StadiumVision

Cisco StadiumVision Director Software Installation and Upgrade Guide

Release 3.1

January 17, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco StadiumVision Director Software Installation and Upgrade Guide

CISCO

StadiumVision

CONTENTS

Preface vii

Document Revision History vii

Document Organization x

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xi

Getting Started Installing or Upgrading Cisco StadiumVision Director 1

Before You Begin 1

Overview of the Installation and Upgrade Process 2

Upgrading an Existing Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 3

Installing a Platform 3 Server with Release 3.1 for the First Time 3

Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.1.0-510 or Later 4

Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server 5

Prerequisites 5

Installation Tasks 6

Downloading the ISO Files from Cisco.com 7

Logging Into the CIMC Interface 8

Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director 9

Launching the KVM Console 10

Mapping the Cisco StadiumVision Director ISO Image 11

Installing the Cisco StadiumVision Director ISO Image 12

Configuring the Network Setup 12

What To Do Next 15

Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2 17

Contents 17

Best Practices 18

Prerequisites 19

Upgrade Tasks 20

Running Proof of Play Reports 20

Upgrading the Software From Release 3.0 SP2 to Release 3.1 20

Extending the Original RAID Volume to Create a Single Group 21
Migrating Content to the Release 3.1 CMS 21
Preparing the Release 3.0 Video Content for Migration 21
Running the Content Migration 23
Upgrading the DMP Firmware 23
Verifying the Upgrade 24
Validating the Content Migration 24
Cleaning Up Legacy Video Files After Migration 25
Removing Legacy Video Files From the Cisco StadiumVision Director Server 25
Removing Legacy Video Files From the DMP 25
What to Do Next 26

Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software 27

Best Practices 27
Prerequisites 28
Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server 29
ISO Upgrade Files 29
Disk Maintenance 29
Upgrade Tasks 29
Downloading ISO Upgrade Files from Cisco.com 30
Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server 31
Prerequisites 31
Logging Into the CIMC Interface 32
Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director 33
Launching the KVM Console 34
Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server 35
Verifying the Upgrade 37
Clearing the Browser Cache 38
Importing the Security Certificate 38
Importing the Security Certificate for Microsoft IE 39
Adding a Security Exception for Mozilla Firefox 39
Logging Into Cisco StadiumVision Director 40
Verifying the Control Panel and Other Menus 41
Verifying that Services are Running 42
Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check 42
Verifying DMPs, Groups, and Zones in the Management Dashboard 44
Verifying the Multicast Configuration 44
Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server 45

What to Do Next 47

Upgrading the DMP Firmware 49

Contents 49

Prerequisites 49

Upgrade Tasks 49

Downloading the DMP Firmware 49

Downloading the DMP-4310G Version 5.4 Firmware 50

Downloading the DMP-4310G Version 5.3.4 Firmware 50

Upgrading the DMP Firmware From the Management Dashboard 50

Disabling Failover on all DMPs 52

Appendix A: Post-Upgrade Checklist 55

Appendix B: Port Reference 57

Cisco StadiumVision Director Ports 57

Cisco StadiumVision Director Input Ports 57

Cisco StadiumVision Director Output Ports 58

Cisco StadiumVision Director Remote Ports 59

Cisco StadiumVision Director Remote Input Ports 59

Cisco StadiumVision Director Remote Output Ports 59

DMP Ports 59

DMP Input Ports 60

DMP Output Ports 60

Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.1 61

Contents 61

Prerequisites 61

Installation Tasks 62

Installing the Hard Drives Into the Server Chassis 62

Creating a New Logical Volume Using the LSI MegaRAID Utility 63

Extending the Original RAID Volume to Create a Single Group 66

What To Do Next 67

Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server 69

CIMC Initial Configuration 69

Prerequisites 69

CIMC Initial Configuration Summary 70

CIMC Firmware Upgrade Guidelines 71

Before You Begin 71
Prerequisites 72
CIMC/BIOS Firmware Upgrade Summary 72

Preface

This document describes the requirements and tasks to install and upgrade the software for Cisco StadiumVision Director Release 3.1.

The content is intended for Cisco StadiumVision system administrators and technical field engineers who are responsible for designing and deploying Cisco StadiumVision solutions. It is expected that readers of this document are familiar with basic IP networking and Linux, have a general understanding of the sports and entertainment business, and understand the objectives and operations of live events.

Document Revision History

Table 1 lists the technical changes made to this document since it was first published.

Table 1 Document Revision History

Date	Change Summary
January 17, 2014	The following changes were made: • Removed the steps for staging the Flash template and deploying the Global DMP Settings commands from the verification task list, and moved them as required tasks in the upgrade task list for better visibility in the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module. • Added the "Staging the Flash Template" and "Deploying the Global DMP Settings" tasks to the upgrade task list for better visibility in the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module.
September 30, 2013	The following changes were made: • Revised the caution to add requirement to install the Release 3.1.0-787 (SP1) full ISO first followed by an upgrade to Release 3.1.0-797 (SP2) as the minimum supported software release to the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5. • Revised the module title and added information about installing Release 3.1.0-797 (SP2) as the minimum supported software release to the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1. • Added caution statement to not alter the RAID configuration prior to installation or upgrade in the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5 and "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29. • Replaced "CDROM" option in the boot order to "Virtual CD/DVD" in the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5 and "Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 71. • Added verification of the BIOS boot order configuration to the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5 and "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29.

Table 1 Document Revision History (continued)

Date	Change Summary
June 18, 2013	The following changes were made: • Added note that DMP failover is disabled by default beginning in Cisco StadiumVision Director Release 3.1.0-787 (SP1) to the "Getting Started Installing or Upgrading Cisco StadiumVision Director" module on page 1 and "Upgrading the DMP Firmware" module on page 51. • Added note about not using periods "." in the DNS hostname in the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5. • Updated the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1 with the following changes: – Added changes to identify that Release 3.1.0-787 (SP1) is the minimum production version for upgrade from Release 3.0.0-433 (SP2) due to important bug fixes. – Added caution statement to advise users to independently back up any video content located in the Video Distribution Manager (VDM) when migrating from Release 3.0 to Release 3.1. – Added additional reminders that the CleanAllVDMVideoFilesTask automatically removes VDM video files from all active DMPs.

Table 1 Document Revision History (continued)

Date	Change Summary
April 10, 2013	The following changes were made: • Updated modules throughout the guide to reflect upgrade support from Release 3.0.0-433 Service Pack 2 (SP2), and no longer from Release 3.0.0-429 SP1. • Added information about contacting Cisco Technical Support to obtain the Cisco StadiumVision Director full ISO file in the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server" module on page 5. • Added information about prerequisite prior to upgrade to Release 3.1 to delete any video files that you have uploaded to the Content library but that are not in Video Distribution Manager (VDM), excluding SSC video files to prevent system restriction of removal post-upgrade. Updates were made in the "Upgrading an Existing Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1" section on page 3 and the "Best Practices" section on page 2. • Updated information about the CleanAllVDMVideoFilesTask in the "Removing Legacy Video Files From the DMP" section on page 10. • Made the following updates in the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29: – Modified the full ISO file name. – Added statement about the TUI verifiying that the ISO filename is the appropriate type for the server (SV-DIRECTOR versus SVD-REMOTE). • Added post-upgrade step to re-enable data sources and restart the External Content Integration Application in the "Appendix A: Post-Upgrade Checklist" module on page 57.
March 27, 2013	Added "Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 71 and updated references to it.
March 25, 2013	The following changes were made: • Updated the information for the init.version and init.build strings that must be manually typed for DMP firmware version 5.4 in the "Upgrading the DMP Firmware From the Management Dashboard" section on page 52. • Added caution from the Release Notes about upgrades from Release 3.0.0-429 SP1 to Release 3.1 losing language support in Release 3.1.0-510 and 3.1.0-632.

Table 1 Document Revision History (continued)

Date	Change Summary
March 20, 2013	Updated for Cisco StadiumVision Director Release 3.1.0-632. The following changes were made: • Addition of information for installing Cisco StadiumVision Director for the first time on a Platform 3 server. • Updates to the content migration procedure when upgrading from Cisco StadiumVision Director Release 3.0 SP1 to Release 3.1. • Enhancements to the NTP server configuration information.
March 6, 2013	First release of this document for Cisco StadiumVision Director Release 3.1.0-510.

Document Organization

Chapter	Description
"Getting Started Installing or Upgrading Cisco StadiumVision Director"	Provides information that you should read before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 3.1 software.
"Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server"	Describes how to install the Cisco StadiumVision Director Release 3.1 software on your newly-purchased Platform 3 server hardware from a full ISO image.
"Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2"	Describes how to upgrade a Cisco StadiumVision Director server previously installed with Release 3.0.0-433 SP2 to Cisco StadiumVision Director Release 3.0.
"Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software"	Describes how to upgrade an existing Cisco StadiumVision Directer server to a later version, including installation of service packs. This procedure is also referred to generally as an ISO upgrade to refer to both the service pack and upgrade ISO process.
"Upgrading the DMP Firmware"	Describes how to upgrade the DMP firmware on the Cisco DMP 4310G.
"Appendix A: Post-Upgrade Checklist"	Provides a checklist that is useful after you upgrade your software on a Cisco StadiumVision Director server.
"Appendix B: Port Reference"	Identifies the ports used by Cisco StadiumVision Director.

Chapter	Description
"Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.1"	Describes how to install two additional 300 GB hard drives (SV-FRU2-HD3G=) for another RAID 1 volume in the Cisco StadiumVision Director Platfrom 2 Server which are required to run Cisco StadiumVision Director Release 3.1 with a minimum of 4 drives.
"Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server"	Provides guidelines for configuring the Cisco Integrated Management Controller (CIMC) interface and performing the initial configuration, and upgrading the CIMC/BIOS firmware on the Cisco UCS C220 servers for Cisco StadiumVision Director (SV-DIR-DIRECTOR-K9, SV-PLATFORM3=).

Related Documentation

- *Release Notes for Cisco StadiumVision Director Release 3.1*
- *Cisco StadiumVision Director Server Administration Guide, Release 3.1*
- For the listing page of all Cisco StadiumVision documentation, go to:

  http://www.cisco.com/en/US/products/ps11274/tsd_products_support_series_home.html

Obtaining Documentation and Submitting 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 the What's New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Getting Started Installing or Upgrading Cisco StadiumVision Director

First Published: March 6, 2013
Revised: June 18, 2013

Read this module before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 3.1 software. It includes the following topics:

- Before You Begin, page 1
- Overview of the Installation and Upgrade Process, page 2

Before You Begin

Be sure that you understand and have met the following prerequisites before you begin to install or upgrade the Cisco StadiumVision Director software:

- Refer to the *Release Notes for Cisco StadiumVision Director Release 3.1* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Determine if you have compatible Cisco Digital Media Player (DMP) models and firmware versions installed. The DMP firmware image is not bundled with the Cisco StadiumVision Director software. You must download the firmware image separately from the software download center site for the Cisco Digital Media Player model. For more information about supported firmware versions, see the *Release Notes for Cisco StadiumVision Director Release 3.1*.
- Be sure that you have a supported browser (Google Chrome Version 24.0, Microsoft Internet Explorer Version 9, Mozilla FireFox Version 18.0.1) and Adobe Flash Player (Version 11.5.502.146) installed for access to Cisco StadiumVision Director.

Note Unless specifically identified as unsupported, other browser versions might work, but their compatibility with Cisco StadiumVision Director cannot be assured.

- Verify that the Cisco StadiumVision Director server is connected to the network using the Ethernet port eth0 on the rear panel.
- To access the Cisco Integrated Management Controller (CIMC) for the software installation, the following requirements are met:
  - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
  - You have a laptop connection with access to the Cisco StadiumVision Director server network.
  - You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
  - You have the CIMC interface login credential. The default credential is **admin** and **password**.

Note Due to the difficulty in recovering from an interrupted installation process if the Linux shell is accidentally closed or the network drops, it is highly recommended that you use a server console connection method that does not pose a risk to the success of upgrade completion if the session breaks during upgrade. You also can use a monitor and keyboard that are directly connected to the Cisco StadiumVision Director server to log into the TUI.

To learn more about the KVM console and the CIMC interface, see the Cisco UCS C-Series Integrated Management Controller Configuration guide that corresponds to your server release at: http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

- Assess your installation environment and see the "Overview of the Installation and Upgrade Process" section on page 2 for more information and to find out what modules in this guide you should follow.

Overview of the Installation and Upgrade Process

There are different tasks required to install or upgrade your Cisco StadiumVision Director server for software Release 3.1 depending on your current server environment:

- Upgrading an Existing Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1, page 3
- Installing a Platform 3 Server with Release 3.1 for the First Time, page 3
- Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.1.0-510 or Later, page 4

Note A full ISO installation on a Platform 2 server is not supported in Cisco StadiumVision Director Release 3.1. Only ISO upgrades are supported.

Upgrading an Existing Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1

Caution If you need to install additional hard drives in the Platform 2 server to meet the 4-drive minimum requirement to support Release 3.1, then you must perform the upgrade in a certain order. The physical installation of the additional drives must precede the upgrade to Release 3.1, followed by extension of the RAID volume post-upgrade, and then content migration and the remainder of the upgrade verification.

The upgrade process for an existing Platform 2 server running Cisco StadiumVision Director Release 3.0.0-433 Service Pack 2 involves the following tasks:

- Running Proof of Play reports.
- Installing two additional hard drives to meet the 4-drive minimum requirement for Release 3.1 (as required)
- Performing an ISO upgrade to Cisco StadiumVision Director Release 3.1 SP1.
- Extending the Original RAID Volume to Create a Single Group (as required for the HDD expansion)
- Migrating Content to the Release 3.1 Content Management System (CMS).
- Upgrading DMP 4310G firmware.
- Disabling DMP failover for all DMPs.
  (Disabled is the default beginning in Cisco StadiumVision Director Release 3.1.0-787 [SP1])
- Verifying the upgrade, including validating the content migration.
- Cleaning up legacy video files after migration.

For detailed information and important best practices and requirements, see the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module in this guide.

Installing a Platform 3 Server with Release 3.1 for the First Time

The installation process for a new Platform 3 server running a Cisco StadiumVision Director software release (3.1) for the first time involves the following tasks:

- Confirmation of CIMC/BIOS version and upgrade as required.
- Installation from CIMC of a full ISO image file that runs an installation program with configuration prompts for your network information.
- Disabling DMP failover for all DMPs.
  (Disabled is the default beginning in Cisco StadiumVision Director Release 3.1.0-787 [SP1])

For detailed information, see the "Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server".

Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.1.0-510 or Later

You can upgrade an existing server already running Release 3.1.0-510 or later software version using an upgrade ISO image file available from Cisco.com and using the upgrade option from the Text Utility Interface (TUI) in the Cisco StadiumVision Director software.

For detailed information, see the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software".

Installing Cisco StadiumVision Director for the First Time on a Platform 3 Server

First Published: March 20, 2013
Revised: September 30, 2013

This module describes how to install the Cisco StadiumVision Director Release 3.1 software on your newly-purchased Platform 3 server hardware from a full ISO image.

Caution New Platform 3 servers come preinstalled with a preliminary image of Cisco StadiumVision Director that is not intended for production operation. You must install the Cisco StadiumVision Director Release 3.1 software from a *full ISO* image (not an upgrade) that you downloaded from Cisco.com to be sure that you are running the released production version of Cisco StadiumVision Director Release 3.1.

NOTE: To support Release 3.1.0-797 (SP2) as the minimum supported 3.1 release on new Platform 3 servers, you must install Release 3.1.0-787 (SP1) first, and then upgrade to Release 3.1.0-797 (SP2).

This module includes the following topics:

- Prerequisites, page 5
- Installation Tasks, page 6
- What To Do Next, page 15

Prerequisites

Caution Do not alter the RAID configuration prior to installation.

Be sure that the following requirements are met before you upgrade your server:

- Your new server is installed in its production location. For more information about installing your Platform 3 hardware, see the *Cisco UCS C220 Server Installation and Service Guide.*
- You have completed the initial server setup and configured the Cisco UCS C-Series Integrated Management Controller (CIMC) interface.

To configure the CIMC, you will need an additional IP address for the server and should be prepared to change the default login and password. Be sure that the server is configured for standalone mode with the following settings:

  - DHCP—Disabled
  - NIC redundancy—None
  - Boot order—Virtual CD/DVD, HDD

For more information, see the "Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 71.

- You have the network information required to configure the Ethernet connection on the Cisco StadiumVision Director server, such as:
  - IP address (IPv4 only) and network mask

    Note The Cisco StadiumVision Director server should be configured with a static IP address or a non-expiring DHCP lease.

  - Default gateway address
  - DNS server address
  - Hostname
- The Cisco StadiumVision Director server is connected to the network and has power.
- Power on the server and verify the boot order in the BIOS (by pressing **F2** while booting) prior to installation.
- To access the Cisco Integrated Management Controller (CIMC) for the software installation, the following requirements are met:
  - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
  - You have a laptop connection with access to the Cisco StadiumVision Director server network.
  - You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
  - You have the CIMC interface login credential. The default credential is **admin** and **password**..

  Refer to the *Release Notes for Cisco StadiumVision Director Release 3.1* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

Installation Tasks

To install Cisco StadiumVision Director for the first time on a Platform 3 server, complete the following tasks:

- Downloading the ISO Files from Cisco.com, page 7 (required)
- Logging Into the CIMC Interface, page 8 (required)
- Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director, page 9 (required)
- Launching the KVM Console, page 10 (required)

- Mapping the Cisco StadiumVision Director ISO Image, page 11 (required)
- Installing the Cisco StadiumVision Director ISO Image, page 12 (required)
- Configuring the Network Setup, page 12 (required)

Downloading the ISO Files from Cisco.com

You are eligible to obtain information about how to access the Cisco StadiumVision Director full ISO file after you have purchased the proper licensing. Contact Cisco Technical Support for information about how to download the ISO file (Table 1).

Note Be sure that you choose the ISO for SV-DIRECTOR and *not* for SVD-REMOTE.

Table 1 shows the filename conventions used for full ISO images for the Cisco StadiumVision Director server.

Table 1 ISO Filename Conventions

Hardware Product ID	Filename Convention[1]
SV-PLATFORM3=	• SV-DIRECTOR-FULL-3.1.0-*nnn*.x86_64.iso • SV-DIRECTOR-FULL-3.1.0-*nnn*.x86_64.iso.md5sum

1. "*nnn*" represents the build number of the image in the file.

Be sure to download the ISO files to a location where you can access them once logged into the CIMC interface.

To verify the integrity of your upgrade file from the download, you can use a command-line or GUI utility on your laptop to calculate the checksum on the .iso file. Open the .md5sum file to compare the value that you calculated with the expected value provided in the .md5sum file. The values should match. If they do not, retry the download.

Logging Into the CIMC Interface

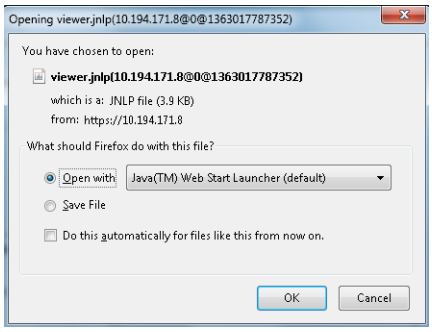
To log into the CIMC interface, complete the following steps:

Step 1 From a laptop connection with access to the Cisco StadiumVision Director server network, open a browser window and type the IP address of the CIMC interface as shown in the following example:

`https://ip-address`

Step 2 If prompted, click **OK** to open the Java viewer.jnlp as shown in Figure 1:

Figure 1 Opening viewer.jnlp File



Step 3 If a security dialog box displays, do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

b. Click **Yes** to accept the certificate and continue.

c. Confirm any additional security certificate exceptions.

Step 4 At the CIMC login screen, note the firmware version displayed (Figure 2).

Tip The firmware version is also displayed in the Cisco Integrated Management Controller (CIMC) Information box on the CIMC console after you log in.

Step 5 From the CIMC login screen, type the username and password for the CIMC interface.

Tip The default credential is **admin** and **password**. If changed during server setup, use the password that you configured.

Figure 2 CIMC Login Screen

Step 6 Click **Log In**.

Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director

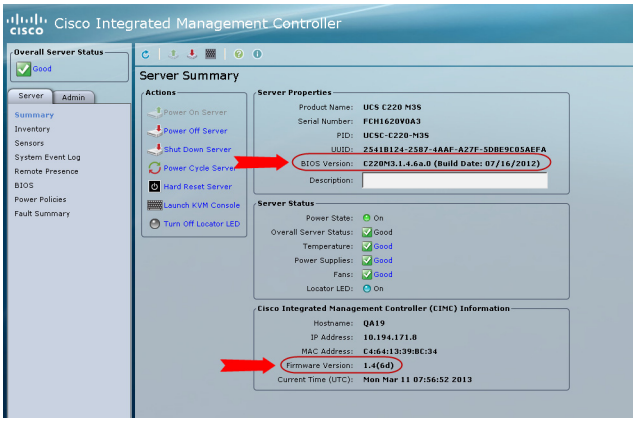
Before you begin, see the "Cisco StadiumVision Director Server Support" section of the *Release Notes for Cisco StadiumVision Director Release 3.1* to find the CIMC/BIOS versions tested for the Platform 3 server.

To verify the minimum CIMC firmware version for Cisco StadiumVision Director, complete the following steps:

Step 1 Be sure that the CIMC firmware version found on the CIMC login screen or in the CIMC console is at the minimum tested version (or later) for the Cisco StadiumVision Director release.

Figure 3 shows where the firmware version is displayed on the CIMC console for both the BIOS and CIMC firmware.

Figure 3 Firmware Version Verification From the CIMC Console



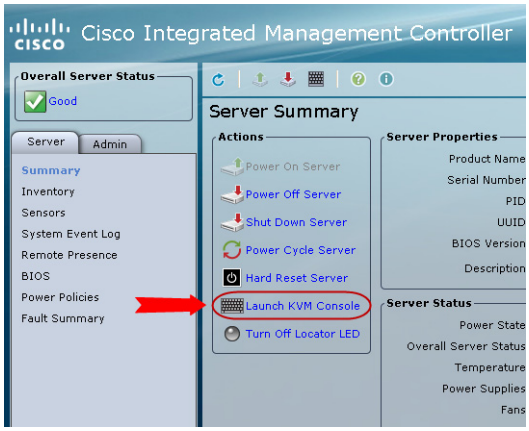
Step 2 If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to "Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 71.

Launching the KVM Console

To launch the KVM console, complete the following steps:

Step 1 From the CIMC console Actions box, click **Launch KVM Console**.

Figure 4 Launch KVM Console



Tip You can also click the keyboard in the icon bar at the top of the console to launch the KVM console.

Step 2 If a security dialog box displays, do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

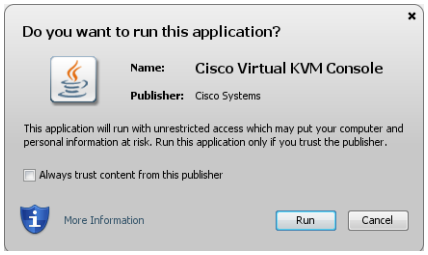
b. Click **Yes** to accept the certificate and continue.

Step 3 At the Cisco KVM Virtual Console confirmation box (Figure 5), do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

b. Click **Run**.

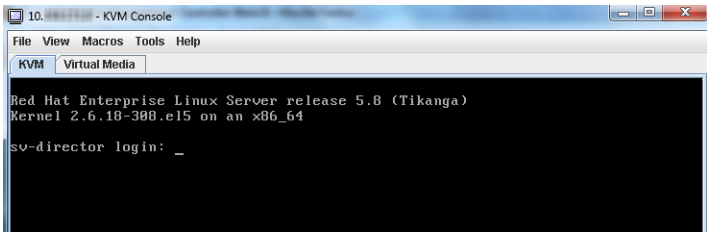
Figure 5 Cisco Virtual KVM Console Confirmation



c. Confirm any additional security certificate exceptions.

Step 4 The KVM Console window is displayed with a login prompt. Do not log in (Figure 6).

Figure 6 Cisco KVM Virtual Console Login Screen



Mapping the Cisco StadiumVision Director ISO Image

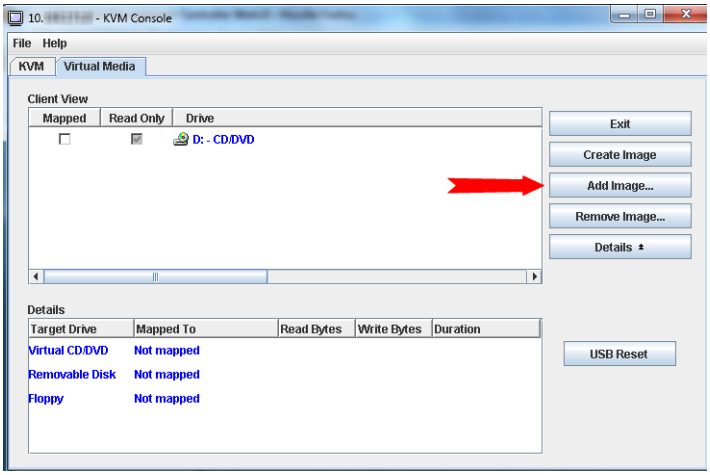
Note This step requires that you have downloaded the Cisco StadiumVision Director full ISO image file for the Platform 3 server from Cisco.com and it is accessible from the computer that you are using to log into the CIMC interface.

To map the Cisco StadiumVision Director ISO image, complete the following steps:

Step 1 From the KVM console window, click the **Virtual Media** tab.

Step 2 From the Virtual Media screen, click **Add Image** (Figure 7).

Figure 7 Virtual Media Screen



Step 3 Navigate to the location of the ISO file that you downloaded and click **Open**.

Note CIMC can experience slow performance. If slow performance occurs, clear the browser cache.

Step 4 In the Client View box, mark the checkbox under the Mapped column to select the ISO source.

Step 5 Confirm that the Virtual CD/DVD has been added under the Virtual Media tab, Virtual CD/DVD.

Step 6 In the Details box, double-click on Virtual CD/DVD, and observe the read bytes counter increasing (refreshes read bytes).

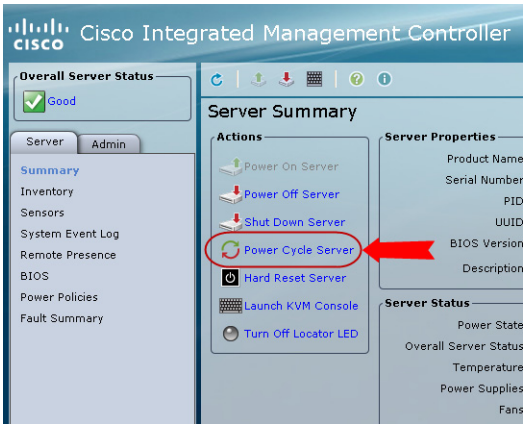
Step 7 Click the KVM tab and minimize the window but do not exit.

Installing the Cisco StadiumVision Director ISO Image

To install the Cisco StadiumVision Director ISO image, complete the following steps:

Step 1 In the Actions box on the CIMC console, click Power Cycle Server (Figure 8).

Figure 8 Power Cycle Server From the CIMC Console



Step 2 At the confirmation prompt, click **OK**.

Step 3 From the KVM console, observe the start of the installation process.

Configuring the Network Setup

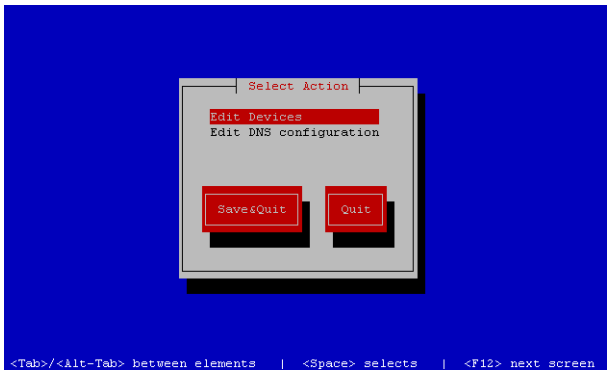
To configure the network setup, complete the following steps:

Step 1 When the Linux Setup Agent window appears in the KVM console, select **Network Configuration** and press **Enter**.

Tip The Linux Setup Agent window will be available for 60 minutes before closing. If you miss responding to the network setup as part of the ISO installation, you can go to the TUI **Main Menu > System Settings > Network Settings** to complete the same network configuration. However, you will also need to manually edit the hosts file, selected from the Network Settings submenu.

Step 2 In the Select Action screen (Figure 9), select **Edit Devices** and press **Enter**.

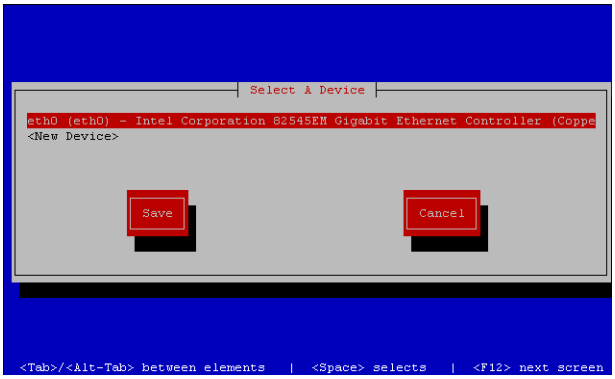
Figure 9 Select Action Screen



Tip If you notice what appears to be stray characters in the Linux interface, verify that your SSH client is using the UTF-8 character set translation.

Step 3 In the Select a Device screen (Figure 10), select **eth0** and press **Enter**.

Figure 10 Select a Device Screen

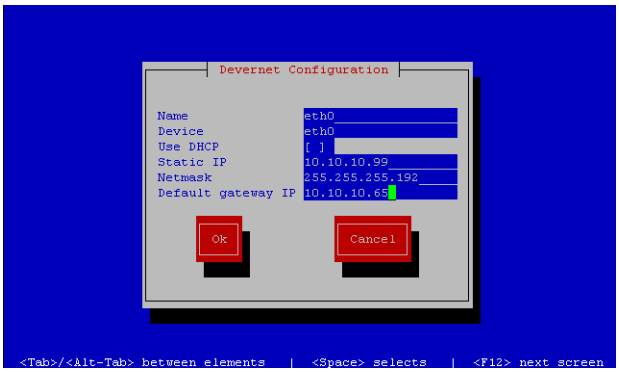


The Ethernet Configuration screen is displayed.

Note The Linux screen is mislabeled “Devernet Configuration.”

Step 4 In the Ethernet Configuration screen (Figure 11), do the following:

Figure 11 Devernet Configuration Screen



a. Press the Tab key until the cursor is positioned on the Static IP address line.

b. Press the backspace key to go to the beginning of the line and type in the IPv4 address of the Cisco StadiumVision Director Server.

Note This should be a different IP address than what you configured for the CIMC interface.

c. Press the tab key to go to the Netmask line. Type the network mask for the IPv4 address.

d. (Optional) In the Default gateway IP line, type the address of the default gateway of your network.

Step 5 When configuration of all options is complete, press the Tab key until the **Ok** button is selected and press **Enter**.

You return to the Select a Device screen.

Step 6 Press the Tab key until the **Save** button is highlighted and press **Enter**.

You return to the Select Action screen.

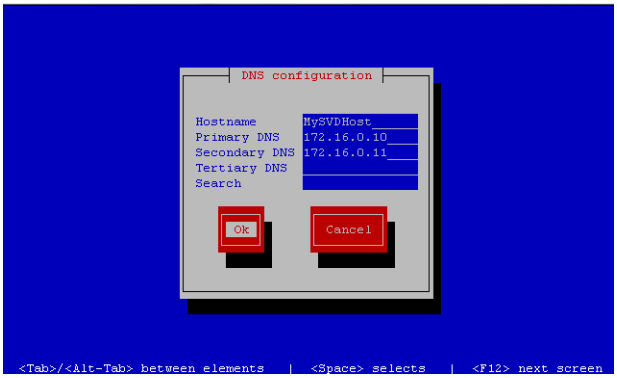
Step 7 Press the down arrow key to select the **Edit DNS configuration** option and press **Enter**.

The DNS configuration screen is displayed.

Step 8 In the DNS configuration screen (Figure 12), select and configure the Hostname and one or more DNS Server IP addresses.

Note Do not use hostnames that contain periods "." within the name.

Figure 12 DNS Configuration Screen



Step 9 Press the Tab key until the **Ok** button is selected and press **Enter**.

You return to the Select Action screen.

Step 10 In the Select Action screen, press the Tab key until the **Save&Quit** button is selected and press **Enter**.

What To Do Next

After you have installed the Cisco StadiumVision Director software, log into the TUI and do the following:

- Configure the system date and time.
- Configure the time zone.
- Restart the Cisco StadiumVision Director software.

See the "Cisco StadiumVision Director Server Text Utility Interface" module of the *Cisco StadiumVision Director Server Administration Guide* to complete initial setup of the server.

Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2

First Published: March 6, 2013
Revised: January 17, 2014

This module describes how to upgrade a Cisco StadiumVision Director Platform 2 server previously installed with a minimum of Release 3.0.0-433 Service Pack 2 to Cisco StadiumVision Director Release 3.1.0-787 (SP1), which contains important bug fixes. After upgrade to Release 3.1.0-787, an upgrade to Release 3.1.0-797 (SP2) is required to install the minimum supported software release for Cisco StadiumVision Director.

Caution A Cisco StadiumVision Director system that is using language support from Release 3.0.0-433 (SP2), will lose that support if upgraded to Release 3.1.0-632. Language support is introduced in Release 3.1.0-787 (SP1).

Contents

- Best Practices, page 2
- Prerequisites, page 3
- Upgrade Tasks, page 4
- Verifying the Upgrade, page 8
- Validating the Content Migration, page 8
- Cleaning Up Legacy Video Files After Migration, page 9

Best Practices

Before you begin upgrading a Cisco StadiumVision Director server from Release 3.0.0-433 Service Pack 2 to Release 3.1.0-787 Service Pack 1 software, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.

Note If your site deploys a large amount of video content, the content migration process might take up to several hours to complete.

- Refer to the *Release Notes for Cisco StadiumVision Director Release 3.1* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you plan to upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.
- To streamline the content migration process and to be sure that all relevant video content is migrated to the unified Content Management System (CMS) in Cisco StadiumVision Director Release 3.1, perform the following tasks:

Caution Be sure that you independently back up any video content located in the Video Distribution Manager (VDM). Cisco StadiumVision Director does not back up VDM content as part of the backup process.

  - Check scripts for any video content with 0 bytes. If this video content is still used, re-import the video using VDM and confirm the content.
  - Additionally, identify any video content that is not currently in use but that you still want to retain. Either upload and activate that content in VDM prior to upgrade, or be prepared to independently import the video content post-upgrade to Release 3.1.
  - From the Control Panel Content interface, look for any external content that is no longer used and delete it. This will eliminate a potentially lengthy process of importing a video that is no longer in use.

Note When you migrate content from Release 3.0 to Release 3.1 after the upgrade process, 0-byte files are ignored. After you have fully verified the content migration, there are steps that can be taken do VDM file cleanup on the Cisco StadiumVision Director server and DMPs.

- Perform a backup and restore of the primary and secondary servers, and then promote the secondary server:
  - Perform a backup of the currently active primary server.
  - Restore the backup data onto the standby secondary server. If using VDM, then you will need to reimport and activate the video files.

Note The config service must be running on the secondary server to do the restore.

For more information about performing a backup and restore on a Cisco StadiumVision Server running release 3.0, see the *Backing Up and Restoring Cisco StadiumVision Director Servers, Release 3.0* guide.

- Promote the secondary server to active.

  For more information about promoting a secondary server to active, see the *Cisco StadiumVision Director Server Redundancy, Release 3.0* guide.

- Access the promoted secondary server to perform the upgrade.
- Due to the difficulty in recovering from an interrupted installation process if the Linux shell is accidentally closed or the network drops, it is highly recommended that you use a server console connection method that does not pose a risk to the success of upgrade completion if the session breaks during upgrade.

  This can be done using a monitor and keyboard that are directly connected to the Cisco StadiumVision Director server to log into the TUI, or through a remote connection with access to the Cisco StadiumVision Director network and using the CIMC interface to log into the TUI.

Prerequisites

Before the Platform 2 server upgrade, be sure that the following requirements are met:

- Be sure that the Cisco StadiumVision Director Platform 2 server meets the following minimum requirements:
  - Two additional 300 GB hard drives are installed for a total of four required drives for Release 3.1. Contact your Cisco Systems sales representative for more information about how to obtain additional hard drives.

    For information about how to install hard drives to support Release 3.1, see "Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.1" module on page 63.
  - The software is at the minimum release level of Release 3.0.0-433 Service Pack 2. If the server is not at the minimum release level, see the "Using the TUI Upgrade Utility to Update an Existing Release 3.0 Server" module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.0*.
  - The Platform 2 server Unified Computing System (UCS) Server Firmware is at version 1.4(2) to avoid problems powering off the server hardware.

    For more information about how to verify and upgrade, see the "Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server" module f the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.0*.
- Be sure that you have compatible Cisco Digital Media Player (DMP) models and firmware versions.

  For more information about DMP hardware and software requirements, see the *Release Notes for Cisco StadiumVision Director Release 3.1*.

- To access the Cisco Integrated Management Controller (CIMC) for the TUI software upgrade, the following requirements are met:
  - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
  - You have a laptop connection with access to the Cisco StadiumVision Director server network.
  - You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
  - You have the CIMC interface login credential. The default is **admin/password**.

Note You also can use a monitor and keyboard that are directly connected to the Cisco StadiumVision Director server to log into the TUI.

Upgrade Tasks

To upgrade your Cisco StadiumVision Director server from Release 3.0 to 3.1, complete the following tasks:

- Running Proof of Play Reports, page 4 (as required)
- Upgrading the Software From Release 3.0 SP2 to Release 3.1, page 4 (required)
- Extending the Original RAID Volume to Create a Single Group, page 5 (as required)
- Migrating Content to the Release 3.1 CMS, page 5 (required)
- Upgrading the DMP Firmware, page 7 (as required)
- Staging the Flash Template, page 8 (required)
- Deploying Global DMP Settings, page 8 (required)

Running Proof of Play Reports

Before you perform the upgrade from Release 3.0 to 3.1, be sure that you have processed any outstanding Proof of Play reports. If you do not run these reports before the upgrade, the data will be lost.

For more information, see the *Cisco StadiumVision Proof of Play* module.

Upgrading the Software From Release 3.0 SP2 to Release 3.1

The upgrade from Cisco StadiumVision Director Release 3.0 to Release 3.1 is performed as an ISO upgrade using the Text Utility Interface (TUI).

For more information about how to perform the ISO upgrade, see the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29.

Note Return to this module after the TUI upgrade to complete the content migration, upgrade verification, and content validation tasks specific to the 3.0-to-3.1 environment.

Extending the Original RAID Volume to Create a Single Group

Note This task is only required if you had to install additional hard drives to meet the minimum hard drive requirement on the Platform 2 server for Cisco StadiumVision Director Release 3.1 as described in the "Prerequisites" section on page 3.

For information about running this task, see the "Extending the Original RAID Volume to Create a Single Group" section on page 68. Return to this module after extending the RAID volume to complete migration of content to the Release 3.1 CMS.

Migrating Content to the Release 3.1 CMS

Note The tasks in this section are performed after you upgrade the software to Release 3.1.

This section includes the following topics:

- Preparing the Release 3.0 Video Content for Migration, page 5 (required)
- Running the Content Migration, page 7 (required)

Preparing the Release 3.0 Video Content for Migration

The Migration Preparation Wizard analyzes the release 3.0 content for the following problems:

- **Missing external video content**—This could be because the video no longer exists in VDM, or both the name and URL were changed in the Control Panel. This list is informational only so that you can correct the problem, which might require recreating/updating the playlists that reference the content after uploading the missing video files. Missing video files will also show up in the system without thumbnails.
- **Detection of a rename of external video content**—This is due to a mismatch found between the name of the external video content file and the name of the video content derived from the reference URL, which will prevent the video from being migrated.

  To avoid having to create new content and update all referenced playlists, you should accept the rename to revert the file name to match the URL. You can replace the content after migration.
- **Detection of duplicate references to the same video content**—This will prevent the content from being migrated. This is likely caused by uploading a new version of a video file of the same name and activating it in VDM.

  To allow the content to be migrated, accept merging of the duplicate content. All playlist references are updated to use the same content, and the duplicate entries are deleted. If not merged, duplicate content will appear in the system without thumbnails.

To migrate release 3.0 video content to the release 3.1 CMS, complete the following steps:

Step 1 Log into the TUI by doing the following:

a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the secondary Cisco StadiumVision Director server using the IP address for your server.

b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.

Step 2 From the Main Menu, go to the **StadiumVision Server Administration > Content migration** menu.

Step 3 Select **Migration Preparation Wizard**.

The migration preparation process starts.

Step 4 If no exceptions for the content to be migrated are found, the following message is displayed:

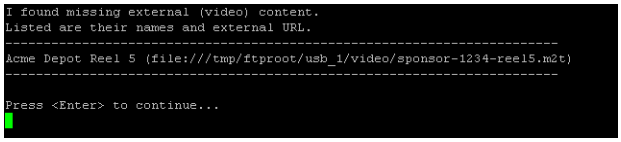
```
I did not detect any issues with your external content.
```

Skip Step 5 and go on to the "Running the Content Migration" section on page 7.

Step 5 If any video content exceptions are found, one or more of the following screens are displayed:

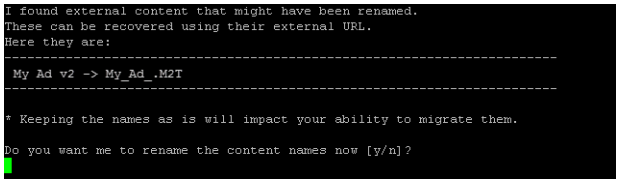
a. If missing video content is found, an informational screen is displayed with the list of files (Figure 1). After noting the content, press **Enter** to continue with the migration.

Figure 1 Missing Video Content



b. If a rename of video content is found, a screen appears listing that content (Figure 2). To migrate the content, the system must rename the video file to match the name in the reference URL. Type **y** to rename the content so that it can be migrated.

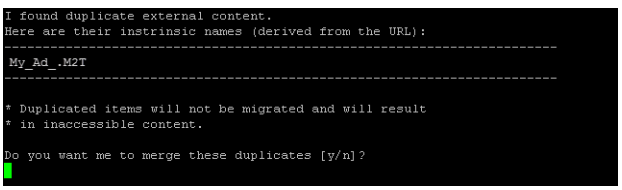
Figure 2 Renamed Video Content



After you type y, the screen returns the confirmation message "Done" when complete. Press **Enter** to continue.

c. If duplicate content references are found, a screen appears listing that content (Figure 3). Type **y** to merge the content and continue with the migration.

Figure 3 Duplicate Video Content



Messages are displayed on the screen as the content is processed, and the message "Completed merging the duplicate content" is displayed. Press **Enter** to continue.

d. After any exception screens are processed, you return to the Content migration menu. Go on to the "Running the Content Migration" section on page 7.

Running the Content Migration

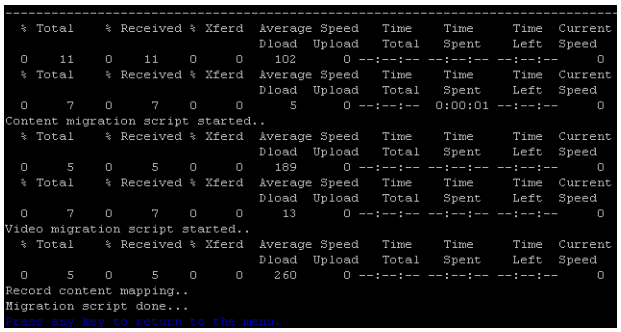
Caution If your site deploys a large amount of video content, the content migration process might take up to several hours to complete. During this time do not restart any services or reboot the server.

To run the content migration, complete the following steps:

Step 1 From the Content migration menu, select **Run migration script**.

Observe the processing of the migration script and look for the "Migration script done" message (Figure 4).

Figure 4 Content Migration Start



Step 2 Press any key to return to the Content Migration menu.

Step 3 Return to the Main Menu and exit the TUI.

Upgrading the DMP Firmware

Cisco StadiumVision Director supports DMP-4310G Version 5.3.4. from Release 3.0 for backward compatibility, as well as the updated DMP firmware version 5.4.

For more information about how to perform the upgrade, see the "Upgrading the DMP Firmware" module on page 51.

Staging the Flash Template

To be sure that any changes that might have been made to the Cisco StadiumVision Director Flash Template (.swf file) are deployed to the DMPs, complete the following steps:

Step 1 Go to the Management Dashboard.

Step 2 From the DMP and TV Controls dashboard drawer, navigate to and select the following command: **DMP and TV Controls > DMP Install > Stage Template**.

Step 3 Select all of the DMP devices where the command should be applied.

Step 4 Click the play button to run the command on the selected devices.

Deploying Global DMP Settings

To apply the global MIB variable settings to all DMPs, complete the following steps:

Step 1 Go to the Management Dashboard.

Step 2 From the DMP and TV Controls dashboard drawer, navigate to and select the following command: **DMP and TV Controls > Global > Global DMP Settings**.

Step 3 Select all of the DMP devices where the command should be applied.

Step 4 Click the play button to run the command on the selected devices.

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

Step 1 Complete the verification tasks as described in the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29.

Step 2 Use the "Appendix A: Post-Upgrade Checklist" module on page 57 to be sure that you have completed the required verification steps.

Validating the Content Migration

Note This step is included as part of the "Appendix A: Post-Upgrade Checklist" module on page 57.

To validate the content migration, complete the following steps:

Step 1 Log into Cisco StadiumVision Director as an administrator.

Step 2 Go to **Control Panel** > **Content**.

Step 3 Verify the content:

- If no content is missing, go on to Step 4.
- If you find missing content (empty icons or content without icons), do the following:
  - Go to the Management Dashboard and verify that the CMS server is running. If the CMS is not running, restart the CMS service and re-verify the content:

    Log into the TUI and go to **Main Menu** > **Services Control** > **Content Management System (CMS)** > **Start Service**.
  - If the missing content is not resolved, restart the Content Migration script and re-verify the content:

    Log into the TUI and go to **Main Menu** > **StadiumVision Server Administration** > **Content Migration** > **Run migration script**.

Step 4 Go to **Control Panel** > **Control** and stage content for all scripts.

Note If staging fails on the DMP due to lack of storage space run the "CleanAllVDMVideoFilesTask" from the Management Dashboard. This task automatically removes VDM video files from all active DMPs. For more information, see the "Cleaning Up Legacy Video Files After Migration" section on page 9.

Cleaning Up Legacy Video Files After Migration

Caution Perform video file clean up only after you have validated the success of your video file migration and scripts. If you clean up files before you run the content preparation wizard and migration, you will get a long list of missing files and invalidate the content migration.

This section describes how to clean up legacy VDM video files from the Cisco StadiumVision Director server and from the DMP.

Removing Legacy Video Files From the Cisco StadiumVision Director Server

To remove legacy video files from the Cisco StadiumVision Director server after migration, complete the following steps:

Step 1 Log into the TUI by doing the following:

a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the primary Cisco StadiumVision Director server using the IP address for your server.

b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.

Step 2 From the Main Menu, go to the **StadiumVision Server Administration > Content migration** menu.

Tip To navigate through the TUI menus you must type the character that corresponds to the menu area where you want to go (a, b, c, and so on) and press **Enter**.

To return to other menus, you must back out of the hierarchy of menus using one of the indicated keys to return you to prior menus.

Step 3 Select **Remove legacy (VDM) video** files.

Step 4 At the confirmation prompt, press **Y** to continue.

Step 5 Press any key to return to the Content Migration menu.

Step 6 Return to the Main Menu and exit the TUI.

Removing Legacy Video Files From the DMP

Note If you are incrementally adding DMPs to the Release 3.1 system that were previously operating with earlier releases of Cisco StadiumVision Director, then you will need to re-run the CleanAllVDMVideoFilesTask. This task automatically removes VDM video files from all active DMPs.

To remove legacy video files from the DMP after migration, complete the following steps:

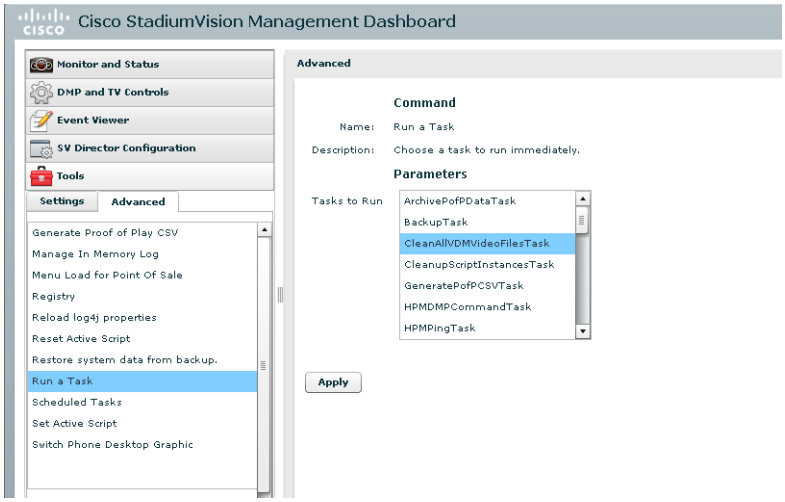
Step 1 Log into Cisco StadiumVision Director as an administrator.

Step 2 Go to the **Management Dashboard**.

Step 3 Go to **Tools > Advanced > Run a Task**.

Step 4 Select the **CleanAllVDMVideoFilesTask** (Figure 5).

Figure 5 CleanAllVDMVideoFilesTask in the Management Dashboard



Step 5 Click **Apply**.

Legacy VDM video files are automatically removed from all active DMPs.

What to Do Next

Caution Due to important bug fixes, Cisco StadiumVision Director Release 3.1.0-797 (SP2) is the minimum supported production software release.

After you have completed your upgrade to Release 3.1.0-787 (SP1), install the upgrade to Release 3.1.0-797 (SP2) using the instructions found in the "Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software" module on page 29.

Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software

First Published: March 6, 2013
Revised: January 17, 2014

Note If you are upgrading an existing Cisco StadiumVision Director server from Release 3.0 SP2 to Release 3.1, see the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1 first.

This module describes how to upgrade an existing server already running Cisco StadiumVision Director, including installation of service packs. This procedure is also referred to generally as an *ISO upgrade* to refer to both the service pack and upgrade ISO process.

This module includes the following topics:

- Best Practices, page 29
- Prerequisites, page 30
- Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server, page 31
- Upgrade Tasks, page 31
- Verifying the Upgrade, page 40
- What to Do Next, page 50

Best Practices

Caution Do not alter the RAID configuration prior to upgrade.

Before you begin upgrading an existing Cisco StadiumVision Director server, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.

- Refer to the *Release Notes for Cisco StadiumVision Director Release 3.1* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.
- Perform a backup and restore of the primary and secondary servers:
  - Perform a backup of the currently active primary server.
  - Restore the backup data onto the standby secondary server.

  Note The config service must be running on the secondary server to do the restore.

  For more information about performing a backup and restore on a Cisco StadiumVision Director Server, see the "Backing Up and Restoring Cisco StadiumVision Director Servers" module of the *Cisco StadiumVision Director Server Administration Guide*.
- Promote the secondary server to primary.

  For more information about promoting a secondary server to primaryin Release 3.1, see the "Configuring Failover Between Redundant Cisco StadiumVision Director Servers" module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.1*.
- Access the promoted secondary server to perform the upgrade.
- Verify the boot order in the BIOS (by pressing **F2** while booting) prior to upgrading; the virtual DVD should be the primary boot device for the Platform 3 server.
- Due to the difficulty in recovering from an interrupted installation process if the Linux shell is accidentally closed or the network drops, it is highly recommended that you use a server console connection method that does not pose a risk to the success of upgrade completion if the session breaks during upgrade.

  This can be done using a monitor and keyboard that are directly connected to the Cisco StadiumVision Director server to log into the TUI, or through a remote connection with access to the Cisco StadiumVision Director network and using the CIMC interface to log into the TUI.

Prerequisites

Be sure that the following requirements are met before you upgrade your server:

- Your server is running a minimum of Cisco StadiumVision Director Release 3.1.0-510 or higher.
- If you are upgrading your server from Release 3.0, you are following the requirements and tasks described in the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module in this guide.
- You have the IP address for the Cisco StadiumVision Director server where you want to upload the ISO upgrade image. You will need to use this information as part of the URL to access the ISO upload utility.
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the *Cisco StadiumVision Release Notes for Release 3.1*.

- You have an installer account on the Cisco StadiumVision Director server.
- To access the Cisco Integrated Management Controller (CIMC) for the TUI software upgrade, the following requirements are met:
  - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
  - You have a laptop connection with access to the Cisco StadiumVision Director server network.
  - You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
  - You have the CIMC interface login credential. The default is admin/password.

Note You also can use a monitor and keyboard that are directly connected to the Cisco StadiumVision Director server to log into the TUI.

Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server

The ISO upgrade procedure for Cisco StadiumVision Director includes the following tasks:

1. Downloading an ISO service pack or upgrade file from the software download site on Cisco.com.
2. Uploading the ISO file from your laptop to the Cisco StadiumVision Director server using the upload utility through your browser.
3. Installing the ISO image using the upgrade utility in the Text Utility Interface (TUI).

ISO Upgrade Files

You can store multiple ISO upgrade files on a Cisco StadiumVision Director server. The files will be displayed with a sequence number and the ISO filename in the TUI upgrade utility for you to select which file to install.

Disk Maintenance

There is no automatic aging of ISO upgrade files, but Cisco StadiumVision Director Release 3.1 introduces a utility to delete ISO upgrade files in the TUI.

The Management Dashboard has a gauge for % Disk Utilization, or you can use the TUI to get file system usage.

Upgrade Tasks

To upgrade your Cisco StadiumVision Director server, complete the following tasks:

- Downloading ISO Upgrade Files from Cisco.com, page 32 (required)
- Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server, page 33 (required)
- Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server, page 37 (required)

- Staging the Flash Template, page 39 (required)
- Deploying Global DMP Settings, page 40 (required)
- Verifying the Upgrade, page 40 (required)

Downloading ISO Upgrade Files from Cisco.com

Be sure to download the upgrade files to a location, such as a laptop computer, where you can access them for installation onto the Cisco StadiumVision Director server.

To download an ISO upgrade file, complete the following steps:

Step 1 Go to the Cisco StadiumVision Director software download site at:

http://software.cisco.com/download/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.1.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Note This site page is also available from the Cisco StadiumVision Director product support page by clicking **Download Software > Cisco StadiumVision Director**.

Step 2 Select the ISO upgrade or service pack file (as available), and optionally the companion MD5 checksum file, and download them.

Table 1 shows the filename conventions used for ISO upgrades.

Note Be sure that you choose the ISO for SV-DIRECTOR and *not* for SVD-REMOTE. The TUI will verify the filenaming to be sure that the ISO that you are uploading is for SV-DIRECTOR.

Table 1 ISO Upgrade Filename Conventions

Hardware Product ID	Filename Convention[1]
SV-DIRECTOR-K9 or SV-PLATFORM2= SV-PLATFORM3=	• SV-DIRECTOR-UPGRADE-3.1.0-*nnn*.x86_64.iso • SV-DIRECTOR-UPGRADE-3.1.0-*nnn*.x86_64.iso.md5sum

1. "*nnn*" represents the build number of the image in the file.

You can download the files using one of the following methods:

- Download both files at one time—Select each file and click **Add to Cart**. Then at the top of the download page, click the "Download Cart (2 items)" link.
- Download each file independently—Click the **Download Now** button in the file selection box for each file.

Step 3 (Optional) To verify the integrity of your upgrade file from the download, you can use a command-line or GUI utility on your laptop to calculate the checksum on the .iso file. Open the .md5sum file to compare the value that you calculated with the expected value provided in the .md5sum file.

The values should match. If they do not, retry the download.

Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server

After you have downloaded the ISO upgrade file from Cisco.com, you need to upload the file to the Cisco StadiumVision Director server using a URL from a browser to access the ISO uploader utility. Once you have uploaded the software to the server, then you will use the TUI to install the upgrade image.

Prerequisites

Be sure that you know the IP address of the Cisco StadiumVision Director server where you want to upload the file, and you have a supported browser version for Cisco StadiumVision Director.

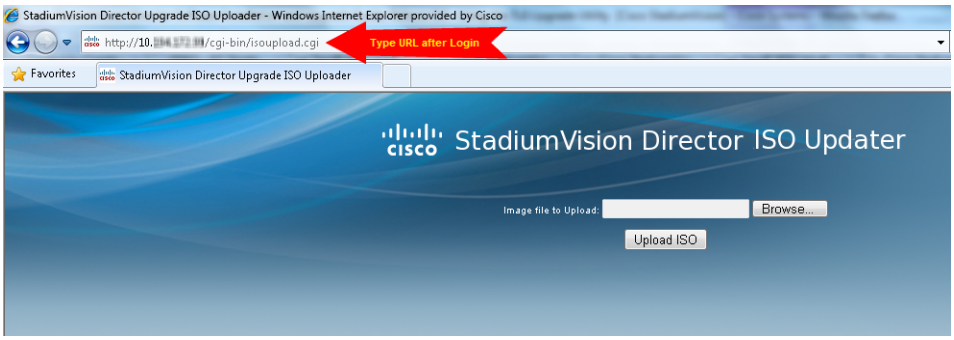
To upload an ISO upgrade file to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Log into Cisco StadiumVision Director as an administrator.

Step 2 From your browser, go to the following URL, where *x.x.x.x* is replaced by the IP address of the server where you want to upload the upgrade software (Figure 1):

`http://`*`x.x.x.x`***`/cgi-bin/isoupload.cgi`**

Figure 1 ISO Updater Utility



Step 3 Click **Browse** (Figure 1).

Step 4 From the File Upload dialog box, navigate to the location of the ISO upgrade file that you downloaded from Cisco.com. Select the file that you want to upload and click **Open**.

Step 5 Click the **Upload ISO** button (Figure 2). The file is sent to the server.

Caution The upload might take several minutes. Do *not* refresh or reload the ISO Updater page while the upload process is running. Any interruption will corrupt the ISO image being uploaded.

Figure 2 ISO File Selection and Upload

When the ISO upload is complete, one of the following occurs:

- When the image is validated and uploaded successfully, a message is displayed stating that the ISO image has been uploaded.
- The image upload failed for some reason and you will need to retry the upload again.

Logging Into the CIMC Interface

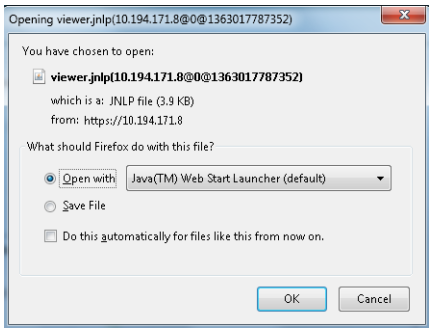
To log into the CIMC interface, complete the following steps:

Step 1 From a laptop connection with access to the Cisco StadiumVision Director server network, open a browser window and type the IP address of the CIMC interface as shown in the following example:

`https://ip-address`

Step 2 If prompted, click **OK** to open the Java viewer.jnlp as shown in Figure 3:

Figure 3 Opening viewer.jnlp File



Step 3 If a security dialog box displays, do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

b. Click **Yes** to accept the certificate and continue.

c. Confirm any additional security certificate exceptions.

Step 4 At the CIMC login screen, note the firmware version displayed (Figure 4).

Tip The firmware version is also displayed in the Cisco Integrated Management Controller (CIMC) Information box on the CIMC console after you log in.

Step 5 From the CIMC login screen, type the username and password for the CIMC interface.

Tip The default credential is **admin** and **password**. If changed during server setup, use the password that you configured.

Figure 4 CIMC Login Screen

Step 6 Click **Log In**.

Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director

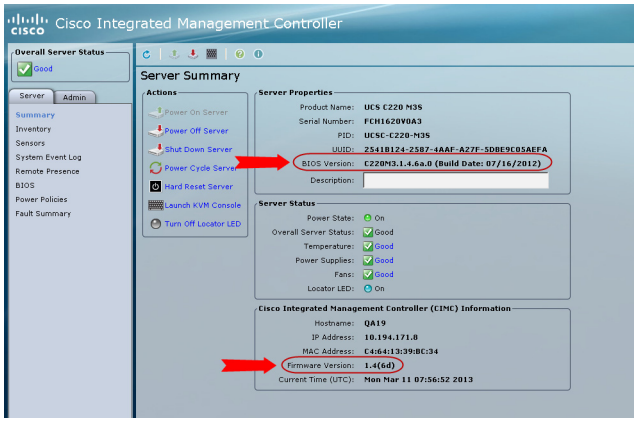
Before you begin, see the "Cisco StadiumVision Director Server Support" section of the *Release Notes for Cisco StadiumVision Director Release 3.1* to find the CIMC/BIOS versions tested for your platform.

To verify the minimum CIMC firmware version for Cisco StadiumVision Director, complete the following steps:

Step 1 Be sure that the CIMC firmware version found on the CIMC login screen or in the CIMC console is at the minimum tested version (or later) for the Cisco StadiumVision Director release.

Figure 5 shows where the firmware version is displayed on the CIMC console for both the BIOS and CIMC firmware.

Figure 5 Firmware Version Verification From the CIMC Console for a Platform 3 Server



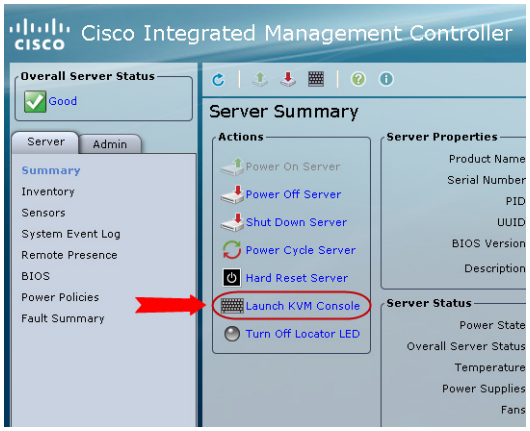
Step 2 If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to the "Updating the BIOS and CIMC Firmware" section of the "Installing the Server" module in the *Cisco UCS C220 Server Installation and Service Guide*.

Launching the KVM Console

To launch the KVM console, complete the following steps:

Step 1 From the CIMC console Actions box, click **Launch KVM Console**.

Figure 6 Launch KVM Console



Tip You can also click the keyboard in the icon bar at the top of the console to launch the KVM console.

Step 2 If a security dialog box displays, do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

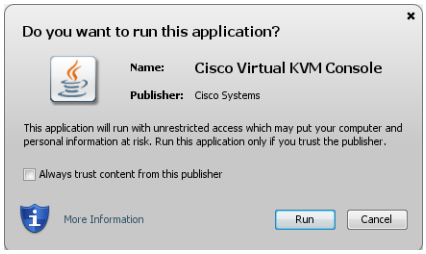
b. Click **Yes** to accept the certificate and continue.

Step 3 At the Cisco Virtual KVM Console confirmation box (Figure 7), do the following:

a. (Optional) Select the checkbox to accept all content from Cisco.

b. Click **Run**.

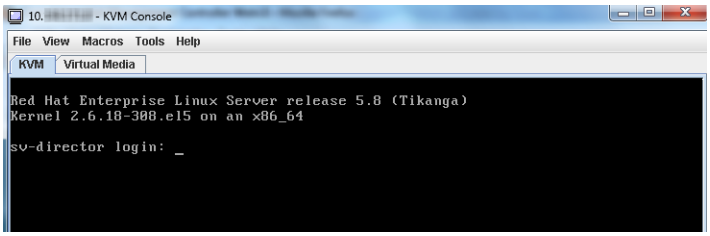
Figure 7 Cisco Virtual KVM Console Confirmation



c. Confirm any additional security certificate exceptions.

Step 4 The KVM Console window is displayed with a login prompt (Figure 8).

Figure 8 Cisco KVM Virtual Console Login Screen



Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server

To install the ISO upgrade image on the Cisco StadiumVision Director server, complete the following steps:

Step 1 Do one of the following to run a secure login to the Cisco StadiumVision Director server:

- Using a directly-connected computer and KVM cable, access the console of the Cisco StadiumVision Director server.

  or

- Log into the CIMC and launch the virtual KVM console.

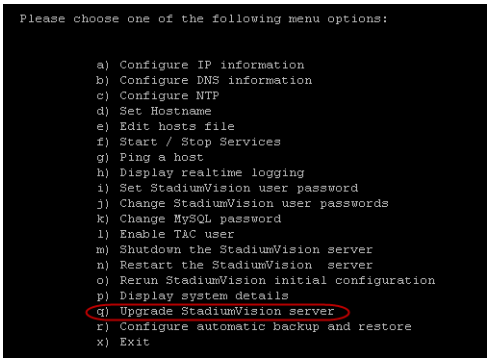
Step 2 When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.

Step 3 From the Main Menu, do the following:

- **For upgrades from Release 3.0:**

  From the TUI Main Menu, select the **Upgrade StadiumVision Server** option (type **q** and press **Enter**) (Figure 9):

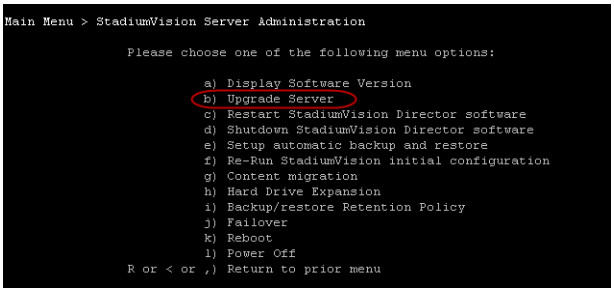
Figure 9 TUI Main Menu Option for Server Upgrade—Release 3.0



- **For upgrades from Release 3.1:**

  From the TUI Main Menu, go to the StadiumVision Server Administration menu. Select the Upgrade Server option (type **b** and press **Enter**) (Figure 10):

Figure 10 TUI StadiumVision Server Administration Menu Option for Server Upgrade—Release 3.1



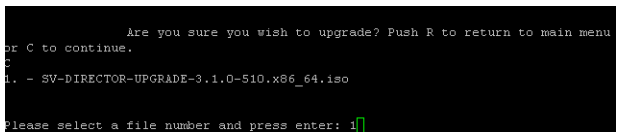
Step 4 When the upgrade configuration confirmation prompt appears, type **c** to continue (Figure 11):

Figure 11 TUI Upgrade Configuration Confirmation

Step 5 All of the ISO upgrade files that you have uploaded are displayed with a sequence number and the image name. Type the sequence number that corresponds to the image that you want to install, and press **Enter**.

Figure 12 shows an example of selection of the first upgrade file for installation.

Figure 12 ISO Upgrade Image File List

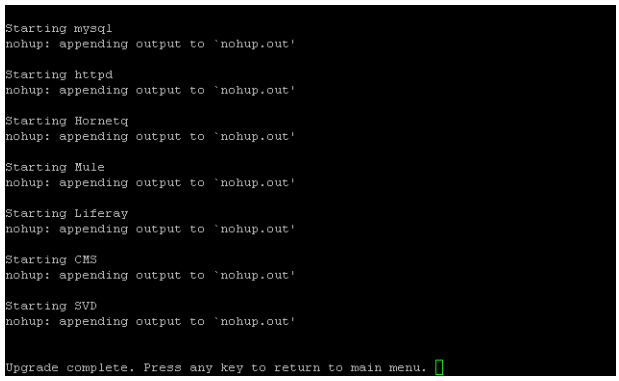


The upgrade process begins.

Caution Wait until the upgrade process completes. *Do not* close the terminal while the upgrade is in progress. You will get notification once the installation is complete.

Step 6 When the "Upgrade complete" message appears, press any key. (Figure 13):

Figure 13 End of ISO Upgrade Process



Step 7 From the StadiumVision Server Administration menu, select Reboot.

Step 8 (**For systems upgrading from Release 3.0 SP2 only**) Return to the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1 to continue with the steps required to migrate content to the release 3.1 CMS.

Staging the Flash Template

To be sure that any changes that might have been made to the Cisco StadiumVision Director Flash Template (.swf file) are deployed to the DMPs, complete the following steps:

Step 1 Go to the Management Dashboard.

Step 2 From the DMP and TV Controls dashboard drawer, navigate to the following command path: **DMP and TV Controls > DMP Install > Stage Template**.

Step 3 Select all of the DMP devices where the command should be applied.

Step 4 Click the play button to run the command on the selected devices.

Deploying Global DMP Settings

To apply the global MIB variable settings to all DMPs, complete the following steps:

Step 1 Go to the Management Dashboard.

Step 2 From the DMP and TV Controls dashboard drawer, navigate to the following command path: **DMP and TV Controls > Global > Global DMP Settings**.

Step 3 Select all of the DMP devices where the command should be applied.

Step 4 Click the play button to run the command on the selected devices.

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 40 (required)
- Importing the Security Certificate, page 41 (required)
- Logging Into Cisco StadiumVision Director, page 42 (required)
- Verifying the Control Panel and Other Menus, page 44 (required)
- Verifying that Services are Running, page 45 (required)
- Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check, page 45 (required)
- Verifying DMPs, Groups, and Zones in the Management Dashboard, page 47 (required)
- Verifying the Multicast Configuration, page 47 (required)
- Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 48 (required if using Quest for commerce integration)

Clearing the Browser Cache

After you perform a Cisco StadiumVision Director software upgrade, you must clear the browser cache to be sure that you are viewing the latest version of Cisco StadiumVision Director.

To clear the browser cache in Mozilla FireFox, complete the following steps:

Step 1 From the menu bar, go to **Tools > Clear Recent History**.

The Clear Recent History dialog box appears.

Tip You can also press Ctrl + Shift + Delete to open the Clear Recent History dialog box.

Step 2 In the "Time range to clear:" box, select **Everything**.

Step 3 Open the Details drop-down list and select the **Cache** checkbox if it does not have a checkmark.

Step 4 Click **Clear Now**.

To clear the browser cache in Microsoft Internet Explorer, complete the following steps:

Step 1 From the menu bar, go to **Tools** > **Delete Browsing History**.

Tip You can also press Ctrl + Shift + Delete to open the Delete Browsing History dialog box.

Step 2 Select the Temporary Internet Files checkbox if it does not have a checkmark.

Step 3 Click **Delete**.

Importing the Security Certificate

When you access a Cisco StadiumVision Director server for the first time using Microsoft Internet Explorer or Mozilla Firefox, a security certificate warning will appear. Some Cisco StadiumVision Director functionality requires that the certificate is imported.

Importing the Security Certificate for Microsoft IE

To import the security certificate in Microsoft Internet Explorer, complete the following steps:

Step 1 When you see the warning page with the title "There is a problem with this website's security certificate," click the "**Continue to this website...**" option.

Step 2 Next to the URL bar on the top of the browser window, click **Certificate Error** and then click the "**View certificates**" link.

Step 3 In the Certificate dialog box, click **Install Certificate...** .

Step 4 In the Certificate Import Wizard dialog box, click **Next>**.

Step 5 In the next step of the wizard, select "Place all certificates in the following store" radio button and then click **Browse...** .

Step 6 In the Select Certificate Store dialog box, select the "Trusted Root Certification Authorities" store and click **Ok**.

Step 7 Click **Next>** in the Certificate Import Wizard dialog.

Step 8 Click **Finish**.

Step 9 In the Security Warning dialog box, click **Yes**.

Confirm that a dialog stating "The import was successful." appears.

Step 10 Close all Microsoft IE windows.

You should now be able to access the Cisco StadiumVision Director server using Microsoft IE without any security certificate warnings.

Adding a Security Exception for Mozilla Firefox

To add the security exception for Mozilla Firefox, complete the following steps:

Step 1 When you see the warning page with the title "This Connection is Untrusted," click the "**I Understand the Risks**" option.

Step 2 Click **Add Exception...**.

Step 3 In the Add Security Exception dialog box, click **Confirm Security Exception**.

Step 4 Close all Mozilla Firefox windows.

You should now be able to access the Cisco StadiumVision Director server using Mozilla Firefox without any security certificate warnings.

Logging Into Cisco StadiumVision Director

To verify that the upgrade to Cisco StadiumVision Director Release 3.1 was successful, and that Cisco StadiumVision Director is up and operating, complete the following steps:

Step 1 Open a browser window and type the URL for the Cisco StadiumVision Director server, in the following sample format, where *x.x.x.x* is the IPv4 address of the Cisco StadiumVision Director server:

`https://`*`x.x.x.x`***`/StadiumVision/login.jsp`**

or alternatively,

`http://`*`x.x.x.x`*

The Cisco StadiumVision Director login screen appears (Figure 14).

Figure 14 Cisco StadiumVision Director Login Screen

Step 2 Verify that Version 3.1 is displayed.

Tip If your window is not displaying Version 3.1, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 40.

Step 3 Type your Cisco StadiumVision Director administrator login credentials and click **Log In**.

Note When you first log into Cisco StadiumVision Director, the default administrator username and password is *admin*.

The Cisco StadiumVision Director Main Menu screen appears (Figure 15).

Figure 15 Cisco StadiumVision Director Main Menu

Verifying the Control Panel and Other Menus

To verify the control panel, complete the following steps:

Step 1 From the Cisco StadiumVision Director Main Menu, click **Control Panel**.

After a few moments of loading resources, the Cisco StadiumVision Control Panel Setup screen will open in a new window.

Step 2 Confirm the version and build number of your Cisco StadiumVision Director software in the lower right corner of the Control Panel window.

Tip If your window is not displaying the appropriate version and build that you loaded, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 40.

Step 3 Verify that you can open the other Cisco StadiumVision Director screens and menus.

Verifying that Services are Running

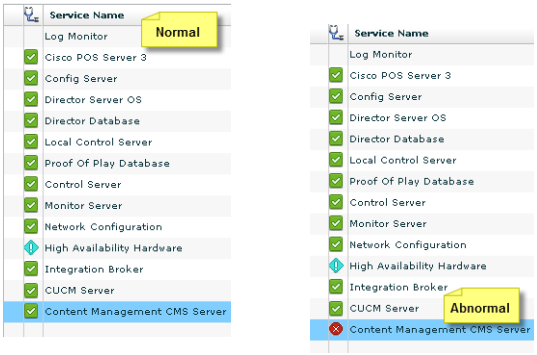
After you upgrade, go to the Management Dashboard to verify that all of the primary Cisco StadiumVision Director services are running.

To verify that services are running, complete the following steps:

Step 1 From the Management Dashboard, expand the Service Alerts pane.

Step 2 Verify that all of the primary services—in particular the Content Management CMS Server—are in "Normal" (green) state without any service alerts.

Figure 16 Verifying Normal Service States



Step 3 If the CMS server or another service in the above list is not in Normal state but should be, use the TUI services menu to restart it.

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

After you upgrade, you need to go to the Management Dashboard and change the Assigned VLAN property under Global DMP Settings for both the 4310 and 4310 v5.x.x settings according to your DMP VLAN configuration.

Configuring this property in the Management Dashboard settings for the DMP 4310s will ensure that the Dashboard value can be checked for compliance with the value being sent by the DMP:

- If all of your DMPs are located on the same VLAN (recommended)—Type the number of the VLAN and save the configuration.
- If all of your DMPs are not located on the same VLAN, or you want to bypass any VLAN compliance checking—Type "**$svd_ignore**" and save the configuration.

The value in the Assigned VLAN property in the Management Dashboard settings for the DMP 4310s is checked against what is being sent by the DMP, unless you have configured $svd_ignore.

Caution DMP auto-registration support requires that the VLAN value is correctly set or "$svd_ignore" is used.

Figure 17 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are not located on the same VLAN using the "$svd_ignore" string.

Note You need to set a value for the Assigned VLAN property for both the 4310 Settings and the 4310 v5.2.3 Settings under Global DMP Settings in the Management Dashboard..

To configure the Assigned VLAN Property, complete the following steps:

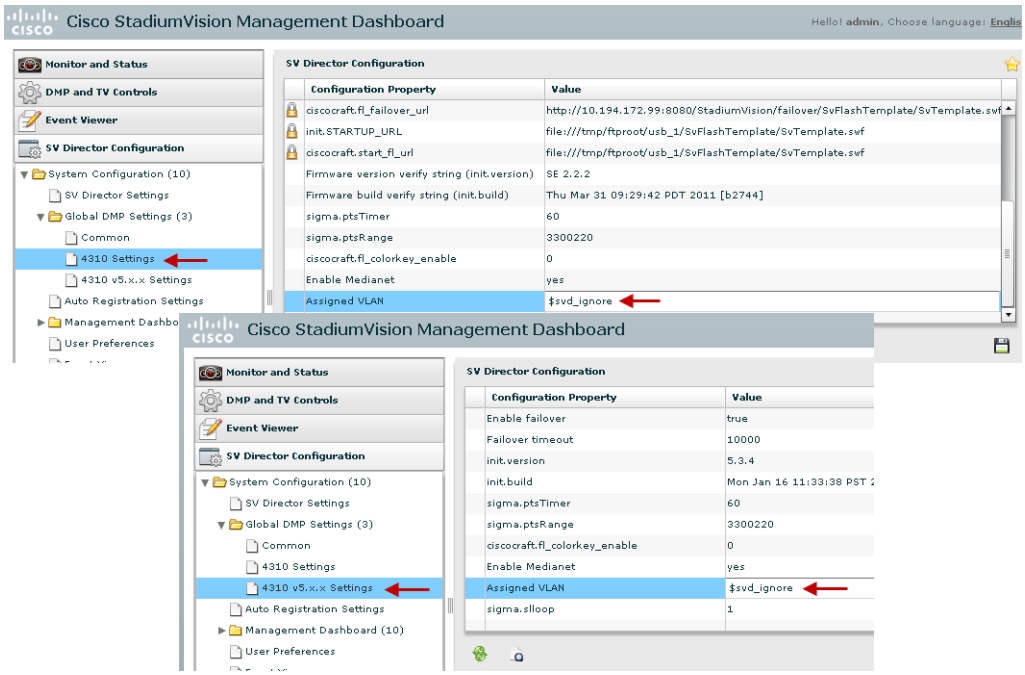
Step 1 Go to the Management Dashboard, and click **SV Director Configuration > System Configuration > Global DMP Settings**.

Step 2 Complete both of the following steps, as shown in Figure 17:

a. Click **4310 Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore.

b. Click **4310 v5.x.x Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or $svd_ignore

Figure 17 Assigned VLAN Property Configuration for DMPs



Step 3 Click the Save icon.

Verifying DMPs, Groups, and Zones in the Management Dashboard

Note Before you verify DMP status, be sure that you have set the Assigned VLAN property for your DMP 4310s so that the VLAN compliance check can be performed. For more information, see the "Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check" section on page 45.

To check DMPs, groups, and zones after you upgrade your software, complete the following steps:

Step 1 Go to the Management Dashboard and verify that all of your groups, zones and DMPs are present and in the green state.

Step 2 From the DMP and TV Controls dashboard drawer, run a Get Status on all DMPs to update Cisco StadiumVision Director's record of DMP MAC addresses using the following dashboard command path: **DMP and TV Controls > Monitoring > Get Status**.

Step 3 Run an Initial Config using the following dashboard command path: **DMP and TV Controls > DMP Install > Initial Config**.

Step 4 Run Get Status to confirm that all DMPs have successfully rebooted and are in good health.

Note This will also update the MAC address for the DMPs.

Step 5 (Optional) Change the DMP State of healthy DMPs to "Production" using the following dashboard command path: **DMP and TV Controls > Auto Registration > Change DMP State**.

Step 6 Run Get Status to check the DMP state after the change.

Step 7 Investigate any DMPs that are not in "Normal" state.

Verifying the Multicast Configuration

Cisco StadiumVision Director uses both unicast and multicast communications for DMP control-plane operation. The Cisco Connected Stadium design requires that Cisco StadiumVision Director uses the 239.193.0.0 multicast group address range.

The multicast group address for Cisco StadiumVision Director is configured in the "MulticastHostPort" registry.

To verify or configure the multicast addressing for Cisco StadiumVision Director, complete the following steps:

Step 1 From the Management Dashboard, select **Tools > Advanced > Registry**.

Step 2 Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.

Step 3 To change the value, click on the value field and specify a multicast address in the range 239.193.0.0/24.

Note Be sure to use the value that is configured in your Cisco Connected Stadium network and include the **:***port*. The recommended default is **:50001**.

Step 4 Click **Apply**.

Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server

Note This task is only required if you are using the Quest Point of Sale system.

After you upgrade, you need to set up the Quest Venue Manager to support sending updates to the Cisco StadiumVision server when menu items change.

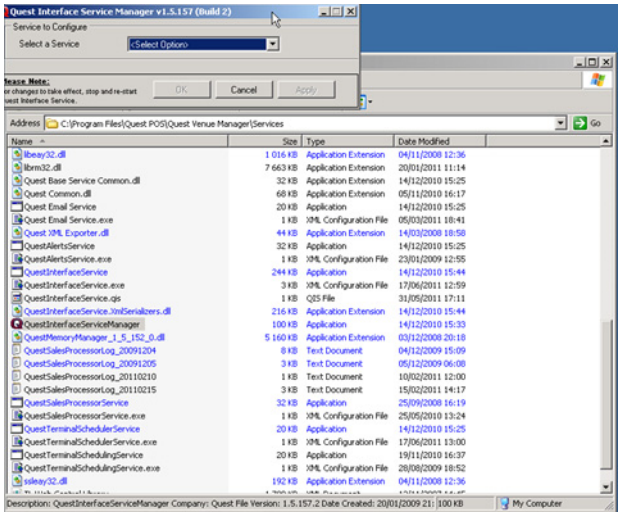
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Access the Quest server.

Step 2 Go to the C:\Program Files\Quest POS\Quest Venue Manager\Services directory.

Step 3 Start the executable application program named "QuestInterfaceServiceManager" (Figure 18).

Figure 18 QuestInterfaceServiceManager Application



Step 4 When the Quest Interface Service Manager application window opens, specify the following options (Figure 19):

a. In the Select a Service box, choose the **Quest Menu Web Service Notification**.

b. Select the **Enabled** checkbox so a checkmark appears.

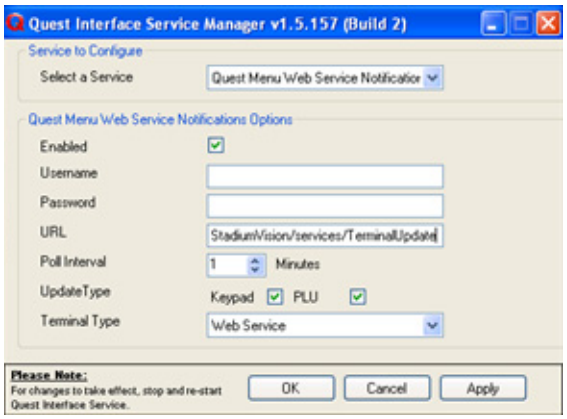
c. In the URL box, enter "**http://svd:8080/StadiumVision/services/TerminalUpdate**."

d. In the Poll Interval box, select **1** minute.

e. Select the **Keypad** and **PLU** update checkboxes so a checkmark appears.

f. In the Terminal Type box, select **Web Service**.

Figure 19 Select a Service to Configure



Step 5 Click **OK**.

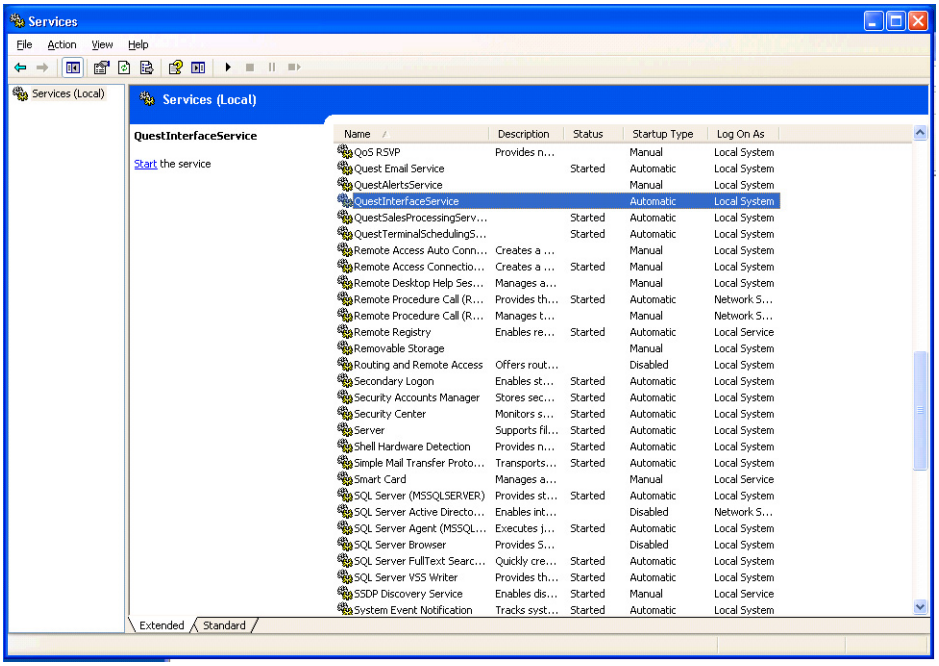
Step 6 Restart the windows service to implement the configuration by completing the following steps:

a. From your laptop, click **Start > Run. . .**

b. When the Run dialog box opens, type "**services.msc**".

c. Find the Quest Interface Service and restart it (Figure 20).

Figure 20 Restart the Quest Interface Service



What to Do Next

Use the "Appendix A: Post-Upgrade Checklist" module on page 57 to be sure that you have completed the required verification steps.

Upgrading the DMP Firmware

First Published: March 6, 2013
Revised: June 18, 2013

This modules described how to download and upgrade the DMP firmware using the Cisco StadiumVision Director Management Dashboard.

Contents

- Prerequisites, page 51
- Upgrade Tasks, page 51

Prerequisites

Before you upgrade the DMP firmware, be sure that the following requirements are met:

- Be sure that you have compatible Cisco Digital Media Player (DMP) models and firmware versions installed.

  For more information about DMP hardware and software requirements, see the *Release Notes for Cisco StadiumVision Director Release 3.1*.

Upgrade Tasks

To upgrade the DMP firmware, complete the following tasks:

- Downloading the DMP Firmware, page 51 (required)
- Upgrading the DMP Firmware From the Management Dashboard, page 52 (required)
- Disabling Failover on all DMPs, page 54 (recommended)

Downloading the DMP Firmware

The DMP firmware image is not bundled with the Cisco StadiumVision Director software. You must download the firmware image separately at the software download center site.

Note DMP-4310G Version 5.4 allows you to use MP4 (H.264 coded only) video files, and adds support for ELO IntelliTouch+ technology. Be sure to use this version if you plan to use these features.

Downloading the DMP-4310G Version 5.4 Firmware

DMP-4310G Version 5.4 firmware is not available from the Cisco Digital Media Players software download site. To download the DMP-4310G firmware, go to the Cisco StadiumVision Director software download site at:

http://software.cisco.com/download/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.1.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Downloading the DMP-4310G Version 5.3.4 Firmware

DMP-4310G Version 5.3.4 firmware is also supported in Release 3.0.

To download the DMP-4310G Version 5.3.4 firmware (filename 5.3.4_FCS_4310.fwimg), go to the Cisco Digital Media Players product page, click the **Download Software** link, and navigate to the Cisco Digital Media Player 4310G:

http://www.cisco.com/en/US/products/ps7220/tsd_products_support_series_home.html

Note Version 5.3.4 is not the latest available version shown on the download site. Be sure to navigate to All Releases > 5 > 5.3.4 to display the supported firmware download for Cisco StadiumVision Director Release 3.0.

Upgrading the DMP Firmware From the Management Dashboard

This section provides a summary of the steps to perform to upgrade your DMP firmware. The example shows configuration of DMP firmware version 5.3.4. For more detailed information, see the related documentation.

To upgrade your DMP firmware, complete the following steps on each DMP as needed:

Step 1 Go to the **Management Dashboard > DMP and TV Controls > DMP Install > Firmware Upgrade**.

Step 2 Upload the firmware file to the server and upgrade the firmware for the DMP 4310Gs.

For more information, see the “Upgrading the Firmware Image” section of the *Cisco StadiumVision Management Dashboard Device Configuration Commands* guide.

Step 3 Go to the **Management Dashboard > SV Director Configuration > System Configuration > Auto Registration Settings**. Confirm or set the following values as required:

- Enable_Auto_Registration = true
- Enable_Auto_Provisioning = true
- Firmware image to use = 5.3.4 or 5.4 (select from the dropdown box)

- Manually type the firmware init.version and init.build values according to your firmware version as follows:

Note The init.version and init.build strings must match exactly with the characters and spacing shown.

  - For firmware version 5.3.4:

    init.version = **5.3.4**

    init.build = **Mon Jan 16 11:33:38 PST 2012 [b3125]**

  - For firmware version 5.4:

Note There are two spaces between "Sep" and "6" in the init.build string for version 5.4.

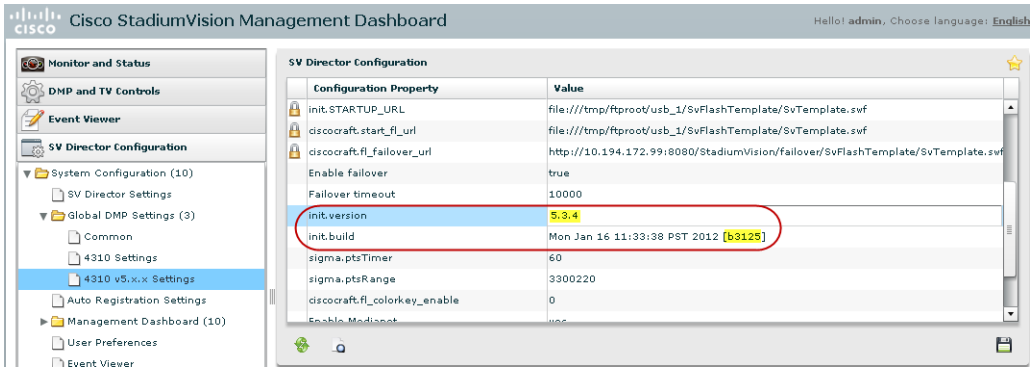
    init.version = **5.4**

    init.build = **Thu Sep 6 08:54:42 PDT 2012 [b4392]**

Step 4 Go to the **Management Dashboard > SV Director Configuration > Global DMP Settings** and confirm the firmware version and build date in the 4310 v5.x.x and 4310 Settings as shown in Figure 1.

Note Be sure that both the 4310 Settings section *and* the 4310 v5.x.x Settings have the same values for init.build and init.version.

Figure 1 Global DMP Settings in Management Dashboard



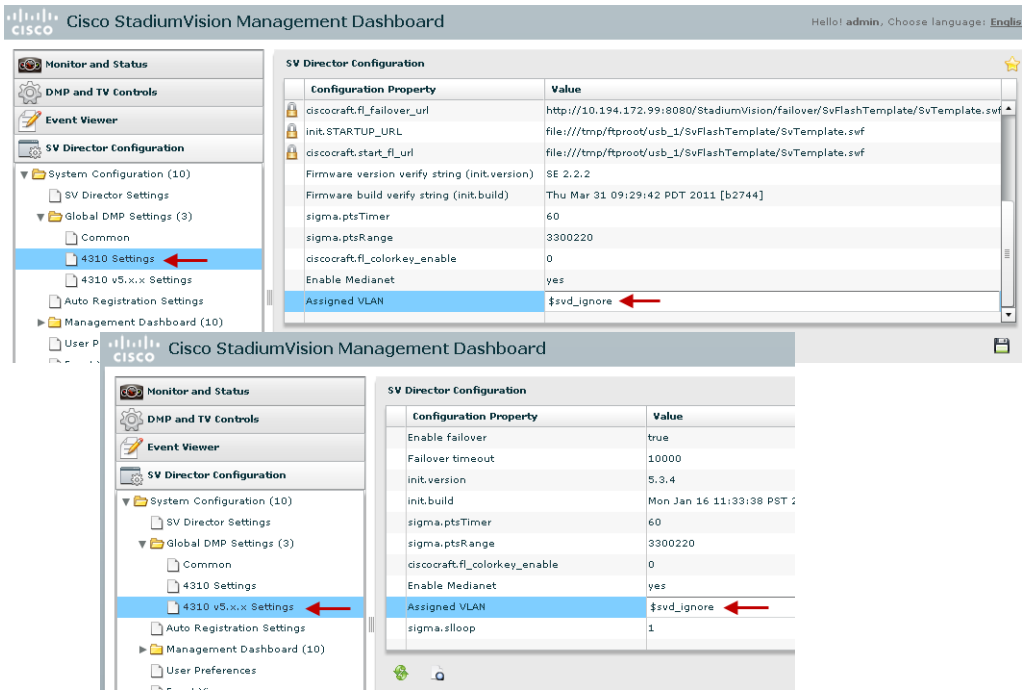
Step 5 Configure the Assigned VLAN property under both the 4310 v5.x.x and 4310 Settings as $svd_ignore or the actual VLAN number on which your DMPs reside. Do *not* leave blank.

Note DMP auto-registration support requires that the VLAN value is correctly set or "**$svd_ignore**" is used.

Figure 1 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are *not located on the same VLAN* using the "$svd_ignore" string.

You will also need to set this Assigned VLAN property value for the 4310 v5.x.x Settings:

Figure 2 Assigned VLAN Property Configuration for DMPs



Step 6 Go to **Management Dashboard > DMP and TV Controls > DMP Install > Firmware Upgrade**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Step 7 Go to **Management Dashboard > DMP and TV Controls > Global Settings > Global DMP Settings**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Step 8 Go to **Management Dashboard > DMP and TV Controls > Monitoring > Get Status**.

Select **All Devices** and click the Play (**>**) icon to run the command.

Disabling Failover on all DMPs

Note DMP failover is disabled by default beginning in Cisco StadiumVision Director Release 3.1.0-787 (SP1).

Sometimes when a DMP is in failover mode during an event and should be displaying content, but the video content is not staged, the TV screen is black. Therefore in Cisco StadiumVision Director Release 3.0, Cisco Systems recommends that failover for DMPs is disabled.

To disable failover on all DMPs, complete the following steps:

Step 1 Log into Cisco StadiumVision Director as an administrator.

Step 2 Click **Management Dashboard**.

Step 3 Go to **DMP and TV Controls > DMP Commands**.

Step 4 Select **Update MIB**.

Step 5 Click **4310 Parameters** tab.

Step 6 In the name cell, type **failover.on**.

Step 7 In the value cell, type **false**.

Step 8 In the Select Devices box, select all DMPs.

Step 9 Press the Play button to execute on selected devices.

Step 10 Turn off failover in the global MIB settings by completing the following steps:

a. From the Management Dashboard, go to **SV Director Configuration > System Configuration > Global DMP Settings > 4310 v5.x.x Settings**.

b. Find the **Enable failover** property.

c. Set the value to **false**.

d. Click **Save changes**.

Appendix A: Post-Upgrade Checklist

First Published: March 6, 2013
Revised: June 10, 2013

The following checklist is useful after you upgrade your software on a Cisco StadiumVision Director server.

.

List Item	Checkoff
1. Complete any specific verification steps documented for your particular upgrade.	❑
2. Clear the browser cache.	❑
3. Verify that the Control Panel shows the Cisco StadiumVision Director version and build number that you installed.	❑
4. If you are using phone control, verify that the phones work.	❑
5. If using IP phones for local TV control, verify that channels can be successfully changed.	❑
6. Verify that channel names and favorites are properly set.	❑
7. If using suite commerce integration, verify that an order can be successfully placed using the IP phone.	❑
8. Verify that all devices are properly in the nonevent_group.	❑
9. Go to the Services Alert window in the Management Dashboard and make sure that all relevant services are green. **Tip** You might need to click the refresh button to be sure that all services are re-polled for status. If needed, you can Disable services that are not part of your installation	❑
10. Verify that all DMPs and TVs in the Management Dashboard are green.	❑
Note This step is for upgrades from Release 3.0 only. **11.** Verify success of the content migration. See the "Validating the Content Migration" section on page 8.	❑

List Item	Checkoff
Note This step is for upgrades from Release 3.0 only.	
12. Clean up and remove legacy VDM files. See the "Cleaning Up Legacy Video Files After Migration" section on page 9.	❑
13. Start an existing event script and validate that screens display the expected content.	❑
14. Stop the event script and validate that screens are powered off.	❑
15. Make a minor edit to the event script and make sure it can be saved.	❑
16. Verify that you can push a new video file in the CMS to the DMPs.	❑
17. If using dynamic menu boards, make a change to a menu item and verify that the change is reflected on the menu board.	❑
18. If using external content integration, be sure to re-enable your data sources in the Control Panel and restart the External Content Integration application from the Management Dashboard.	❑
19. Perform a server backup for the upgrade configuration.	❑
20. After satisfying your site's testing and event requirements, failback to the primary server and upgrade it to the same version of software that you validated on your secondary server. For more information, see the "Configuring Failover Between Redundant Cisco StadiumVision Director Servers" module in the *Cisco StadiumVision Director Server Administration Guide*.	❑
21. After you perform failback, be sure that you reconfigure your backup and restore environment using the Text Utility Interface (TUI).	❑
22. (**As needed for sites with a large volume of video content**) Reduce the number of backups that are retained by the system. For more information, see the "Backing Up and Restoring Cisco StadiumVision Director Servers" module in the *Cisco StadiumVision Director Server Administration Guide*.	❑

Appendix B: Port Reference

First Published: March 6, 2013
Revised: March 20, 2013

The following tables identify the default ports used by Cisco StadiumVision Director:

- Cisco StadiumVision Director Ports, page 59
- Cisco StadiumVision Director Remote Ports, page 61
- DMP Input Ports, page 62

Cisco StadiumVision Director Ports

The Cisco StadiumVision Director ports are divided into tables for input and output ports.

Cisco StadiumVision Director Input Ports

Table 1 lists the input ports used by all Cisco StadiumVision Director servers.

Table 1 Cisco StadiumVision Director Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	22	SSH	Remote login.
Laptop / DMP	TCP	80	Apache	Redirect to port 8080.
DMP	UDP	514	Syslog	Proof of play, Alerts.
DMP	TCP	8080	Tomcat / Apache	Fetch config/data.
Laptop	TCP	8080	Tomcat / Apache	Main web UI.
Laptop	TCP	9090	Tomcat for Liferay	Liferay web UI (Dynamic Menu Board application).

Table 2 lists the additional input ports used by Cisco StadiumVision Director server instances only during troubleshooting access froma PC.

Table 2 Cisco StadiumVision Director Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	7041	Java	JMX management interface for control server instance.
Laptop	TCP	7042	Java	JMX management interface for config server instance.
Laptop	TCP	7043	Java	JMX management interface for monitor server instance.
Laptop	TCP	7045	Java	JMX management interface for CMS server instance.
Laptop	TCP	7050	Java	JMX management interface for local control.

Cisco StadiumVision Director Output Ports

Table 3 Cisco StadiumVision Director Output Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	FTP	21	FTP server	Fetching integration broker data over FTP. Playlist integration.
StadiumVision Director	TCP	22	ssh	DMP troubleshooting.
StadiumVision Director	TCP	80	httpd	Redirect to 443.
StadiumVision Director	TCP	443	httpd	4310 web UI.
StadiumVision Director	TCP	80 / 443		Fetching integration broker data. Fetching legacy ticker data.
StadiumVision Director	TCP	8089	tomcat	Configuration update for multicast rebroadcaster.
StadiumVision Director	UDP	Default: 50001	DMP flash template	Multicast commands (default is 239.192.0.254:50001).

Cisco StadiumVision Director Remote Ports

The Cisco StadiumVision Director Remote ports are divided into tables for input and output ports.

Cisco StadiumVision Director Remote Input Ports

Table 1 lists the input ports used by all Cisco StadiumVision Director Remote servers.

Table 4 Cisco StadiumVision Director Remote Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	22	sshd	SSH for TUI.
Laptop	TCP	7140	java	JMX management interface for Cisco StadiumVision Director Remote.
StadiumVision Director	TCP	8080	httpd	Multicast rebroadcaster configuration, content distribution.
StadiumVision Director	TCP	8089	tomcat	Configuration update for multicast rebroadcaster.
StadiumVision Director	UDP	Default: 7777	Multicast rebroadcaster	Unicast commands for the individual Cisco StadiumVision Director Remote server from the central Cisco StadiumVision Director server.
StadiumVision Director	UDP	Default: 50001	Multicast rebroadcaster	Multicast commands (Default is 239.192.0.254:50001)

Cisco StadiumVision Director Remote Output Ports

Table 5 lists the output ports used by all Cisco StadiumVision Director Remote servers.

Table 5 Cisco StadiumVision Director Remote Output Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director Remote	TCP	8080	httpd	Get multicast rebroadcater from Cisco StadiumVision Director server.
StadiumVision Director Remote	UDP	Default: 7778	DMP flash template	Multicast commands (Default is 239.193.1.1:7778)

DMP Ports

The DMP ports are divided into tables for input and output ports.

DMP Input Ports

Table 6 lists the input ports used by the DMP.

Table 6 DMP Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	443	httpd	4310 web UI, unicast messaging from Cisco StadiumVision Director
StadiumVision Director	UDP	varies	DMP flash template	Multicast commands (default is 239.192.0.254:50001)
Headend	UDP	varies	Sigma chipset	Multicast video

DMP Output Ports

Table 7 lists the output ports used by the DMP.

Table 7 DMP Output Ports

Originator	Protocol	Port	Target Application	Usage
DMP	UDP	514	syslog	Proof of play. Alerts.
Cisco StadiumVision Director	TCP	8080	httpd	Fetching of DMP config, autoprovisioning, and related.
DMP	TCP	9090	Tomcat for Liferay	Dynamic Menu Board application interface.

Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.1

First Published: March 20, 2013

The Cisco StadiumVision Director Platform 2 server ships with two 300 GB hard drives configured with RAID 1 mirroring for redundancy. This module describes how to install two additional 300 GB hard drives (SV-FRU2-HD3G=) for another RAID 1 volume in the Cisco StadiumVision Director Platfrom 2 Server which are required to run Cisco StadiumVision Director Release 3.1 with a minimum of 4 drives.

Caution If you need to install additional hard drives in the Platform 2 server to meet the 4-drive minimum requirement to support Release 3.1, then you must perform the upgrade in a certain order. The physical installation of the additional drives must precede the upgrade to Release 3.1, followed by extension of the RAID volume post-upgrade, and then content migration and the remainder of the upgrade verification.

Contents

- Prerequisites, page 63
- Installation Tasks, page 64

Prerequisites

Be sure that the following requirements are met before you upgrade your server:

- Your current CIMC/BIOS firmware version is a minimum of 1.4(2).
- You have completed running any proof of play reports.
- You have completed a backup and have a copy stored externally to the Cisco StadiumVision Director servers.
- You have installed Cisco StadiumVision Director Release 3.0.0-433 SP2 on your Platform 2 servers.
- You have physical access to the server.
- A monitor and keyboard are connected to the Cisco StadiumVision Director server.

- You can log into the server at the console or over the network with SSH.
- You have two new 300 GB R2 Disk Spare drives (SV-FRU2-HD3G=) for the Platform 2 server.

Note These hard drives are no longer generally available. If you need to obtain spare drives, contact your Cisco Systems sales representative for more information.

Installation Tasks

To install additional hard drives, complete the following tasks:

- Installing the Hard Drives Into the Server Chassis, page 64 (required)
- Creating a New Logical Volume Using the LSI MegaRAID Utility, page 65 (required)
- Extending the Original RAID Volume to Create a Single Group, page 68 (required)

Installing the Hard Drives Into the Server Chassis

This task describes how to physically install two additional 300 GB drives into the Cisco StadiumVision Director Platform 2 server.

To install the hard drives into the server chassis, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director server with the "installer" credentials either directly at the console or over the network using SSH.

Note Unless the values have been changed, the default userid is "installer" with password "cisco!123."

Step 2 When the StadiumVision Director Configuration menu for the Text Utility Interface (TUI) appears, type **m** and press **Enter** to shut down the server.

Step 3 Amessage appears asking you to confirm the shutdown.

```
WARNING: THIS WILL SHUTDOWN THE SERVER!! Are you sure?

PRESS Y TO CONTINUE, PRESS N TO CANCEL
```

Type **Y**.

The server begins to shut down and a series of messages are displayed:

```
System is shutting down. You will be logged out shortly.
Broadcast message from root (pts/0) (Tue May 8 21:28:00 2012):

The system is going DOWN for system halt in 1 minute!
```

Note If the server reboots instead of powers down it is probably running an older firmware. For more information, see the "Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server".

Step 4 Install the new 300 GB hard drives into Slot 2 and Slot 3 of the server chassis.

For information about physically installing the hard drives on the Platform 2 server, see the "Maintaining the Server" chapter of the *Cisco UCS C200 Installation and Service Guide*.

Creating a New Logical Volume Using the LSI MegaRAID Utility

This task creates another RAID 1 logical volume composed of the two new drives.

For more information about RAID on the Cisco StadiumVision Director Platform 2 server, such as the meaning of the beep codes, see the "RAID Controller Considerations" chapter of the *Cisco UCS C200 Installation and Service Guide*.

Note It is recommended that you have a mouse or other similar device attached to the sever so that you can perform the installation steps more easily.

To create a new logical volume using the LSI MegaRAID utility, complete the following steps:

Step 1 Power on the Cisco StadiumVision Director server where you physically installed the two new hard drives.

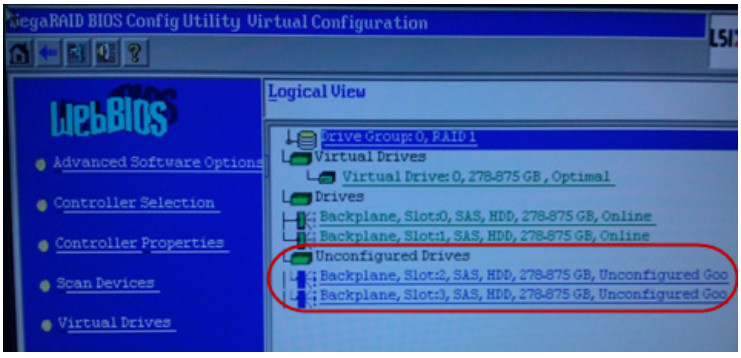
Step 2 Press **Ctrl-H** to open the LSI MegaRAID utility when prompted.

Note Be sure to press Ctrl-H when prompted by the LSI MegaRAID utility. If you miss the prompt or reach the boot menu before seeing it, press Ctrl-Alt-Del to reboot the server and try again.

Step 3 Create a new logical volume with the two new drives in a RAID 1 configuration by completing the following steps:

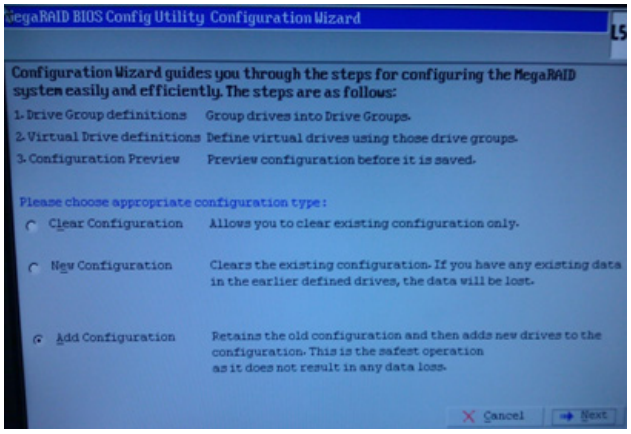
Note Only drives in "Unconfigured Good" state are available for RAID configuration. New drives must show up as unconfigured before you proceed (Figure 1).

Figure 1 Unconfigured Drives in Good State



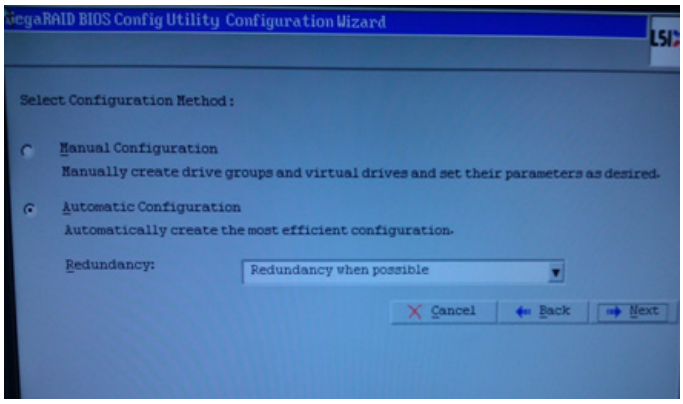
a. Select **Add Configuration** and click **Next** (Figure 2).

Figure 2 Add Configuration Wizard



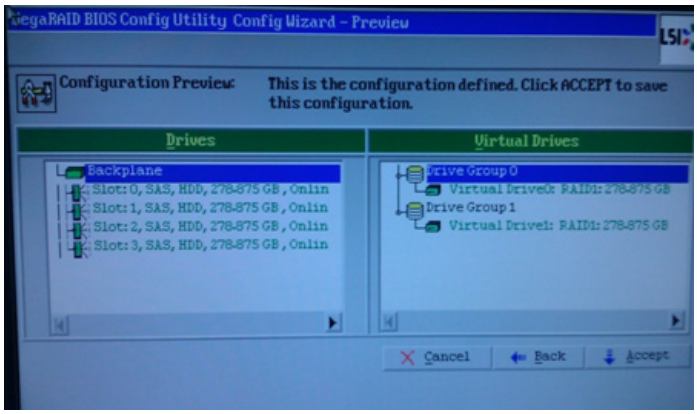
b. Select **Automatic configuration** with the **Redundancy when possible** option. Click **Next** (Figure 3).

Figure 3 Configuration Method Screen



c. The Configuration Preview screen is displayed showing the 4 hard drives in 2 drive groups. Click **Accept** (Figure 4).

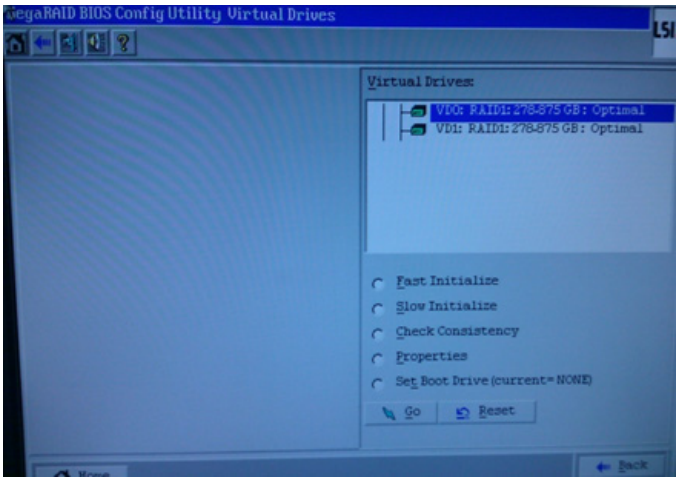
Figure 4 Accept Configuration Preview



A fast disk initialization automatically begins.

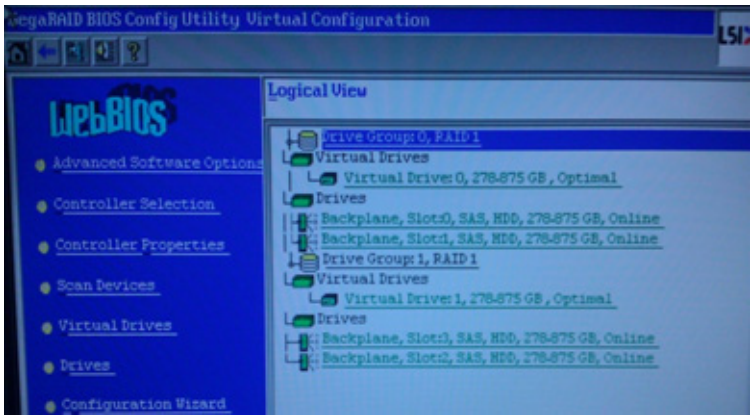
d. When the screen showing initialization options is displayed, only click **Back** (Figure 5).

Figure 5 Initialization Options—Click Back Only



e. The Logical View screen shows the 4 hard drives online, including the two new drives in Slot 2 and Slot 3 (Figure 6).

Figure 6 Logical View of Hard Drives



Step 4 Exit the MegaRAID utility.

Extending the Original RAID Volume to Create a Single Group

Caution Stop here. Go to the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1 and perform the task to upgrade the software to Release 3.1. Extending the RAID volume needs to be performed *after* you have upgraded your server to the Release 3.1.0-632 software and before you migrate your content to the Release 3.1 CMS.

This task describes how to extend at the OS level the original logical volume on which Cisco StadiumVision Director is installed to include the new RAID 1 volume. This will create a volume group where Cisco StadiumVision Director sees the four drives as one volume with a total of 600 GB storage.

To extend the original RAID volume to create a single group in the Release 3.1 software, complete the following steps:

Step 1 Log into the TUI by doing the following:

a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the secondary Cisco StadiumVision Director server using the IP address for your server.

b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.

Step 2 From the Main Menu, go to the **StadiumVision Server Administration > Hard Drive Expansion** option.

Step 3 When the following confirmation message appears, type Y if you are prepared to continue, or N to cancel.

```
WARNING: You will lose data that may be stored in the new drives. Do you want to continue?
PRESS Y TO CONTINUE, PRESS N TO CANCEL
```

Step 4 Press any key to return to the StadiumVision Server Administration menu.

Step 5 Continue to return to the Main Menu and exit the TUI.

What To Do Next

After you extend the RAID volume, return to the "Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1 SP1 and SP2" module on page 1 to complete the upgrade tasks and perform the migration of content to the Release 3.1 CMS.

Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server

First Published: March 27, 2013
Revised: September 30, 2013

This document provides guidelines for configuring the Cisco Integrated Management Controller (CIMC) interface and performing the initial configuration, and upgrading the CIMC/BIOS firmware on the Cisco UCS C220 servers for Cisco StadiumVision Director (SV-DIR-DIRECTOR-K9, SV-PLATFORM3=) .

Note Use the information in this appendix only as a guide to the tasks that you need to perform for CIMC configuration or upgrade, but follow the procedures in the referenced Cisco UCS documents.

This section includes the following topics:

- CIMC Initial Configuration, page 71 (required)
- CIMC Firmware Upgrade Guidelines, page 73 (as required)

CIMC Initial Configuration

This section includes the following topics:

- Prerequisites, page 71
- CIMC Initial Configuration Summary, page 72

Prerequisites

Be sure that the following requirements are met before you do the CIMC initial configuration:

- You have a monitor, keyboard, and mouse that you can connect to the server.
- You have the following information for configuring the internal Cisco Integrated Management Controller (CIMC) interface:
  - You have an additional IP address for static configuration.

Tip This is a different IP address than the IP address that you configure for the eth0 network interface on the Cisco StadiumVision server.

  - You have the VLAN ID if the server will be installed on a network VLAN.
  - You are prepared to change the default CIMC login password.
- You have a laptop with access to the Cisco StadiumVision network.
- Your computer meets the minimum browser and Flash player requirements for the Cisco StadiumVision server, and also has Java 1.6 or later installed.

  See the release notes for your Cisco StadiumVision product and release at:

  http://www.cisco.com/en/US/products/ps11274/prod_release_notes_list.html
- You have a copy of or access to the following documents on Cisco.com:
  - *Cisco UCS C220 Server Installation and Service Guide*

    Familiarize yourself with the "Initial Server Setup" topic of the "Installing the Server" chapter.
  - *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4*

    (or the version that corresponds to your firmware release found at: http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html.)

    Familiarize yourself with the "Overview" chapter, and the "Managing the Server Boot Order" section of the "Managing the Server" chapter.

CIMC Initial Configuration Summary

This section provides an overview of the basic tasks to be completed when performing the initial CIMC configuration in standalone mode for a Cisco StadiumVision server after you have unpacked and inspected it and prepared it for installation.

To perform the CIMC initial configuration, complete the following tasks:

	Description
	Configuring the CIMC Interface **Note** The instructions for configuring the CIMC interface are found in the "Initial Server Setup" topic of the "Installing the Server"chapter in the *Cisco UCS C220 Server Installation and Service Guide*.
Step 1	During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility.
Step 2	Configure the CIMC interface with the following settings: • DHCP—Disabled. You must change this option to enter a static IP address. • CIMC IP—IPv4 address for your CIMC interface, with corresponding subnet mask. • VLAN—Dependent on client network. • Change the CIMC password. The default credential is **admin** and **password**.
Step 3	Press **F10** to save your configuration and reboot the server.

	Description
	Configuring the NIC Properties **Note** Information about configuring the NIC properties are found in the "Initial Server Setup" topic of the "Installing the Server"chapter in the *Cisco UCS C220 Server Installation and Service Guide*.
Step 4	From a laptop with access to the Cisco StadiumVision network, use a browser and type the IP address that you configured for the CIMC interface to connect to the CIMC console.
Step 5	Log into the CIMC console with username **admin** and the password that you configured in Step 2.
Step 6	From the **Admin** tab, click **Network**, and go to the **Network Settings** page. In the NIC Properties box configure the following settings and save your changes: • NIC mode—Dedicated • NIC Redundancy—None
	Configuring the Server Boot Order **Note** The instructions for configuring the server boot order are found in the "Managing the Server Boot Order" section of the "Managing the Server" chapter of the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4*
Step 7	From the **Server** tab, click **BIOS**.
Step 8	Configure the following boot order and save your changes: • Virtual CD/DVD • HDD

CIMC Firmware Upgrade Guidelines

This section includes the following topics:

- Before You Begin, page 73
- Prerequisites, page 74
- CIMC/BIOS Firmware Upgrade Summary, page 74

Before You Begin

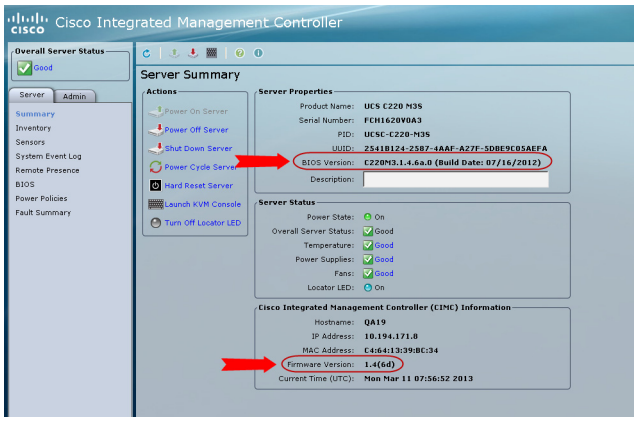
See the release notes for your Cisco StadiumVision product and release at:

http://www.cisco.com/en/US/products/ps11274/prod_release_notes_list.html

- Find the minimum CIMC/BIOS versions tested for your Cisco StadiumVision Director (SV-DIR-DIRECTOR-K9, SV-PLATFORM3=) platform.

- From your Cisco StadiumVision platform, verify the CIMC and BIOS firmware versions in the CIMC console (Figure 1).

Figure 1 Firmware Verification From the CIMC Console



Note Unless there is another reason why an upgrade has been found to be needed, no upgrade should be needed if your server firmware is at the minimum tested version (or later) for the Cisco StadiumVision release that you are running.

Prerequisites

Be sure that the following requirements are met before you perform a CIMC/BIOS firmware upgrade:

- You have a copy of or access to the following documents on Cisco.com:
  - *Release Notes for Cisco UCS C-Series Software, Release 1.4(6)*

    (or the version that corresponds to your firmware release found at: http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html)
  - *Cisco Host Upgrade Utility Release 1.4(6) Quick Start Guide*

    (or the version that corresponds to your firmware release found at: http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html)

    Familiarize yourself with all of the requirements in these documents to perform your CIMC/BIOS firmware upgrade.
- You have access to Cisco.com to download the firmware ISO file.

CIMC/BIOS Firmware Upgrade Summary

Caution Be sure to follow the requirements in the release notes and the Host Upgrade Utility (HUU) guide for your firmware, including making sure that you upgrade both the CIMC and BIOS at the same time and from the HUU ISO file.

To perform the CIMC/BIOS firmware upgrade, complete the following tasks:

	Description
Step 1	Using the release notes for the firmware version that you need to install, find the name of the ISO file that applies to the Cisco UCS C220 server for that firmware. **Note** The release 1.4(x) firmware HUU ISO files are platform-specific.
Step 2	Follow the instructions in the Host Upgrade Utility guide: **Note** The Cisco UCS C220 server does not have a CD/DVD drive. • Go to Cisco.com and download the HUU ISO file. • Follow the instructions to load the ISO that you downloaded and be sure that both the CIMC and BIOS firmware are upgraded together.