



Quick Start Guide for Cisco Digital Media Suite 5.4.x

Revised: September 17, 2011



Audience

We prepared this material with specific expectations of you.

✓ You are qualified to configure an enterprise server in your organization's datacenter.

This guide supports you during the first boot process and initial configuration of Cisco Digital Media Suite 5.4.x (Cisco DMS) component products. It contains the following sections.

- [Set Up and Configure Cisco Digital Media Manager, page 1](#)
- [Use DMM to Register and Configure Digital Media Players, page 5](#)
- [Learn More About..., page 8](#)

Set Up and Configure Cisco Digital Media Manager

Use the checklist in this section to set up a DMM 5.4 appliance and configure its software.

Before You Begin

- Obtain the IP address and subnet mask to assign to your DMM appliance.
- Obtain the IP addresses of the default network gateway, the primary DNS server, and the secondary DNS server.
- Ensure that a DNS entry has been created and published for the DMM appliance.
- Ensure that you have obtained the license keys to unlock the software features on your DMM appliance. For information about obtaining license keys, see the Licenses chapter of User Guide for Cisco Digital Media Manager 5.4.x on Cisco.com.

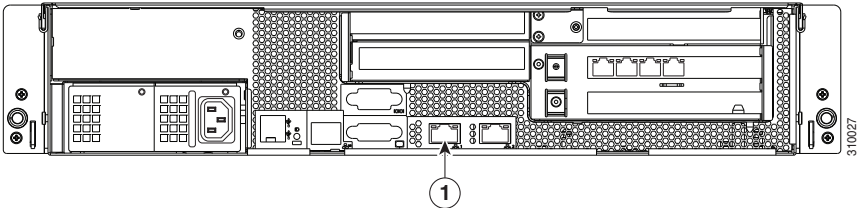


Americas Headquarters:





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

- Make sure you are running a supported browser, as described in our [release notes](#).
- Enable popup windows in your browser if they are disabled. You can complete the checklist only when popup windows are enabled.

Procedure

✓	Task	Steps
☐	1. Set up the server.	<p>a. Unpack the equipment from its container and verify that all components are present.</p> <p>b. Plug in the redundant power cords.</p> <p>c. Connect an Ethernet cable to you network and to the appliance. (The number 1 in this illustration indicates which physical interface on a DMM appliance should connect to your network.)</p>  <p>d. Connect a monitor to the VGA output on the back of the appliance.</p> <p>e. Connect a standard PS2 keyboard to the purple PS2 port on the back of the appliance.</p> <p>f. Power On the appliance.</p> <p>g. Press Enter at the “Start of First Boot” message.</p>
☐	2. Specify the fully qualified, DNS-resolvable hostname for your DMM appliance.	<p>For example, you might enter <code>server.example.com</code>.</p> <p>Note This field requires an FQDN. Do not enter an IP address.</p> <p>Then, choose OK.</p>
☐	3. Supply the required network information.	<p>a. As prompted, enter:</p> <ul style="list-style-type: none"> • The server IP address • The subnet mask • The default gateway IP address or DNS-resolvable hostname • The primary DNS server IP address or DNS-resolvable hostname • The secondary DNS server IP address or DNS-resolvable hostname <p>b. Then, choose OK.</p>
☐	4. Confirm that you entered the correct network settings.	<p><i>Are the settings correct?</i></p> <p>a. Choose Yes or No. Then, if you chose No, go back and correct any errors.</p>

✓	Task	Steps
<input type="checkbox"/>	5. Configure settings for the appliance network interface card (NIC).	<p><i>Should the NIC auto-negotiate the fastest possible transmission mode when it is connected to another device?</i></p> <ul style="list-style-type: none"> Choose Yes or No. Then, if you chose No: <ul style="list-style-type: none"> a. Choose the NIC speed and choose OK. b. Select the duplex method and choose OK. c. Choose Yes.
<input type="checkbox"/>	6. Set the time zone settings.	<ul style="list-style-type: none"> a. Use the Up/Down arrow keys to navigate through the Time Zone list. b. Stop when the correct time zone is displayed. Then, choose OK. <p><i>Are the settings correct?</i></p> <ul style="list-style-type: none"> c. Choose Yes or No. Then, if you chose No, go back and correct any errors.
<input type="checkbox"/>	7. Set the current month, year, and day.	<ul style="list-style-type: none"> a. Use the Tab key and the Up/Down arrow keys to navigate and change the selected values. b. When you are done, choose OK. <p><i>Are the settings correct?</i></p> <ul style="list-style-type: none"> c. Choose Yes or No. Then, if you chose No, go back and correct any errors.
<input type="checkbox"/>	8. Set the current hour, minute, and second.	<p>Use the 24 hour time format (24 hours that increment from 0100 to 2400).</p> <ul style="list-style-type: none"> a. Use the Tab key and the Up/Down arrow keys to navigate and change the selected values. b. When you are done, choose OK. <p><i>Are the settings correct?</i></p> <ul style="list-style-type: none"> c. Choose Yes or No. Then, if you chose No, go back and correct any errors.
<input type="checkbox"/>	9. Set the administrator password for <i>Appliance Administration Interface</i> (AAI), a command console for your DMM server.	<ul style="list-style-type: none"> a. Enter a password for the <i>admin</i> account. Then, choose OK. b. Re-enter the password. Then, choose OK twice. <p>Note This is the default account to use AAI. These are not the credentials to open DMM in your browser.</p> <p>Tip Your password must contain at least six characters. However, we recommend that you use at least eight characters, including numbers and a mixture of uppercase and lowercase letters from the Latin-1 character set.</p>

✓	Task	Steps
	10. Set the recovery password.	<p>a. Enter a password for the <i>pwadmin</i> account. Then, choose OK.</p> <p>b. Re-enter the password. Then, choose OK twice.</p> <p>Note DO NOT LOSE THE <i>pwadmin</i> PASSWORD. You cannot recover it if you do. This account is used to recover the admin and superuser account passwords and to run diagnostic tools when troubleshooting with Cisco technical support engineers.</p> <p>The appliance reboots.</p>
	11. Log in to Cisco DMM.	<p>Tip Use the server FQDN that you configured in Step 2.</p> <p>a. Go to <a href="https://<DMM_FQDN>:8443/">https://<DMM_FQDN>:8443/.</p> <p>b. Log in with these credentials:</p> <ul style="list-style-type: none"> Username: superuser Password: admin (This password is valid only once. You change it immediately.) <p>c. Click Accept to agree to the the End User License Agreement.</p>
	12. Configure the superuser account.	<p>a. Specify which carefully monitored email address should receive all DMM system notification messages and all “contact your administrator” messages from DMM users who cannot log in.</p> <p>b. Enter and confirm your NEW password for the superuser account.</p> <p>c. Click Save.</p> <p>The license installation page opens.</p>
	13. Install the license keys to activate your purchased Cisco DMS features.	<p>a. Click Browse.</p> <p>b. Find and choose the license file where you saved it.</p> <p>c. Click Open.</p> <p>d. Click Install License.</p> <p>The features and modules that you purchased are now enabled.</p>

Use DMM to Register and Configure Digital Media Players

DMM can discover your DMPs and add them to your device inventory for simplified, remote management. Such operations follow this sequence.

1. DMM identifies each device in the specified address range where TCP port 7777 is open.
2. DMM confirms which of these devices are DMPs.
3. DMPs receive information about your DMM server, and are then instructed to restart.
4. Restarted DMPs send their updated information to DMM and set their own status to “Up.”
5. DMM generates new database records for all DMPs that are newly autoregistered.
6. DMM assigns newly registered DMPs to any DMP groups that match the specified address range.
7. DMM assigns newly registered DMPs to the “All DMPs” group.



Tip



You can stop untrusted DMM appliances from seizing control of your DMPs. Simply configure your network firewall to restrict which devices can send inbound traffic to your DMPs over TCP port 7777.

When you autoregister DMPs that are new to your DMM appliance, they restart immediately even when they are known already to another DMM appliance, and even when they are running an event. Therefore, when your organization uses more than one DMM appliance, be careful to autoregister only those DMPs that you are not already managing centrally elsewhere. Otherwise, you might temporarily disrupt media playback for the signs in your network.

Before You Begin

- DMM-native (non-Medianet) DMP autoregistration uses NMAP. Verify that the routers, switches, and firewalls between your DMM appliance and the NMAP address range for non-Medianet autoregistration allow TCP port 7777 to send and receive packets. Verify also that ICMP (ping) traffic is allowed to pass from your DMM appliance to your DMPs on this port. When any of this traffic is blocked anywhere along its route, non-Medianet autoregistration cannot occur. (CSCtk02451)
- We recommend that you autoregister DMPs **after** normal business hours. Autoregistration of 5,000 DMPs takes approximately 4 minutes in a fast network and does not use polling.
- DMM runs any non-Medianet autoregistration job once each time that you schedule it to run. DMM does not scan the specified NMAP range continuously for DMPs that you might add in the future. Therefore, when you plan to add DMPs frequently, you should schedule a non-Medianet autoregistration event to recur accordingly.
- Make sure you are running a supported browser, as described in our [release notes](#).

Procedure (Continued)

	14. (As Needed) Log in to DMM again if you aren't still logged in.	<p>Tip Use the server FQDN that you configured in Task 2 and the superuser password that you configured in Task 12.</p> <ol style="list-style-type: none"> Go to <a href="https://<DMM_FQDN>:8443/">https://<DMM_FQDN>:8443/. Log in with these credentials: <ul style="list-style-type: none"> Username: superuser Password: <i><your_password></i>
	15. Discover the DMPs in your network.	<ol style="list-style-type: none"> Choose Network and Endpoints > Digital Media Players > Advanced Tasks. Click the DMP Discovery row in the Application Types list. Do one of the following. <ul style="list-style-type: none"> When you will define a new range for autoregistration <ol style="list-style-type: none"> Click Add New Application. Name and describe the deployable event that should use these settings. When you will edit a saved range for autoregistration <ol style="list-style-type: none"> Click the Applications list row whose settings should be edited. Click Edit Application. Set the necessary values. Then, click Submit to save your work. Choose Network and Endpoints > Digital Media Players > DMP Manager. Click Run Task, above the DMP List table. The Run Task dialog box opens. Choose the DMP Discovery application that you created. Click OK. <p>Note You can schedule multiple DMP autoregistration operations to run simultaneously only when they will all search the same one subnet. However, when you define DMP autoregistration operations to search more than one subnet, you must not schedule them to run simultaneously, or even to overlap. When they overlap, only the first of them can run at all. Furthermore, DMM does not show any error message to explain why the similar operations all failed. Therefore, you should plan to stagger the start times by at least 35 minutes apiece when you schedule DMP autoregistration tasks that will search multiple subnets. In a very large network that contains thousands of DMPs, the necessary interval might be longer than 35 minutes.</p>

16. Normalize the password for all of your DMPs.	<p>a. Choose Network and Endpoints > Digital Media Players > Advanced Tasks > System Tasks.</p> <p>b. Click Add New Application.</p> <p>c. Enter a name and description for the new task. Then, Choose Set from the Request Type list.</p> <p>d. Enter <code>init.WEB_password=new_password</code> in the Request field, where <code>new_password</code> should become the new Web User password for all of your DMPs.</p> <p>Tip Use proper syntax for URI encoding.</p> <p>Note Special characters, including exclamation points (!), question marks (?), ampersands (&), at signs (@), and asterisks (*) are forbidden in DMP passwords. All letters in a DMP password must be part of the ISO/IEC 8859-1 (Latin) character set. (CSCsq41233; CSCsw47873; CSCub67295)</p> <p>e. Click Submit to save the task and make it available for use.</p> <p>f. Choose Network and Endpoints > Digital Media Players > DMP Manager.</p> <p>g. Click All DMPs in the DMP Groups selector. Then, click Run Task. The Run Task dialog box opens.</p> <p>h. Click the “init.WEB_password” system task that you saved. Then, click OK.</p> <p>i. Choose Network and Endpoints > Settings > Server Settings.</p> <p>j. Enter the required values.</p> <ul style="list-style-type: none"> • Servlet Server Address—If you have not already done so, enter the DNS-resolvable hostname and domain for the appliance that is serving <i>Cisco Digital Signs</i>, such as dmm.example.com. • DMP User Name—Enter admin. • DMP User Password—Enter the new DMP Web Account password. <p>k. Click Save.</p>
--	--

Learn More About...

To Learn About	Go To
Cisco Digital Media Suite	
Cisco DMS products and technologies	http://cisco.com/go/dms
Cisco DMS technical documentation	http://cisco.com/go/dms/docroadmap
Cisco DMS APIs and SDK	http://developer.cisco.com/web/dms
Cisco DMS SNMP MIB	http://cisco.com/go/dms/mib
Cisco Connected Sports	
Cisco StadiumVision	http://cisco.com/go/stadiumvision
Cisco	
Service contracts	http://cisco.com/go/csc
Standard warranties	http://cisco.com/go/warranty ¹
Technical support	http://cisco.com/go/support
Technical documentation	http://cisco.com/go/techdocs
Product security	http://cisco.com/go/psirt
Sales	http://cisco.com/go/ordering

Obtain Documentation or Submit a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2002–2012 Cisco Systems, Inc. All rights reserved.