CHAPTER 23

Proof of Play

Revised: April 4, 2012
OL-15762-04

Audience

We prepared this material with specific expectations of you.

✓ You will audit and run reports that demonstrate your playback of media assets on your Cisco Digital Signs.

Concepts

Overview

You can audit which assets your DMPs play... and where... and when... and for how long—across any supported range of dates that you specify. This feature supports a maximum of 200 DMPs.

Proof of play reports are available per DMP, per DMP group, and per *insertion*. We use a dedicated proof of play service to collect these records and generate these reports.

Restrictions

Caution

Proof-of-play features fail unless:

- The Syslog Collector IP Address entry in DMPDM points to your DMM appliance.
- The fully qualified domain name of your DMM appliance contains fewer than 30 characters.

Implications of Changing the DMM Appliance Hostname

Will you use AAI to change the hostname of a DMM appliance on which proof-of-play features are enabled (**CSCtr00731**)*?* There is no common reason to do this. We recommend that you do not. Nonetheless, we will not stop you.

BEFORE YOU CHANGE THE HOSTNAME

- Export your proof-of-play logs.

AFTER YOU CHANGE THE HOSTNAME

- Log in to the web interface for DMM at its new hostname, and then immediately reconfigure the proof-of-play feature.

WHY IS THIS NECESSARY?

We assume that your information is confidential and we strive to protect it from unauthorized access. Therefore, DMM self-registration of a feature license considers the combination of the appliance hostname and its hardware serial number.

After its appliance hostname is changed, DMM will reject its prior self-registration of your license to use proof-of-play features. Although the license is still valid and is still correctly associated with your hardware serial number, your DMM appliance cannot load proof-of-play logs from any server whose hostname differs from its own. It cannot read from them or write to them. Likewise, you cannot use proof-of-play features on any host but the one that self-registered the license.

Although you can return a hostname to its original value, doing so still might not be sufficient to satisfy an ongoing requirement for full and uninterrupted access to proof-of-play features and logfiles. Consider this scenario.

1. The hostname is changed from **A** to **B**. Therefore, B cannot use the feature license that A self-registered and cannot use the logfiles that DMM generated on behalf of A.
2. The hostname is then returned to **A**. Therfore, A can access its own data from any time when the hostname was A, including the original instance. However, it cannot use the feature license that B self-registered and cannot use the logfiles that DMM generated on behalf of B.

We recommend that you prevent these complications and disruptions by leaving the hostname in its original state.

Implications of Changing the User Authentication Method

Will you change the user authentication method from LDAP mode to Federation mode (SSO) for a Cisco DMS deployment that includes proof of play (**CSCtq55094**)*?* Fundamental changes to user authentication are not routine but can be useful occasionally.

However, account records in the new SSO user base might not correspond exactly to account records in the old LDAP user base. It is possible, in fact, that some long-established login credentials might cease to be valid for Cisco DMS users. And so, if the proof-of-play user role assignment in your network is associated with one of these nullified user accounts, the affected user cannot view proof-of-play insertions or run reports for insertions.

In this case, you must assign the proof-of-play role to a user account that exists in the SSO user base.

Implications of Changing Which Assets a Playlist Includes

In this release, proof-of-play reports for a given playlist during a given time range might not be correct (**CSCtr97593**). In some cases, these reports can:

- Omit playback records retroactively for assets that you trimmed from the playlist at a later time. (These assets were once correctly part of the playlist and their playback count from that time is relevant to this report.)
- Insert playback records retroactively for assets that you added to the playlist at a later time. (These assets were once correctly excluded from the playlist and their playback count from that time is not relevant to this report.)

Glossary

Timesaver **Go to terms that start with**... [**I** | **R**].

I

insertion The campaign or other common goal among any one set of presentations, playlists, and assets that you consider an affinity group.

R

Return to Top

requestor The agency or other entity that requests an insertion or prepares resources for an insertion.

Insertions

Cisco Digital Signs includes methods to identify and assemble an affinity group from any combination of presentations, playlists, and assets. We call this affinity group package an *insertion*.

Mingled elements within an insertion all share one clear and unifying purpose. For example, the elements of your first insertion might all advertise a community celebration, even though they use various languages or differ in other, key ways. However, you recognize for your own purposes that at least one significant factor (the community celebration, in this example) unites them as an affinity group.

The benefit of insertions is that you can audit and verify the scope of playback—individually and collectively—for all elements that support one goal, initiative, policy, campaign, or event. On a DMP-by-DMP basis, you can discover and demonstrate exactly which assets:

- Played successfully, and when.
- Were interrupted or prevented from playing, and when.

Note

- **Proof of play features in Cisco Digital Signs ignore the playback of assets that Cisco developed—including all samples and templates that you receive with DMM.**
- **Syslog data provides the start and stop time stamps for playback.** From time to time, some of these time stamps might seem wrong even though they are technically correct. In this case, puzzling results will report a playback duration of 0 min and 0 sec for any insertion element whose start time and stop time were identical—for any reason. The likeliest explanation is that a stop command interrupted playback coincidentally during the same second in which an insertion element was scheduled to start playback (CSCtr57386).

A populated insertion audits the playback of:

- Each asset that you reference *directly*, as a single element regardless of its context.
- Each asset that you reference *indirectly*, as one element within the context of a playlist or presentation.

Workflow

1. Add assets to your media library.
2. Develop, schedule, and publish presentations and playlists.
3. Define report collection parameters for proof-of-play.
4. Run reports.

Procedures

- Prepare DMPs to Support Proof of Play, page 23-4
- Create Requestors, page 23-7
- Create Insertions, page 23-7
- Run a Report, page 23-8
- Export a Report, page 23-9
- View Previous Reports, page 23-10
- Use the Proof of Play Dashboard, page 23-10
- Use Deployment Reports, page 23-11

Prepare DMPs to Support Proof of Play

- Enable Syslog and NTP, page 23-5
- Enable Proof of Play Features in DMM, page 23-6

Enable Syslog and NTP

Procedure

Step 1 Do one of the following.

- *Would you like to enable these services from Digital Signs?*

  Use elements in Digital Signs to enable these services.

  a. Choose **Advanced Tasks > System Tasks**.
  b. Create a new system task.
  c. Enter a meaningful name in the Name field, such as **Enable PoP access on DMPs**.
  d. Choose **Set** from the Request Type list, and then enter this string:

  ```
  init.syslog=on&init.syslog_collector=<DMM_routable_IP>&mib.save=1
  &mng.reboot=1
  ```

  e. Click **Submit**.
  f. Click **OK**.
  g. Deploy to all DMPs that should support proof of play.

- *Would you like to enable these services from DMPDM?*

  Use elements in DMPDM to enable these services

  a. Click **Browser** in the Settings list.
  b. Enter the routable IP address of your DMM appliance in the Syslog Collector IP Address field.
  c. Click **Apply**.
  d. Click **NTP** in the Settings list, and then choose **On** from the Enable NTP Service list.
  e. Enter pool.ntp.org in the Hostname 1 field, if you have not already done so.
  f. Choose your locale from the Time Zone list, and then click **Apply**.
  g. Save Configuration
  h. Restart.

Step 2 Stop. You have completed this procedure.

Enable Proof of Play Features in DMM

Procedure

Step 1 Log in as superuser.

Step 2 Choose **Proof of Play > Configuration**.

Step 3 Enter the fully qualified, DNS-resolvable DMM appliance domain name in the DMM FQDN field.

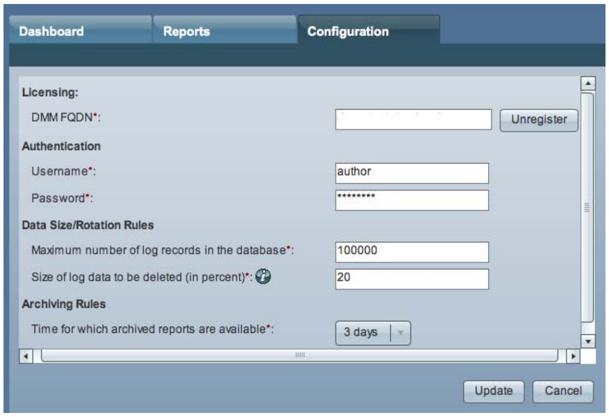
For example: *dmm.example.com*

Step 4 Click **Register**.

Step 5 Use fields in the Authentication area to enter the superuser name and password for your DMM appliance.

Step 6 Define settings in the Data Size/Rotation Rules area.

Step 7 Choose an option in the Archiving Rules area to set how many days of playback data to accumulate before archiving it.



Licensing:

DMM FQDN*:

Authentication

Username*: author

Password*: ********

Data Size/Rotation Rules

Maximum number of log records in the database*: 100000

Size of log data to be deleted (in percent)*: 20

Archiving Rules

Time for which archived reports are available*: 3 days

Step 8 Click **Update**.

Step 9 Stop. You have completed this procedure.

Create Requestors

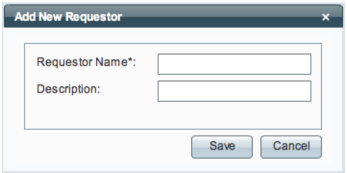
Procedure

Step 1 Choose **Digital Signage > Insertions**, and then click **Manage Requestors**.

The Manage Requestors dialog box opens.

Step 2 Click **Add New Requestors**.

The Add New Requestor dialog box opens.



Step 3 Enter at least a name but also, optionally, a description.

Step 4 Click **Save**.

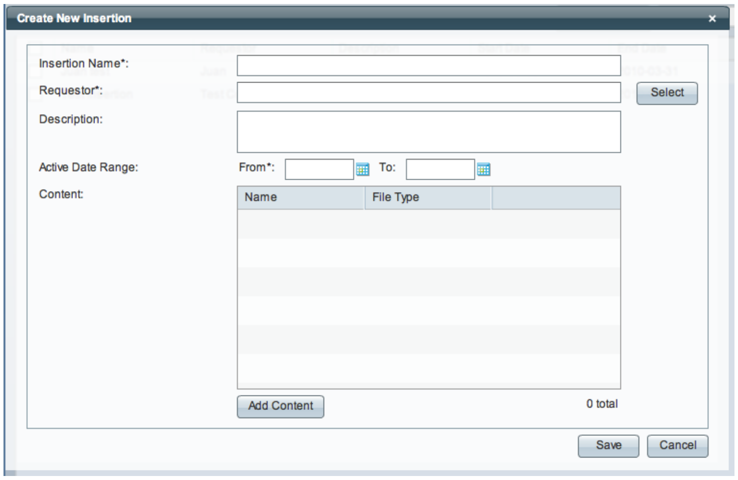
Step 5 Stop. You have completed this procedure.

Create Insertions

Procedure

Step 1 Choose **Digital Signage > Insertions**, and then click **Create Insertion**.

The Create New Insertion dialog box opens.



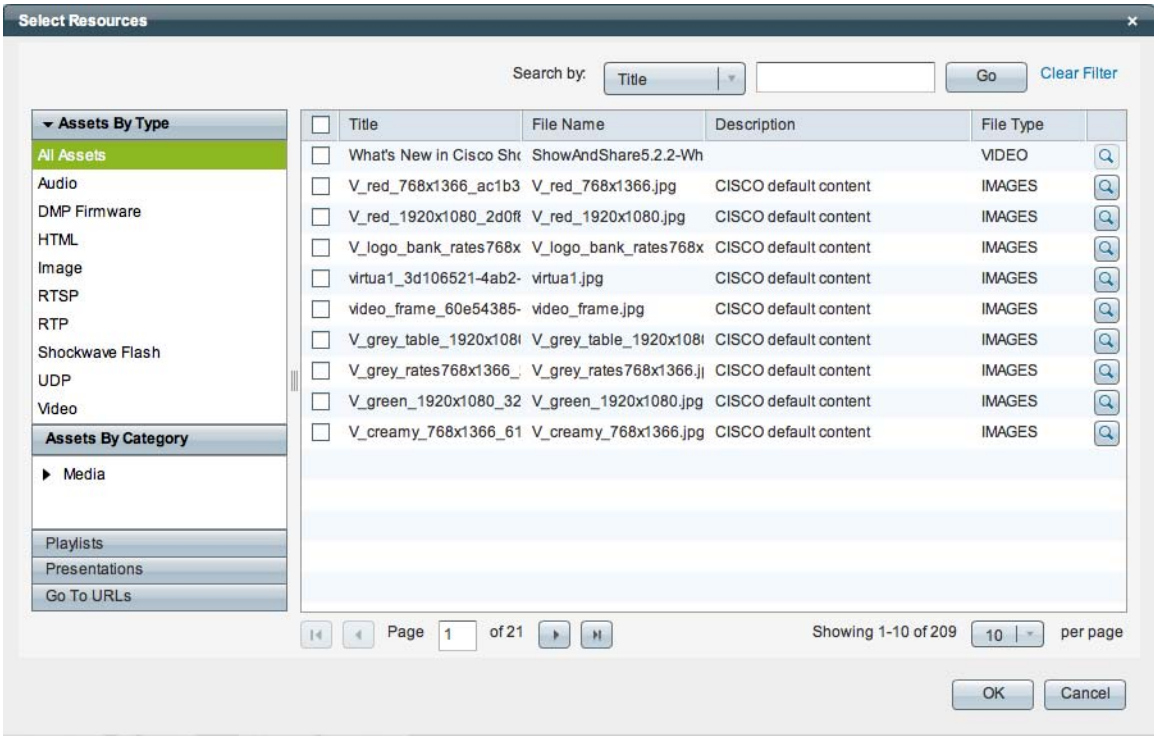
Step 2 Enter a name for this insertion.

Step 3 Associate a requestor with this insertion.

Step 4 Choose when this insertion should become active, and then choose when it should stop.

Step 5 Click **Add Content**.

The Select Resources dialog box opens.



□	Title	File Name	Description	File Type
□	What's New in Cisco Sh(	ShowAndShare5.2.2-Wh		VIDEO
□	V_red_768x1366_ac1b3	V_red_768x1366.jpg	CISCO default content	IMAGES
□	V_red_1920x1080_2d0f(	V_red_1920x1080.jpg	CISCO default content	IMAGES
□	V_logo_bank_rates768x	V_logo_bank_rates768x	CISCO default content	IMAGES
□	virtua1_3d106521-4ab2-	virtua1.jpg	CISCO default content	IMAGES
□	video_frame_60e54385-	video_frame.jpg	CISCO default content	IMAGES
□	V_grey_table_1920x108(	V_grey_table_1920x108(	CISCO default content	IMAGES
□	V_grey_rates768x1366_	V_grey_rates768x1366.j|	CISCO default content	IMAGES
□	V_green_1920x1080_32	V_green_1920x1080.jpg	CISCO default content	IMAGES
□	V_creamy_768x1366_61	V_creamy_768x1366.jpg	CISCO default content	IMAGES

Step 6 Use check boxes in the table to mark assets that you might use.

- Use options on the left to filter what the table shows.
- Use pagination controls under the table to control how many assets you see.
- Use the Search function above the table to locate particular assets quickly.

Step 7 Click **OK** to populate your insertion with the assets that you marked.

Step 8 Stop. You have completed this procedure.

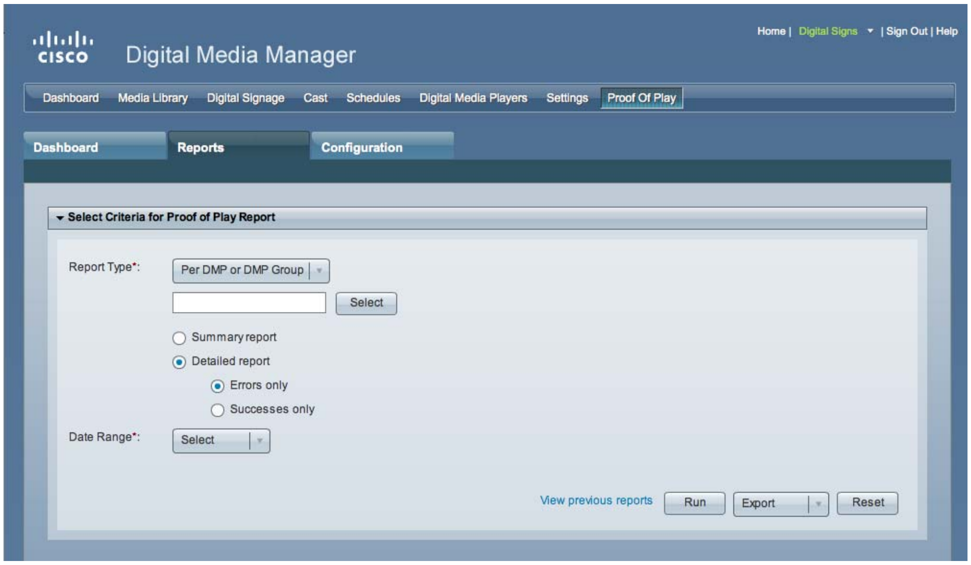
Run a Report

Procedure

Step 1 Choose **Proof of Play > Reports**.

Step 2 Choose reporting criteria.

- Report Type options are **Insertion**, **DMP**, or **DMP Group**.
- Reporting scope options are **Summary** and **Detailed**.
  - A summary report counts successes and failures.
  - A detailed report counts either successes *or* failures.
- You must specify the date range.



Report Type*: Per DMP or DMP Group

○ Summary report
● Detailed report
● Errors only
○ Successes only

Date Range*: Select

Step 3 Click **Run**.

Step 4 Stop. You have completed this procedure.

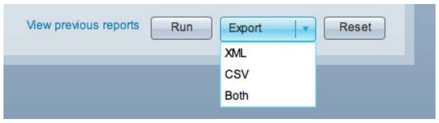
Export a Report

Before You Begin

- Complete the "Run a Report" section on page 23-8.

Procedure

Step 1 Choose a format from the Export list.



Step 2 Stop. You have completed this procedure.

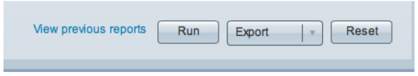
View Previous Reports

Before You Begin

- Complete the "Run a Report" section on page 23-8.

Procedure

Step 1 Click **View previous reports**.

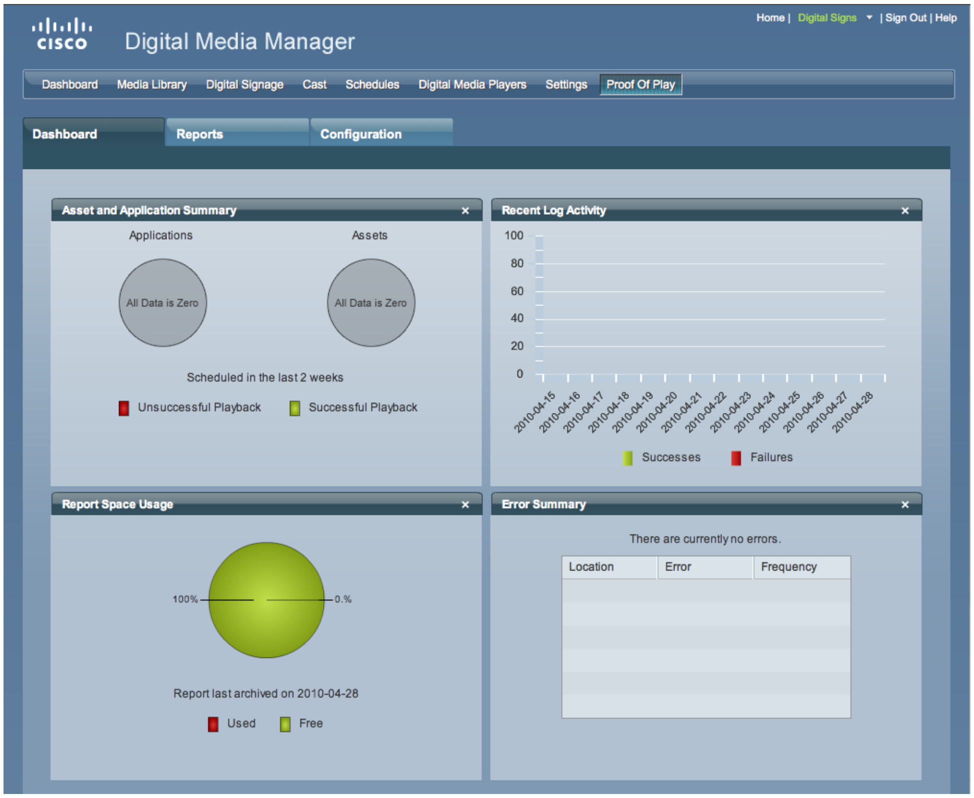


Step 2 Stop. You have completed this procedure.

Use the Proof of Play Dashboard

Procedure

Step 1 Choose **Proof of Play > Dashboard**.



Scheduled in the last 2 weeks

Report last archived on 2010-04-28

There are currently no errors.

Location	Error	Frequency

Step 2 Stop. You have completed this procedure.

Use Deployment Reports

You can view, configure, and export additional reports for the presentations and tasks that you have deployed in your digital signage network.

Procedure

Step 1 Choose **Schedules > Reports**.

Step 2 Check the check boxes for the relevant DMP groups.

Step 3 Enter date range values in the From field and the To field.

Step 4 From the Report Type list, select the report type.

Step 5 Click **Go**.

Step 6 Stop. You have completed this procedure.

Reference

- FAQs and Troubleshooting, page 23-11

FAQs and Troubleshooting

- FAQs, page 23-11
- Troubleshooting, page 23-12

FAQs

Q. What might prevent proof-of-play features from working at all?

A. The fully qualified domain name (FQDN) for your DMM appliance must not exceed 30 characters.

```
dmm.example.com                    ←——  VALID for Proof of Play
123456789012345678901234567890
digitalmediamanager.example.com    ←——  NOT VALID for Proof of Play
```

Q. How do insertions differ from presentations and playlists?

A. They are fundamentally different.

- Before playback can start for a presentation or playlist, you must target DMP groups and reserve timeslots for playback.
- After a reserved timeslot has elapsed, you can verify whether playback occurred as scheduled for its programming.

Q. Are insertions required in proof of play?

A. No. Insertions are just one of three supported report types. You can also obtain proof of play reports per DMP or per DMP group.

Q. **Can I associate one asset with multiple insertions?**

A. Yes.

Q. **What triggers universal proof of play auditing for an asset?**

A. There are two scenarios in which we validate each instance of playback for an asset.

Scenario	Details	Exceptions
Your insertions already include all presentations and playlists that use the asset.	In this case, because you have not used the asset anywhere outside of an insertion, we verify its every instance of playback.	This universal verification becomes conditional when you use the asset anywhere outside an insertion.
You added the asset explicitly to an insertion.	In this case, we audit playback for this asset no matter how or when you play it, or in what context.	When you play it as *just one part* of a presentation or playlist that **is not**—*in its own right*—part of any insertion: • We **do not** verify playback for the playlist as a whole. • We **do not** verify playback for any other assets than the one that you audit explicitly.

Q. **What triggers conditional proof of play auditing for an asset?**

A. We might validate some instances of playback but not others. We cannot audit playback consistently for an asset whose instances of playback occur sometimes outside any insertion.

Q. **What prevents proof of play auditing for an asset?**

A. We cannot validate instances of playback for an asset whose every instance of playback occurs outside any insertion.

Q. **What are the implications for emergency events?**

A. See CSCtd23249

Troubleshooting

The log file location for proof of play features is: **`/var/apache-tomcat/proofofplay-core.log`**