Getting Started Guide for Cisco Digital Media Players

Revised: November 8, 2010
78-19212-02 (A0)

This guide explains how to set up a Cisco Digital Media Player in your network. It assumes that your DMP firmware reports a "build date" after October 2010.

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

Start Here

Important Safety Warnings

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Read the installation instructions before connecting the system to the power source. Statement 1004

The device is designed to work with TN power systems. Statement 19

The power supply must be placed indoors. Statement 331

This equipment is intended to be grounded. Ensure that the host is connected to an earth ground during normal use.

When installing the unit, always make the ground connection first and disconnect it last.

Use only the Cisco-supplied combination of power cord, plug, and adapter—if any—that shipped with the equipment, or which you ordered separately. Otherwise, if you use other such supplies, including similar supplies that Cisco might sell for use with similar equipment, you:

- **Might damage or destroy data, equipment, or other property.**
- **Might cause any combination of electrical shock, electrical fire, injury, or loss of life.**
- **Will void the warranties for Cisco equipment.**

Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240 VAC, 10A international)

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device. Statement 1019

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. Statement 1021

Installation of the equipment must comply with local and national electrical codes. Statement 1074

Ultimate disposal of this product should be handled according to all national laws and regulations.

General Precautions

Observe the following precautions.

- Never open the equipment. Only an authorized technician should service its components.
- If any of the following conditions occur, unplug the equipment and contact an authorized technician.
  - The power cable, extension cord, or plug is damaged.
  - Any foreign object has entered the equipment.
  - The equipment has been exposed to any liquid.
  - The equipment has been dropped or damaged.
  - The equipment does not operate correctly when you follow its operating instructions.
- Do not spill anything on the equipment.
- Observe extension cord and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cord or power strip does not exceed 80 percent of the extension cord or power strip ampere ratings limit.
- Do not modify power cords or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.

Protect Against Electrostatic Discharge

Static electricity might harm sensitive components. To prevent this damage, discharge static electricity from your body before you touch the equipment. You can also take the following steps to prevent damage that might result from electrostatic discharge.

- When transporting equipment, first place it in an antistatic container or packaging.
- Do not leave equipment where other people can handle and possibly damage it.
- Take additional care when handling equipment during cold weather. Heating reduces indoor humidity and increases static electricity.

Regulatory Compliance and Safety Information

See http://cisco.com/en/US/products/ps7220/prod_installation_guides_list.html.

Cisco DMS Overview

Cisco Digital Media Suite (Cisco DMS) is an ecosystem for networked digital video. It is also the collective name for a broad range of hardware products, software products, and accessories. We sell and license these separately but they work together seamlessly.

Cisco DMS is a key component of several Cisco portfolios. To learn about the full range of Cisco DMS products and technologies, see http://cisco.com/go/dms.

DMP Overview

Cisco Digital Media Players (DMPs) are highly reliable, compact, solid-state devices for IP networks. DMPs process High Definition and Standard Definition video, multimedia and animations, web pages, and other supported content types for playback. You expose targeted audiences to this programming when you schedule its availability—live or on demand—on a public presentation system that is attached to a DMP. The presentation system might be a display (monitor), touchscreen, video projector, or video wall.

DMP 4305G	DMP 4310G	DMP 4400G
		

DMPs consume very little power and are designed for fast deployment throughout IP networks of any size, without the burden of high ongoing operational cost. DMPs are compatible with popular systems for networked content distribution, including *Cisco Application and Content Networking System* (ACNS) and *Cisco Wide Area Application Services* (WAAS).

Any two DMP models might differ in their features, attributes, strengths, limitations, and general availability. Some DMPs differ from others, for example, in their support for interactivity through touch. To learn what your DMP supports, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.

DMPs are a major component of *Cisco Digital Media Suite* (Cisco DMS) and *Cisco StadiumVision*, both of which we describe elsewhere in this guide.

- DMPDM, page 4
- TVzilla, page 5
- Cisco Hinter, page 5
- Optional DMP Accessories, page 6

DMPDM

Tip **We optimize and certify DMPs for use with centralized management solutions that we sell and license separately.** See the "Consider How You Will Use and Manage Your DMP" section on page 7.

A lightweight webserver on every DMP runs a web-based "craft interface" called *Digital Media Player Device Manager*, or DMPDM. Because DMPDM is limited to the simplest functions and does not scale beyond its own host DMP, we recommend that you manage all DMPs centrally.

DMPDM has two main purposes. With it, you can:

- Configure one DMP during its initial setup.
- Manage one DMP and one presentation system in isolation. (Or, when you use signal splitters or daisy chaining, your DMP can deliver media to multiple presentation systems that are close to it—as would be the case with a video wall.)

Note ***StadiumVision* deployments should avoid using DMPDM, except to check the firmware's "build date" or release version number.** For other tasks, please use the management dashboard software and documentation that came with your *StadiumVision* purchase.

Tip **A software user guide for DMPDM is available on Cisco.com.** See http://cisco.com/go/dms/dmpdm.

TVzilla

A Cisco-customized web browser is sometimes preinstalled on DMPs. We call this browser *TVzilla*.

Note **Does your DMP model run TVzilla in this release?** Some might not. See http://cisco.com/go/dms/dmp/datasheets.

TVzilla uses code from the open source Mozilla project, and supports JavaScript. TVzilla supports the following file types.

- HTML and TXT
- GIF, JPEG, and PNG
- SWF (Shockwave Flash)—for supported versions, see your DMP datasheet at http://cisco.com/go/dms/dmp/datasheets.

You cannot install browser plug-ins or any other software in TVzilla, whether to support additional file types or for any other purpose. No Java Runtime Environment is installed.

Cisco Hinter

A technique called *interleaved RTP* makes it possible for some centrally managed DMPs to play delay-insensitive unicast MPEG streams through RTSP connections. A streaming server can then transmit this "hinted" video to DMPs on demand. The key advantages of interleaved RTP are that data loss is impossible inside the hinted program stream, and yet synchronization of audio to video never suffers, even in high-definition.

Cisco Hinter is software to prepare and stage MPEG files for interleaved RTP transmission through the open source Darwin Streaming Server component on a *Cisco Digital Media Manager* (DMM) appliance.

Note **Thus, this utility and this feature are not available in deployments that use *Cisco StadiumVision*.** There is no DMM appliance in *StadiumVision*.

Cisco Hinter versions for Windows and Linux users are freely downloadable from any DMM appliance that is fully licensed for *Cisco Digital Signs*. To understand *Cisco Hinter* and *Cisco Digital Signs* fully, see the DMM user guide on Cisco.com.

Optional DMP Accessories

Note **We reserve the right to introduce, redesign, or discontinue any accessory as needed.**

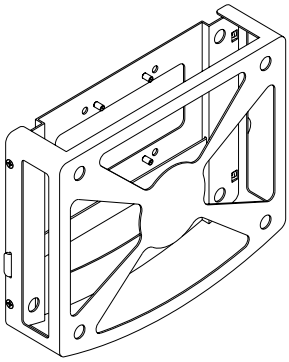
We have designed optional accessories to enhance your DMP experience. For example, you might order handheld remote control units or VESA-compliant mount kits.

Remote Controls

Cisco sells handheld remote control units that you can use to operate DMPs. We sell these optional remote control units separately to conserve natural resources and prevent needless waste.

- Consult the remote control datasheet to learn exactly the maximum distance from which your remote control can control your DMP.
- To order remote controls, contact your Cisco sales partner.
- Remote control documentation is available on Cisco.com.

Mount Kits



Cisco sells fabricated sheet metal cases to stabilize and protect Cisco DMPs in any supported mounting scenario. With these cases, you can mount DMPs securely to walls, pillars, suspended-grid ceiling T-joints, metal poles, or VESA-compliant flat-panel displays. DMP mount kits are a versatile and cost-effective alternative to complex cabinet-making and construction projects. They do not block ventilation or heat dissipation.

- To order DMP mount kits, contact your Cisco sales partner.
- Mount kit documentation is available on Cisco.com.

Plan and Prepare

Consider How You Will Use and Manage Your DMP

Tip **Cisco Medianet technologies can help you to manage the DMPs in your network.** To understand DMP support for Medianet, see *User Guide for Cisco Digital Media Suite* on Cisco.com.

An organization might buy and use one DMP in isolation but this is rarely the case. Almost every DMP is part of a network that includes many other DMPs.

The ideal DMP management system (or combination of systems) for your organization depends on how many DMPs you have and how you plan to use them. Beyond this, a management system might impose its own installation and setup requirements for DMPs.

Topics in this section describe Cisco products to manage DMPs in various settings.

Manage One DMP in Isolation

See DMPDM, page 4.

Centrally Manage Digital Signage Services

Cisco Digital Signs provides a flexible environment in which to create and centrally manage a local, regional, or global IP network of DMPs and their attached presentation systems—such as Cisco-branded displays in our *LCD Professional* series.

- Simple but powerful design and publishing features in *Digital Signs* help you to create media libraries, employ networked content distribution, schedule playback for programming, and prepare reports to prove that playback occurred.
- Life-saving features support public emergency preparedness and response.
- Purely administrative features help you to manage DMPs and their attached presentation systems.
  - Define and issue remote commands.
  - Poll current and historical status.
  - Adjust the sound and picture.

Commonly popular DMP deployment sites for *Digital Signs* include lobbies, classrooms, showrooms, service counters, exhibit halls, dining halls, waiting rooms, and offices. Used well, *Digital Signs* can help your organization to enhance customer experience, educate students, and entertain patrons.

Centrally Manage IPTV Services

Cisco Cast features help your organization to deliver video-on-demand and live broadcast TV channels over a local, regional, or global IP network of DMPs and their attached presentation systems—such as Cisco-branded displays in our *LCD Professional* series.

- Browse or search with interactive on-screen menus and program guides.
- Show live or on-demand:
  - news
  - financial information
  - sales and marketing messages
  - educational or instructional media
  - corporate communications
  - entertainment
  - any other video asset that is suitable for your purpose
- Alternatively, hospitality and healthcare providers might use *Cisco Cast* features to support in-room IPTV.

Centrally Manage Sports and Entertainment Venue Services

Cisco StadiumVision is an advanced solution for centralized IPTV video content management and delivery. It integrates video from multiple sources—in Standard Definition (SD), High Definition (HD), or both—to automate video delivery in stadiums, arenas, and similar venues.

Platform services software and control panels help you to manage a network of DMPs. Combined with Cisco video acquisition infrastructure at the head-end, these DMPs use new or existing video displays in a venue to enhance patron enjoyment of live events and deliver in-house advertising. Your deployment can leverage the displays in bleachers (terraces), restaurants, clubs, and luxury suites to deliver a range of uniquely interactive messages automatically to patrons in various areas.

With *StadiumVision*, you can add, organize, combine, and deliver any supported combination of in-house programming and external network channels for playback to your patrons.

Qualify a Location for Setup

Cable length, signal strength, and other factors limit where you can set up a DMP—relative to the location of its AC power source, its presentation system, and any person on site who will use a remote control to operate the DMP.

- General Environmental Conditions, page 9
- Site-Specific Conditions, page 10

General Environmental Conditions

Table 1 describes the temperature, humidity, and altitude ranges that a DMP can tolerate.

Table 1 Environmental Tolerance Ranges

Measurable Condition	Model	Supported Range		
Temperature (Ambient)				
Operating — long-term or short-term	**DMP 4305G**	*Min.*	**41°F**	5°C
		Max	**104°F**	40°C
	DMP 4310G	*Min.*	**32°F**	0°C
		Max.	**122°F**	50°C
	DMP 4400G	*Min.*	**41°F**	5°C
		Max	**104°F**	40°C
Nonoperating or storage	**DMP 4305G**	*Min.*	**-4°F**	-20°C
		Max.	**140°F**	60°C
	DMP 4310G	*Min.*	**-4°F**	-20°C
		Max.	**158°F**	70°C
	DMP 4400G	*Min.*	**-4°F**	-20°C
		Max	**140°F**	60°C
Relative Humidity (Noncondensing; Ambient)				
Operating	**DMP 4305G**	*Min.*	**20** percent	
		Max.	**85** percent	
	DMP 4310G	*Min.*	**10** percent	
		Max.	**85** percent	
	DMP 4400G	*Min.*	**20** percent	
		Max.	**85** percent	
Nonoperating or storage	**DMP 4305G**	*Min.*	**0** percent	
		Max.	**95** percent	
	DMP 4310G	*Min.*	**0** percent	
		Max.	**95** percent	
	DMP 4400G	*Min.*	**0** percent	
		Max.	**95** percent	

Table 1 Environmental Tolerance Ranges (continued)

Measurable Condition	Model	Supported Range		
Altitude (Above sea level)				
Operating, nonoperating, and storage	**DMP 4305G**	*Min.*	**0 ft**	0 m
		Max.	**13,780 ft**	4,200 m
	DMP 4310G	*Min.*	**0 ft**	0 m
		Max.	**13,780 ft**	4,200 m
	DMP 4400G	*Min.*	**0 ft**	0 m
		Max.	**13,780 ft**	4,200 m

Site-Specific Conditions

Assess each location where you might want to use this equipment.

Adequate Shelter

Install and use this equipment indoors—or outdoors in a covered area.

- Never install or use it in a wet environment.
- Never install or use it near radiators or other heat sources.

Supported Voltage

There are—*at most*—only two supported methods to power this equipment.

- **Use the standard electrical power cord that came with the equipment.** Cord length determines the maximum possible distance from the equipment to any AC electrical outlet that it can use. The outlet itself must use standard voltage for your locale, within the range from 100V to 240V. We recommend that you use a surge suppressor, line conditioner, or uninterruptable power supply (UPS). Please position all cables and power cords carefully. Route all cables, the power cord, and the plug so that they cannot be stepped on or tripped over. Never allow anything to rest on equipment cables or cords.

  OR

- **Use 802.3af power over Ethernet (PoE), assuming that your equipment model supports this feature.** We describe PoE setup elsewhere in this guide. To learn if your equipment model supports this feature, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.

DHCP Access

Each new DMP (and each DMP on which you restore factory-default settings) uses DHCP to obtain its first IP address. Therefore, a DHCP server **must be reachable** from the site where you set up a DMP. Later, after your DMP is fully configured, it can use either static or dynamic IP addressing.

Signal Integrity

When physical cables are too long, the signals that they carry can degrade. Signal loss can also affect wireless connections—including the infrared connection between a DMP and its remote control. When signal integrity suffers, equipment performance suffers.

Unpack the Equipment

Check Package Contents

The shipping container that you received contains your equipment product kit. This kit contains a printed packing list. Compare the packing list to the kit. The packing list tells you how to request a replacement if anything is missing from the kit, is defective, or is damaged.

Note **Do not discard or recycle the printed packing list.** You will use it.

Start to Keep Records Now

Before you recycle or discard the shipping container that you received, examine it. Then, write down or photograph any important information that is:

- Printed directly on the shipping container.
- Printed on any material that is affixed or fastened to the shipping container.

This information might help you to obtain warranty service, replacement parts, or technical support if you ever need them.

Connect Equipment

Physical Interfaces (I/O Ports)

Table 2 describes the connectors, sensors, and buttons on each DMP model.

DMP 4305G

DMP 4310G

DMP 4400G

Table 2 DMP Interfaces

Category and Subcategory		Chassis Label	DMP 4305G	DMP 4310G	DMP 4400G
Electrical Power					
DC	5V	• POWER 5V DC	**1**	0	0
	12V	• DC 12V	0	**1**	0
		• Power DC	0	0	**1**
PoE[1]	IEEE 802.3af	• RJ-45	0	**1**	0

Table 2 DMP Interfaces (continued)

Category and Subcategory			Chassis Label	DMP 4305G	DMP 4310G	DMP 4400G
Network Connectivity						
Wired[2]	Fast Ethernet	10/100	• 10/100	**1**	0	0
			• RJ45	0	**1**	0
	Gigabit Ethernet[3]	10/100/1000	• RJ-45	0	0	**1**
Wireless	IEEE 802.11b/g		• Antenna	0	0	**1**
Debugging (for Cisco use only)						
—			• CONSOLE	0	**1**	0
Media Signal						
Wired[4]	Video connectors	HDMI 1.1	• HDMI	**1**	0	**1**
		HDMI 1.3[5]		0	**1**	0
		Component[6]	• YPbPr/ S-Video	0	**1**	0
			• S-VIDEO/ YPbPr	**1**	0	0
			• S-Video	0	0	**1**
		Composite[7]	• CVBS	**1**	0[8]	**1**
	Audio connectors	3.5mm jack[9]	• Audio	0	**1**	**1**
		RCA	• SPDIF	0	0	**1**
			• RIGHT	**1**	0	0
			• LEFT	**1**	0	0
Infrared						
Wired	Receiver extension	3.5 mm jack	• IR Extension	0	**1**	**1**
Wireless	Receiver	Sensor for remote control	• —	**1**	**1**	**1**
Serial (Comm Ports)						
Wired	Data	USB 1.0	• USB	**1**	0	0
		USB 2.0[10]		0	**2**	**2**
		RS-232 *(9-pin DB9 to 9-pin DB9)*	• RS232	**1**	0	**1**
		RS-232 *(9-pin DB9 to 3.55mm jack)*		0	**1**	0

Table 2 DMP Interfaces (continued)

Category and Subcategory		Chassis Label	DMP 4305G	DMP 4310G	DMP 4400G
Human					
Power On/Off	Button	• Power	0	**1**	0
Device Reset	Recessed button	• Reset	**1**	**1**	**1**

1. IEEE 802.3af interface with integrated switching regulator.
2. Category 5 or better. Maximum length: 328 ft (100 m). For any distance greater than 165 ft (50 m), we recommend that you use Category 5e or Category 6 certified Ethernet cabling. For installation behind walls, we recommend plenum-rated cabling unless it does not satisfy the requirements set forth in your regional building code. **We do not ship any Ethernet cable with any DMP model.** You must obtain this cable separately.
3. Wake-on-LAN.
4. For maximum supported media signal cable lengths, see the "Understand How to Choose Media Signal Cables" section on page 23. Each video and audio signal cable that we ship with DMPs is 6 ft (approximately 1.83 m) long.
5. Backward-compatible to HDMI 1.1.
6. Use an S-Video signal cable with a YPbPr-to-S-Video adapter to transmit and receive YPbPr data signals.
7. See the "Understand How to Work Around the Low Signal Quality of Composite Video Cables" section on page 25.
8. Although there is no Composite CVBS connector on a DMP 4310G, its YPbPr/S-Video connector supports Composite CVBS when you use an S-Video-to-Composite adapter.
9. Stereo audio output, irrespective of the cable type for video output.
10. Maximum USB cable length is 15 ft (approximately 5 m).

Connect to a Power Source

DMPs use electrical power to run. Your DMP model and geographic locale might both affect which power plug your DMP uses.

DMP Power Cord Options

Table 3 International Power Cord Standards

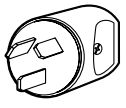
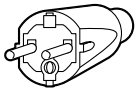
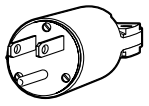
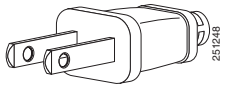
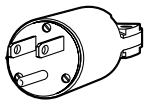
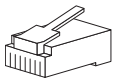
Locale	Standard	Plug Type
• ***Australia*** • ***New Zealand***	• SAA/3 • AS/NZS 3112-1993	 120356
• ***European Union (except Italy)*** • ***Argentina*** • ***Brazil***	• CEE 7/7 • VIIG	 120357

Table 3 International Power Cord Standards (continued)

Locale	Standard	Plug Type
• ***Japan***	• JIS C8303 (NEMA 5-15P)	 120354
	• JIS 38303	 251248
• ***North America*** • ***Central America*** • ***Columbia*** • ***Ecuador***	• NEMA 5-15P • CS22.2, No.42	 120354
• ***United Kingdom***	• BS89/13	 120359
Any Locale		
• ***Power Over Ethernet (PoE)***	• RJ-45	

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Connect to a 100V–240V AC Socket, page 16
- Use 802.3af Power over Ethernet (PoE), page 16

Connect to a 100V–240V AC Socket

Warning **Use ONLY the power adapter, power cord, and plugs that we supply for your DMP model explicitly. DO NOT USE OTHERS, even if they appear identical or appear to work with another DMP model.**

Before You Begin

- Did your Cisco equipment ship with a power cord and AC adapter? Or did it ship with an AC adapter and multiple, snap-on plugs? Your packing list states which supplies Cisco planned to ship. (Alternatively, you might have purchased a Cisco power cord and AC adapter as accessories for your equipment.)
- To learn which Cisco power cords and AC adapters are compatible with your DMP, see its datasheet at http://www.cisco.com/go/dms/dmp/datasheets.

Procedure

Step 1 Does your DMP power cord require assembly? If so, assemble it.

a. Identify the correct snap-on plug for your region.

b. Snap that plug onto the AC adapter.

Step 2 Connect the DMP power cable to the AC adapter.

Step 3 Connect the DC barrel connector to the DC power supply on the DMP chassis.

Step 4 Connect to an AC electrical outlet that you know is grounded. It must use the correct voltage level for your locale. Supported levels range from 100V to 240V.

Note **To protect your DMP from electrical surges, we recommend that you use a surge protector or an uninterruptable power supply from a reputable manufacturer.**

Step 5 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- DMP Power Cord Options, page 14
- Use 802.3af Power over Ethernet (PoE), page 16

Use 802.3af Power over Ethernet (PoE)

Note

- **You can power a DMP 4310G through its Ethernet cable.** Other DMP models do not support this feature.
- **A DMP 4310G has two USB interfaces on its chassis.** When you use PoE to power a DMP 4310G, we recommend that you use no more than one of these USB interfaces at a time. IEEE 802.3af PoE is limited in its capacity and might not be sufficient to power your DMP and two USB peripherals simultaneously.
- **When both PoE power and AC power are detected, AC power overrides PoE and disconnects the PoE circuit.**

Procedure

Step 1 Use the On/Off power button on the DMP chassis to verify that your DMP is turned **Off**.

Step 2 Connect a standard, Category 5 Ethernet cable to your DMP.

Step 3 Attach the other end of the Ethernet cable to a PoE-enabled network switch that operates inside your network.

Step 4 Use the On/Off power switch on the DMP chassis to turn your DMP **On**.

Step 5 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- DMP Power Cord Options, page 14
- Connect to a 100V–240V AC Socket, page 16

Connect to a Network

Use a connection method—wired or wireless—that your DMP and topology both support. Physical Ethernet connections take priority over 802.11 b/g on DMPs where both are active.

Tip **To learn which connection methods your DMP supports, see Table 2.** Alternatively, if the table does not describe your DMP model, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.

- Understand Whether the IP Address Will Be Static or Dynamic, page 17
- Establish an Ethernet Connection, page 18
- Wireless (802.11 b/g) Connection Procedures, page 22

Understand Whether the IP Address Will Be Static or Dynamic

The factory-default behavior for every DMP is to obtain and use a dynamic IP address from a DHCP server in its local network segment.

Nonetheless, your DMP must have an IP address—even when you will deploy it where the local network segment does not include any DHCP server among its nodes. In this case, you must configure your DMP before you deploy it. This technique is sometimes called a *green field deployment*. The configuration steps differ in Ethernet and wireless networks.

Related Topics

- Prepare Your DMP to Use a Static IP Address Over Ethernet, page 32
- Prepare Your DMP to Use a Static IP Address Over Wireless, page 34

Establish an Ethernet Connection

Before You Begin

- Does a security policy in your network restrict DHCP address assignments to known MAC addresses? If so, locate the **MAC** address printed on a sticker that is affixed to your DMP. Then, share this address with your security policy administrator.
- Does your DMP support wireless networking? If so, consider whether you might prefer to use that method instead of this one.

Procedure

Step 1 Plug one end of a standard Ethernet cable into the corresponding interface on your DMP.

Step 2 Plug the other end of this cable into a network hub, network switch, or router whose network uses DHCP to allocate IP addresses dynamically.

Step 3 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Wireless (802.11 b/g) Connection Procedures, page 22

Wireless Connection Concepts

- Glossary, page 18
- Workflow, page 21
- Understand WEP Keys and Passphrases, page 21

Glossary

Timesaver Go to terms that start with... [**numerals** | **A** | **C** | **E** | **P** | **S** | **T** | **W**].

numerals

802.11b A wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g A wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

A

AAA Authentication, Authorization, and Accounting.

See also EAP-FAST, EAP-MD5 server, LEAP server, and PEAP server.

access point A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

C

Return to Top

CCMP AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. It is based on the Advanced Encryption Standard (AES), as defined in the National Institute of Standards and Technology's FIPS Publication 197. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

See also WEP keys.

E

Return to Top

EAP *Extensible Authentication Protocol*. A protocol that WPA uses to authorize user access in wireless networks. Common implementations include EAP-FAST and EAP-MD5.

EAP-FAST EAP-FAST is a two-phase implementation of the EAP authentication protocol:

- Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credentials).
- Phase 1, authentication. Uses the PAC to establish a tunnel with the server and authenticate the username and password.

See also AAA and EAP.

EAP-MD5 server Servers that use EAP to provide dynamic, session-specific wireless encryption keys, central user administration, and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords.

See also AAA and EAP.

P

Return to Top

PEAP server *Protected EAP* server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also AAA, EAP-MD5 server, and WEP keys.

PSK Pre-Shared Key.

S

Return to Top

SSID

Service Set ID. A unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish among multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

Caution **The Broadcast SSID setting must be enabled on your wireless access points.** Otherwise, your DMPs are prevented from connecting to your WLAN or obtaining IP addresses.

Caution **Whenever you change SSID settings for your WLAN, your DMPs will lose their wireless network connections.** After they are disconnected, they cannot reconnect automatically. In this case, an affected DMP will appear to associate to your WLAN access point but will not receive any IP address.

T

Return to Top

TKIP

Temporal Key Integrity Protocol, also known as key hashing, is used as part of server-based EAP authentication.

W

Return to Top

WEP

Wired Equivalent Privacy is a method to encrypt data transmitted on a wireless network.

WEP keys

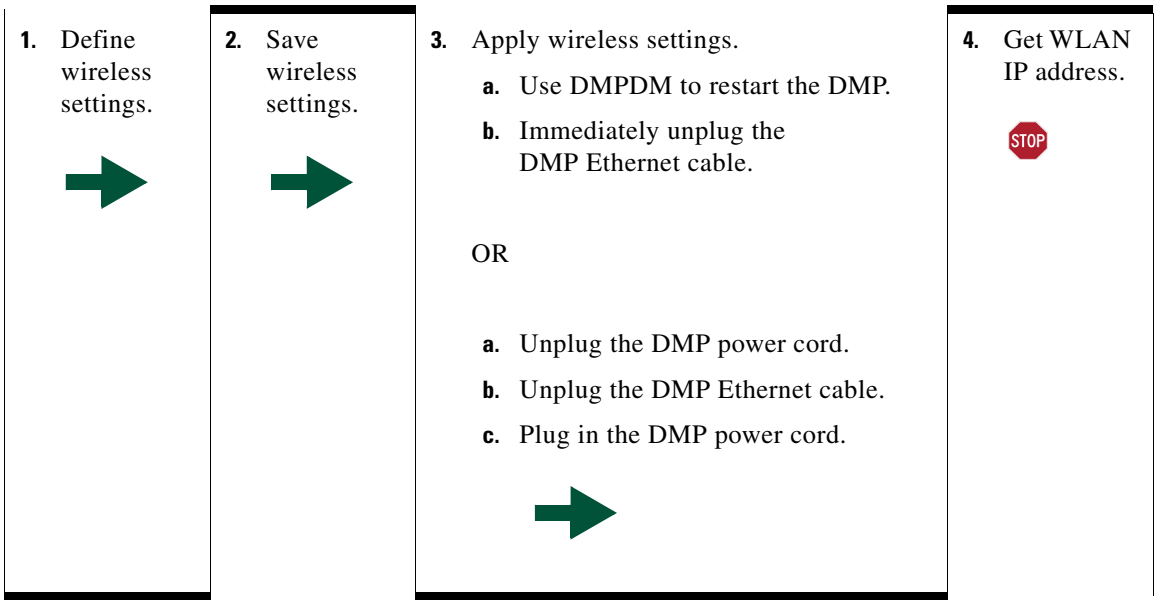
Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism to secure wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing decryption only by users with the correct WEP keys.

WPA

Wi-Fi Protected Access. WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP for data protection and 802.1X for authenticated key management.

Workflow

It is not necessary, useful, or correct to restart a DMP immediately after you define its 802.11 settings. Instead, the typical workflow is as follows.



Understand WEP Keys and Passphrases

Timesaver **Does your wireless network use WPA instead of WEP?** If so, you can ignore this topic.

Many 802.11 access points (wireless routers) accept only a hexadecimal passphrase for WEP-64 and WEP-128. And yet, DMPs accept only an ASCII passphrase for WEP. For this reason, it might be necessary at times to translate your WEP passphrase from ASCII to hexadecimal. Many third-party converters are available. We do not offer any Cisco converter for this purpose.

The typical WEP process is as follows.

1. Pick an ASCII passphrase. For example, *PassphraseWEP128*.
2. Convert your string of ASCII characters to the hexadecimal key or keys for your network.
   - WEP-64 uses four short hexadecimal keys.
   - WEP-128 uses one long hexadecimal key.
3. Configure your DMP to use the ASCII from which you derived the hexadecimal.
4. Configure your wireless router to use the appropriate hexadecimal key or keys.

Related Topics

- Wireless (802.11 b/g) Connection Procedures, page 22

Wireless (802.11 b/g) Connection Procedures

Note **You can configure wireless network settings during a later phase of DMP setup, if your DMP supports this feature.** However, there are other tasks that you must finish first. When you are ready to configure wireless settings, these topics say how.

- Establish a Wireless Network Connection, page 30
- Prepare Your DMP to Use a Static IP Address Over Wireless, page 34

Connect to a Presentation System

A DMP transmits signals to a public presentation system that you choose, such as a flat-panel display or projector that is connected to the DMP.

- This system might use projection or display technologies that are analog or digital.
- It might support Standard Definition (SD) or High Definition (HD).
- Its output fidelity depends in part upon which signal cables (and adapters) connect it to your DMP.

Tip **A feature of *Cisco Digital Signs* can detect automatically when some display brands and models are turned On or Off.** To connect one of these displays to your DMP, you must use an RS-232 serial cable in addition to the video signal cable. *Cisco Digital Signs* documentation on Cisco.com explains how to use this feature in your network.

Topics in this section teach you about these presentation systems, signal cables, and adapters.

- Concepts, page 22
- Procedures, page 25

Presentation System Concepts

- Understand Which Displays Work Best with DMPs, page 23
- Understand How to Choose Media Signal Cables, page 23
- Understand How to Work Around the Low Signal Quality of Composite Video Cables, page 25
- Understand How HDMI and DVI Differ, page 25

Understand Which Displays Work Best with DMPs

We certify that DMPs work as designed with Cisco LCD flat-screen displays. All displays in this series are engineered for intensive use in public settings. See http://cisco.com/go/dms/lcd.

In most cases, DMPs can use displays that comply with modern, international standards. We recommend the following if you use a third-party display.

- **Digital, not analog.**
- **High-definition, not standard-definition.**
- **Professional-grade, not consumer-grade.** Digital signs and public IPTV installations run many more hours each day than a consumer-grade display is engineered to run. A consumer-grade system is likely to fail years sooner than a professional-grade system would under these conditions.
- **LCD, not plasma.** Digital signage uses static images more often than it uses full-motion video. Most often, content is web-based or animated in Flash. The nature of these media types means that some pixels are not updated frequently in digital signage. LCDs are less susceptible to burn-in than plasma displays are. Even though image persistence is sometimes a problem on LCD displays, it is almost always self-correcting and is unlikely to occur when you follow manufacturer guidelines for managing your displays correctly.
- **Built-in support for RS-232 signalling.** This recommendation is important in direct proportion to the number of displays that you will manage.

Understand How to Choose Media Signal Cables

Caution **Poorly shielded cable can sometimes promote undesired signal leakage (*egress*), interference from over-the-air signals (*ingress*), or crosstalk between cables that are in close physical proximity.**

Special considerations apply when you obtain a signal cable that is longer or of a different type than cables that we included in your product kit. For DMP models that support the following signal cable types, the maximum supported lengths are:

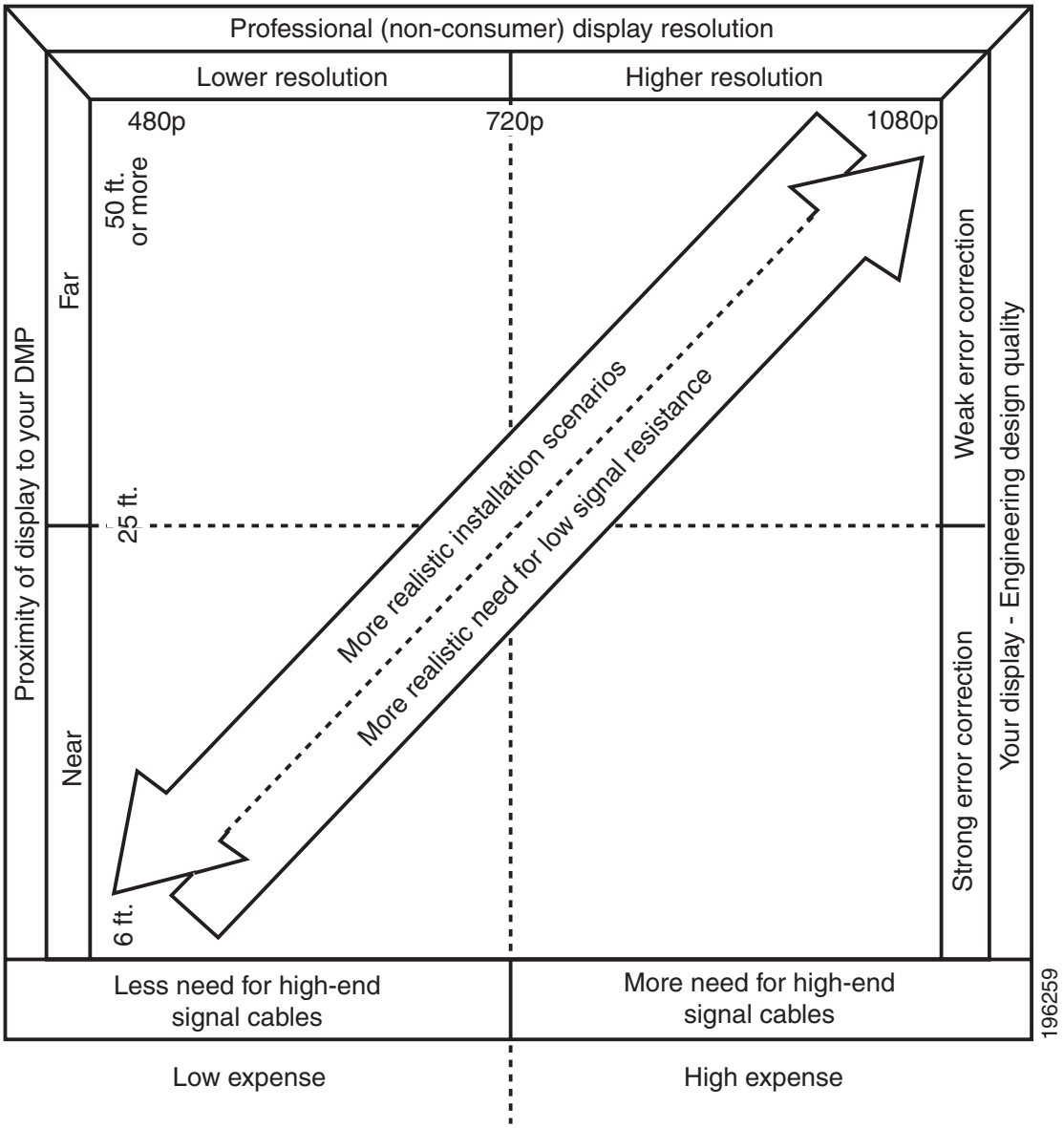
- Composite—10 ft (approximately 3 m)
- HDMI—16 ft (approximately 5 m)
- RCA—10 ft (approximately 3 m)
- S-Video—10 ft (approximately 3 m)
- SPDIF—10 ft (approximately 3 m)

Cable Quality

The best signal cables objectively are those with the lowest signal resistance. Factors that affect signal resistance include wire gauge, cable shielding quality, and cable connector quality. However, the same materials and engineering designs that reduce signal resistance add to the cost of manufacturing. This added cost is passed along to a consumer. So, it is useful to understand when signal resistance is not relevant. Knowing this can help you to manage and reduce expenses without necessarily lowering your standards. High cost is not inevitable. Nor is it proof of high quality. Sometimes, in fact, high quality (low signal resistance) is irrelevant.

Even mediocre signal cables are sometimes sufficient, and such cables are often very affordable. Figure 1 illustrates the most important factors to consider when you choose signal cables.

Figure 1 Signal Cable Purchasing Factors to Consider



Beyond the general guidelines that Figure 1 illustrates, two additional factors might constrain which types of signal cable you can use.

- **The technology, brand, and model of your display**—Check its product documentation to understand its compatibility with various signal cable types.
- **The DMP model**—Table 2 on page 12 states which I/O ports are available on various DMP models. Alternatively, if the table does not describe your DMP model, see its datasheet at http://www.cisco.com/go/dms/dmp/datasheets. Your packing list states which signal cables Cisco planned to ship with your DMP.

Related Topics

- Connect to a Presentation System, page 22

Understand How to Work Around the Low Signal Quality of Composite Video Cables

Note **When image signals are transmitted through a composite cable, image quality suffers.** When you use a composite cable and your DMP shows any web-based media, small text might be difficult to read in TVzilla. To work around this limitation, you can lower the browser resolution setting in DMPDM.

Related Topics

- TVzilla, page 5
- Connect to a Presentation System, page 22

Understand How HDMI and DVI Differ

With most modern, digital presentation systems, you can use an HDMI cable for both video and audio.

Other such systems might not connect until you combine the HDMI cable with an HDMI-to-DVI adapter for video. However, DVI does not support the transmission of audio signals. In this case, you can use the provided audio cable for audio.

Related Topics

- Connect to a Presentation System, page 22

Presentation System Procedures

- Use an HDMI Connection, page 26
- Use a Connection that Combines HDMI with DVI, page 26
- Connect to a Touchscreen, page 27
- Connect to an Analog Display or Projector, page 28

Use an HDMI Connection

Timesaver **Is your display a touchscreen?** If so, you can this topic. Instead, see the "Connect to a Touchscreen" section on page 27.

Procedure

Step 1 Connect the HDMI cable to the **HDMI** interface on the back panel of your DMP.

Step 2 Connect the other end of the cable to your presentation system.

Step 3 Turn **On** the presentation system.

Step 4 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Use a Connection that Combines HDMI with DVI, page 26

Use a Connection that Combines HDMI with DVI

Timesaver **Is your display a touchscreen?** If so, you can ignore this topic. Instead, see the "Connect to a Touchscreen" section on page 27.

HDMI and DVI differ in their support for audio signals and use connectors that are shaped differently, but otherwise are identical. Thus, an adapter can help you to connect to your DMP any presentation system that supports DVI but not HDMI. When you do this, however, you must also use a separate signal cable to transmit audio signals, or there will not be any audio.

Before You Begin

- Obtain an HDMI-to-DVI adapter.

Procedure

Step 1 Make connections for video.

a. Connect the HDMI cable to the **HDMI** interface on the back panel of your DMP.

b. Fasten an HDMI-to-DVI adapter to the free end of the cable.

c. Connect the free end of the DVI adapter to the corresponding interface on your presentation system.

Step 2 Make connections for audio.

a. Plug the 3.5mm audio jack into the **Audio** interface on the back panel of your DMP.

b. Connect the other end of the audio cable to the corresponding interface on your presentation system.

Step 3 If the presentation system is not already turned on, turn it **On** now.

Step 4 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Use an HDMI Connection, page 26

Connect to a Touchscreen

Tip **Some touchscreens work as designed only after they are calibrated manually.** If your touchscreen is one of these, its calibration occurs during a later stage of DMP setup. The list of related topics for this procedure states where you can learn about calibration.

DMP connections to a touchscreen are mostly the same as for other digital displays. However, touchscreens employ a special cable that supports interactivity through touch. This might be either an RS-232 serial cable or a USB cable, depending on the touchscreen model. Although some models support both cable types for interactivity, you can use only one type at a time.

Before You Begin

- Verify that your DMP model supports touchscreen technologies and that we support the touchscreen brand, model, and device driver that you will use. See http://www.cisco.com/go/dms/compatibility.
- Check the documentation for your touchscreen to learn whether it requires a serial connection or a USB connection to your DMP, or if it supports both.

Procedure

Step 1 Connect an HDMI cable to the **HDMI** interface on the back panel of your DMP.

Step 2 Connect the other end to your touchscreen.

OR

If your touchscreen supports DVI connections and not HDMI connections:

- Fasten an HDMI-to-DVI adapter to the free end of the cable.
- Connect the free end of the DVI adapter to the corresponding interface on your touchscreen.

Tip **You can use an HDMI splitter or other supported method to attach multiple presentation systems to a DMP.** However, only one of these systems can be a touchscreen.

Step 3 Do only one of the following.

- Connect a USB cable to the **USB** interface on the back panel of your DMP. Then, connect the other end to your touchscreen.

  Does your DMP model have only one USB connector? If so, you might prefer to connect an external hard drive there for added local storage. In this case, an RS-232 serial cable would be the better choice for connecting a touchscreen to your DMP.

- Connect an RS-232 serial cable to the **RS232** interface on the back panel of your DMP. Then, connect the other end to your touchscreen.

Step 4 Turn **On** the touchscreen.

Tip **Does a message on the touchscreen say that it must download a "characterization" file?** This happens only when your touchscreen uses technologies from Elo TouchSystems and when you have never turned it On previously (or after its flash memory card is reformatted). When you see this message, please disregard it. The touchscreen will obtain its characterization file automatically during a later stage of DMP setup.

Step 5 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Choose and Calibrate a Touchscreen Driver, page 37

Connect to an Analog Display or Projector

Tip **DMPs support connections to analog presentation systems,.** However, we recommend strongly that you use *digital* presentation systems whenever possible.

Procedure

Step 1 Make connections for video.

a. Plug one yellow jack from the RCA video cable into the **CVBS** interface on the back panel of your DMP.

b. Connect the free end of this cable to the corresponding interface on your presentation system.

Step 2 Make connections for audio.

a. Plug the 3mm jack on the RCA audio cable into the **AUDIO** interface on the back panel of your DMP.

b. Connect the free end of this cable to the corresponding interface on your presentation system.

Step 3 If the presentation system is not already turned on, turn it **On** now.

Step 4 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Understand How to Work Around the Low Signal Quality of Composite Video Cables, page 25

Configure Settings

- Log in to DMPDM, page 29

RECOMMENDED SETTINGS

- Configure Video Output, page 36
- Configure NTP Settings for Time-Dependent Features, page 40

OPTIONAL SETTINGS

- Establish a Wireless Network Connection, page 30
- Prepare Your DMP to Use a Static IP Address Over Ethernet, page 32
- Prepare Your DMP to Use a Static IP Address Over Wireless, page 34
- Choose and Calibrate a Touchscreen Driver, page 37

Log in to DMPDM

Before You Begin

- This procedure assumes that you connected your DMP to its presentation system, and now they are both turned On.

Procedure

Step 1 While your presentation system shows the Cisco logo and shows an IP address for your DMP, write down the IP address.

Tip **Later, you can change how long this splash screen is visible during startup.** See the "Edit the Splash Screen Duration to Obscure the DMP IP Address" section on page 43.

Step 2 Point your browser to the IP address that you wrote down.

Note **Use HTTPS as the connection protocol.** The connection fails when you use HTTP instead of HTTPS. This failure occurs by design, to support security in your network.

Step 3 Respond to the prompt. It sometimes varies.

- **Does it ask you to EDIT a password before you can log in?**

  The first time that you start DMPDM, it prompts you to change its factory-defined master password. You will never see this prompt again, unless you restore your DMP to its factory-default settings.

  a. Enter a new master password that contains at least eight characters, which combine uppercase and lowercase letters with numerals

  b. Click **Activate**.

- **Does it ask you to ENTER a password so that you can log in?**

  a. Use the login name **admin**.

  b. Use whichever master password you saved most recently.

Step 4 Stop. Remain logged in. You have completed this procedure.

Related Topics

- Protect Your DMP from Unauthorized Management

Establish a Wireless Network Connection

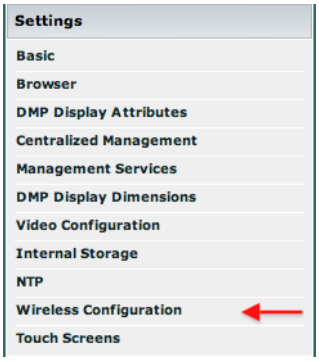
Timesaver **Complete this optional procedure at your discretion.**

Before You Begin

- Do the hardware and firmware for your DMP support wireless networking? DMP 4305G and DMP 4310G endpoints **do not**.
  - To verify whether you must use an Ethernet cable, see Table 2 on page 12.
  - Alternatively, if Table 2 does not describe your DMP model, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.
- The Broadcast SSID setting must be enabled on your wireless access points (also known as *wireless routers* or *WLAN controllers*). Otherwise, your DMPs cannot connect to your WLAN and are prevented from obtaining IP addresses.
- We do not support “open” wireless networks. They are a security risk.
- Does a security policy in your network restrict DHCP address assignments to known MAC addresses? If so, locate the **WLAN** address printed on a sticker that is affixed to your DMP. Then, share this address with your security policy administrator.
- Verify that your wireless network is working correctly, is available, and you understand how it authenticates connection requests.
- Establish an Ethernet Connection.
- Log in to DMPDM.

Procedure

Step 1 Click **Wireless Configuration** in the Settings list.



Tip **Do you see this option in DMPDM?** If not, your DMP might not support wireless networking. See Table 2 on page 12.

Step 2 Choose **Enabled** from the Wireless Interface list.

Each 802.11 wireless network is assigned a name to distinguish it from other networks. The technical term for this network name is *Service Set Identifier*, or SSID.

Step 3 Double-click the SSID for your network in the Detected Networks table.

OR

When you do not see your SSID in the Detected Networks table, do the following.

a. Enter in the Network SSID field the SSID for your network.

b. Choose from the Security list the security method for your network. Its options are:

- WEP-64bit
- WEP-128bit
- WPA-PSK
- WPA-EAP
- WPA2-PSK
- WPA2-EAP

The security method that you choose controls, in part, which fields and options this DMPDM page shows to you.

- When you see the PSK field and you chose a WEP-based security method, enter in it the key from which your 64-bit or 128-bit passphrase is cryptographically derived.
- When you see the PSK field and you chose a WPA-based or WPA-2-based security method, enter in it the pre-shared key for your network.
- When you see the Encryption list, choose from it either **TKIP** or **CCMP AES**.

- When you see the EAP list, choose from it either **FAST**, **MD5**, or **PEAP (ver.0)**.
- When you see the Username and Password fields, enter in them respectively a valid username for your wireless network and the password for that username.

c. Choose **Enabled** from the Dynamic IP Addressing (DHCP) list.

Tip **Will you ever deploy your DMP in a wireless network that does not have any DHCP server?** If so, this guide can tell you how to configure a static IP address on your DMP.

d. Click **Probe** to check whether these settings work correctly with your wireless network.

e. When you are satisfied with your choices, Click **Select**.

f. Click **Save Configuration** in the Administration list, and then click **Save**.

Step 4 Disconnect the Ethernet cable from your DMP.

Step 5 Click **Restart DMP** in the Administration list, and then click **Restart**.

Step 6 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12
- Establish an Ethernet Connection, page 18
- Prepare Your DMP to Use a Static IP Address Over Wireless, page 34

Prepare Your DMP to Use a Static IP Address Over Ethernet

Timesaver **Complete this optional procedure at your discretion.** It explains what to do when a DMP's ultimate deployment site does not use DHCP.

Before You Begin

- Establish an Ethernet Connection.

  OR

  Obtain an Ethernet crossover cable.
- Do one of the following.
  - Transport your DMP to a site where the local network segment includes a DHCP server and ensure that you have access there to a web browser.
  - Configure any system at your current location to run temporarily as a DHCP server and ensure that you have access to a web browser.

Procedure

Step 1 Connect your DMP to its presentation system.

Step 2 Turn **On** the presentation system and then do one of the following.

- Use a standard, category 5 (RJ-45) Ethernet cable—either 10/100 or 10/100/1000, depending on your DMP model—to connect your DMP to the network segment that includes the DHCP server.
- Use an Ethernet crossover cable to connect your DMP directly to the DHCP server.

Step 3 If the DHCP server process is not running yet on the DHCP server, start that process now—along with any processes that it uses.

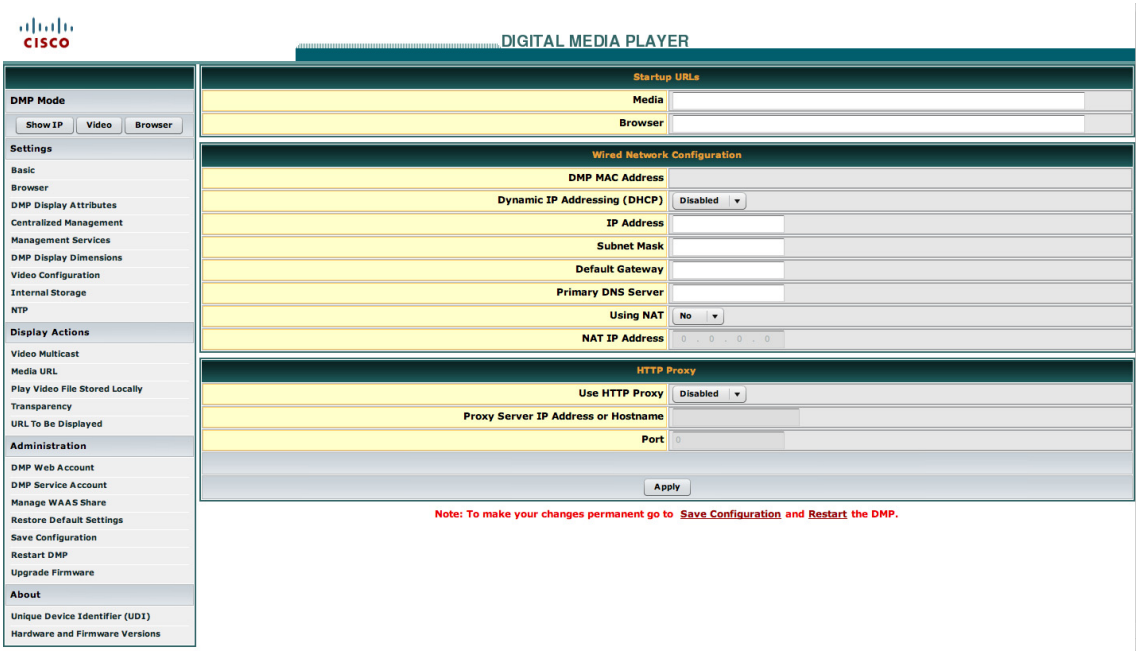
Step 4 Turn **On** your DMP and make a note of the IP address that it shows on its presentation system.

Step 5 Point your browser to the IP address.

Note **Is your DMP brand-new?** Or, have its settings been restored to factory defaults? If so, DMPDM prompts you to define a master password for your DMP. You must do this before you can do anything else. See the "Log in to DMPDM" section on page 29.

Step 6 When prompted to log in, use the master username and password that you defined.

DMPDM loads its basic settings page in your browser. Options in DMPDM vary by DMP model.



Step 7 Choose **Disabled** from the Dynamic IP Addressing (DHCP) list, and then:

a. Enter in the IP Address field the static IP address that your DMP should use.

b. Enter in the Subnet Mask field the netmask that your DMP should use with its static IP address.

c. Enter in the Default Gateway field the network gateway that your DMP should use with its static IP address.

d. Enter in the Primary DNS Server field the DNS server that your DMP should use with its static IP address.

Step 8 Will a network address translation (NAT) service give your DMP a private IP address? If so:

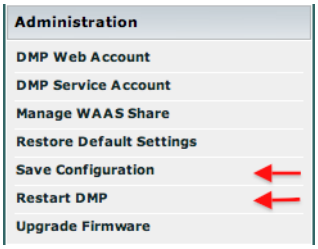
a. Choose **Yes** from the Using NAT list.

b. Enter in the NAT IP Address field the 1-to-1 public address (which is configured on the local router) that corresponds to the private IP address.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 11 Click **Restart DMP** in the Administration list, and then click **Restart**.



Step 12 Ship or deliver the DMP to its deployment site, and then:

a. Connect it to its presentation system.

b. Connect it to its local network segment.

c. Connect it to its power source.

Step 13 Stop. You have completed this procedure.

Related Topics

- Prepare Your DMP to Use a Static IP Address Over Wireless, page 34

Prepare Your DMP to Use a Static IP Address Over Wireless

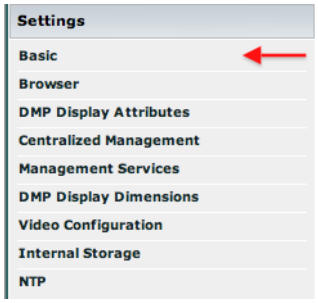
Timesaver **Complete this optional procedure at your discretion.** It explains what to do when a DMP's ultimate deployment site does not use DHCP.

Before You Begin

- Verify that your wireless network is working correctly, is available, and you understand how it authenticates connection requests.
- Establish an Ethernet Connection.
- Establish a Wireless Network Connection.
- Log in to DMPDM.

Procedure

Step 1 Click **Basic** in the Settings list.



Step 2 Choose **Disabled** from the Dynamic IP Addressing (DHCP) list, and then:

a. Enter in the IP Address field the static IP address that your DMP should use.

b. Enter in the Subnet Mask field the netmask that your DMP should use with its static IP address.

c. Enter in the Default Gateway field the network gateway that your DMP should use with its static IP address.

d. Enter in the Primary DNS Server field the DNS server that your DMP should use with its static IP address.

Step 3 Will a network address translation (NAT) service give your DMP a private IP address? If so:

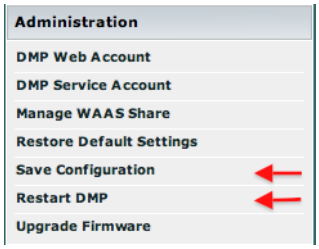
a. Choose **Yes** from the Using NAT list.

b. Enter in the NAT IP Address field the 1-to-1 public address (which is configured on the local router) that corresponds to the private IP address.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 6 Click **Restart DMP** in the Administration list, and then click **Restart**.



Step 7 Ship or deliver the DMP to its deployment site, and then:

a. Connect it to its presentation system.

b. Connect it to its local network segment.

c. Connect it to its power source.

Step 8 Stop. You have completed this procedure.

Related Topics

- Prepare Your DMP to Use a Static IP Address Over Ethernet, page 32

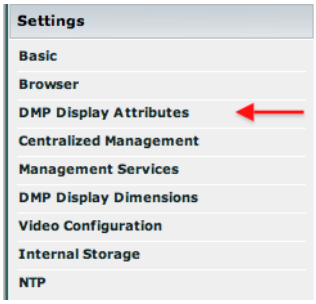
Configure Video Output

Before You Begin

- Connect your DMP to its presentation system.
- Log in to DMPDM.

Procedure

Step 1 Click **DMP Display Attributes** in the Settings list.



The display autodetection feature is enabled by default. However, it fails unless you use either:

- An HDMI signal cable.
- An HDMI signal cable in combination with an HDMI-to-DVI adapter.

Note **Are you satisfied with the choices and entries that the autodetection feature made for you?** If so, you are done with this section and you can go now to the "Protect Your DMP from Unauthorized Management" section on page 44. Otherwise, if you are not satisfied—or if your display does not support HDMI connections—do the following.

a. Choose **Disable** from the DMP Display Autodetection (requires HDMI) list.

b. Choose a standard from the Display Standard list that applies in your country. For example, even though our factory default selection is NTSC_M, your country might use **PAL** instead.

c. Choose your connector and signal type from the Interface (DMP display output) list. For example, you might use **SVIDEO**.

   If you do not know which options to choose, see the manufacturer documentation for your presentation system.

Step 2 Choose from the Color Space list the absolute color space that your presentation system uses.

Step 3 Did you choose RGB as the color space? If so, choose an option from the Color Component Order list to define the order in which to store red, green, and blue data.

The color component order is sometimes called the left-to-right additive color model.

Step 4 Move any or all of the sliders as needed to compensate for presentation system deficiencies in video (brightness, contrast, or saturation) or audio (channel volume).

Step 5 Click **Apply** to confirm your choices and to implement them until you change them or until you restart your DMP.

Step 6 Click **Show IP**—in the DMP Mode area—to test whether your choices are suitable ones for your presentation system.

Your presentation system should show a Cisco logo and should show the IP address for your DMP.

Tip **Later, you can change how long this splash screen is visible during startup.** See the "Edit the Splash Screen Duration to Obscure the DMP IP Address" section on page 43.

Step 7 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 8 Stop. You have completed this procedure.

Related Topics

- Physical Interfaces (I/O Ports), page 12

Choose and Calibrate a Touchscreen Driver

This procedure applies to you only when your DMP supports interactivity through touch and your presentation system is a touchscreen. Furthermore, it assumes that you completed the "Connect to a Touchscreen" section on page 27.

Before You Begin

- Do the hardware and firmware for your DMP support touchscreen technologies? DMP 4305G and DMP 4310G endpoints **do not**.
- Do we support the touchscreen brand, model, and device driver that you will use? See http://www.cisco.com/go/dms/compatibility.
- Log in to DMPDM.

Procedure

Step 1 Does your touchscreen show a message that says it must download a "characterization" file?

- If so:
  - Do not disturb or interrupt this process. It occurs only once, automatically.
  - The process takes approximately 10 minutes to finish. When it is finished, your touchscreen will clear the message automatically.
  - ***Stop***. *You have completed this procedure and there is no need to perform any of its other steps.*
- Otherwise, go to Step 2.

Step 2 Because some touchscreen drivers cannot be calibrated on a DMP while it is playing video, use DMPDM to stop all videos.

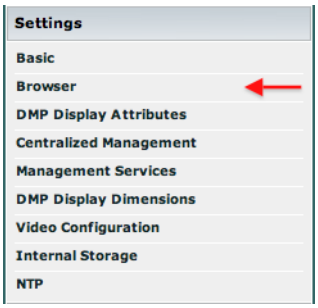
a. Click **Video Multicast** in the Display Actions list, and then click **Stop**.

b. Click **Media URL** in the Display Actions list, and then click **Stop**.

Step 3 Choose the browser rotation angle for your touchscreen.

Supported rotation angles are 0°, 90°, 180°, and 270°.

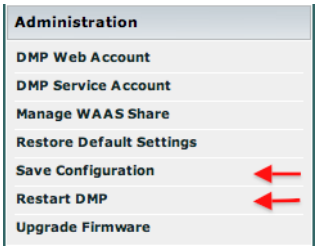
a. Click **Browser** in the Settings list.



b. Choose an option from the Screen Rotation Angle (clockwise) list, and then click **Apply**.

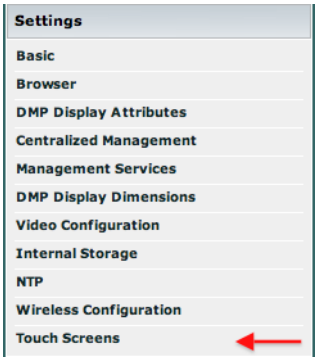
c. Click **Save Configuration** in the Administration list, and then click **Save**.

d. Click **Restart DMP** in the Administration list, and then click **Restart**.



Step 4 After your DMP restarts, log in again to DMPDM.

Step 5 Click **Touch Screens** in the Settings list.



Tip **Do you see this option in DMPDM?** If not, your DMP might not support it. But you can learn whether any firmware upgrade is available that adds this feature to your DMP model.

- See our release notes—http://cisco.com/go/dms/releasenotes.
- See our compatibility information—http://cisco.com/go/dms/compatibility.

If newer firmware is available, follow the published instructions to obtain it. Then, complete the firmware upgrade procedure in your DMPDM user guide at http://cisco.com/go/dms/dmpdm.

The nature of your Cisco DMS service contract might limit:

- Which upgrades are available to you.
- Where and how you obtain upgrades.
- Whether you must pay anything to obtain upgrades.

To learn about Cisco service contracts, see http://cisco.com/go/cscc.

a. Check the Currently Loaded Driver row to see which touchscreen driver, if any, is active on your DMP.

The driver might be **3M**, **Zytronic**, **Elo**, **GeneralTouch**, or possibly something else. As we test various drivers, we might update this list between any two releases.

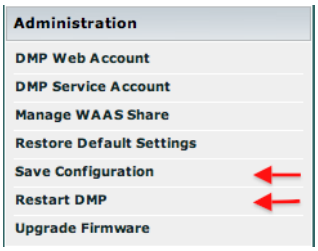
Your DMP must use a driver that is compatible with your touchscreen.

b. If the active driver is not compatible with your touchscreen, choose the compatible driver from the Choose Touch Screen to Activate list.

c. Click **Apply**.

d. Click **Save Configuration** in the Administration list, and then click **Save**.

e. Click **Restart DMP** in the Administration list, and then click **Restart**.

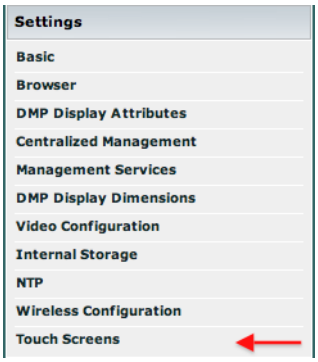


Tip **The Elo and GeneralTouch drivers are self-calibrating.**

Step 6 If you chose 3M, Zytronic, or another driver that must be calibrated manually:

a. After your DMP has restarted, log in again to DMPDM.

b. Click **Touch Screens** in the Settings list.



c. Click **Calibrate** <*driver_name*> **Screen**, where *driver_name* is the name of the driver that you chose.

- Messages on the touchscreen prompt you to touch its surface in various places. Follow these prompts exactly. For example, the calibration utility might prompt you to touch exactly five areas or exactly nine areas.
- Time is limited. When you do not complete this exercise within the brief period that is allotted for it, the calibration utility times out automatically.
- Repeat these steps for manual calibration if the driver utility times out before you can finish.

Note **You must repeat the calibration whenever you:**

- Rotate a touchscreen or change its resolution.
- Replace a touchscreen.

Step 7 Stop. You have completed this procedure.

Related Topics

- Connect to a Touchscreen, page 27

Configure NTP Settings for Time-Dependent Features

IP-enabled devices including DMPs can use *network time protocol* (NTP) to synchronize themselves with radio and atomic clocks located on the Internet. Thus, the accuracy of their local time-keeping is ensured. NTP can synchronize distributed clocks within milliseconds over long time periods. You must configure NTP settings on any DMP through which you will provide:

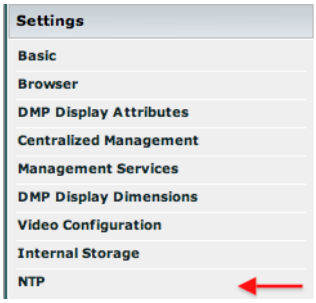
- IPTV services with *Cisco Cast*.
- Proof-of-play services with *Cisco Digital Signs*.
- Any other service that is dependent upon accurate Start and Stop times.

Before You Begin

- Log in to DMPDM.

Procedure

Step 1 Click **NTP** in the Settings list.



Step 2 Choose **On** from the Enable NTP Service list.

Step 3 Use the fields marked Hostname 1, Hostname 2, and Hostname 3 to specify which NTP servers your DMP should use.

- Hostname 1—Enter the DNS-resolvable name of the network time server to use by default. This is your primary time server. Your DMP will not use any other unless this one is not available.

  Note **We recommend that you set the default NTP hostname to pool.ntp.org.**

- Hostname 2—Enter the DNS-resolvable name of a network time server to use whenever the primary time server is not available.
- Hostname 3—Enter the DNS-resolvable name of a network time server to use whenever the secondary time server is not available.

Step 4 Choose from the Time Zone list the time zone that is correct and local for your DMP at its location.

Step 5 Enter in the Refresh Interval field the maximum number of milliseconds that are permitted to elapse before your DMP retrieves a fresh time stamp from its NTP server. The factory-default maximum is 17 ms.

Step 6 Click **Apply** to confirm and test your choices.

Your entries are recorded to volatile memory and take effect—but only until you change them or restart your DMP.

Step 7 When you are satisfied that you chose the correct settings, click **Save Configuration** in the Administration list, and then click **Save**.

Your entries take effect permanently and will persist even after your DMP restarts.

Step 8 Stop. You have completed this procedure.

Related Topics

- Log in to DMPDM, page 29

Secure Data

Concepts (Security)

Understand DMP User Accounts and Passwords

You use the *Web Account* when you log in to DMPDM itself.

In contrast, the *Service Account* is a user account with FTP and SFTP login privileges. It is available only on DMPs whose FTP service is enabled.

Note **Unless or until you change these passwords individually, they are both identical to the master password that you configured in the "Log in to DMPDM" section on page 29.** You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

Related Topics

- Understand Whether to Change DMP Passwords Centrally, page 42
- Change DMP Passwords in DMPDM, page 45
- Save a Record of Your DMP Passwords in Cisco Digital Signs, page 50

Understand Whether to Change DMP Passwords Centrally

Scenario	Best Practice
You have very few DMPs and will manage each of them in isolation.	Use DMPDM to change their DMP Web Account and DMP Service Account passwords one at a time, manually.
You have many DMPs and will manage them centrally.	Use the fully licensed Cisco Digital Signs software on your Digital Media Manager appliance to change both passwords globally for all of the DMPs that you have added to a DMP group. **Note** Before you can manage any DMP centrally, you must configure it to support centralized management.

Related Topics

- Change DMP Passwords in DMPDM, page 45
- Protect Your DMP from Unauthorized Management, page 44
- Save a Record of Your DMP Passwords in Cisco Digital Signs, page 50

Understand URI Encoding Syntax

When you enter the text string in *Cisco Digital Signs* to change a DMP password, that string must use the correct syntax for *URI encoding*.

- You must enter a plus sign (**+**) instead of a space wherever the value for a queryable object should contain a space. For example, if the queryable object is "user" and its value is "John Smith," you would enter "user=John+Smith" in your string.
- Do any values in the string contain an actual plus sign? If so, you must encode the plus sign explicitly as **%2B**.
- Exclamation points (**!**), question marks (**?**), ampersands (**&**), and asterisks (*****) are forbidden in values.

Tip **Would you like to learn more about URI encoding and syntax?** If so, see RFC 1630 at http://tools.ietf.org/html/rfc1630.

Procedures (Security)

Edit the Splash Screen Duration to Obscure the DMP IP Address

Timesaver **Complete this optional procedure at your discretion.**

You can change how long your DMP shows its splash screen during startup. This is useful when, for example, your organization prefers not to reveal an IP address casually to all observers.

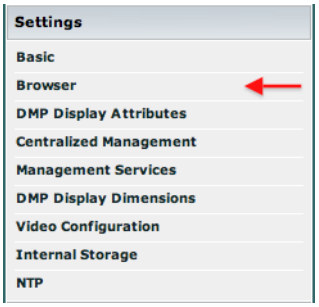
- A duration of 30,000 milliseconds (30 seconds) is the factory default.
- A duration of 1 millisecond turns off the splash screen.
- Any duration in the range from 2 to 5,000 milliseconds (5 seconds) does not have any effect.

Before You Begin

- Log in to DMPDM.

Procedure

Step 1 Click **Browser** in the Settings list.



Step 2 Enter a new duration in milliseconds in the **Splash Screen Display Time (in milliseconds)** field.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 5 Stop. You have completed this procedure.

Protect Your DMP from Unauthorized Management

Caution **Configure your network firewall to restrict access to DMPs over TCP port 7777.** Permit such access from only the DMM appliance where your fully licensed copy of *Cisco Digital Signs* is installed. If you do not know how to define an access control list (ACL), ask the security policy administrator for your network or see the manufacturer documentation for your firewall.

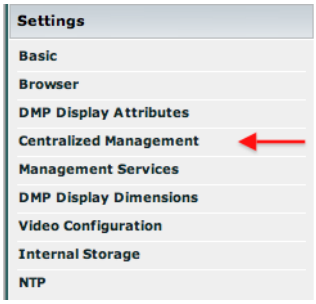
When you use *Cisco Digital Signs* to manage a network of DMPs centrally, you must configure each DMP to secure and trust its communication with *Cisco Digital Signs*.

Before You Begin

- Log in to DMPDM.

Procedure

Step 1 Click **Centralized Management** in the Settings list.



Step 2 Enter in the Digital Signs Server Timeout (sec) field the maximum number of seconds that your DMP should wait for a response from your DMM appliance.

Step 3 Enter the routable DMM appliance IP address or DNS-resolvable hostname in the **DMM Appliance IP Address** field.

Note **Has *Cisco Digital Signs* autodiscovered your new DMP?** If so, the DMM Appliance IP Address field might already be populated with the correct information for your DMM appliance.

Step 4 Click **Apply** to confirm and test your choices.

Your entries are recorded to volatile memory and take effect—but only until you change them or restart your DMP.

Step 5 When you are satisfied that you chose the correct settings, click **Save Configuration** in the Administration list, and then click **Save**.

Your entries take effect permanently and will persist even after your DMP restarts.

Note **Your DMM appliance and your DMP use HTTPS to communicate securely over TCP port 7777 when centralized management is enabled.**

Step 6 Stop. You have completed this procedure.

Related Topics

- Protect Your DMP from Unauthorized Management, page 44
- Log in to DMPDM, page 29

Manage Passwords

Change DMP Passwords in DMPDM

Timesaver **Will you manage your DMPs centrally?** If so, this topic does not apply to you. Instead, see the "Change the Web Account Password for Centrally Managed DMPs" section on page 47 and the "Change the Service Account (FTP/SFTP) Password for Centrally Managed DMPs" section on page 49.

Note **Until you change these passwords individually, they will be identical to the master password that you configured in the "Log in to DMPDM" section on page 29.** You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

You can use DMPDM to change the DMP *Web Account* password and *Service Account* password on one DMP.

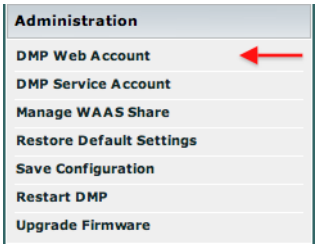
Before You Begin

- Log in to DMPDM.

Procedure

Step 1 Change the Web Account password.

a. Click **DMP Web Account** in the Administration list.

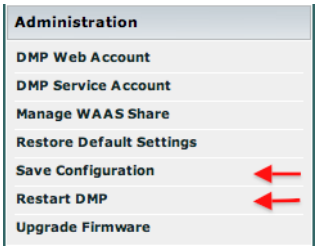


b. Enter your new password in the Password field and again in the Repeat Password field.

c. Click **Apply**.

d. Click **Save Configuration** in the Administration list, and then click **Save**.

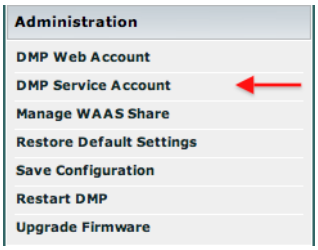
e. Click **Restart DMP** in the Administration list, and then click **Restart**.



Note **Because you changed the password, your trusted DMM appliance—if any—is prevented temporarily from communicating with this DMP.**

Step 2 Change the DMP Service Account password.

a. Click **DMP Service Account** in the Administration list.



b. Enter your new password in the Password field and again in the Repeat Password field.

c. Click **Apply**.

d. Click **Save Configuration** in the Administration list, and then click **Save**.

Step 3 (**Optional**) Is your DMP managed centrally? If so, repeat Step 3 in the "Protect Your DMP from Unauthorized Management" section on page 44.

Step 4 Stop. You have completed this procedure.

Proper communication is restored between your DMP and your trusted DMM appliance.

Change the Web Account Password for Centrally Managed DMPs

Note

- **This procedure assumes that you manage your DMPs centrally.** Furthermore, it assumes that you use *Cisco Digital Signs* and not *Cisco StadiumVision* for this purpose.
- **Until you change this password individually, it will be identical to the master password that you configured in the "Log in to DMPDM" section on page 29.** You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

All DMPs that you manage centrally must share identical user credentials for their DMP *Web Account*.

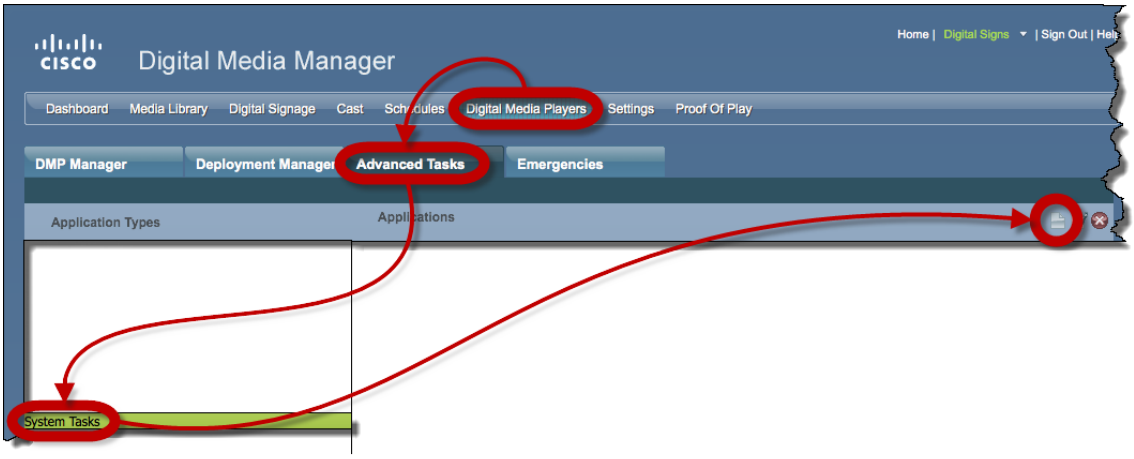
You can use *Cisco Digital Signs* to change the Web Account password simultaneously on DMPs all throughout your network.

Before You Begin

- Protect Your DMP from Unauthorized Management.
- Check that you have installed the license to use *Cisco Digital Signs* on your DMM appliance.
- Log in to the instance of *Cisco Digital Signs* that is licensed to run on your DMM appliance, and verify that your user account permissions there allow you to manage DMPs.

Procedure

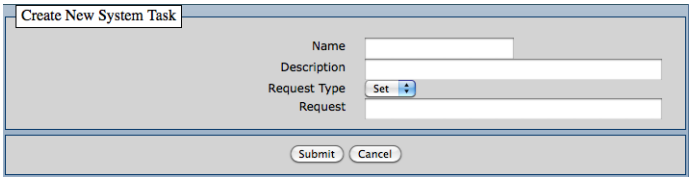
Step 1 Choose **Digital Media Players > Advanced Tasks > System Tasks**, and then click the blank page icon to create a new system task.



Step 2 Enter a name and description for the new task.

Step 3 Choose **Set** from the Request Type list.

Step 4 In the Request text box, enter **`init.WEB_password=`***`new_password`*, where *new_password* is exactly the password that you want to assign to the DMP Web Account user.



Tip **Remember that all request strings must use the correct syntax for URI encoding.** See the "Understand URI Encoding Syntax" section on page 43.

Step 5 Click **Submit** to save the task and make it available to use.

Step 6 Send the password-changing instruction simultaneously to multiple DMPs in your network.

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

b. Choose a group from the DMP Groups object selector.

c. Check the check box for each DMP where the DMP Web Account password should change.

d. Choose from the Select an Event Type list the system task that you named in Step 2.

e. Click **Submit**.

Step 7 Stop. You have completed this procedure.

Change the Service Account (FTP/SFTP) Password for Centrally Managed DMPs

Note

- **This procedure assumes that you manage your DMPs centrally.** Furthermore, it assumes that you use *Cisco Digital Signs* and not *Cisco StadiumVision* for this purpose.
- **Until you change this password individually, it will be identical to the master password that you configured in the "Log in to DMPDM" section on page 29.** You can change them when they should differ. However, they will become identical again in the future if you edit the master password.

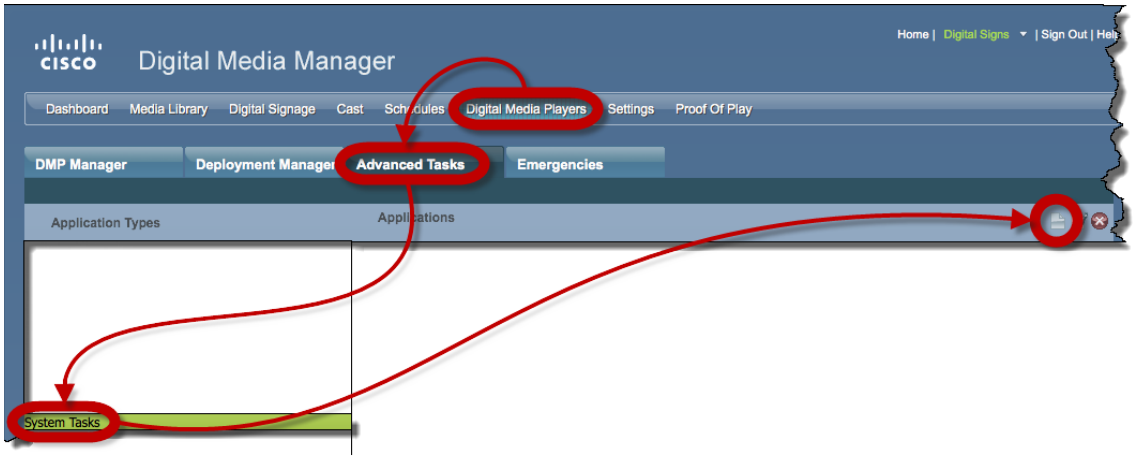
All DMPs that you manage centrally must share identical user credentials for their DMP *Service Account*. You can use *Cisco Digital Signs* to change the Service Account password simultaneously on DMPs all throughout your network.

Before You Begin

- Protect Your DMP from Unauthorized Management.
- Check that you have installed the license to use *Cisco Digital Signs* on your DMM appliance.
- Log in to the instance of *Cisco Digital Signs* that is licensed to run on your DMM appliance, and verify that your user account permissions there allow you to manage DMPs.

Procedure

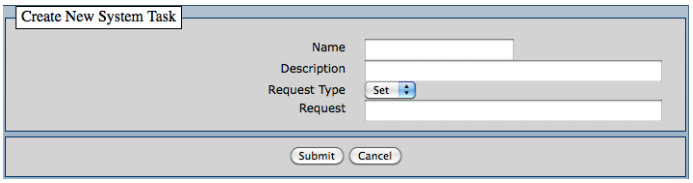
Step 1 Choose **Digital Media Players > Advanced Tasks > System Tasks**, and then click the blank page icon to create a new system task.



Step 2 Enter a name and description for the new task.

Step 3 Choose **Set** from the Request Type list.

Step 4 In the Request text box, enter **`init.FTP_password=`***`new_password`*, where *new_password* is exactly the password that you want to assign to the DMP Service Account user.



Tip **Remember that all request strings must use the correct syntax for URI encoding.** See the "Understand URI Encoding Syntax" section on page 43.

Step 5 Click **Submit** to save the task and make it available to use.

Step 6 Send the password changing instruction simultaneously to multiple DMPs in your network.

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

b. Choose a group from the DMP Groups object selector.

c. Check the check box for each DMP where the DMP Service Account password should change.

d. Choose from the Select an Event Type list the system task that you named in Step 2.

e. Click **Submit**.

Step 7 Stop. You have completed this procedure.

Save a Record of Your DMP Passwords in Cisco Digital Signs

Tell *Cisco Digital Signs* what user credentials to use when it manages your DMPs centrally.

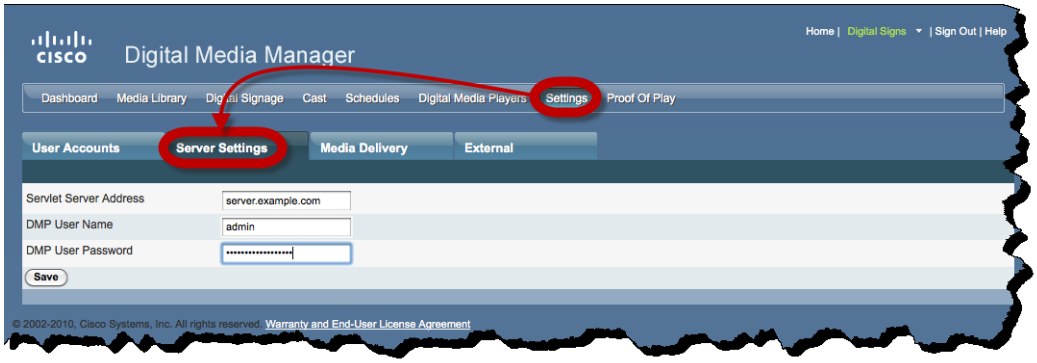
Note **This procedure assumes that you manage your DMPs centrally.** Furthermore, it assumes that you use *Cisco Digital Signs* and not *Cisco StadiumVision* for this purpose.

Before You Begin

- Protect Your DMP from Unauthorized Management.
- Check that you have installed the license to use *Cisco Digital Signs* on your DMM appliance. (You use *DMS-Admin* to install such licenses and to learn which features you have licensed.)
- Log in to the instance of *Cisco Digital Signs* that is licensed to run on your DMM appliance, and verify that your user account permissions there allow you to manage DMPs.
- Verify that your DMPs all use identical credentials, as explained in the "Understand DMP User Accounts and Passwords" section on page 42.

Procedure

Step 1 Choose **Settings > Server Settings**.



Step 2 Enter the required values.

- **Servlet Server Address**—If you have not already done so, enter the DNS-resolvable hostname and domain for the appliance that is serving *Cisco Digital Signs*, such as **dmm.example.com**.
- **DMP User Name**—Enter **admin** or, when you have changed the DMP Web Account username from the default value, enter the new username that you assigned.
- **DMP User Password**—Enter the password that corresponds to the username.

Step 3 Click **Save**.

Step 4 Stop. You have completed this procedure.

Caution **DMP credentials must match exactly in DMPDM and *Cisco Digital Signs*.** If you ever use a system task in *Cisco Digital Signs* to change DMP credentials, you must then return here and enter matching values. Otherwise, *Cisco Digital Signs* will use the wrong credentials when it tries to communicate with your DMPs. Then, after communication fails, it will consider your DMPs to be unreachable and unmanageable.

Reference (Security)

SSL Encryption Ciphers That DMPs Support

DMPs support the following SSL ciphers in HTTPS connections.

- ADH-AES128-SHA
- ADH-AES256-SHA
- ADH-DES-CBC3-SHA
- AES128-SHA
- AES256-SHA
- DES-CBC-MD5
- DES-CBC-SHA
- DES-CBC3-MD5
- DES-CBC3-SHA
- DHE-DSS-AES128-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-DSS-DES-CBC3-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-RSA-DES-CBC3-SHA
- EXP-DES-CBC-SHA
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5
- IDEA-CBC-MD5
- IDEA-CBC-SHA
- RC2-CBC-MD5
- RC4-MD5
- RC4-SHA

Troubleshoot DMP Setup, Operation, and Health

Simple Things to Check When You Troubleshoot a DMP

Does the DMP power up when you plug it in?

- ❑ If your DMP model has a power button, have you turned it On?
- ❑ Is the AC adapter plug seated properly in the electrical outlet?
- ❑ Is the power cord also attached securely to the DC power supply on your DMP?
- ❑ Is the electrical outlet itself working correctly?

What LED lights are shining inside the DMP?

- ❑ Compare what you see to the "Check the LEDs" section on page 54.

After you start the DMP, does it show a splash screen?

- ❑ Is the DMP is in its production network (or testbed)?
- ❑ Is the DMP connected to a working presentation system?
- ❑ Does the splash screen show any other IP address than you expect?

Note **Is the splash screen disabled?** If not, you should see it on the attached presentation system soon after you start a DMP. The factory-default duration is 30 seconds. However, it might be much less in your case when anyone in your organization has changed this user-configurable setting.

Does Cisco Digital Media Manager report that the DMP is unreachable?

- ❑ Can you ping the last-known IP address for the DMP?
- ❑ Can you also ping any different IP address that the splash screen might have shown instead?

  If you assigned a static IP address to your DMP but its splash screen reports a different address, you might not have saved your work in DMPDM. See the "Understand Whether the IP Address Will Be Static or Dynamic" section on page 17.
- ❑ Has the DHCP address assignment changed for the DMP?
- ❑ Are DHCP leases in your network allowed to expire?
- ❑ When your browser loads the last-known IP address for the DMP, does DMPDM start?

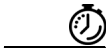
Check the LEDs

The DMP chassis contains a green LED and a red LED. After your DMP is attached to its AC power source, you should see light from both LEDs through the DMP front grille. The LEDs tell you when your DMP has power and when it has an IP address. To work as designed, it must have both.

Table 4 Troubleshoot with LEDs

LED Status		
Green	Red	Troubleshooting Notes
On	On	Your DMP is connected to its power source and is receiving electrical power. However, it has not yet obtained an IP address to use. Your DMP should obtain its IP address within 2 minutes. When the red LED persists: • **For a wired network connection**—Are both ends of the Ethernet cable plugged in? • **For a wireless network connection**—Is the wireless network active? • Does restarting your DMP resolve this problem? • Was any IP address in effect previously for your DMP? If so, can you ping that IP address? If you do not remember what the address was, there are ways to obtain it. Turn **On** a presentation system that is connected to your DMP and is configured or calibrated as necessary, and then try one of these methods. – Press **Show IP** on the handheld remote control unit for your DMP. Write down the IP address that the presentation system shows to you. (Remote controls for DMPs are sold separately.) – Restart the DMP. If its splash screen is configured in DMPDM to persist for any visible duration, write down the IP address that the splash screen shows to you. **Tip** *Alternatively, you can check your router's ARP table.* • When your DMP uses dynamic IP addresses that it receives from a DHCP server: – Has anything disrupted network traffic flow between your DMP and its DHCP server? – Is the DHCP server turned On and working correctly? – Does the DHCP server issue IP address leases that expire?
On	Off	Your DMP is connected to its power source and is receiving electrical power. Furthermore, it has obtained and is now using an IP address.
Off	Off	Your DMP does not have any electrical power and, thus, cannot obtain or use any IP address. Check that: • You are not experiencing a local or regional power outage. • All connectors are seated firmly. • Cords, plugs, adapters, and sockets do not show any signs of physical damage. • No one used software or sent commands to turn your DMP Off.
Blinking		Infrared signal interference has affected your DMP. Investigate the source of this interference. Shield or move equipment as necessary to restore normal operation.

Before You Submit Any Service Request



Timesaver

First, please check our DMP documentation on Cisco.com. We revise it continually and strive to answer every question. DMP documentation is always available, fully searchable, and its only purpose is to help you. See http://tools.cisco.com/squish/462c8.

If needed, please check our public support forum. Experts monitor this forum daily and stand ready to guide you past common or unusual issues with your DMPs. You can also search the support forum to learn if your questions are already answered. See http://tools.cisco.com/squish/4e32C.

In addition, you can use 'Bug Tool' on Cisco.com to learn what we know about any problem that affects DMPs. The entries in Bug Tool might warn against a problem's root cause, say how to work around it, or explain how to recover from it. Or, they might tell you we fixed the problem in a software patch or release. See http://tools.cisco.com/squish/106b1.

If you still want to open a service request, gather and prepare notes about your equipment and network.

- What was the last task that you performed with your DMP before its problems began?
- What serial number and MAC address are visible on your DMP chassis?
- What was the Cisco sales order number for your DMP?
- What firmware release number is installed on your DMP?
- What number, if any, identifies your Cisco service contract?

FAQs

DMPDM FAQs

Q. Can I disable DMPDM if my organization does not plan to use it?

A. Yes. Save and send this command to your DMP as an advanced task from *Cisco Digital Signs*.

```
init.startService_mibifc=no&mib.save=1&mng.reboot=1
```

Q. Can I re-enable DMPDM after someone has disabled it?

A. Yes. Save and send this command to your DMP as an advanced task from *Cisco Digital Signs*.

```
init.startService_mibifc=yes&mib.save=1&mng.reboot=1
```

Splash Screen FAQs

Q. Can I add my own logo to the DMP splash screen or change its design in any other way?

A. No, not in this release. (Its information and design are in DMP firmware.)

Q. Can I change the splash screen duration?

A. Yes. See Edit the Splash Screen Duration to Obscure the DMP IP Address, page 43.

Wireless Connectivity FAQs

Q. Can I use a wireless DMP model as an access point for other devices?

A. No, not in this release.

Q. Which IP address is active on my DMP when its Ethernet and 802.11 interfaces are both connected?

A. Ethernet connections take priority over Wi-Fi connections on DMPs where both are active.

Q. Does a DMP 4305G support Wi-Fi?

A. No.

Q. Does a DMP 4310G support Wi-Fi?

A. No.

Q. What might prevent my DMP from receiving an IP address on a wireless network?

A. These are among the possible reasons.

- The Broadcast SSID setting must be enabled on your wireless access points. Is it enabled?
- You must reconfigure your wireless DMPs whenever you change SSID settings in your WLAN. Did you forget to do this?
- Some WLAN administrators enforce a security policy that restricts DHCP address assignments to known MAC addresses. Does your administrator do this?
- Is your WLAN working correctly?
- Do any network address translation settings for your DMP differ from NAT behaviors in your network?

Touchscreen FAQs

Q. What can cause a properly calibrated touchscreen to operate as if it is not calibrated?

A. If this happens to you, unplug the serial cable (or USB cable) that connects this touchscreen to your DMP. Then, plug that cable back in again.

Logical Port FAQs

Q. Which logical ports on my DMPs should my firewall ever allow?

A. As of November 2010, these are the only ports that a DMP might ever use.

20/21 FTP	**80/8080** HTTP	**443/7777** SSL
22 SFTP	**123** NTP	**514** SYSLOG
53 DNS	**139/445** CIFS	**554** RTSP

Power-over-Ethernet FAQs

Q. What will happen if I try to use AC power and PoE simultaneously on a DMP?

A. When both PoE power and AC power are detected, AC power overrides PoE and disconnects the PoE circuit.

Q. Does my use of PoE affect the operation of any other DMP feature?

A. A DMP 4310G has two USB interfaces on its chassis. When you use PoE to power a DMP 4310G, we recommend that you use no more than one of these USB interfaces at a time. IEEE 802.3af PoE is limited in its capacity and might not be sufficient to power your DMP and two USB peripherals simultaneously.

Remote Control FAQs

Q. How can I improve the effectiveness of a DMP remote control?

A. Compensate for known factors.

Check the battery	Is a battery present?
	Is it installed correctly?
	Is it fully charged?

Check the DMP mount

Your DMP is equipped with an infrared (IR) sensor that receives, recognizes, and reacts to the signals from a DMP remote control.

However, the way that you mount your DMP can limit how well it responds to these signals. For example, the mounting method might block the IR sensor. This in turn might cause you to attach an IR extension cable to your DMP, as a workaround.

But even when you mount the receptor from this extension where it is not obstructed—and even though this method improves the reception of IR signals that are blocked otherwise—IR extension cables are not perfect. The physics that underlie their design ensure that **these cables always have some signal loss**,

Furthermore, greater cable length contributes greater signal loss. Thus, the field (angle) of transmission becomes narrower for a remote control and the range (distance) becomes shorter in direct proportion to the length of the IR extension cable.

Check for sunlight

Prevent sunlight from shining directly on your DMP's IR sensor. And take further steps as needed to stop halogen bulbs from shining at the sensor.

Learn More About...

To Learn About	Go To
Cisco Digital Media Suite	
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

To Learn About	Go To
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**

Use of Open Source Software

Cisco supports open standards, open protocols, and the open source community.

- For a complete list of open source components in this product, see its licenses and notices at http://cisco.com/en/US/products/ps7220/products_licensing_information_listing.html.
- To learn about our history of supporting open standards and open source, see http://cisco.com/web/about/doing_business/open_source/index.html.

Printed in Taiwan