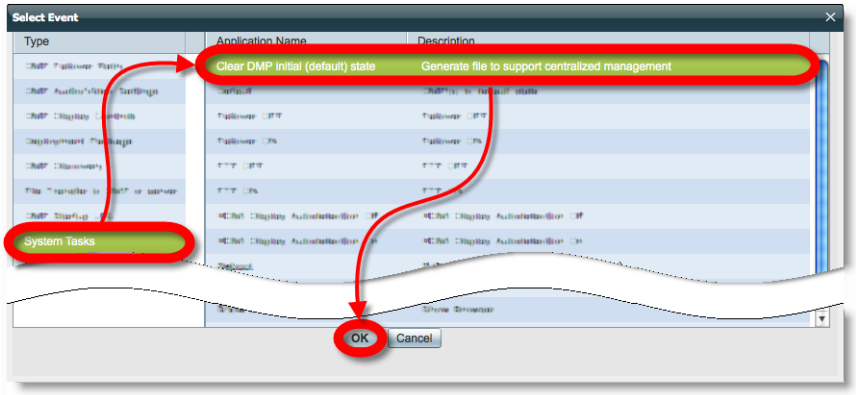


Step 5 Schedule an event to send the task to DMPs that are in the initial state.

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.

What to Do Next

- Proceed to the "Stop All Applications on DMPs" section on page 22.

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.

Before You Begin

Because you cannot submit a task to a DMP with user account credentials that are different from those specified in DMM-DSM 5.1:

- Ensure that the credentials on the DMPs that you are upgrading match the credentials that are specified in DMM-DSM 5.1 under Settings > Server Settings.
- If the credentials do not match, use DMPDM to log in to these DMPs and manually change the User Names and Passwords to match the credentials that are configured in DMM-DSM 5.1. Alternatively, see the quick start guide for a DMP to learn how you can change these login credentials simultaneously for all of the DMPs that you manage.

Procedure

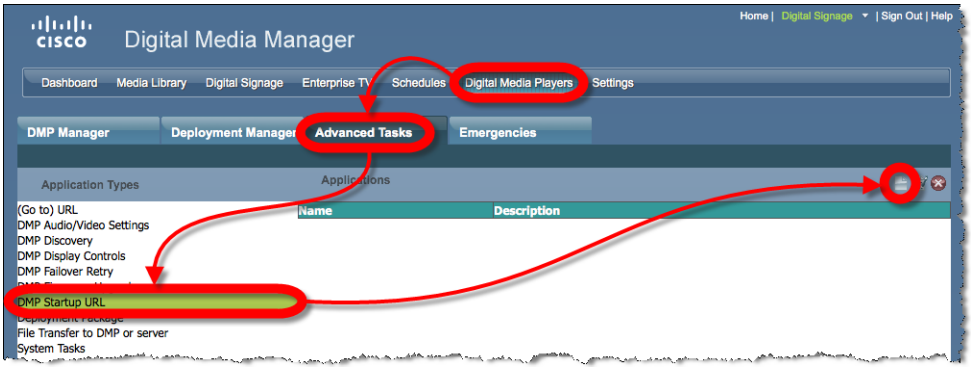
Step 1 Choose **Digital Signage** from the global navigation or click **Digital Signage** on the dashboard.

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.

What to Do Next

- If your network contains any DMP 4305G endpoints, proceed to the "Upgrade the Kernel on DMP 4305G Endpoints Only" section on page 24.
- Otherwise, proceed to the "Upgrade the Firmware and Root File System on All DMP Endpoints (4305G and 4400G)" section on page 27.

Upgrade the Kernel on DMP 4305G Endpoints Only

You must upgrade the kernel before you upgrade the firmware on a DMP 4305G.

Before You Begin

- Stop all applications on affected DMPs. See the "Stop All Applications on DMPs" section on page 22.
- If you use ACNS, we recommend that you send DMP kernel 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 kernel to multiple DMPs.
- We recommend that you do not upgrade any more than 20 DMPs at a time and that all upgrades occur outside normal business hours for your organization.

Warning **Make sure that the DMPs never lose power while they are burning their kernel during an upgrade. If they lose power during this critical period, they will be severely damaged.**

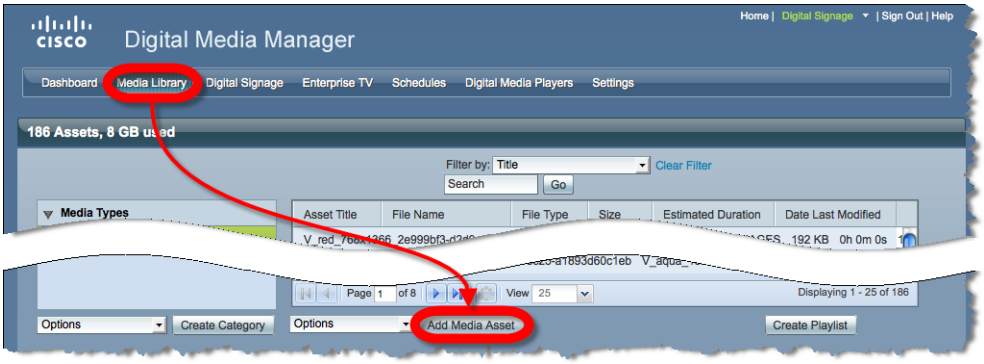
Note **We do not support** upgrade to Cisco DMS 5.2 on Cisco DMP 4300G endpoints. See http://cisco.com/en/US/prod/collateral/video/ps9339/ps6681/Prod_EoL_C51-451180.html.

Procedure

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

Step 2 Add the kernel image to your media library as an asset.

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



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

c. Click **Browse**, choose the kernel file from the software upgrade CD, and then click **Open**.

d. Enter a meaningful description in the Title field.

e. Check 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 kernel file has been added in the table that the page shows.

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

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_Kernel_Upgrade** in the Name field.

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

e. Click the kernel 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_Kernel_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.

Step 6 (**Optional**) Verify that the kernel was upgraded.

a. Point your browser to **https://**<*DMP_IP_Address*>**/get_param?p=sinfo.version**.

b. Check that the returned result says exactly this:

```
sinfo.version   T_STRING        Linux version 2.4.22 (compiler@compiler) (gcc version
3.3.2) #1 Wed Dec 9 22:10:26 PST 2009
```

Step 7 Stop. You have completed this procedure.

Upgrade the Firmware and Root File System on All DMP Endpoints (4305G and 4400G)

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

Warning **Upgrade the kernel on all DMP 4305G endpoints. See the "Upgrade the Kernel on DMP 4305G Endpoints Only" section on page 24.**

- Stop all applications on affected DMPs. See the "Stop All Applications on DMPs" section on page 22.
- 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 20 DMPs at a time and that all upgrades occur outside normal business hours for your organization.

Warning **Make sure that the 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.**

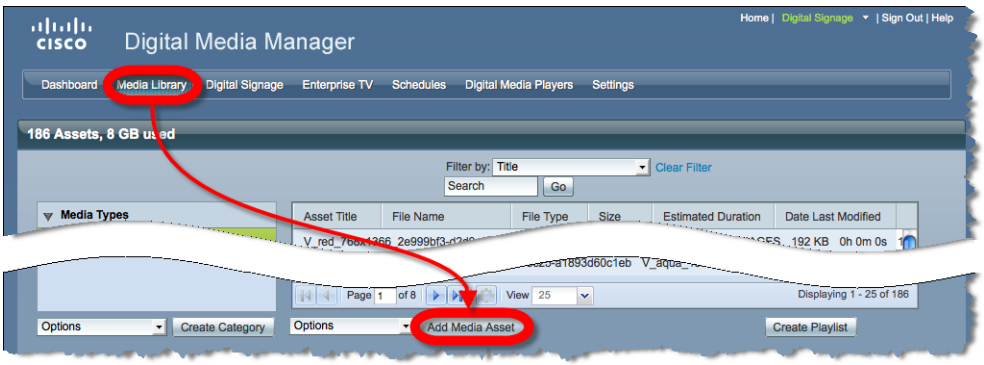
Note **We do not support** upgrade to Cisco DMS 5.2 on Cisco DMP 4300G endpoints. See http://cisco.com/en/US/prod/collateral/video/ps9339/ps6681/Prod_EoL_C51-451180.html.

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.

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 CD, 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**.

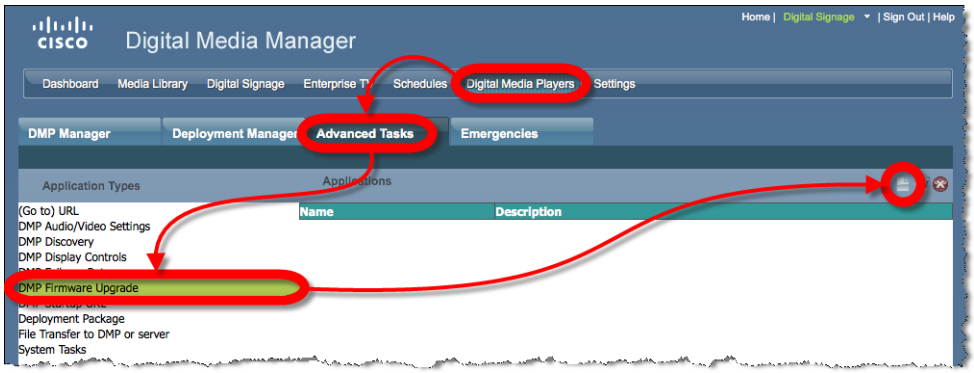
Do not click any button or move away from this page in your browser until the upload is finished. After it is finished, the page refreshes automatically. You should see that a description of the firmware file has been added in the table that the page shows.

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

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.

Step 6 (**Optional**) After the upgrade is completed and you refresh your browser, verify that the DMP List area on the DMP Manager tab indicates 5.2 in the Version column for the DMPs that you upgraded.

Step 7 Stop. You have completed this procedure.

Note

- Until you upgrade your DMM appliance to 5.2, the appliance cannot centrally manage these upgraded DMPs.
- The DMP Web account username, which you use when you log in to DMPDM, is changed automatically when you upgrade a DMP to 5.2. The new username for this account is **admin**. We enforce strong passwords automatically for this account and reject weak passwords.
- After you upgrade a DMP to 5.2, it uses HTTPS instead of HTTP. However, your DMP self-signs its own SSL certificate. All browser connections and API calls to your DMP must accept this certificate one time for every new session.

What to Do Next

- Proceed to the "Restart Your DMM Appliance" section on page 31.

Configure Syslog on DMPs, Even if You Will Not Use It

In this release, DMPs

Procedure

Step 1 Do one of the following

- Do you use DMPDM to manage each DMP in isolation?

  When you will use DMPDM to configure one DMP at a time

  a. x

  b. x

  c. x

- Do you use DMM to centrally manage DMPs?

  When you will use Digital Signs to configure multiple DMPs simulataneously

  Create and deploy an advanced task that delivers this payload:

```
https://admin:<password>@<DMP_IP_address>:7777/
set_param?
init.syslog_poll_int=3000&
init.syslog_collector=<routable_IP_address_or_DMP_loopback_address>&
init.syslog=off&
mib.save=1&
mng.reboot=1
```

d(Optional) If you turned syslog On temporarily, merely so you could configure it, turn it back Off. Then, save the changed settings again and restart your DMP again.

Restart Your DMM Appliance

Procedure

Step 1 Restart your DMM appliance.

Step 2 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Upgrade Digital Media Manager Appliances" section on page 31.

Upgrade Digital Media Manager Appliances

To upgrade DMM appliances, complete the following procedures in the order shown, as needed:

1. Back Up Digital Media Manager Appliances, page 31
2. Unmount All WAAS Shares, page 32
3. Install the Software Upgrade for Digital Media Manager, page 32
4. Log in to DMS-Admin for the First Time and Verify the Software Upgrade, page 34
5. Verify That Existing Licenses Upgraded Successfully, page 35

Back Up Digital Media Manager Appliances

Use this procedure to back up the settings, configurations, and metadata for your DMM appliance.

Caution We recommend that you back up only to a USB device. This method preserves your data if the upgrade fails. Backups do not contain the media files or other assets.

Procedure

Step 1 Log in as **admin** to Appliance Administration Interface (AAI).

Step 2 Choose **DMM_CONTROL > BACKUP_DMM > USB**.

Warning **After the backup is saved, disconnect any USB drive that is connected to your appliance. Otherwise, the USB drive is REFORMATTED and ERASED.**

FURTHERMORE, UPGRADE FAILS.

You cannot restore your appliance from a backup that you have erased.

DO NOT IGNORE THIS WARNING!

Step 3 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Unmount All WAAS Shares" section on page 32.

Unmount All WAAS Shares

Procedure

Step 1 Unmount all WAAS file shares before you upgrade Cisco DMS appliances.

Step 2 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Install the Software Upgrade for Digital Media Manager" section on page 32.

Install the Software Upgrade for Digital Media Manager

Caution Upgrading requires that the appliance be restarted twice, automatically. After the first restart is finished, a system prompt asks, "Do you want to proceed with upgrade?"

Answer **Yes**.

Otherwise, if you answer No:

- You prevent the second restart, which causes the appliance to become unstable.
- Another system prompt appears, which asks whether to perform a fresh install instead of an upgrade.
- If you answer No, the appliance ejects the CD and, after you restart the appliance, it prompts you again with the first question, "Do you want to proceed with upgrade?"

Note 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 this procedure to install the upgrade on your DMM appliance. The installation takes about 15 minutes.

Before You Begin

- Back up your DMM appliance. For more information, see the "Back Up Digital Media Manager Appliances" section on page 31.

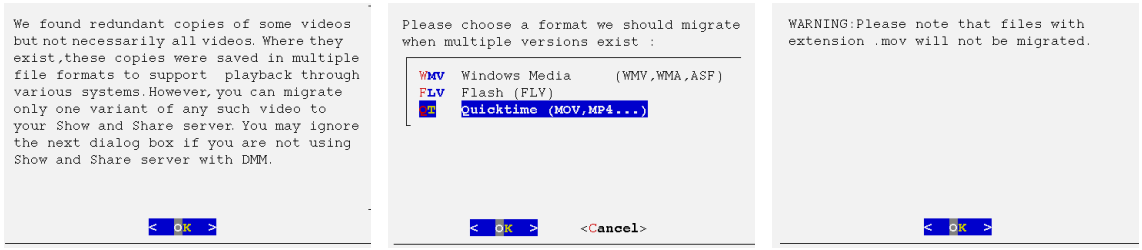
Procedure

Step 1 Insert the CD into the chassis CD-ROM drive.

Step 2 In AAI, choose **APPLIANCE_CONTROL > SOFTWARE_UPDATE**.

Step 3 Follow the on-screen instructions to update the software.

AAI might ask you to choose one video format. This happens because Video Portal 5.1 stored each video in as many different formats as you configured your portal to support. However, it would be inefficient now to migrate each of those variants. So, the format that you specify here is the only format that we will migrate when a video exists in multiple formats.



Note In cases where a video exists in only one format, we will migrate it even if its format differs from the one that you choose here. **The only exception is that we do not migrate .mov files under any circumstances.**

Step 4 Press **Enter** to complete the upgrade process. The appliance restarts upon completion.

Step 5 Stop. You have completed this procedure.

What to Do Next

- Proceed to "Log in to DMS-Admin for the First Time and Verify the Software Upgrade" section on page 34.

Log in to DMS-Admin for the First Time and Verify the Software Upgrade

Use this procedure to log in to DMS-Admin for the first time after you upgrade and to verify that the upgrade is successful.

Procedure

Step 1 Using **HTTPS**, point your browser at port **8443** on your upgraded DMM appliance.

Tip Be sure to use the appliance DNS name and not its IP address.

For example, `https://dmm.example.com:8443`.

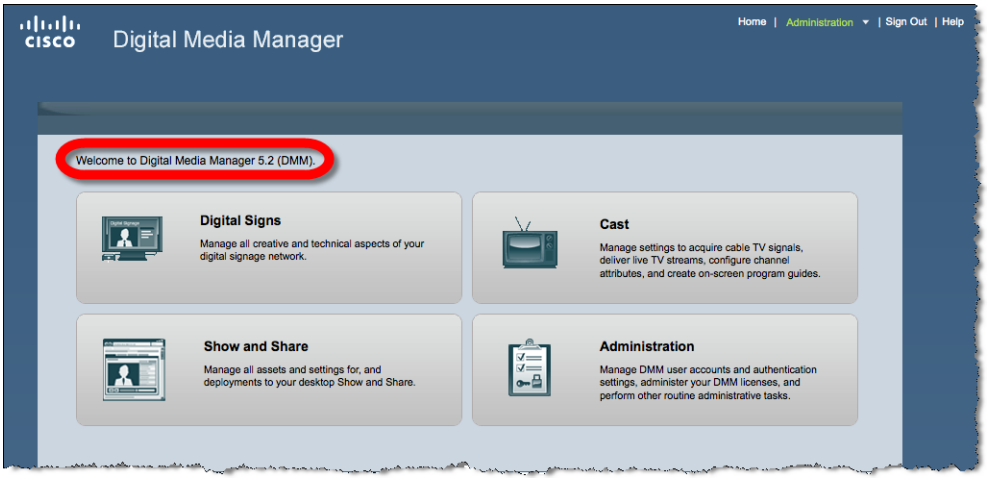
Step 2 Log in as **superuser** by using the account credentials that you configured in Cisco DMS 5.1.

OR

If you do not have a superuser account, enter the following default login, and change the credentials when prompted:

- Username: **superuser**
- Password: **admin**

Step 3 When the splash screen appears, confirm that it refers explicitly to Digital Media Manager 5.2.



Note If the version is not 5.2, contact Cisco TAC.

Step 4 Stop. You have completed this procedure.

What to Do Next

- Proceed to the "Verify That Existing Licenses Upgraded Successfully" section on page 35.

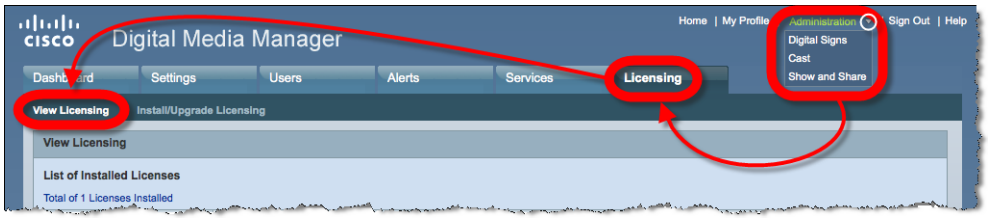
Verify That Existing Licenses Upgraded Successfully

Use this procedure to verify that existing licenses were upgraded correctly for each DMM software feature module that you are licensed to use.

Procedure

Step 1 Choose **Administration** from the global navigation.

Step 2 Choose **Licensing > View Licensing**.



The installed licenses are described.

Tip If you were licensed previously to use Video Portal 5.1.*x*, you should see that you now have a license pack installed that authorizes 100 *Show and Share* authors.

Step 3 Confirm that all of your licensed feature modules are enabled, such as the one for Digital Signs.

Note If your licenses are incomplete, log in to AAI on your DMM appliance and then choose **APPLIANCE_CONTROL > RESTART_OPTIONS > RESTART_WEB_SERVICES**.

If restarting web services does not solve the problem, contact Cisco TAC. If the support engineer asks that you send Cisco a copy of the Tomcat log file, see the "Obtaining or Transferring a Copy of the System Log" topic on Cisco.com in the *Appliance Administration Guide* for the Cisco DMS release version that you use.

Step 4 Stop. You have completed this procedure.

What to Do Next

Proceed to one of the following sections:

- If you purchased new Cisco DMS 5.2 licenses, proceed to the "Install DMS 5.2 Licenses" section on page 36.
- If you use *Digital Signs*, proceed to the "Verify Information for Digital Signs" section on page 43.
- If you use *Show and Share*, proceed to the "Verify Information for Show and Share" section on page 40.

Install DMS 5.2 Licenses

If you purchased licenses for Cisco DMS 5.2, use this procedure to install them.

Tip See *User Guide for Cisco Digital Media Manager 5.2.x* on Cisco.com for information about using the *Cisco Cast* and SNMP Notification modules.

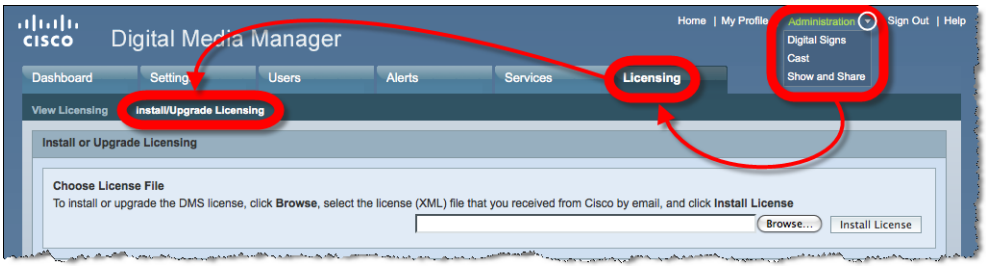
Before You Begin

- Obtain a license for each new Cisco DMM software feature module that you purchased. See the "Obtain Cisco DMS 5.2 Licenses" section on page 12.

Procedure

Step 1 Choose **Administration** from the global navigation.

Step 2 Choose **Licensing > Install/Upgrade Licensing**.



Step 3 Click **Browse** to specify the license file, and then click **Open**.

Step 4 Click **Install License**.

Step 5 Stop. You have completed this procedure.

What to Do Next

Proceed to one of the following sections:

- If you used Cisco Video Portal, proceed to the "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.
- If you use Digital Signs, proceed to the "Verify Information for Digital Signs" section on page 43.

Upgrade Video Portal Appliances to Run Show and Share

Complete these tasks in the orders shown, as needed for your deployment.

- Back Up Video Portal 5.1 Appliances That You Will Upgrade to Run Show and Share, page 37
- Install the Software Upgrade for Show and Share, page 38

Back Up Video Portal 5.1 Appliances That You Will Upgrade to Run Show and Share

Caution To preserve your data if the upgrade fails, we recommend that you plug a USB drive into the appliance USB port and back up only to the USB drive. **Backups do not contain media files.**

Tip Remember to use the export feature in Video Portal Reports if you want to save data from its reports. We will not migrate this information when you upgrade.

Use this procedure to back up a Cisco Video Portal 5.1.*x* appliance. **This backup creates a file that includes only database and configuration information for the appliance.** We do not include any assets in the backup. If you stored assets on your Video Portal appliance, complete the "Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance" section on page 16.

Procedure

Step 1 Log in as **admin** to Appliance Administration Interface (AAI).

Step 2 Choose **APPLIANCE_CONTROL > BACKUP_VP > USB**.

Warning **After the backup is saved, disconnect any USB drive that is connected to your appliance. Otherwise, the USB drive is REFORMATTED and ERASED.**

FURTHERMORE, UPGRADE FAILS.

You cannot restore your appliance from a backup that you have erased.

DO NOT IGNORE THIS WARNING!

Step 3 Stop. You have completed this procedure.

What to Do Next

- Proceed to "Install the Software Upgrade for Show and Share" section on page 38.

Install the Software Upgrade for Show and Share

Note We did not support any storage of content files on Cisco Video Portal appliances in Cisco DMS 5.1.*x* and earlier releases. If you deployed any files to your Video Portal appliance, this upgrade **will delete all the files automatically**. You will not be able to retrieve or use them after they are deleted. For more information, see the "Download Files That Were Stored Locally on Your Video Portal 5.1 Appliance" section on page 16.

Caution Do not use underscores or any other special characters in hostnames. DNS standards do not support these characters.

Before You Begin

- Obtain the *Show and Share* ISO image. See the "Obtain the CDs or DVDs to Upgrade Cisco DMS Appliances" section on page 14.
- This procedure assumes that you already upgraded your DMM appliance and have installed the license to use *Show and Share*. See the "Upgrade Digital Media Manager Appliances" section on page 31.

Procedure

Step 1 Insert the CD into the Video Portal 5.1.*x* appliance chassis CD-ROM drive.

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

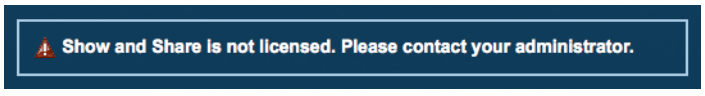
Step 3 Choose **APPLIANCE_CONTROL > SOFTWARE_UPDATE**.

Step 4 Follow the on-screen instructions to update the software.

Step 5 Press **Enter** to complete the upgrade process. The appliance restarts.

Note Upgrading requires that the appliance be restarted twice, automatically. After the first restart is finished, you must answer **Yes** at the "Do you want to proceed with upgrade?" prompt. Otherwise, if you answer No and prevent the second restart, the appliance becomes unstable.

Tip This procedure assumes that you already upgraded your DMM appliance and have installed the license to use *Show and Share*. Otherwise, when you try to use *Show and Share* before its license is installed on your DMM appliance, you see this message:



See the "Upgrade Digital Media Manager Appliances" section on page 31.

Step 6 Stop. You have completed this procedure.

What to Do Next

- Pair Your Cisco DMS 5.2 Appliances, page 39

Pair Your Cisco DMS 5.2 Appliances

After you upgrade your Digital Media Manager appliance and your *Show and Share* appliance, you must pair them.

Caution Pairing fails and upgrade fails when you complete these steps in the wrong order. To succeed, you must use AAI on your *Show and Share* appliance **before** you use AAI on your DMM appliance. **You must not reverse this order or try to use AAI simultaneously on both appliances.**

Before You Begin

- Complete the "Install the Software Upgrade for Digital Media Manager" section on page 32.
- Complete the "Install the Software Upgrade for Show and Share" section on page 38.

Procedure

Step 1 From the upgraded appliance that now runs *Show and Share* 5.2:

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

b. Choose **APPLIANCE_CONTROL > PAIR APPLIANCE**.

c. Choose **DMM**.

Warning **Do not choose any other option than DMM.**

d. Enter the fully-qualified domain name (FQDN) for your upgraded DMM appliance.

This is the DNS name. **Do not enter an IP address.**

e. Press **Enter**.

Your upgraded *Show and Share* appliance receives and successfully imports a digital certificate from your upgraded DMM appliance.

Step 2 From the upgraded appliance that now runs Digital Media Manager 5.2:

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

b. Choose **APPLIANCE_CONTROL > PAIR APPLIANCE**.

c. Choose **SHOW_AND_SHARE**.

Warning **Do not choose any other option than SHOW_AND_SHARE.**

d. Enter the fully-qualified domain name (FQDN) for your upgraded *Show and Share* appliance.

   This is the DNS name. **Do not enter an IP address.**

e. Press **Enter**.

   Your upgraded DMM appliance receives and successfully imports a digital certificate from your upgraded *Show and Share* appliance.

Step 3 Stop. You have completed this procedure.

What to Do Next

Proceed to one of the following sections:

- If you use *Digital Signs*, proceed to the "Verify Information for Digital Signs" section on page 43.
- If you use *Show and Share*, proceed to the "Verify Information for Show and Share" section on page 40.

After Your Appliances are Paired

Complete the tasks from this workflow, as needed.

1. Verify Information for Show and Share, page 40
2. Verify Information for Digital Signs, page 43
3. Schedule a Future Event to Pre-position (Stage) Content for Cisco ACNS, page 46
4. Schedule an Event to Resubmit Playlists and Presentations to DMPs, page 47
5. Prepare a Web Proxy Server for Use with Cisco DMS, page 48

   OR

   Use an Alternative Method That Substitutes for a Web Proxy Server, page 48

Verify Information for Show and Share

To verify that *Show and Share* configuration migrated successfully during the upgrade or to modify the configuration, proceed to the "Verify File Hosting Locations for Show and Share" section on page 41

If you do not use Cisco *Show and Share* features, proceed to the "Verify Information for Digital Signs" section on page 43.

Verify File Hosting Locations for Show and Share

Use this procedure to verify that *Show and Share* file hosting location values are correct in *Show and Share Administration*.

Procedure

Step 1 Use your browser to log in to your *Show and Share* appliance as its superuser.

Step 2 Choose **Administration** from the global navigation.

Step 3 Choose **Setup > Show and Share**.

Your browser loads the File Hosting Locations page.

- If the "Publish locally to <*your_Show_and_Share_appliance*>" check box is checked, we will store all published files locally on your *Show and Share* appliance itself. In addition, your *Show and Share* appliance works automatically as the streaming server for your .FLV and .MP4 videos.
- Otherwise, if the "Publish locally to <*your_Show_and_Share_appliance*>" check box is **not checked**, the File Hosting Locations page loads a set of drawers. There are five drawers by default.

Optional	Whether or not you publish locally, it is optional that you define these values: • H.264 Hosting Locations • MP3 Hosting Location • Windows Media Hosting Location • FLV Hosting Location When you publish locally, we ignore these values. Otherwise, elements within the optional drawers help you to specify distinct, external file hosting locations for various asset types that you plan to host. You can edit, add, and delete optional drawers as needed. **Note** Any external file hosting location for .FLV videos or .MP4 videos **must be a streaming server** and not merely a webserver. Otherwise, video editing features, slides, and transitions for .FLV and .MP4 videos will not work as designed. A webserver might be sufficient for .MP3 or .WMV files, but we recommend that you use a streaming server anyway.
Mandatory	Unless you publish locally, **you must define the values in the Default Hosting Location drawer.** We use the Default Hosting Location for every asset type unless and until you specify asset-specific hosts in the optional drawers. **Note** When you define this mandatory location but do not define locations in the optional drawers, this location **must be a streaming server** and not merely a webserver. Otherwise, video editing features, slides, and transitions for .FLV and .MP4 videos will not work as designed.

Step 4 Verify or modify values in each drawer, unless you checked the "Publish locally" check box.

Note Missing or incorrect values cause *Show and Share* deployments to fail for the relevant file type.

Setting	Description
Publish locally to <*your_appliance*>	All published assets will be stored locally on your Show and Share appliance. You must enter the Show and Share AAI admin account password in the Password field. **Note** Although this release supports local storage of published assets on your Show and Share appliance, which is also a streaming server, we recommend that you host files on a dedicated streaming server instead.

<*asset type*> Hosting Location

File Hosting Location Name		A human-readable name. It might be the same as the relevant file type.
File Hosting Server Settings	Accepts files with extensions	The filename extensions that identify types of files. This information tells us where we should store various files and how we should retrieve them for playback. These are the default values: • **H.264 Hosting Location** – *.mp4 – *.m4v – *.mpv4 • **MP3 Hosting Location** – *.mp3 • **Windows Media Hosting Location** – *.wmv – *.asf – *.asx – *.wma • **FLV Hosting Location** – *.flv
	File upload protocol	The protocol or method for file transfer. Either FTP or SFTP.
	Host address	The DNS-resolvable hostname or routable IP address of the remote server where you will deploy files of the relevant file type.
	Login name	A user account with the required privileges to use the remote server.
	Login password	The assigned password for the login name that you specified.
	Directory root location	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`.
	Directory root URL path	The absolute URL where Show and Share will host and reference your files.

Step 5 Click **Save** at the bottom of the page.

Step 6 Stop. You have completed this procedure.

What to Do Next

Proceed to one of the following sections:

- If you use *Digital Signs*, proceed to the "Verify Information for Digital Signs" section on page 43.
- If you use *Show and Share*, proceed to the "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.

Verify Information for Digital Signs

To verify that Cisco Digital Signs migrated successfully or to edit its configuration, complete the following procedures.

- Verify Content Deployment Locations, page 43
- Verify DMP Inventory and Network Statuses, page 45

If you do not use Digital Signs, proceed to the "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.

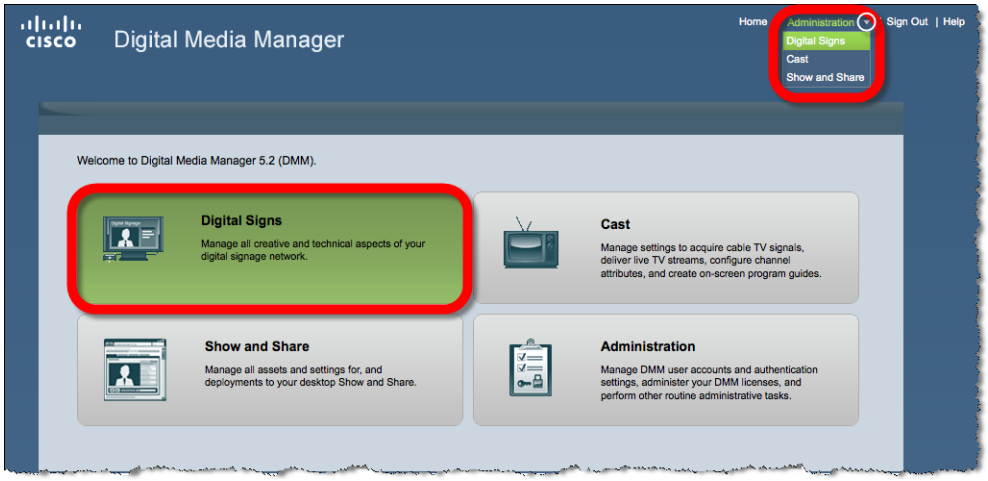
Verify Content Deployment Locations

Use this procedure to verify in Cisco Digital Signs that external deployment server locations are correct.

Procedure

Step 1 Use your browser to log in to your DMM appliance as its superuser.

Step 2 Choose **Digital Signs** from the global navigation or click **Digital Signs** on the dashboard.



Step 3 Choose **Settings > External**.

Step 4 Verify or change the values for your external deployment servers:

Setting	Description
External Publishing Server List	
Click a server to highlight it so that you can edit or delete it. Digital Signs automatically shows the Change External Publishing Server pane for the corresponding server where you can edit its settings.	
Add 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 or 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 next item), 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 previous item), 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	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 port 80.
User Name	The FTP username. It is acceptable to use the name *anonymous*.
Password	You must enter the FTP password, and then re-enter it.
Confirm Password	

Step 5 Click **Save**.

Step 6 Stop. You have completed this procedure.

What to Do Next

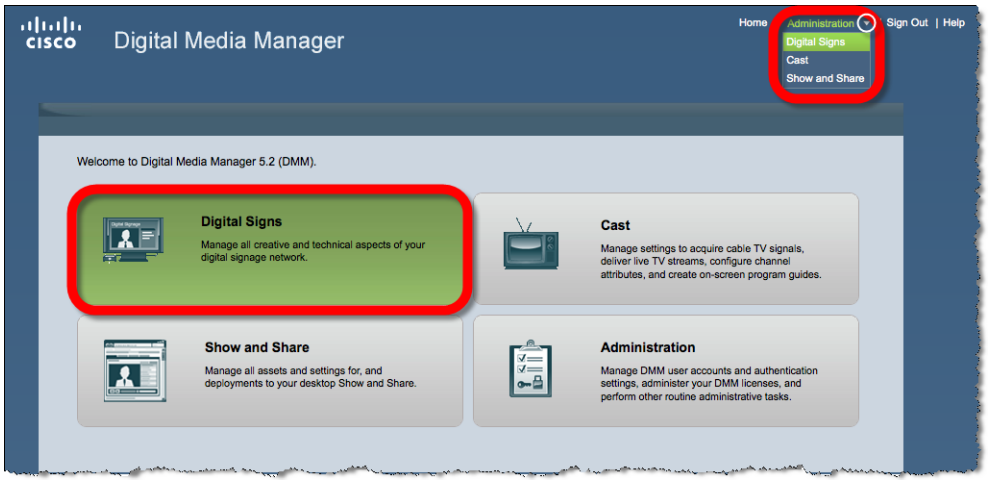
- Proceed to the "Verify DMP Inventory and Network Statuses" section on page 45.

Verify DMP Inventory and Network Statuses

Use this procedure to make sure that your preexisting inventory of DMPs is intact and that Digital Signs is receiving DMP status messages.

Procedure

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



Step 2 Choose **Digital Media Players > DMP Manager**.

Step 3 Verify that all of your DMPs show green checkmarks in the Status column.

Step 4 Stop. You have completed this procedure.

Troubleshooting

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 5.2.x* on Cisco.com.

What to Do Next

Proceed to one of the following sections:

- If you use ACNS, proceed to "Schedule a Future Event to Pre-position (Stage) Content for Cisco ACNS" section on page 46.
- If you do not use ACNS, proceed to "Schedule an Event to Resubmit Playlists and Presentations to DMPs" section on page 47.

Schedule a Future Event to Pre-position (Stage) Content for Cisco ACNS

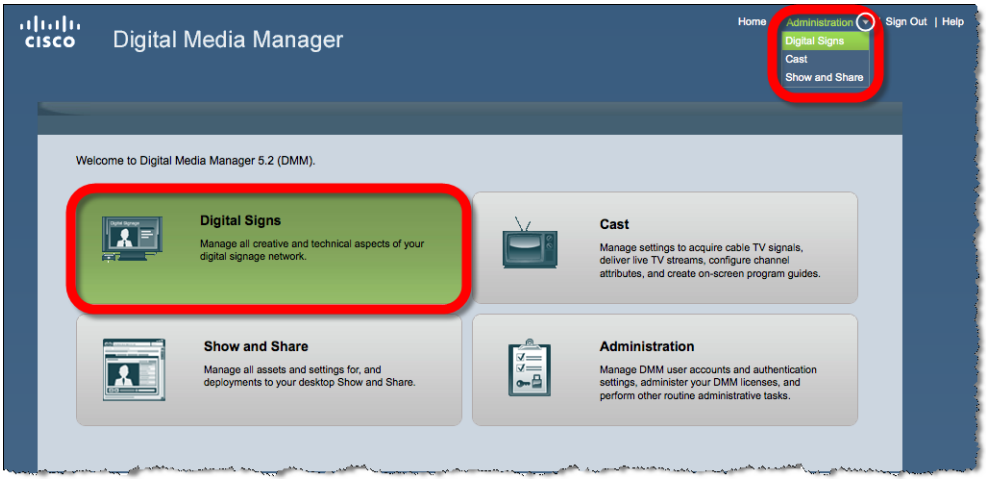
If you use Cisco ACNS for content distribution in your digital signage network, use this procedure to schedule a future event. This action generates your playlist and manifest files for your DMPs and CDM.

Before You Begin

- Because DMPs will fail to play presentations without prepositioning for ACNS, we recommend that you schedule the event at least one hour in the future to allow enough time for prepositioning.
- Verify the ACNS settings in *Digital Signs* under Settings > Media Delivery. The DMM shows the default ACNS channel for your signage content that you choose under these settings.

Procedure

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



Step 2 Choose **Schedules > Play in Future.**

Step 3 Schedule a task to play content on the DMPs.

a. Click **Add an Event**.

b. Click **Select Groups**, and then choose the groups.

c. Click **Digital Signage**, and then choose the presentation or playlist.

d. Specify the date, time, and frequency.

e. Click **Save**.

Step 4 Click **Save All** to save the schedule.

Step 5 Click **Publish All** to publish the schedule.

Step 6 (**Optional**) Verify that DMM automatically updated this schedule in the manifest file website that you defined in Cisco ACNS.

Step 7 Stop. You have completed this procedure.

What to Do Next

- If you use a Video Portal appliance, proceed to "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.

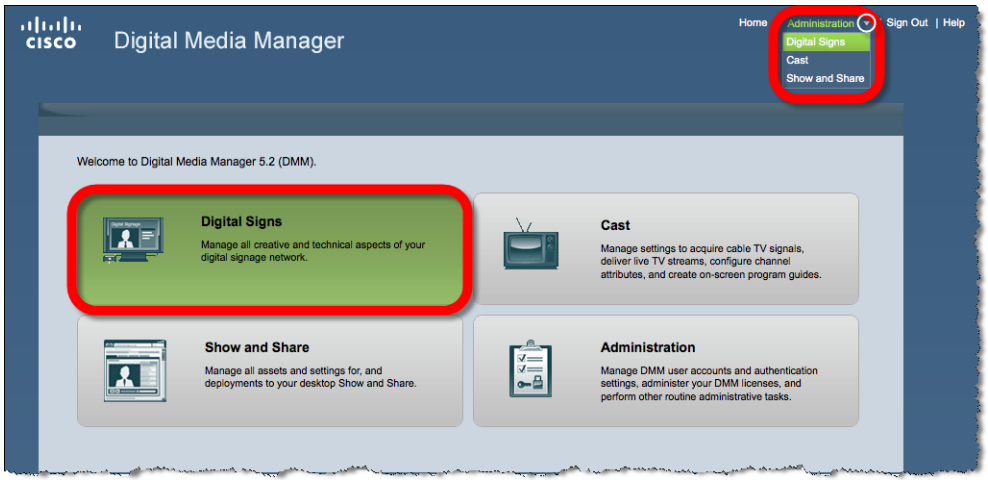
Schedule an Event to Resubmit Playlists and Presentations to DMPs

If you do not use ACNS, use this procedure to schedule an immediate event to resubmit your playlists and presentations to your DMPs.

Tip Or you can schedule a future event. For instructions, see the scheduling procedure in the "Schedule a Future Event to Pre-position (Stage) Content for Cisco ACNS" section on page 46.

Procedure

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



Step 2 Choose **Schedules > Play Now**.

Step 3 Choose **Digital Signage** from the Select an Event Type list.

Step 4 Click the name of the presentation or playlist in the Select Content area, and then click **OK**.

Step 5 Click the name of the DMP group in the Select a DMP area.

Step 6 Click **Submit**, and then click **OK** when the success message appears.

Step 7 Stop. You have completed this procedure.

What to Do Next

- If you use a *Show and Share* appliance, proceed to "Upgrade Video Portal Appliances to Run Show and Share" section on page 36.

Prepare a Web Proxy Server for Use with Cisco DMS

Widespread security improvements throughout Cisco DMS 5.2 mean that you must now configure and use a web proxy server for Cisco DMS whenever:

- Any of your presentations or playlists for digital signage include external (cross-domain) assets, such as RSS feeds.
- Any of your text transcripts for Show and Share are stored externally.

Then, in the root directory on your proxy server, you must save an XML file with the filename **CROSSDOMAIN.XML**.

Example File Syntax

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM
"http://www.adobe.com/xml/dtds/cross-domain-policy.dtd">

<cross-domain-policy>
        <site-control permitted-cross-domain-policies="master-only"/>
        <allow-access-from domain="*"/>
        <allow-http-request-headers-from domain="*" headers="SOAPAction"/>
</cross-domain-policy>
```

Otherwise, if you do not use a cross-domain proxy, your digital signs and your Show and Share site will not show any of these external assets.

Note To understand the CROSSDOMAIN.XML file and its purpose, see:

- http://www.adobe.com/devnet/flashplayer/articles/fplayer9_security.html
- http://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
- http://developer.yahoo.com/javascript/howto-proxy.html

Use an Alternative Method That Substitutes for a Web Proxy Server

Other options are available to you if you do not use a web proxy server already in your network and you prefer not to use one for Cisco DMS.

- Use RSS Feeds from Servers That Allow Cross-Site Scripting, page 48
- Use a Hosted Proxy Service for Web Mashups, Such As Yahoo Pipes, page 49

Use RSS Feeds from Servers That Allow Cross-Site Scripting

Examples

- http://edition.cnn.com/services/rss/
- http://www.msnbc.msn.com/id/5216556/ns/about_msnbccom-rss_feeds/#Topheadlines
- http://weather.yahooapis.com/forecastrss?w=2488042
- http://www.foxnews.com/rss/index.html
- http://www.nytimes.com/services/xml/rss/index.html
- http://feeds.fool.com/usmf/foolwatch

Use a Hosted Proxy Service for Web Mashups, Such As Yahoo Pipes

Note Cisco is not responsible for the Yahoo Pipes service and does not support it. Our references to it here are merely examples.

You can use a hosted proxy service. One example of such services is Yahoo Pipes, which is freely available to anyone at http://pipes.yahoo.com.

Procedure

Step 1 Create an account.

Step 2 Configure one or more pipes for the public data sources that you use.

Step 3 After you create and save a pipe, click the Get as RSS button. Your pipe's RSS URL is approximately: http://pipes.yahoo.com/pipes/pipe.run?_id=_[redacted]_render=rss.

Step 4 Copy your pipe's RSS URL and paste it into a text editor.

Step 5 Use your text editor to change the server hostname from pipes.yahoo.com to **pipes.yahooapis.com**, *but do not change anything else in the URL.*

Step 6 Copy this modified URL and use it in Cisco DMS, as needed.

Configure Show and Share 5.2

Before You Begin

- Pair Your Cisco DMS 5.2 Appliances, page 39

Procedure

Step 1 Verify in DMS-Admin that your Show and Share licenses are installed.

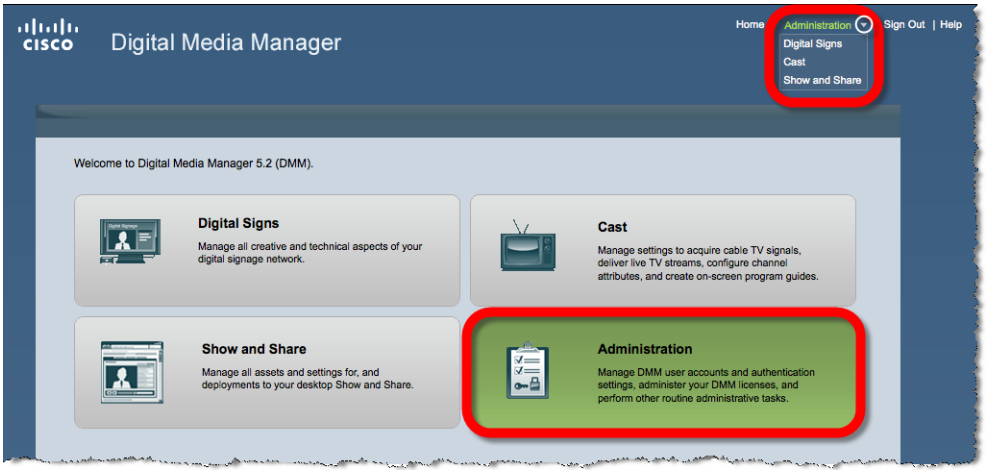
a. Using **HTTPS**, point your browser at port **8443** on your upgraded DMM appliance.

Tip Be sure to use the fully qualified appliance DNS name and not its IP address.

For example, `https://dmm.example.com:8443`.

b. Log in as **superuser**.

c. Choose **Administration** from the global navigation or click **Administration** on the dashboard.



d. Choose **Licensing > View Licensing**.

e. Verify that you see these options in the Features column:

- Show and Share Module
- *At least one of these*:
  - Show and Share Content Author Pack:1000
  - Show and Share Content Author Pack:500
  - Show and Share Content Author Pack:100
  - Show and Share Content Author Pack:50
  - Show and Share Content Author Pack:10

Tip The 100-user author pack is installed automatically when you upgrade from Video Portal.

Step 2 Install any additional licenses that remain to be installed. Alternatively, if you have not purchased and received any additional licenses, you can skip this step.

a. Choose **Licenses > Install/Upgrade Licensing**.

b. Click **Browse**, find and click the license file where you saved it, and then click **Open**.

c. Click **Install License**.

If you receive multiple license key files, repeat this step until all of your licenses are installed.

Step 3 Configure *Show and Share* behaviors as its administrator.

a. Using **HTTPS**, point your browser at port **8443** on your upgraded Show and Share appliance.

b. Be sure to use the appliance DNS name and not its IP address.

For example, `https://showandshare.example.com:8443`.

c. Log in as **superuser**.

d. Choose **Administration** from the global navigation.

e. (**As needed**) Complete procedures in *User Guide for Cisco Show and Share Administration 5.2.x* on Cisco.com that tell you how to:

✓	Task
❑	Change file hosting locations. Also, if you used Secure Connection Protocol (SCP) for deployments in Video Portal 5.1, you must use SFTP now.
❑	Change user role assignments. **Video Portal 5.1 user role assignments do not transfer to *Show and Share* 5.2 during an upgrade.**
❑	Change permissions and settings. • Choose whether the workflow for publishing should require approvals. • Assign an approver to each author, if you have required approvals for publishing.
❑	Define subject categories for your *Show and Share* server.
❑	Upload and publish any videos that we did not migrate automatically. We migrate **only the published videos** from Video Portal 5.1.
❑	Configure any upcoming live events. **We do not migrate live events** from Video Portal 5.1.
❑	Choose which videos in *Show and Share* should be the Featured Videos.
❑	Choose a skin.
❑	Define a ticker.

Step 4 Stop. You have completed this procedure.

What to Do Next

- Enjoy Cisco DMS 5.2.

FAQs and Troubleshooting

DMM Upgrade

Q. Why did upgrade fail on my DMM appliance? AAI returned this error message:

A. There are a few possible explanations.

- **First**—You might have made a mistake.
  - Please check that you did not merely boot your DMM appliance from its upgrade DVD.
  - Please check that you used the correct upgrade DVD and not one for any other appliance.
  - Please check that we support your appliance model for this upgrade.
- **Second**—The upgrade ISO image might have been corrupted before you tried to burn it as a DVD. Please verify the checksum of the ISO image, as well as its size in bytes. If these differ from their expected values, your copy of the ISO image is corrupted. Please obtain a new copy.
- **Third**—The DVD media might have been damaged before you tried to upgrade from it.
  1. Use AAI to generate a sysreport.
  2. Extract and then open **var/log/dmsupgrade.log**.
  3. Search in the log for this string:
     `No such file or directory`
  4. If you find this string anywhere in dmsupgrade.log and you have not established already that the ISO image was corrupted before you burned it as a DVD, then the DVD media that you used is damaged. Please obtain another blank DVD and try again to burn the valid ISO.

Tip If you cannot generate a sysreport or if its file size is zero bytes, delete any unnecessary tmp files and then try again.

Remarks

Related Cisco DMS Documentation

To locate all Cisco DMS product documentation, see the *Guide to Documentation for the Cisco Digital Media System* at the following URL:

http://www.cisco.com/en/US/products/ps6681/products_documentation_roadmaps_list.html

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