



Proof of Play

Revised: May 13, 2015
OL-15762-03

- [Concepts](#)
- [Procedures](#)
- [Reference](#)



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.



Note

This material pertains to multiple releases of Cisco DMS.

5.2.0

5.2.1

5.2.2

5.2.3

Concepts

- [Overview, page 21-1](#)
- [Glossary, page 21-2](#)
- [Insertions, page 21-2](#)
- [Workflow, page 21-3](#)

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.

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.

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 times for playback.**

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 21-3](#)
- [Create Requestors, page 21-6](#)
- [Create Insertions, page 21-6](#)
- [Run a Report, page 21-7](#)
- [Export a Report, page 21-8](#)
- [View Previous Reports, page 21-9](#)
- [Use the Proof of Play Dashboard, page 21-9](#)
- [Use Deployment Reports, page 21-10](#)

Prepare DMPs to Support Proof of Play

- [Enable Syslog and NTP, page 21-4](#)
- [Enable Proof of Play Features in DMM, page 21-5](#)

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.

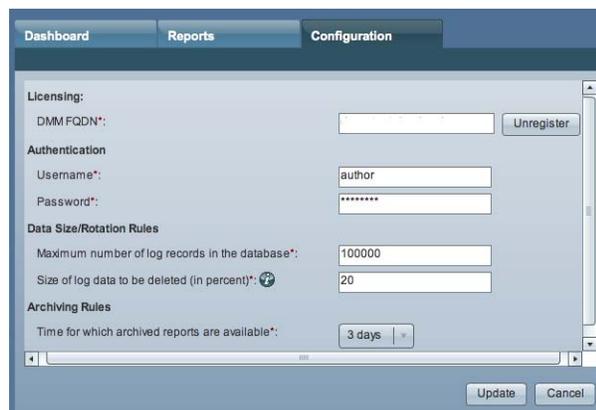
- *Would you like to enable these services from DMPDM?* **Use elements in DMPDM to enable these services**
 - a. Click **Browser** in the Settings list.
 - b. Enter the routable IP address of your DMM appliance in the Syslog Collector IP Address field.
 - c. Click **Apply**.
 - d. Click **NTP** in the 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.



The screenshot shows the 'Configuration' tab of the DMM web interface. It contains the following sections and fields:

- Licensing:** A text input field for 'DMM FQDN*' and an 'Unregister' button.
- Authentication:** Text input fields for 'Username*' (containing 'author') and 'Password*' (masked with asterisks).
- Data Size/Rotation Rules:** Text input fields for 'Maximum number of log records in the database*' (containing '100000') and 'Size of log data to be deleted (in percent)*' (containing '20').
- Archiving Rules:** A dropdown menu for 'Time for which archived reports are available*' set to '3 days'.

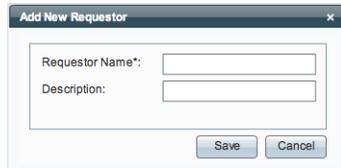
At the bottom right of the configuration area are 'Update' and 'Cancel' buttons.

- 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.

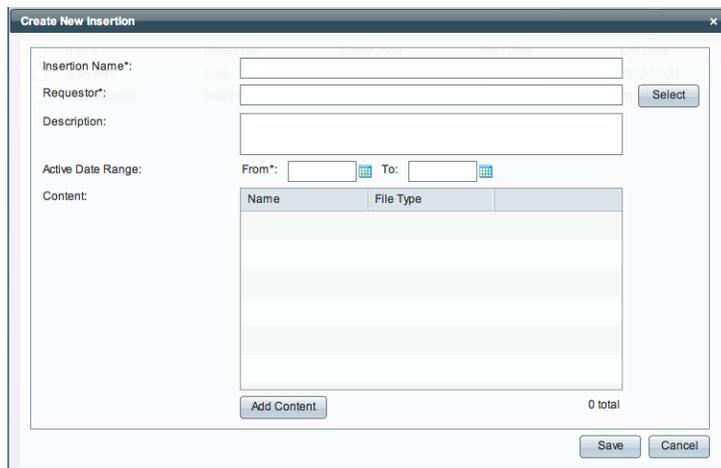


- Step 3** Enter at least a name but also, optionally, a description.
- Step 4** Click **Save**.
- Step 5** Stop. You have completed this procedure.

Create Insertions

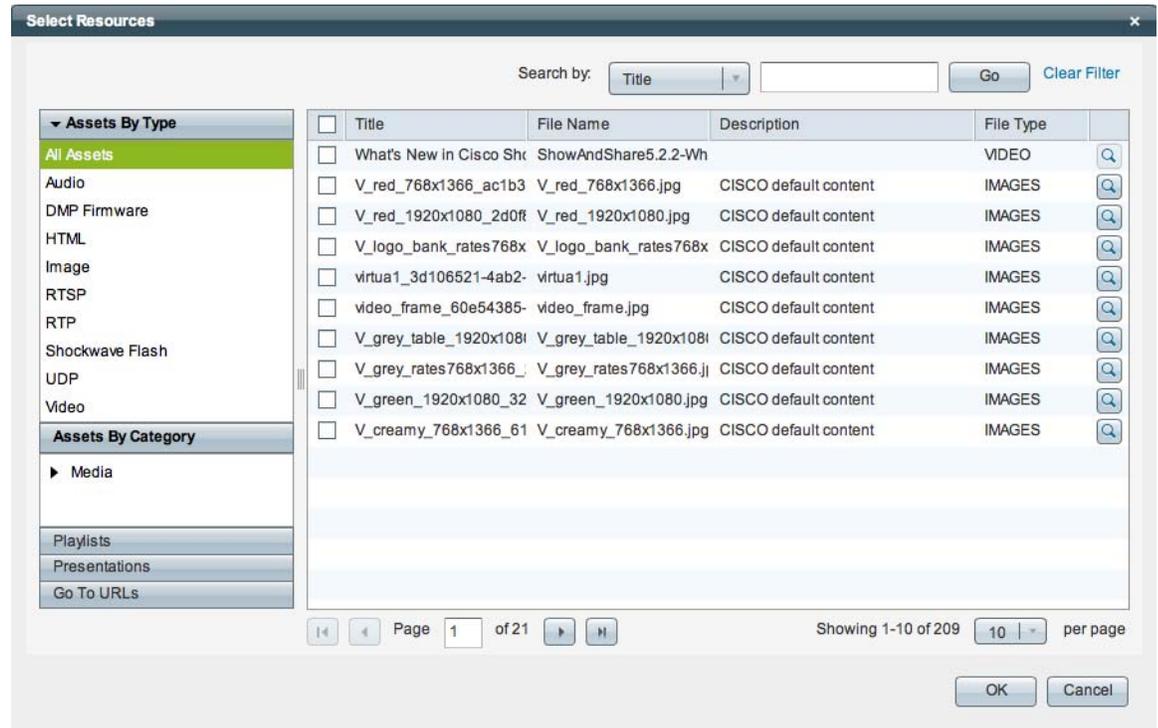
Procedure

- 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.

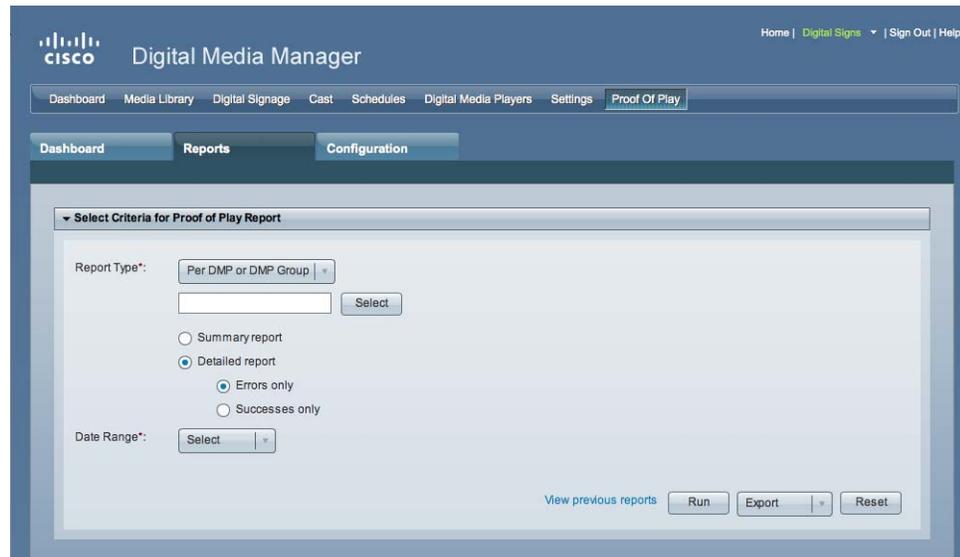


- Step 6** Use check boxes in the table to mark assets that you might use.
- Use options on the left to filter what the table shows.
 - Use pagination controls under the table to control how many assets you see.
 - Use the Search function above the table to locate particular assets quickly.
- Step 7** 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.



Step 3 Click **Run**.

Step 4 Stop. You have completed this procedure.

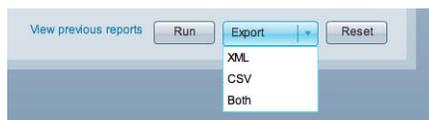
Export a Report

Before You Begin

- Complete the “Run a Report” section on page 21-7.

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 21-7.

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**.



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 21-10](#)

FAQs and Troubleshooting

- [FAQs, page 21-10](#)
- [Troubleshooting, page 21-11](#)

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.

<code>dmm.example.com</code>	← VALID for Proof of Play
<code>123456789012345678901234567890</code>	
<code>digitalmediamanager.example.com</code>	← 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 <i>just one part</i> of a presentation or playlist that is not — <i>in its own right</i> —part of any insertion: <ul style="list-style-type: none"> 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`

