



# How to Configure Automatic Proof of Play Export

## Dynamic Signage Director

**Software Release: 5.0.0-123 and Later Releases**

**First Published: 2016-10-10**

## Contents

- [Introduction , page 1](#)
- [Requirements, page 2](#)
- [Required Configuration, page 2](#)
- [Optional Configuration, page 4](#)
- [Workflow Summary, page 4](#)

## Introduction

The Automatic Proof of Play (PoP) Export feature is useful when you want to use another tool or application to consume the PoP CSV data from Cisco Vision Dynamic Signage Director.

When PoP is enabled for a script, the Summary and Detailed PoP data (in CSV format) is automatically exported to a designated server using Secure FTP (SFTP) or Secure HTTP (HTTPS).

After you have enabled the automatic export feature globally in the system, and also PoP for a script, you can verify the status of the export function under the new “Transmitted” column on the Control Panel Proof of Play screen. A green icon means the data has been transmitted; red means it failed.

### Retry Behavior for Failed Transmission

After 30 seconds from script completion (the default Delay Auto Upload period), the system automatically attempts to export the PoP data to the designated server. If the transmission fails, the following behavior occurs:

- The system initially retries up to three times (or, the number of times specified in the Pop Upload Retry Count property).
- If the PoP export fails after the initial retry attempts, a system task (PofpUploadRetryTask) runs in the background to detect any failed transmissions.
- The system task continues to attempt the PoP data export up to a maximum of 50 retries (or, the number of times specified in the Max Pop Upload Retry Count property.)

**NOTE:** When Automatic PoP Export is enabled, the standard PoP reporting features remain available in Cisco Vision Dynamic Signage Director Release 5.0. You do not need to do manual report generation if Automatic PoP Export is enabled.

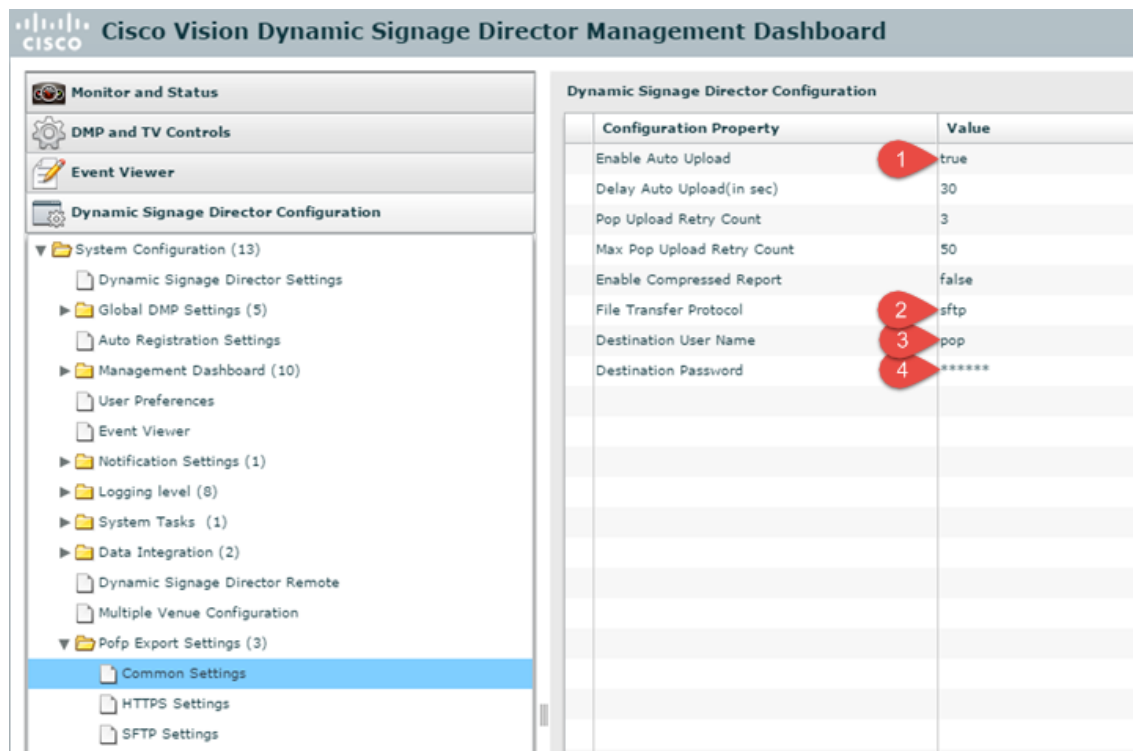
## Requirements

- A server is available on the network over SFTP or HTTPS as the destination server for the PoP data.
- A user account is set up and the path on the destination server is available.

## Required Configuration

1. Log in to Cisco Dynamic Signage Director as an administrator.
2. From the Management Dashboard, go to:  
**Dynamic Signage Director Configuration > System Configuration > Pofp Export Settings**
3. Set the **Enable Auto Upload** property to **true** and configure the other required Common properties:

**Figure 1 Management Dashboard PoP Export Required Settings**



|   |   |   |  |
|---|---|---|--|
| 1 | Enable Auto Upload—Type value of <b>true</b> .  | 2 | File Transfer Protocol—Type value of <b>sftp</b> or <b>https</b> .   |
| 3 | Destination User Name—Type the user name for the account on the destination server where the data will be exported. | 4 | Destination Password—Type the password that corresponds to the account user name that you specified on the destination server where the data will be exported. |

Required Configuration

- Then, based on the File Transfer Protocol property under Common Settings, go to either **HTTPS Settings** or **SFTP Settings** to complete the configuration.

**Figure 2 HTTPS Properties**

| Dynamic Signage Director Configuration |  |
|--|--|
| Configuration Property                 | Value  |
| Secure Web Address                     | https://10.194.170.131:7443/secure_http/uploadReport |
| Accept Self Signed Certificate         | true   |

|   |  |   |  |
|---|--|---|--|
| 1 | Secure Web Address—Type the HTTPS URL including IP address and path on the destination server. | 2 | Accept Self Signed Certificate—Type value of <b>true</b> (default) or <b>false</b> . |
|---|--|---|--|

**Figure 3 SFTP Properties**

| Dynamic Signage Director Configuration |                |
|--|----------------|
| Configuration Property                 | Value          |
| File Server IP Address or FQDN         | 10.194.173.108 |
| File Server Port                       | 22             |
| File Server Relative Folder Path       | /              |

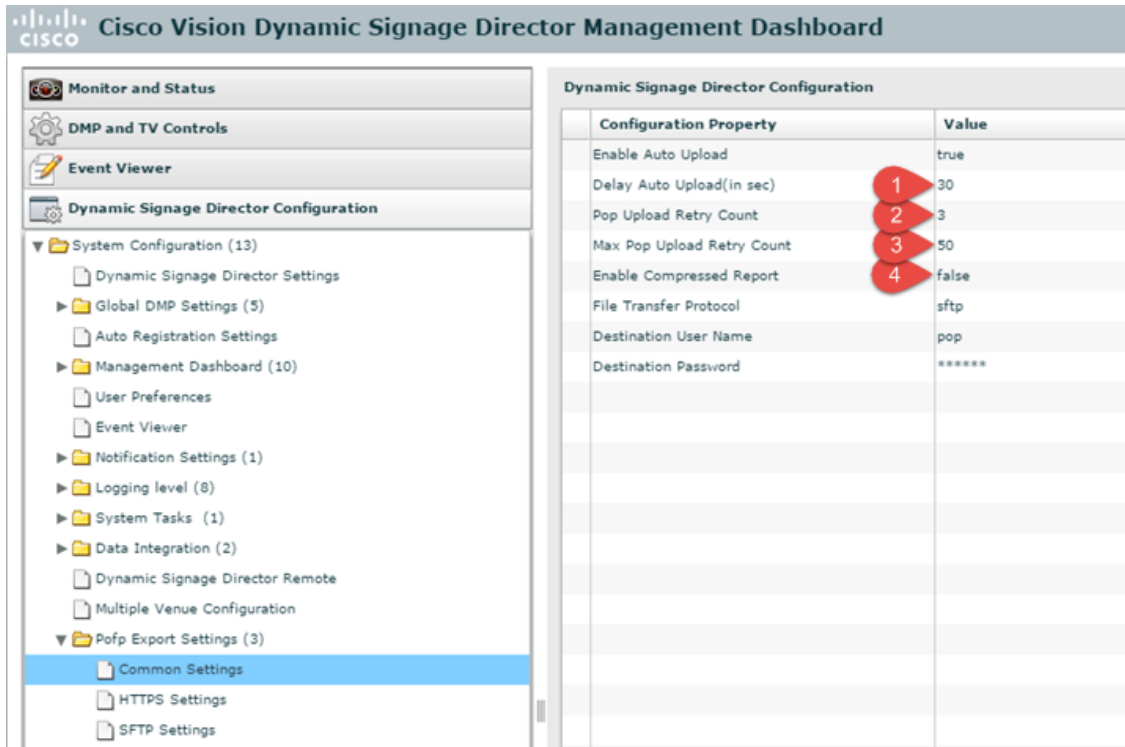
|   |   |   |   |
|---|---|---|---|
| 1 | File Server IP Address or FQDN—Type the IP address or fully-qualified domain name of the destination server where the data will be exported.  | 2 | File Server Port—Type value of <b>22</b> (standard SFTP port), or other port required by your server. |
| 3 | File Server Relative Folder Path—Specify the relative folder path for the server home directory. A value of “/” will store the data in the server home directory path. A value of “/mypopdata” will put the data in a sub-folder of the home directory with the name “mypopdata.” |   |   |

- Save the configuration.

## Optional Configuration

This section describes the optional settings that you can configure for automatic PoP export.

**Figure 4 Management Dashboard PoP Export Optional Settings**



|   |   |   |  |
|---|---|---|--|
| 1 | Delay Auto Upload (in sec)—Number of seconds that the system waits (after the script ends) before exporting the data to the destination server. The default is 30 seconds.  | 2 | Pop Upload Retry Count—Number of attempts that the system initially makes to upload the PoP data to the destination server after a script completes. The default is 3 retries. |
| 3 | Max Pop Upload Retry Count—Maximum number of attempts that the background <i>PofpUploadRetryTask</i> system task retries upload of PoP data that has failed to transmit to the destination server. The default is 50 retries. | 4 | Enable Compressed Report—A value of <b>true</b> enables compression of the PoP report data for transmission. The default is false.   |

## Workflow Summary

This section describes the configuration and operation workflows for automatic PoP export.

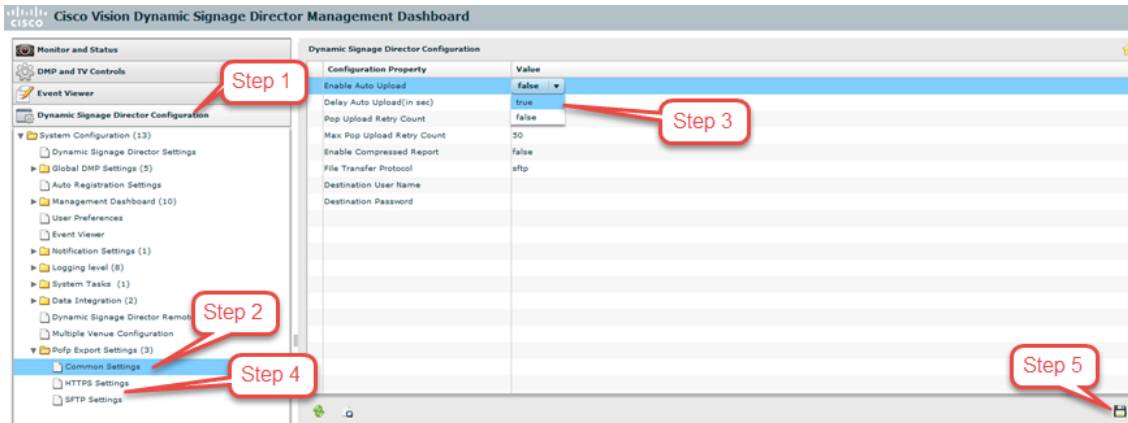
### Management Dashboard Workflow

#### Supported User Roles

- Administrator

The Automatic PoP Export feature is enabled and configured globally for all scripts in the system from the Management Dashboard.

Workflow Summary



1. From the Management Dashboard, go to **Dynamic Signage Director Configuration**.
2. Click **Pop Export Settings > Common Settings**.
3. Set the required and optional (as needed) properties.  
See [Required Configuration, page 2](#) and [Optional Configuration, page 4](#).
4. Based on the configured File Transfer Protocol type for the destination server, set the HTTPS or SFTP settings.
5. Save the configuration.

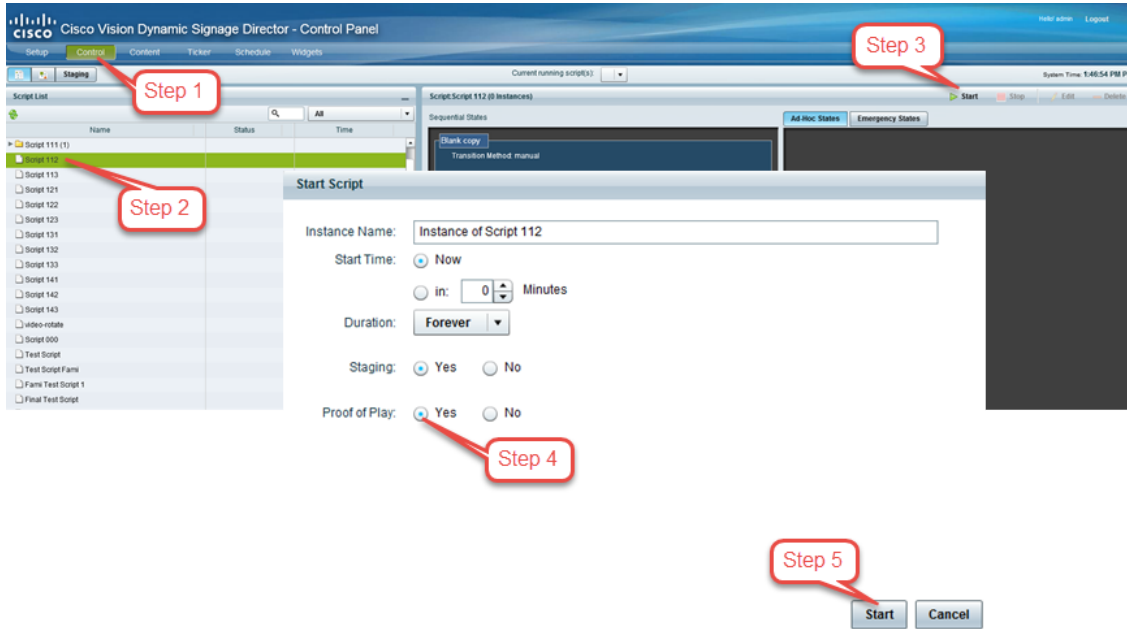
## Control Panel – Control Workflow

### Supported User Roles

- Administrator
- Event Operator
- Venue Administrator
- Venue Operator

Proof of Play is enabled for a script in the Control Panel. The Automatic PoP Export feature must be enabled globally, and Proof of Play also must be enabled for a script, to generate and export PoP reports.

Workflow Summary



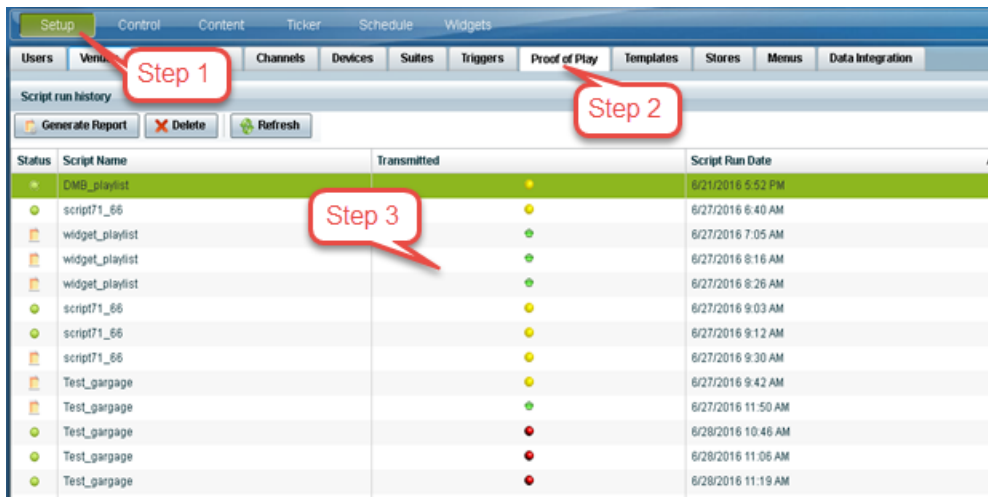
1. From the Control Panel, go to **Control**.
2. Select the desired script.
3. Click **Start**.
4. Set Proof of Play to **Yes**.
5. Click **Start**.

Control Panel – Setup Workflow

Supported User Roles

- Administrator

Go to the Control Panel Setup screen to verify the status of PoP report export status.



Workflow Summary

1. From the Control Panel, go to **Setup**.
2. Click **Proof of Play**.
3. In the Transmitted column, verify the status of the PoP report export for your script.

| Button Color | Description            |
|--------------|------------------------|
| Green        | Export is successful.  |
| Yellow       | Export is in progress. |
| Red          | Export failed.         |

## Workflow Summary

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

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

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

© 2016 Cisco Systems, Inc. All rights reserved.