StadiumVision

Cisco StadiumVision Director Software Installation and Upgrade Guide

Release 4.0

October 27, 2015

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

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

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

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

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

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

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

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

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

Cisco StadiumVision Director Software Installation and Upgrade Guide
© 2015 Cisco Systems, Inc. All rights reserved.

CISCO

StadiumVision

CONTENTS

Preface vii

Document Revision History vii

Document Organization viii

Related Documentation viii

Obtaining Documentation and Submitting a Service Request ix

Getting Started Installing or Upgrading Cisco StadiumVision Director 1

Before You Begin 1

Hardware Prerequisites 2

Overview of the Installation and Upgrade Process 3

Installing on a Virtual Server for the First Time 3

Installing a Platform 3 Server for the First Time 4

Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director 4

Installing Cisco StadiumVision Director for the First Time 7

Prerequisites 7

Installation Tasks 9

Downloading the ISO Files from Cisco.com 9

Logging Into the CIMC Interface 10

Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director 11

Launching the KVM Console 12

Mapping the Cisco StadiumVision Director ISO Image 13

Installing the Cisco StadiumVision Director ISO Image 14

Configuring the Network Setup 14

What To Do Next 17

Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts 19

Best Practices 19

Prerequisites 21

Information About Using the Software Manager to Update Existing Cisco StadiumVision Director Software 21

ISO Upgrade Files 21

Disk Maintenance 21
Upgrade Tasks 22
Downloading ISO Upgrade Files from Cisco.com 22
Uploading and Installing an ISO Upgrade File on the Cisco StadiumVision Director Server 23
Prerequisites 23
Task 23
Reactivating Custom Fonts 24
Staging the Flash Template for Cisco DMP 4310G Devices 24
Deploying Global DMP Settings for the Cisco DMP 4310G 25
Installing Language Packs 25
Installing Fonts 26
Guidelines for Installing Fonts 27
Procedure 27
What to Do Next 28

Verifying the Upgrade 29
Clearing the Browser Cache 29
Importing the Security Certificate 30
Adding a Security Exception for Mozilla Firefox 30
Logging Into Cisco StadiumVision Director 30
Verifying the Control Panel and Other Menus 31
Verifying that Services are Running 31
Configuring the Media Player for VLAN Compliance Checking 32
Verifying Media Players, Groups, and Zones in the Management Dashboard 34
Verifying the Multicast Configuration 34
Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server 35
Completing the Post-Upgrade Checklist and Testing 37

Upgrading the DMP 4310G Firmware 39
Contents 39
Prerequisites 39
Upgrade Tasks 39
Downloading the DMP Firmware 39
DMP-4310G Version 5.4.1 RB2P 40
Upgrading the DMP Firmware From the Management Dashboard 40
Disabling Failover on all DMPs 42

Upgrading the SV-4K Firmware 43
Contents 43
Prerequisites 43

Provisioning Tasks 44
Downloading the SV-4K Firmware 44
Uploading the SV-4K Firmware to Cisco StadiumVision Director 44
Configuring the SV-4K for Auto-Registration 45

Appendix A: Post-Upgrade Checklist 47

Appendix B: Port Reference 51

Cisco StadiumVision Director Ports 51
Cisco StadiumVision Director Input Ports 51
Cisco StadiumVision Director Output Ports 52
Cisco StadiumVision Director Remote Ports 53
Cisco StadiumVision Director Remote Input Ports 53
Cisco StadiumVision Director Remote Output Ports 53
Media Player Ports 54
Common Media Player Input Ports 54
Input Ports—DMP 4310G Only 55
Input Ports—SV-4K Only 55
Common Media Player Output Ports 56
Output Ports—SV-4K Only 56

Appendix C: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server 57

CIMC Initial Configuration 57
Prerequisites 57
CIMC Initial Configuration Summary 58
CIMC Firmware Upgrade Guidelines 59
Before You Begin 59
Prerequisites 60
CIMC/BIOS Firmware Upgrade Summary 60

Appendix D: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software 63

Best Practices 63
Prerequisites 64
Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server 65
ISO Upgrade Files 65
Disk Maintenance 65
Upgrade Tasks 65
Downloading ISO Upgrade Files from Cisco.com 66
Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server 67

Prerequisites 67
Logging Into the CIMC Interface 68
Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director 69
Launching the KVM Console 70
Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server 71
Staging the Flash Template for the DMP 4310G 73
Deploying Global DMP Settings for the Cisco DMP 4310G 73
What to Do Next 73

Preface

This document describes the requirements and tasks to install and upgrade the software for Cisco StadiumVision Director Release 4.0.

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, Linux, and VMware virtualization.

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
October 27, 2015	Added required task for reboot of SV-4K devices after an ISO upgrade to the "Upgrade Tasks" section on page 22 and some other minor edits in the "Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts" module.
August 31, 2015	The following updates were made: • Reorganized the "Hardware Prerequisites" section on page 2 and enhanced the "Minimum Virtual Machine System Requirements for Cisco StadiumVision Director" section on page 2 with addition of Table 2 on page 3 to provide information about tested VM hardware and OS specifications. • Added "Clearing Expired Flash SWZ Files From Browser" section on page 30 as a required task after upgrades. • Changed reference from laptop to the Quest Server in Step 6.a. of the "Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server" section on page 37.

Table 1 Document Revision History (continued)

Date	Change Summary
May 18, 2015	The following updates were made for Cisco StadiumVision Director Release 4.0.0-601: • Modified the language pack statement to reference Release 4.0.0-601 in the "Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts" module on page 19. • Revised the post-upgrade checklist item to add requirement for closing the browser in addition to clearing the browser cache in the "Appendix A: Post-Upgrade Checklist" module on page 63.
May1, 2015	The following updates were made for Cisco StadiumVision Director Release 4.0.0-525: • The following changes were made in the "Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts" module on page 19: – Task was added for reactivating custom fonts after upgrade. – Language pack statement was modified to reference Release 4.0.0-525. – Revised steps in the "Installing Language Packs" section on page 25 and added instructions for loading locales on the SV-4K media players. – Revised steps in the "Installing Fonts" section on page 26. • Updated the figure in the "Upgrading the SV-4K Firmware" module on page 43.
March 20, 2015	First release of this document for Cisco StadiumVision Director Release 4.0.0-402.

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 4.0 software.
"Installing Cisco StadiumVision Director for the First Time"	Describes how to install the Cisco StadiumVision Director Release 4.0 software on your newly-purchased Platform 3 server hardware from a full ISO image.
"Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts"	Describes how to upgrade a Cisco StadiumVision Director server already running Cisco StadiumVision Director 3.2 to a later release of Cisco StadiumVision Director software, as well as how to install language packs and fonts.
"Verifying the Upgrade"	Describes how to verify that the upgrade process was successful.
"Upgrading the DMP 4310G Firmware"	Describes how to upgrade the DMP firmware on the Cisco DMP 4310G.

Chapter	Description
"Upgrading the SV-4K Firmware"	Describes how to obtain and upload the SV-4K firmware, and how to configure the auto-registration settings.
"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.
"Appendix C: 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=).
"Appendix D: 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.

Related Documentation

- *Release Notes for Cisco StadiumVision Director Release 4.0*
- *Cisco StadiumVision Director Server Administration Guide, Release 4.0*
- *Cisco StadiumVision Director Localization Guide, Release 4.0*
- For the listing page of all Cisco StadiumVision documentation, go to:

  http://www.cisco.com/c/en/us/support/video/stadiumvision/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 20, 2015
Revised: August 31, 2015

Read this module before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 4.0 software. It includes the following topics:

- Before You Begin, page 1
- Overview of the Installation and Upgrade Process, page 4

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 4.0* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Determine if you have compatible media player models and firmware versions installed.

  The media player firmware images are not bundled with the Cisco StadiumVision Director software. You must download the firmware image separately. For more information about supported firmware versions, see the *Release Notes for Cisco StadiumVision Director Release 4.0*.
- Be sure that you have a supported browser (Google Chrome Version 38.0, Mozilla FireFox Version 33.1, and Adobe Flash Player (Version 15.0.0.189) 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 4 for more information and to find out what modules in this guide you should follow.

Hardware Prerequisites

You can install Release 4.0 on a Platform 2 or Platform 3 server, or use your own server to run the Cisco StadiumVision Director software. Follow the requirements in this section to be sure that your virtual environment meets the minimum and tested specifications.

This section includes the following topics:

- Minimum Virtual Machine System Requirements for Cisco StadiumVision Director, page 2
- VMware vSphere Tested Versions for Cisco StadiumVision Director, page 3
- Restrictions for Virtual Server Support, page 4

Minimum Virtual Machine System Requirements for Cisco StadiumVision Director

Be sure that your configuration meets the minimum system requirements in Table 1 and supports a VMware virtual machine environment with a compatible vSphere version (See "VMware vSphere Tested Versions for Cisco StadiumVision Director" section on page 3.).

Note Cisco StadiumVision Director servers are meant to be physically located close to the DMPs that they operate with, such as at the remote venue edge, and communicating to the players over a LAN. For information about installation-related licensing compliance, see the "Installation Requirements for Licensing Compliance" section of the *Release Notes for Cisco StadiumVision Director Release 4.0*.

Table 1 Minimum System Requirements for a Virtualized Environment running Cisco StadiumVision Director

System Component	Minimum Requirement
Forward Write (fwrite) in operations per second (ops)	10,000
Hard Drive Capacity	900 GB **Note** The hard drives must be configured as a single logical volume. A RAID volume is strongly recommended.
Processor	Dual processor equivalent to an Intel Xeon Processor E5-2460 (15 MB cache, 2.50 GHz clock, 7.20 GT/s Intel® QPI)
Virtual RAM (VRAM)	32 GB
Virtual CPUs	24

Table 2 provides additional information about the tested VM hardware and OS specifications that you should use when configuring a virtual machine to support Cisco StadiumVision Director.

Table 2 Virtual Machine Hardware and OS Specifications Tested for Cisco StadiumVision Director Server

System Component	Specification
VM Hardware	Version 8
Guest Operating System	Linux 5 64-bit
Network Adapter	E1000
SCSI Controller	LSI Logic Parallel or LSI Logic SAS
Disk Provisioning	Thick

VMware vSphere Tested Versions for Cisco StadiumVision Director

Cisco StadiumVision Director has been tested with VMware vSphere version 5.1 and 5.5. Other VMware vSphere versions cannot be guaranteed to work with Cisco StadiumVision Director Release 4.0.

Note Any VMware license that does not allow your virtual machine to be set to the minimum requirements described in Table 1 is not supported.

Restrictions for Virtual Server Support

Be sure that you consider the following restrictions before you configure a virtual server environment for Cisco StadiumVision Director:

- Migrating to a virtualized environment on your existing Platform 2 or Platform 3 servers is not supported. For more information, see the "Important Migration and Upgrade Notes" section of the Release Notes.
- When using a virtual server environment, Cisco Technical Support only provides support for the Cisco StadiumVision software. No support is provided for third-party hardware or the virtual OS environment installed by the customer.
- The recommended configuration is for a dual virtual server environment to support a primary and backup server using the standard Cisco StadiumVision Director backup/restore and failover tools.
- Cisco has not tested and does not provide support for any VMware tools in a Cisco StadiumVision system. If your site chooses to use backup, recovery or other tools outside of the Cisco StadiumVision Director software to manage your virtual servers, then you accept the risks and responsibility associated with securing your data.

Overview of the Installation and Upgrade Process

There are different tasks required to install or upgrade your Cisco StadiumVision Director server for software Release 4.0 depending on your current server environment:

- Installing on a Virtual Server for the First Time, page 4
- Installing a Platform 3 Server for the First Time, page 5
- Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director, page 5

Note A full ISO installation on a Platform 2 server is not supported in Cisco StadiumVision Director Release 4.0. Only ISO upgrades are supported.

Installing on a Virtual Server for the First Time

The installation process for a virtual server running Cisco StadiumVision Director software for the first time involves the following tasks:

- Verify that your virtual server meets the requirements listed in Table 1.
- Install VMWare client software.

Note Cisco StadiumVision Director has been tested with VMware vSphere version 5.1 and 5.5. Other VMware vSphere versions cannot be guaranteed to work with Cisco StadiumVision Director Release 4.0.

Any VMware license that does not allow your virtual machine to be set to the minimum requirements described in Table 1 is not supported.

- Load the Cisco StadiumVision Director Release full ISO.

- Run the installation.
- Upgrading the Cisco DMP 4310G and SV-4K firmware.

Installing a Platform 3 Server for the First Time

The installation process for a new Platform 3 server running Cisco StadiumVision Director 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 Cisco DMP 4310Gs.
(Disabled is the default)
- Upgrading the Cisco DMP 4310G and SV-4K firmware.

For detailed information, see the "Installing Cisco StadiumVision Director for the First Time" on page 7.

Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director

You can upgrade an existing server already running Cisco StadiumVision Director software using an upgrade ISO image file available from Cisco.com and using the upgrade option from the Software Manager in the Cisco StadiumVision Director web browser interface.

Caution Before you upgrade your system from Cisco StadiumVision Director Release 3.2 to Release 4.0, run a basic System State Report (SSR), download the SSR, and store it externally from Cisco StadiumVision Director. Once you have upgraded both your primary and secondary servers to Release 4.0, they will be configured to retain a single backup file only. You will no longer have access to any 3.2 data after the first 4.0 backup is completed. If for some reason you must revert to Release 3.2, contact Cisco Technical Support and provide them with your SSR file to help you restore it.

To help avoid any need to fall back to Release 3.2, be sure to follow carefully all recommended best practices and post-upgrade tasks as documented in this guide, including thoroughly testing your system to your site requirements before failing over and upgrading your backup server to Release 4.0.

The upgrade process for an existing Cisco StadiumVision Director server involves the following tasks:

- Upgrading the Cisco StadiumVision Director software.
- Upgrading the Cisco DMP 4310G and SV-4K firmware.

For detailed information, see the "Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts" on page 19.

Installing Cisco StadiumVision Director for the First Time

First Published: March 20, 2015

This module describes how to install the Cisco StadiumVision Director Release software on your newly-purchased Platform 3 server hardware from a full ISO image, as well as the requirements for installing Cisco StadiumVision Director on a VM (virtual machine).

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 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.

This module includes the following topics:

- Prerequisites, page 7
- Installation Tasks, page 9
- What To Do Next, page 17

Prerequisites

Caution Do not alter the RAID configuration prior to installation.

Refer to the *Release Notes for Cisco StadiumVision Director Release 4.0* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

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

Platform 3 Servers

- 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 C: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 57.

- 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**..

Virtualized Server Environment

Installing Cisco StadiumVision Director in a virtualized server environment includes setting up your server environment, running the full ISO for Cisco StadiumVision Director, and configuring the network. For more information see the "Hardware Prerequisites" section on page 2 and "Installing on a Virtual Server for the First Time" section on page 4 in the "Getting Started Installing or Upgrading Cisco StadiumVision Director" module on page 1.

Installation Tasks

Note This section includes the tasks to install Cisco StadiumVision Director for the first time on a Platform 3 server.

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 9 (required)
- Logging Into the CIMC Interface, page 10 (required)
- Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director, page 11 (required)
- Launching the KVM Console, page 12 (required)
- Mapping the Cisco StadiumVision Director ISO Image, page 13 (required)
- Installing the Cisco StadiumVision Director ISO Image, page 14 (required)
- Configuring the Network Setup, page 14 (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-4.0.0-*nnn*.x86_64.iso • SV-DIRECTOR-FULL-4.0.0-*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

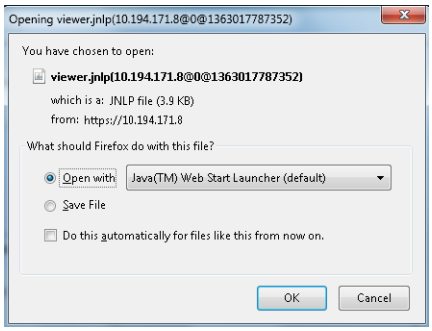
To log into the CIMC interface, complete the following steps:

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

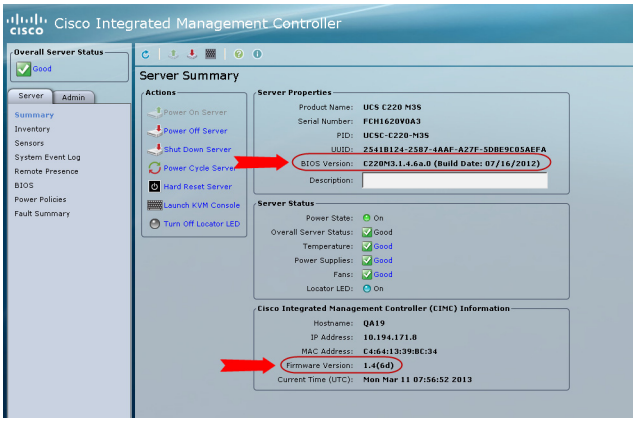
Before you begin, see the "Cisco StadiumVision Director Server Support" section of the *Release Notes for Cisco StadiumVision Director Release 4.0* to find the CIMC/BIOS versions tested for the Platform 3 server.

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



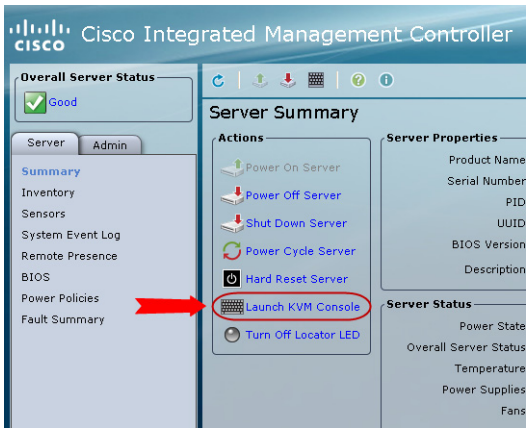
Step 2 If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to "Appendix C: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module on page 57.

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.

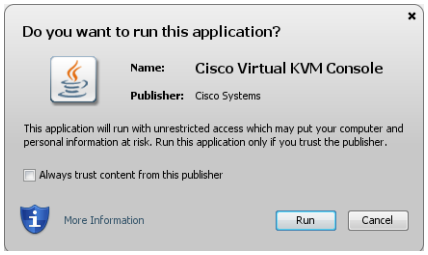
b. Click **Yes** to accept the certificate and continue.

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**.

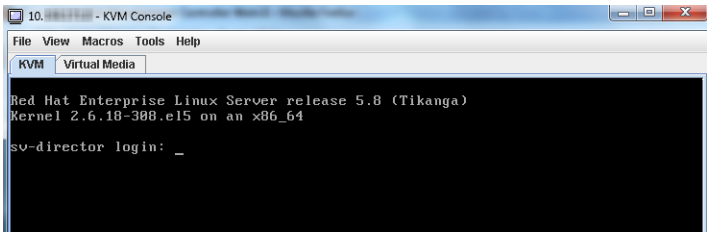
Figure 5 Cisco Virtual KVM Console Confirmation



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

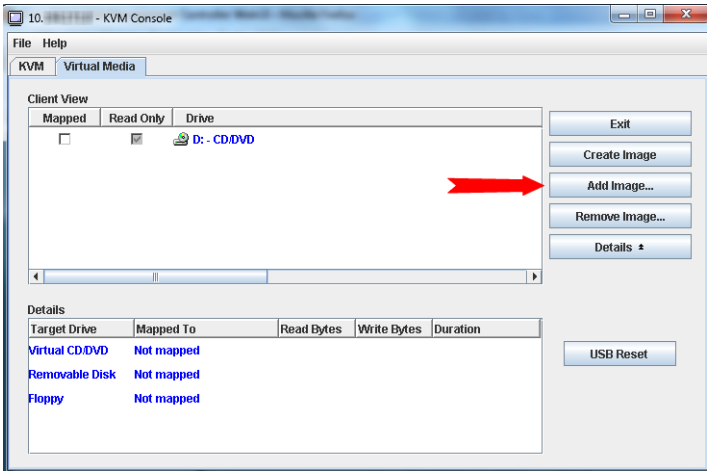
Note This step requires that you have downloaded the Cisco StadiumVision Director full ISO image file for the Platform 3 server from Cisco.com and it is accessible from the computer that you are using to log into the CIMC interface.

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).

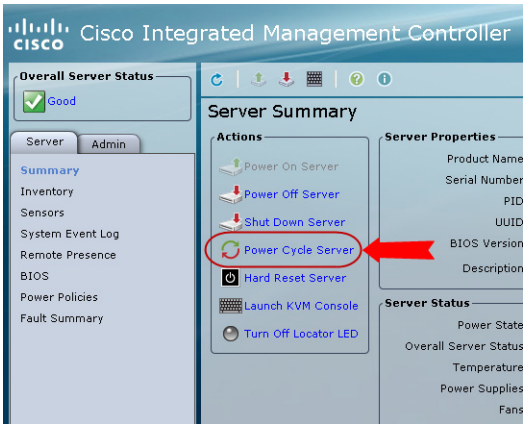
Step 7 Click the KVM tab and minimize the window but do not exit.

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

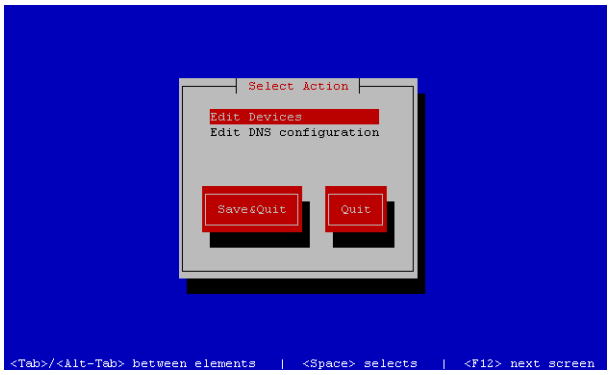
To configure the network setup, complete the following steps:

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**.

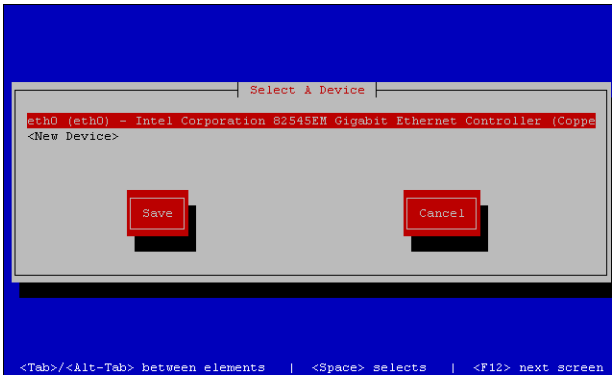
Figure 9 Select Action Screen



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

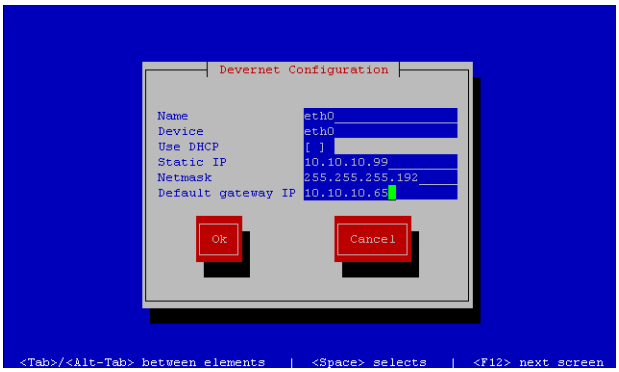


The Ethernet Configuration screen is displayed.

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.

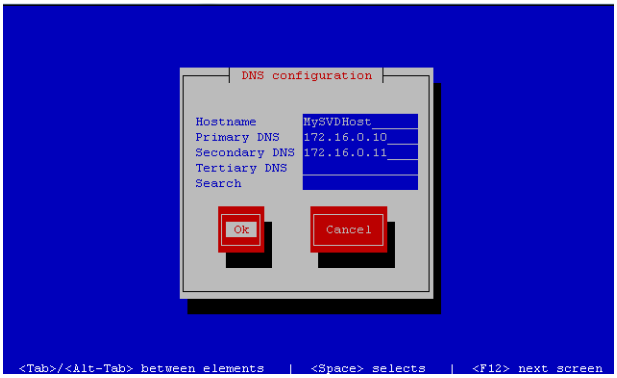
Step 7 Press the down arrow key to select the **Edit DNS configuration** option and press **Enter**.

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, do the following:

Note For initial deployments of the SV-4K media player, be sure to follow the instructions in the *Cisco StadiumVision SV-4K Media Player Deployment Guide*.

- Upgrade the Cisco DMP 4310G firmware (as required).

  See "Upgrading the DMP 4310G Firmware" module on page 39.
- Upgrade the SV-4K firmware (required).

  See "Upgrading the SV-4K Firmware" module on page 43.
- Go to the "Configuring Cisco StadiumVision Director Server System Settings" module of the *Cisco StadiumVision Director Server Administration Guide* to complete initial setup of the server, and do the following:
  - Configure NTP on Cisco StadiumVision Servers and DMPs.
  - Configure NTP and PTP for the SV-4K media players.

Note By default, the Cisco DMP 4310G and SV-4K media players use the Cisco StadiumVision Director server as the NTP source. When using PTP on the SV-4K, only the PTP master SV-4K device references an NTP source. If you want to change the NTP source used by the SV-4K, then you need to change the SV-4K global settings.

  - Configure multicast ports for Cisco StadiumVision Director.

Using the Software Manager to Upgrade Cisco StadiumVision Director Software, Language Packs, and Fonts

First Published: March 20, 2015
Revised: October 27, 2015

This module describes using the Cisco StadiumVision Director Software Manager to:

- Upgrade an existing server already running Cisco StadiumVision Director (Release 3.2 or later) to a later release in the supported upgrade path for Cisco StadiumVision Director software.
- Install language packs and fonts.

This module includes the following topics:

- Best Practices, page 19
- Prerequisites, page 21
- Information About Using the Software Manager to Update Existing Cisco StadiumVision Director Software, page 21
- Upgrade Tasks, page 22
- Installing Language Packs, page 25
- Installing Fonts, page 26
- What to Do Next, page 28

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 4.0* 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, Release 4.0*.
- Promote the secondary server to primary.

  For more information about promoting a secondary server to primary, see the "Configuring Failover Between Redundant Cisco StadiumVision Director Servers" module of the *Cisco StadiumVision Director Server Administration Guide, Release 4.0*.
- 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 web browser interface.

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 3.2.0-520 or higher.
- Run a basic System State Report (SSR), download the SSR, and store it externally from Cisco StadiumVision Director.

Caution Once you have upgraded both your primary and secondary servers to Release 4.0, they will be configured to retain a single backup file only. You will no longer have access to any 3.2 data after the first 4.0 backup is completed. If for some reason you must revert to Release 3.2, contact Cisco Technical Support and provide them with your SSR file to help you restore it.

To help avoid any need to fall back to Release 3.2, be sure to follow carefully all recommended best practices and post-upgrade tasks as documented in this guide, including thoroughly testing your system to your site requirements before failing over and upgrading your backup server to Release 4.0.

- 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 4.0*.

Information About Using the Software Manager to Update Existing Cisco StadiumVision Director Software

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 Software Manager.
3. Installing the ISO image using the install function in the Software Manager.

ISO Upgrade Files

You can store multiple ISO upgrade files on a Cisco StadiumVision Director server. The files will be displayed with a version number and the ISO filename in the Software Manager web browser interface for you to select which file to install.

Disk Maintenance

There is no automatic aging of ISO upgrade files, but you can delete files directly in the Software Manager. ISO files can also be deleted via the TUI: **Troubleshooting > Disk Monitoring > Delete Files > Clean upgrade ISO files**.

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 22 (required)
- Uploading and Installing an ISO Upgrade File on the Cisco StadiumVision Director Server, page 23 (required)
- Reactivating Custom Fonts, page 24 (as required)
- Rebooting SV-4K Devices, page 24 (required)
- Staging the Flash Template for Cisco DMP 4310G Devices, page 24 (required)
- Deploying Global DMP Settings for the Cisco DMP 4310G, page 25 (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.

Note This site page is 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.

Table 1 ISO Upgrade Filename Conventions

Hardware Product ID	Filename Convention[1]
SV-DIRECTOR-K9 or SV-PLATFORM2= SV-PLATFORM3=	• SV-DIRECTOR-UPGRADE-4.0.0-*nnn*.x86_64.iso • SV-DIRECTOR-UPGRADE-4.0.0-*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 the Software Manager UI to verify the checksum on the .iso file.

The md5 checksum is calculated by the system, and is shown on the Software Manager UI. Compare what is shown on the UI and the downloaded md5 checksum.

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

Uploading and Installing an ISO Upgrade File on the Cisco StadiumVision Director Server

After you have downloaded the ISO upgrade file from Cisco.com, you will use the Software Manager to both upload the file to the Cisco StadiumVision Director server. and 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.

Task

To upload and install an ISO upgrade file on 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.

Step 3 Click **Manage Software**.

Step 4 From the **Upgrade** tab, click **Upload**.

Step 5 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**. The file is sent to the server.

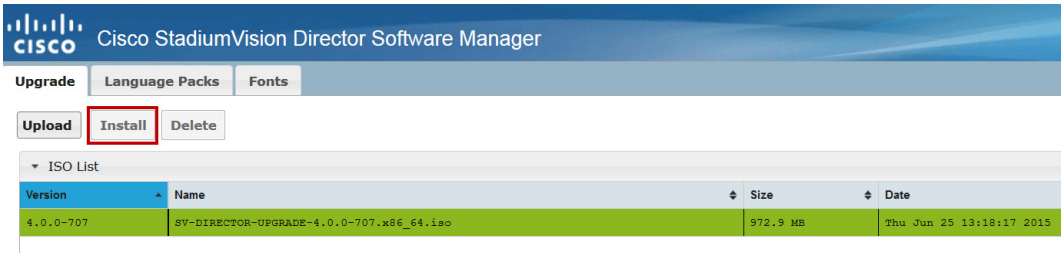
When the ISO upload is complete, one of the following occurs:

- 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.

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

Step 6 Select the image file and click **Install** (Figure 1).

Figure 1 ISO File Selection and Install



Step 7 The installation process begins, and status messages are displayed.

Step 8 After the installation is complete, Cisco StadiumVision services are restarted.

Reactivating Custom Fonts

If you have already installed custom fonts in Cisco StadiumVision Director prior to upgrade, then you will need to reactivate those fonts from the Software Manager after you upgrade.

To reactivate custom fonts, complete the following steps:

Step 1 From the Cisco StadiumVision Director main menu, click **Manage Software**.

Step 2 From the Software Manager screen, click **Fonts**.

Step 3 Select the fonts to be activated.

Step 4 Click **Activate Selected**.

Step 5 (Cisco DMP 4310G only) Stage the Flash Template.

Rebooting SV-4K Devices

After you have completed an ISO upgrade for Cisco StadiumVision Director, you must reboot all of the SV-4K devices in the system to obtain the latest runtime software.

Staging the Flash Template for Cisco DMP 4310G Devices

To be sure that any changes that might have been made to the Cisco StadiumVision Director Flash Template (.swf file) are deployed to the Cisco DMP 4310G, 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 Cisco DMP 4310G devices where the command should be applied.

Tip If you have a mixed deployment of SV-4K and Cisco DMP 4310G devices, then you can use the new Search filter to filter by Model and select only DMP 4310 devices.

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

Deploying Global DMP Settings for the Cisco DMP 4310G

To apply the global MIB variable settings to all Cisco DMP 4310G devices, 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 Cisco DMP 4310G devices.

Installing Language Packs

Note Language packs are release-specific. You can install language packs for Release 4.0.0-601 when they become available, after you have installed or upgraded to Release 4.0.0-601.

You have increased flexibility to upload and install only the specific language(s) that you want to support through the independent installation of Language Packs as they become available for the release. The upload and installation of the language packs is performed using the new Software Manager from the Cisco StadiumVision Director main menu.

To install language packs, complete the following steps:

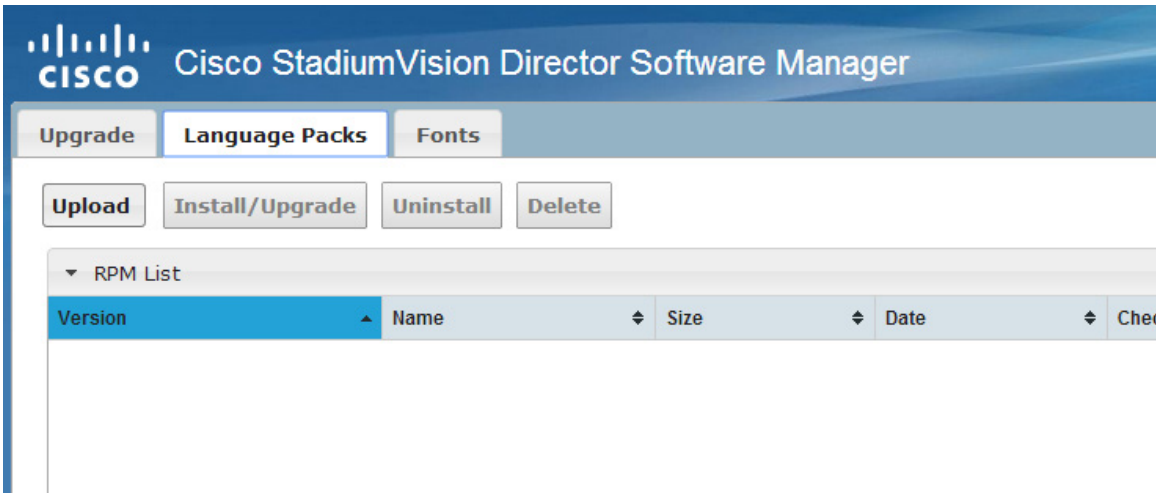
Step 1 Download the desired language pack from Cisco.com.

Step 2 Log into Cisco StadiumVision Director as an administrator.

Step 3 From the main menu, click **Manage Software**.

Step 4 From the Software Manager screen, click **Language Packs** (Figure 2).

Figure 2 Language Packs Tab



Step 5 Click **Upload**.

Step 6 In the File Upload dialog box, navigate to the downloaded Language Pack RPM file, and click **Open**.

The language pack is sent to the server.

Step 7 Click **Install/Upgrade** to install the language pack.

Note If using a secondary Cisco StadiumVision Director server, the language pack should be installed on both the primary and secondary servers.

Step 8 (SV-4Ks only) To transfer the locales to the SV-4K media players, do the following:

a. From the Management Dashboard, go to:

DMP and TV Controls > DMP Install > Restore Default Settings

b. In the Select Devices panel, select the SV-4K media player devices.

Tip If you have a mixed deployment of SV-4K and Cisco DMP 4310G devices, then you can use the new Search filter to filter by Model and select only SV-4K devices.

c. To execute the command, click the play (>) button located at bottom left of the panel.

Installing Fonts

Note Follow these guidelines to install new fonts on your system for use in the Widgets tool. If you have already installed custom fonts prior to upgrade, then you only need to reactivate them. See the "Installing Language Packs" section on page 25.

This section includes the following topics:

- Guidelines for Installing Fonts, page 27
- Procedure, page 27

Guidelines for Installing Fonts

Consider the following guidelines before installing fonts:

- To save system memory on the media player, install fonts that have the minimal set of required characters.
- Cisco StadiumVision Director can support approximately 30,000 installed glyphs.
- Asian languages like Chinese (which contain more glyphs) require more memory.
- The fallback font is Arial; it will be used as the default font in cases where the widget is referencing a font that is not available.
- Only True Type (.ttf) and OpenType (.otf) fonts are supported.

Procedure

To install fonts, complete the following steps:

Step 1 Obtain the desired fonts.

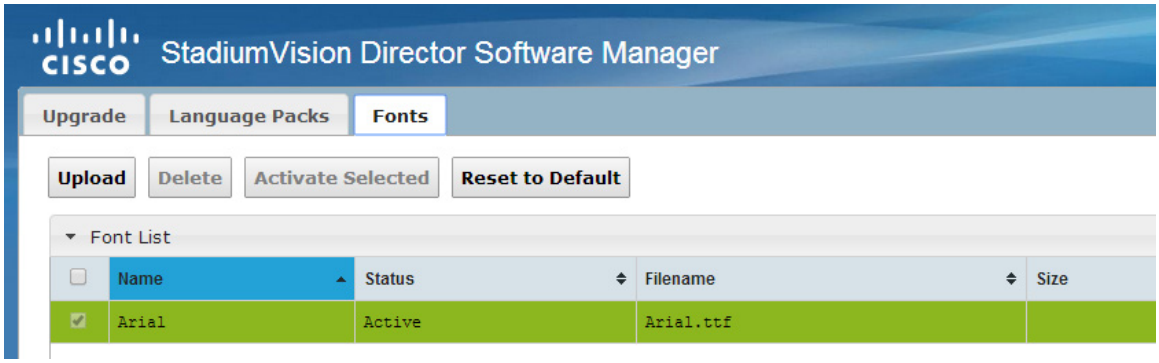
Note Fonts must be TrueType (.ttf) or OpenType (.otf).

Step 2 Log into Cisco StadiumVision Director as an administrator.

Step 3 From the main menu, click **Manage Software**.

Step 4 From the Software Manager screen, click **Fonts** (Figure 3).

Figure 3 Fonts Tab



Step 5 Click **Upload**.

Step 6 In the Font Upload dialog box, do the following:

a. Click **Browse**.

b. Navigate to the location of your font file and click **Open**.

c. Click **Upload**.

Step 7 Click the checkbox of the font to be activated.

Step 8 Click **Activate Selected** to make the font available in Cisco StadiumVision Director.

What to Do Next

- Follow the steps in the "Verifying the Upgrade" module to verify that the upgrade process was successful.
- Use the "Appendix A: Post-Upgrade Checklist" module on page 63 to be sure that you have completed the required verification steps.

Verifying the Upgrade

First Published: March 20, 2015
Revised: August 31, 2015

This module describes how to verify that the upgrade process was successful.

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 29 (mandatory)
- Clearing Expired Flash SWZ Files From Browser, page 30 (required)
- Importing the Security Certificate, page 32 (required)
- Logging Into Cisco StadiumVision Director, page 32 (required)
- Verifying the Control Panel and Other Menus, page 33 (required)
- Verifying that Services are Running, page 33 (required)
- Configuring the Media Player for VLAN Compliance Checking, page 34 (required)
- Verifying Media Players, Groups, and Zones in the Management Dashboard, page 36 (required)
- Verifying the Multicast Configuration, page 36 (required)
- Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 37 (required if using Quest for commerce integration)
- Completing the Post-Upgrade Checklist and Testing, page 39 (required)

Clearing the Browser Cache

Caution It is critical that *all* Cisco StadiumVision Director users clear their browser cache to prevent permanent database corruption and to be sure that you are running the latest version of Cisco StadiumVision Director. Be sure to notify all users of the Cisco StadiumVision Director system to clear their browser cache before using the system after an upgrade.

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**.

Clearing Expired Flash SWZ Files From Browser

This section includes the following tasks:

- Clearing the Flash Player Cache, page 30
- Deleting Other Cached Files From Flash, page 31

Clearing the Flash Player Cache

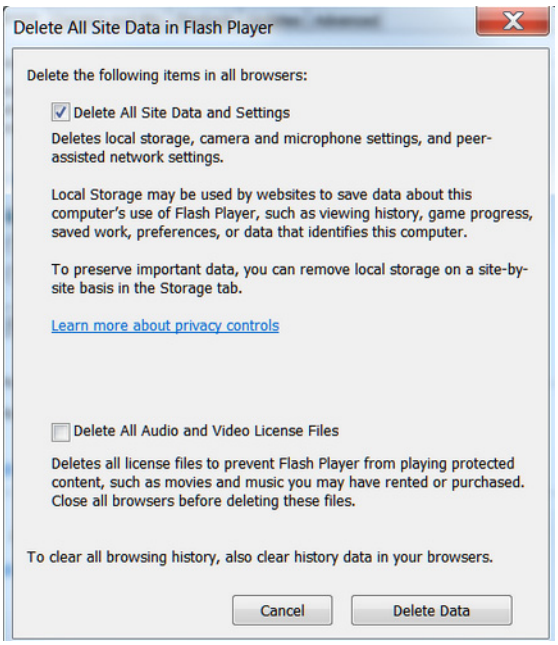
To clear the Flash player cache, complete the following steps:

Step 1 Go to **Control Panel > Flash Player**.

Step 2 In the Flash Player Manager Settings dialog box (Storage tab), click **Delete All**.

Step 3 Select Delete All Site Data and Settings (Figure 1).

Figure 1 Delete All Site Data in Flash Player Dialog Box—Windows Client Example



Step 4 Click **Delete Data**.

Deleting Other Cached Files From Flash

To delete other cached files from Flash, complete the following steps:

Step 1 Close the browser window.

Step 2 Delete cached files in the following paths for your browser application, and depending on your laptop client:

- From a Windows client:
  - For Chrome

    C:\Users*username***\AppData\Local\Google\Chrome\User Data\Default\Pepper Data\Shockwave Flash\CacheWritableAdobeRoot\AssetCache**

  - For Mozilla Firefox

    C:\Users*username***\AppData\Local\Mozilla\Firefox\Profiles**

Tip The AppData folder is a hidden folder in Microsoft Windows. If you cannot view it, go to **Control Panel > Folder Options** and verify the option is set to display hidden files and folders.

- From an Apple Mac OS X client:
  - For Chrome

    /Users/*username***/Library/Application Support/Google/Chrome/Default/Pepper Data/Shockwave Flash/CacheWritableAdobeRoot/AssetCache/**

– For Mozilla Firefox

/Users/*username***/Library/Application Support/Firefox/Profiles/**

Importing the Security Certificate

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

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 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 .

Step 2 Verify that the correct version is displayed.

Tip If your window is not displaying the correct version, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 29.

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.

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 29.

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

Verifying that Services are Running

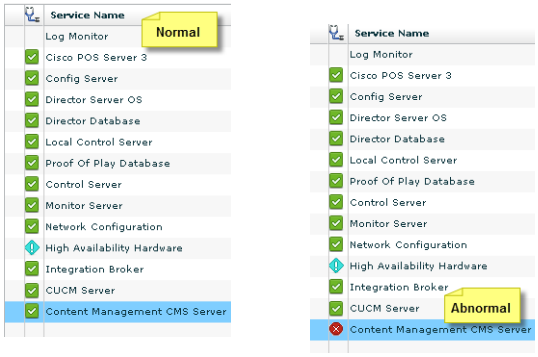
After you upgrade, go to the Management Dashboard to verify that all of the primary Cisco StadiumVision Director services are running.

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 2 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 Media Player for VLAN Compliance Checking

After you upgrade, you need to go to the Management Dashboard and change the Assigned VLAN property according to your VLAN configuration for the media players if you want to perform VLAN compliance checking.

Note Setting the assigned VLAN property for the Cisco DMP 4310G or SV-4K media players is only recommended if all devices are located on the same VLAN. When a value is set, it is checked against what is being sent by the media player. Otherwise, you should configure **$svd_ignore**, which is the default.

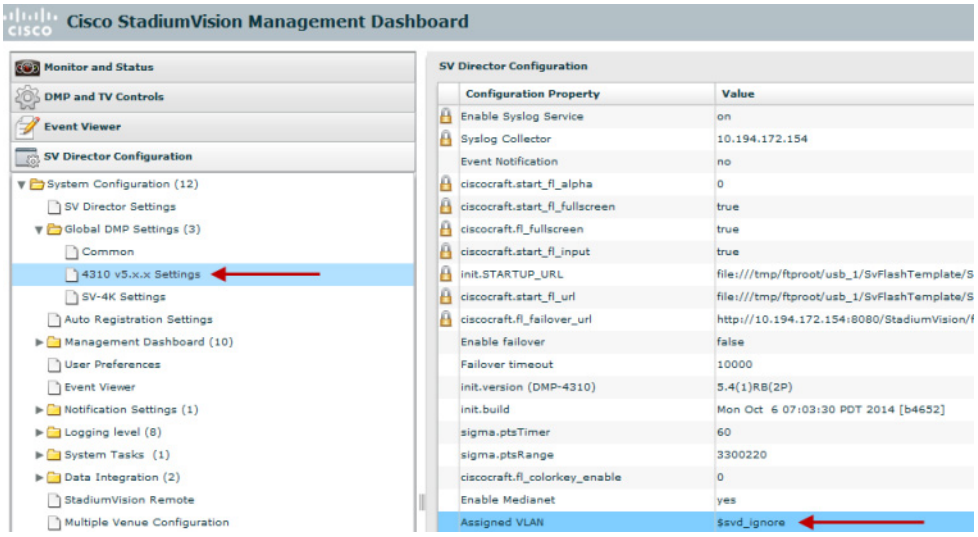
To configure the Assigned VLAN property, complete the following steps:

Step 1 From the Management Dashboard, go to **SV Director Configuration > System Configuration > Global DMP Settings**.

Step 2 Do the following depending on your media player model:

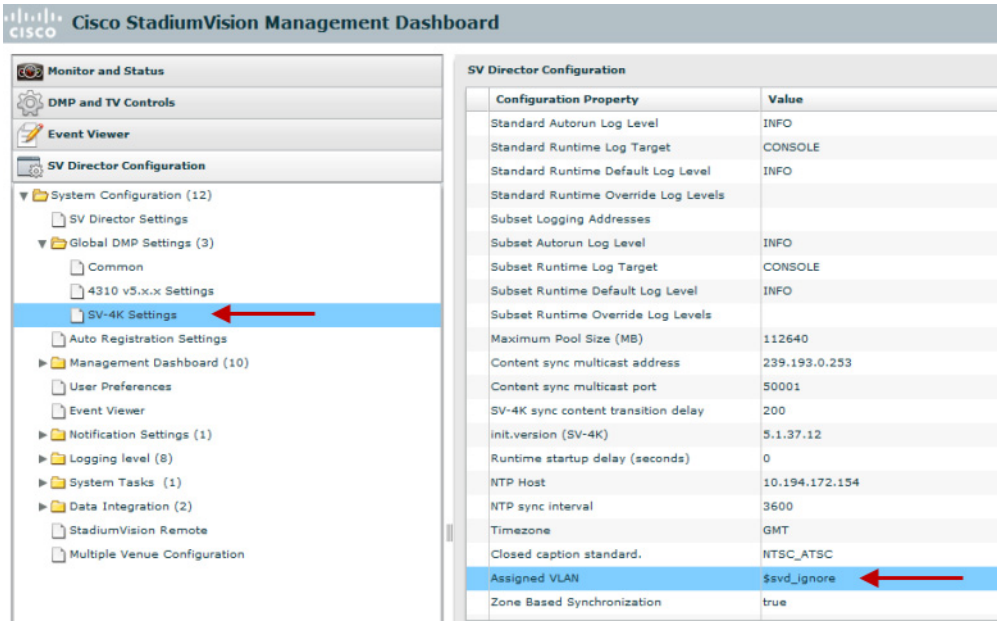
- For the DMP 4310G—Go to **4310 v5.x.x Settings** (Figure 3).

Figure 3 Assigned VLAN Property Configuration for the Cisco DMP 4310G



- For the SV-4K—Go to **SV-4K Settings** (Figure 4).

Figure 4 Assigned VLAN Property Configuration for the SV-4K



Step 3 Find the Assigned VLAN property, and do the following:

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

Caution Cisco DMP 4310 auto-registration support requires that the VLAN value is correctly set or "$svd_ignore" is used.

Step 4 Click the Save icon.

Verifying Media Players, Groups, and Zones in the Management Dashboard

Note Before you verify media player status, be sure that you have set the Assigned VLAN property so that the VLAN compliance check can be performed. For more information, see the "Configuring the Media Player for VLAN Compliance Checking" section on page 34.

To check media players, 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 media players are present and in the green state.

Step 2 From the DMP and TV Controls dashboard drawer, run the Get Status command on all devices to update Cisco StadiumVision Director's record of MAC addresses:

DMP and TV Controls > Monitoring > Get Status.

Step 3 Run Get Status to confirm that all devices have successfully rebooted and are in good health.

Note This will also update the MAC address for the media players.

Step 4 (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 5 Run Get Status to check the device state after the change.

Step 6 Investigate any devices 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.

For more information about multicast configuration, see the "Configuring Multicast Ports for Cisco StadiumVision Director" topic in the "Configuring the Cisco StadiumVision Director Server System Settings" module of the *Cisco StadiumVision Director Server Administration Guide, Release 4.0*.

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.

The steps described in this section assume that Quest has the notification service installed and enabled.

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.

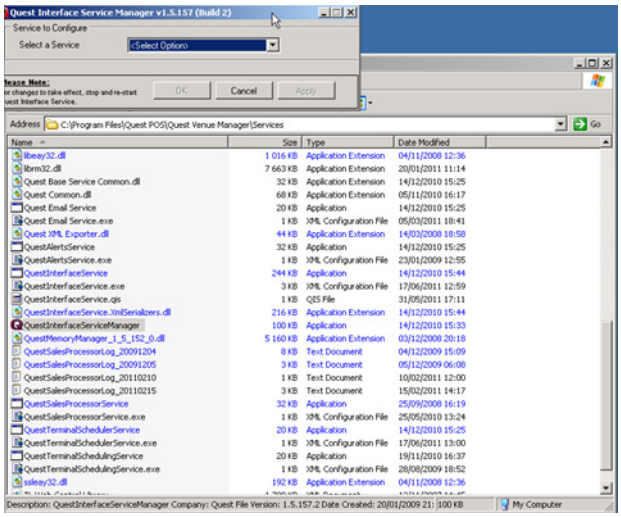
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

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 5).

Figure 5 QuestInterfaceServiceManager Application



Step 4 When the Quest Interface Service Manager application window opens, specify the following options (Figure 6):

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

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

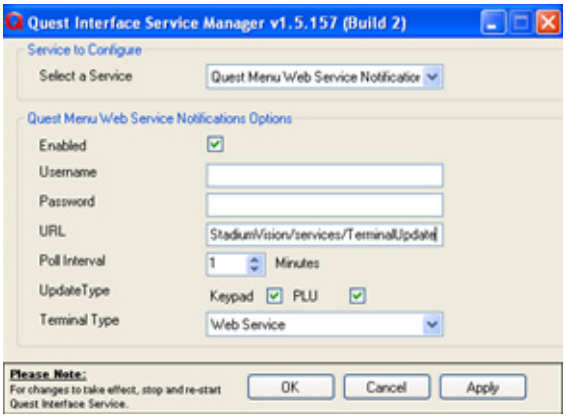
c. In the URL box, enter "**http://svd:8080/StadiumVision/services/TerminalUpdate**".

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 6 Select a Service to Configure



Step 5 Click **OK**.

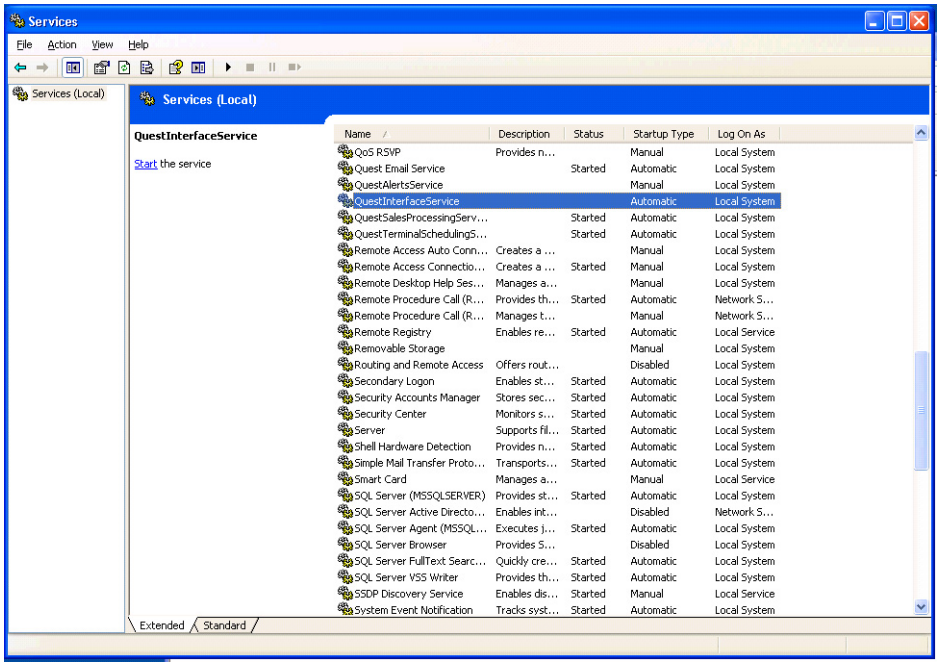
Step 6 Restart the windows service to implement the configuration by completing the following steps:

a. From the Quest Server, click **Start > Run. . .**

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

c. Find the Quest Interface Service and restart it (Figure 7).

Figure 7 Restart the Quest Interface Service



Completing the Post-Upgrade Checklist and Testing

Use the "Appendix A: Post-Upgrade Checklist" module on page 63 to be sure that you have completed the required verification steps.

Upgrading the DMP 4310G Firmware

First Published: March 20, 2015

This modules described how to download and upgrade the DMP 4310G firmware using the Cisco StadiumVision Director Management Dashboard.

Contents

- Prerequisites, page 39
- Upgrade Tasks, page 39

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 4.0*.

Upgrade Tasks

To upgrade the DMP firmware, complete the following tasks:

- Downloading the DMP Firmware, page 39 (required)
- Upgrading the DMP Firmware From the Management Dashboard, page 40 (required)
- Disabling Failover on all DMPs, page 42 (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 5.4.1 RB2P is required for the GNU Bash fix.

DMP-4310G Version 5.4.1 RB2P

To download the DMP-4310G Version 5.4.1RB2P firmware, go to the Cisco Digital Media Players product page for the Cisco DMP 4310G:

http://www.cisco.com/c/en/us/support/video/digital-media-player-4310g/model.html

1. Click the **Downloads** tab and then **Digital Media Player (DMP) System Upgrades**.
2. Go to **All Releases > 5 > 5.4.1_RB_2P**.
3. Click **Download** to get the 5.4.1_RB2_2P_FCS_4310.fwimg file.

Upgrading the DMP Firmware From the Management Dashboard

This section provides a summary of the steps to perform to upgrade your DMP firmware. 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 = 5.4(1)RB(2P) (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.

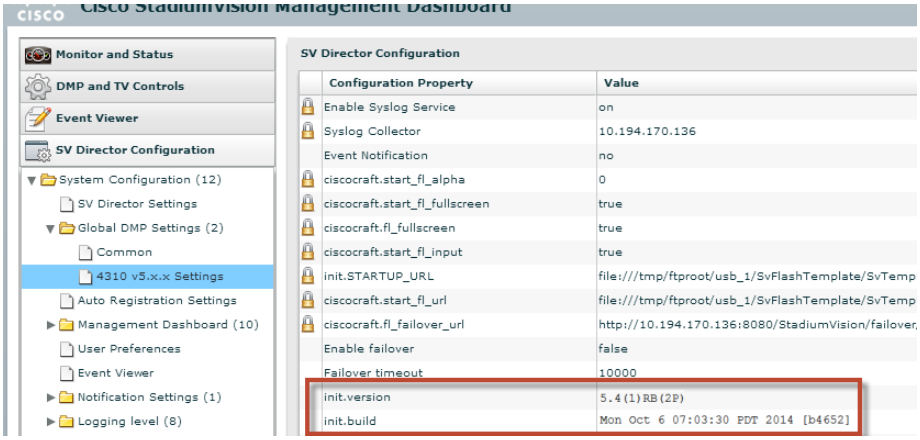
  - For firmware version 5.4.1 RB2P:

    init.version = 5.4(1)RB(2P)
    init.build = Mon Oct 6 07:03:30 PDT 2014 [b4652]

Note In the "init.build" string there are 2 spaces between "Oct" and "6".

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 Settings as shown in Figure 1.

Figure 1 Global DMP Settings in Management Dashboard

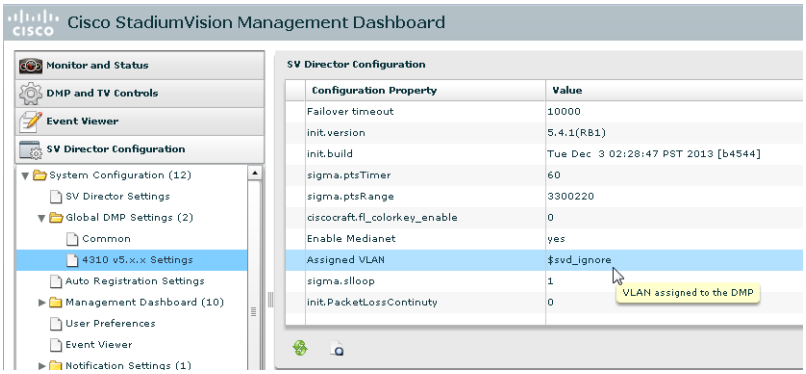


Step 5 Configure the Assigned VLAN property under the 4310 v5.x.x as $svd_ignore or the actual VLAN number on which your DMPs reside. Do *not* leave blank.

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

You will need to set the Assigned VLAN property value for the 4310 v5.x.x Settings (Figure 2):

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 and later releases, 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**.

Upgrading the SV-4K Firmware

First Published: March 20, 2015
Revised: May 1, 2015

Note This module describes how to upgrade the firmware for an existing SV-4K deployment. If you are deploying an SV-4K media player for the first time, see the *Cisco StadiumVision SV-4K Media Player Deployment Guide*.

The SV-4K firmware is not provisioned the same way as the Cisco DMP 4310G. The primary difference is that the SV-4K firmware upgrade is not initiated from the Management Dashboard, but is done automatically when the SV-4K device starts up or reboots.

Each time the SV-4K device is powered on or reboots, a compliance check is done against the firmware that is loaded on the device against the Cisco StadiumVision Director auto-registration settings. If the firmware versions do not match, the SV-4K initiates a firmware upgrade automatically.

Contents

- Prerequisites, page 43
- Provisioning Tasks, page 44

Prerequisites

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

- You have read the *Cisco StadiumVision Release Notes for Release 4.0* to obtain the latest information and to verify the supported SV-4K firmware upgrade paths.
- The Connected Stadium switch is configured, including the required LLDP for proper POE+ operation.
- A DHCP server has been configured with required Option 60 and Option 43 properties.

For more information, see the *Cisco Connected Stadium Design Guide* available to qualified Cisco StadiumVision partners on ciscoet.com.

Provisioning Tasks

To provision the SV-4K firmware, complete the following tasks:

- Downloading the SV-4K Firmware, page 44 (required)
- Uploading the SV-4K Firmware to Cisco StadiumVision Director, page 44 (required)
- Configuring the SV-4K for Auto-Registration, page 45 (required)

Downloading the SV-4K Firmware

The SV-4K firmware image is not bundled with the Cisco StadiumVision Director software. You must download the firmware image separately from a password-protected site and then upload it to Cisco StadiumVision Director.

For information about how to download the SV-4K firmware, see the "How to Download SV-4K Firmware" document, available to qualified Cisco StadiumVision partners on ciscoet.com.

Tip Be sure to download the firmware to a device that you also can use to access the Cisco StadiumVision Director software.

Uploading the SV-4K Firmware to Cisco StadiumVision Director

After you have obtained the SV-4K firmware image from the external vendor, you must upload the image to Cisco StadiumVision Director.

Note You only go to the Firmware Upgrade page in the Management Dashboard to upload the SV-4K firmware. You *do not* run the command to provision the software on the SV-4K (like you do for the Cisco DMP 4310G). Each time the SV-4K device powers on or reboots, a compliance check is done against the firmware that is loaded on the device against the Cisco StadiumVision Director auto-registration settings. If the firmware versions do not match, the SV-4K initiates a firmware upgrade automatically.

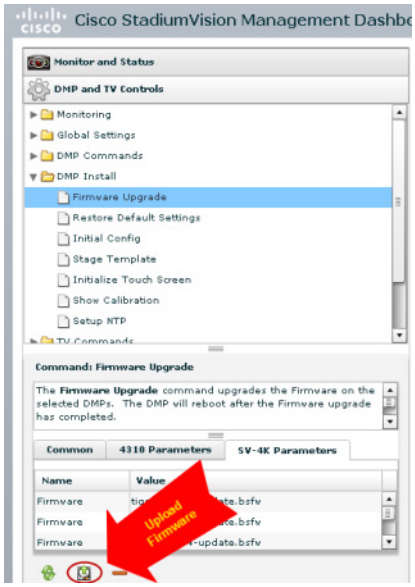
To upload the SV-4K firmware, complete the following steps:

Step 1 From the device where you downloaded the SV-4K firmware, log into Cisco StadiumVision Director as an administrator.

Step 2 Go to the **Management Dashboard > DMP and TV Controls > DMP Install > Firmware Upgrade**.

Step 3 Select the SV-4K Parameters tab and click the upload icon.

Figure 1 SV-4K Firmware Upload



Step 4 Navigate to the SV-4K firmware image file and click **OK**.

An upload status string appears at the bottom of the screen that indicates when the firmware upload is complete.

Configuring the SV-4K for Auto-Registration

Before the firmware can be provisioned to the SV-4K media player, it must be uploaded to Cisco StadiumVision Director, and then configured in the auto-registration settings.

Caution Once you have upgraded to firmware version 5.1.37.12 or later, do *not ever* downgrade to a preliminary 5.0.x version.

To configure the SV-4K for auto-registration, complete the following steps:

Step 1 From the Management Dashboard, go to:

SV Director Configuration > System Configuration > Auto Registration Settings.

Step 2 In the Configuration Property panel, find and configure the following properties (Figure 2):

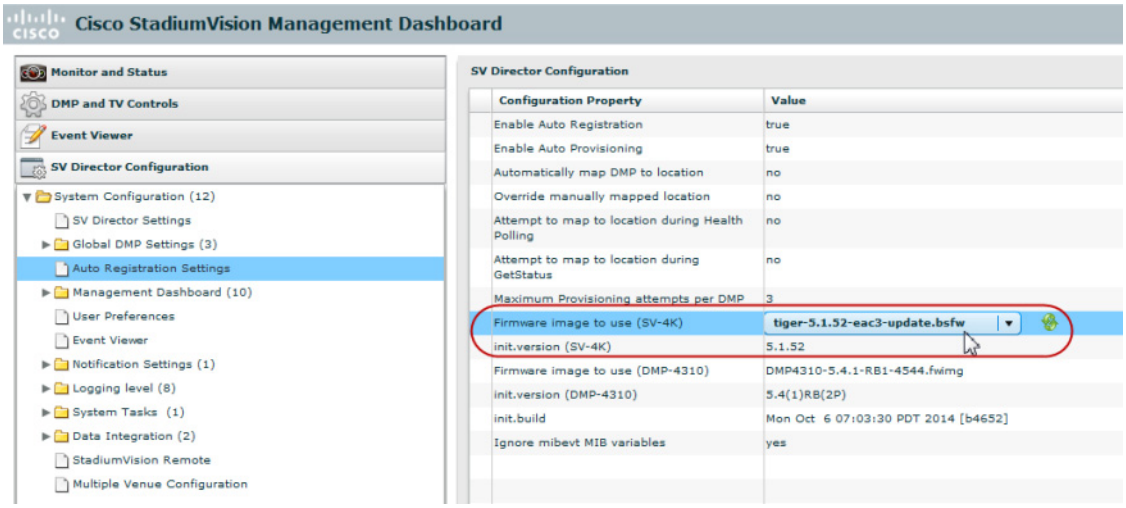
- Firmware image to use (SV-4K)—Select from dropdown box.

Tip If you have just uploaded the firmware image, you need to click the Refresh icon next to the drop-down box for the new file to appear.

- init.version (SV-4K)—Type the version.

Note Be sure that you configure the "Firmware image to use" and "init.version" properties that are labeled for the SV-4K.

Figure 2 SV-4K Auto-Registration Settings



Step 3 Save the changes.

Step 4 Power on or reboot the SV-4K.

Verify the startup sequence. For more information on the startup sequence, see the *Cisco StadiumVision SV-4K Media Player Deployment Guide*.

Appendix A: Post-Upgrade Checklist

First Published: March 20, 2015
Revised: May 18, 2015

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. Do the following in your browser. **a.** Clear the browser cache. **b.** Close all browser windows and wait for 10 seconds before restarting. ⚠ **Caution** Notify *all* Cisco StadiumVision Director users about the mandatory requirement to clear their browser cache and to shutdown/restart the browser software before accessing the latest Cisco StadiumVision Director software.	❑
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.	❑

List Item	Checkoff
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.	❑
11. Start an existing event script and validate that screens display the expected content.	❑
12. Stop the event script and validate that screens are powered off.	❑
13. Make a minor edit to the event script and make sure it can be saved.	❑
14. Verify that you can push a new video file in the Content Management System (CMS) to the DMPs.	❑
15. If using dynamic menu boards, make a change to a menu item and verify that the change is reflected on the menu board.	❑
16. 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.	❑
17. (**As needed for sites that schedule the CMSRestartTask**) Delete the CMSRestartTask from the Scheduled Tasks area of the Management Dashboard. **Note** In Cisco StadiumVision Director Release 4.0, the CMS is automatically restarted after a backup is run.	❑
18. Perform a server backup for the upgrade configuration.	❑

List Item	Checkoff
19. After satisfying your site's testing and event requirements, fail back to the primary server and upgrade it to the same version of software that you validated on your secondary server. **Caution** Before you upgrade your system from Cisco StadiumVision Director Release 3.2 to Release 4.0, run a basic System State Report (SSR), download the SSR, and store it externally from Cisco StadiumVision Director. Once you have upgraded both your primary and secondary servers to Release 4.0, they will be configured to retain a single backup file only. You will no longer have access to any 3.2 data after the first 4.0 backup is completed. If for some reason you must revert to Release 3.2, contact Cisco Technical Support and provide them with your SSR file to help you restore it. To help avoid any need to fall back to Release 3.2, be sure to follow carefully all recommended best practices and post-upgrade tasks as documented in this guide, including thoroughly testing your system to your site requirements before failing over and upgrading your backup server to Release 4.0. For more information, see the "Configuring Failover Between Redundant Cisco StadiumVision Director Servers" module in the *Cisco StadiumVision Director Server Administration Guide*.	❑
20. After you perform failback, be sure that you reconfigure your backup and restore environment using the Text Utility Interface (TUI).	❑

Appendix B: Port Reference

First Published: March 20, 2015

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

- Cisco StadiumVision Director Ports, page 51
- Cisco StadiumVision Director Remote Ports, page 53
- Media Player Ports, page 54

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	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 from a 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.
External NTP server	UDP	123	NTP	Time synchronization (StadiumVision Director as NTP client).
DMP	UDP	514	Syslog	Proof of play, Alerts.

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	UDP	123	NTP server	As request to NTP server, and as response to DMPs.
StadiumVision Director	TCP	443	httpd	4310 web UI.
StadiumVision Director	TCP	80 / 443		Fetching integration broker data. Fetching legacy ticker data.
StadiumVision Director	TCP	8000	autorun.brs	SV-4K control port (http)
StadiumVision Director	TCP	8089	tomcat	Configuration update for multicast rebroadcaster.

Table 3 Cisco StadiumVision Director Output Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	UDP	varies (default:50001)	DMP flash template	Multicast commands (default is 239.192.0.254:50001).
StadiumVision Director	UDP	varies (default:50080-50099)	DMP flash template	Multicast commands when per-script multicast is enabled.

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.
External NTP server	UDP	123	NTP	Time synchronization response.
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	UDP	123	NTP	NTP requests initiated by StadiumVision Director Remote to its NTP server.
StadiumVision Director Remote	UDP	Default: 7778	DMP flash template	Multicast commands (Default is 239.193.1.1:7778)

Media Player Ports

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

- Common Media Player Input Ports, page 54
- Input Ports—DMP 4310G Only, page 55
- Input Ports—SV-4K Only, page 55
- Common Media Player Output Ports, page 56
- Output Ports—SV-4K Only, page 56

Common Media Player Input Ports

Table 7 lists the input ports used by both the Cisco DMP 4310G and the SV-4K media players.

Table 6 Common Media Player Input Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	UDP	varies (default: 50001)	DMP flash template	Multicast commands (default is 239.192.0.254:50001)
StadiumVision Director	UDP	varies (default: 50080-50099)	DMP flash template	Multicast commands when per-script multicast is enabled.
Headend	UDP	varies	Sigma chipset	Multicast video
NTP server	UDP	123	NTP	Time sync response.

Input Ports—DMP 4310G Only

In addition to the common media player output ports (Table 6), Table 7 lists the input ports only used by the Cisco DMP 4310G.

Table 7 DMP Input Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	TCP	22	SSH/Rsync	Rsync for content staging.
Laptop	TCP	22	SSH	SSH diagnostic port
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)
StadiumVision Director	UDP	varies (default:50080-50099)	DMP flash template	Multicast commands when per-script multicast is enabled.
Headend	UDP	varies	Sigma chipset	Multicast video
NTP server	UDP	123	NTP	Time sync response.

Input Ports—SV-4K Only

In addition to the common media player output ports (Table 6), Table 8 lists the input ports only used by the SV-4K media player.

Table 8 SV-4K Input Ports

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	22	SSH	SSH diagnostic port.
Laptop	TCP	80	SV-4K diagnostic web server (dws)	—
Laptop	TCP	2099	SV-4K javascript inspector (for debugging)	—
StadiumVision Director	TCP	8000	SV-4K control and debugging web server	—
SV-4K	UDP	319, 320	PTP	Event and general messages for time sync (SV-4K).
SV-4K	UDP	50001, 50002	SV-4K sync manager port	—

Common Media Player Output Ports

Table 9 lists the output ports used by both the Cisco DMP 4310G and the SV-4K media players.

Table 9 Common Media Player Output Ports

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director	TCP	8080	httpd	Fetching of DMP config, autoprovisioning, and related.
DMP 4310G / SV-4K	TCP	80	httpd	External content URL.
DMP 4310G / SV-4K	TCP	8888	java (Mule)	Fetching preview (data pull requests) from Integration Broker.
DMP 4310G / SV-4K	TCP	9090	Tomcat for Liferay	Dynamic Menu Board application interface.
DMP 4310G / SV-4K	TCP	33333	java (Mule)	Fetching data integration images from Integration Broker.
StadiumVision Director	UDP	123	NTP	Time sync request.
DMP 4310G / SV-4K	UDP	514	syslog	Proof of play. Alerts.

Output Ports—SV-4K Only

In addition to the common media player output ports (Table 9), Table 10 lists the output ports used only by the SV-4K media player.

Table 10 SV-4K Output Ports

Originator	Protocol	Port	Target Application	Usage
SV-4K	UDP	319, 320	PTP	Event and general messages for time sync.
SV-4K	UDP	50001, 50002	SV-4K sync manager port	For sync master.

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

First Published: March 20, 2015

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 57 (required)
- CIMC Firmware Upgrade Guidelines, page 59 (as required)

CIMC Initial Configuration

This section includes the following topics:

- Prerequisites, page 57
- CIMC Initial Configuration Summary, page 58

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/c/en/us/support/video/stadiumvision/products-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 59
- Prerequisites, page 60
- CIMC/BIOS Firmware Upgrade Summary, page 60

Before You Begin

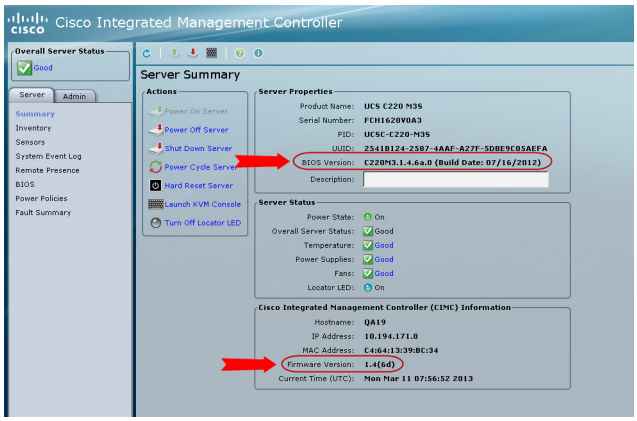
See the release notes for your Cisco StadiumVision product and release at:

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/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/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.

Appendix D: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software

First Published: March 20, 2015

This module describes an alternate metho 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 63
- Prerequisites, page 64
- Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server, page 65
- Upgrade Tasks, page 65
- What to Do Next, page 73

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 4.0* 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, Release 4.0*.
- Promote the secondary server to primary.

  For more information about promoting a secondary server to primary in Release 4.0, see the "Configuring Failover Between Redundant Cisco StadiumVision Director Servers" module of the *Cisco StadiumVision Director Server Administration Guide, Release 4.0*.
- 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 3.2.0-520 (SP2) or higher.
- 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 4.0*.
- 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 there is 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 66 (required)
- Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server, page 67 (required)
- Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server, page 71 (required)
- Staging the Flash Template for the DMP 4310G, page 73 (required)
- Deploying Global DMP Settings for the Cisco DMP 4310G, page 73 (required)
- What to Do Next, page 73 (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.

Note This site page is 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-4.0.0-*nnn*.x86_64.iso • SV-DIRECTOR-UPGRADE-4.0.0-*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.

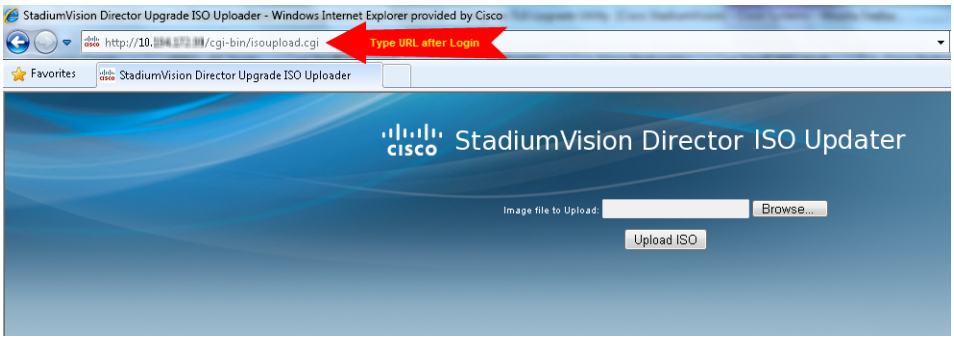
To upload an ISO upgrade file to the Cisco StadiumVision Director server, complete the following steps:

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

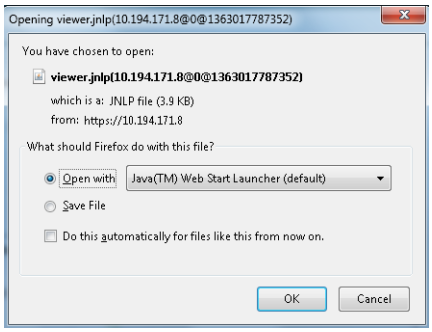
To log into the CIMC interface, complete the following steps:

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

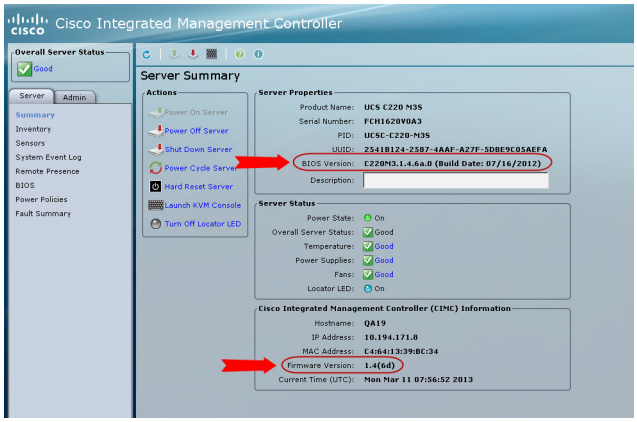
Before you begin, see the "Cisco StadiumVision Director Server Support" section of the *Release Notes for Cisco StadiumVision Director Release 4.0* to find the CIMC/BIOS versions tested for your platform.

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



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.

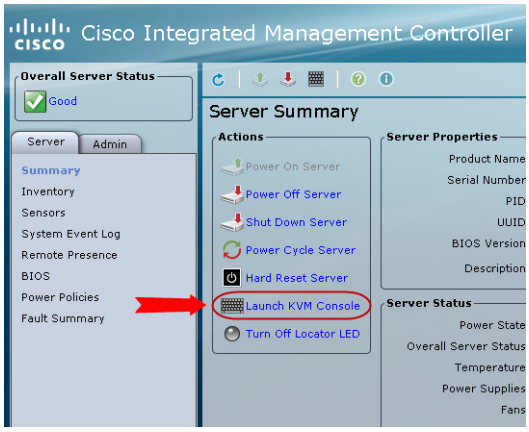
Step 2 If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to the "Appendix C: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server" module.

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.

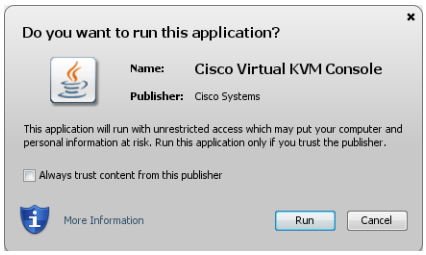
b. Click **Yes** to accept the certificate and continue.

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**.

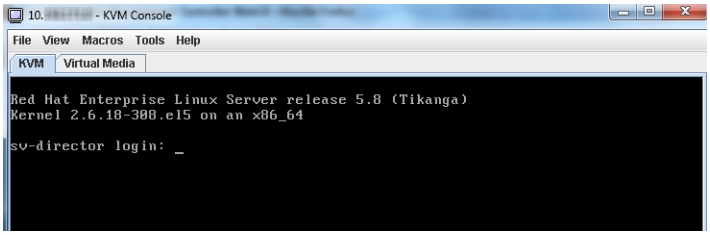
Figure 7 Cisco Virtual KVM Console Confirmation



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

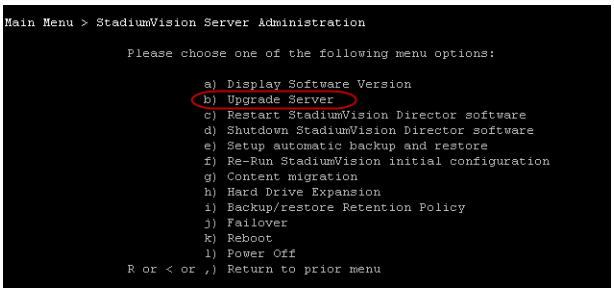
- Log into the CIMC and launch the virtual KVM console.

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:

From the TUI Main Menu, go to the StadiumVision Server Administration menu. Select the Upgrade Server option (type **b** and press **Enter**) (Figure 9):

Figure 9 TUI StadiumVision Server Administration Menu Option for Server Upgrade



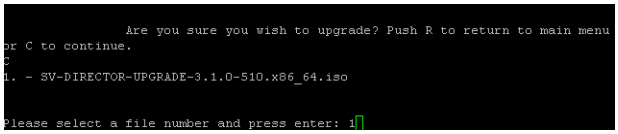
Step 4 When the upgrade configuration confirmation prompt appears, type **c** to continue (Figure 10):

Figure 10 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 11 shows an example of selection of the first upgrade file for installation.

Figure 11 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.

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

Staging the Flash Template for the DMP 4310G

To be sure that any changes that might have been made to the Cisco StadiumVision Director Flash Template (.swf file) are deployed to the Cisco DMP 4310Gs, 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 for the Cisco DMP 4310G

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.

What to Do Next

- Follow the steps in the "Verifying the Upgrade" module to verify that the upgrade process was successful.
- Use the "Appendix A: Post-Upgrade Checklist" module on page 63 to be sure that you have completed the required verification steps.