# User Guide for Cisco Digital Media Player Device Manager 5.3.x

May 4, 2015

**Cisco Systems, Inc.**
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-15764-04

# CONTENTS


# Health and Safety Overview

**Revised May 4, 2015**



**Warning** **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.**

**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.
- 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.
- 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.
- Installation of the equipment must comply with local and national electrical codes.
- 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 or 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 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.


# DMP Specifications

**Revised May 4, 2015**



| DMP 4305G | DMP 4310G | DMP 4400G |
|---|---|---|
|  |  |  |

# Environmental Conditions

Table 2-1 describes the temperature, humidity, and altitude ranges that a DMP can tolerate.

*Table 2-1 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 |

*Table 2-1 Environmental Tolerance Ranges (continued)*

| Measurable Condition | Model | Supported Range | | |
|---|---|---|---|---|
| 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 | |
| **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.

# DMP Physical Specifications and Interfaces (I/O Ports)

Table 2 on page 2-5 describes the connectors, sensors, and buttons on each DMP model.

**DMP 4305G**


| | | | |
|---|---|---|---|
| **Width:** 7.5 in (190 mm) | **Height:** 1.5 in (38 mm) | **Depth:** 5 in (127 mm) | **Weight:** 1 lb (0.45 kg) |
| **Power Consumption:** 12W peak and 5W average | | **Input Current:** 3 ADC | |

### DMP 4310G


| | | | |
|---|---|---|---|
| **Width:** 7.5 in (190 mm) | **Height:** 1.5 in (38 mm) | **Depth:** 5 in (127 mm) | **Weight:** 1 lb (0.45 kg) |
| **Power Consumption:** 12W peak and 8W average | | **Input Current:** 2 ADC | |

### DMP 4400G


| | | | |
|---|---|---|---|
| **Width:** 10 in (254 mm) | **Height:** 2 in (51 mm) | **Depth:** 8 in (203 mm) | **Weight:** 4.4 lb (2 kg) |
| **Power Consumption:** 30W peak and 15W average | | **Input Current:** 3 ADC | |

*Table 2 DMP Interfaces*

| Category and Subcategory | | | Chassis Label | DMP 4305G | DMP 4310G | DMP 4400G |
|---|---|---|---|---|---|---|
| **Electrical Power** | | | | | | |
| DC input voltage | 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 |
| **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[4] | IEEE 802.11b/g | | • Antenna | 0 | 0 | **1** |
| **Debugging (for Cisco use only)** | | | | | | |
| — | | | • CONSOLE | 0 | **1** | 0 |
| **Media Signal** | | | | | | |
| Wired[5] | Video connectors | HDMI 1.1 | • HDMI | **1** | 0 | **1** |
| | | HDMI 1.3[6] | | 0 | **1** | 0 |
| | | Component[7] | • YPbPr/ S-Video | 0 | **1** | 0 |
| | | | • S-VIDEO/ YPbPr | **1** | 0 | 0 |
| | | | • S-Video | 0 | 0 | **1** |
| | | Composite[8] | • CVBS | **1** | 0[9] | **1** |
| | Audio connectors | 3.5mm jack[10] | • 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[11] | • — | **1** | **1** | **1** |

*Table 2 DMP Interfaces (continued)*

| Category and Subcategory | | | Chassis Label | DMP 4305G | DMP 4310G | DMP 4400G |
|---|---|---|---|---|---|---|
| **Serial (Comm Ports)** | | | | | | |
| Wired | Data | USB 1.0 | • USB | **1** | 0 | 0 |
| | | USB 2.0[12] | | 0 | **2** | **2** |
| | | RS-232 *(9-pin DB9 to 9-pin DB9)* | • RS232 | **1** | 0 | 1 |
| | | RS-232 *(9-pin DB9 to 3.5 mm jack)* | | 0 | **1** | 0 |
| **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. Supporting EAP-FAST, WEP, WPA, and WPA2.
5. For maximum supported media signal cable lengths, see the "Choose Suitable Media Signal Cables" section on page 6-3. Each video and audio signal cable that we ship with DMPs is 6 ft (approximately 1.83 m) long.
6. Backward-compatible to HDMI 1.1.
7. Use an S-Video signal cable with a YPbPr-to-S-Video adapter to transmit and receive YPbPr data signals.
8. 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..
9. 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.
10. Stereo audio output, irrespective of the cable type for video output.
11. Maximum distance from remote control to DMP is 15 ft (5 m).
12. Maximum USB cable length is 15 ft (5 m).

# Power Cord Options

*Table 2-3 International Power Cord Standards*

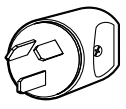
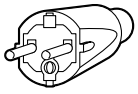
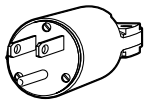
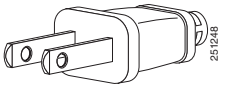
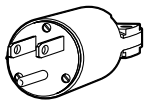
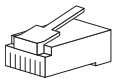
| Locale | Standard | Plug Type |
|---|---|---|
| • ***Australia*** <br> • ***New Zealand*** | • SAA/3 <br> • AS/NZS 3112-1993 |  120356 |
| • ***European Union (except Italy)*** <br> • ***Argentina*** <br> • ***Brazil*** | • CEE 7/7 <br> • VIIG |  120357 |

*Table 2-3 International Power Cord Standards (continued)*

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

**Related Topics**

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Receive Electrical Power from a 100V–240V AC Socket, page 4-2
- Receive Electrical Power from 802.3af Power over Ethernet (PoE), page 4-3

# Internal 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 2-4 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:<br>• **For a wired network connection**—Are both ends of the Ethernet cable plugged in?<br>• **For a wireless network connection**—Is the wireless network active?<br>• Does restarting your DMP resolve this problem?<br>• 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.<br>– 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.)<br>– 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.<br>**Tip Alternatively, you can check your router's ARP table.**<br>• When your DMP uses dynamic IP addresses that it receives from a DHCP server:<br>– Has anything disrupted network traffic flow between your DMP and its DHCP server?<br>– Is the DHCP server turned On and working correctly?<br>– 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:<br>• You are not experiencing a local or regional power outage.<br>• All connectors are seated firmly.<br>• Cords, plugs, adapters, and sockets do not show any signs of physical damage.<br>• 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. |


# Welcome

**Revised May 4, 2015**



# Concepts



## About This Guide

This guide describes Cisco software called *Digital Media Player Device Manager* (DMPDM). DMPDM is preinstalled on every *Digital Media Player* (DMP) that supports Cisco DMS 5.3. This guide assumes that you already completed setup procedures for your DMP, and therefore:

- **Your DMP is already connected to:**
  - A network that includes a DHCP server.
  - Its public presentation system.
  - Its AC power source.
- **You already:**
  - Checked the LEDs to confirm that your DMP has power and has obtained an IP address.
  - Learned what dynamic IP address the DHCP server assigned to your DMP.
  - Used your browser to log in to the DMPDM administrative account.
  - Changed the factory-default passwords.
  - Used DMPDM to configure video output to the presentation system.
  - Used DMPDM to identify its trusted DMM appliance.

**Caution** **Are any of the preceding statements not yet true for you?** If so, you must set up your DMP before you use this guide. See http://cisco.com/en/US/products/ps7220/prod_installation_guides_list.html.

# 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 3-2
- TVzilla, page 3-3
- Cisco Hinter, page 3-3
- Remote Controls, page 3-4


## 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 3-5.

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 with a video wall. Popular uses include:

- Marketing—Describe products and services directly to your in-store customers.
- Customer experience—Deliver entertainment and information to reduce perceived wait times.
- Messaging—Broadcast executive and internal communications in real time.
- Training—Deliver cost-effective, flexible training.
- Information—Deliver real-time schedules, news, and way-faring information where people need it.
- Advertising—Sell advertising time and space to third parties.
- Branding—Communicate about your brand consistently.

**Note** ***StadiumVision*** **deployments should avoid 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.

## 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.

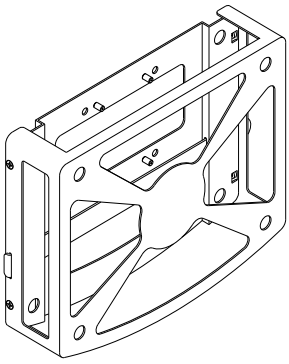
### Remote Controls

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.

**Tip** **Cisco Unified Communications Manager administrators can configure a service through which Cisco IP Phones and mobile phones can emulate a remote control.** Phone users can then operate the IPTV features of *Cisco Cast*. To learn how to configure this service and use it, see the *Cisco Cast* documentation 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.

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

# Consider How You Will Use and Manage Your DMP

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 any particular organization depends on how many DMPs it has and how it plans to use them. Beyond this, a management system might impose its own installation and setup requirements for DMPs. To understand any such requirements, see the documentation on Cisco.com.

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



## Understand DMP Modes

You can use a DMP in isolation, so that it operates independently of every other DMP. When you deploy one DMP in isolation, you use DMPDM to configure it and control its daily operation.

Or, you can deploy multiple DMPs throughout a LAN or WAN. In this case, you use *Cisco Digital Media Manager* or *Cisco StadiumVision* to configure and manage your DMPs centrally.

## Manage One DMP in Isolation

This guide teaches you how. See DMPDM, page 3-2.

## 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 include those to:
  - Define and issue remote commands to DMPs and their attached presentation systems.
  - Poll the current and historical status of DMPs and their attached presentation systems.
  - Adjust the resolution, brightness, contrast, and related settings for presentation systems.

Commonly popular DMP deployment sites under *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.

- Search the 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 and existing video displays in your 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.


# Connect to a Power Source

**Revised May 4, 2015**

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



# Concepts



## DMP 4310G Notice Regarding Power over Ethernet (PoE)

Starting in 2009, a handful of Cisco StadiumVision customers participated in a special program to receive DMP 4310G endpoints whose hardware design was not yet utterly final. During this limited, pre-release program, we manufactured such units under the Cisco product ID "DMP-4310G-SE-K9." Partway through the limited release, we changed one physical component in the hardware design to improve the Power over Ethernet (PoE) performance of a DMP 4310G.

**Is even one of these statements true for you?**

- Your DMP 4310G was manufactured in or after September 2010.
- Your DMP 4310G serial number is *USI1434xxxx* or greater.
- We manufactured your DMP 4310G under the Cisco product ID "DMP-4310G-52-K9."

**When even one of these statements is true, your DMP 4310G uses the improved PoE component. Nothing further about this topic applies to you or your DMP.**

Otherwise, when even one statement is false, your DMP 4310G uses the original PoE component. We have identified a corner case in which these DMPs might not receive full PoE power. Suppose that a very long Ethernet cable connects the DMP 4310G to a network switch from the Cisco 3560 Series. And suppose also that the Ethernet cable length is so great that the level of PoE power becomes noticeably diminished after traveling its full distance to the DMP. In this scenario, your DMP cannot compensate for the degraded power because switches in the Cisco 3560 Series do not permit adjustments to their PoE power output.

We recommend that you do not obtain power for such DMPs from network switches in the Cisco 3560 Series. When you must do so, then take care to use the shortest possible Ethernet cord. Alternatively, you might use network switches from the Cisco 3750 Series, which offer configurable PoE power output.

# Procedures



## Receive Electrical Power from 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** If your DMP power cord must be assembled, 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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Power Cord Options, page 2-6
- Receive Electrical Power from 802.3af Power over Ethernet (PoE), page 4-3

# Receive Electrical Power from 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


- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Power Cord Options, page 2-6
- Receive Electrical Power from a 100V–240V AC Socket, page 4-2


# Connect to a Network

**Revised May 4, 2015**

Use a connection method—wired or wireless—that your DMP and topology both support.

**Tip** **Physical Ethernet connections take priority over 802.11 b/g on DMPs where both are active.** To learn which connection methods your DMP supports, see Table 2-1 on page 2-3. Alternatively, if the table does not describe your DMP model, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.



# Concepts



## 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 10-19
- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21

# Procedures



## Connect Over Ethernet

### 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 socket 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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Connect Over Wireless (802.11 b/g), page 2

## Connect Over Wireless (802.11 b/g)

**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.

- Connect Over Wireless (802.11 b/g), page 5-2
- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21


# Connect to a Presentation System

**Revised May 4, 2015**

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 DMP 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



## Understand S-Video Limitations

When you use an S-Video cable to pass High Definition video signals to a DMP, the picture quality is not High Definition. This happens because the S-Video standard is engineered to pass analog video signals in Standard Definition.

When you will use an S-Video signal cable, we recommend a maximum resolution of 728 x 576 @ 25Hz and a maximum cable length of 10 feet (approximately 3 meters).

# 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.

### DMP 4310G Notice Regarding HDMI/DVI Effects on Autodetection

A corner case exists that is mildly disruptive. It is not likely to affect your organization. To understand this corner case, assume that all of the following statements are true simultaneously.

- Your DMP model is 4310G.
- Your presentation system's media signal interface is DVI, not HDMI.
- EDID data in the firmware for your presentation system misrepresents its native resolution.
- The falsely claimed resolution is an HDMI standard instead of a VESA standard.

In this case, your DMP 4310G proceeds as if the native resolution is low, to ensure that your digital sign shows anything at all.

**Tip** **This constraint does not affect a DMP 4305G or a DMP 4400G.** These models do not use the same microprocessor that a DMP 4310G uses.

To work around this behavior, disable the autodetect feature in DMPDM and then choose the actual resolution manually.

# 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 must 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 circumstances.
- **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.

# Choose Suitable 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:

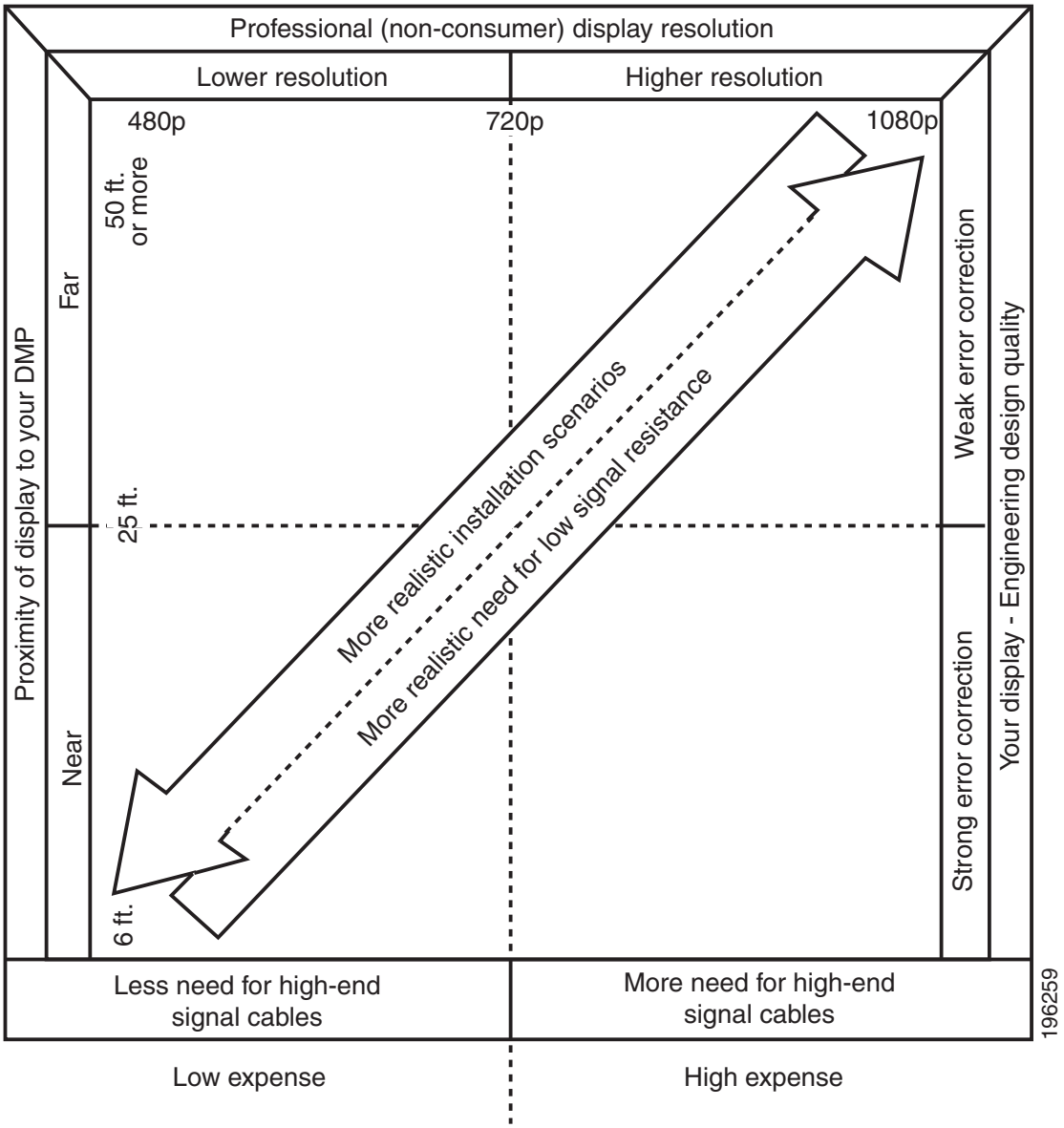
- Composite — 10 ft (approximately 3 m)
- HDMI 1.1 — 16 ft (approximately 5 m)
- RCA — 10 ft (approximately 3 m)
- S-Video — 10 ft (approximately 3 m)
- SPDIF — 10 ft (approximately 3 m)

### 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 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 6-1

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

**Note** **When video 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 3-3
- Connect to a Presentation System, page 6-1

# Procedures



# Use an HDMI Connection

**Timesaver** **Is your display a touchscreen?** If so, this topic is not for you. Instead, see the "Connect to a Touchscreen" section on page 6-7.

**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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Use a Connection that Combines HDMI with DVI, page 6-6

# Use a Connection that Combines HDMI with DVI

**Timesaver** **Is your display a touchscreen?** If so, this topic is not for you. Instead, see the "Connect to a Touchscreen" section on page 6-7.

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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Use an HDMI Connection, page 6-5

# 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.

  If your DMP model has only one USB connector, 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 CF 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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Choose and Calibrate a Touchscreen Driver, page 9-3

# 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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Understand How to Work Around the Low Signal Quality of Composite Video, page 6-5


# Start Here

**Revised: May 4, 2015**

Topics in this section explain how to maintain and administer your DMP.



# Concepts



## DMPDM Workflow

The typical workflow in DMPDM assumes that you will test settings before you commit to them.

Settings in DMPDM might revert to their most recent state after your DMP restarts. This occurs by design, so that you can test new settings. If your changes cause unforseen problems, you can abandon them without consequence. And, when your changes are satisfactory, you can commit to them.

- Click **Apply** to test new values for a condition or setting. After this click, the change takes effect. However, this change is temporary and reversible. The values that you overwrote will return the next time that your DMP restarts, unless you commit to them explicitly.
- Choose **Administration > Save Configuration** to store changed settings permanently. After this click, the changes persist even after your DMP restarts. When the Save Configuration page appears, you must click **Save** to actually save your work.

### Related Topics


- "Save Configured Settings" section on page 7-5

# DMPDM Differences by Firmware Release and DMP Model

Your DMP model and its installed firmware version dictate which elements and supported features you see in DMPDM.



## DMPDM on a DMP 4305G

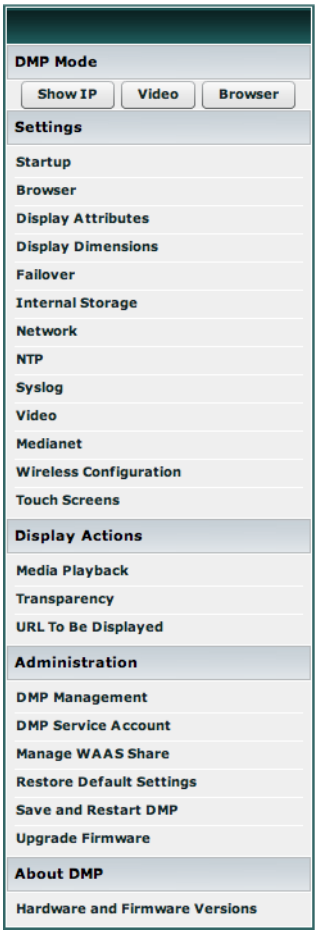
### Firmware Release 5.3.0

# DMPDM on a DMP 4310G

### Firmware Release 5.3.0

## DMPDM on a DMP 4400G

### Firmware Release 5.3.0




# Procedures

# 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.

**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.

# Save Configured Settings

You can save every change that you made to the values for every option in DMPDM since the last time that you clicked Save or the last time that you restarted the DMP.

**Tip** **Changes to some DMP configuration settings do not take effect until after the DMP restarts.** Check the instructions for a procedure to see if you must restart your DMP after you change a setting.

### Procedure

**Step 1** Complete whichever variation of this step applies to you. It might vary between any two DMP models, and also between the model-specific firmware versions from any two maintenance releases.

| Firmware Version | DMP Model | | |
|---|---|---|---|
| | DMP 4310G  | DMP 4400G  | DMP 4305G  |
| 5.3.0 | a. Click **Save and Restart DMP** in the Administration list.<br>b. Click **Save**.<br>c. Click **Restart**. | | |

The saved configuration persists even after your DMP restarts.

**Step 2** Stop. You have completed this procedure.

### Related Topics

- Restart Your DMP, page 7-6
- DMPDM Workflow, page 7-1

# Restart Your DMP

### Procedure

**Step 1** Complete whichever variation of this step applies to you. It might vary between any two DMP models, and also between the model-specific firmware versions from any two maintenance releases.

| Firmware Version | DMP Model | | |
|---|---|---|---|
| | DMP 4310G  | DMP 4400G  | DMP 4305G  |
| 5.3.0 | a. Click **Save and Restart DMP** in the Administration list.<br>b. Click **Restart**. | | |

**Step 2** Stop. You have completed this procedure.

# Rare but Essential Tasks



## Configure NTP Settings for Time-Dependent Features, As Needed

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 time server while this one is 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 7-5

## Restore Factory Default Settings

You can restore factory settings to your DMP.

**Caution** **When you restore the factory settings to your DMP, you delete your configuration of every setting.** If you delete your settings accidentally, you must reenter every value manually.

**Procedure**

**Step 1** Click **Restore Default Settings** in the Administration list.

**Step 2** Click **Restore** when the Restore Default Settings page appears.

Your DMP restarts automatically and its factory settings are restored.

**Step 3** (**Optional**) *Will you deploy your DMP where there is no local DHCP server?* If so, complete the "Preconfigure a DMP To Run Without a Local DHCP Server" procedure in the getting started guide for your DMP.

**Step 4** Log in with the factory default username **admin**.

**Step 5** Reconfigure your DMP and change its default passwords, when prompted.

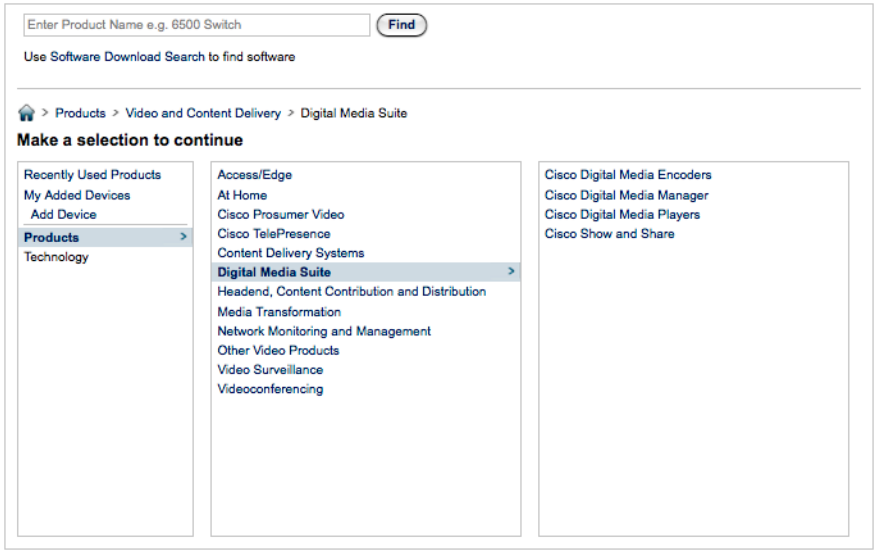
To learn how, see *Getting Started Guide for Cisco Digital Media Players* at http://cisco.com/en/US/docs/video/digital_media_systems/dmp/getting/started/guide/5_2_x/dmp5_2_x.html.

**Step 6** Stop. You have completed this procedure.

# Investigate Which DMP Firmware Updates Are Available

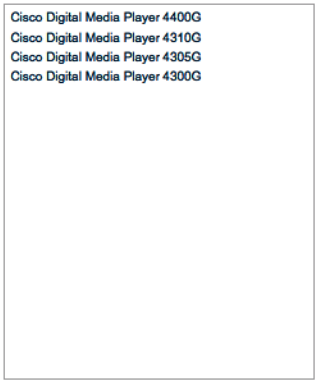
## Procedure

**Step 1** Log in to your Cisco.com account, and then go to http://cisco.com/cgi-bin/tablebuild.pl/dms.

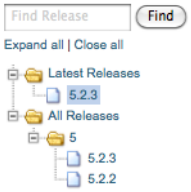



**Step 2** Click **Digital Media Players** in the far-right column.

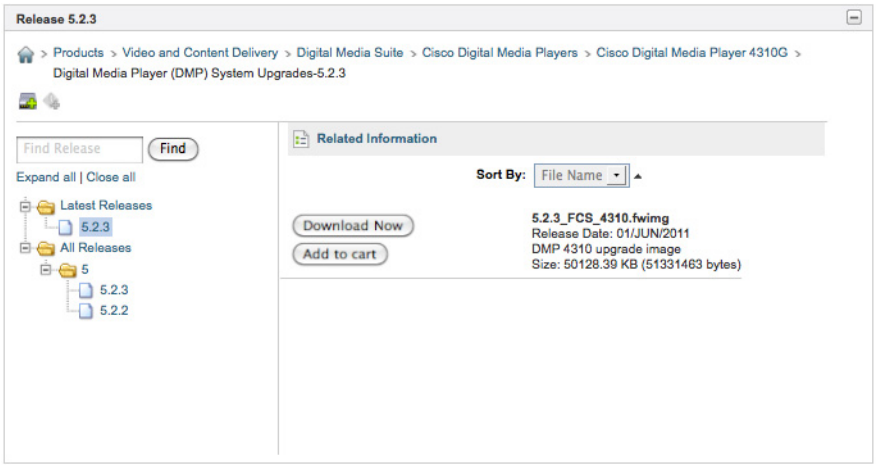
The selector shifts all columns to the left by one slot. This movement exposes the options for another navigation level in the far-right column.




**Step 3** Click the name of a DMP model to see a selection tree that lists its available firmware versions.

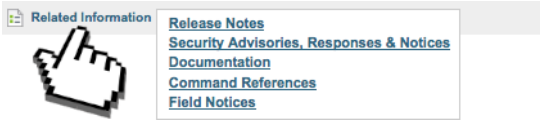


**Step 4** Expand the tree as needed, and then click a release number to see its details.




**Note** **Every firmware file is DMP model-specific.**

**Tip** Allow your pointer to hover for a moment over the **Related Information** link. Doing so reveals more options that you might consider helpful.




**Step 5** Follow the prompts to download your preferred firmware within a compressed archive file.

**Step 6** Decompress the archive.

It contains a README file, which:

- States how the new firmware might affect your equipment and network.
- Includes installation procedures.

**Step 7** Complete procedures that the README file recommends for you.

**Step 8** Stop. You have completed this procedure.

## Upgrade (or Downgrade) DMP Firmware

You can install an update to the firmware for your DMP.

**OR**

If your DMP firmware is so comparatively recent that it does not work well with older software on your DMM server, you can install older firmware on your DMP.

### Before You Begin

- Investigate which DMP firmware releases are available on Cisco.com.
- Confirm that the "Enable Cisco TAC Troubleshooting Access" feature is enabled in DMPDM. If you must enable it manually, you must *also* restart your DMP before this change can take effect.

### Procedure

**Step 1** Click **Upgrade Firmware** in the Administration list.

**Step 2** Click **Browse**—or its equivalent if your browser applies a different name to this button—when the Upgrade Firmware page appears.

**Step 3** Navigate to the firmware update that you downloaded, and then choose it.

**Step 4** Click **Start Upgrade**.

**Note** **Do not close or browse away from this page until messages in DMPDM state that your DMP has loaded the firmware image and started to burn it.** Otherwise, upgrade fails.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- Enable or Disable Types of Access to Your DMP, page 8-6
- UI Reference: Elements to Upgrade or Downgrade DMP Firmware, page 7-12

## View DMP Hardware and Firmware Versions

### Procedure

**Step 1** Click **Hardware and Firmware Versions** to see information about your DMP.

You cannot change the information.

**Step 2** Stop. You have completed this procedure.

# Reference



# UI Reference Topics



### UI Reference: Elements to Upgrade or Downgrade DMP Firmware

*Table 7-1 Elements on the Upgrade Firmware Page*

| Field | Description |
|---|---|
| **Upgrade Firmware** | |
| Image File | The full pathname to the binary file. If you do not know the full pathname, click **Browse**. |
| **Upgrade Status** | |
| Status | Indicates whether a firmware upgrade is in progress:<br>• **Firmware upgrade not active**—There is no upgrade in progress.<br>• **Burn in progress**—An upgrade is in progress. |
| Progress | Status indicator for an upgrade in progress. |


# DMP Access and Security Settings

**Revised: May 4, 2015**



# Concepts



## 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 7-5.** 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 8-2
- Manage and Edit Passwords, page 8-5

# 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.<br>**Note** **Before you can manage any DMP centrally, you must configure it to support centralized management.** |

**Related Topics**

- Manage and Edit Passwords, page 8-5
- Protect Your DMP from Unauthorized Management, page 8-3

# Procedures

- Edit the Splash Screen Duration to Obscure the DMP IP Address, page 8-2
- Protect Your DMP from Unauthorized Management, page 8-3
- Manage and Edit Passwords, page 8-5
- Enable or Disable Types of Access to Your DMP, page 8-6
- Enable or Disable Centralized Management, page 8-7

# 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.

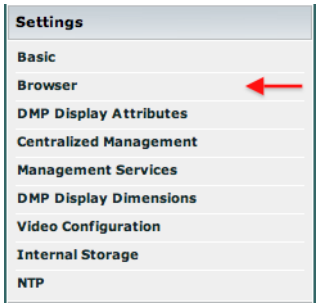
- A duration of 30,000 milliseconds (30 seconds) is the factory default.
- A duration of 1 millisecond turns off the splash screen.
- Any duration in the range from 2 to 5,000 milliseconds (5 seconds) does not have any effect.

**Before You Begin**

- Log in to DMPDM, page 7-5.

### 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.

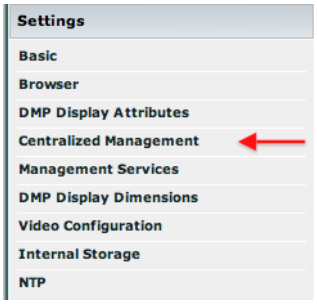
When you use *Cisco Digital Signs* to manage a network of DMPs centrally, you must configure each DMP to secure and trust its communication with *Cisco Digital Signs*.

### Before You Begin

- Log in to DMPDM, page 7-5.

### 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 8-3
- Log in to DMPDM, page 7-5

# Manage and Edit Passwords

**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 7-5.** 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.

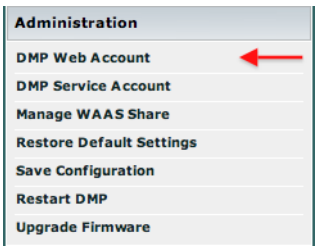
### Before You Begin

- Log in to DMPDM, page 7-5.

### Procedure

**Step 1** Change the Web Account password.

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

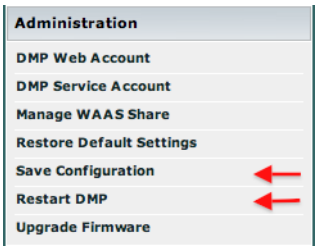



b. Enter your new password in the Password field and again in the Repeat Password field.

c. Click **Apply**.

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

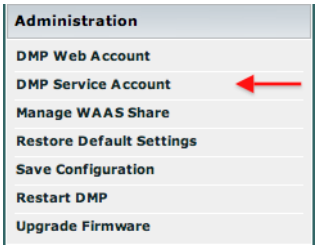
e. Click **Restart DMP** in the Administration list, and then click **Restart**.




**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 8-3.

**Step 4** Stop. You have completed this procedure.

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

# Enable or Disable Types of Access to Your DMP

You can enable or disable various kinds of administrative access to your DMP.

### Procedure

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

**Step 2** Enter or edit the required values, and then click **Apply**.

**Step 3** Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

**Step 4** Restart your DMP.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- Elements to Define Management Services, page 8-8
- Restart Your DMP, page 7-6

# Enable or Disable Centralized Management

You can enable a remote DMM appliance to manage your DMP as part of a digital signage network.

### Procedure

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

**Step 2** Enter or edit the required values.

**Step 3** Click **Apply** to confirm that you are satisfied with the entries or changes that you made and to record them in volatile memory, .

After you click Apply, the entries or changes take effect. However, the previously defined values will return the next time that your DMP restarts.

**Step 4** (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?*

a. Choose **Administration > Save Configuration**.

b. Click **Save** when the Save Configuration page appears.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- Elements to Define Centralized Management Settings, page 8-8

# Reference


- SSL Encryption Ciphers That DMPs Support, page 8-7
- UI Reference Topics, page 8-8


## 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

# UI Reference Topics



## Elements to Define Centralized Management Settings

*Table 8-1 Elements on the Centralized Management Page*

| Element | Description |
|---|---|
| **Centralized Management** | |
| DMM-DSM Server Timeout (in seconds) | The maximum number of seconds that your DMP will wait for a response from the DMM appliance that you identify in the DMM Host text box. |
| DMM Appliance IP Address | The routable IP address of the one DMM appliance that your DMP trusts. Alternatively, the DMP loopback IP address, 127.0.0.1. |

### Related Topics

- Enable or Disable Centralized Management, page 8-7

## Elements to Define Management Services

*Table 8-2 Elements on the Management Services Page*

| Element | Description |
|---|---|
| **Management Services** | |
| Enable Cisco TAC Troubleshooting Access | ⚠ **Caution** **We recommend that you assign a strong password to the Cisco TAC account and never reveal this password to anyone except your trusted support engineer after you open a support case with Cisco.** Later, after your support case is closed, we recommend that you change the password.<br><br>Indicates whether DMP login access is enabled or disabled for Cisco technical support staff.<br>• **Enabled**—Your DMP allows Cisco technical support staff to log in.<br>• **Disabled**—Your DMP *does not* allow Cisco technical support staff to log in.<br><br>This feature is enabled by default but, in most cases, we do not support any use of this feature by anyone except a Cisco employee.<br><br>**Note** **This feature must be enabled during firmware upgrades.** |
| Event Notifications | Indicates whether you enabled or disabled the feature to send event notification messages to one, trusted DMM appliance that you can choose.<br>• **Enabled**—Your DMP sends notification messages.<br>• **Disabled**—Your DMP *does not* send notification messages. |

*Table 8-2 Elements on the Management Services Page (continued)*

| Element | Description |
|---|---|
| FTP Server | Indicates whether you enabled or disabled the feature to run an FTP server and an SFTP server from your DMP. You might enable the FTP and SFTP services temporarily, for example, when you want to create a local copy on your DMP of an asset that you stored at a remote site.<br>**Note We recommend that you disable the FTP and SFTP services when you do not plan to use them.** |
| Mount WAAS Share on Startup | Indicates whether your DMP will use the CIFS protocol to automatically mount the network share that you designated on the WAAS Share Settings page.<br>• **On**—Upon starting, your DMP mounts the network share automatically.<br>• **Off**—Upon starting, your DMP *does not* mount the network share automatically.<br>**Note DMPs can mount only one shared volume at a time.** |
| **TAC Account** | |
| Password<br>Repeat Password | The password for Cisco TAC to use while troubleshooting your DMP, if you chose Enabled from the Enable TAC Troubleshooting Access list. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral. |

**Related Topics**

- Enable or Disable Types of Access to Your DMP, page 8-6
- Upgrade (or Downgrade) DMP Firmware, page 7-11
- Enable or Disable Centralized Management, page 8-7
- Mount or Unmount a Network Share, page 11-3

## Elements to Define DMPDM Login Credentials

*Table 8-3 Elements on the DMP Web Account Page*

| Element | Description |
|---|---|
| **DMP Web Account** | |
| User Name | The login name for DMPDM. |
| Password<br>Repeat Password | The password that is associated with the DMPDM username. You must enter the password two times on the DMP Web Account page to confirm that you typed it correctly. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral. |

**Related Topics**

- Manage and Edit Passwords, page 8-5

## UI Reference: Elements to Define DMP Service Account (ftp and sftp) Login Credentials

*Table 8-4 Elements on the DMP Service Account Page*

| Element | Description |
|---|---|
| **FTP Server Account** | |
| User Name | The login name for the DMP Service user account. The factory default is to use the login name **ftp**. |
| Password<br>Repeat Password | The password that is associated with the DMP Service account login name. The factory default is to use the password **admin**, but we warned you to change it when you first set up your DMP. See the quick start guide for your DMP model type on Cisco.com.<br>You must enter the password two times on the FTP Service Account page—one time apiece in each of these fields—to confirm that you typed it correctly. The password must contain at least 8 characters and, of these, at least one character must be an uppercase letter, at least one must be a lowercase letter, and at least one must be a numeral. |

### Related Topics

- Manage and Edit Passwords, page 8-5


# Configure Settings for Touchscreens, Projectors, and Displays

**Revised: May 4, 2015**



# Concepts



## Overview

A DMP transmits signals to a public presentation system of some kind, such as a monitor or projector that is connected to the DMP. This presentation system might use projection or display technologies that are analog or digital, and its output fidelity depends in part upon which signal cables (and adapters) connect it to your DMP.

## Example Settings for DMP Display Attributes

*When you use an HDMI cable to connect your DMP to a 1920 x1200 LCD flat panel display:*

- Display Standard—VESA_1920x1200x60RB
- Display Output Interface—HDMI
- Color Space—RGB_16_235
- Color Component Order—RGB

*When you use a composite/S-Video cable to connect your DMP to an analog display:*

- Display Standard—NTSC_M
- Display Output Interface—Composite/S-Video
- Color Space—None
- Color Component Order—RGB

**Related Topics**

- Adjust DMP Display Attributes, page 9-6
- UI Reference: Elements to Define Attributes of a DMP Display, page 9-8

# Supported Touchscreen Drivers

| DMP Model | Supported Drivers |
|---|---|
| **DMP 4400G** | • 3M MicroTouch<br>• ELO Acoustic Pulse Recognition systems and non-APR systems<br>• ELO non-Acoustic Pulse Recognition systems<br>• GeneralTouch ST6001S and ST6201<br>• Zytronic Zybrid |
| **DMP 4310G** | • 3M Touch Systems Capacitive Pulse SCT<br>• 3M Dispersive Signal DST<br>• 3M Projected Capacitive PCT (with single touch)<br>• ELO non-Acoustic Pulse Recognition systems<br>• GeneralTouch ST6001S and ST6201 |

# Procedures

# Choose and Calibrate a Touchscreen Driver

This procedure applies to you only if 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 6-7.

### 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.
- Log in to DMPDM.

### Procedure

**Step 1** If your touchscreen shows a message that says it must download a touchscreen characterization file:

- 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.

**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** **If you do not see this option in DMPDM, your DMP might not support this feature.** If you believe that its hardware design allows for the possibility of such support, check whether any firmware upgrade is available for your DMP that adds support for this feature:

- Cisco DMS release notes—http://cisco.com/go/dms/releasenotes.
- Cisco DMS compatibility information—http://cisco.com/go/dms/compatibility.

If such firmware is available, obtain it and then complete the DMP firmware upgrade procedure in the 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 DMPDM 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.

- When messages appear on the touchscreen surface that prompt you to touch the surface in various places, follow the prompts exactly. For example, the calibration utility might prompt you to touch exactly five areas or exactly nine areas.
- If 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 calibrate your driver.

**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 6-7

# 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** Enabling HDMI autodetection with unsupported displays will cause high CPU on the DMP. From the GUI, you will see autodetection failed. You need to manually configure the properties of the unsupported display.

**Note** **If you are satisfied with the choices and entries that DMPDM made for you as a result of its DMP display autodetection, you are done with this section and you can go now to the "Protect Your DMP from Unauthorized Management" section on page 8-3.**

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** (**If you chose RGB as the color space**) 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** (**Optional**) Move any or all of the sliders 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 if 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.

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

**Step 8** Stop. You have completed this procedure.

# Adjust DMP Display Attributes

### Procedure

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

**Step 2** Enter or edit the required values.

**Step 3** Click **Apply** to confirm that you are satisfied with the entries or changes that you made and to record them in volatile memory.

After you click Apply, the entries or changes take effect. However, the previously defined values will return the next time that your DMP restarts.

**Step 4** (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?*

a. Choose **Administration > Save Configuration**.

b. Click **Save** when the Save Configuration page appears.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define Attributes of a DMP Display, page 9-8
- Example Settings for DMP Display Attributes, page 9-1

# Adjust Horizontal and Vertical Settings

You can adjust the proportions, horizontal position, and vertical position of content that you show on a DMP display.

### Procedure

**Step 1** In the Settings list, click **DMP Display Dimensions**.

**Step 2** Enter or edit the required values.

**Step 3** Click **Apply** to confirm that you are satisfied with the entries or changes that you made and to record them in volatile memory.

After you click Apply, the entries or changes take effect. However, the previously defined values will return the next time that your DMP restarts.

**Step 4** (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?* Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define DMP Display Dimensions, page 9-11

# Reprogram the Buttons on Your Handheld Remote Control

### Before You Begin

- Your DMP model must be 4310G.

### Procedure

**Step 1** Click **Remote Mappings** in the Settings list.

**Step 2** Repeat this step for each button whose behavior should be changed.

**a.** Choose an option from the Remote Button list to designate which button you will reprogram.

**b.** Choose an option from the Action list to assign a new behavior to the designated button.

- Reset to Default—Restore our factory-default behavior to the designated button.
- Map to Key Value—Remap one button to another.
- Map to System Function—Choose among these functions.
  - Show IP
  - Mute
  - Volume Up
  - Volume Down
  - Power
- Custom—Enter a custom parameter.

**Step 3** Click **Apply** to confirm that you are satisfied with the entries or changes that you made and to record them in volatile memory.

After you click Apply, the entries or changes take effect. However, the previously defined values will return the next time that your DMP restarts.

**Step 4** (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?* Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

**Step 5** Stop. You have completed this procedure.

# Reference



# UI Reference Topics



## UI Reference: Elements to Define Attributes of a DMP Display

*Table 9-1 Elements on the DMP Display Attributes Page*

| Element | Description |
|---|---|
| **DMP Display Attributes** | |
| DMP Display Autodetection (requires HDMI) | Indicates whether you have enabled automated detection of the DMP display type. Choose an option:<br>• **Enabled**—Autodetection is enabled.<br>• **Disabled**—Autodetection is disabled. |
| Autodetection Status | Indicates whether autodetection succeeded. |
| Frame Rate | Indicates whether your display uses PAL (50 Hz) or NTSC (60 Hz). Most displays that support HDMI connections also support both the PAL and NTSC frame rate standards. If you choose the wrong value, image quality is degraded. |

*Table 9-1 Elements on the DMP Display Attributes Page (continued)*

| Element | Description |
|---|---|
| Composite Display Standard | All DMP model types (4300G, 4305G, and 4400G) show at least these values:<br>• NTSC_M<br>• NTSC_M_714<br>• NTSC_M_Japan<br>• NTSC_M_Japan_714<br>• PAL_60<br>• PAL_60_714<br>• PAL_BG<br>• PAL_BG_702<br>• PAL_BG_704<br>• PAL_M<br>• PAL_M_714<br>• PAL_N<br>• PAL_N_702<br>• PAL_N-704<br>DMP 4400Gs show other values in addition to these. |
| Display Standard | The name of the standard that your DMP display uses. Generally, this attribute names the manufacturer and the type of display (such as plasma or LCD), in combination with other information. To learn which option is the correct one for you to select, see the manual that came with your DMP display. |
| Interface (DMP display output) | The type of video cable that connects your DMP to your DMP display. The options are:<br>• Composite/S-Video—Either of these:<br>– **Composite**—Analog cable that binds three wires together and terminates in three separate plugs. There is one plug *each* for:<br>~ The video signal.<br>~ Signals in the left audio channel.<br>~ Signals in the right audio channel.<br>– **S-Video**—Analog cable with a 4-pin connector. Transmits separate standard-definition video signals for brightness and color.<br>• HDMI—Digital cable with a 19-pin connector. Transmits standard-, enhanced-, or high-definition video signals uncompressed and transmits multi-channel digital audio signals.<br>**Note You must use a composite/RCA cable for the left and right audio channels if you use HDMI-to-DVI for the video signal.** |

*Table 9-1 Elements on the DMP Display Attributes Page (continued)*

| Element | Description |
|---|---|
| Color Space | The absolute color space that your DMP display uses. To learn which option is the correct one for you to select, see the manual that came with your DMP display. The options are:<br>• None<br>• RGB_16_235<br>• RGB_0_255<br>• YUV_601<br>• YUV_709 |
| Color Component Order | The order in which to store red, green, and blue data if you selected RGB as the color space. The color component order is sometimes also known as a left-to-right additive color model. Most modern displays use RGB. To learn which option is the correct one for you to select, see the manual that came with your DMP display. The options are:<br>• RGB<br>• RBG<br>• GRB<br>• GBR<br>• BRG<br>• BGR |
| Brightness | The setting that compensates for any deficiencies in the on-screen brightness of your DMP display. Brightness compensation values can range from –128 to 127. |
| Contrast | The setting that compensates for any deficiencies in the on-screen contrast of your DMP display. Contrast compensation values can range from 0 to 255. |
| Saturation | The setting that compensates for any deficiencies in the on-screen color saturation of your DMP display. Saturation compensation values can range from 0 to 255. |
| Audio Channel Volume (left)<br>Audio Channel Volume (right) | The setting to control how loudly or softly your DMP delivers (to its attached DMP display) the sound from the relevant audio channel. Volume can range from 0 to 100, where 0 is silent. This is separate from the volume setting for the DMP display, which you might adjust with a remote control.<br>• If you set the volume to 0 *on your DMP*, you cannot compensate for the silence by adjusting the volume setting on your DMP display. Instead, you must set an audible volume on the DMP.<br>• If you set the volume to 0 *on your DMP display*, you cannot compensate for the silence by adjusting the volume setting on your DMP. Instead, you must set an audible volume on the DMP display. |

*Table 9-1 Elements on the DMP Display Attributes Page (continued)*

| Element | Description |
|---|---|
| **HDMI Display Information** | |
| Manufacturer | Shows the manufacturer name and the year in which your DMP display was manufactured. Blank if you used any interface except HDMI to connect your DMP to its DMP display, or if HDMI autodetection failed. You cannot edit this value. |
| Description | Shows the native resolution (width and height in pixels), the scan type (progressive or interlace), and the frame rate in Hz. The value is blank if you used any interface except HDMI to connect your DMP to its DMP display, or if HDMI autodetection failed. You cannot edit this value. |
| Version | Shows the version number of the EDID protocol or the CEA protocol by which autodetection occurred. Blank if you used any interface except HDMI to connect your DMP to its DMP display, or if HDMI autodetection failed. You cannot edit this value. |
| Connector Type | Shows the connector type (HDMI or DVI) that is in use. Blank if you used any interface except HDMI to connect your DMP to its DMP display, or if HDMI autodetection failed. You cannot edit this value. |
| Supported Standards | Shows all of the standards that your DMP display supports and shows which standard you selected. Blank if you used any interface except HDMI to connect your DMP to its DMP display, or if HDMI autodetection failed. You cannot edit this value. |

### Related Topics

- Adjust DMP Display Attributes, page 9-6
- Example Settings for DMP Display Attributes, page 9-1

## UI Reference: Elements to Define DMP Display Dimensions

*Table 9-2 Elements on the DMP Display Dimensions Page*

| Element | Description |
|---|---|
| **DMP Display Dimensions** | |
| DMP Display X Axis (abscissa) Center Point (in relative units) | The absolute center point of your DMP display, as measured from left to right (on the *x*-axis), in pixels. The value by default is 2048.<br>• Reduce the value to move displayed content closer to the left edge.<br>• Increase the value to move displayed content closer to the right edge. |
| DMP Display Y Axis (ordinate) Center Point (in relative units) | The absolute center point of your DMP display, as measured from top to bottom (on the *y*-axis), in pixels. The value by default is 2048.<br>• Reduce the value to move displayed content closer to the top edge.<br>• Increase the value to move content closer to the bottom edge. |

*Table 9-2 Elements on the DMP Display Dimensions Page (continued)*

| Element | Description |
|---|---|
| Displayable Width (in relative units) | The total width in pixels of your DMP display. The maximum value is 4096 pixels.<br>• Reduce the value to reduce the width of displayed content.<br>• Increase the value to increase the width of displayed content. |
| Displayable Height (in relative units) | The total height in pixels of your DMP display. The maximum value is 4096 pixels.<br>• Reduce the value to reduce the height of displayed content.<br>• Increase the value to increase the height of displayed content. |

**Related Topics**

- Adjust Horizontal and Vertical Settings, page 9-7


# Configure Network Settings

**Revised: May 4, 2015**



# Concepts



## Glossary

Timesaver

Go to terms that start with... [ numerals | A | C | D | E | L | M | 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 compatibilitywith 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.

**autoregistration** *See* MSI registration service.

**Auto Smartports**[1] A collection of interface-level switch commands bundled together as a macro that configures a switchport without human intervention. Upon detecting a connection to one of its physical interfaces (or "ports"), a Medianet-ready switch uses CDP packets or a similar mechanism[2]—in tandem with a *port-based network access control* (PNAC) standard such as 802.1x/MAB—to learn what type of device has connected to it. Device identification triggers the appropriate Auto Smartports macro to run automatically on the switch and configure its interface appropriately for the detected device type. This behavior eases the administrative burden of configuring multiple switchports manually. (Similarly, when there is a "link-down" event on the port, the switch removes the macro.) In the ITU model and framework for network management, known as *FCAPS*, Auto Smartports macros act in support of what's called *configuration management*.

See *Auto Smartports Configuration Guide, Release 12.2(58)SE* at http://cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_58_se/configuration/guide/aspcg.html.

1. Infrequently abbreviated as *ASP*.
2. Such as Link-Level Discovery Protocol (LLDP) packets, packets that include specific MAC addresses or Organizational Unique Identifiers (OUIs), or attribute-value pairs within a RADIUS response.

## C

*Return to Top*

**CCMP**

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

*See also* WEP keys.

**CDP**

*Cisco Discovery Protocol*. DMPs and other devices that support CDP can communicate facts about themselves, amongst themselves, over any physical network medium that supports *Subnetwork Access Protocol* (SNAP) encapsulation. CDP uses the *data link layer*, which connects physical network media to upper-layer protocols. And because CDP operates at this level, two or more CDP devices that support different network layer protocols (for example, IP and *Novell IPX*) can learn about each other.

Specifically, CDP causes devices to advertise not only their existence, but also their platform types, protocols, IP addresses, and SNMP-agent addresses to neighboring devices on their LAN switch or WAN. And when their connected switch is Medianet-ready, device identification can also trigger an Auto Smartports macro to run automatically.

Thus, CDP facilitates discovery—by network management applications—of Cisco devices that are neighbors of known devices. And this is particularly useful when such previously undiscovered neighbors use lower-layer, transparent protocols. After they possess information about such devices, network management applications can send SNMP queries to them.

In addition, CDP detects native VLAN and port duplex mismatches.

## D

↑ *Return to Top*

**DHCP**

*Dynamic Host Configuration Protocol*. A standard method for devices to request, and servers to allocate, IP addresses in a network without human intervention.

**DHCP option 125**

An optional DHCP relay class that:

- Injects “vendor-identifying, vendor-specific information” into the request (within a DHCP DISCOVER message) to receive a dynamic IP address.
- Identifies the type of client sending the DHCP DISCOVER message.

In turn, a DHCP server that is configured to support Option 125 can relay the client-generated request to some other DHCP server. This mechanism allows an organization to designate DHCP servers for clients that meet particular criteria. For example, you might want all of your DMPs to receive their IP addresses from a DHCP server that you reserve for this purpose exclusively.

## E

*Return to Top*

**EAP**

EAP is the Extensible Authentication Protocol that WPA uses to authorize user access to 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. Use 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.

## L

↑ *Return to Top*

**Location Services**

Mechanism by which a device can learn its actual physical ("civic") location through its connection to a Medianet-ready switch. Upon learning its location, the device can then share this information with peers, management servers, and other equipment on its network. The physical location of a DMP is almost always an important factor in which central management server it should trust, which assets it should play, which commands it should run, and which schedule it should follow.

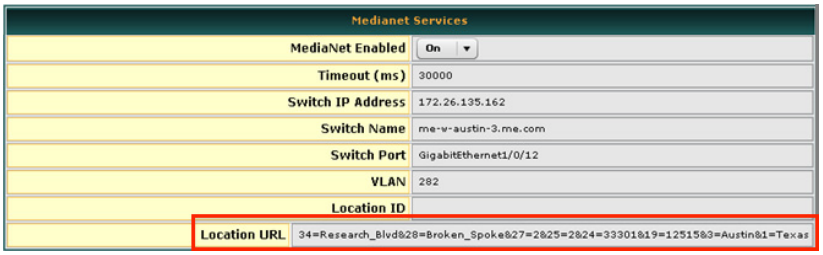
Someone must configure two essential values on your Medianet-enabled switch: "*civic-location-id*" and "*additional-location-information*." These values are encapsulated into a CDP message that endpoints receive.

***civic-location-id***

This value describes the physical site—including the municipality, street address, floor designation, and so on—where a switch and its attached nodes are deployed.

***additional-location-information***

This value describes any additional details to inject into the encapsulated CDP message. As this is a data injection, it depends wholly on the presence of a defined *civic-location-id* value. Absent **that** value, there is no way for **this** value to reach any endpoint. Later, when you plug a Medianet-ready DMP into a properly configured switch, the Location Services feature of MSI populates the Location URL field automatically in DMPDM.




**Note** **CDP and LLDP constrain how much location information you can store on a Medianet-enabled switch.** Make sure that this information never exceeds 255 bytes.

**Note** **A DMP 4400G cannot receive or use Location Services information over Wi-Fi.** Its connection type to your Medianet-enabled switch must be Ethernet.

## M

↑ *Return to Top*

**Medianet**

End-to-end intelligent architecture for optimized delivery of rich media to a variety of endpoints throughout an enterprise. Cisco Medianet is media-aware, endpoint-aware, and network-aware.

**MSI**

*Media Services Interface*. Announces services to a DMP or any other Medianet-ready device that you connect to a Medianet-enabled switch. MSI tells devices about their neighbors and their civic location.

**MSI registration service**

Medianet feature by which:

- Devices send encrypted registration requests to management servers.
- Servers receive such requests, respond to them, and store records in a local database.

**MSI service discovery**

Mechanism that applies DHCP option 125 packets to advertise—and poll for—the availability of particular services in a network. Service Discovery also notes which hosts provide these services. For your purposes as a DMP administrator, Medianet should know that a DMM server is available and know exactly which addressable node it is on your network. So naturally, you must configure your DHCP server to facilitate this information-sharing model. Configuration methods vary among platforms and implementations.

An example here shows entries in the **dhcpd.conf** file for a Linux-based DHCP server called *dhcpd*. Entries like these advertise the IP address of your authoritative DMM appliance—converted here from decimal to hex and shown in red—to any DMPs that should trust its directives implicitly.

```
option domain-name "example.com";
option domain-name-servers 192.168.1.1;
option option-125 code 125 = string;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.200 192.168.1.210;
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
}
class "DMM" {
match if option option-125 = "\x00\x00\x00\x09\x06\x13\x04\x01\x44\x4d\x4d";
option option-125
"\x00\x00\x00\x09\x0b\x14\x09\x01\x80\x6b\xe0\xbc\x1f\x90\x00\x01";
}
```

**Tip** **The Linux CLI can easily convert IP address octets from decimal to hexadecimal.**

`$ echo 'ibase=10;obase=16;` octet `' | bc` ← *(Remember to use a closing quote mark before the pipe.)*

And so, in keeping with the previous conversion example, shown in red....

- **128** becomes **x80**
- **107** becomes **x6b**
- **224** becomes **xe0**
- **188** becomes **xbc**

In contrast, the DHCP offering in Windows Server 2008 (and, likewise, Windows Server 2003) cannot handle DHCP option 125 queries natively. Therefore, you must install a "callout" DLL that injects this ability into the server before you can configure it to advertise the availability of any service.

**Note** For **32-bit** Windows Server, the DLL filename is DHCPSDDLL**x86**.DLL.
For **64-bit** Windows Server, the DLL filename is DHCPSDDLL**x64**.DLL.

Afterward, you must edit **\Medianet\msi\apps\dhcpsddll\src\dhcpsdconfig.reg** to include a *3-tuple* (**IP,port,transport**), converted to hexadecimal, that identifies your DMM appliance as a provider of centralized management for DMPs.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Settings]
"DebugLevel"=dword:00000000
"IgnoreProcessItFromChain"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Records\1]
"DMM"=hex:0a,c2,33,2a,1f,90,00,01
```

And finally, you must add two keys to the Windows registry, under
`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Paramters`

- **CalloutEnabled REG_DWORD 1**
- **CalloutDlls REG_MULTI_SZ** <*full_path_to_DLL*>

**Note** **See the Medianet documentation on Cisco.com for detailed instructions.**

## 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. It is 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.

## 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 for securing 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 de-encryption 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.

# 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.

**Note** **Many third-party converters are available.** We do not offer any Cisco converter for this purpose.

The typical WEP process is as follows.

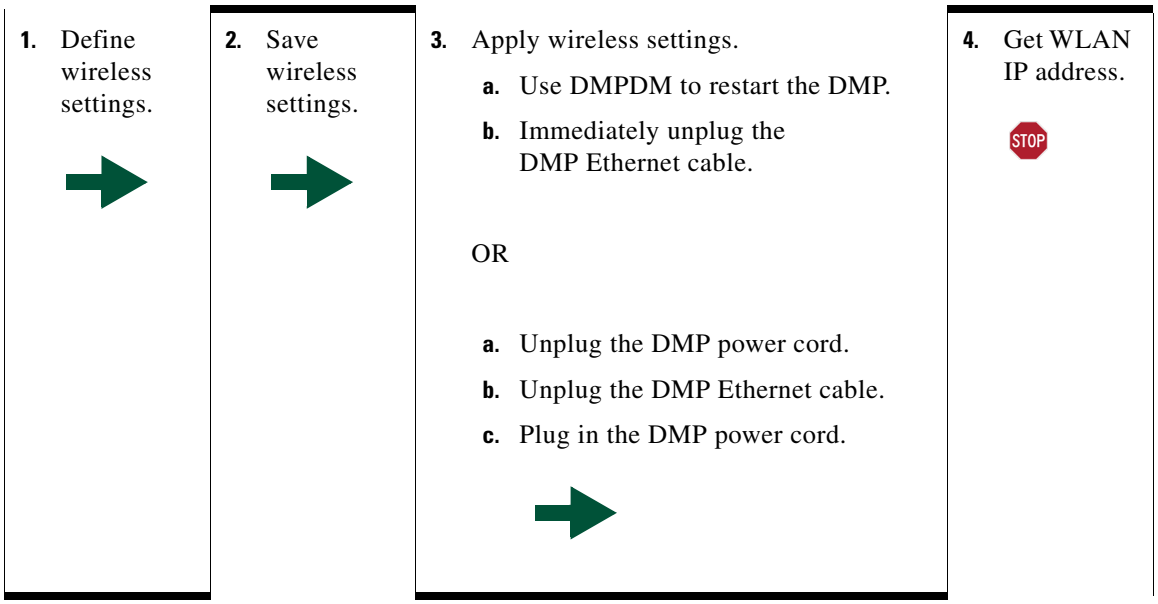
1. Pick an ASCII passphrase. For example, *PassphraseWEP128*.
2. Convert your string of ASCII characters to the hexadecimal key or keys for your network.
   - WEP-64 uses four short hexadecimal keys.
   - WEP-128 uses one long hexadecimal key.
3. Configure your DMP to use the ASCII from which you derived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

### Related Topics

- Configure a Wireless Network Connection, page 10-16
- Configure a Wireless Network Connection, page 10-16

# Workflow to Define Wi-Fi Settings

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.



# Partial Support for Cisco Medianet 2.1 Features

Cisco Medianet is an end-to-end architecture for networks that deliver rich-media experiences. Some DMP endpoints support some Cisco Medianet 2.1 features.

**Note** **We do not support any Medianet features on DMP 4305G endpoints.**

**Tip**

- **To assess your network for Medianet readiness, see http://cisco.com/go/mra.**
- **To review solution reference network designs (SRNDs) for Medianet, see http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html.**

| | |
|---|---|
|  **DMP 4310G** | DMP 4310G endpoints support discovery via DHCP and can learn their physical location. In addition, they know and can broadcast their product type, model, and software version. Through their use of your Medianet, they can receive their IP address, VLAN assignment, and network configuration settings automatically. Furthermore, they receive information from Medianet through DHCP[1] that helps them to autoregister themselves with your DMM server. Later, after a successful autoregistration, the splash screen on these DMPs includes key parameters and states explicitly that setup succeeded. |
|  **DMP 4400G** | Medianet 2.1 feature support by DMP 4400G endpoints is equivalent to support by DMP 4310G endpoints, **with just one exception**. Ordinarily, a DMP 4400G can participate in networks via either an Ethernet connection or a Wi-Fi connection. **However:**<br><br>A Wi-Fi connection by a DMP 4400G prevents it from obtaining or using any Location Services information that Medianet might be configured to provide. |

1. With DHCP option 125 (V-I Vendor-Specific Information) for service discovery, after you configure your supported DHCP server to support this option. See **RFC 3925**.

**Note** **These features are designed to simplify the largest deployments, whereas DMPDM is designed to support the smallest deployments.** If you manage your DMP primarily via DMPDM, your benefit from Medianet integration will be minimal.

# Understand Medianet Autoconfiguration for DMP 4310G Endpoints

DMP 4310G and 4400G endpoints can use CDP to announce and identify themselves on networks.

**AND**

You might use Ethernet cables to connect such DMPs to switches where the autoconfiguration (Auto Smartports) features of Medianet are enabled.

When you do, these switches recognize from the CDP announcements that the newly connected devices are DMPs.

After recognizing that a DMP is attached to one of its Ethernet ports, the switch can apply to this port a set of built-in configuration macros (Auto Smartports) that are optimized specifically for DMPs. By configuring so many settings automatically, Medianet can accelerate and simplify DMP mass deployments, QoS configuration, and asset tracking. In turn, these simplified deployments can lower your operating costs.

# Information That Medianet and DMPs Exchange

Medianet and a DMP 4310G can exchange these types of data.

- name of the chassis
- system name
- system object
- hardware revision
- firmware revision
- software revision
- seial number
- manufacturing name
- model name
- asset identifier
- CDP timeout
- VLAN assignment
- switch port assignment
- switch name and model
- switch IP address
- loation string

If you would like to learn more about Medianet, see http://cisco.com/go/medianet.

# Restrictions

### Wireless Networks

- **Ethernet connections take priority over Wi-Fi connections on DMPs where both are active.**
- We do not support “open” Wi-Fi networks. They are a security risk.
- We do not support media streams to DMPs over Wi-Fi networks. The experience is poor.
- DMP 4305G endpoints do not support Wi-Fi.

### Autoregistration

- Autoregistration depends upon the Cisco TAC Troubleshooting Access option for DMPs and fails unless this option is enabled.

### Login Credentials

- All DMPs that you manage centrally in DMM must share one identical set of DMPDM login credentials.

### Medianet

- When a DMP 4310G relies upon a Medianet switch where more than one VLAN uses DHCP, the DMP might come to use the wrong IP address. For this to occur, temporary conditions that do not sever the DMP's AC power connection must nonetheless interrupt its network connection through the switch. (Thus, this problem cannot possibly occur while the DMP uses PoE.) Specifically, the Medianet switch assigns its default VLAN to your DMP. But then—after your DMP’s network connection is interrupted and restored—your Medianet switch assigns to your DMP a dynamic IP address from another VLAN on your Medianet switch. This easily prevented mismatch disrupts centralized management of your DMP. To prevent this problem or to recover from it, you can download and run the patch from Cisco.com.

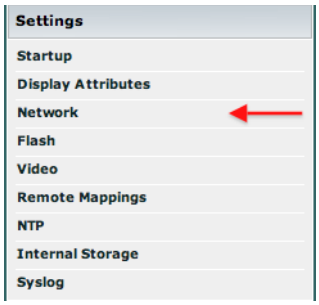
# Procedures



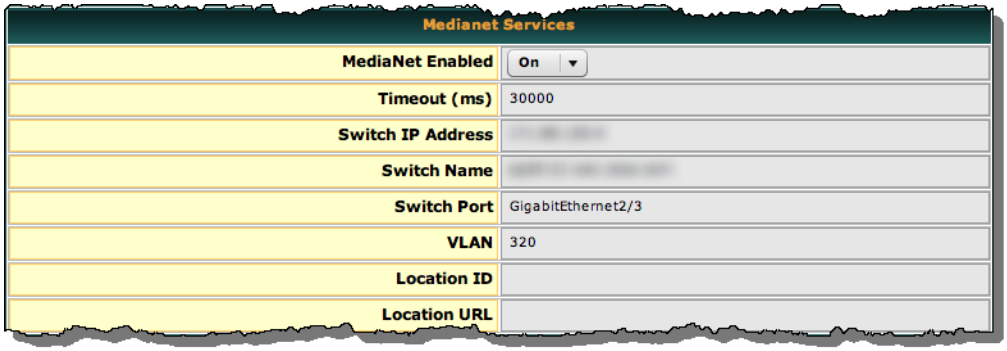
## Activate Medianet Support

### Procedure

**Step 1** Click **Network** in the Settings area.




**Step 2** Choose **On** from the Medianet Enabled list in the Medianet Services area.




**Step 3** Save this changed setting, and then restart your DMP.

# Configure HTTP Proxy Server Settings for a DMP 4310G

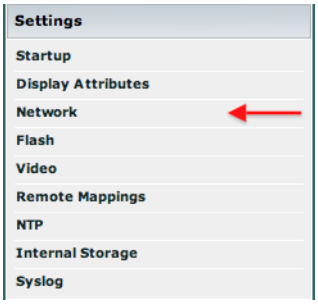
**Note**

- **The only transport protocol that we can proxy in this release is HTTP over :80 or :8080.**
- **The only asset types that we can proxy in this release are video and SWF.**

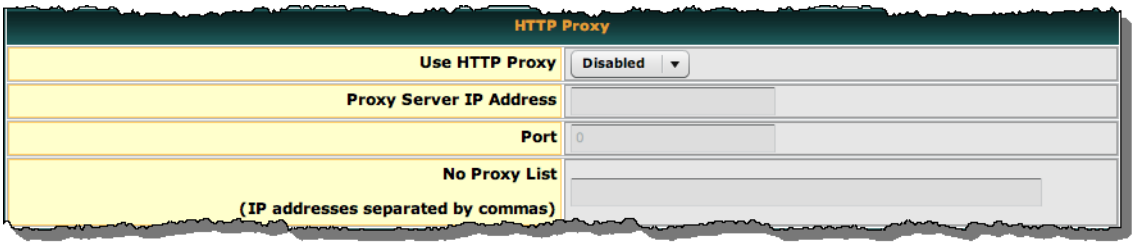
You can configure a DMP 4310G to use a proxy server and you can specify which of your content servers should be exempt from this proxy service.

### Procedure

**Step 1** Click **Network** in the Settings area.




**Step 2** Choose Enabled from the Use HTTP Proxy list.



**Step 3** Three fields become editable.

**Proxy Server IP Address**

- To proxy the playback of **video assets** from an HTTP server, you must enter the routable IP address of your proxy server. Do not enter a hostname. Do not use any wildcards.
- To proxy the playback of **SWF assets** from an HTTP server, you can enter *either* the routable IP address *or* the FQDN (DNS-resolvable hostname) of your proxy server. Do not enter any wildcards.

**Port**—Enter either **80** or **8080**. Do not enter any other value.

**No Proxy List (IP addresses separated by commas)**

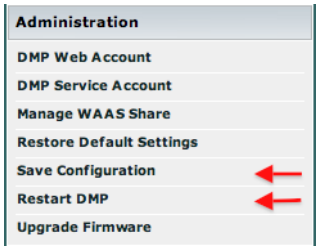
- To bypass your proxy when you play **video assets** from particular HTTP servers, you must enter comma-separated IP addresses. These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy video playback from any other HTTP server. Do not enter any hostnames. Do not enter any wildcards.
- To bypass your proxy when you play **SWF assets** from particular HTTP servers, you can enter *either* comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy video playback from any other HTTP server. Do not enter any wildcards.

**Note** **Proxy settings do not have any effect on RSS traffic.** When an RSS request crosses from one Internet domain to another, your DMP is its own proxy.

**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**.



# Configure HTTP Proxy Server Settings for a DMP 4400G or DMP 4305G

**Note** **The only transport protocol that we can proxy in this release is HTTP over :80 or :8080.**

You can configure a DMP 4400G or DMP 4305G to use a proxy server and you can specify which of your content servers should be exempt from this proxy service.

**Procedure**

**Step 1** Click **Network** in the Settings area.

**Step 2** Choose **Enabled** from the Use HTTP Proxy list.

**Step 3** Three fields become editable.

- **Proxy Server IP Address or Hostname**—The routable IP address *or* the FQDN (DNS-resolvable hostname) of your proxy server. Do not enter any wildcards..
- **Port**—Enter either **80** or **8080**. Do not enter any other value.
- **No Proxy List**—To bypass your proxy when you play assets from particular HTTP servers, you can enter *either* comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy content from any other HTTP server. Do not enter any wildcards.

**Note** **Proxy settings do not have any effect on RSS traffic.** When an RSS request crosses from one Internet domain to another, your DMP is its own proxy.

**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**.

# Configure a Wireless Network Connection

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

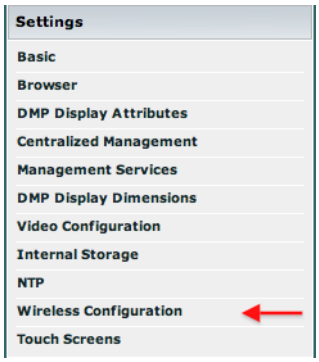
**Before You Begin**

- 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 2-5.
  - Alternatively, if Table 2 on page 2-5 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.
- Connect Over Ethernet.
- Log in to DMPDM, page 7-5.

**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 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.

**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, you can configure your DMP to use a static IP address.

d. (**Optional**) 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

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Connect Over Ethernet, page 2
- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21

# 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

- Connect Over Ethernet, page 2.

  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.

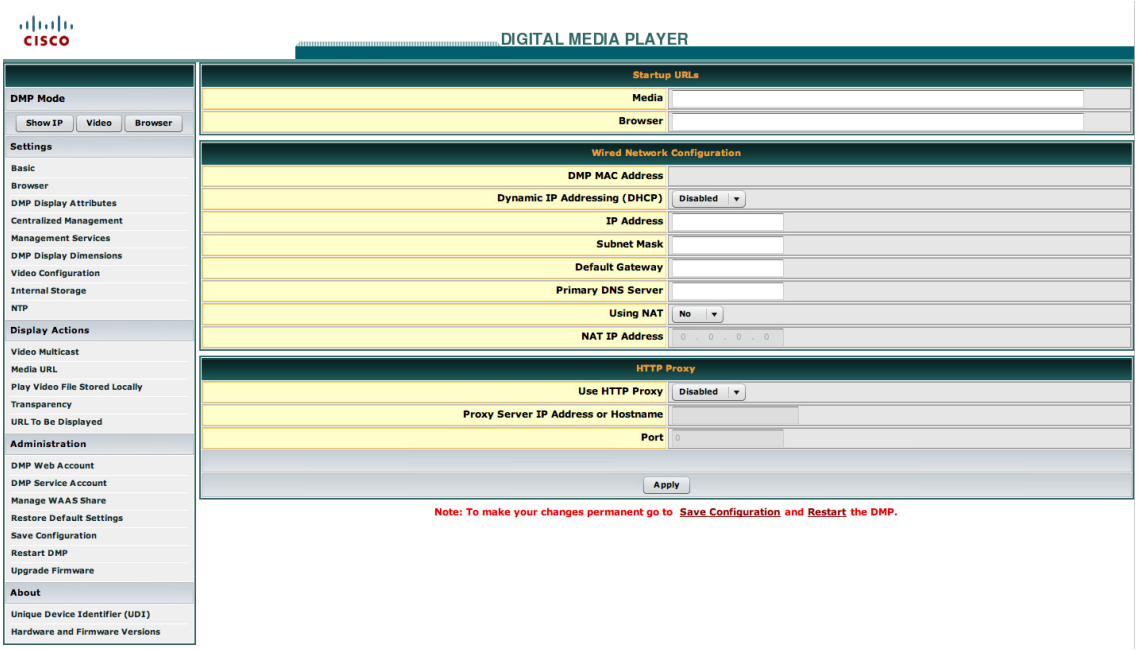
**Step 4** Turn **On** your DMP and make a note of the IP address that it shows on its presentation system.

**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 7-5.

**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.




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

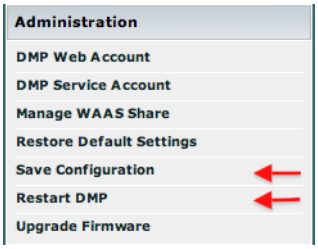
**a.** Choose **Yes** from the Using NAT list.

**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

- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21

## Assign a Static IP Address to a Wireless DMP 4400G

### Procedure

**Step 1** Log in to your wireless access point as an administrator.

**Step 2** Use its administrative features to assign a static IP address to your DMP.

**Step 3** Stop. You have completed this procedure.

### Related Topics

- Prepare Your DMP to Use a Static IP Address Over Ethernet, page 10-19

## Show the Assigned IP Address

### Before You Begin

- If you have not yet obtained an IP address for your DMP, see the quick start guide for your DMP model type to learn how to connect and set up your DMP.

### Procedure

**Step 1** Click Show IP to learn the IP address of your DMP.

The address is briefly visible on your DMP display.

**Step 2** Stop. You have completed this procedure.

# Reference

# Network Settings Reference

## UI Reference: Elements to Define Basic Network Settings

*Table 10-1 Elements on the Basic Page*

| Element | Description |
|---|---|
| **Startup URLs** | |
| Media | The URL or local path that points to an encoded digital video file, which your DMP should load automatically and show immediately after every restart. The URL or pathname cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding. The value that you enter is case-sensitive.<br>Supported transport protocols and URL types are as follows:<br>• **http://**<*ip_address*>**/**<*path_and_filename*><br>• **udp://**<*ip_address_of_multicast_server*>**/**<*port_number*><br>• **file:**///tmp/ftproot/usb_1/<*path_and_filename*> **—For files on the internal flash drive**<br>• **file:**///tmp/ftproot/usb_2/<*path_and_filename*> **—For files on a mounted USB drive**<br>• **file:**///tmp/ftproot/CIFS/<*path_and_filename*> **—For files on a mounted network share**<br>**Note The video file must be encoded in a way that your DMP supports.**<br>**Tip To simulate an audio-only file if your DMP does not support their use directly, play an MPEG-2 file that contains all of the audio data that you want to play and contains just one frame of video data.** |
| Browser | The HTTP URL of any document that the embedded browser should load automatically and show immediately after each restart. For example, the URL that you enter might point to an HTML page with an embedded Flash file that animates the logo for your organization. The URL cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding.<br>**Tip We recommend that you do not point to any document or site that requires human interaction to be useful, interesting, or entertaining, because there is no keyboard or mouse that you can use to interact with what you show on your DMP display.** |
| **Wired Network Configuration** | |
| DMP MAC Address | An uneditable representation of the MAC address that is associated with the NIC in your DMP. |
| Dynamic IP Addressing (DHCP) | Indicates whether your DMP uses a static IP address or a dynamic IP address. Options in the list are as follows:<br>• **Enabled**— Your DMP uses a dynamic IP address that it obtained from a DHCP server.<br>• **Disabled**— Your DMP uses a static IP address. |
| IP Address | The IP address that is assigned to your DMP.<br>**Note If your DHCP server changes the IP address assignment for a centrally managed DMP while the DMP is running, instead of waiting for the DMP to restart, you must restart the DMP.** Otherwise, you cannot use DMM-DSM to centrally manage that DMP. |

*Table 10-1 Elements on the Basic Page (continued)*

| Element | Description |
|---|---|
| Domain Name | The DNS-resolvable domain name for your organization, such as **example.com**.<br>When you disable DHCP and assign a static IP address to your DMP, its configuration to resolve local hostnames is no longer completely automatic. You must specify the domain name so that your DNS server can convert local device names, such as **server**, to fully qualified domain names, such as **server.example.com** —which are then resolvable to IP addresses for routing. |
| Subnet Mask | The IPv4 netmask that the DMP-local network segment uses. |
| Default Gateway | The IP address that is assigned to whatever router provides outside network access to and from devices on the DMP-local network segment. |
| Primary DNS Server | The routable IP address or DNS-resolvable hostname of the primary DNS server for whichever network segment is local to your DMP. We recommend that you enter the IP address, not the hostname. |
| Using NAT | Indicates whether your DMP uses private IP addressing. Choose an option from the list.<br>• **Yes**—Your DMP uses a private IP address.<br>• **No**—Your DMP does not use a private IP address. |
| NAT IP Address | The globally routable IP address that DMM-DSM should use to manage your DMP, if your DMP has a private IP address due to network address translation (NAT). |
| **HTTP Proxy** | |
| Use HTTP Proxy | Indicates whether your DMP uses a proxy server. Choose an option from the list.<br>• **Enabled**—Your DMP sends and receives HTTP traffic through the specified proxy.<br>• **Disabled**—Your DMP does not use a proxy. |
| Proxy Server IP Address or Hostname | The routable proxy server IP address or DMS-resolvable hostname. DMPDM ignores any address that you enter unless you chose Enabled from the Use HTTP Proxy list. |
| Port | The logical TCP port number through which the proxy server provides HTTP proxy services. DMPDM ignores any port that you enter unless you chose Enabled from the Use HTTP Proxy list. |
| No Proxy List | Either comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy content from any other HTTP server. Do not enter any wildcards. |

# FAQs and Troubleshooting



## DMP Network Connectivity

**Q. What prevents me from centrally managing my DMP?**

**A.** Ask yourself these questions.

- Has your DHCP server changed the IP address assignment for your DMP?
- Was your DMP running when its address changed?

If these statements are true, do not wait for your DMP to restart automatically. Instead, restart it manually. Until it is restarted, it cannot be centrally managed.


# File Storage

**Revised: May 4, 2015**



# Concepts



## Understand Internal Storage Capacity

**Caution** **Do not open a DMP.**

Internal storage is formatted to this capacity.

| DMP Model | Storage Medium | Formatted Capacity |
|---|---|---|
| DMP 4305G | CF | 2GB |
| DMP 4310G | SSD | 32GB |
| DMP 4400G | SD | 4GB |

# Performance Guidelines for Local Storage

We recommend that you do not upload files to the /tmp/ftproot subdirectory. Instead, use **/tmp/ftproot/usb_1**.

If you upload files to /tmp/ftproot accidentally, and then DMP performance suffers, you can restore your DMP to its normal operating condition easily. Just unplug it, wait 15 seconds, and then plug it in again.

**Note** **This method deletes the files that you uploaded.**

# Local Storage Restrictions for DMP 4310G

A DMP 4310G that uses an attached USB storage volume might corrupt or erase data on this attached volume. Likewise, a DMP 4310G might lose its ability to mount this attached volume. After the DMP reaches this general state, it sometimes reports incorrectly that the attached volume is still mounted and working.

These problems can occur when you disconnect the external volume from the upper USB interface on a DMP 4310G and then, without any delay, plug it immediately into the lower USB interface on the same DMP. However, these problems do not occur in every such case. In our tests, they occurred approximately 1 percent of the time.

To reduce your possible exposure to these problems, wait no less than 3 seconds after you connect or disconnect an attached volume, before you do the reverse. In our tests, this best practice eliminated the risk.

Restart the DMP if it merely unmounts its attached volume.

There is no workaround after the attached volume is erased or its data becomes corrupted. All that you can do after the fact is reformat the volume and restore its data from a recent backup.

# Procedures



# Define Storage Settings



## Manage Permissions for Internal Storage

You can set the permissions for internal storage in your DMP.

**Procedure**

**Step 1** Click **Internal Storage** in the Settings list.

**Step 2** View or edit the values, then click **Apply**.

After you click Apply, the entry or change takes effect. However, the previously defined value will return the next time that your DMP restarts.

**Step 3** (**Optional**) *Would you like to put all changed values into effect permanently, so that they persist even after your DMP restarts?* Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

It is not necessary to restart your DMP.

**Step 4** Stop. You have completed this procedure.

#### Related Topics

- UI Reference: Elements to Define Internal Storage Settings, page 11-4

## Mount or Unmount a Network Share

**Note** **DMPs can mount only one shared volume at a time.**

#### Procedure

**Step 1** Click **Manage WAAS Share** in the Administration list.

**Step 2** Enter or edit the required values, and then click **Apply**.

**Step 3** Do one of the following.

- Click **Mount Share** to connect your DMP to this network share immediately.
- Click **Unmount** to disconnect your DMP from this share.

**Step 4** Stop. You have completed this procedure.

#### Related Topics

- UI Reference: Elements to Define Network Share Settings, page 11-4
- Enable or Disable Types of Access to Your DMP, page 8-6

# Reference

- UI Reference Topics, page 11-3

# UI Reference Topics

- UI Reference: Elements to Define Internal Storage Settings, page 11-4
- UI Reference: Elements to Define Network Share Settings, page 11-4

## UI Reference: Elements to Define Internal Storage Settings

*Table 11-1 Elements on the Internal Storage Page*

| Element | Description |
|---|---|
| Present | Indicates whether the internal SD card is present.<br>**Note This value does not indicate anything about the presence of any external USB flash drives or USB hard drives that you might have mounted.** |
| Access Mode | Indicates whether the internal SD card is writable or if it is read-only. |
| Capacity (in megabytes) | Shows the total capacity. |
| Free Space (in megabytes) | Shows the total free space. |

**Related Topics**

- Manage Permissions for Internal Storage, page 11-2

## UI Reference: Elements to Define Network Share Settings

*Table 11-2 Elements on the WAAS Share Settings Page*

| Element | Description |
|---|---|
| Status | Says whether your DMP has a network share mounted now. If connection attempts have failed, says how many more times your DMP will try to mount the share. |
| Hostname/IP Address | The DNS-resolvable hostname or routable IP address of the CIFS share server.<br>**Note DMPs can mount only one shared volume at a time.** |
| Shared Directory | The name of the CIFS share. |
| Domain (optional) | The WINS domain name. |
| Username | The username for mounting the share. |
| Password | The password that is associated with the username. |


# Browser Settings ('TVzilla')

**Revised: May 4, 2015**



# Concepts



**Note** **Cisco DMP 4310G endpoints do not have any browser in this release**

## Understand URL Behaviors

If you enter URLs for both video content and browser content, the actual result depends on a combination of these factors:

- Whether you click Video or Browser (to show only that one kind of content).
- What height and width values you enter for the embedded browser.
- What amount of transparency you assign to the HTML plane.

URLs cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding.

### Related Topics

- Adjust TVzilla Settings, page 12-5
- Adjust Whether TVzilla is Transparent, Translucent, or Opaque, page 12-6

# Understand Content Substitution ('Failover')

Your DMP has three stages for content substitution.

- Stage 1: Sequence of Operations, page 12-2
- Stage 2: Sequence of Operations, page 12-2
- Stage 3: Sequence of Operations, page 12-3

**Note** **You can edit values that affect DMP behaviors during content substitution.** These are the editable values:

- Failover URL
- Failover Timeout (in milliseconds)
- Maximum Number of Failover Attempts
- Recovery URL
- Recovery Timeout (in milliseconds)

## Stage 1: Sequence of Operations

When an HTTP status code of 404 or 500 prevents your DMP from obtaining the content that you scheduled it to play, your DMP enters stage 1 failover. Stage 1 operations for failover occur in a predictable sequence. Your DMP:

1. Verifies that you entered a URL in the Recovery URL field.
2. Verifies that the Recovery URL is reachable.
3. Verifies that the assets at the Recovery URL are valid.
4. Plays assets from the Recovery URL, instead of playing assets that were scheduled for playback.

When any operation fails during stage 1 failover, your DMP enters stage 2.

### Related Topics

- Stage 2: Sequence of Operations, page 12-2

## Stage 2: Sequence of Operations

When an error of any kind prevents your DMP from retrieving and playing Recovery URL assets, your DMP enters stage 2 failover. Stage 2 operations for failover occur in a predictable sequence. Your DMP:

1. Verifies that you entered a URL in the Failover URL field.
2. Verifies that the Failover URL is reachable.
3. Verifies that assets at the Failover URL are valid.
4. Plays assets from the Failover URL, instead of playing assets from the Recovery URL.

Playback of the Failover URL persists until one of the following occurs.

- The error condition ends, which prevented your DMP from completing stage 1 successfully. In this case, your DMP stops playing the Failover URL assets and starts to play assets from the Recovery URL.
- The error condition ends, which triggered stage 1. In this case, your DMP obtains and plays the assets that it was scheduled to play.
- You use the "Stop All Applications" system task in Cisco Digital Signs (on your DMM server).

When any operation fails during stage 2 failover, your DMP enters stage 3.

#### Related Topics

- Stage 1: Sequence of Operations, page 12-2
- Stage 3: Sequence of Operations, page 12-3

## Stage 3: Sequence of Operations

When errors interfere with stages 1 and 2, your DMP enters stage 3 failover. Stage 3 operations for failover occur in a predictable sequence. Your DMP:

1. Your DMP starts to play a video loop from ROM, which shows a butterfly beating its wings.
2. Playback of the video loop persists until one of the following occurs:
   - The error condition ends, which prevented your DMP from completing stage 1 successfully. In this case, your DMP stops playing the butterfly video and starts to play assets from the Recovery URL.
   - The error condition ends, which triggered stage 1. In this case, your DMP obtains and plays the assets that it was scheduled to play.
   - You use the "Stop All Applications" system task in Cisco Digital Signs (on your DMM server).
   - You restart or shut down your DMP.

The video clip in ROM has no other purpose than stage 3 failover. You cannot change it and you cannot delete it.

#### Related Topics

- Stage 1: Sequence of Operations, page 12-2
- Stage 2: Sequence of Operations, page 12-2

# Understand HTTP 'HEAD' Request Timeout

Before it tries to download content from a webserver, your DMP first makes sure that the content exists at its expected address. Your DMP starts this validation by sending the webserver what's called an *HTTP HEAD* request. Then, when the webserver responds within 1 second to verify that the expected address is valid, your DMP sends an *HTTP GET* request that triggers the actual download.

### Timeout Benefit

When the webserver takes more than 1 second to respond **OR** when its response is negative, your DMP enters a content substitution ("failover") state. In this state, your DMP substitutes available assets for unavailable ones. So, instead of showing a black screen, this behavior causes an affected digital sign to play alternative content that you chose previously. The underlying logic for this behavior anticipates a serious problem and overcomes it gracefully.

### Timeout Risk

However, this logic cannot account for all possible scenarios. When a webserver would otherwise verify (after 2 seconds, for example, or even 1.2 seconds) that an asset's address is valid, your DMP misinterprets the delay and enters its content failover state unnecessarily.

### You Can Disable the Timeout

You can use either of these methods to disable the timeout on just one DMP (**CSCua03897**).

- Point your desktop browser to **https://admin:**<*password*>**@**<*DMP_FQDN*>**:7777/set_param?video.force_wget_use=0&mib.save=1**, where:
  - <*DMP_FQDN*> is the DNS-resolvable hostname for exactly this DMP.
  - <*password*> is whichever password you set most recently for this DMP's *admin* user.

  **OR**

- Point Filezilla to **https://admin:**<*password*>**@localhost:7777/set_param?video.force_wget_use=0&mib.save=1**, where <*password*> is whichever password you set most recently for this DMP's *admin* user.

**Note** **To reenable the timeout, change the set_param command string to:** `video.force_wget_use=1&mib.save=1`.

# Supported Fonts

TVzilla supports some bitmap fonts and some TrueType fonts; it will substitute an installed font for any unsupported font.

Other typographic representations that you might show on a DMP display, such as the opening titles for a theatrical film, do not require that any font be installed. Similarly, when a font is embedded within a Flash file that you show, the Flash file will load correctly even if the corresponding font is not installed on your DMP.

See *User Guide for Cisco Digital Media Manager 5.3.x* on Cisco.com to learn precisely which fonts your DMP supports.

# Procedures



## Adjust TVzilla Settings

You can change how TVzilla, the embedded browser in your DMP, operates in certain situations.

### Procedure

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

**Step 2** Enter or edit the required values, and then click **Apply**.

**Step 3** Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

**Step 4** Restart your DMP.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define TVzilla Settings, page 12-7
- Restart Your DMP, page 7-6

## Show TVzilla in Full-Screen Mode

### Procedure

**Step 1** Click Browser to fill the screen on your DMP display with TVzilla.

The "video content" plane is hidden.

**Tip** **Click Video to exit this full-screen mode.**

**Step 2** Stop. You have completed this procedure.

### Related Topics

- Specify Which URL to Load in TVZilla, page 12-6

# Adjust Whether TVzilla is Transparent, Translucent, or Opaque

When you simultaneously play videos and run TVzilla, the "HTML content" plane is always on top of (in front of) the "video content" plane. However, you can adjust the visual density of TVzilla, so that it is fully opaque, fully transparent, or any degree of translucency between those two extremes.

The "video content" plane is always fully opaque. You cannot adjust it.

### Procedure

**Step 1** Click **Transparency** in the Display Actions list.

**Step 2** Enter or edit the required values.

**Step 3** Click **Apply** to confirm that you are satisfied with the entry or change that you made and to record it in volatile memory.

After you click Apply, the entry or change takes effect. However, the previously defined value will return the next time that your DMP restarts.

**Step 4** (**Optional**) *Would you like to put all values into effect permanently, so that they persist even after your DMP restarts?* Choose **Administration > Save Configuration** and, when the Save Configuration page appears, click **Save**.

**Step 5** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define Transparency Settings for HTML Content, page 12-10

# Specify Which URL to Load in TVZilla

You can load a web page or other content on the HTML content plane (TVzilla). The HTTP URL that you enter persists until you use this procedure again to enter a different URL or until the next time that you restart your DMP. You cannot save the URL entry so that it persists after a restart.

### Procedure

**Step 1** Click **URL to be Displayed** in the Display Actions list.

**Step 2** Enter or edit the HTTP URL, and then click **Go**.

**Step 3** (**Optional**) *Would you like to stop showing the specified content?* Do one of the following.

- Click Video.
- Enter an HTTP URL that points to different content, and then click **Go**.

**Step 4** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Specify Which URL TVzilla Should Load, page 12-10

# Reference



# UI Reference Topics



## Browser Settings Reference



### UI Reference: Elements to Define TVzilla Settings

*Table 12-1 Elements on the Browser Page*

| Element | Description |
|---|---|
| **Browser** | |
| Adobe Flash Player Plug-in Version | Indicates whether the browser should support Flash 6 or Flash 7. Our Flash support extends to SWF files only, not to FLV files. We do not support audio in SWF files. This setting is visible only when you use DMPDM on a DMP 430xG; it is not relevant to a DMP 4400G, which always uses Flash 9 or 10 for this purpose. |
| Screen Rotation Angle (clockwise) | Indicates whether you have rotated the HTML content plane and shows the amount of rotation. You might choose to rotate the HTML content plane if you have rotated your DMP display.<br>The rotation feature applies only to content that plays on the HTML content plane. To play video vertically, you must first encode it vertically. |
| Browser Alpha Channel Transparency (0-255) | **Note** **Although this setting might look identical to a setting described in the "Adjust Whether TVzilla is Transparent, Translucent, or Opaque" section, they are different.** You use this setting to configure transparency for the browser.<br>The amount of transparency that you configure for all content that your DMP shows in the embedded browser. Values can range from 0 to 255, where:<br>• **0**—Content in the browser is completely transparent.<br>• **255**—Content in the browser is completely opaque. |
| Splash Screen Display Time (in milliseconds) | Indicates in milliseconds how long the splash screen persists on your DMP display when you start or restart your DMP. |
| Screen Resolution Autodetection (requires DMP Display Autodetection) | Indicates whether screen resolution detection is enabled. You can enable this feature only after you have enabled the feature to autodetect DMP display attributes (which is available from the DMP Display Attributes page). If you want to set the browser resolution manually, you must disable this feature. |

*Table 12-1 Elements on the Browser Page (continued)*

| Element | Description |
|---|---|
| Maximum Detected Screen Width (in pixels) | Indicates the HTML content pane width in pixels, if you are using the autodetected maximum width. Permitted values range from 640 to 1920. You might want to change this value if you know that your DMP display supports widths greater than the default value of 1366, but 1366 is the autodetected width. You can edit this value only if you selected Enabled from the Screen Resolution Autodetection list. |
| Maximum Detected Screen Height (in pixels) | Indicates the HTML content pane height in pixels, if you are using the autodetected maximum height. Permitted values range from 480 to 1080. You might want to change the value of you know that your DMP display supports heights greater than the default value of 768, but 768 is the autodetected height. You can edit this value only if you selected Enabled from the Screen Resolution Autodetection list. |
| HDMI-detected Screen Resolution (in pixels) | Indicates in real time the width and height in pixels that the attached DMP display is showing, if you selected Enabled from the Screen Resolution Autodetection list and if your DMP uses an HDMI cable to attach to its DMP display.<br>**Tip** **Cisco content creation guidelines for digital signage assume that the screen resolution width is 1366 pixels and the screen resolution height is 768 pixels.** When the autodetected values are different than these, we strongly recommend that you do the following.<br>1. Choose **DMP Display Attributes**.<br>2. From the DMP Display Autodetection (requires HDMI) list, choose **Disabled**.<br>3. From the Display Standard list, choose **VESA_1360x768x60.**<br>4. From the Interface (DMP display output) list, choose **HDMI.**<br>These selections will apply 1360 and 768 as the width and height values to use, respectively, ensuring that your content for digital signage works as designed—despite the trivial 6-pixel deviation in the width value, as compared to the content creation guidelines. |
| Screen Width (in pixels) | ⚠ **Caution** **When you will show content simultaneously on the HTML plane and the video plane, you must not enter any width that is greater than 1366 pixels.**<br>Indicates the HTML content pane width in pixels, if you are using a custom width. Permitted values range from 640 to 1920. You can edit this value only if you selected Disabled from the Screen Resolution Autodetection list. |
| Screen Height (in pixels) | ⚠ **Caution** **When you will show content simultaneously on the HTML plane and the video plane, you must not enter any height that is greater than 768 pixels.**<br>Indicates the HTML content pane height in pixels, if you are using a custom height. Permitted values range from 480 to 1080. You can edit this value only if you selected Disabled from the Screen Resolution Autodetection list. |
| Cache (only when Internal Storage Access Mode is "Read and Write") | Indicates whether the browser is caching content to local storage on your DMP. Caching is possible only when you have selected the Read and Write option from the Internal Storage Access Mode list on the Internal Storage page. |

*Table 12-1 Elements on the Browser Page (continued)*

| Element | Description |
|---|---|
| Syslog | Indicates whether you have enabled the logging of system messages on your DMP. Choose an option:<br>• **Enabled**—Syslog enabled.<br>• **Disabled**—Syslog disabled. |
| Syslog Collector IP Address | The IP address of the device that should collect syslog messages from your DMP. |
| Failover URL | The URL for the content that your DMP will show during stage-one failover. If the value is wrong, you can edit it. If you edit it, your edits will not take effect until you restart your DMP. |
| Failover Timeout (in milliseconds) | The number of milliseconds that your DMP should wait after each failed attempt to load the content from a URL, before it tries again. |
| Maximum Number of Failover Attempts | The number of times that your DMP should try to load the content from a URL before it considers that URL to be unreachable. |
| Recovery URL | The URL to show immediately on a DMP display after its attached DMP restarts for any reason, unless other content is scheduled to be shown. If the value is wrong, you can edit it. If you edit it, your edits take effect as soon as you click Apply. |
| Recovery Timeout (in milliseconds) | The maximum number of seconds that your DMP will wait for a response from the server that you identify in the Recovery URL field. |

### Related Topics

- Adjust TVzilla Settings, page 12-5
- Understand Content Substitution ('Failover'), page 12-2

## UI Reference: Elements to Define Transparency Settings for HTML Content

*Table 12-2 Elements on the Transparency Page*

| Element | Description |
|---|---|
| **Transparency** | |
| Browser Alpha Channel Transparency/Opacity (0-255) | **Note** **Although this setting might look identical to a setting described in the "Adjust TVzilla Settings" section, they are different.** You use *this* setting to configure transparency for the HTML content plane.<br><br>The amount of transparency that you configure for all content that your DMP shows on the HTML plane. The HTML plane and the video plane can overlap and you will see the video content plane *through* the HTML content pane if both of the following are true:<br>• You show video content and HTML content simultaneously.<br>• The HTML content plane touches any of the same *x*-axis and *y*-axis coordinates that the video content plane touches.<br><br>Values can range from 0 to 255, where:<br>• **0**—The HTML content plane is completely hidden and only the video content plane is visible.<br>• **128**—The HTML plane overlays the video plane and content is equally visible on both planes.<br>• **255**—The video content plane is completely hidden and only the HTML content plane is visible.<br><br>**Note** **The HTML content plane might sometimes contain a graphic that is already partially transparent in its own right (so that, for example, its rounded edges look smooth against the background color).** This type of transparency pertains only to interaction between that graphic and other objects on the same plane. So, if you then change the Browser Transparency value to 255, for example, this does not mean you will be able to see the video plane through the partially transparent graphic on the HTML content plane. Instead, in this case, the video plane is still completely hidden, as expected. |

## UI Reference: Elements to Specify Which URL TVzilla Should Load

*Table 12-3 Elements on the URL to be Displayed Page*

| Element | Description |
|---|---|
| **URL To Be Displayed** | |
| URL | The HTTP URL that loads a web page (or other content) on the HTML content plane. The URL cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding. |

### Related Topics

- Specify Which URL to Load in TVZilla, page 12-6

CHAPTER 13

# Configure Video and Audio Settings

**Revised: May 4, 2015**



# Concepts



## Performance Factors



### Understand Jitter

Differing amounts of transmission delay might affect any two packets in a multicast stream. *Jitter* compares the transmission delays for two packets and measures the scope of difference between them.

### Understand the Jitter Buffer

Each DMP reserves 5 MB in its RAM to buffer incoming packets from multicast streams. This method is meant to reduce the risk of jitter during playback. The *jitter buffer* capacity of DMPs is sufficient to store from an MPEG-2 transport stream:

- 8 seconds of SD video, encoded to 5 Mbps
- 2.2 seconds of HD video, encoded to 18 Mbps

## Understand Presentation Time Stamp (PTS) Values

Some of the metadata inside MPEG-2 files and streams is meant to ensure that:

- Video and audio data are synchronized correctly during playback.
- Playback occurs at the correct speed.

The metadata element that controls these behaviors is called the *presentation time stamp*, or PTS. The original encoding of an MPEG-2 file automatically adds PTS metadata values to it. These values state when a video or audio frame must be presented to the client system, relative to the timing of nearby frames. So, in a typical MPEG-2 transport stream:

- Each video frame travels with one PTS value that describes it uniquely.
- Several audio frames travel together with one PTS value that describes them collectively.

## Understand System Time Clock (STC) Values

When your DMP receives an MPEG-2 transport stream, it inspects the packets to find and make use of PTS values within them. The first time that your DMP finds a PTS value in a transport stream, it generates a *system time clock* (STC) value for its own use. Then, multiple events occur in tandem.

- Approximately 24 milliseconds after your DMP recognizes that the multicast stream has delivered a PTS value, its generated STC value triggers playback of the corresponding video and audio data. This brief delay contributes to proper playback of the stream.
- Your DMP considers the video frame rate and other factors to make programatic assumptions about what the second PTS value will say and when it should arrive. Based on these assumptions, it generates a second STC value. Your DMP repeats this process each subsequent time that it finds a PTS value. It only ever discards a generated STC value when it learns that one of its assumptions was wrong.

## Understand Why PTS-STC Discrepencies Flood the Buffer and Cause Latency

If anything delays a PTS value from arriving when the corresponding STC value anticipates that it should arrive, the visible result is latency during playback. This occurs because the jitter buffer must hold more data than it is intended to hold.

Many factors might affect how “late” a PTS value can be, including network congestion, CPU load on the DMP, and how the originating encoder is configured. For example, how does the encoder interleave audio with video, and does it use B frames?

The arrival time for any PTS value can never be guaranteed, even in the best networks.

# Guidelines

- Limit and Reduce Latency, page 13-2

## Limit and Reduce Latency

You can reduce the risk of latency and limit its effects. Simply configure the originating encoder to:

- Use I frames and P frames only. It **should not** use B frames.
- Minimize the interleave time for audio and video.

# Workflows



## Workflow to Play Assets from the Memory Card

Complete this sequence of procedures to upload supported assets to the SD card in your DMP, and then play them.

1. Enable FTP and SFTP access.
   *See Enable or Disable Types of Access to Your DMP, page 8-6.*
2. Configure login credentials for the FTP and SFTP user accounts.
   *See Manage and Edit Passwords, page 8-5.*
3. Upload assets to the **/tmp/ftproot/usb_1** subdirectory on your DMP.
4. Play the media that you uploaded.
   *See Watch or Stop Video from a File Stored on Your DMP, page 13-6.*

# Procedures



# Configure Settings



## Adjust Jitter Buffer Control (Advanced Multicast) Settings

**Note** DMPs do not support multicast streaming over Wi-Fi.

You can control how your DMP synchronizes audio with video in a multicast stream.

**Procedure**

**Step 1** Depending on your DMP model and its firmware version, do one of the following.

- Click **Advanced Multicast** in the Settings list.
- Click **Video** in the Settings list.

**Step 2** Enter or edit required values in the Multicast Jitter Buffer Control area, and then click **Apply**.

**Step 3** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define Jitter Buffer (Advanced Multicast) Settings, page 13-8

## Turn Full-Screen Video Mode On or Off

### Procedure

**Step 1** Click Video to fill the screen on your DMP display with *only* the video content plane.

The HTML content plane is hidden.

**Step 2** Stop. You have completed this procedure.

### Related Topics

- Watch or Stop Video from a UDP Multicast Stream, page 13-5.
- Watch or Stop Video from an HTTP URL, page 13-5.
- Watch or Stop Video from a File Stored on Your DMP, page 13-6.

# Play Media

- Play Assets from a USB Flash Drive, page 13-4
- Watch or Stop Video from a UDP Multicast Stream, page 13-5
- Watch or Stop Video from an HTTP URL, page 13-5
- Watch or Stop Video from a File Stored on Your DMP, page 13-6

## Play Assets from a USB Flash Drive

You can save supported media files to a USB flash drive, attach that drive to your DMP, and then show the files on the attached DMP display.

### Procedure

**Step 1** Move copies of the relevant media files from their source device to the root level of the USB flash drive that you will use.

**Step 2** Unmount the USB flash drive from the source device, and then attach it to your DMP.

**Step 3** Play the media files.

**Step 4** Stop. You have completed this procedure

### Related Topics

- Watch or Stop Video from a File Stored on Your DMP, page 13-6

## Watch or Stop Video from a UDP Multicast Stream

You can start or stop playback of video from a UDP multicast stream.

### Procedure

**Step 1** Click **Video Multicast** in the Display Actions list.

**Note** **DMPs do not support multicast streaming over Wi-Fi.**

**Step 2** Enter or edit the required values.

**Step 3** Do one of the following.

- Click **Start** to play the stream.
- Click **Stop** to exit the stream.

**Step 4** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define Video Multicast Settings, page 13-6

## Watch or Stop Video from an HTTP URL

To show on your DMP display the video content from an HTTP URL, or to stop showing that video content, do the following.

### Procedure

**Step 1** Click **Video URL** in the Display Actions list.

**Step 2** Enter or edit the required values.

**Step 3** Do one of the following.

- Click **Start** to play the video.
- Click **Stop** to exit the video.

There might be a delay of as long as 3 seconds.

**Step 4** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Define Video URLs, page 13-7

## Watch or Stop Video from a File Stored on Your DMP

You can start or stop playback of video from DMP local storage. The storage volume might be the internal SD card or an external USB flash drive or USB hard drive that is mounted.

### Procedure

**Step 1** Click **Play Video File Stored Locally** in the Display Actions list.

**Step 2** Enter or edit the required values.

**Step 3** Do one of the following.

- Click **Start** to play the video.
- Click **Stop** to exit the video.

**Step 4** Stop. You have completed this procedure.

### Related Topics

- UI Reference: Elements to Play Locally Stored Video, page 13-7

# Reference



# UI Reference Topics



## UI Reference: Elements to Define Video Multicast Settings

*Table 13-1 Elements on the Video Multicast Page*

| Element | Description |
|---|---|
| **Video Multicast** | |
| Multicast Group IP Address | The DNS-routable IP address:<br>• To which the encoder or streaming server must send content.<br>• From which all client systems will receive the UDP multicast stream.<br>**Note DMPs do not support multicast streaming over Wi-Fi.** |
| Port Number | The logical port on your DMP that receives the stream. |

### Related Topics

- Watch or Stop Video from a UDP Multicast Stream, page 13-5

## UI Reference: Elements to Define Video URLs

*Table 13-2 Elements on the Video URL Page*

| Element | Description |
|---|---|
| **Video URL** | |
| URL | Use ISO/IEC-8859 (Latin-1) character encoding to specify the HTTP URL. This includes:<br>• The server's routable IP address or DNS-resolvable hostname.<br>• The full pathname, which points exactly to the video file on the server.<br>**Note** **The entire URL must contain fewer than 254 characters. It must not contain any spaces.**<br>**Tip** **When the HTTP service runs on a nonstandard logical port, use the typical method (`:8080`, for example) to include a port number in the URL.** |

## UI Reference: Elements to Play Locally Stored Video

*Table 13-3 Elements on the Play Video File Stored Locally Page*

| Element | Description |
|---|---|
| **Play Video File Stored Locally** | |
| Local Storage Path | The local path to the video file.<br>• *Did you store the asset on the Secure Digital (SD) flash drive inside your DMP?* Start the pathname with **/tmp/ftproot/usb_1/**.<br>• *Did you store the asset on an external USB drive that is attached to your DMP?* Start the pathname with **/tmp/ftproot/usb_2/**. |

### Related Topics

- Watch or Stop Video from a File Stored on Your DMP, page 13-6

# UI Reference: Elements to Define Jitter Buffer (Advanced Multicast) Settings

*Table 13-4 Elements on the Advanced Multicast Page*

| Element | Description |
|---|---|
| **When the DMPDM navigation path on your DMP is Settings > Advanced Multicast** | |
| Enable Automatic STC Adjustment | Indicates whether STC adjustment is automated. |
| Jitter Drifting | Indicates the rate of drift, as measured in 50-millisecond increments. Choose an option from the list. Options range incrementally from exactly **50 ms** to exactly **1500 ms**, after which the one additional option is **> 1500 ms**. The factory-default value is 1500 ms.<br>50 ms is the best possible condition. |
| Multicast Pre-buffer Time (0-2200) | Counts in milliseconds how long the pre-buffer should endure, per PTS. Enter 0 (zero) to use no pre-buffer. |
| **When the DMPDM navigation path on your DMP is Settings > Video** | |
| Low Mark of (PTS-STC) (ms) | Media playback duration (in milliseconds) that specifies the smallest permissible buffer size. This value and the High Mark value define the low and high thresholds, respectively, for your DMP's jitter buffer. The actual buffer size might reach either extreme but is more likely to straddle a midpoint.<br>Except when nothing at all is buffered, this is the least amount of media that will buffer en route to its decoding. Buffer size is proportionate to latency, so a larger buffer proportionately improves the capacity for jitter control.<br>Whenever your presentation system is one tile in a video wall—or feeds signals to other tiles via RS-232 daisy-chaining—this value should be within 100 ms of the High Mark value. Otherwise, the tiles in your video wall might fall out of sync. |
| High Mark of (PTS-STC) (ms) | Media playback duration (in milliseconds) that specifies the largest permissible buffer size. This value and the Low Mark value define the high and low thresholds, respectively, for your DMP's jitter buffer. The actual buffer size might reach either extreme but is more likely to straddle a midpoint.<br>The buffer will never hold any more media than this. Buffer size is proportionate to latency, so a larger buffer proportionately improves the capacity for jitter control.<br>Whenever your presentation system is one tile in a video wall—or feeds signals to other tiles via RS-232 daisy-chaining—this value should be within 100 ms of the Low Mark value. Otherwise, the tiles in your video wall might fall out of sync. |
| Time of Calculating Average (PTS-STC) (sec) | Interval (in seconds) that your DMP reserves to calculate the average size of its own jitter buffer and adjust the STC, as needed to alter the data size.<br>In most case, 60 seconds works well. |
| Statistics of (PTS-STC) | Click **Display** to view information about your DMP's jitter buffer. |