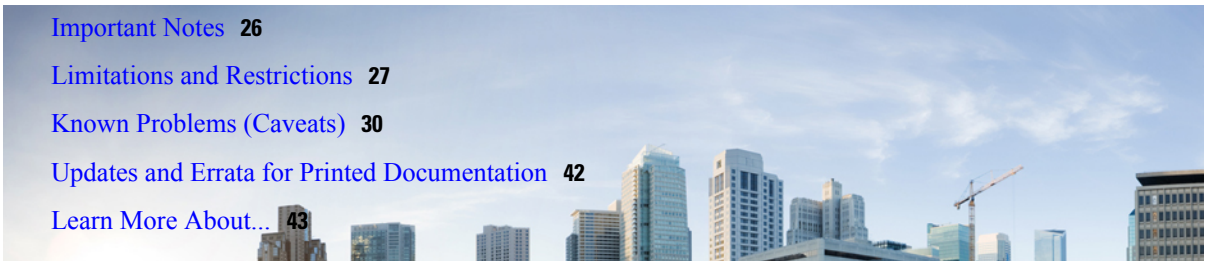
Release Notes for Cisco Digital Media Suite 5.3.x



Revised: March 29, 2017,

Release Notes for Cisco Digital Media Suite 5.3.x

This document describes new and changed features, requirements, and known problems for Cisco Digital Media Suite (DMS) 5.3.x products.

Note Cisco DMS releases 5.3.1, 5.3.2, and 5.3.3 are not generally available.

The only generally available releases are 5.3.0, 5.3.4, 5.3.5, and 5.3.6, which are also the only releases that this document describes in any detail.

CRITICAL HOTFIX AVAILABLE

CSCty22538 Communication can fail between Cisco Digital Media Manager (DMM) and its inventory of Cisco Digital Media Players (DMPs). In an affected deployment, error messages indicate that digital certificate expiration is the root cause.

Model	**Certificate Expiration Date by DMP Firmware Release**									
	5.2	**5.2.1**	**5.2.2**	**5.2.2.1**	**5.2.2.3**	**5.2.3**	**5.2.3.2**	**5.3**	**5.3.4**	**5.3.5**
DMP 4305G	*2012-02-24*		N.A.	N.A.	**OK** *2037-12-18*	*2012-02-24*	N.A.	*2012-02-24*	N.A.	**OK** *2037-12-18*
DMP 4310G	N.A.	N.A.	*2012-02-24*			*2012-02-24*	*2021-10-18*	*2012-02-24*	*2021-10-18*	
DMP 4400G	*2012-02-24*	*2013-08-29*				*2013-08-29*	N.A.	*2013-08-29*		

HOTFIX	You can recover from these communication failures in 10 minutes or less by loading a hotfix on your DMM server. See http://cisco.com/web/software/282100271/56598/DMM-patch-CSCty22538-Readme.txt . • The hotfix also works around a related failure, in which DMP certificate expiration disrupts use of a DMM advanced task called "File Transfer to DMP" (**CSCty23792**). • The hotfix DOES NOT improve disrupted IP phone-based remote control of the Cisco Cast electronic program guide (**CSCty36771**). The hotfix is fragile. IF YOU DO NOT use the permanent solution described below, any future upgrade of your DMM server could cause it to lose contact again with your affected DMPs. In such cases, you must then REAPPLY the hotfix.
PERMANENT FIX	You can prevent these communication failures altogether by installing DMP firmware release 5.3.5, which resolves these known defects: **CSCty22538**, **CSCty23792**, and **CSCty36771**. **Note** To download this DMP firmware, you must have a valid service contract associated to your Cisco.com profile. If you do not have a service contract you can get one through your Cisco account team, your Cisco partner, or a qualified Cisco reseller. Then, once you have the service, you must associate it to your Cisco.com user ID at https://tools.cisco.com/RPF/profile/edit_entitlement.do?Tab=3. **1** Apply the hotfix to your DMM server, if you have not already done so. Otherwise, it cannot direct your DMPs to install their new firmware. **2** Obtain the new DMP firmware. **a** Log in to your Cisco.com account, and then go to http://cisco.com/cisco/software/navigator.html?mdfid=280936311&flowid=21001 . **b** Click your DMP model in the Cisco Digital Media Players list. **c** Click **Expand All** in the versions tree, and then click **5.3.5**. **d** Click **Download**. **3** Install the new DMP firmware, as described in your Cisco DMS upgrade guide at http://cisco.com/en/US/products/ps6681/prod_installation_guides_list.html .

Strategies to Overcome CSCty22538

If today...

(A) You Run DMM 5.2 on a 7835-H1 or 7835-H2 Appliance

You can choose between two supported workflows to overcome the effects of CSCty22538.

Caution Until you complete one of these workflows, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2

Workflow A1	Your DMM server can run the 5.2.2 release without any effects of CSCty22538.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.
3. Install firmware release 5.2.2.3 [1] on your DMPs.
4. Upgrade DMM (not DMPs) to 5.2.1[2] .
5. Upgrade DMM (not DMPs) to 5.2.2[3] .
6. Stop. You have completed this workflow.

Strategy to Run DMM 5.2.2.1

Workflow A2	Your DMM server can run the 5.2.2.1 release without any effects of CSCty22538.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.

1 To follow this link appropriately, you must be logged in to your Cisco.com account.
2 To follow this link appropriately, you must be logged in to your Cisco.com account.
3 To follow this link appropriately, you must be logged in to your Cisco.com account.

a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

b. The hotfix has taken effect if the Status column includes even one green checkmark.

3. Install firmware release 5.2.2.3 [4] on your DMPs.
4. Upgrade DMM (not DMPs) to 5.2.1[5] .
5. Upgrade DMM (not DMPs) to 5.2.2[6] .
6. Upgrade DMM (not DMPs) to 5.2.2.1.[7] [8]
7. Stop. You have completed this workflow.

(B) You Run DMM 5.2.1 on a 7835-H1 or 7835-H2 Appliance

You can choose between two supported workflows to overcome the effects of CSCty22538.

Caution Until you complete one of these workflows, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2

Workflow B1	**Your DMM server can run the 5.2.2 release without any effects of CSCty22538.**

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.
3. Install firmware release 5.2.2.3 [9] on your DMPs.
4. Upgrade DMM (not DMPs) to 5.2.1[10] .
5. Upgrade DMM (not DMPs) to 5.2.2[11] .
6. Stop. You have completed this workflow.

4 To follow this link appropriately, you must be logged in to your Cisco.com account.
5 To follow this link appropriately, you must be logged in to your Cisco.com account.
6 To follow this link appropriately, you must be logged in to your Cisco.com account.
7 The 5.2.2.1 release is available exclusively for H1 and H2 server models.
8 To follow this link appropriately, you must be logged in to your Cisco.com account.
9 To follow this link appropriately, you must be logged in to your Cisco.com account.
10 To follow this link appropriately, you must be logged in to your Cisco.com account.
11 To follow this link appropriately, you must be logged in to your Cisco.com account.

Strategy to Run DMM 5.2.2.1

Workflow B2	Your DMM server can run the 5.2.2.1 release without any effects of CSCty22538.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.
3. Install firmware release 5.2.2.3 [12] on your DMPs.
4. Upgrade DMM (not DMPs) to 5.2.1[13] .
5. Upgrade DMM (not DMPs) to 5.2.2[14] .
6. Upgrade DMM (not DMPs) to 5.2.2.1. [1516]
7. Stop. You have completed this workflow.

(C) You Run DMM 5.2.1 on a 7835-H3 Appliance

You can choose between two supported workflows to overcome the effects of CSCty22538.

Caution Until you complete one of these workflows, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2

Workflow C1	Your DMM server can run the 5.2.2 release without any effects of CSCty22538.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.

12 To follow this link appropriately, you must be logged in to your Cisco.com account.
13 To follow this link appropriately, you must be logged in to your Cisco.com account.
14 To follow this link appropriately, you must be logged in to your Cisco.com account.
15 To follow this link appropriately, you must be logged in to your Cisco.com account.
16 The 5.2.2.1 release is available exclusively for our 7835-H1 and 7835-H2 server models.

3 Install firmware release 5.2.2.3 [17] on your DMPs.

4 Upgrade DMM (not DMPs) to 5.2.2[18] .

5 Stop. You have completed this workflow.

Strategy to Run DMM 5.3

Workflow C2	Your DMM server can run the 5.3 release without any effects of CSCty22538.

1 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

2 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

3 Install firmware release 5.3.5 [19]on your DMPs.

4 Upgrade DMM (not DMPs) to 5.2.2 [20].

5 Upgrade DMM (not DMPs) to 5.2.3 [21].

6 Upgrade DMM (not DMPs) to 5.3 [22].

7 Stop. You have completed this workflow.

(D) You Run DMM 5.2.2 on a 7835-H1 or 7835-H2 Appliance

You can choose between two supported workflows to overcome the effects of CSCty22538.

Caution Until you complete one of these workflows, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2

Workflow D1	Your DMM server can run the 5.2.2 release without any effects of CSCty22538.

17 To follow this link appropriately, you must be logged in to your Cisco.com account.
18 To follow this link appropriately, you must be logged in to your Cisco.com account.
19 To follow this link appropriately, you must be logged in to your Cisco.com account.
20 To follow this link appropriately, you must be logged in to your Cisco.com account.
21 To follow this link appropriately, you must be logged in to your Cisco.com account.
22 To follow this link appropriately, you must be logged in to your Cisco.com account.

1 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

2 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

3 Install firmware release 5.2.2.3 [23] on your DMPs.

4 Uninstall the hotfix:

   a Insert the hotfix CD into your DMM appliance.

   b Log in at the console as admin.

   c In AAI, choose APPLIANCE_CONTROL > SOFTWARE_UPDATE > REMOVE_PATCH.

   d Press Enter and follow the prompts to continue.

5 Stop. You have completed this workflow.

Strategy to Run DMM 5.2.2.1

Workflow D2	Your DMM server can run the 5.2.2.1 release without any effects of CSCty22538.

1 Upgrade DMM (not DMPs) to 5.2.2.1.[24][25]

2 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

3 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

4 Install firmware release 5.2.2.3 [26] on your DMPs.

5 Uninstall the hotfix:

   a Insert the hotfix CD into your DMM appliance.

   b Log in at the console as admin.

   c In AAI, choose APPLIANCE_CONTROL > SOFTWARE_UPDATE > REMOVE_PATCH.

   d Press Enter and follow the prompts to continue.

6 Stop. You have completed this workflow.

---

23 To follow this link appropriately, you must be logged in to your Cisco.com account.

24 To follow this link appropriately, you must be logged in to your Cisco.com account.

25 The 5.2.2.1 release is available exclusively for our 7835-H1 and 7835-H2 server models.

26 To follow this link appropriately, you must be logged in to your Cisco.com account.

(E) You Run DMM 5.2.2 on a 7835-H3 or UCS210 Appliance

You can choose between two supported workflows to overcome the effects of CSCty22538.

Caution Until you complete one of these workflows, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2

Workflow E1	**Your DMM server can run the 5.2.2 release without any effects of CSCty22538.**

Note Unlike an MCS 7835-H3 appliance, a UCS210 appliance will not auto-eject the hotfix disc from its CD/DVD drive after you install or remove the hotfix. When you are not using the hotfix disc on a UCS server, remember to eject the disc manually.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.
3. Install firmware release 5.2.2.3 [27] on your DMPs.
4. Uninstall the hotfix:
   a. Insert the hotfix CD into your DMM appliance.
   b. Log in at the console as admin.
   c. In AAI, choose APPLIANCE_CONTROL > SOFTWARE_UPDATE > REMOVE_PATCH.
   d. Press Enter and follow the prompts to continue.
5. Stop. You have completed this workflow.

Strategy to Run DMM 5.3

Workflow E2	**Your DMM server can run the 5.3 release without any effects of CSCty22538.**

[27] To follow this link appropriately, you must be logged in to your Cisco.com account.

Note Unlike an MCS 7835-H3 appliance, a UCS210 appliance will not auto-eject the hotfix disc from its CD/DVD drive after you install or remove the hotfix. When you are not using the hotfix disc on a UCS server, remember to eject the disc manually

1 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

2 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

3 Install firmware release 5.3.5 [28] on your DMPs.

4 Upgrade DMM (not DMPs) to 5.2.3 [29].

5 Upgrade DMM (not DMPs) to 5.3 [30].

6 Stop. You have completed this workflow.

(F) You Run DMM 5.2.2.1 on a 7835-H1 or 7835-H2 Appliance

Only one supported workflow can help you to overcome the effects of CSCty22538.

Caution Until you complete this workflow, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.2.2.1

Workflow F1	Your DMM server can run the 5.2.2.1 release without any effects of CSCty22538.

1 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

2 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

3 Install firmware release 5.2.2.3 [31] on your DMPs.

4 Uninstall the hotfix:

28 To follow this link appropriately, you must be logged in to your Cisco.com account.
29 To follow this link appropriately, you must be logged in to your Cisco.com account.
30 To follow this link appropriately, you must be logged in to your Cisco.com account.
31 To follow this link appropriately, you must be logged in to your Cisco.com account.

a. Insert the hotfix CD into your DMM appliance.

b. Log in at the console as admin.

c. In AAI, choose APPLIANCE_CONTROL > SOFTWARE_UPDATE > REMOVE_PATCH.

d. Press Enter and follow the prompts to continue.

5. Stop. You have completed this workflow.

(G) You Run DMM 5.2.3 on a 7835-H3 or UCS210 Appliance

Only one supported workflow can help you to overcome the effects of CSCty22538.

Caution Until you complete this workflow, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.3

Workflow G1	**Your DMM server can run the 5.3 release without any effects of CSCty22538.**

Note Unlike an MCS 7835-H3 appliance, a UCS210 appliance will not auto-eject the hotfix disc from its CD/DVD drive after you install or remove the hotfix. When you are not using the hotfix disc on a UCS server, remember to eject the disc manually.

1. If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.
2. Make sure that the hotfix is working correctly in DMM.
   a. Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.
   b. The hotfix has taken effect if the Status column includes even one green checkmark.
3. Install firmware release 5.3.5 [32] on your DMPs.
4. Upgrade DMM (not DMPs) to 5.3 [33].
5. Stop. You have completed this workflow.

(H) You Run DMM 5.3 on a 7835-H3 or UCS210 Appliance

Only one supported workflow can help you to overcome the effects of CSCty22538.

32 To follow this link appropriately, you must be logged in to your Cisco.com account.

33 To follow this link appropriately, you must be logged in to your Cisco.com account.

Caution Until you complete this workflow, CSCty22538 retains the potential to disrupt Cisco DMS in your network.

Strategy to Run DMM 5.3

Workflow H1	Your DMM server can run the 5.3 release without any effects of CSCty22538.

Note Unlike an MCS 7835-H3 appliance, a UCS210 appliance will not auto-eject the hotfix disc from its CD/DVD drive after you install or remove the hotfix. When you are not using the hotfix disc on a UCS server, remember to eject the disc manually.

1 If you have not done so already, install the CRITICAL HOTFIX AVAILABLE, on page 4.

2 Make sure that the hotfix is working correctly in DMM.

   a Choose **Digital Signs > Digital Media Players > DMP Manager**, and then click **ALL DMPs** in the DMP Groups tree.

   b The hotfix has taken effect if the Status column includes even one green checkmark.

3 Install firmware release 5.3.5 [34] on your DMPs.

4 Uninstall the hotfix:

   a Insert the hotfix CD into your DMM appliance.

   b Log in at the console as admin.

   c In AAI, choose APPLIANCE_CONTROL > SOFTWARE_UPDATE > REMOVE_PATCH.

   d Press Enter and follow the prompts to continue.

5 Stop. You have completed this workflow.

Patch to Fix CSCtz28796

The **DMM_CSCtz28796.iso** utility can help to prevent unexpected DMM server shutdowns on an MCS 7835-H3 appliance whose serial number is earlier than (lower than) *xxx***947***xxx* . We describe CSCtz28796 in Cisco Bug Tool at http://tools.cisco.com/squish/c132d .

You can download **DMM_CSCtz28796.iso** at http://tools.cisco.com/squish/53D5f . Please see its README file at: http://cisco.com/web/software/282100271/56598/DMM_CSCtz28796_Readme.txt .

[34] To follow this link appropriately, you must be logged in to your Cisco.com account.

Note Do not use this patch on any DMM server chassis except MCS 7835-H3 appliances.

Patch to Fix CSCur03217 (Shellshock Vulnerability)

This is a generic patch for all DMM release 5.3.x versions to fix the Shellshock vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the Shellshock patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCur38536 (DMM SSL V3 POODLE Issue)

This is a generic patch for all DMM release 5.3.x versions to fix the SSL Poodle vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the SSL Poodle patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCus69527 (GHOST Vulnerability)

This is a generic patch for all DMM release 5.3.x versions to fix the GHOST Glibc vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the GHOST Glibc patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCut15831 (NTPd.org Vulnerability)

This is a generic patch for all DMM release 5.3.x versions to fix the NTPd.org vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the NTPd.org patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCut45957 (March 2015 OpenSSL Vulnerabilities)

This is a generic patch for DMM release 5.3.x versions to fix the March 2015 OpenSSL vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the March 2015 OpenSSL patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCuu96437 (Leap Second Vulnerability)

This is a generic patch for DMM release 5.3.x versions to fix the Leap Second vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply this Leap Second fix patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCtl89028 and CSCue73197 (dmm53x_opensso_ldap.iso)

This is a generic patch for DMM release 5.3.x versions to fix the following defects:

- CSCtl89028—DMM sends multiple LDAP search requests when multiple bookmarks are used.
- CSCue73197—LDAP users cannot log in if the filter search base is base DN.

If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply this patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCuu82425 (June 2015 OpenSSL Vulnerability)

This is a generic patch for all DMM release 5.3.x versions to fix the June 2015 OpenSSL vulnerability. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply this patch.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCuz96384 (SHA2 CSR Creation Support) and CSCva05078 (RC4 Vulnerability)

This is a generic patch for all DMM release 5.3.x versions. If you are applying the patch from release 5.3.6 RB1 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the fix.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCur99074 (DMM Backup USB Issue)

This is a generic patch release for all DMM release 5.3.6 RBx versions to fix the DMM backup USB issue.

You are recommended to upgrade your DMM to release 5.3.6 RB2 and then apply the fix.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

Patch to Fix CSCuz92699 (June 2016 NTP Vulnerability)

This is a generic patch release for all DMM release 5.3.x versions to fix the June 2016 NTP vulnerability. If you are applying the patch from release 5.3.6 RB2 or before, the patch will no longer be present on the system if DMM is upgraded after the patch installation.

You are recommended to upgrade your DMM to release 5.3.6 RB3 and then apply the June 2016 NTP fix.

For more information on upgrading a standalone DMM, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-315185

For more information on upgrading a DMM with failover configuration, see the following URL:

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/5_x/5_3/dms/upgrade/guide/536UpgradeGuide.html#pgfId-335669

New and Changed Features

Cisco Digital Media Players

Cisco DMS 5.3.4 introduces the "**ciscocraft.memlimit_action**" MIB for your use in system tasks, advanced tasks, and API programming. This new MIB controls how your DMP 4310G responds when playback of a SWF asset depletes all memory.

Although the MIB supports any of the following values, **WE RECOMMEND THAT YOU USE 3 ONLY .**

0	Use the nonconfigurable algorithm from earlier releases, which determined programatically whether to reload or shut down the SWF.
1	Shut down the SWF.
2	Reload the SWF.
3	**Restart (reboot) the DMP.**

Cisco Show and Share

MXE 3500 Version 3.3 Support

Cisco Show and Share now supports the Cisco Media Experience Engine 3500 version 3.3. Cisco MXE 3500 3.3 brings additional capabilities to Cisco Show and Share, such as the Pulse feature set, and support for additional video upload formats, including WebEx .arf files.

Multiple Video Resolution Support

Administrators can configure Cisco Show and Share to transcode uploaded and recorded videos to 360p, 480p, or 720p resolutions.

Viewers can then select a playback quality that fits with their available bandwidth. Viewers on slower connections can select a lower resolution to avoid choppy video playback.

This feature requires that a Cisco MXE 3500 is associated with Cisco Show and Share and that transcoding is enabled. The Cisco MXE must be running version 3.3 software or version 3.2 software with the updated transcoding profiles applied.

Mobile Client Application Support

Cisco Show and Share 5.3 supports access through a mobile application. Administrators can enable or disable mobile application access. Viewers can download the mobile application to a supported iOS device and view, rate, comment, and upload videos to Cisco Show and Share.

Mobile application access requires that a Cisco MXE 3500 running 3.3 software is associated with Cisco Show and Share.

Note The Cisco Show and Share mobile client application is beta and is suitable for early pilots and trials. We do not recommend an enterprise production deployment at this time. The mobile technology space is evolving quickly with new devices and software versions, so the beta application is subject to change.

Pulse Keyword and Speaker Identification

Administrators can enable the Pulse feature set for Cisco Show and Share. The Pulse feature set includes speaker and spoken word identification in videos uploaded or recorded in Cisco Show and Share. When enabled, a new tab, called Pulse, appears on the video playback window.

Viewers can use the Pulse features to search for videos, filter video lists. or navigate to specific speakers or keywords within a video.

The Pulse features require that a Cisco MXE 3500 running version 3.3 software is associated with Cisco Show and Share.

Quicktime Plugin Download Control

Cisco Show and Share uses the Quicktime browser plugin to play live event videos. By default, if the plugin is not present on the client browser, Cisco Show and Share automatically attempts to download it from the Internet. Administrators can now disable the automatic download of the Quicktime plugin.

Acceptable Use Link Customization

Administrators can change the target for the Warranty and End User License Agreement link at the bottom of the Cisco Show and Share page to point to their company acceptable use agreement.

System-Wide Settings Screen Redesign

The System-Wide Settings screen has been redesigned to make it easier to maintain and configure features.

New Supported Languages

You can now display the interface in German, Portuguese-Brazil, and Italian.

Note The Italian language option is provided as a Beta feature. You may experience some inconsistencies in the interface if you choose this language.

WebEx Recording Upload Support

If your system has an integrated Cisco MXE 3500 running version 3.3 software, you can upload WebEx .arf files for transcoding.

Recorded Video Transcoding Support

If your system has an integrated Cisco MXE running version 3.3 software and a valid Pulse license, and your system administrator has enabled the Pulse feature set, videos recorded directly in the Cisco Show and Share are transcoded, which enables the Pulse features and the multiple resolution support for them. The Pulse-enabled transcoding is required for display of recorded Show and Share video on mobile devices.

Cisco Digital Media Manager

Licensing Enhancement

A new page has been added to make it easier to request activation licenses for features of Cisco DMS.

Expanded IdP Support

Federation Mode for Cisco DMS now supports your use of PingFederate as an identity provider (IdP) for single sign on (SSO).

Feature Support and Device Compatibility

Cisco Digital Media Suite Components

See *Specifications, Supported Features, and Compatibility Information for Cisco Digital Media Suite* on Cisco.com to learn about the feature support and compatibility of Cisco DMS components across releases.

http://www.cisco.com/c/en/us/td/docs/video/digital_media_systems/dmscompat3.html

Cisco Show and Share

Cisco Digital Media Manager release 5.3.0 is compatible only with Cisco Show and Share Release 5.3.7.

Cisco Digital Media Manager release 5.3.6-RB1 and future releases are NOT compatible with Cisco Show and Share Release 5.3.7.

Cisco TelePresence Content Server

This table lists compatible Content Server and Cisco Show and Share versions.

Software version	Show and Share 5.2.1[35]	Show and Share 5.2.2	Show and Share 5.2.3	Show and Share 5.3
Content Server 5.0	Y	Y	N	N
Content Server 5.1	Y	Y	Y	N
Content Server 5.2	N	N	Y	Y
Content Server 5.3	N	N	Y	Y

35 Content Server recordings with Joined and stacked layouts will not be scaled correctly in the Show and Share Release 5.2.1 media player.

Client System Requirements

Cisco DMS Component Software	Operating System	Browser[36]				
		MSIE	Chrome	Firefox	Safari	Opera
Show and Share	**Microsoft Windows**	• **7**.*x* • **8**.*x* • **9** .*x*[37]	Not Supported	• **3.6**.*x* • **4**.*x*	Not Supported	Not Supported
Digital Signs						
Cast						
Digital Media Designer						
DMS-Admin						
DMPDM						
Show and Share	**AppleMac OS X**	*N.A.*	Not Supported	• **3.6**.*x* • **4**.*x*	• **5**.*x*	Not Supported
Digital Signs						
Cast						
Digital Media Designer						
DMS-Admin						
DMPDM						
Show and Share	**Linux**	*N.A.*	Not Supported	• **3.6.6**	Not Supported	Not Supported
Digital Signs						
Cast						
Digital Media Designer						
DMS-Admin						
DMPDM						

36 Alongside any supported browser, you must have Java Runtime Environment (JRE) 1.6.0 or later installed.

[37] Microsoft Internet Explorer 9. x is supported for Cisco Show and Share only. It is not compatible with Cisco Signs or Cisco Digital Media Manager.

Browser Proxy Support

- We support the use of browser proxies with DMPDM.
- We **DO NOT SUPPORT** the use of browser proxies with DMM.

Installation and Upgrade Notes

This section includes the following topics.

Software Release Availability and Entitlements

Note Cisco DMS releases 5.3.1, 5.3.2, and 5.3.3 are not generally available. The only generally available releases are **5.3.0, 5.3.4, 5.3.5,** and **5.3.6**, which are also the only releases that this document describes in any detail.

A maintenance release might apply to some Cisco DMS servers or endpoints, but not others. Also, the method to obtain software can vary by device or by release. Topics in this section specify which 5.3.x software releases are relevant to a given device and state how you might obtain such software for that device (**CSCtx12287**).

FOR YOUR REFERENCE

- To buy factory-new Cisco DMS equipment, on which major or minor release software is preinstalled, see http://cisco.com/go/ordering .
- To learn about Cisco service contracts, see http://cisco.com/go/cscc .
- To use a service contract entitlement, see http://tools.cisco.com/gct/Upgrade/jsp/productUpgrade.jsp .
- To use the Cisco Software Center, see one of the following.
  - **Digital Media Manager**

    http://cisco.com/cisco/software/type.html?mdfid=28071249&flowid=4306
  - **Digital Media Players**

    http://cisco.com/cisco/software/type.html?mdfid=280936311&flowid=4313
  - **Show and Share**

    http://cisco.com/cisco/software/type.html?mdfid=280171242&flowid=31002

Software Release Availability and Entitlements by Server Type

Available Software for Digital Media Manager Servers
This table compares the general availability of, and supported entitlements to obtain, software for Cisco DMM servers.

Table 1: DMM Server Software

Release No.	General Availability for DMM Servers	Method to Obtain		
		Factory-Installed	Contract Entitlement	Warranty Entitlement
5.3	Y	Y[38]	Y[39]	N
5.3.1	N	N	N	N
5.3.2	N	N	N	N
5.3.3	N	N	N	N
5.3.4	N	N	N	N
5.3.5	N	N	N	N
5.3.6	Y	N	Y	Y

38 Preinstalled software on factory-new equipment

39 Free with a valid service contract. Terms and conditions may vary.

Available Software for Show and Share Servers

This table compares the general availability of, and supported entitlements to obtain, software for Cisco Show and Share servers.

Table 2: Show and Share Server Software

Release No.	General Availability for DMM Servers	Method to Obtain		
		Factory-Installed	Contract Entitlement	Warranty Entitlement
5.3	Y	Y[40]	Y[41]	N
5.3.1	N	N	N	N
5.3.2	N	N	N	N
5.3.3	N	N	N	N
5.3.4	N	N	N	N
5.3.5	N	N	N	N
5.3.6	N	N	N	N
5.3.7	Y	N	Y	Y

40 Preinstalled software on factory-new equipment
41 Free with a valid service contract. Terms and conditions may vary.

Software Release Availability and Entitlements by Endpoint Type

Available Software for DMP 4400G Endpoints
This table compares the general availability of, and supported entitlements to obtain, software for Cisco DMP 4400G endpoints.

Table 3: Cisco DMP 4400G Endpoint Software

Release No.	**General Availability for DMM Servers**	**Method to Obtain**		
		Factory-Installed	Contract Entitlement	Warranty Entitlement
5.3	Y	Y[42]	Y[43]	N
5.3.1	N	N	N	N
5.3.2	N	N	N	N
5.3.3	N	N	N	N
5.3.4	Y	N	Y	Y[44]
5.3.5	Y	N	Y	Y
5.3.6	Y	N	Y	Y

42 Preinstalled software on factory-new equipment
43 Free with a valid service contract. Terms and conditions may vary.
44 Free Cisco Software Center download under the warranty conditions of a prior, qualifying purchase. Terms and conditions may vary.

Available Software for DMP 4310G Endpoints
This table compares the general availability of, and supported entitlements to obtain, software for Cisco DMP 4310G endpoints.

Table 4: Cisco DMP 4310G Endpoint Software

Release No.	**General Availability for DMM Servers**	**Method to Obtain**		
		Factory-Installed	Contract Entitlement	Warranty Entitlement
5.3	Y	Y[45]	Y[46]	Y[47]
5.3.1	N	N	N	N
5.3.2	N	N	N	N
5.3.3	N	N	N	N

5.3.4	Y	N	Y	Y
5.3.5	Y	N	Y	Y
5.3.6	Y	N	Y	Y

45 Preinstalled software on factory-new equipment
46 Free with a valid service contract. Terms and conditions may vary.
47 Free Cisco Software Center download under the warranty conditions of a prior, qualifying purchase. Terms and conditions may vary.

Available Software for DMP 4305G Endpoints
This table compares the general availability of, and supported entitlements to obtain, software for Cisco DMP 4305G endpoints.

Table 5: Cisco DMP 4305G Endpoint Software

Release No.	**General Availability for DMM Servers**	**Method to Obtain**		
		Factory-Installed	Contract Entitlement	Warranty Entitlement
5.3	Y	Y[48]	Y[49]	N
5.3.1	N	N	N	N
5.3.2	N	N	N	N
5.3.3	N	N	N	N
5.3.4	N	N	N	N
5.3.5	Y	N	Y	Y[50]
5.3.6	N	N	N	N

48 Preinstalled software on factory-new equipment
49 Free with a valid service contract. Terms and conditions may vary.
50 Free Cisco Software Center download under the warranty conditions of a prior, qualifying purchase. Terms and conditions may vary.

Installation Notes

- **Cisco DMS appliances require a DNS server to work correctly.** Enter fully-qualified domain names (FQDNs) and not IP addresses during setup in AAI. Otherwise, Cisco DMS cannot operate as designed and most of its functions will fail.
- Do not append a trailing dot to any FQDN during setup.
- To maintain network security, your DMM appliances and Show and Share appliances use digital certificates to communicate. These certificates use the DNS-resolvable hostname to identify each appliance uniquely. Therefore, you must enter the DNS-resolvable hostname for each appliance during setup when prompted to enter the fully-qualified domain name (FQDN) in AAI.

- You must also configure each of your DMS appliances in AAI to point correctly to the DNS server for your network and configure that DNS server to associate the IP addresses that your DMS appliances use with the FQDNs that their digital certificates use.

Upgrade Notes

For instructions on how to upgrade your Cisco Digital Media Suite, see Upgrade Guide for Cisco Digital Media Suite Release 5.3 on Cisco.com.

- **When you have a valid SAS contract** for an earlier Cisco DMS release, which entitles you to upgrade at no additional cost, use the Product Upgrade Tool at http://cisco.com/upgrade . Enter your SAS contract number and place an order for the upgrade.
- **When you do not have a valid SAS contract** for an earlier Cisco DMS release, you must order this upgrade. For information about ordering, see the data sheet at: http://cisco.com/en/US/products/ps6682/products_data_sheets_list.html .
- **When you upgrade a failover configuration**, you must revert the configuration to standalone, upgrade both pairs, and then re-configure failover. See the failover guide on Cisco.com for information about converting your configuration to standalone mode and configuring failover after the upgrade. http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dms/failover_guide/dmsfailover.html .
- **When you use Federation Mode (single sign-on) authentication** in Cisco DMS 5.2.3, you must reimport SP metadata into IDP server after you upgrade DMM from 5.2.3 to 5.3. For information about how to export the SP metadata, see the "Configure SSO Services" section of the Authentication and Federated Identity chapter in User Guide for Cisco Digital Media Manager 5.3.x on Cisco.com: http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dmm/user/guide/admin/auth.html .

Important Notes

This section includes the following topics:

DMP 4310G Notice Regarding Power over Ethernet (PoE)

Starting in 2009, a handful of Cisco StadiumVision customers who participated in a special program to receive DMP 4310G endpoints received pre-release hardware. During this 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 a 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 the 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, 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.

Low Memory Causes DMPs to Restart Automatically

Rather than crashing when they run low on memory, DMPs are designed to restart automatically, which clears their memory and causes downtime of less than 1 minute, as opposed to the lengthy downtime that a hard crash would cause. In the rare cases when DMPs do run out of memory and restart automatically, SWF files are almost always responsible. The known scenarios when this can occur are as follows.

- The file size is greater than 500KB for your SWF file. Larger SWF files do work correctly in most cases, but we recommend as a best practice that you should always strive to use the smallest possible SWF files. Smaller files are far less likely to be burdensome to your DMPs.
- Your SWF file uses bitmapped image files outside itself that have a very large file size, either individually or collectively. Any bitmapped image files that you use in the production of a SWF file should be small files. If a bitmapped file has a large file size, it is important for you to understand that merely reducing the height and width of its placeholder on your canvas in Adobe Flash (or any similar authoring tool that you might use to develop a SWF file) will not reduce the actual file size.
- The web page that you are showing uses too many embedded SWF files.

Additional Recommendations

We recommend that you use the following guidelines when you create SWF files.

- The resolution of the SWF can be up to 1920x1080 when animations that are contained within the SWF are small and are restricted to a 640x480 region.
- Avoid redraw of the whole screen in your Flash animation.
- Multiple movements distributed across a screen will burden a DMP more than movements that are concentrated in one relatively small area.
- The FLV recommended resolution should be 320x240.

Limitations and Restrictions

Review the following table before you begin working with Cisco DMS components. These are known limitations that have not been fixed. Read the "Important Notes" section on page 27 section for additional information.

Table 6: Limitations and Restrictions in Cisco DMS

Identifier	Description
Digital Media Player	

Identifier	Description
CSCtc85169	Creating a system task to turn on/off syslog service on DMP. **Workaround:** To turn the syslog service on, create a new system task with the request type of SET and the request init.syslog=on&mib.save=1&mng.reboot=1. To turn the syslog service off, create a new system task with the request type of SET and the request init.syslog=off&mib.save=1&mng.reboot=1.
CSCtc58337	PoP: need a system task to bulk configure syslog server IP on DMP. **Workaround:** Apply a system task to all DMPs that will be used for PoP with a request type of **SET** and the request [illegible]
CSCtc80177	swf performance in 4305 is slow in DMD playlist The swf file added as a playlist item in the DMD plays slowly on the 4305. The playback speed is noticeably slower than it was in DMD 5.1. This issue occurs under the following conditions: • Swfs in a media playlist • Deployed on the 4305 **Workaround:** If possible, add the swf item as a media object, and not as an item in the media playlist. With this, the swf file should play at a higher speed. However, you do lose the features of a playlist. This issue is much more noticeable on swf files with continuous animation. It is advisable to use swf files composed more of static images on the 4305. if possible, try to decrease the amount of animation used in swf files deployed on the 4305.
CSCtd65883	4400G Wifi lose connectivity if WLAN config DHCP required enabled **Workaround:** Clear the DHCP request option on the access point. This prevents the access point from requiring a DHCP ACK from the DMP client.
CSCsq62648	DMP 4305G restarts after 15 seconds when playing the emergency_animated template. **Workaround:** None. This template is designed for the DMP 4400G. We recommend that you do not play content on the DMP 4305G that is specific to the DMP 4400G.
CSCtg23880	DMP 4305 can not properly display MSN webpage. The image is stretched and it is cut off on the top and left. **Workaround:** None.

Identifier	Description
Cisco Digital Signs	
CSCso63214	When its resources are limited, a DMP 4305G endpoint resets without a splash screen and without illuminating the red LED that should be visible through the chassis front grille because of limited resources. **Workaround:** Upgrade to a DMP 4400G, which is more powerful and does not exhibit this behavior.
CSCso78514	Using the local file option to add a media asset that is larger than 2G causes the upload menu to remain open indefinitely. **Workaround:** None. This is a browser limitation. We recommend that you upload a file that is smaller than 2G and that you use an external server for large files.
CSCso83562	On the Play in Future tab, scheduling monthly and yearly recurring jobs during a leap year results in scheduling anomalies for jobs that occur during the month of February in subsequent months and years. **Workaround:** None.
CSCsw67738	After *Cisco DMS Content Distribution* (DMS-CD) adds or deletes files on an external USB drive that is attached to a DMP, the DMP might mount this drive as Read-Only or might not mount it at all. Content distribution to or from usb_2 sometimes corrupts the file system on drives from certain manufacturers. In our testing, we have seen this on Western Digital Passport drives 0.5 percent of the time and on Maxtor drives 70 percent of the time. We have removed Maxtor from our list of supported manufacturers. **Workaround:** Disconnect the USB drive from your DMP and reformat the USB drive to use FAT32 as its file system.
CSCsw89590	When you make selections in *Cisco Cast* to show an on-screen PIN that mobile phone users can use to authenticate their phones for emulation of the DMP remote control, the PIN might take as long as 2 minutes to appear on-screen. **Workaround:** Wait 2 minutes.

Identifier	Description
CSCtg92808	image sl/s Transition effect performance needs improvement for 4400. Slow and choppy transition effect performance. This issue occurs under the following conditions: • Using transition effects in a slideshow • Deployed on the 4400 **Workaround:** Use the "No effect" option for the slideshow effect.
CSCua92177	Certificate with PKCS#7SIGNED DATA header and footer value is not supported on DMM.

Known Problems (Caveats)

This section contains the following topics:

Caveats Resolved in Cisco Show and Share Release 5.3.7

Note **This software release applies only to the Cisco Show and Share appliance**.

For more information, see the *Release Notes for Cisco Show and Share Release 5.3.7* at this URL:
http://www.cisco.com/en/US/products/ps6682/prod_release_notes_list.html

Caveats Resolved in 5.3.6 RB3

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB3.

Note Before you upgrade to release 5.3.6 RB3, you need to upgrade to release 5.3.6 RB2 first if you are with a lower version, and then install the DMM backup USB issue patch (see the "Patch to Fix CSCur99074 (DMM Backup USB Issue)" section on page 15) prior to your upgrade to release 5.3.6 RB3. If the DMM backup USB issue patch is already installed, ignore this note and proceed with the upgrade.

Table 7: Resolved Caveats for Cisco DMS 5.3.6 RB3

Identifier	Description
CSCur74598	libxslt heap-based buffer overflow code execution vulnerability
CSCub34207	Privilege escalation using bzip2 integer overflow vulnerability

Identifier	Description
CSCus07367	Perl hashing routines remote Denial of Service vulnerability.
CSCus69527	DMM_GHOST_Patch.iso (Evaluation of glibc GHOST vulnerability - CVE-2015-0235)
CSCur74475	Multiple vulnerability on Libxml2 component
CSCut15831	DMM_RB1_NTP_Patch.iso (December 2014 - NTPd.org vulnerabilities)
CSCuu96437	LeapSecond (LEAP SECOND: Leap second update susceptibility)
CSCuu82425	openssl_june (Evaluation of dmm for OpenSSL June 2015)
CSCur03217	Cisco Digital Media manager- ShellShock Vulnerability
CSCuc73420	ISC BIND subsequent RDATA Query Processing Remote Denial of Service vulnerability
CSCur74291	ISC BIND DNSSEC Trust Anchors Remote Denial of Service vulnerability
CSCux34692	Evaluation of DMS for Java_December_2015
CSCuy07345	Evaluation of DMS for OpenSSL January 2016
CSCuz96384	DMM SHA2 CSR creation support
CSCuz44223	Evaluation of DMS for NTP_April_2016
CSCuz52441	Evaluation of DMS for OpenSSL May 2016
CSCva05078	DMM RC4 vulnerability
CSCva37503	Filter issue in DMM -> DMP Manager page on 5.3.6(RB2)

Caveats Resolved in 5.3.6 RB2_P3

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB2_P3.

Table 8: Resolved Caveats for Cisco DMS 5.3.6 RB2_P3

Identifier	Description
DMP4310	

Identifier	Description
CSCuv26173	Evaluation of DMP4310 for OpenSSL July 2015 vulnerability.
DMP4400	
CSCuv46148	Evaluation of DMP4400 for OpenSSL July 2015 vulnerability.

Caveats Resolved in 5.3.6 RB2_P2

The following table describes the caveats that were resolved in Cisco DMS 5.4.1 RB2_P2.

Table 9: Resolved Caveats for Cisco DMS 5.3.6 RB2_P2

Identifier	Description
DMP4310 and DMP4400	
CSCut46084	March 2015 OpenSSL vulnerabilities.

Caveats Resolved in 5.3.6 RB2_P1

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB2P1.

Table 10: Resolved Caveats for Cisco DMS 5.3.6 RB2P1

Identifier	Description
DMP4310 and DMP4400	
CSCur72619	DMP 4400 and 4310 affected by Poodle vulnerability.

Caveats Resolved in 5.3.6 RB2P

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB2P.

Table 11: Resolved Caveats for Cisco DMS 5.3.6 RB2P

Identifier	Description
DMP4310	
CSCur05628	Cisco Digital Media Players - ShellShock vulnerability.

Caveats Resolved in 5.3.6 RB2

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB2.

Table 12: Resolved Caveats for Cisco DMS 5.3.6 RB2

Identifier	Description
DMM	
CSCuh55350	DMM file system full or down due to OpenSSO debug logs.
CSCul42910	DMD presentation cannot display Arabic text appropriately on DMP.
CSCum53875	DMM eCDS integration failed due to Lisp Error when password contains @.
CSCup24174	Multiple vulnerabilities in OpenSSL - June 2014.
CSCue24310	Apache Tomcat security vulnerabilities 5.3.0.
CSCuo45435	Observed crafted URL error message for valid URL.
CSCuo78864	SnS Login failed. The requested URL for redirection is not allowed.
DMP4310	
CSCup92446	Multiple vulnerabilities in OpenSSL - June 2014.
DMP4400	
CSCty48753	DMP4400 cannot get an IP when on Wireless WPA2/PSK/AES.
CSCum80961	Incorrect error message posted for corrupted upgrade file.
CSCup92446	Multiple vulnerabilities in OpenSSL - June 2014.

Caveats Resolved in 5.3.6 RB1

The following table describes the caveats that were resolved in Cisco DMS 5.3.6 RB1.

Table 13: Resolved Caveats for Cisco DMS 5.3.6 RB1

Identifier	Description
CSCud60025	Multiple images can cause flash file to cause moving blocks.

Identifier	Description
CSCud65354	CAST fails to sync XMLTV file missing stop attribute in the programme tag.
CSCue29017	Syslog and debug logs fill up /var/log partition.
CSCty67516	Digital Signs Preview Fails when using VLC Plugin.
CSCue26214	Simultaneous Audio Advance Task & Playlists schedule cause blank screen.
CSCue88991	DMD playlist should validate the entered URL.
CSCub23849	DMM allows redirection to a custom website through URL crafting.
CSCui70438	When DMS-CD using CAST, VOD does not play from local storage on DMP-4400.
CSCua38320	DMM allows import from LDAP of user DN over 200 characters.
CSCud03326	Error saving a presentation in Cisco DMM.
CSCue85388	TestRoot is not Working. DMM reports "/" file system is Full.
CSCtn54063	Exceeding DMS Batch upload of 17gig causes DMS to become inaccessible.
CSCuc02299	DSM file transferred to DMP changes internal storage setting to read only.
CSCua21277	DMP 4305 and 4310 do not have Domain field.
CSCud12361	Multiple DMPs locked up (reboot needed) after packet loss.
CSCud63061	DMP randomly reboots while playing a video playlist.
CSCud49290	Hide/Show mouse cursor on touch screens.

Caveats Resolved in 5.3.6

The following table describes the caveats that were resolved in Cisco DMS 5.3.6.

Table 14: Resolved Caveats for Cisco DMS 5.3.6

Identifier	Description
CSCtx06064	In Some cases, deployment package take more than one try to finish
CSCtn66678	DMP-4400 5.2.2 lockup when playing slideshow
CSCts70805	No Proxy' don't block the request of SWF from playlist to HTTP proxy
CSCtx87063	WMV videos with PTS gap larger than 100ms stop abruptly on the DMP
CSCtx92355	Duplicate entry in logrotate configuration breaks log rotation
CSCtz01275	Large numbers of events in database causes timeout on alerts page
CSCts95061	DMS Crash DMP 4310, when launches video without extension
CSCts95659	DMP CIFS choppy video after upgrade from 5.2 to 5.2.2
CSCtt33038	DMPs not sending HTTP responses to reboot commands
CSCtt42832	Black border on 4310 full screen channel with CAST
CSCtu08481	Network connectivity needs to be checked before HA process starts
CSCtx98810	In rare situations, all auth config changes fail due to missing pwd file
CSCty72691	DMD text scrolling disabled after choosing “Save As”
CSCty77185	DMP not displaying accented characters in scrolling text box
CSCtz60684	LDAP bookmark update fails if over 500 entries with AD 2008
CSCua08311	DMP-4310G: DVI source automatically switches back to HDMI on LG TV
CSCua27942	DMS Signs Scheduled tasks for Play in Future event doesn’t STOP playing

Caveats Resolved in 5.3.5

The following table describes the caveats that were resolved in Cisco DMS 5.3.5.

Table 15: Resolved Caveats for Cisco DMS 5.3.5

Identifier	Description
CSCty22538	DMP certificate expired
CSCty23792	Advanced Task > File Transfer to DMP broken after DMP cert expires
CSCty36771	Cast IP Phone does not work after DMP certificate expires

Caveats Resolved in 5.3.4

The following table describes the caveats that were resolved in Cisco DMS 5.3.4.

Table 16: Resolved Caveats for Cisco DMS 5.3.4

Identifier	Description
Cisco Digital Media Player 4400G	
CSCtt33038	DMPs not sending HTTP responses to reboot commands
Cisco Digital Media Player 4310G	
CSCtw90991	Option to reboot DMP instead of restart SWF [51]
CSCtt33038	DMPs not sending HTTP responses to reboot commands
CSCtx32864	WMV does not have audio **Caution** You must restart your DMP after you install Cisco DMS 5.3.4. Until you do so, this problem remains.

51 Cisco DMS 5.3.4 introduces the " ciscocraft.memlimit_action " MIB for your use in system tasks, advanced tasks, and API programming. This new MIB controls how your DMP 4310G responds when playback of a SWF asset depletes all memory. Although the MIB supports any of the following values, WE RECOMMEND THAT YOU USE 3 ONLY. • 0 — Use the nonconfigurable algorithm from earlier releases, which determined programatically whether to reload or shut down the SWF. • 1 — Shut down the SWF. • 2 — Reload the SWF. • 3 — Restart (reboot) the DMP.

Caveats Resolved in 5.3

The following table describes the caveats that were resolved in Cisco DMS 5.3.

Table 17: Resolved Caveats for Cisco DMS 5.3

Identifier	Description
Digital Media Suite (Cisco DMS)	
CSCsq69897	SNMP walk operation to DMM does not traverse entire subtree

Identifier	Description
CSCti82190	In UCS210/200 when manually change NIC setting will show error msg
CSCtq30219	Cannot login in federation, LDAP modes after backup and restore
CSCtr54397	Login fails if LDAP admin password contains certain characters
CSCtr76298	LDAP users cannot login if admin DN has comma followed by space
Cisco Digital Signs	
CSCto84410	DMM becomes sluggish and freezes with 370+ presentation and 60+ playlists
CSCtg64423	Detail error report - start timestamps not matching with syslog
CSCtr55906	DMM Limited permissions profile can start EMERGENCY for all DMPs Groups
CSCts70278	DMP Manager group assignment not properly updated in Flash
Cisco Show and Share	
CSCtq13850	User shouldn't be prompted to install QuickTime for Show and Share if not needed
CSCtq86727	Unable to upload any videos do Show and Share after upgrade
CSCts26446	Save to VoD link incorrect if DME IP was changed

Open Caveats

The following table describes possible unexpected behavior by Cisco DMS components.

Table 18: Open Caveats for Cisco DMS 5.3

Identifier	Description
Cisco Digital Media Suite	

Identifier	Description
CSCtt08465	OpenAM fails authentication if IdP choose persistent NameID attribute In federation mode, user logs in to IdP but DMS issues a fatal error ("Although your credentials...") and fails the session. This occurs when: • DMS is in identity federation mode. • IdP is configured to issue persistent NameID attribute **Workaround:** Do the following: **1** Reconfigure IdP to issue transient NameID attribute. **2** If (1) is not possible, user can enter the same URL in DMS that required authentication; this time s/he is able to access DMS applications. **3** If (2) is not desirable, contact Cisco TAC to fix SP configuration to handle persistent attribute issued by IdP.
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCtx49797 CSCtx49797	AAI reports incorrectly that the server hardware model is unknown. **Workaround:** Find the model number printed on the server casing.
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCua38320 CSCua38320	The DMM has a limitation to 200 characters for the User DN field of users being imported from Active Directory via LDAP. This internal limitation is due to the size of user table in the DMM database. **Workaround:** None. (DMS 5.4 has resolved/removed this limitation)
Cisco Cast	

Identifier	Description
CSCtj48360	4310 Cast incorrectly highlight EPG if sub hour div and stay long on EPG A DMP 4310G does not always render yellow highlighting correctly in the electronic program guide (EPG) listings for Cisco Cast. As you navigate through EPG program listings, yellow highlights on screen should always indicate which listing is the current focus of your navigation. However, this highlighting can become offset from your true focus. Before the EPG reaches this state, all of the following must be true simultaneously. • A DMP 4310G controls the digital sign that shows your EPG. • Your EPG navigation focus reaches to the outermost edge of your navigable EPG -- whether top, bottom, left, or right. • You use an arrow button or other control that is not valid for your current focus. • The reason this control is not valid in this context is that it would move focus beyond the outermost edge. **Workaround:** To recover from this state, press any valid button. Alternatively, double-press the same arrow button or other control that you previously invoked in error. The yellow highlight is then restored to your true focus.
CSCtt42832	Black border on 4310 full screen channel with CAST On the DMP 4310, when selecting a channel from EPG a black border is seen and the stream does not fill the entire screen. Issue seen when selecting from “Program Guide”, “Live Channels” or “Video on demand”. It is not seen when creating a playlist with a multicast stream or on the 4400. **Workaround:** None.
Cisco Digital Signs	

Identifier	Description
CSCtg97013	Running a slide show on 4305 reboots after 6 hours A slideshow running on the 4305 reboots after 6-8 hours. The issues occur in the following conditions: • DMP 4305 • Images in slideshow • Video failover enabled **Workaround:** The reboot issue can be resolved by disabling the video failover option. This option has also been turned off by default on the DMP. Users can also use an image playlist with a preload time instead of an image slideshow. In typical use cases, video failover should not be required in presentations with image slide shows.
CSCth10635	4400/4305: Starting and stopping DMP presentations take longer then 5.1. **Workaround:** Use a public playlist instead of a DMD presentation as it is implemented completely in JavaScript as opposed to using the Flash player.
CSCti60435	4400/4305: Allow playlist background to display through transparent swf SWF displays white background despite color setting **Workaround:** Place an object of the desired color on the lowest layer of the swf to act as a background
CSCtj31811	4310: Slide show transition will slow down the SWF in All media and rss A slide show transitioning to the next image may cause any concurrently playing swf and/or RSS feed to slow down. Conditions: • Slide show is present with animated transitions • RSS feed and/or all-media playlist containing a swf item playing simultaneously • Deployed on the 4310 **Workaround:** Use the “No-effect” transition option for the slide show object.

Identifier	Description
CSCtn66678	DMP-4400 lockup when playing slideshow Cisco DMP-4400 will get lockup when playing specific slideshows and the following message will appear after few minutes in the display: “A script in this movie is causing Adobe Flash Player 10 to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?” This happens when you have a image slideshow. **Workaround:** Create a media playlist instead of creating a presentation in DMD.
CSCtq15140	Unable to stop Emergencies causing Play in Future to fail Emergencies are started but cannot be stopped. **Workaround:** Do the following **1** Select the DMP group showing “red” under DMM >> Digital Media Players >> Emergencies **2** Start an emergency on that group **3** Stop the emergency from that group
Cisco Show and Share	
CSCtx69098	Video/Slideshow Upload via Internet Explorer fails due to KB2585542 **Workaround:** You can restore the upload functionality by going into the IE Internet Options->Advanced->Security and uncheck "TLS 1.0".
CSCti94360	Show and Share does not delete local media deployed to external server As noted in the documentation, local copies of media files that are editable by Cisco Show and Share are maintained on the appliance, even if external hosting has been enabled for the file type. These files are needed in case a user wants to go back and edit the media. **Workaround:** None. These files can only be deleted by TAC. Once deleted, the associated media will not be editable.

Identifier	Description
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCts33571 CSCts33571	SNS: Changes in views and rating take long time to get updated Change in views and ratings are not reflected on the homepage until the video is played again. Rate a video and go to the Cisco Show and Share main page. The change in the rating is not reflected on the home page, but sorting the video list by rating or number of views puts the video in the correct order. This can make the video appear to be out of order. **Workaround:** View the video that had the view or ratings added then the homepage will update with the changes.
CSCud22759	For Show and Share Release 5.3 or later integrated with Cisco MXE 3500 Release 3.3.1 or later, Show and Share WebCam recording is not sent to MXE 3500 for transcoding. The WebCam videos are Flash and, thus, cannot be played on mobile devices. **Workaround:** Enable Pulse on Show and Share administration (**Administration -> Manage-> Preferences and Settings**) to send WebCam generated videos to the MXE 3500. The analytics data will be generated if the MXE 3500 is licensed for analytics.

Updates and Errata for Printed Documentation

Online-only documents on Cisco.com for Cisco DMS are updated as needed, and we recommend that you check Cisco.com regularly for updates.

This section describes errors and omissions in the **printed** documentation for Cisco DMS equipment and accessories, which were corrected — or *will be* corrected — in subsequent printings.

Getting Started Guide for Cisco Digital Media Players (78-19212-02)

Did your DMP ship with a printed copy of *Getting Started Guide for Cisco Digital Media Players* (78-19212-02), whose front-cover revision date is November 8, 2010?

If so, your printed copy contains errors about IP address configuration. It states that DMPDM settings on a DMP 4400G can cause your DMP to use a static IP address on a wireless network. However, we removed this option from DMPDM, where DHCP is now the only described address assignment method for wireless client DMPs.

Tip You can still assign a static IP address to a DMP 4400G. Simply do so from your wireless access point.

Remote Control Quick Start Guide for Cisco Digital Media Players

In some printings, the “Requirements and Limitations” section states incorrectly that “Cisco Digital Media Player (DMP) 4400G devices, and 4305G devices after July 2008, ship with a remote control.” The remote control is an optional item that you must purchase separately.

Mounting Kit Assembly Guide for Cisco Digital Media Players

In some printings, Cisco product numbers are wrong for mount kits.

- Any use of “69-1802 -01” is incorrect. The correct part number is “DMP-PRCASE-4305 -S1.”
- Any use of “69-1803 -01” is incorrect. The correct part number is “DMP-PRCASE-4400 -S1.”

Quick Start Guide for Cisco Digital Media Player (4305G and 4400G)

Some printings of these two guides contain identical errors:

- *Quick Start Guide for Cisco Digital Media Player 4305G*
- *Quick Start Guide for Cisco Digital Media Player 4400G*

The errors are as follows:

- The Checking the Package Contents topic states incorrectly (**CSCta34388**) that your product kit includes a battery-powered remote control unit. However, the remote control is an optional item that you must purchase separately.
- The Concepts text on page 3 mentions “protective case” accessories for DMPs, which discourage tampering and prevent theft. The accessory category was renamed after these guides were printed. The category name is now “mount kit.”
- Also because the accessory category was renamed, the topic “Learning About the Protective Case for DMPs” became invalidated in multiple ways after these guides were printed:
  - The topic heading should say “Learning About the Mounting Kit for DMPs.”
  - The topic text mischaracterizes the title for mount kit assembly documentation. The correct title is *Mounting Kit Assembly Guide for Cisco Digital Media Players* .
- Any use of “69-1802 -01” is incorrect. The correct part number is “DMP-PRCASE-4305 -S1.”
- Any use of “69-1803 -01” is incorrect. The correct part number is “DMP-PRCASE-4400 -S1.”

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

To Learn About	Go To
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/cscc
Standard warranties	http://cisco.com/go/warranty
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.	

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands