



StadiumVision



Cisco StadiumVision Director Software Installation and Upgrade Guide

Release 3.2

April 7, 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
© 2014 Cisco Systems, Inc. All rights reserved.



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	4
Upgrading from Release 3.1 SP2 to Release 3.2	4
Installing on a Virtual Server with Release 3.2 for the First Time	5
Installing a Platform 3 Server with Release 3.2 for the First Time	5
Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.2.0-489 or Later	5
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
Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2	19
Contents	19
Best Practices	20
Prerequisites	21
Upgrade Tasks	21
Running Proof of Play Reports	22

- Upgrading the Software From Release 3.1 SP2 to Release 3.2 22
- Extending the Original RAID Volume to Create a Single Group 22
- Upgrading the DMP Firmware 22
- Staging the Flash Template 22
- Deploying Global DMP Settings 23
- Verifying the Upgrade 23
- Verifying the Upgrade 25**
 - Clearing the Browser Cache 25
 - Importing the Security Certificate 26
 - Adding a Security Exception for Mozilla Firefox 26
 - Logging Into Cisco StadiumVision Director 26
 - Verifying the Control Panel and Other Menus 27
 - Verifying that Services are Running 27
 - Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check 28
 - Verifying DMPs, Groups, and Zones in the Management Dashboard 29
 - Verifying the Multicast Configuration 30
 - Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server 30
- Using the Software Manager to Upgrade Cisco StadiumVision Director Release 3.2 Software, Language Packs, and Fonts 33**
 - Best Practices 33
 - Prerequisites 34
 - Information About Using the Software Manager to Update Existing Cisco StadiumVision Director Software 35
 - ISO Upgrade Files 35
 - Disk Maintenance 35
 - Upgrade Tasks 35
 - Downloading ISO Upgrade Files from Cisco.com 36
 - Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server 37
 - Prerequisites 37
 - Staging the Flash Template 38
 - Deploying Global DMP Settings 38
 - Installing Language Packs 38
 - Installing Fonts 39
 - Guidelines for Installing Fonts 39
 - What to Do Next 40
- Upgrading the DMP Firmware 41**
 - Contents 41

Prerequisites	41
Upgrade Tasks	41
Downloading the DMP Firmware	41
DMP-4310G Version 5.4.1 RB2P	42
Upgrading the DMP Firmware From the Management Dashboard	42
Disabling Failover on all DMPs	44

Appendix A: Post-Upgrade Checklist 45

Appendix B: Port Reference 47

Cisco StadiumVision Director Ports	47
Cisco StadiumVision Director Input Ports	47
Cisco StadiumVision Director Output Ports	48
Cisco StadiumVision Director Remote Ports	49
Cisco StadiumVision Director Remote Input Ports	49
Cisco StadiumVision Director Remote Output Ports	49
DMP Ports	51
DMP Input Ports	51
DMP Output Ports	51

Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.2 53

Contents	53
Prerequisites	53
Installation Tasks	54
Installing the Hard Drives Into the Server Chassis	54
Creating a New Logical Volume Using the LSI MegaRAID Utility	55
Extending the Original RAID Volume to Create a Single Group	58
What To Do Next	59

Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server 61

CIMC Initial Configuration	61
Prerequisites	61
CIMC Initial Configuration Summary	62
CIMC Firmware Upgrade Guidelines	63
Before You Begin	63
Prerequisites	64
CIMC/BIOS Firmware Upgrade Summary	64

Appendix E: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software 67

- Best Practices 67
- Prerequisites 68
- Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server 69
 - ISO Upgrade Files 69
 - Disk Maintenance 69
- Upgrade Tasks 69
 - Downloading ISO Upgrade Files from Cisco.com 70
 - Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server 71
 - Prerequisites 71
 - Logging Into the CIMC Interface 72
 - Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director 73
 - Launching the KVM Console 74
 - Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server 75
 - Staging the Flash Template 77
 - Deploying Global DMP Settings 77
- What to Do Next 77



Preface

This document describes the requirements and tasks to install and upgrade the software for Cisco StadiumVision Director Release 3.2.

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

Document Revision History

[Table 1](#) lists the technical changes made to this document since it was first published.

Table 1 Document Revision History

Date	Change Summary
April 7, 2015	Added updates to the “Using the Software Manager to Upgrade Cisco StadiumVision Director Release 3.2 Software, Language Packs, and Fonts” module on page 33, including a new required task for reactivating custom fonts after upgrade.
November 17, 2014	The following changes were made: <ul style="list-style-type: none"> Removed references to obsolete Release 3.2.0-489 in the “Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2” module on page 19. The “Upgrading the DMP Firmware” module on page 41 has been revised to document the “firmware image to use,” “init.version,” and “init.build” strings to be used to specify DMP firmware version 5.4.1 RB2P for the GNU Bash fix.
July 23, 2014	The following changes were made: <ul style="list-style-type: none"> Revised the information about tested VMware vSphere versions and clarified the note about VMware licenses that are not supported in the “Hardware Prerequisites” section on page 2. Removed reference to using the Software Manager as a means for upgrade in the “Upgrading the Software From Release 3.1 SP2 to Release 3.2” section on page 22

Table 1 Document Revision History (continued)

Date	Change Summary
May 14, 2014	Added emphasis of existing requirement for all users to clear browser cache after upgrade to prevent database corruption in the “Verifying the Upgrade” module on page 25 and the “Appendix A: Post-Upgrade Checklist” module on page 45 .
April 21, 2014	First release of this document for Cisco StadiumVision Director Release 3.2

Document Organization

Chapter	Description
“Getting Started Installing or Upgrading Cisco StadiumVision Director”	Provides information that you should read before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 3.2 software.
“Installing Cisco StadiumVision Director for the First Time”	Describes how to install the Cisco StadiumVision Director Release 3.2 software on your newly-purchased Platform 3 server hardware from a full ISO image.
“Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2”	Describes how to upgrade a Cisco StadiumVision Director server previously installed with Release 3.1.0-797 (SP2) to Cisco StadiumVision Director Release 3.2.
“Verifying the Upgrade”	Describes how to verify that the upgrade process was successful.
“Using the Software Manager to Upgrade Cisco StadiumVision Director Release 3.2 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.
“Upgrading the DMP Firmware”	Describes how to upgrade the DMP firmware on the Cisco DMP 4310G.
“Appendix A: Post-Upgrade Checklist”	Provides a checklist that is useful after you upgrade your software on a Cisco StadiumVision Director server.
“Appendix B: Port Reference”	Identifies the ports used by Cisco StadiumVision Director.
“Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.2”	Describes how to install two additional 300 GB hard drives (SV-FRU2-HD3G=) for another RAID 1 volume in the Cisco StadiumVision Director Platform 2 Server which are required to run Cisco StadiumVision Director Release 3.2 with a minimum of 4 drives.

Chapter	Description
“Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server”	Provides guidelines for configuring the Cisco Integrated Management Controller (CIMC) interface and performing the initial configuration, and upgrading the CIMC/BIOS firmware on the Cisco UCS C220 servers for Cisco StadiumVision Director (SV-DIR-DIRECTOR-K9, SV-PLATFORM3=).
“Appendix E: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software”	Describes how to upgrade an existing Cisco StadiumVision Director 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 3.2](#)
- [Cisco StadiumVision Director Server Administration Guide, Release 3.2](#)
- [Cisco StadiumVision Director Localization Guide, Release 3.2](#)
- 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: April 21, 2014

Revised: July 23, 2014

Read this module before you perform an initial installation or upgrade of the Cisco StadiumVision Director Release 3.2 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 3.2](#) for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- The Cisco StadiumVision Director Platform 2 server ships with two 300 GB hard drives configured with RAID 1 mirroring for redundancy. Two additional 300 GB hard drives (SV-FRU2-HD3G=) for another RAID 1 volume in the Cisco StadiumVision Director Platform 2 Server are required to run Cisco StadiumVision Director Release 3.2 with a minimum of 4 drives.



Note

If you need to install additional hard drives in the Platform 2 server to meet the 4-drive minimum requirement to support Release 3.2, then you must perform different upgrade tasks in a certain order.

The physical installation of the additional drives must precede the upgrade to Release 3.1.0-797 (SP2), which is the required prerequisite release to upgrade to Release 3.2.

Refer to the “[Upgrading a Cisco StadiumVision Director Platform 2 Server from Release 3.0 SP2 to Release 3.1](#)” in the [Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.1](#).

- Determine if you have compatible Cisco Digital Media Player (DMP) models and firmware versions installed. The DMP firmware image is not bundled with the Cisco StadiumVision Director software. You must download the firmware image separately from the software download center site for the Cisco Digital Media Player model. For more information about supported firmware versions, see the [Release Notes for Cisco StadiumVision Director Release 3.2](#).
- Be sure that you have a supported browser (Google Chrome Version 31.0, Mozilla FireFox Version 26.0, and Adobe Flash Player (Version 11.9.900.170) 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 3.2 on a Platform 2 or Platform 3 server, or use your own server to run the Cisco StadiumVision Director software. Be sure that your configuration meets the minimum system requirements in [Table 1](#) and supports a VMware virtual machine environment.

**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 3.2](#).

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

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 3.2.

**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 3.2 depending on your current server environment:

- [Upgrading from Release 3.1 SP2 to Release 3.2, page 4](#)
- [Installing on a Virtual Server with Release 3.2 for the First Time, page 5](#)
- [Installing a Platform 3 Server with Release 3.2 for the First Time, page 5](#)
- [Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.2.0-489 or Later, page 5](#)



Note

A full ISO installation on a Platform 2 server is not supported in Cisco StadiumVision Director Release 3.2. Only ISO upgrades are supported.

Upgrading from Release 3.1 SP2 to Release 3.2



Caution

If you need to install additional hard drives in the Platform 2 server to meet the 4-drive minimum requirement to support Release 3.2, then you must perform the upgrade in a certain order. The physical installation of the additional drives must precede the upgrade to Release 3.2, followed by extension of the RAID volume post-upgrade, and then content migration and the remainder of the upgrade verification.

The upgrade process for an existing server running Cisco StadiumVision Director Release 3.1-0-797 Service Pack 2 involves the following tasks:

- Running Proof of Play reports.
- Installing two additional hard drives to meet the 4-drive minimum requirement for Release 3.2 (as required for a Platform 2 Server).
- Performing an ISO upgrade to Cisco StadiumVision Director Release 3.2.
- Extending the Original RAID Volume to Create a Single Group (as required for the HDD expansion on a Platform 2 server).
- Upgrading DMP 4310G firmware.
- Disabling DMP failover for all DMPs. (Disabled is the default beginning in Cisco StadiumVision Director Release 3.1.0-787 [SP1])
- Verifying the upgrade, including validating the content migration.

For detailed information and important best practices and requirements, see the [“Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2”](#) module in this guide.

Installing on a Virtual Server with Release 3.2 for the First Time

The installation process for a virtual server running Cisco StadiumVision Director software release 3.2 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 3.2.

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 3.2 full ISO.
- Run the installation.

Installing a Platform 3 Server with Release 3.2 for the First Time

The installation process for a new Platform 3 server running Cisco StadiumVision Director Release 3.2 for the first time involves the following tasks:

- Confirmation of CIMC/BIOS version and upgrade as required.
- Installation from CIMC of a full ISO image file that runs an installation program with configuration prompts for your network information.
- Disabling DMP failover for all DMPs.
(Disabled is the default beginning in Cisco StadiumVision Director Release 3.1.0-787 [SP1])
- Upgrading the DMP 4310G Firmware.

For detailed information, see the “[Installing Cisco StadiumVision Director for the First Time](#)”.

Upgrading an Existing Cisco StadiumVision Director Server Already Running Cisco StadiumVision Director Release 3.2.0-489 or Later

You can upgrade an existing server already running Release 3.2.0-489 or later software version 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.

For detailed information, see the “[Using the Software Manager to Upgrade Cisco StadiumVision Director Release 3.2 Software, Language Packs, and Fonts](#)”.



Installing Cisco StadiumVision Director for the First Time

First Published: April 21, 2014

This module describes how to install the Cisco StadiumVision Director Release 3.2 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 3.2 software from a *full ISO* image (not an upgrade) that you downloaded from Cisco.com to be sure that you are running the released production version of Cisco StadiumVision Director Release 3.2.

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 3.2](#) 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 D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server”](#) module on page 61.

- 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 with Release 3.2 for the First Time”](#) section on page 5 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=	<ul style="list-style-type: none"> • SV-DIRECTOR-FULL-3.2.0-<i>nnn</i>.x86_64.iso • SV-DIRECTOR-FULL-3.2.0-<i>nnn</i>.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.

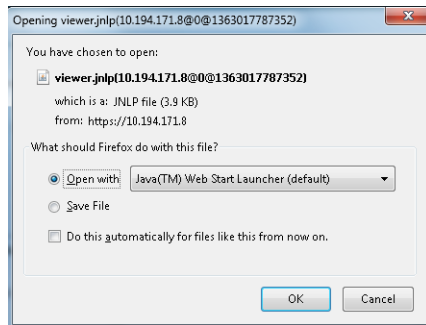
To verify the integrity of your upgrade file from the download, you can use a command-line or GUI utility on your laptop to calculate the checksum on the .iso file. Open the .md5sum file to compare the value that you calculated with the expected value provided in the .md5sum file. The values should match. 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:
- (Optional) Select the checkbox to accept all content from Cisco.
 - Click **Yes** to accept the certificate and continue.
 - Confirm any additional security certificate exceptions.
- Step 4** At the CIMC login screen, note the firmware version displayed ([Figure 2](#)).



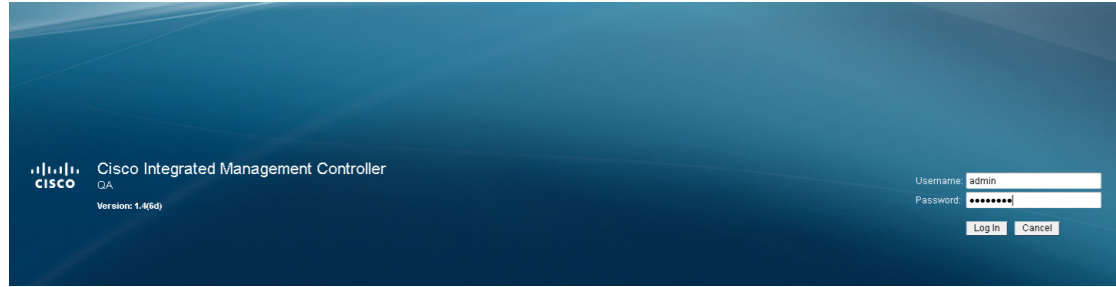
Tip The firmware version is also displayed in the Cisco Integrated Management Controller (CIMC) Information box on the CIMC console after you log in.

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



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

Figure 2 CIMC Login Screen



Step 6 Click **Log In**.

Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director

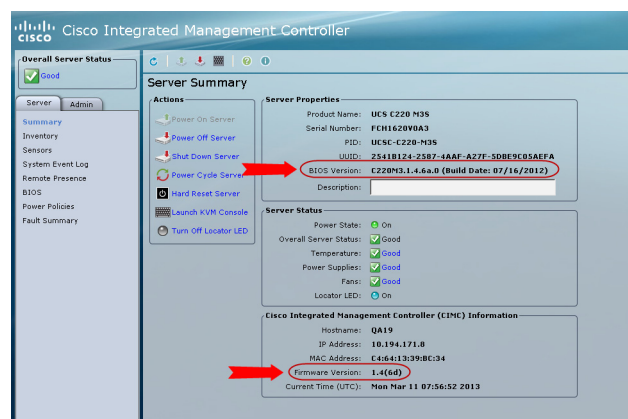
Before you begin, see the “Cisco StadiumVision Director Server Support” section of the [Release Notes for Cisco StadiumVision Director Release 3.2](#) to find the CIMC/BIOS versions tested for the Platform 3 server.

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

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

[Figure 3](#) shows where the firmware version is displayed on the CIMC console for both the BIOS and CIMC firmware.

Figure 3 Firmware Version Verification From the CIMC Console



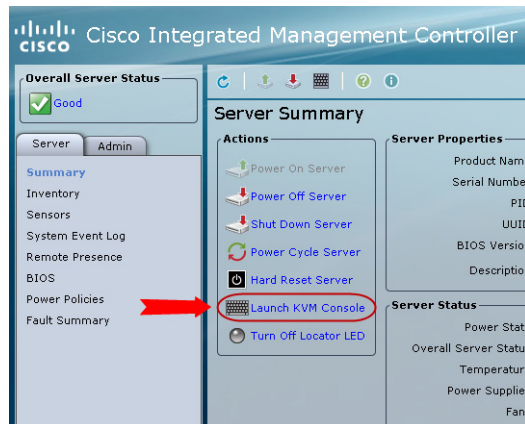
Step 2 If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to “[Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server](#)” module on page 61.

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**.

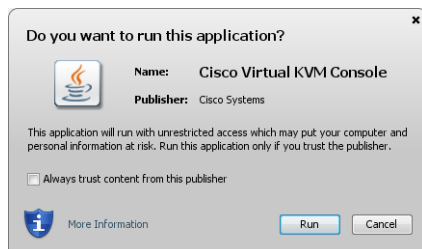
Figure 4 Launch KVM Console



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

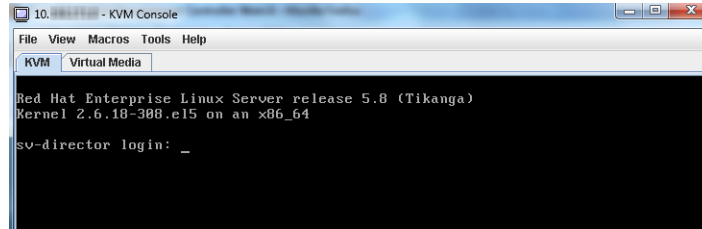
- Step 2** If a security dialog box displays, do the following:
- (Optional) Select the checkbox to accept all content from Cisco.
 - Click **Yes** to accept the certificate and continue.
- Step 3** At the Cisco KVM Virtual Console confirmation box (Figure 5), do the following:
- (Optional) Select the checkbox to accept all content from Cisco.
 - Click **Run**.

Figure 5 Cisco Virtual KVM Console Confirmation



- Confirm any additional security certificate exceptions.

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

Figure 6 Cisco KVM Virtual Console Login Screen

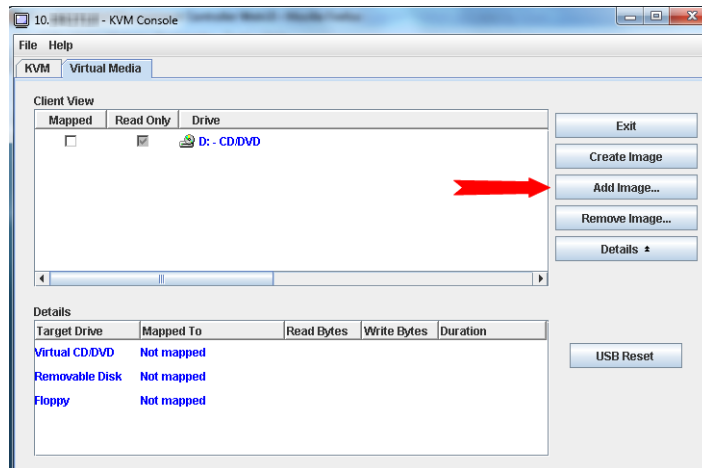
Mapping the Cisco StadiumVision Director ISO Image

**Note**

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

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

- Step 1** From the KVM console window, click the **Virtual Media** tab.
- Step 2** From the Virtual Media screen, click **Add Image** (Figure 7).

Figure 7 Virtual Media Screen

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

**Note**

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

- Step 4** In the Client View box, mark the checkbox under the Mapped column to select the ISO source.
- Step 5** Confirm that the Virtual CD/DVD has been added under the Virtual Media tab, Virtual CD/DVD.

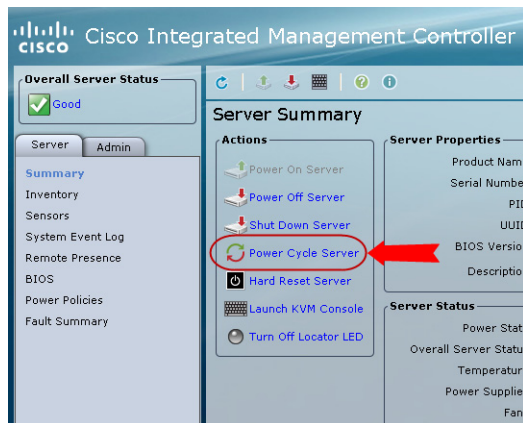
- Step 6** In the Details box, double-click on Virtual CD/DVD, and observe the read bytes counter increasing (refreshes read bytes).
- Step 7** Click the KVM tab and minimize the window but do not exit.

Installing the Cisco StadiumVision Director ISO Image

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

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

Figure 8 Power Cycle Server From the CIMC Console



- Step 2** At the confirmation prompt, click **OK**.
- Step 3** From the KVM console, observe the start of the installation process.

Configuring the Network Setup

To configure the network setup, complete the following steps:

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

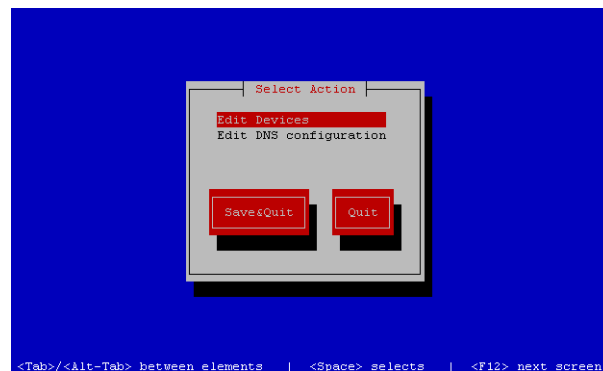


Tip

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

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

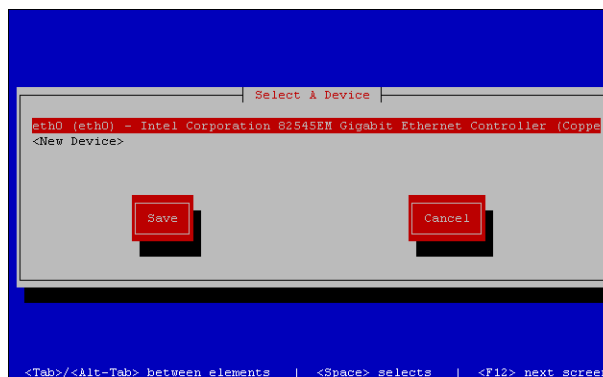
Figure 9 Select Action Screen



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

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

Figure 10 Select a Device Screen



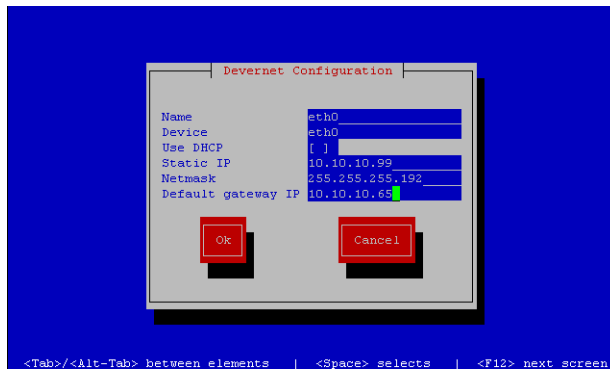
The Ethernet Configuration screen is displayed.



Note The Linux screen is mislabeled “Devernet Configuration.”

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

Figure 11 *Devernet Configuration Screen*



- a. Press the Tab key until the cursor is positioned on the Static IP address line.
- b. Press the backspace key to go to the beginning of the line and type in the IPv4 address of the Cisco StadiumVision Director Server.



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

- c. Press the tab key to go to the Netmask line. Type the network mask for the IPv4 address.
- d. (Optional) In the Default gateway IP line, type the address of the default gateway of your network.

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

You return to the Select a Device screen.

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

You return to the Select Action screen.

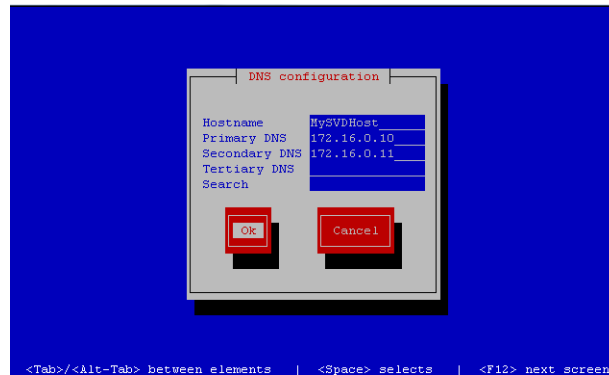
Step 7 Press the down arrow key to select the **Edit DNS configuration** option and press **Enter**.

The DNS configuration screen is displayed.

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



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

Figure 12 DNS Configuration Screen

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

You return to the Select Action screen.

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

What To Do Next

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

- Configuring NTP on Cisco StadiumVision Servers and DMPs
- Configuring Multicast Ports for Cisco StadiumVision Director

See the “[Configuring Cisco StadiumVision Director Server System Settings](#)” module of the *Cisco StadiumVision Director Server Administration Guide* to complete initial setup of the server.



Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2

First Published: April 21, 2014

Revised: November 17, 2014

This module describes how to upgrade a Cisco StadiumVision Director Platform 2 server previously installed with a minimum of Release 3.1.0-797 Service Pack 2 to Cisco StadiumVision Director Release 3.2.

**Caution**

A Cisco StadiumVision Director system that is using language support from Release 3.1.0-797 (SP2), will lose that support if upgraded to Release 3.2. Support for other language translations must be installed as they become available as Language Packs using the new Software Manager from the Cisco StadiumVision Director main menu.

**Note**

Certain locales are not supported in Release 3.2, such as right-to-left languages.

**Note**

Language packs must be installed after upgrading to Cisco StadiumVision Director Release 3.2. See the [“Installing Fonts”](#) section on page 40 for details on installing fonts.

Contents

- [Best Practices, page 20](#)
- [Prerequisites, page 21](#)
- [Upgrade Tasks, page 21](#)
- [Verifying the Upgrade, page 23](#)

Best Practices

Before you begin upgrading a Cisco StadiumVision Director server from Release 3.1.0-797 Service Pack 2 to Release 3.2 software, consider the following best practices:

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the [Release Notes for Cisco StadiumVision Director Release 3.2](#) for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you plan to upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.
- Perform a backup and restore of the primary and secondary servers, and then promote the secondary server:
 - Perform a backup of the currently active primary server.
 - Restore the backup data onto the standby secondary server.



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

For more information about performing a backup and restore on a Cisco StadiumVision Server running release 3.1, see the “[Backing Up and Restoring Cisco StadiumVision Director Servers](#)” module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.1*.

- Promote the secondary server to active.

For more information about promoting a secondary server to active, see the “[Configuring Failover Between Redundant Cisco StadiumVision Director Servers](#)” module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.1*.

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

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

Prerequisites

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

- Be sure that the Cisco StadiumVision Director server meets the following minimum requirements:
 - As required for the Platform 2 server, two additional 300 GB hard drives are installed for a total of four required drives for Release 3.2. Contact your Cisco Systems sales representative for more information about how to obtain additional hard drives.

For information about how to install hard drives to support Release 3.2, see “[Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.2](#)” module on page 53.

- The software is at the minimum release level of Release 3.1.0-797 Service Pack 2. If the server is not at the minimum release level, see the “[Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Director Software](#)” module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.1*.
- The Platform 2 server Unified Computing System (UCS) Server Firmware is at version 1.4(2) to avoid problems powering off the server hardware.

For more information about how to verify and upgrade, see the “[Upgrading the CIMC and BIOS Firmware on a Cisco StadiumVision Director Platform 2 Server](#)” module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.0*.

- Be sure that you have compatible Cisco Digital Media Player (DMP) models and firmware versions. For more information about DMP hardware and software requirements, see the [Release Notes for Cisco StadiumVision Director Release 3.2](#).
- To access the Cisco Integrated Management Controller (CIMC) for the TUI software upgrade, the following requirements are met:
 - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
 - You have a laptop connection with access to the Cisco StadiumVision Director server network.
 - You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
 - You have the CIMC interface login credential. The default is **admin/password**.

**Note**

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

Upgrade Tasks

To upgrade your Cisco StadiumVision Director server from Release 3.1 to 3.2, complete the following tasks:

- [Running Proof of Play Reports, page 22](#) (as required)
- [Upgrading the Software From Release 3.1 SP2 to Release 3.2, page 22](#) (required)
- [Extending the Original RAID Volume to Create a Single Group, page 22](#) (as required)
- [Upgrading the DMP Firmware, page 22](#) (required)

- [Staging the Flash Template, page 22](#) (required)
- [Deploying Global DMP Settings, page 23](#) (required)

Running Proof of Play Reports

Before you perform the upgrade from Release 3.1 to 3.2, be sure that you have processed any outstanding Proof of Play reports. If you do not run these reports before the upgrade, the data will be lost.

For more information, see the [Cisco StadiumVision Proof of Play](#) module.

Upgrading the Software From Release 3.1 SP2 to Release 3.2

The upgrade from Cisco StadiumVision Director Release 3.1 to Release 3.2 is performed as an ISO upgrade using the Text Utility Interface (TUI).

For more information about how to perform the ISO upgrade, see the [“Appendix E: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software”](#) module on page 67.

Extending the Original RAID Volume to Create a Single Group



Note

This task is only required if you had to install additional hard drives to meet the minimum hard drive requirement on the Platform 2 server for Cisco StadiumVision Director Release 3.1 as described in the [“Prerequisites”](#) section on page 21.

For information about running this task, see the [“Extending the Original RAID Volume to Create a Single Group”](#) section on page 58. Return to this module after extending the RAID volume to complete the remaining upgrade tasks, including Upgrading the DMP Firmware.

Upgrading the DMP Firmware

Cisco StadiumVision Director supports DMP-4310G Version 5.4.1 Build 4544.

For more information about how to perform the upgrade, see the [“Upgrading the DMP Firmware”](#) module on page 41.

Staging the Flash Template

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

-
- Step 1** Go to the Management Dashboard.
 - Step 2** From the DMP and TV Controls dashboard drawer, navigate to and select the following command: **DMP and TV Controls > DMP Install > Stage Template.**
 - Step 3** Select all of the DMP devices where the command should be applied.

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

Deploying Global DMP Settings

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

- Step 1** Go to the Management Dashboard.
- Step 2** From the DMP and TV Controls dashboard drawer, navigate to and select the following command:
DMP and TV Controls > Global > Global DMP Settings.
- Step 3** Select all of the DMP devices where the command should be applied.
- Step 4** Click the play button to run the command on the selected devices.
-

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

- Step 1** Complete the verification tasks as described in the [“Appendix E: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software”](#) module on page 67.
- Step 2** Use the [“Appendix A: Post-Upgrade Checklist”](#) module on page 45 to be sure that you have completed the required verification steps.
-



Verifying the Upgrade

First Published: April 21, 2014

Revised: June 4, 2014

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 25](#) (mandatory)
- [Importing the Security Certificate, page 26](#) (required)
- [Logging Into Cisco StadiumVision Director, page 26](#) (required)
- [Verifying the Control Panel and Other Menus, page 27](#) (required)
- [Verifying that Services are Running, page 27](#) (required)
- [Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check, page 28](#) (required)
- [Verifying DMPs, Groups, and Zones in the Management Dashboard, page 29](#) (required)
- [Verifying the Multicast Configuration, page 30](#) (required)
- [Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 30](#) (required if using Quest for commerce integration)

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**.
-

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 to Cisco StadiumVision Director Release 3.2 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 Version 3.2 is displayed.



Tip If your window is not displaying Version 3.2, be sure that you have cleared the browser cache as describe in the [“Clearing the Browser Cache”](#) section on page 25.

- 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 25](#).

- 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 1 Verifying Normal Service States

Service Name	Status
Log Monitor	Normal
Cisco POS Server 3	Normal
Config Server	Normal
Director Server OS	Normal
Director Database	Normal
Local Control Server	Normal
Proof Of Play Database	Normal
Control Server	Normal
Monitor Server	Normal
Network Configuration	Normal
High Availability Hardware	Normal
Integration Broker	Normal
CUCM Server	Normal
Content Management CMS Server	Abnormal

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

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

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

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

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

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



Caution

DMP auto-registration support requires that the VLAN value is correctly set or “\$svd_ignore” is used.



Note

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

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

- Step 1** Go to the Management Dashboard, and click **SV Director Configuration > System Configuration > Global DMP Settings**.
- Step 2** Complete both of the following steps, as shown in [Figure 2](#):
- Click **4310 v5.x.x Settings**. Find the Assigned VLAN property. In the box, type either the VLAN number where the DMP resides, or \$svd_ignore

Figure 2 Assigned VLAN Property Configuration for DMPs

The figure consists of two screenshots of the Cisco StadiumVision Management Dashboard. The top screenshot shows the 'SV Director Configuration' page with the 'Assigned VLAN' property highlighted in blue and set to '\$svd_ignore'. The bottom screenshot shows the '4310 v5.x.x Settings' page with the 'Assigned VLAN' property highlighted in blue and set to '\$svd_ignore'. Red arrows in both screenshots point to the 'Assigned VLAN' property value.

Step 3 Click the Save icon.

Verifying DMPs, Groups, and Zones in the Management Dashboard



Note

Before you verify DMP status, be sure that you have set the Assigned VLAN property for your DMP 4310s so that the VLAN compliance check can be performed. For more information, see the [“Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check”](#) section on page 28.

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

- Step 1** Go to the Management Dashboard and verify that all of your groups, zones and DMPs are present and in the green state.
- Step 2** From the DMP and TV Controls dashboard drawer, run a Get Status on all DMPs to update Cisco StadiumVision Director’s record of DMP MAC addresses using the following dashboard command path: **DMP and TV Controls > Monitoring > Get Status**.
- Step 3** Run an Initial Config using the following dashboard command path: **DMP and TV Controls > DMP Install > Initial Config**.
- Step 4** Run Get Status to confirm that all DMPs have successfully rebooted and are in good health.



Note

This will also update the MAC address for the DMPs.

- Step 5** (Optional) Change the DMP State of healthy DMPs to “Production” using the following dashboard command path:
DMP and TV Controls > Auto Registration > Change DMP State.
- Step 6** Run Get Status to check the DMP state after the change.
- Step 7** Investigate any DMPs that are not in “Normal” state.
-

Verifying the Multicast Configuration

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

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

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 3.2*.

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.

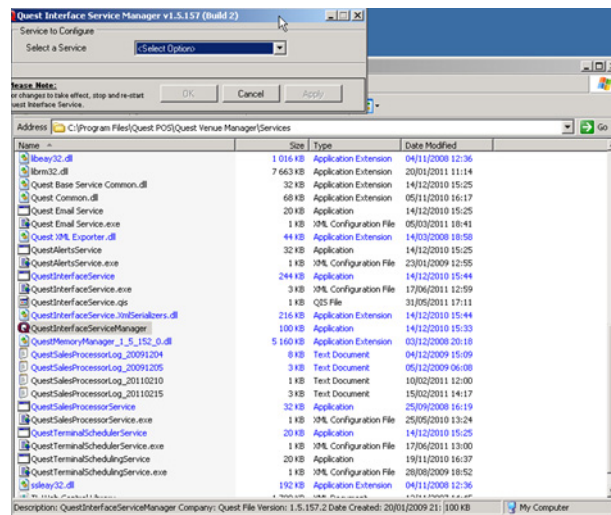
The steps described in this section assume that Quest has the notification service installed and enabled.

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:

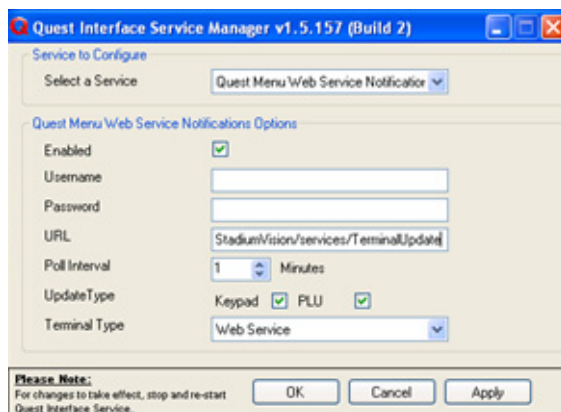
- Step 1** Access the Quest server.
- Step 2** Go to the C:\Program Files\Quest POS\Quest Venue Manager\Services directory.
- Step 3** Start the executable application program named “QuestInterfaceServiceManager” (Figure 3).

Figure 3 QuestInterfaceServiceManager Application



- Step 4** When the Quest Interface Service Manager application window opens, specify the following options (Figure 4):
 - 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 4 Select a Service to Configure

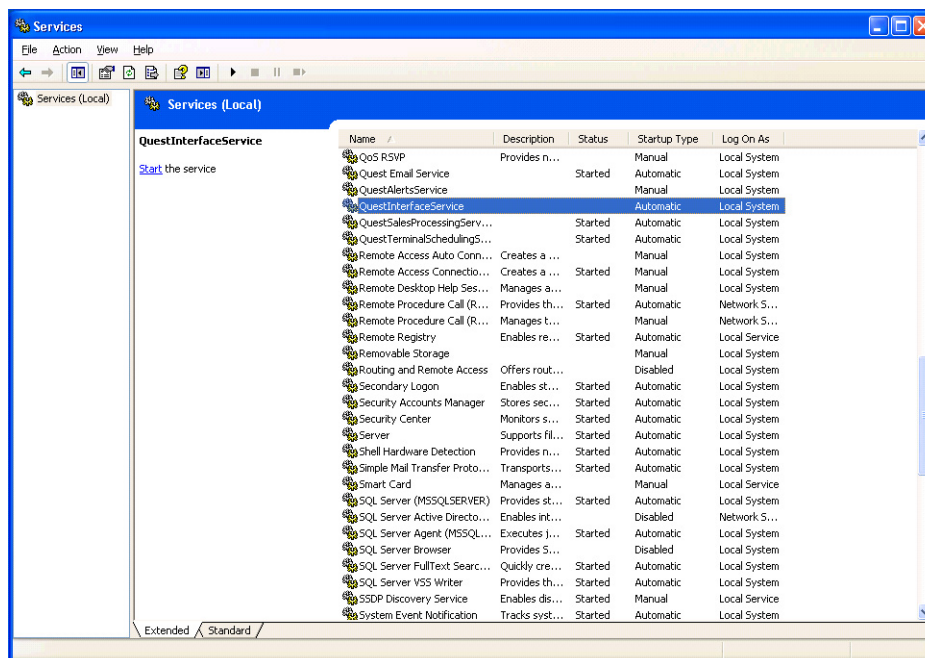


Step 5 Click **OK**.

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

- a. From your laptop, click **Start > Run...**
- b. When the Run dialog box opens, type “**services.msc**”.
- c. Find the Quest Interface Service and restart it (Figure 5).

Figure 5 Restart the Quest Interface Service





Using the Software Manager to Upgrade Cisco StadiumVision Director Release 3.2 Software, Language Packs, and Fonts

First Published: April 21, 2014

Revised: April 7, 2015



Note

If you are upgrading an existing Cisco StadiumVision Director server from Release 3.1 SP2 to Release 3.2, see the [“Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2” module on page 19](#) first.

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

- Upgrade an existing server already running Cisco StadiumVision Director 3.2 to a later release of Cisco StadiumVision Director software.
- Install language packs and fonts.

This module includes the following topics:

- [Best Practices, page 33](#)
- [Prerequisites, page 34](#)
- [Information About Using the Software Manager to Update Existing Cisco StadiumVision Director Software, page 35](#)
- [Upgrade Tasks, page 35](#)
- [Installing Language Packs, page 39](#)
- [Installing Fonts, page 40](#)
- [What to Do Next, page 41](#)

Best Practices



Caution

Do not alter the RAID configuration prior to upgrade.

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

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the [Release Notes for Cisco StadiumVision Director Release 3.2](#) 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 3.2](#).

- Promote the secondary server to primary.

For more information about promoting a secondary server to primary in Release 3.2, see the “[Configuring Failover Between Redundant Cisco StadiumVision Director Servers](#)” module of the [Cisco StadiumVision Director Server Administration Guide, Release 3.2](#).
- 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 3.2.0-489 or higher.
- If you are upgrading your server from Release 3.1, follow the tasks described in the “[Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2](#)” module in this guide.

- You have the IP address for the Cisco StadiumVision Director server where you want to upload the ISO upgrade image. You will need to use this information as part of the URL to access the ISO upload utility.
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the [Cisco StadiumVision Release Notes for Release 3.2](#).

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

After upgrading to Cisco StadiumVision Director Release 3.2, you can use the Software Manager to upgrade to later versions of Cisco StadiumVision Director. 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 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 36](#) (required)
- [Uploading and Installing an ISO Upgrade File on the Cisco StadiumVision Director Server, page 37](#) (required)
- [Reactivating Custom Fonts, page 38](#) (as required)
- [Staging the Flash Template, page 38](#) (required)
- [Deploying Global DMP Settings, page 39](#) (required)

Downloading ISO Upgrade Files from Cisco.com

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

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

- Step 1** Go to the Cisco StadiumVision Director software download site at:
<http://software.cisco.com/download/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.2.0&reind=AVAILABLE&rellifecycle=&reltype=latest>



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

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

[Table 1](#) shows the filename conventions used for ISO upgrades.



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

Table 1 ISO Upgrade Filename Conventions

Hardware Product ID	Filename Convention ¹
SV-DIRECTOR-K9 or SV-PLATFORM2= SV-PLATFORM3=	<ul style="list-style-type: none"> SV-DIRECTOR-UPGRADE-3.2.0-<i>nnn</i>.x86_64.iso SV-DIRECTOR-UPGRADE-3.2.0-<i>nnn</i>.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.

Procedure

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:

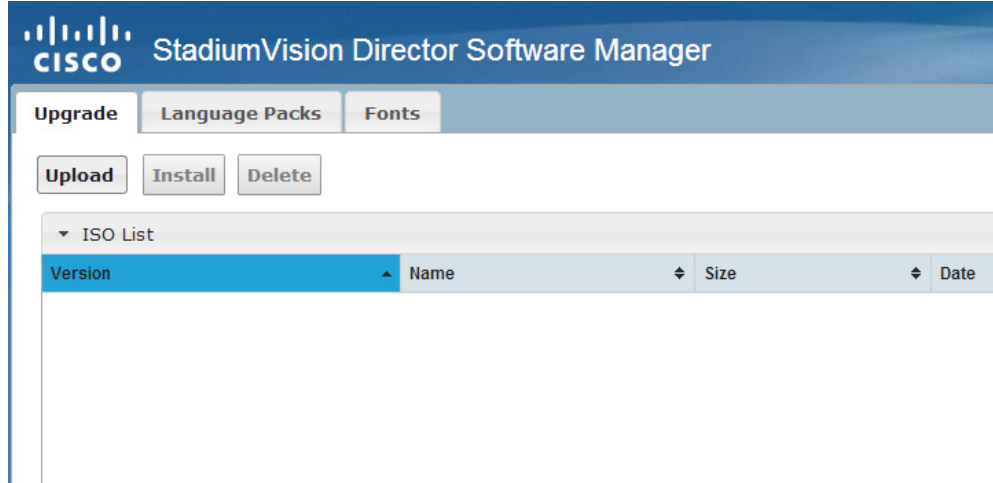
- When the image is validated and uploaded successfully, a message is displayed stating that the ISO image has been uploaded.
- The image upload failed for some reason and you will need to retry the upload again.



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** Click the **Install** button (Figure 1).

Figure 1 ISO File Selection and Upload

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 Release 3.2 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** Stage the Flash Template.
-

Staging the Flash Template

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

-
- Step 1** Go to the Management Dashboard.
 - Step 2** From the DMP and TV Controls dashboard drawer, navigate to the following command path: **DMP and TV Controls > DMP Install > Stage Template**.
 - Step 3** Select all of the DMP devices where the command should be applied.

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

Deploying Global DMP Settings

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

- Step 1** Go to the Management Dashboard.
- Step 2** From the DMP and TV Controls dashboard drawer, navigate to the following command path:
DMP and TV Controls > Global > Global DMP Settings.
- Step 3** Select all of the DMP devices where the command should be applied.
- Step 4** Click the play button to run the command on the selected devices.
-

Installing Language Packs

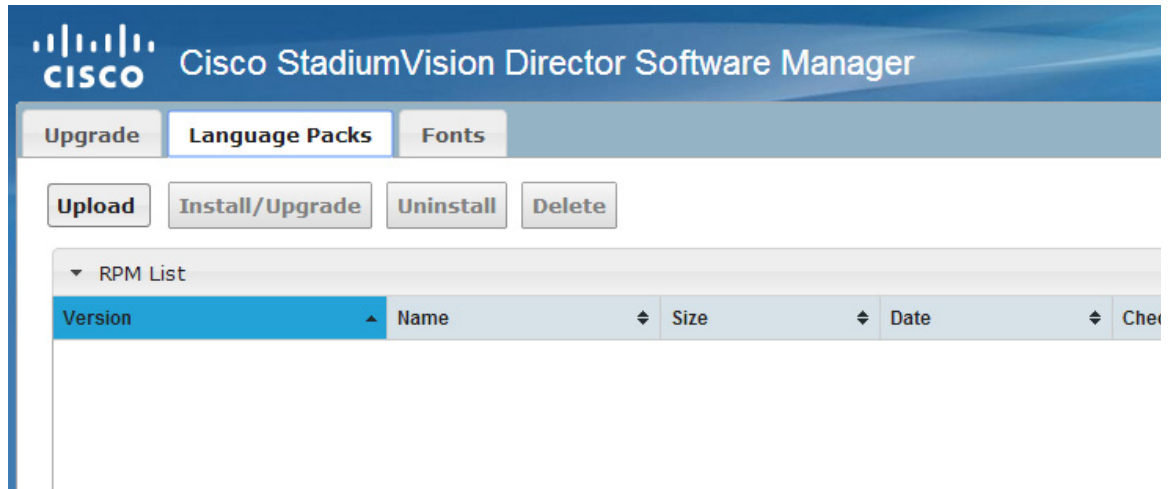
Beginning in Cisco StadiumVision Director Release 3.2, you now have increased flexibility to upload and install only the specific language(s) that you want to support through the independent installation of Language Packs as they become available for the release. The upload and installation of the language packs is performed using the new Software Manager from the Cisco StadiumVision Director main menu.

In prior Cisco StadiumVision Director releases, localization upgrades included automatic installation of all supported languages bundled as part of a service pack which no longer applies to language support in Release 3.2.

To install language packs, complete the following steps:

- Step 1** Download the desired language pack from Cisco.com.
- Step 2** Login into Cisco StadiumVision Director as **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 Go to the downloaded Language Pack RPM, and click **Open**. The language pack is sent to the server.

Step 6 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.

Installing Fonts



Note Follow these guidelines to install new fonts on your system. If you have already installed custom fonts prior to upgrade, then you only need to reactivate them. See the [“Reactivating Custom Fonts” section on page 38](#).

This section includes the following topics:

- [Guidelines for Installing Fonts, page 40](#)
- [Procedure, page 41](#)

Guidelines for Installing Fonts

Consider the following guidelines before installing fonts:

- To save system memory on the DMP, 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).

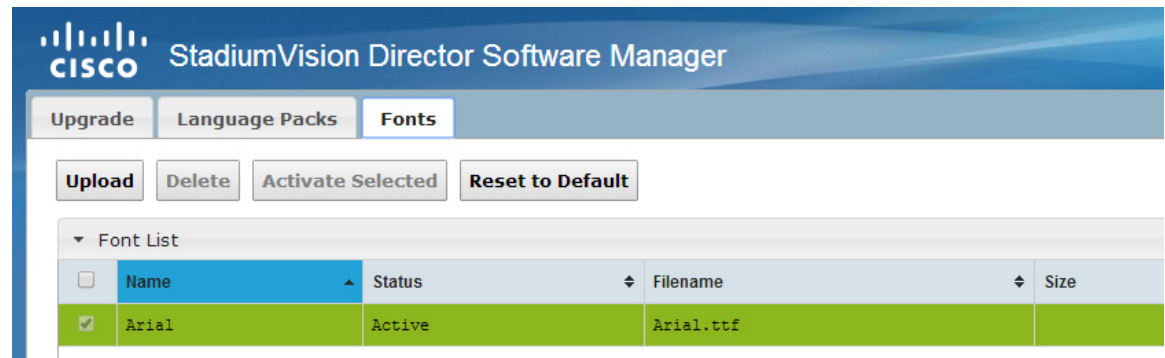
Step 2 Login into Cisco StadiumVision Director as **administrator**.

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

Step 4 Click on the **Manage Software** icon.

Step 5 From the Software Manager screen, click **Fonts** (Figure 3).

Figure 3 Fonts Tab



Step 6 Go to the downloaded font file, and click **Open**.

Step 7 Click **Upload**.
The font file is sent to the server.

Step 8 Click the checkbox of the font to be activated.

Step 9 Click **Activate Selected** to make the font active.

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 45 to be sure that you have completed the required verification steps.



StadiumVision

Upgrading the DMP Firmware

First Published: April 21, 2014

Revised: November 17, 2014

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

Contents

- [Prerequisites, page 41](#)
- [Upgrade Tasks, page 41](#)

Prerequisites

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

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

For more information about DMP hardware and software requirements, see the [Release Notes for Cisco StadiumVision Director Release 3.2](#).

Upgrade Tasks

To upgrade the DMP firmware, complete the following tasks:

- [Downloading the DMP Firmware, page 41](#) (required)
- [Upgrading the DMP Firmware From the Management Dashboard, page 42](#) (required)
- [Disabling Failover on all DMPs, page 44](#) (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.

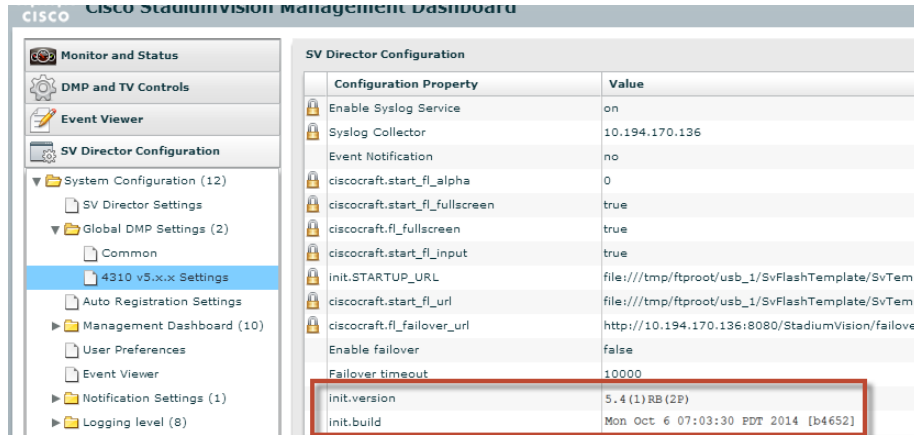
- For firmware version 5.4.1 RB2P:
init.version = 5.4(1)RB(2P)
init.build = Mon Oct 6 07:03:30 PDT 2014 [b4652]

**Note**

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



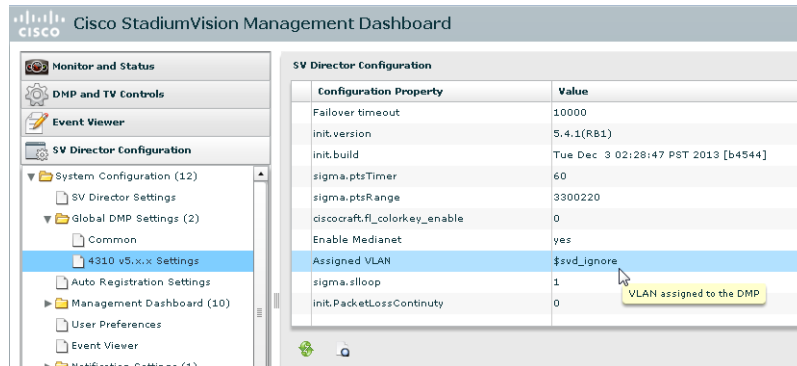
Step 5 Configure the Assigned VLAN property under the 4310 v5.x.x as \$svd_ignore or the actual VLAN number on which your DMPs reside. Do *not* leave blank.



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**.
-



Appendix A: Post-Upgrade Checklist

First Published: April 21, 2014
Revised: May 14, 2014

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.	<input type="checkbox"/>
2. Clear the browser cache.	<input type="checkbox"/>
 Caution Notify <i>all</i> Cisco StadiumVision Director users about the mandatory requirement to clear their browser cache 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.	<input type="checkbox"/>
4. If you are using phone control, verify that the phones work.	<input type="checkbox"/>
5. If using IP phones for local TV control, verify that channels can be successfully changed.	<input type="checkbox"/>
6. Verify that channel names and favorites are properly set.	<input type="checkbox"/>
7. If using suite commerce integration, verify that an order can be successfully placed using the IP phone.	<input type="checkbox"/>
8. Verify that all devices are properly in the nonevent_group.	<input type="checkbox"/>
9. Go to the Services Alert window in the Management Dashboard and make sure that all relevant services are green.	<input type="checkbox"/>
Tip You might need to click the refresh button to be sure that all services are re-pollled 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.	<input type="checkbox"/>

List Item	Checkoff
11. Start an existing event script and validate that screens display the expected content.	<input type="checkbox"/>
12. Stop the event script and validate that screens are powered off.	<input type="checkbox"/>
13. Make a minor edit to the event script and make sure it can be saved.	<input type="checkbox"/>
14. Verify that you can push a new video file in the CMS to the DMPs.	<input type="checkbox"/>
15. If using dynamic menu boards, make a change to a menu item and verify that the change is reflected on the menu board.	<input type="checkbox"/>
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.	<input type="checkbox"/>
17. Perform a server backup for the upgrade configuration.	<input type="checkbox"/>
18. After satisfying your site's testing and event requirements, failback to the primary server and upgrade it to the same version of software that you validated on your secondary server. For more information, see the “Configuring Failover Between Redundant Cisco StadiumVision Director Servers” module in the <i>Cisco StadiumVision Director Server Administration Guide</i> .	<input type="checkbox"/>
19. After you perform failback, be sure that you reconfigure your backup and restore environment using the Text Utility Interface (TUI).	<input type="checkbox"/>
20. (As needed for sites with a large volume of video content) Reduce the number of backups that are retained by the system. For more information, see the “Backing Up and Restoring Cisco StadiumVision Director Servers” module in the <i>Cisco StadiumVision Director Server Administration Guide</i> .	<input type="checkbox"/>



Appendix B: Port Reference

First Published: April 21, 2014

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

- [Cisco StadiumVision Director Ports, page 47](#)
- [Cisco StadiumVision Director Remote Ports, page 49](#)
- [DMP Input Ports, page 51](#)

Cisco StadiumVision Director Ports

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

Cisco StadiumVision Director Input Ports

[Table 1](#) lists the input ports used by all Cisco StadiumVision Director servers.

Table 1 *Cisco StadiumVision Director Input Ports*

Originator	Protocol	Port	Target Application	Usage
Laptop	TCP	22	SSH	Remote login.
Laptop / DMP	TCP	80	Apache	Redirect to port 8080.
DMP	UDP	514	Syslog	Proof of play, Alerts.
DMP	TCP	8080	Tomcat / Apache	Fetch config/data.
External NTP server	UDP	123	NTP	Time synchronization (StadiumVision Director as NTP client).
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.

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	8089	tomcat	Configuration update for multicast rebroadcaster.
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 rebroadcaster from Cisco StadiumVision Director server.

Table 5 *Cisco StadiumVision Director Remote Output Ports*

Originator	Protocol	Port	Target Application	Usage
StadiumVision Director Remote	UDP	Default: 7778	DMP flash template	Multicast commands (Default is 239.193.1.1:7778)
StadiumVision Director	UDP	123	NTP	NTP requests initiated by StadiumVision Director Remote to its NTP server.

DMP Ports

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

DMP Input Ports

Table 6 lists the input ports used by the DMP.

Table 6 DMP Input Ports

Originator	Protocol	Port	Target Application	Usage
NTP server	UDP	123	NTP	Time sync response.
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

DMP Output Ports

Table 7 lists the output ports used by the DMP.

Table 7 DMP Output Ports

Originator	Protocol	Port	Target Application	Usage
DMP	UDP	514	syslog	Proof of play. Alerts.
StadiumVision Director	UDP	123	NTP	Time sync request.
Cisco StadiumVision Director	TCP	8080	httpd	Fetching of DMP config, autoprovisioning, and related.
DMP	TCP	9090	Tomcat for Liferay	Dynamic Menu Board application interface.



Appendix C: Installing Additional Hard Drives in the Platform 2 Server to Prepare for Upgrade to Release 3.2

First Published: April 21, 2014

The Cisco StadiumVision Director Platform 2 server ships with two 300 GB hard drives configured with RAID 1 mirroring for redundancy. This module describes how to install two additional 300 GB hard drives (SV-FRU2-HD3G=) for another RAID 1 volume in the Cisco StadiumVision Director Platform 2 Server which are required to run Cisco StadiumVision Director Release 3.2 with a minimum of 4 drives.



Caution

If you need to install additional hard drives in the Platform 2 server to meet the 4-drive minimum requirement to support Release 3.2, then you must perform different upgrade tasks in a certain order.

The physical installation of the additional drives must precede the upgrade to Release 3.1.0-797 (SP2), which is the required prerequisite release to upgrade to Release 3.2.

Refer to the [Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.1](#) followed by extension of the RAID volume post-upgrade, and then content migration and the remainder of the upgrade verification.

Contents

- [Prerequisites, page 53](#)
- [Installation Tasks, page 54](#)

Prerequisites

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

- Your current CIMC/BIOS firmware version is a minimum of 1.5(1).
- You have completed running any proof of play reports.
- You have completed a backup and have a copy stored externally to the Cisco StadiumVision Director servers.

- You have installed Cisco StadiumVision Director Release 3.1.0-797 SP2 on your Platform 2 servers.
- You have physical access to the server.
- A monitor and keyboard are connected to the Cisco StadiumVision Director server.
- You can log into the server at the console or over the network with SSH.
- You have two new 300 GB R2 Disk Spare drives (SV-FRU2-HD3G=) for the Platform 2 server.



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

Installation Tasks

To install additional hard drives, complete the following tasks:

- [Installing the Hard Drives Into the Server Chassis, page 54](#) (required)
- [Creating a New Logical Volume Using the LSI MegaRAID Utility, page 55](#) (required)
- [Extending the Original RAID Volume to Create a Single Group, page 58](#) (required)

Installing the Hard Drives Into the Server Chassis

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

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

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



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

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

- Step 3** A message appears asking you to confirm the shutdown.

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

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

Type **Y**.

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

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

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



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

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

For information about physically installing the hard drives on the Platform 2 server, see the [“Maintaining the Server”](#) chapter of the *Cisco UCS C200 Installation and Service Guide*.

Creating a New Logical Volume Using the LSI MegaRAID Utility

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

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



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

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

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

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



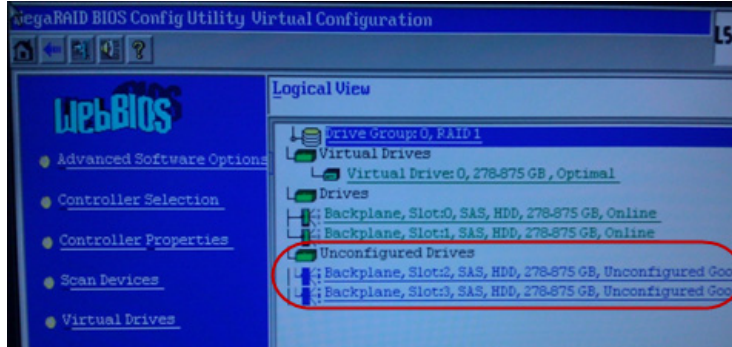
Note Be sure to press Ctrl-H when prompted by the LSI MegaRAID utility. If you miss the prompt or reach the boot menu before seeing it, press Ctrl-Alt-Del to reboot the server and try again.

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



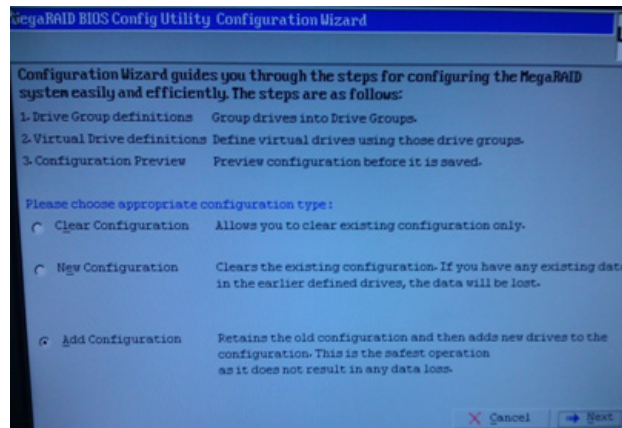
Note Only drives in “Unconfigured Good” state are available for RAID configuration. New drives must show up as unconfigured before you proceed ([Figure 1](#)).

Figure 1 *Unconfigured Drives in Good State*



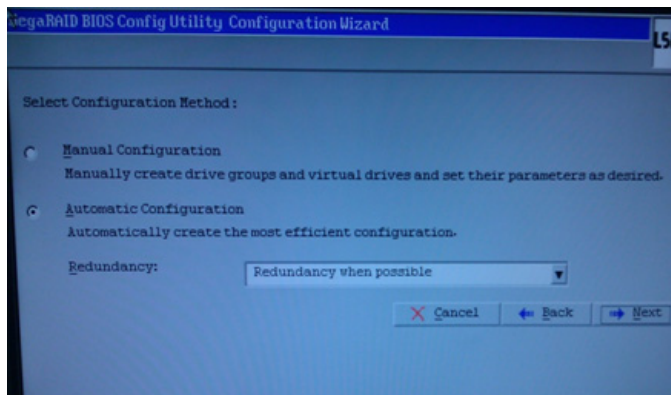
- a. Select **Add Configuration** and click **Next** (Figure 2).

Figure 2 *Add Configuration Wizard*



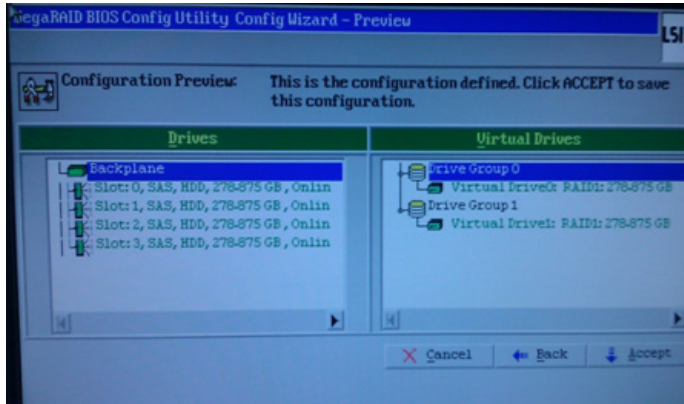
- b. Select **Automatic configuration** with the **Redundancy when possible** option. Click **Next** (Figure 3).

Figure 3 *Configuration Method Screen*



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

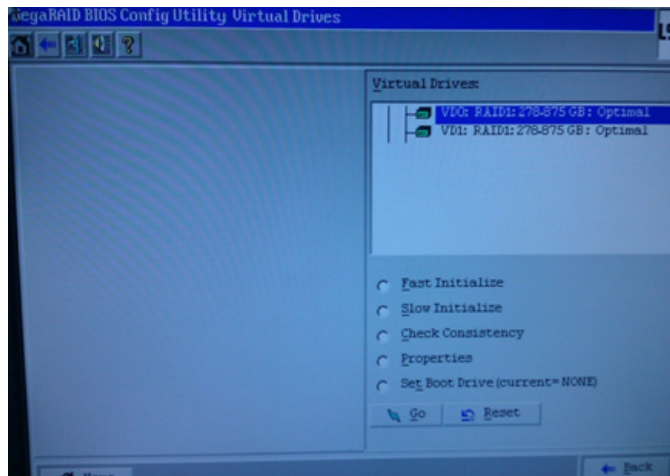
Figure 4 *Accept Configuration Preview*



A fast disk initialization automatically begins.

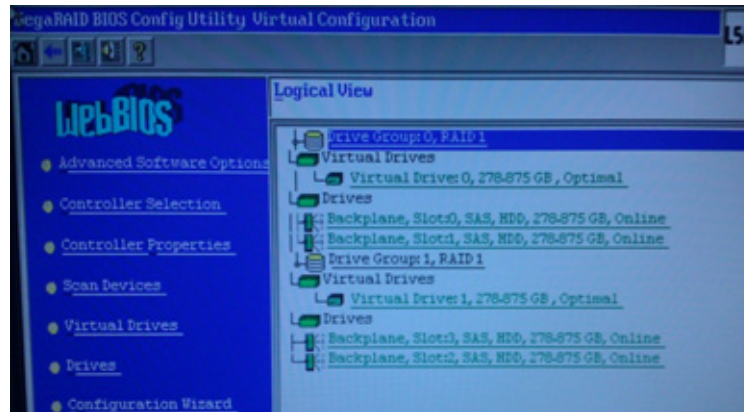
- d. When the screen showing initialization options is displayed, only click **Back** (Figure 5).

Figure 5 *Initialization Options—Click Back Only*



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

Figure 6 Logical View of Hard Drives



- Step 4** Exit the MegaRAID utility.

Extending the Original RAID Volume to Create a Single Group

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

To extend the original RAID volume to create a single group in the Release 3.2 software, complete the following steps:

-
- Step 1** Log into the TUI by doing the following:
- a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the secondary Cisco StadiumVision Director server using the IP address for your server.
 - b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
- Step 2** From the Main Menu, go to the **StadiumVision Server Administration > Hard Drive Expansion** option.
- Step 3** When the following confirmation message appears, type Y if you are prepared to continue, or N to cancel.
- ```
WARNING: You will lose data that may be stored in the new drives. Do you want to continue?
PRESS Y TO CONTINUE, PRESS N TO CANCEL
```
- Step 4** Press any key to return to the StadiumVision Server Administration menu.
- Step 5** Continue to return to the Main Menu and exit the TUI.
-

## What To Do Next

After you extend the RAID volume, return to the [“Upgrading a Cisco StadiumVision Director Server from Release 3.1 SP2 to Release 3.2”](#) to complete the upgrade tasks and perform the migration of content to the Release 3.2 CMS.

■ What To Do Next





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

**First Published: April 21, 2014**

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 61](#) (required)
- [CIMC Firmware Upgrade Guidelines, page 63](#) (as required)

## CIMC Initial Configuration

This section includes the following topics:

- [Prerequisites, page 61](#)
- [CIMC Initial Configuration Summary, page 62](#)

## 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](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                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <b>Configuring the CIMC Interface</b><br><b>Note</b> The instructions for configuring the CIMC interface are found in the “Initial Server Setup” topic of the “Installing the Server” chapter in the <i>Cisco UCS C220 Server Installation and Service Guide</i> .                                                                                                                                                            |
| <b>Step 1</b> | During bootup, press <b>F8</b> when prompted to open the BIOS CIMC Configuration Utility.                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 2</b> | Configure the CIMC interface with the following settings: <ul style="list-style-type: none"> <li>• DHCP—Disabled. You must change this option to enter a static IP address.</li> <li>• CIMC IP—IPv4 address for your CIMC interface, with corresponding subnet mask.</li> <li>• VLAN—Dependent on client network.</li> <li>• Change the CIMC password. The default credential is <b>admin</b> and <b>password</b>.</li> </ul> |
| <b>Step 3</b> | Press <b>F10</b> to save your configuration and reboot the server.                                                                                                                                                                                                                                                                                                                                                            |

|               | Description                                                                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <p><b>Configuring the NIC Properties</b></p> <p><b>Note</b> Information about configuring the NIC properties are found in the “Initial Server Setup” topic of the “Installing the Server” chapter in the <i>Cisco UCS C220 Server Installation and Service Guide</i>.</p>                                                               |
| <b>Step 4</b> | 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.                                                                                                                                                          |
| <b>Step 5</b> | Log into the CIMC console with username <b>admin</b> and the password that you configured in <a href="#">Step 2</a> .                                                                                                                                                                                                                   |
| <b>Step 6</b> | <p>From the <b>Admin</b> tab, click <b>Network</b>, and go to the <b>Network Settings</b> page.</p> <p>In the NIC Properties box configure the following settings and save your changes:</p> <ul style="list-style-type: none"> <li>• NIC mode—Dedicated</li> <li>• NIC Redundancy—None</li> </ul>                                      |
|               | <p><b>Configuring the Server Boot Order</b></p> <p><b>Note</b> 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 <i>Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.4</i></p> |
| <b>Step 7</b> | From the <b>Server</b> tab, click <b>BIOS</b> .                                                                                                                                                                                                                                                                                         |
| <b>Step 8</b> | <p>Configure the following boot order and save your changes:</p> <ul style="list-style-type: none"> <li>• Virtual CD/DVD</li> <li>• HDD</li> </ul>                                                                                                                                                                                      |

## CIMC Firmware Upgrade Guidelines

This section includes the following topics:

- [Before You Begin](#), page 63
- [Prerequisites](#), page 64
- [CIMC/BIOS Firmware Upgrade Summary](#), page 64

### Before You Begin

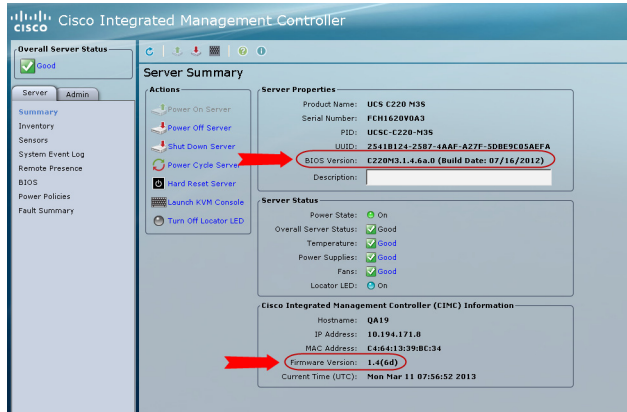
See the release notes for your Cisco StadiumVision product and release at:

[http://www.cisco.com/en/US/products/ps11274/prod\\_release\\_notes\\_list.html](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](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                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p>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.</p> <p><b>Note</b> The release 1.4(x) firmware HUU ISO files are platform-specific.</p>                                                                                                                            |
| <b>Step 2</b> | <p>Follow the instructions in the Host Upgrade Utility guide:</p> <p><b>Note</b> The Cisco UCS C220 server does not have a CD/DVD drive.</p> <ul style="list-style-type: none"><li>• Go to Cisco.com and download the HUU ISO file.</li><li>• Follow the instructions to load the ISO that you downloaded and be sure that both the CIMC and BIOS firmware are upgraded together.</li></ul> |





## Appendix E: Using the TUI Upgrade Utility to Upgrade the Cisco StadiumVision Software

**First Published: April 21, 2014**

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

The TUI must be used to upgrade from Release 3.1 to Release 3.2. Once the 3.2 upgrade is complete, this functionality is replaced by the Software Manager.

This module includes the following topics:

- [Best Practices, page 67](#)
- [Prerequisites, page 68](#)
- [Information About Using the TUI Upgrade Utility to Update an Existing Cisco StadiumVision Director Server, page 69](#)
- [Upgrade Tasks, page 69](#)
- [What to Do Next, page 77](#)

### Best Practices



#### Caution

---

Do not alter the RAID configuration prior to upgrade.

---

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

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the [Release Notes for Cisco StadiumVision Director Release 3.2](#) for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

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




---

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

---

For more information about performing a backup and restore on a Cisco StadiumVision Director Server, see the “Backing Up and Restoring Cisco StadiumVision Director Servers” module of the *Cisco StadiumVision Director Server Administration Guide*.

- Promote the secondary server to primary.
 

For more information about promoting a secondary server to primary in Release 3.2, see the “Configuring Failover Between Redundant Cisco StadiumVision Director Servers” module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.2*.
- Access the promoted secondary server to perform the upgrade.
- Verify the boot order in the BIOS (by pressing **F2** while booting) prior to upgrading; the virtual DVD should be the primary boot device for the Platform 3 server.
- Due to the difficulty in recovering from an interrupted installation process if the Linux shell is accidentally closed or the network drops, it is highly recommended that you use a server console connection method that does not pose a risk to the success of upgrade completion if the session breaks during upgrade.

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

## Prerequisites

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

- Your server is running a minimum of Cisco StadiumVision Director Release 3.1.0-797 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 3.2*.
- You have an installer account on the Cisco StadiumVision Director server.
- To access the Cisco Integrated Management Controller (CIMC) for the TUI software upgrade, the following requirements are met:
  - Your computer meets the minimum browser and Flash player requirements for Cisco StadiumVision Director, and also has Java 1.6 or later installed.
  - You have a laptop connection with access to the Cisco StadiumVision Director server network.



- You have the IP address of the CIMC interface on the Cisco StadiumVision Director server.
- You have the CIMC interface login credential. The default is admin/password.

**Note**

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

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

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

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

### ISO Upgrade Files

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

### Disk Maintenance

There is no automatic aging of ISO upgrade files, but Cisco StadiumVision Director Release 3.1 introduced 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 70](#) (required)
- [Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server, page 71](#) (required)
- [Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server, page 75](#) (required)
- [Staging the Flash Template, page 77](#) (required)
- [Deploying Global DMP Settings, page 77](#) (required)
- [What to Do Next, page 77](#) (required)

## Downloading ISO Upgrade Files from Cisco.com

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

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

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

<http://software.cisco.com/download/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.2.0&reind=AVAILABLE&rellifecycle=&reltype=latest>



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

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

[Table 1](#) shows the filename conventions used for ISO upgrades.



**Note** Be sure that you choose the ISO for SV-DIRECTOR and *not* for SVD-REMOTE. The TUI will verify the filenameing 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 <sup>1</sup>                                                                                                                                  |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SV-DIRECTOR-K9 or<br>SV-PLATFORM2= | <ul style="list-style-type: none"> <li>SV-DIRECTOR-UPGRADE-3.2.0-<i>nnn</i>.x86_64.iso</li> <li>SV-DIRECTOR-UPGRADE-3.2.0-<i>nnn</i>.x86_64.iso.md5sum</li> </ul> |
| SV-PLATFORM3=                      |                                                                                                                                                                   |

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.

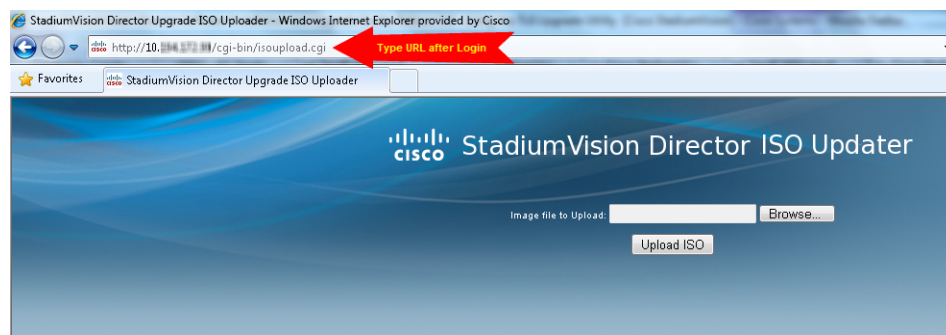
### Prerequisites

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

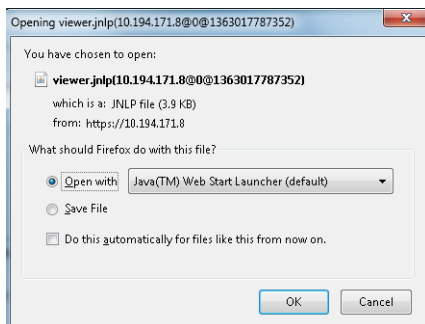
When the ISO upload is complete, one of the following occurs:

- 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:
- (Optional) Select the checkbox to accept all content from Cisco.
  - Click **Yes** to accept the certificate and continue.
  - Confirm any additional security certificate exceptions.
- Step 4** At the CIMC login screen, note the firmware version displayed ([Figure 4](#)).

**Tip**

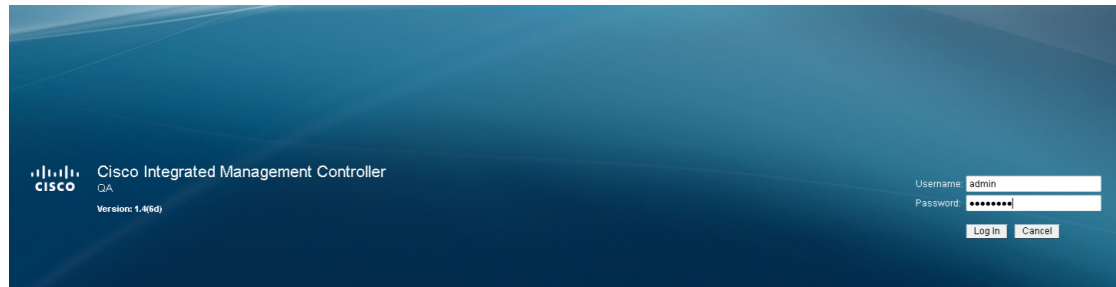
The firmware version is also displayed in the Cisco Integrated Management Controller (CIMC) Information box on the CIMC console after you log in.

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

**Tip**

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

**Figure 4** *CIMC Login Screen*



**Step 6** Click **Log In**.

## Verifying the Minimum CIMC Firmware Version for Cisco StadiumVision Director

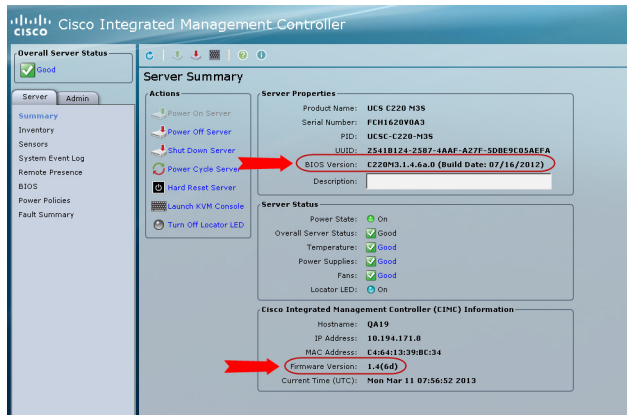
Before you begin, see the “Cisco StadiumVision Director Server Support” section of the [Release Notes for Cisco StadiumVision Director Release 3.2](#) to find the CIMC/BIOS versions tested for your platform.

**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.

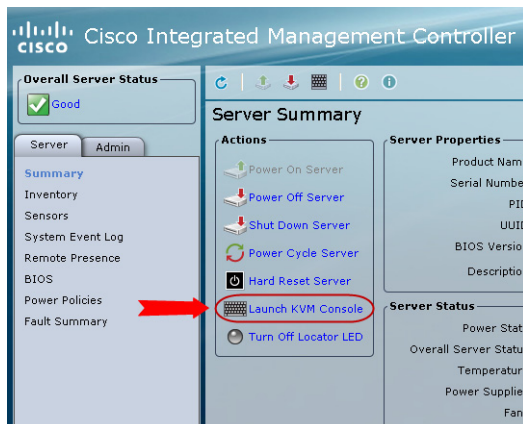
- Step 2** If necessary to upgrade the CIMC/BIOS firmware on the Platform 3 server, refer to the [“Appendix D: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server”](#) module.

## 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

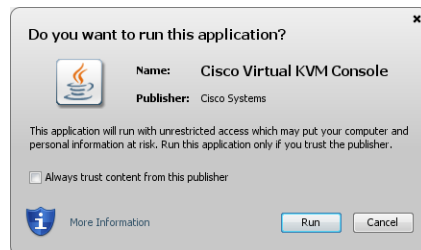




**Tip** You can also click the keyboard in the icon bar at the top of the console to launch the KVM console.

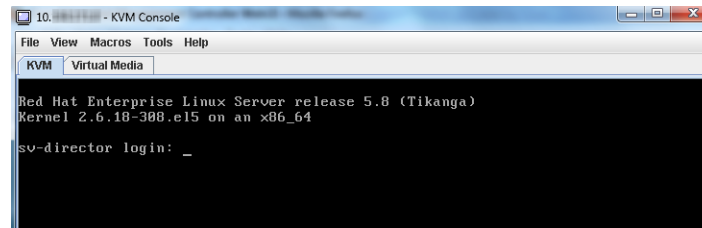
- Step 2** If a security dialog box displays, do the following:
- (Optional) Select the checkbox to accept all content from Cisco.
  - Click **Yes** to accept the certificate and continue.
- Step 3** At the Cisco Virtual KVM Console confirmation box (Figure 7), do the following:
- (Optional) Select the checkbox to accept all content from Cisco.
  - Click **Run**.

**Figure 7** Cisco Virtual KVM Console Confirmation



- Confirm any additional security certificate exceptions.
- Step 4** The KVM Console window is displayed with a login prompt (Figure 8).

**Figure 8** Cisco KVM Virtual Console Login Screen



## Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server

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

- Step 1** Do one of the following to run a secure login to the Cisco StadiumVision Director server:
- Using a directly-connected computer and KVM cable, access the console of the Cisco StadiumVision Director server.
  - or
  - Log into the CIMC and launch the virtual KVM console.

- Step 2** When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
- Step 3** From the Main Menu, do the following:
- **For upgrades from Release 3.1:**  
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—Release 3.1

```

Main Menu > StadiumVision Server Administration

Please choose one of the following menu options:

a) Display Software Version
b) Upgrade Server
c) Restart StadiumVision Director software
d) Shutdown StadiumVision Director software
e) Setup automatic backup and restore
f) Re-Run StadiumVision initial configuration
g) Content migration
h) Hard Drive Expansion
i) Backup/restore Retention Policy
j) Failover
k) Reboot
l) Power Off
R or < or ,) Return to prior menu

```

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

**Figure 10** TUI Upgrade Configuration Confirmation

```

Are you sure you wish to upgrade? Push R to return to main menu
or C to continue.

```

- 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

```

Are you sure you wish to upgrade? Push R to return to main menu
or C to continue.

1. - SV-DIRECTOR-UPGRADE-3.1.0-510.x86_64.iso

Please select a file number and press enter: 1

```

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

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

- 
- Step 1** Go to the Management Dashboard.
  - Step 2** From the DMP and TV Controls dashboard drawer, navigate to the following command path: **DMP and TV Controls > DMP Install > Stage Template.**
  - Step 3** Select all of the DMP devices where the command should be applied.
  - Step 4** Click the play button to run the command on the selected devices.
- 

## Deploying Global DMP Settings

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

- 
- Step 1** Go to the Management Dashboard.
  - Step 2** From the DMP and TV Controls dashboard drawer, navigate to the following command path: **DMP and TV Controls > Global > Global DMP Settings.**
  - Step 3** Select all of the DMP devices where the command should be applied.
  - Step 4** Click the play button to run the command on the selected devices.
- 

## 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 45 to be sure that you have completed the required verification steps.

■ What to Do Next