



StadiumVision



Cisco StadiumVision Director Server Administration Guide

Release 3.2

June 13, 2014

Americas Headquarters

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

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 Server Administration Guide
© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

Document Revision History	ix
Document Organization	ix
Related Documentation	x
Obtaining Documentation and Submitting a Service Request	2-xi

PART 1

Cisco StadiumVision Director Architecture Overview

Cisco StadiumVision Director Server Architecture	1-1
Standard Cisco StadiumVision Director Network Architecture	1-1
Cisco StadiumVision Director Server Redundancy	1-2
Centralized Cisco StadiumVision Director Network Architecture	1-4
WAN Optimization	1-4
Hierarchical Management	1-5
Server Platforms	1-6
Cisco StadiumVision Director Servers	1-6
Cisco StadiumVision Director Platform 2 Server	1-7
Cisco StadiumVision Director Platform 3 Server	1-7
Virtualized Server Environment Support	1-7
Cisco StadiumVision Director Remote Server	1-9

PART 2

Cisco StadiumVision Director Server Setup

Configuring the Cisco StadiumVision Director Server System Settings	1-3
Contents	1-3
Prerequisites for Configuring Cisco StadiumVision Director Server System Settings	1-3
How to Configure Cisco StadiumVision Director Server System Settings	1-4
Completing Initial Configuration of System Settings After a Full ISO Installation	1-4
Configuring the Cisco StadiumVision Director Server Network Interface	1-5
Editing the Hosts File	1-8
Restarting the Network Service on the Server	1-9
Generating the SSL Certificate	1-9
Configuring NTP on Cisco StadiumVision Servers and DMPs	1-10

- Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs 1-10
- Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers 1-11
- Restarting the Cisco StadiumVision Software 1-15
- Configuring the Date and Time Manually 1-16
- Configuring NTP on DMPs 1-16
 - Applying the Standard NTP Configuration on all DMPs in the System 1-16
 - Modifying the Standard NTP Configuration Globally on all DMPs 1-17
 - Modifying the Standard NTP Configuration on Selected DMPs in the System 1-19
 - Verifying DMP Time Synchronization 1-21
- Configuring Multicast Ports for Cisco StadiumVision Director 1-23
 - Information about Multicast Support in Cisco StadiumVision Director 1-23
 - Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director 1-26
 - How to Configure Multicast Ports in Cisco StadiumVision Director 1-27
- What To Do Next 1-29
- Configuring Cisco StadiumVision Director Remote Servers 1-31**
 - Contents 1-31
 - Prerequisites for Configuring Cisco StadiumVision Director Remote Servers 1-31
 - Information About Configuring Cisco StadiumVision Director Remote Servers 1-32
 - Management Dashboard Monitoring and the Global Credential 1-32
 - Main Menu Applications 1-33
 - How to Configure Cisco StadiumVision Director Remote Servers 1-33
 - Configuring Connectivity to the Cisco StadiumVision Director Server 1-33
 - Configuring the Cisco StadiumVision Director Server IP Address on the Remote Server 1-34
 - Configuring the Global Credential on the Cisco StadiumVision Director Server 1-34
 - Setting the JMX Account Password on the Cisco StadiumVision Director Remote Server 1-37
 - Configuring the Admin Password 1-38
 - Configuring the Date and Time Options on the Remote Server 1-39
 - What To Do Next 1-39
- Configuring Cisco StadiumVision Director for Multiple Venue Support 1-41**
 - Contents 1-41
 - Prerequisites for Configuring Multiple Venue Support 1-41
 - Restrictions for Configuring Multiple Venue Support 1-42
 - Information About Configuring Multiple Venue Support 1-43
 - Cisco StadiumVision Director Remote Servers 1-43
 - Role-Based Access Control for Hierarchical Management of Multiple Venues 1-44
 - Administrator 1-44
 - Content Manager 1-44

Venue Operator	1-44
Other Legacy RBAC Roles	1-45
Understanding Venue Association	1-45
Understanding Scripts and Staging Behavior in a Multi-Venue Environment	1-45
Script Best Practices	1-45
Script Staging Behavior	1-46
How to Configure Multiple Venue Support	1-46
Enabling Multiple Venue Support in Cisco StadiumVision Director	1-46
Adding Venues to Cisco StadiumVision Director	1-47
Associating Venues with Cisco StadiumVision Director Objects	1-48
Guidelines for Associating Venues	1-49
Venue Association Procedure	1-49
Troubleshooting Venue Association Conflicts	1-50
Removing Venues From Cisco StadiumVision Director	1-51
Selecting Venue Scope	1-52
Monitoring Venues From the Management Dashboard	1-53
How to Modify Per-Site Multicast Optimization Registry Settings	1-54
Multicast Registry Keys for Per-Site Multicast Optimization in Cisco StadiumVision Director	1-54
Guidelines for Per-Site Multicast Optimization Registry Settings	1-55
Configuring the Per-Site Multicast Optimization Registry Settings	1-56
How to Migrate Deployed Devices From a Single Venue to a Multiple Venue System	1-56
Prerequisites	1-56
Exporting a Device List for the Original System Configuration	1-57
Creating New Venues	1-58
Removing All Locations From Existing Groups	1-58
Removing Locations From Existing Suites	1-59
Associating Initial Locations to Venues	1-59
Completing Venue-Specific Information and Association of Locations Using BAT	1-59
Populating Group Information in the New Device List	1-60

PART 3**Cisco StadiumVision Director
Account Management**

System Accounts on the Cisco StadiumVision Director Servers	2-1
Information About System Accounts	2-1
Common System Accounts	2-2
Other System Accounts	2-3
How to Change System Account Passwords	2-4

User Management in Cisco StadiumVision Director 3-5

- Information About User Management 3-5
 - Administrator Role Overview 3-5
 - RBAC Roles Overview 3-6
 - Access Summary by Role 3-7

PART 4

Cisco StadiumVision Director System Management

Backing Up and Restoring Cisco StadiumVision Director Servers 3-3

- Contents 3-3
- Prerequisites for Backing Up and Restoring Cisco StadiumVision Director Servers 3-3
- Restrictions for Backing Up and Restoring Cisco StadiumVision Director Servers 3-4
- Information About Backing Up and Restoring Cisco StadiumVision Director Servers 3-4
 - Backup Environment 3-4
 - What Cisco StadiumVision Director Data is Backed Up 3-5
 - Disk Storage and Maintenance 3-5
 - Restore Environment 3-6
- How to Backup a Cisco StadiumVision Director Server 3-6
 - Enabling the Backup Account on the Secondary Server 3-6
 - Setting Up the Primary Server for Automatic Backup and Restore 3-7
 - Scheduling a Regular Backup 3-9
 - Starting a Backup Manually for Immediate Execution 3-10
 - Verifying Backup Completion 3-11
 - Modifying the Number of Days for Backup File Retention 3-11
- How to Restore a Cisco StadiumVision Director Server 3-12
 - Starting a Restore Manually for Immediate Execution 3-13
 - Restarting the Cisco StadiumVision Director Software 3-14

Configuring Failover Between Redundant Cisco StadiumVision Director Servers 4-15

- Contents 4-15
- Prerequisites for Configuring Failover Between Redundant Cisco StadiumVision Director Servers 4-16
- Restrictions for Configuring Failover Between Redundant Cisco StadiumVision Director Servers 4-16
- Information About Failover Between Redundant Cisco StadiumVision Director Servers 4-16
- How to Promote a Standby Secondary Server to the Active Server 4-18
 - Starting and Configuring the Services on the Secondary Server 4-19
 - Restoring the Secondary Server with System Data From a Backup File 4-19
 - Stopping Services and Auto-Restart, and Shutting Down the Primary Server 4-19
 - Shutting Down Services on the Secondary Server 4-20

Changing the IP Address on the Secondary Server	4-20
Prerequisites	4-20
Procedure	4-20
Restarting the Network Service on the Secondary Server	4-21
Verifying Network Connectivity to the Secondary Server	4-22
Clearing the ARP Cache on the Switch	4-22
Restarting Cisco StadiumVision Director on the Secondary Server	4-23
Verifying the Cisco StadiumVision Director Configuration on the Secondary Server	4-23
How to Restore the Primary Server to Active	4-24
Prerequisites	4-24
Stopping Services and Auto-Restart on the Secondary Server	4-24
Changing the IP Address on the Secondary Server	4-25
Prerequisites	4-25
Procedure	4-25
Restarting Cisco StadiumVision Director on the Secondary Server	4-26
Verifying Network Connectivity on the Secondary Server	4-26
Starting and Configuring the Services on the Original Primary Server	4-27
Restoring the Original Primary Server with System Data From a Backup File	4-27
Restarting the Local Control Service on the Primary Server	4-28
Verifying Network Connectivity to the Primary Server	4-28
Verifying the Cisco StadiumVision Director Configuration on the Original Primary Server	4-29

PART 5**Cisco StadiumVision Director
System Tools****Cisco StadiumVision Director Server Text Utility Interface** 5-3

Contents	5-3
Information About the TUI	5-3
Overview of the TUI Menus	5-4
Working with the TUI Interface	5-7
Menu Navigation	5-7
File Editor	5-7
How to Use the TUI	5-8
Logging Into the TUI	5-8
Displaying System Information	5-9
Exiting the TUI	5-10
Related Documentation	5-10

PART 6**Cisco StadiumVision Director
Server Troubleshooting**

- System State Reports 6-1**
 - Information About System State Reports 6-1
 - How to Run a System State Report 6-2
 - Running a System State Report Manually 6-3
 - Scheduling a System State Report 6-3
 - Viewing Reports 6-3
 - Viewing Scheduled Reports and Previous Reports 6-4
 - Viewing the Contents of the Zip File 6-4



Preface

This document describes the tasks involved in setting up and maintaining the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers in 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.

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
June 13, 2014	Updated the document with the following changes: <ul style="list-style-type: none"> • Revised a typographic error in the transport.dynamic.send_range registry key default value in “Multicast Registry Keys in Cisco StadiumVision Director” table. • Revised the “How to Restore a Cisco StadiumVision Director Server” section on page 13 to remove a statement about doing a periodic restore to update the secondary server and add a recommendation to follow the procedures in the failover module when needing to failover/restore content on the secondary server.
April 21, 2014	First release of this document for Cisco StadiumVision Director Release 3.2.0-489 and Cisco StadiumVision Director Remote Release 3.2.0-82.

Document Organization

Chapter	Description
“Cisco StadiumVision Director Server Architecture”	Describes the network architectures supported in Cisco StadiumVision Director Release 3.2, including the centralized Cisco Stadiumvision Director network architecture, and the server platforms used to implement the solution.
“Configuring the Cisco StadiumVision Director Server System Settings”	Describes how to configure the initial setup of the Cisco StadiumVision Director server.
“Configuring Cisco StadiumVision Director Remote Servers”	Describes how to configure the initial setup of Cisco StadiumVision Director Remote server network connectivity and communication with the Cisco StadiumVision Director server.
“Configuring Cisco StadiumVision Director for Multiple Venue Support”	Describes how to enable and manage multiple venue support on Cisco StadiumVision Director Remote servers.
“System Accounts on the Cisco StadiumVision Director Servers”	Describes the default system accounts implemented by Cisco StadiumVision Director for access and control of certain server functions. Aside from the admin account, these system accounts are generally separate from the user accounts that secure access to the Cisco StadiumVision Director feature configuration and operation.
“User Management in Cisco StadiumVision Director”	Describes the Role-Based Access Control (RBAC) function in Cisco StadiumVision Director to control user access to only the portions of the system for which they are trained and authorized to use.
“Backing Up and Restoring Cisco StadiumVision Director Servers”	Describes how to setup and schedule backups between a primary and secondary server, and restore data between them.
“Configuring Failover Between Redundant Cisco StadiumVision Director Servers”	Describes the warm standby environment between two servers that run the Cisco StadiumVision Director software, where one of the servers operates as the primary active server, and the other server operates as a secondary backup server. This module explains how you can configure the backup server to become the active server if a failure occurs, and also how to restore the primary server.

Chapter	Description
“Cisco StadiumVision Director Server Text Utility Interface”	Provides an overview of the Text Utility Interface (TUI) for both the Cisco Stadiumvision Director and Cisco StadiumVision Director Remote servers. The TUI provides a console-based interface for use by system installers, administrators, and troubleshooting personnel to perform routine system tasks such as modifying system configurations, changing passwords, and checking system logs.
“System State Reports”	Provides information about the System State Report feature that enables easy capture and export of system state data for Cisco StadiumVision servers. This information can be sent to a remote support engineer to help troubleshoot any issues that occur with the system.

Related Documentation

- [Release Notes for Cisco StadiumVision Director Release 3.2](#)
- [Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.2](#)
- For the listing page of all Cisco StadiumVision documentation, go to:
http://www.cisco.com/en/US/products/ps11274/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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



StadiumVision



PART 1

Cisco StadiumVision Director Architecture Overview



Cisco StadiumVision Director Server Architecture

First Published: April 21, 2014

The standard Cisco StadiumVision Director network consists of all components of the solution implemented at a single site or venue. Cisco StadiumVision Director Release 3.1 introduced support for a centralized Cisco StadiumVision Director server that can be used to manage and control content for multiple venues using a distributed architecture of Cisco StadiumVision Director Remote servers connected to the central site over the Cisco Connected Stadium wide-area network (WAN).

This module describes the network architectures supported in Cisco StadiumVision Director Release 3.2 and the server platforms used to implement the solution. It includes the following topics:

- [Standard Cisco StadiumVision Director Network Architecture, page 1](#)
- [Centralized Cisco StadiumVision Director Network Architecture, page 4](#)
- [Server Platforms, page 5](#)

Standard Cisco StadiumVision Director Network Architecture

The three primary areas of the standard Cisco StadiumVision Director network architecture include:

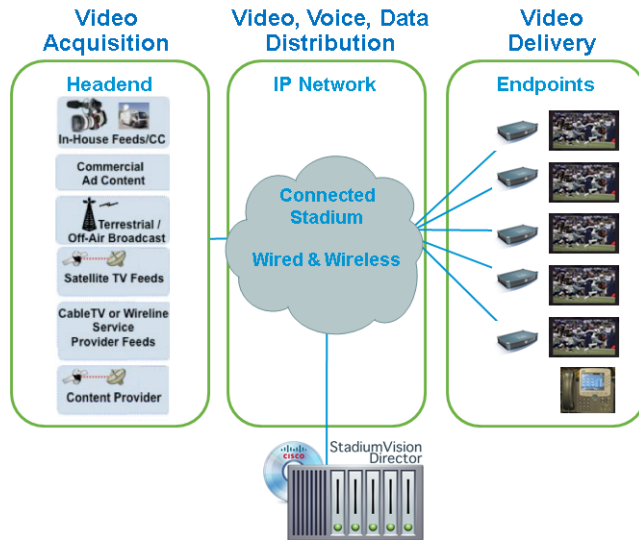
- Headend

The Cisco StadiumVision headend is designed to acquire, process, and encode the video content used in the Cisco StadiumVision solution.

- IP network
- Endpoints

Figure 1 shows the basic network architecture for a Cisco StadiumVision Director network.

Figure 1 Basic Cisco StadiumVision Director Architecture



Cisco StadiumVision Director Server Redundancy

Cisco StadiumVision Director supports an environment of two servers that run the Cisco StadiumVision Director software, where one of the servers operates as the primary active server, and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Figure 2 Cisco StadiumVision Director Server Redundancy

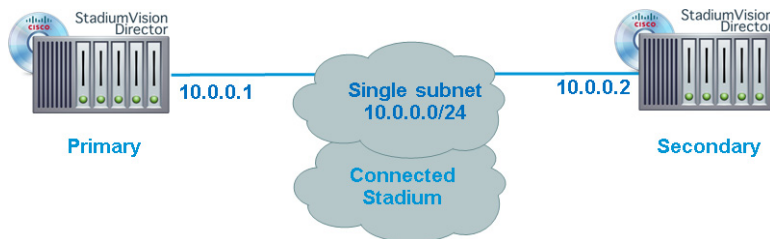


Figure 3 shows the architecture of Cisco StadiumVision Director server redundancy under normal network conditions and operation. The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet in the Cisco Connected Stadium network.

While the secondary server is still connected to the network, notice that communication and control only occurs between the primary Cisco StadiumVision Director server and the rest of the network, including the Digital Media Players (DMPs).

The secondary server is only connected to the network to be made available as a backup to the primary should a failure occur. In addition, the secondary server can (and should) be configured to be backed up with data from the primary server on a scheduled basis so that it can be ready as a warm standby.

Figure 3 Cisco StadiumVision Director Server Redundancy Under Normal Operation

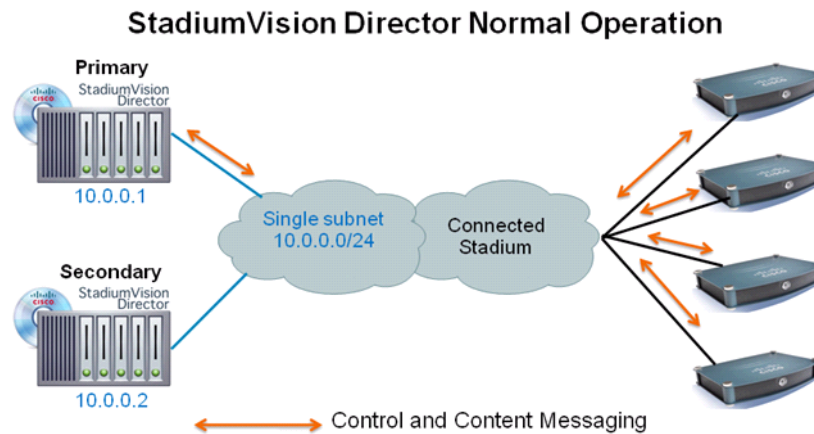
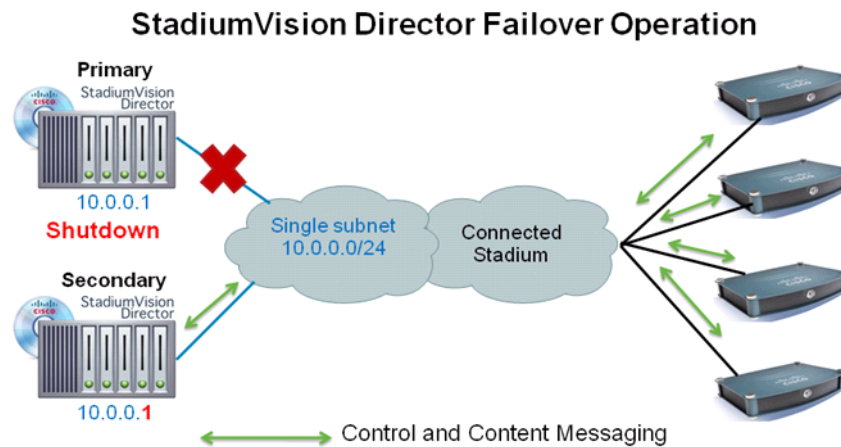


Figure 4 shows the redundancy environment when connectivity from the primary Cisco StadiumVision Director server fails. When the primary server fails, a manual process must take place to restore the secondary server from a backup, shut down the primary server, and activate the secondary server as the primary.

Figure 4 Cisco StadiumVision Director Server Redundancy Under Manual Failover



Notice that the secondary server must be reconfigured to use the same IP address the original primary server. In this example, the secondary server IP address is changed to 10.0.0.1 (from 10.0.0.2) to match the primary server address. When the process is complete, communication and control only occurs between the newly activated secondary server and the rest of the network.

**Note**

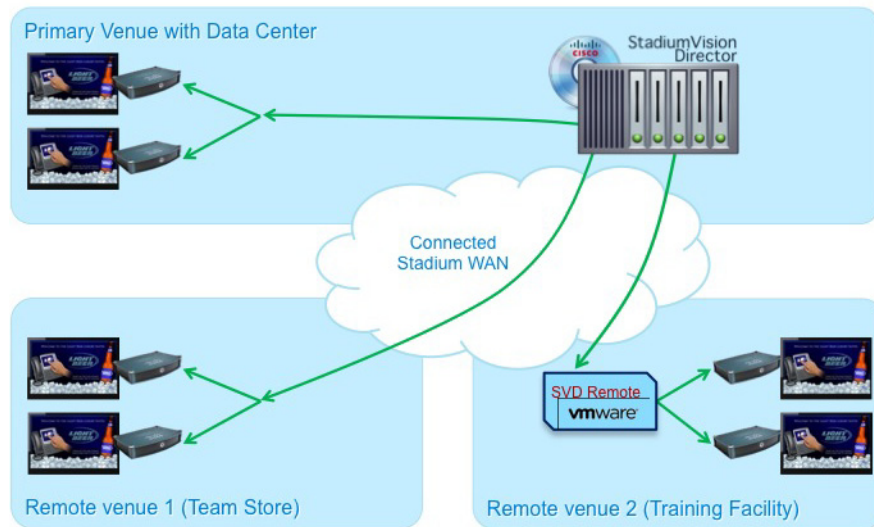
The word “failover” does not mean automatic activation of a secondary server. The failover process is manual with the secondary server acting as a warm standby.

For more information about how to perform the failover process, see the [“Configuring Failover Between Redundant Cisco StadiumVision Director Servers”](#) module on page 15.

Centralized Cisco StadiumVision Director Network Architecture

Figure 5 shows a central Cisco StadiumVision Director server connected to the headend, with network connections over the Cisco Connected Stadium WAN to multiple remote sites to Cisco StadiumVision Director Remote servers.

Figure 5 Centralized Cisco StadiumVision Director with Remote Sites



Cisco StadiumVision Director Remote Servers are installed at remote sites to provide a way of targeting site-specific content to locally-installed DMPs in a distributed Cisco StadiumVision Director network environment, where event operation can also be limited to designated venue operators.

Hierarchical Management

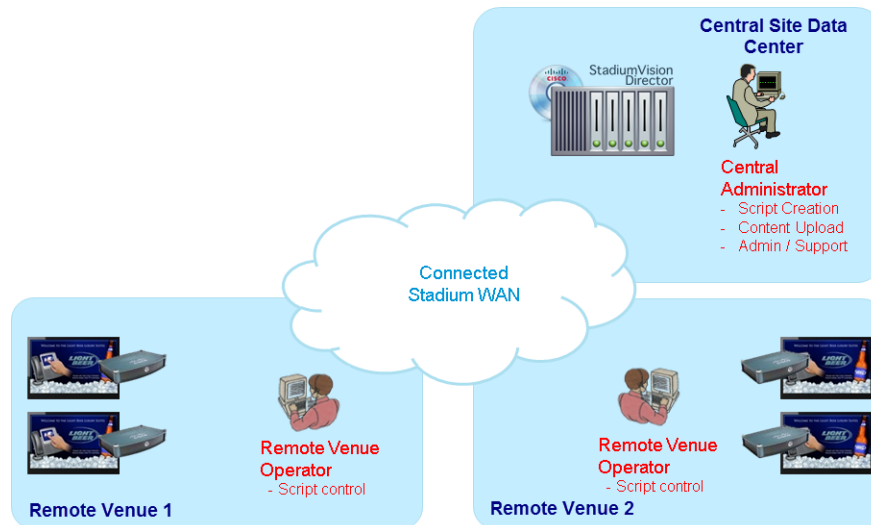
The centralized Cisco StadiumVision Director architecture implements control of multiple venues using Hierarchical Management, which includes the following areas of functionality:

- Introduction of the Venue Operator role that can be used to limit access and control of event operation at one or more assigned remote sites.

- Organization of venue operator, location, playlist, and script objects into site-specific groups by the Administrator role using venue association to manage access and control.

Figure 6 shows the use of Hierarchical Management in Cisco StadiumVision Director, where a central site user with administrator role-based access control (RBAC) permissions is located at the central site data center where the primary Cisco StadiumVision Director server resides.

Figure 6 Hierarchical Management in Centralized Cisco StadiumVision Director



The administrator can perform all venue-related functions, including assigning venue operators, content and scripts into their corresponding venue-specific scopes of control. At the remote venues, the remote venue operators can control the scripts associated to their assigned venue scope-of-control.

For more information, see the following modules of this guide:

- For a description of the supported user roles in Cisco StadiumVision Director, see the [“User Management in Cisco StadiumVision Director”](#) module on page 5.
- For information about configuring remote venues in a centralized Cisco StadiumVision Director network architecture, see the [“Configuring Cisco StadiumVision Director for Multiple Venue Support”](#) module on page 41.

Server Platforms

This section describes the server platforms supported by the Cisco StadiumVision Director server and the Cisco StadiumVision Director Remote server:

- [Cisco StadiumVision Director Servers, page 5](#)
- [Cisco StadiumVision Director Remote Server, page 8](#)

Cisco StadiumVision Director Servers

The Cisco StadiumVision Director Release 3.2 software can be supported on the following platforms:

- [Cisco StadiumVision Director Platform 2 Server, page 6](#)

- [Cisco StadiumVision Director Platform 3 Server, page 6](#)
- [Virtualized Server Environment Support, page 6](#)

Cisco StadiumVision Director Platform 2 Server

Cisco StadiumVision Director Release 3.2 requires a minimum of four data drives. Therefore, the Platform 2 server *must* have two additional 300 GB drives installed to support Cisco StadiumVision Director Release 3.2.



Note

The extra drives are mandatory for Release 3.2. For more information about the installation of additional hard drives on the Cisco StadiumVision Director Platform 2 server, contact your sales representative.

Figure 7 Front Panel of a Cisco StadiumVision Director Platform 2 Server



Cisco StadiumVision Director Platform 3 Server

The Cisco StadiumVision Director Platform 3 server (Cisco UCS C220 M3 server) is the newest platform to support Cisco StadiumVision Director Release 3.2 and has six drives in its default configuration for SV-DIR-DIRECTOR-K9 product ID (PID).



Note

If you order a spare Platform 3 server (SV-PLATFORM3=) only 2 drives are in the default configuration. Therefore, 4 additional data drives are required (SV-HD-A03-D300GA2=).

Figure 8 Front Panel of a Cisco UCS C220 M3 Rack Server



Virtualized Server Environment Support

You can use another Cisco device or third-party server to run the Cisco StadiumVision Director software beginning in Release 3.2. Be sure that your configuration meets the minimum system requirements in [Table 1](#) and supports a VMware ESX virtualized environment with a compatible ESX version (See [“VMware vSphere ESX Tested Versions for Cisco StadiumVision Director”](#) section on page 7.)

**Note**

Cisco StadiumVision Director servers are meant to be physically located close to the DMPs that they operate with, 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 the Cisco StadiumVision Director Server in a Virtualized Environment

System Component	Minimum Requirement
Processor	Two processors each equivalent to an Intel Xeon Processor E5-2460 (15 MB cache, 2.50 GHz clock, 7.20 GT/s Intel® QPI)
Forward write (fwrite) operations per second	10,000
Virtual CPUs	24
Virtual Disk Space	900 GB
Virtual RAM (VRAM)	32 GB

VMware vSphere ESX Tested Versions for Cisco StadiumVision Director

Cisco StadiumVision Director has been tested with VMware vSphere ESX version 5.1 and 5.5. Other VMware vSphere ESX versions cannot be guaranteed to work with Cisco StadiumVision Director Release 3.2.

**Note**

Any free version of ESX software, including VMware vSphere Hypervisor is not supported.

For more information about installing Cisco StadiumVision Director servers, see the [Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.2](#).

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 for Cisco StadiumVision Director Release 3.2](#).
- 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.

Cisco StadiumVision Director Remote Server

You can use your own server or install a Cisco UCS C22 server to run the Cisco StadiumVision Director Remote software. If using your own server, then the configuration *must* meet the minimum system requirements in [Table 2](#) and support a VMware ESXi virtualized environment.

Table 2 Minimum System Requirements for the Cisco StadiumVision Director Remote Server

System Component	Minimum Requirement
Hard Drive Capacity	300 GB Note The hard drives must be configured as a single logical volume. A RAID volume is strongly recommended.
Processor	Single processor equivalent to an Intel Xeon Processor E5-2420 (15 MB cache, 1.90 GHz clock, 7.20 GT/s Intel® QPI)
Virtual RAM (VRAM)	16 GB

For details about the Cisco UCS C22 M3 Rack Server, see the [Cisco UCS C22 M3 Rack Servers Data Sheet](#).

For more information about installing the Cisco UCS C22 M3 Rack Server hardware with the Cisco StadiumVision Director Remote software, see the [Cisco StadiumVision Director Remote Installation and Upgrade Guide](#).



StadiumVision



PART 2

Cisco StadiumVision Director Server Setup



Configuring the Cisco StadiumVision Director Server System Settings

First Published: April 21, 2014

Revised: June 13, 2014

This document is intended for Cisco StadiumVision Director administrators and describes how to configure the initial setup of the Cisco StadiumVision Director server.

Contents

- [Prerequisites for Configuring Cisco StadiumVision Director Server System Settings](#), page 3
- [How to Configure Cisco StadiumVision Director Server System Settings](#), page 4
- [What To Do Next](#), page 29

Prerequisites for Configuring Cisco StadiumVision Director Server System Settings

Before you configure Cisco StadiumVision Director servers, be sure that the following requirements are met:

- The Cisco StadiumVision Director server hardware and software is installed. For more information, see the [Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.2](#).
- The Cisco StadiumVision Director Server is installed and you know the IP address.
- 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 the network information required to configure the Ethernet connection on the Cisco StadiumVision Director Remote server, such as:
 - IP address (IPv4 only) and network mask



Note The Cisco StadiumVision Director Remote server should be configured with a static IP address or a non-expiring DHCP lease. In addition, DHCP Server Option 43 should be set up to point to the primary server’s URL for auto-registration to work.

- Default gateway address
- DNS server address
- Hostname
- You have either physical console access or an SSH client such as PuTTY to log into the Cisco StadiumVision Director server.
- You know the installer account credentials on the Cisco StadiumVision Director server.
- You understand how to use the Text Utility Interface (TUI). For more information, see the “[Cisco StadiumVision Director Server Text Utility Interface](#)” module. For simplicity in these tasks, the instruction to “select” a particular menu item implies that you type the character that corresponds to the menu option and press **Enter**.
- For NTP configuration requirements, see the “[Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs](#)” section on page 10.
- For multicast configuration requirements, see the “[Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director](#)” section on page 26.

How to Configure Cisco StadiumVision Director Server System Settings

This section includes the following tasks:

- [Completing Initial Configuration of System Settings After a Full ISO Installation, page 4](#) (required)
- [Configuring the Cisco StadiumVision Director Server Network Interface, page 5](#) (as required)
- [Editing the Hosts File, page 8](#) (as required)
- [Restarting the Network Service on the Server, page 9](#) (as required)
- [Generating the SSL Certificate, page 9](#) (as required)
- [Configuring NTP on Cisco StadiumVision Servers and DMPs, page 10](#) (required)
- [Configuring Multicast Ports for Cisco StadiumVision Director, page 23](#) (required)

Completing Initial Configuration of System Settings After a Full ISO Installation

When you install a full ISO on a Platform 3 server, you configure certain network settings in the Linux interface as part of the ISO installation such as the server IP address and DNS configuration.

As long as the network configuration is successfully completed as part of the installation, then the only remaining system configuration is to set the date and time options on the server and restart the Cisco StadiumVision Director software.

For detailed information about how to configure the date and time options, see the “[Configuring NTP on Cisco StadiumVision Servers and DMPs](#)” section on page 10.

**Note**

If for some reason you were unable to complete the Linux network configuration as part of the ISO installation, then you need to complete all of the tasks in this module.

Configuring the Cisco StadiumVision Director Server Network Interface

**Note**

If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

This task describes how to access the Linux menus from the TUI to configure the Cisco StadiumVision Director server network interface.

To configure the Cisco StadiumVision Director server network interface, complete the following steps:

- Step 1** Log into the TUI as installer on the server using a directly-connected console or SSH client. The TUI Main Menu is displayed.
- Step 2** From the Main Menu, go to **System Settings > Network Settings > Setup Network Information**.

**Tip**

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

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

- Step 3** At the Configure Network confirmation screen, press any key to continue to enter the Linux network configuration interface.

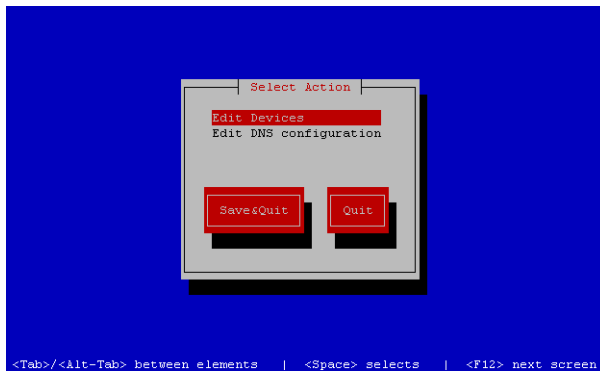
The Select Action Linux screen is displayed with the **Edit Devices** option selected.

**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.

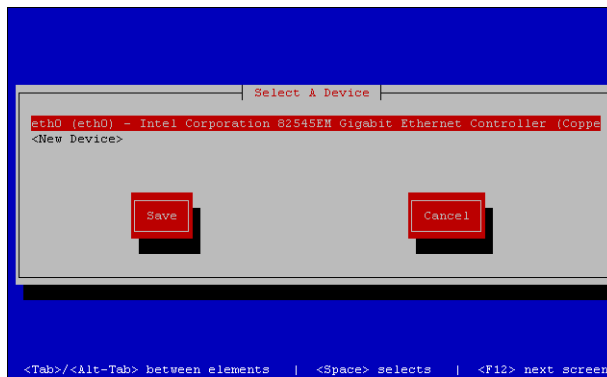
Step 4 In the Select Action screen, select **Edit Devices** and press **Enter**.

Figure 1 *Select Action Screen*



Step 5 In the Select a Device screen, select **eth0** and press **Enter**.

Figure 2 *Select a Device Screen*



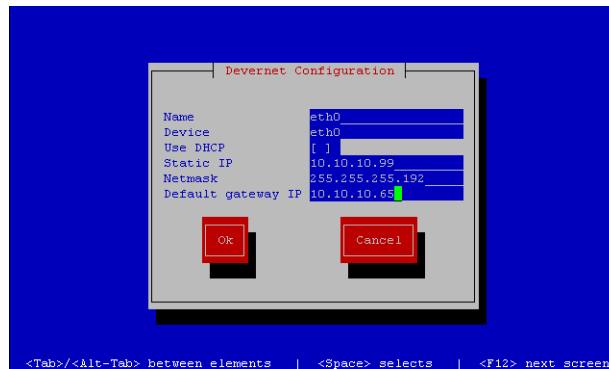
The Ethernet Configuration screen is displayed.



Note The Linux screen is mislabeled “Devernet Configuration.”

Step 6 In the Ethernet Configuration screen (Figure 3), do the following:

Figure 3 *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 7 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 8 Press the Tab key until the **Save** button is highlighted and press **Enter**.

You return to the Select Action screen.

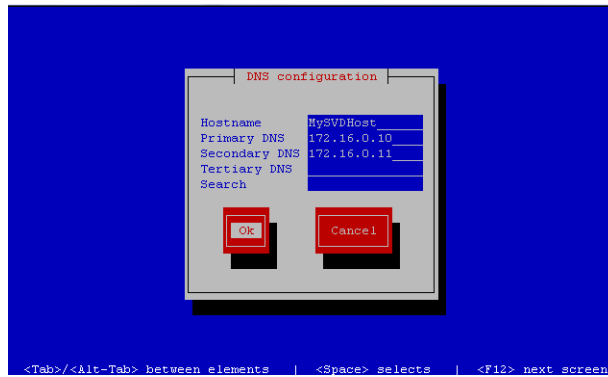
Step 9 Press the down arrow key to select the **Edit DNS configuration** option and press **Enter**.

The DNS configuration screen is displayed.

Step 10 In the DNS configuration screen (Figure 4), 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 4 DNS Configuration Screen

- Step 11** Press the Tab key until the **Ok** button is selected and press **Enter**.
You return to the Select Action screen.
- Step 12** In the Select Action screen, press the Tab key until the **Save&Quit** button is selected and press **Enter**.
You return to the TUI Configure Network menu.

Editing the Hosts File



Note

If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

Before you begin, be sure that you know how to use the vi editor. For more information, see the [“Cisco StadiumVision Director Server Text Utility Interface”](#) module on page 3.

To edit the hosts file, complete the following steps:

- Step 1** From the TUI Network Settings menu, select the **Edit hosts file** option.
- Step 2** At the confirmation prompt, press any key to open the `/etc/hosts` file for editing.
- Step 3** Change the line with IP address “10.10.10.10” to a comment (insert a # character at the beginning of the line) as shown in the following example:
- ```
#10.10.10.10
```
- Step 4** Change the line for the IPv6 localhost entry “::1” to a comment as shown in the following example:
- ```
#: :1
```
- Step 5** Add a line for the server IP address and hostname as shown in the following example, where `x.x.x.x` is the IPv4 address of the Cisco StadiumVision Director server, and `hostname` is the name to identify the server:
- ```
x.x.x.x hostname
```



### Note

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

- Step 6** Press **Esc** to enter vi command mode.
- Step 7** Save the changes to the file by typing the following command:  
:wq
- Step 8** Press any key to return to the Network Settings menu.
- 

## Restarting the Network Service on the Server

**Note**

If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

---

After you complete the network configuration on the Cisco StadiumVision Director server, restart the network service to apply the network configuration.

---

- Step 1** Log into the TUI as installer on the server using a directly-connected console or SSH client. The TUI Main Menu is displayed.
- Step 2** From the Main Menu, go to **Services Control > Networking > Restart networking**. The network interface eth0 is restarted.
- Step 3** Confirm that the command completed successfully.
- Step 4** Press any key to return to the Networking menu.
- Step 5** Return to the Main Menu.
- 

## Generating the SSL Certificate

**Note**

If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

---

**To generate the SSL certificate, complete the following steps:**

---

- Step 1** From the Main Menu, go to **System Settings > Network Settings**.
- Step 2** Select the **Generate certificate file** option.
- Step 3** When the confirmation warning prompt appears, type **Y** to continue and generate a new SSL certificate. To cancel without generating a new certificate, type **N**.
- Step 4** Press any key to return to the Network Settings menu.
-

## Configuring NTP on Cisco StadiumVision Servers and DMPs

Network Time Protocol (NTP) service is required in Cisco StadiumVision Director on the following devices:

- Cisco StadiumVision Director servers
- Cisco StadiumVision Director Remote servers
- DMPs

NTP provides the most reliable clocking for your Cisco StadiumVision network. NTP helps ensure synchronicity between redundant servers and the Cisco StadiumVision Director remote servers, and optimizes playlist synchronization on the DMPs.

You should verify the NTP configuration for your Cisco StadiumVision servers, since the default NTP source is a Red Hat Linux public pool and might not be the NTP server source that you want to use for your venue.

Configuration of the DMP NTP source is done within the Cisco StadiumVision Director Management Dashboard. As a best practice, the Cisco StadiumVision Director server is already set as the NTP host by default. This does not need to be changed unless the venue requires a different NTP source.



### Caution

In Release 3.2, the Cisco StadiumVision Director server is itself enabled as an NTP host to provide timing to the *DMPs only*. You also can use the Cisco StadiumVision Director server as the NTP host for your remote servers. Do not use Cisco StadiumVision Director as an NTP host for other devices in your network.

This section includes the following tasks:

- [Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs, page 10](#) (required)
- [Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers, page 11](#) (required)
- [Configuring NTP on DMPs, page 16](#) (required)
- [Verifying DMP Time Synchronization, page 21](#)

## Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs

Before configuring NTP on Cisco StadiumVision Director Servers and DMPs, be sure that the following requirements are met:

- You understand how to use vi editor commands.
- You understand the NTP host requirements for your Cisco StadiumVision servers:
  - If you do not want to use the default public pool of NTP servers for the Cisco StadiumVision servers, you have the IP address or DNS name of the NTP host for your network.
  - If you plan to use a public pool of NTP servers, be sure that the servers are reachable from the Cisco StadiumVision network. By default, the `ntp.conf` file on Cisco StadiumVision Director servers has configured the following Red Hat Linux public pool of servers:

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```



**Tip**

For more information about using NTP pool servers see the Network Time Protocol website at:

<http://support.ntp.org/bin/view/Servers/NTPPoolServers>

- If you plan to change the default best practice of using the Cisco StadiumVision Director server as the NTP source for DMPs, be sure that the following requirements are met:
  - You have configured the NTP host for the Cisco StadiumVision Director server first.
  - You have upgraded the DMP firmware to DMP-4310G Version 5.4.1(RB1) (Build 4544).  
For more information about how to upgrade the DMP firmware, see the *Cisco StadiumVision Director Software Installation and Upgrade Guide* for your release.
  - For optimal synchronization, use the same NTP server that is configured for the Cisco StadiumVision Director server. However, it is not required.
  - The DMP must not reference an NTP server pool. If the Cisco StadiumVision Director server references an NTP server pool (the default), then select a specific server from that same pool as the NTP server for the DMPs.
  - Only IPv4 is supported for the NTP server address on the DMPs.
  - The NTP server for the DMPs must not be a load-balanced server.
- The Cisco StadiumVision network is configured to allow bidirectional transmission of UDP messages on port 123 for NTP messages.

UDP port 123 is used for communication between the Cisco StadiumVision servers and NTP hosts, and the DMPs and NTP host (by default, this is the Cisco StadiumVision Director server).

For a complete port reference for Cisco StadiumVision Director servers, see the “Port Reference” module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide* for your release.

## Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers

When you install or upgrade the Cisco StadiumVision Director or Cisco StadiumVision Director Remote servers, you need to configure the system date and time in the TUI. You also need to configure the time zone.

**Note**

Although you can manually configure the system date and time on your servers when necessary, this should be avoided for your production network.

- [Setting Up the NTP Source on Cisco StadiumVision Servers, page 11](#) (required)
- [Configuring the Time Zone, page 12](#) (required)
- [Restarting the Cisco StadiumVision Software, page 15](#) (required)
- [Configuring the Date and Time Manually, page 16](#) (if necessary)

### Setting Up the NTP Source on Cisco StadiumVision Servers

**Note**

Complete this task only if you do not want to use the default public pool of servers.

Standard NTP server configuration uses the word “server” followed by the Domain Name System (DNS) name or IP address of an NTP server. By default, the `ntp.conf` file on Cisco StadiumVision Director servers has configured the following Red Hat Linux public pool of servers:

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

For these servers to be used as a reference clock, they must be reachable from the Cisco StadiumVision network.

If you want to use your own server, be sure to add it and comment out these default pool servers in the `ntp.conf` file. Otherwise, you do not need to do any further editing of the `ntp.conf` file in this task.

**To set up the NTP host on Cisco StadiumVision servers, complete the following steps:**

- 
- Step 1** From the TUI Main Menu, go to **System Settings > Date and Time Settings > Setup NTP Source**.  
A confirmation screen to Configure NTP and edit the `ntp.conf` file is displayed.
- Step 2** To open the `ntp.conf` file for edit, press any key.  
The `ntp.conf` file opens in the vi editor and the cursor is positioned at the end of the last configured NTP server line. If this is not the case, navigate to the server configuration section.
- Step 3** To enter INSERT line editing mode, type **i**.  
The vi editor changes to INSERT mode.
- Step 4** If you have a server that you want to use as the reference clock source at your site, do the following:
- Add a line and type “**server ip-address**” or “**server dns-name,**” where *ip-address* or *dns-name* is replaced by the IP address or name of the NTP server that you want to configure.
  - Go to the lines where the pool servers are configured and add a “#” sign in front to comment them out of the configuration as shown below:
- ```
#server 0.rhel.pool.ntp.org
#server 1.rhel.pool.ntp.org
#server 2.rhel.pool.ntp.org
```
- Step 5** To exit INSERT mode and return to vi command mode, press **Esc**.
- Step 6** To save your changes, type **:wq**.
The configuration is saved and the `ntpd` service is restarted. Verify that you see the “OK” confirmation that the `ntpd` has started.
- Step 7** To return to the Date and Time Settings menu, press any key.
-

Configuring the Time Zone

Configuring the time zone is required for both the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers.



Note

Although there is an option to set the time zone in the Venues interface of the Control Panel on the Cisco StadiumVision Director server, this option is informational only and is also used for proof-of-play reporting. The actual time zone for the venue is configured from the TUI on the remote server.

This section includes the following tasks:

- [Finding the Time Zone Code for System Configuration, page 13](#) (optional)
- [Configuring the System Time Zone, page 14](#) (required)

Finding the Time Zone Code for System Configuration

Use this task if you need to find out the time zone code to configure the server's time zone information.



Note

This task provides information only and does not actually configure the time zone.

To find the time zone code for system configuration, complete the following steps:

- Step 1** From the Date and Time Settings menu, do the following:
- Select **Change Timezone**.
 - Type the number that corresponds to the applicable continent or ocean for the location of the remote server.
 - Type the number that corresponds to the country.
 - Type the number for the time zone (as applicable).
 - When the confirmation of the time zone information that you configured is displayed, type **1** (for Yes) to accept your settings, or **2** (for No) to cancel ([Figure 5](#)).

Figure 5 Time Zone Confirmation Prompt

```
The following information has been given:

    United States
    Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:   Mon Feb 18 16:42:55 PST 2013.
Universal Time is now: Tue Feb 19 00:42:55 UTC 2013.
Is the above information OK?
1) Yes
2) No
#?
```

- After confirming Yes at the prompt, note the time zone string that is provided. [Figure 6](#) shows a sample time zone code for America/Los_Angeles.

Figure 6 Sample Time Zone Code

```

The following information has been given:

    United States
    Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:   Mon Feb 18 16:56:47 PST 2013.
Universal Time is now: Tue Feb 19 00:56:47 UTC 2013.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
    TZ='America/Los_Angeles'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
America/Los_Angeles
Press any key to return to the menu.

```

- Step 2** Press any key to return to the Date and Time Settings menu.
- Step 3** Configure the system time zone using the appropriate code for the server location. See the [“Configuring the System Time Zone”](#) section on page 14.

Configuring the System Time Zone

Prerequisites

Before you configure the system time zone, you should know the following information:

- How to use vi editor commands.
- The time zone code for the server location. If you need to look up the time zone code, see the [“Finding the Time Zone Code for System Configuration”](#) section on page 13.

Procedure

To configure the system time zone so that it persists after restart of the server, complete the following steps:

- Step 1** From the TUI Main Menu on the server, go to **System Settings > Date and Time Settings > Change System Timezone**.
- Step 2** At the prompt to edit the system clock file, press any key to continue.
The `/etc/sysconfig/clock` file is opened for editing.
- Step 3** Use the vi editor to specify your time zone. [Figure 7](#) shows an entry for the **“America/Los_Angeles”** time zone code.



Tip

The quotation marks and underscore symbols are required.

Configuring the Date and Time Manually



Note

This task is provided as a precaution if you should find it necessary to manually set the system date and time. Manual date and time configuration should be avoided on a production system and NTP service used instead.

To configure the date and time manually, complete the following steps:

-
- Step 1** From the TUI Main Menu on the server, go to **System Settings > Date and Time Settings > Change Date and Time**.
- Step 2** At the confirmation prompt, type **Y** to continue.
- Step 3** Type the new date and time in the format: MMDDhhmm[[CC] YY] [.ss], where:
- MMDDhhmm is required (MM is month, DD is day, hh is hour, and mm is minutes).
 - CC is the century (first 2 digits of the year) and is optional for use with YY. For example “20” in the year 2013.
 - YY is the last 2 digits of the year and is optional. For example “13” in the year 2013.
 - .ss is seconds and is optional.
- Step 4** Press any key to return to the Date and Time Settings menu.
-

Configuring NTP on DMPs

Beginning in Release 3.2, you must configure NTP on the Cisco StadiumVision Director server *and* the DMPs. Granules are no longer used in Cisco StadiumVision Director for timing with the DMPs.

Through default MIB settings on the DMPs, the following values are preset and should not be modified:

- Time zone—Etc/UTC Coordinated Universal Time.
- Daylight Savings Time—Off.

Generally, the only values that you might consider changing are the NTP host and the sync interval. These values can be configured both globally and for selected DMPs.

This section includes the following tasks:

- [Applying the Standard NTP Configuration on all DMPs in the System, page 16](#) (recommended)
- [Modifying the Standard NTP Configuration Globally on all DMPs, page 17](#) (optional)
- [Modifying the Standard NTP Configuration on Selected DMPs in the System, page 19](#) (optional)
- [Verifying DMP Time Synchronization, page 21](#) (recommended)

Applying the Standard NTP Configuration on all DMPs in the System

The NTP service is automatically enabled for DMPs and uses the Cisco StadiumVision Director server as the host. If you do not plan to change the NTP host, then you can simply run the **Global DMP Settings** command to apply the standard configuration on all DMPs in the system.

To configure apply the standard NTP configuration on all DMPs, complete the following steps:

-
- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the **Management Dashboard**.
- Step 3** Go to **DMP and TV Controls > Global Settings > Global DMP Settings**.
- Step 4** Select All Devices and click the Play (>) icon to run the command.
- All global MIB settings, including the new NTP settings, are sent to all DMPs.
-

Modifying the Standard NTP Configuration Globally on all DMPs

Table 1 provides information about all of the global DMP NTP properties that can be specified in the Management Dashboard to control NTP service on all DMPs.

Table 1 Global DMP Common NTP Property Values

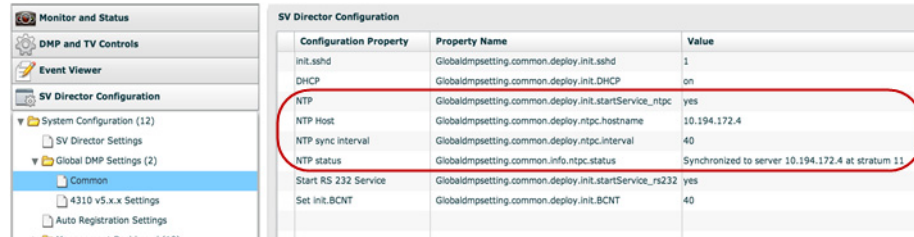
Property (Registry Key)	Description	Values
NTP (Globaldmpsetting.common.deploy.init.startService_ntpc)	Enables or disables running of the NTP service on the DMP.	<ul style="list-style-type: none"> yes—(Default) Enables NTP service to support playlist synchronization across DMPs. no—Disables NTP service.
NTP Host (Globaldmpsetting.common.deploy.hostname)	IPv4 address of the NTP server.	Default—IP address of the Cisco StadiumVision Director server.

Table 1 Global DMP Common NTP Property Values

Property (Registry Key)	Description	Values
NTP sync interval (Globaldmpsetting.common.deploy.ntpc.interval)	Number of seconds that the DMP waits before trying to sync time with the configured NTP host. The DMP clock drifts, so setting the NTP sync interval too high can cause observable deterioration of synchronization over time. Playlist synchronization improves when the DMP updates its clock.	40 (Default) Note Do not specify a value less than 40 due to a known problem in the DMP 4310G.
NTP status (Globaldmpsetting.common.info.ntpc.status)	Expected NTP status from the DMP for DMP compliance checking.	<ul style="list-style-type: none"> • Synchronized to server <i>svd-ip</i> at stratum <i>n</i>—Uses the IP address of the Cisco StadiumVision Director server and its NTP stratum level. Note If you change the NTP Host, you need to change keep this string but change the <i>svd-ip</i> and <i>n</i> arguments to reflect the corresponding values for that new host. <ul style="list-style-type: none"> • \$svd_ignore—(Default) Skips this field during DMP compliance testing.

To modify the standard NTP configuration globally on all DMPs, complete the following steps:

-
- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the **Management Dashboard**.
- Step 3** Click **SV Director Configuration > System Configuration > Global DMP Settings > Common** (Figure 8).

Figure 8 Common Global DMP Settings for NTP


Configuration Property	Property Name	Value
init.sshd	Globaldmpsetting.common.deploy.init.sshd	1
DHCP	Globaldmpsetting.common.deploy.init.DHCP	on
NTP	Globaldmpsetting.common.deploy.init.startService_ntpc	yes
NTP Host	Globaldmpsetting.common.deploy.ntpc.hostname	10.194.172.4
NTP sync interval	Globaldmpsetting.common.deploy.ntpc.interval	40
NTP status	Globaldmpsetting.common.info.ntpc.status	Synchronized to server 10.194.172.4 at stratum 11
Start RS 232 Service	Globaldmpsetting.common.deploy.init.startService_rs232	yes
Set init.BCNT	Globaldmpsetting.common.deploy.init.BCNT	40

Step 4 To change the NTP Host, type the IPv4 address of the NTP server that you want the DMPs to reference.

Step 5 (Optional) In the NTP status property, change the IP address and stratum number according to the new NTP host.



Note To skip this field when performing DMP compliance checking, use the `$svd_ignore` value.

Step 6 (Optional) Change other global NTP properties as required for your environment. Refer to [Table 1](#).

Step 7 Click the disk icon to Save changes ([Figure 9](#)).

Figure 9 Save Changes Icon

Step 8 Go to **DMP and TV Controls > Global Settings > Global DMP Settings**.

Step 9 Select All Devices and click the Play (>) icon to run the command.

All global MIB settings, including the new NTP settings, are sent to all DMPs.

Modifying the Standard NTP Configuration on Selected DMPs in the System

[Table 2](#) describes all of the NTP MIBs and their default values.



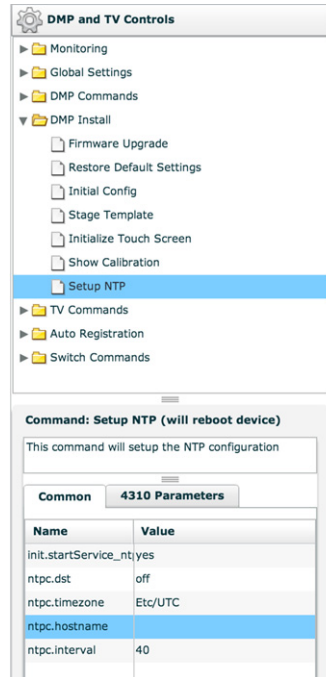
Note Under normal operation, only the `ntpc.hostname` and `ntpc.interval` MIBs should be modified.

Table 2 DMP NTP MIB Descriptions and Settings

MIB	Description	Required?	Values
init.startService_ntpc	NTP service on the DMP. Note Avoid modifying this MIB.	Yes	<ul style="list-style-type: none"> yes—(Default) Enables NTP service to support playlist synchronization across DMPs. no—Disables NTP service.
ntpc.dst	Daylight savings time parameter of the NTP service. Note Avoid modifying this MIB.	Yes	<ul style="list-style-type: none"> on—(Default). off—(Required).
ntpc.timezone	Time zone parameter of the NTP service. Note Avoid modifying this MIB.	Yes	Etc/UTC —(Default). Coordinated Universal Time. Note The Etc/UTC value is case sensitive and must be typed as shown.
ntpc.hostname	NTP server address (IPv4 format only).	Yes, when DMP NTP service is enabled.	<ul style="list-style-type: none"> No value—(Default). IPv4 address—(Required).
ntpc.interval	Number of seconds that the DMP waits before trying to sync time with the configured NTP host. The DMP clock drifts, so setting the NTP sync interval too high can cause observable deterioration of synchronization over time. Playlist synchronization improves when the DMP updates its clock.	Yes	40 (Default) Note Do not specify a value less than 40 due to a known problem in the DMP 4310G.

To modify the standard NTP configuration on selected DMPs, complete the following steps:

-
- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the **Management Dashboard**.
- Step 3** Click **DMP and TV Controls > DMP Install > Setup NTP** (Figure 10).

Figure 10 DMP and TV Controls Setup NTP MIBs

- Step 4** From the Common tab in the Command:Setup NTP section, specify the values of the NTP MIB variables according to the recommended and required values in In the Select Devices panel, select the DMPs where you want to setup the NTP service.
- Step 5** Click the Play button to set the MIB values on the selected devices.

Verifying DMP Time Synchronization

You can find DMPs that are having problems synchronizing with the NTP server using the DMP compliance check in the Management Dashboard.

Before you can run a valid DMP compliance check for the DMP synchronization status, the “**Synchronized to server *svd-ip at stratum n***” value of the NTP status global DMP properties must reflect the IP address of your NTP host and its stratum level.



Note

Outside of Cisco StadiumVision Director, if you know the DMP IP address, you can find a single DMP’s NTP status using a web browser and going to either of the following URLs:

http://dmpIpAddress

https://dmpIpAddress/get_param?p=*

Find “ntp.status”. A sample line depicting unsuccessful time synchronization is:
ntp.status T_STRING Not Synchronized

To verify DMP time synchronization, complete the following steps:

- Step 1** Do one of the following to find and confirm the stratum level for the NTP host:
- If you are using the Cisco StadiumVision Director server as the NTP host:
 - Log into the TUI and go to **Troubleshooting > NTP > Local clock state** (Figure 11).

Figure 11 Stratum Field in Local Clock State TUI Output

```

assID=0 status=06f4 leap_none, sync_ntp, 15 events, event_peer/strat_chg,
version="ntpd 4.2.2p1@1.1570-o Tue Oct 25 12:54:50 UTC 2011 (1)",
processor="x86_64", system="Linux/2.6.18-128.el5", leap=00, stratum=2,
precision=-19, rootdelay=73.305, rootdispersion=25.968, peer=29765,
refid=10.81.254.131,
reftime=d6ce2ac9.2e4403ff Fri, Mar 14 2014 18:26:33.180, poll=8,
clock=d6ce2bc3.d079406e Fri, Mar 14 2014 18:30:43.814, state=4,
offset=12.638, frequency=34.718, jitter=11.517, noise=8.480,
stability=2.409, tai=0
Press any key to return to the menu.
  
```



Tip Alternatively, you can run a DMP **Get Status** command on one of the DMPs from the Management Dashboard and find the value reported in its ntpc.status MIB value.

- If you are using an NTP host other than the Cisco StadiumVision Director server:
 - Log into the TUI and go to **Troubleshooting > NTP > Show configured peers and clients**. Find the configured NTP host in the “refid” field and its corresponding stratum level under the “st” column.

Figure 12 Stratum Field in Show Configured Peers and Clients Output

```

-----
remote      refid      st t when poll reach  delay  offset  jitter
-----
*rtsp5-b5-rbb-ntp .GPS.      1 u 194 256 377  73.305  6.785  8.052
*rtsp10-a9-rbb-nt .GPS.      1 u  97 256 377  73.371 18.909 10.486
LOCAL(0)     .LOCL.     10 l  44  64 377   0.000   0.000  0.002
Press any key to return to the menu.
  
```

- Step 2** Go to the **Management Dashboard** and do the following:
- In the NTP status property, type the value to “**Synchronized to server svd-ip at stratum n**” and be sure that the IP address is set to your NTP host and the stratum level matches the level that you confirmed in [Step 1](#).
 - Run the **Global DMP settings** command to apply the configuration to all DMPs.

See the “[Modifying the Standard NTP Configuration Globally on all DMPs](#)” section on page 17 for more information.

- Step 3** Go to the **Management Dashboard**.
- Step 4** Click **DMP and TV Controls > Monitoring > Get Status**.
- Step 5** At the bottom of the screen, go to **Status > Compliance**.
- Step 6** Find ntpc.status MIB and look for information about the synchronization status, such as “Not synchronized.”

If your DMPs are not synchronized, see the “[What To Do Next](#)” section on page 23.

What To Do Next

If you find that DMPs are not synchronized:

- Confirm that you have met the requirements described in the “[Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs](#)” section on page 10.
- Verify your NTP host configuration to be sure that the proper IP address is configured.
- Verify reachability of the NTP server from the DMPs in your Cisco StadiumVision network.

For more information about other NTP troubleshooting on your network, refer to the following URL:

<http://doc.ntp.org/3-5.93e/debug.html>

**Note**

After you verify DMP NTP synchronization, be sure to reset the NTP status field back to \$svd_ignore because the stratum value can change.

Configuring Multicast Ports for Cisco StadiumVision Director

This section includes the following topics:

- [Information about Multicast Support in Cisco StadiumVision Director, page 23](#)
- [Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director, page 26](#)
- [How to Configure Multicast Ports in Cisco StadiumVision Director, page 27](#)

Information about Multicast Support in Cisco StadiumVision Director

This section includes the following topics:

- [Per-Script Multicast Optimization, page 23](#)
- [Multicast Registry Keys in Cisco StadiumVision Director, page 25](#)

Per-Script Multicast Optimization

In Cisco StadiumVision Director Release 3.2, the original Multicast Optimization introduced in Release 3.1 is replaced by Per-Script Multicast Optimization (for up to 20 different scripts) to reduce the number of multicast messages that each DMP must process.

Per-Script Multicast Optimization is designed to reduce the load on DMPs when the following conditions are present in Cisco StadiumVision Director:

- More than one event script is run simultaneously in a venue.
The scripts can be running across multiple venues, scripts running in a single venue, or running in systems without Cisco StadiumVision Director Remote servers.
- The External Content Integration feature is used, which sends multiple messages to the DMPs in a script.

Table 3 provides a summary of the two different multicast optimization features supported in Cisco StadiumVision Director.

Table 3 Summary of Multicast Optimization Features in Cisco StadiumVision Director

Feature Name	Release	Scope	Remote Servers Required	Default
Multicast Optimization ¹	3.1 only	Per Site	Yes	Automatic when multi-venue support is enabled.
Per-Script Multicast Optimization	3.2 and later	Per Script (20 maximum) ²	No	Disabled.

1. For information about per-site multicast optimization in Cisco StadiumVision Director Release 3.1, see the “Multicast Optimization for Remote Venues” topic in the “Configuring Cisco StadiumVision Director for Multiple Venue Support” module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.1*.
2. If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.

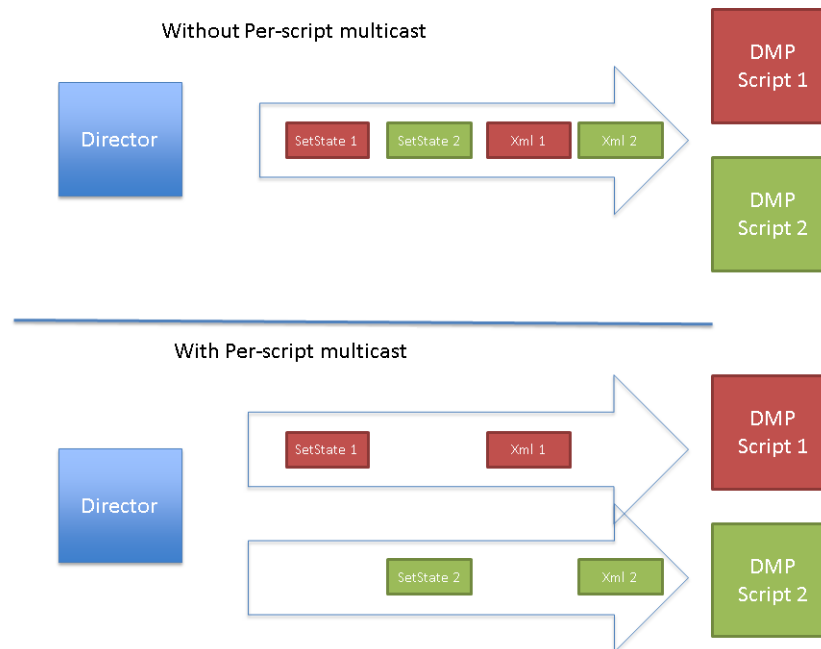
Benefits of Per-Script Multicast

In releases of Cisco StadiumVision Director 3.1 and earlier, the server uses a single multicast channel for all DMPs. In Release 3.2, you can configure multiple multicast channels, over which the server sends only the multicast messages needed for a particular event script for up to 20 scripts.

If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.

Figure 13 shows this message separation. Each DMP goes from seeing four packets to seeing two. More importantly, each DMP now only has to process one XML payload, which is important when the XML payloads are sizeable.

Figure 13 Multicast Messaging With and Without Per-Script Multicast Optimization



All DMPs, including those associated with a Cisco StadiumVision Director Remote server, listen on these per-script multicast channels.

For messages that apply to multiple event scripts, the message is duplicated and sent to each multicast channel. Therefore, this feature can increase the load on Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers (increasing the number of messages sent and copying of messages) as a tradeoff for reducing the number of messages seen and processed by DMPs. However, this load is expected to be negligible.

Multicast Registry Keys in Cisco StadiumVision Director


Cisco StadiumVision Director uses multicast messages for DMP control-plane operation. Cisco Connected Stadium network design assigns the following multicast group addresses for use by Cisco StadiumVision Director:

- 239.193.0.0/24—For control communication
- 239.192.0.0/24—For video communication (This network should be avoided for the multicast configuration described in this module.)

Multicast addressing is configured using registry keys from the Cisco StadiumVision Director Management Dashboard.

Table 4 describes the registry keys in Cisco StadiumVision Director that control the multicast configuration.

Table 4 *Multicast Registry Keys in Cisco StadiumVision Director*

Registry Key	Default Value	Description
MulticastHostPort	239.192.0.254:50001  Caution This default multicast address should be changed after installation to use the 239.193.0.0/24 address range, or the network that is configured in your Cisco Connected Stadium network for Cisco StadiumVision control.	Sets the global multicast address and port for Cisco StadiumVision Director.
transport.dynamic.enable	<ul style="list-style-type: none"> False (for upgraded servers). Per-Script Multicast Optimization is disabled and the Cisco StadiumVision Director server sends all communication over the MulticastHostPort address directly to all DMPs and Cisco StadiumVision Director Remote servers, including all remote DMPs. True (for new installations) 	Enables and disables Per-Script Multicast optimization.
transport.dynamic.send_range	50080-50099 If the MulticastHostPort registry key is 239.193.0.254:50001, then 239.193.0.254:50080–239.193.0.254:50099 is used as the range of Global hostports for the running scripts.	Specifies the range of ports for Per-Script Multicast Optimization. These ports are used with the network specified in the MulticastHostPort registry key, to define a range of additional global hostports to be assigned for running scripts.

Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director

Before you configure multicast ports, be sure that the following requirements are met:

- Be sure that you understand the multicast addressing in use for all areas of your Cisco StadiumVision network, including Cisco Connected Stadium and Cisco StadiumVision Mobile networks. Confirm that there are not any multicast address/port overlaps.



Caution

Because of the large number of ports that per-script multicast configuration requires, and the possibility for hard-to-diagnose failures if video is routed to a DMP's control channel (which can occur when the port numbers are the same and even if the group/host portion is different), it is critical to verify that the port ranges you plan to use are not used by any other source of multicast in the network.

- For a summary of all of the input and output ports in use by Cisco StadiumVision Director and Cisco StadiumVision Director Remote, see the “Appendix B: Port Reference” module in the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 3.2*.

- For more information about the recommended multicast addressing for the Cisco Connected Stadium network, see the *Cisco Connected Stadium Design Guide* available from your Cisco Systems representative.
- The network is properly configured to route the global multicast host port to be visible for all DMPs in the Cisco StadiumVision network, including those at remote venues and associated to venues in a multi-venue environment.

How to Configure Multicast Ports in Cisco StadiumVision Director

This section includes the following tasks:

- [Configuring the Global Multicast Host Port in Cisco StadiumVision Director, page 27](#) (required)
- [Configuring Per-Script Multicast in Cisco StadiumVision Director, page 27](#) (recommended)

Configuring the Global Multicast Host Port in Cisco StadiumVision Director

The global multicast host port is used by Cisco StadiumVision Director to send messages to DMPs when they are not part of a script, when per-script multicast is disabled, or when the number of scripts running exceeds to configured maximum of per-script multicast ports.

It is configured in the “MulticastHostPort” registry key in the Management Dashboard.

**Note**

The default value currently uses the address 239.192.0.254:50001 and should be changed to a network address in the range 239.193.0.0/24.

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** Click on the value field and specify a multicast address in the range 239.193.0.0/24 and port number.

**Note**

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

- Step 4** Click **Apply**.

Configuring Per-Script Multicast in Cisco StadiumVision Director

By default, Per-Script Multicast Optimization is disabled and the Cisco StadiumVision Director server sends all communication over the MulticastHostPort address directly to all DMPs and Cisco StadiumVision Director Remote servers, including all remote DMPs.

To take advantage of per-script multicast optimization it must be enabled for systems being upgraded to Release 3.2.0-489. Otherwise, it is enabled by default for new installations.

To configure per-script multicast, complete the following steps:

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

Step 2 To enable per-script multicast, change the values of the following registry keys:

- **transport.dynamic.enable**—Specify a value of **true**.
- **transport.dynamic.send_range**—(As Required) Change the range of ports to comply with your network configuration. The default is 50080-50099.



Note Be sure that these ports do not overlap with other multicast ports in use on your network.

Step 3 Click **Apply**.

Step 4 Reload the Flash template on all DMPs:

- a. From the DMP and TV Controls dashboard drawer, navigate to and select the following command: **DMP and TV Controls > DMP Install > Stage Template**.
- b. Select all of the DMP devices where the command should be applied.
- c. Click the Play button to run the command on the selected devices.

Step 5 To verify the configuration:

- a. Start and stop event scripts and change states.
- b. Verify that the multicast port that the DMP is listening on is one of the per-script ports (50080-50099 by default), rather than the global multicast hostport (50001).

If the scripts do not start and stop, see the [“Troubleshooting Per-Script Multicast Configuration” section on page 28](#).

Troubleshooting Per-Script Multicast Configuration

This section includes information about troubleshooting the following behaviors when per-script multicast optimization is enabled:

- [Scripts Unable to Start or Stop, page 28](#)
- [DMPs Rebooting, page 29](#)

Scripts Unable to Start or Stop

Verify that the multicast packets are reaching the DMPs using any or all of the following methods:

- Look at the `sv_msg_mcast_trace.log` available from the Troubleshooting menu of the TUI for Cisco StadiumVision Director in the Control logs.
- Use a packet sniffer device at Cisco StadiumVision Director and/or at the DMP.
- Inspect the multicast configuration of the Cisco Connected Stadium switch by turning on debug for multicast group subscriptions.

**Tip**

It is valuable to know the multicast group/port that a specific DMP should be listening on. This can be validated using the dmpconfig debug feature, by going to the URL:

`http://svd-ip:8080/StadiumVision/dmpconfig/000000000000?ipaddr=x.x.x.x`, where

`x.x.x.x` is the IP address of the DMP to be debugged.

In the XML output provided, you will see the multicast IP address and port in use.

DMPs Rebooting

DMPs rebooting or becoming unresponsive while per-script multicast is enabled is most likely due to some multicast video port overlap with the ports used for multicast control.

To diagnose this condition:

- Inspect all multicast port numbers in the configuration to investigate any multicast group/port overlaps.
- Using a packet sniffer, inspect network traffic on a separate box and via port span rather than on a DMP.

What To Do Next

After you have configured the system settings for your Cisco StadiumVision Director servers, be sure to do the following:

- Configure the backup environment between your primary and secondary servers. For more information, see the [“Backing Up and Restoring Cisco StadiumVision Director Servers” module on page 3](#).
- If you are configuring Cisco StadiumVision Director Remote servers:

The centralized Cisco StadiumVision Director server is configured by default to use a global account for communication with all Cisco StadiumVision Director Remote servers to support monitoring of venues from the Management Dashboard. Using the default configuration, you can specify a common password to be used by all Cisco StadiumVision Director Remote servers.

You can change the default configuration and specify a unique password for each remote server. To do this, you must modify the global credential on the Cisco StadiumVision Director server, and then configure a password in the Venues interface from the Control Panel on the Cisco StadiumVision Director server.

Whether you are using a common or unique password, the remote server must be configured to use the same password that is configured on the Cisco StadiumVision Director server for that venue.

For more information about configuring Cisco StadiumVision Director to support remote servers and multiple venue support, see the following modules:

- [“Configuring Cisco StadiumVision Director Remote Servers” module on page 31](#).
- [“Configuring Cisco StadiumVision Director for Multiple Venue Support” module on page 41](#).



Configuring Cisco StadiumVision Director Remote Servers

First Published: April 21, 2014

Beginning in Cisco StadiumVision Director Release 3.1, a centralized server site can be deployed with multiple remote sites in a multi-venue architecture. This document is intended for Cisco StadiumVision Director administrators and describes how to configure the initial setup of Cisco StadiumVision Director Remote server network connectivity and communication with the Cisco StadiumVision Director server.

Contents

- [Prerequisites for Configuring Cisco StadiumVision Director Remote Servers, page 31](#)
- [Information About Configuring Cisco StadiumVision Director Remote Servers, page 32](#)
- [How to Configure Cisco StadiumVision Director Remote Servers, page 33](#)
- [What To Do Next, page 39](#)

Prerequisites for Configuring Cisco StadiumVision Director Remote Servers

Before you configure Cisco StadiumVision Director remote servers, be sure that the following requirements are met:

- The Cisco StadiumVision Director Remote server hardware and software is installed. For more information, see the [Cisco StadiumVision Director Remote Installation and Upgrade Guide](#).
- The Cisco StadiumVision Director Server is installed and you know the IP address.

- You understand the use of the global credential for Management Dashboard monitoring, and you have determined a common password for use by all remote servers, or unique passwords for each venue. The JMX password must be a minimum length of 6 characters.
- You know the time zones where the remote servers are installed and the NTP source address (if used).
- You have either physical console access or an SSH client such as PuTTY to log into both the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers.
- You know the installer account credentials on the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers.
- You understand how to use the Text Utility Interface (TUI). For more information, see the “[Cisco StadiumVision Director Server Text Utility Interface](#)” module. For simplicity in these tasks, the instruction to “select” a particular menu item implies that you type the character that corresponds to the menu option and press **Enter**.

Information About Configuring Cisco StadiumVision Director Remote Servers

This section includes the following topics:

- [Management Dashboard Monitoring and the Global Credential, page 32](#)
- [Main Menu Applications, page 33](#)

Management Dashboard Monitoring and the Global Credential

The centralized Cisco StadiumVision Director server is configured by default to use a global account for communication with all Cisco StadiumVision Director Remote servers to support monitoring of venues from the Management Dashboard. Using the default configuration, you can specify a common password to be used by all Cisco StadiumVision Director Remote servers.

You can change the default configuration and specify a unique password for each remote server. To do this, you must modify the global credential on the Cisco StadiumVision Director server, and then configure a password in the Venues interface from the Control Panel on the Cisco StadiumVision Director server.

Whether you are using a common or unique password, the remote server must be configured to use the same password that is configured on the Cisco StadiumVision Director server for that venue.

**Note**

The global credential is *not* a user password for the remote server.

Main Menu Applications

The Cisco StadiumVision Director Remote server supports the following applications from its Main Menu using the admin user credential:

- System State Reports

The System State Report feature enables easy capture and export of system state data for Cisco StadiumVision servers. This information can be sent to a remote support engineer to help troubleshoot any issues that occur with the system. For more information, see the [“System State Reports” module on page 1](#).

- Software Manager

Allows you to install ISO files for fresh installs or upgrades after the first installation of Cisco StadiumVision Director Remote Release 3.2 software.

**Note**

Installation of language packs and custom fonts are not supported for Cisco StadiumVision Director Remote Release 3.2.

The Main Menu is accessible with HTTP or HTTPS access using a web browser and specifying the IP address of the remote server.

To use these applications, the admin user password must be configured from the TUI System Accounts menu after Cisco StadiumVision Director Remote Release 3.2 is installed.

How to Configure Cisco StadiumVision Director Remote Servers

This section includes the following tasks:

- [Configuring Connectivity to the Cisco StadiumVision Director Server, page 33](#) (required)
- [Configuring the Admin Password, page 38](#) (required)
- [Configuring the Date and Time Options on the Remote Server, page 39](#) (required)


Configuring Connectivity to the Cisco StadiumVision Director Server

This section includes the following tasks:

- [Configuring the Cisco StadiumVision Director Server IP Address on the Remote Server, page 34](#) (required)
- [Configuring the Global Credential on the Cisco StadiumVision Director Server, page 34](#) (required)
- [Setting the JMX Account Password on the Cisco StadiumVision Director Remote Server, page 37](#) (required)

Configuring the Cisco StadiumVision Director Server IP Address on the Remote Server

To configure the Cisco StadiumVision Director Server IP address on the remote server, complete the following steps:

-
- Step 1** From the TUI Network Settings menu, select the **Setup StadiumVision Director Address** option.
- Step 2** At the prompt, type the IP address (or host name) of the Cisco StadiumVision Director server and press **Enter**.
-  **Tip** To exit without configuring the IP address, do not type anything and simply press **Enter** to cancel.
-
- Step 3** Press any key to return to the Network Settings menu.
- Step 4** Return to the Main Menu.
- Step 5** Restart the Cisco StadiumVision Director Remote services by going to **StadiumVision Remote Server Administration > Restart StadiumVision Remote Software**.
-

Configuring the Global Credential on the Cisco StadiumVision Director Server

The global credential configuration on the Cisco StadiumVision Director Server determines how JMX account passwords are configured to support Management Dashboard monitoring of remote venues.



Note The global credential is *not* a user account for the remote server.

You can configure a common or unique password:

- [Configuring a Common Password on the Cisco StadiumVision Director Server for all Remote Servers, page 34](#)
- [Configuring a Unique Password on the Cisco StadiumVision Director Server for Each Remote Server, page 35](#)



Note Be sure to note the password that you configure on the Cisco StadiumVision Director server to be sure that you configure the same one on the applicable remote servers.

Configuring a Common Password on the Cisco StadiumVision Director Server for all Remote Servers

To configure a common password on the Cisco StadiumVision Director server for all remote servers, complete the following steps:

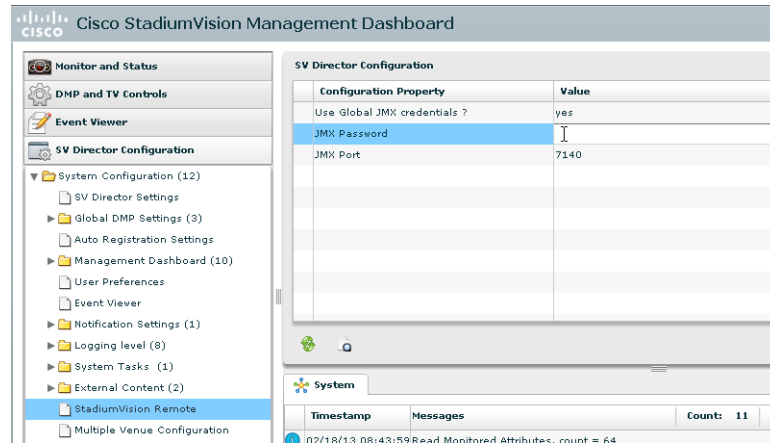
-
- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the **Management Dashboard**.
- Step 3** Click **SV Director Configuration > System Configuration > StadiumVision Remote**.
- Step 4** Confirm that the **Use Global JMX credentials?** property is set to **Yes**. This is the default.

- Step 5** In the JMX Password property value box, type the password (minimum of 6 characters) that you want to use for all remote servers (Figure 1).



Note This password will be auto-populated when you add new venues in the Control Panel.

Figure 1 Global JMX Account Password on the Cisco StadiumVision Director Server



- Step 6** Click the disk icon to save the configuration (Figure 2).

Figure 2 Save Changes Icon



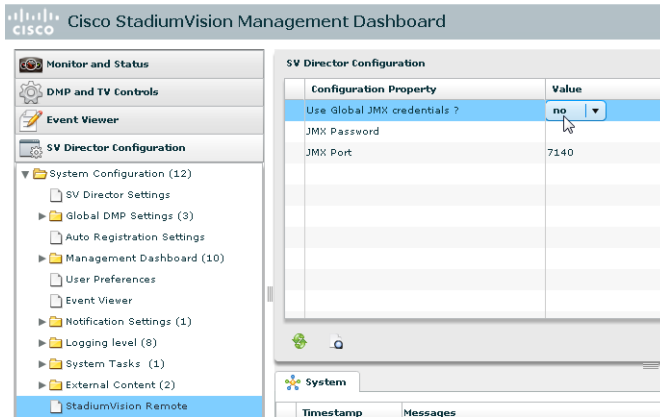
Configuring a Unique Password on the Cisco StadiumVision Director Server for Each Remote Server

To configure a unique password on the Cisco StadiumVision Director Server for each remote server, complete the following steps:

- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the **Management Dashboard**.
- Step 3** Click **SV Director Configuration > System Configuration > StadiumVision Remote**.

- Step 4** In the **Use Global JMX credentials?** property, click the arrow and select **No** in the drop-down box (Figure 3).

Figure 3 Disable the Global Credential on the Cisco StadiumVision Director Server



- Step 5** Click the Refresh Property Values icon.
- Step 6** Exit the Management Dashboard.
- Step 7** Go to **Control Panel > Setup > Venues**.



Note

To complete this configuration on the Cisco StadiumVision Director server, you must enable the system to support multiple venues and configure them in the Control Panel. For more information on venue configuration, see the “[Configuring Cisco StadiumVision Director for Multiple Venue Support](#)” module on page 41.

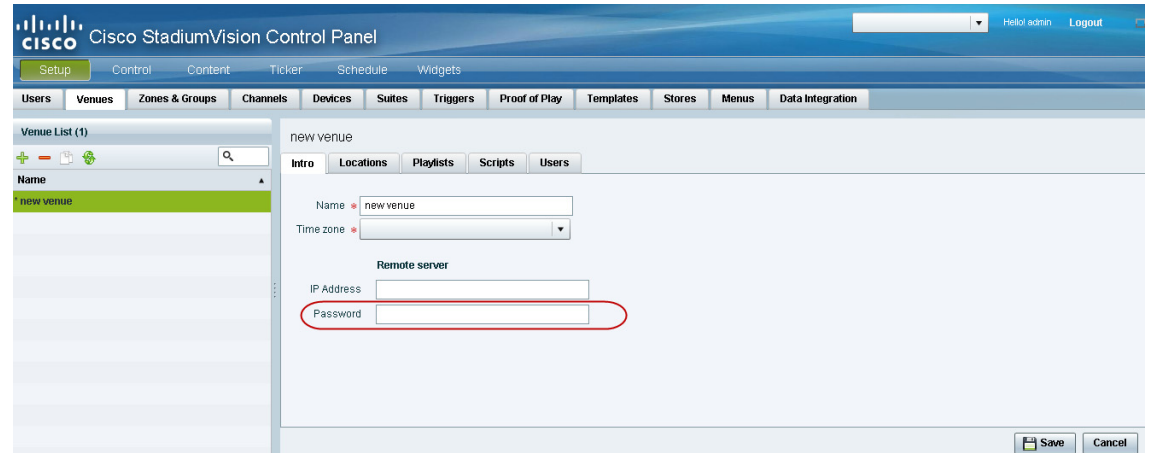
- Step 8** Add a new venue (or select an existing name from the Venue list) and specify the required Name, Time zone, and remote server IP address.
- Step 9** In the remote server Password box, type the unique password (minimum of 6 characters) for this venue (Figure 4).



Tip

Although you can always configure this option, it is only used when the “Use JMX Global credentials?” is set to No in the Management Dashboard.

Figure 4 Remote Server Password Configuration



Step 10 Click Save.

Setting the JMX Account Password on the Cisco StadiumVision Director Remote Server

To set up the capability for monitoring of the Cisco StadiumVision Director Remote server by the central Cisco StadiumVision Director server, the JMX account password on the remote server must be configured to match the configuration on the Cisco StadiumVision Director server.

To change the JMX account password on the Cisco StadiumVision Director Remote server, complete the following steps:

Step 1 Log into the TUI as installer on the remote server using a directly-connected console or SSH client. The TUI Main Menu is displayed.

Step 2 From the Main Menu, go to **System Accounts > Change JMX password**.



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

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

Step 3 At the new password prompt, type the password that you configured on the Cisco StadiumVision Director server for this venue and press **Enter**.



Note To cancel the password configuration, do not enter any characters when prompted and simply press **Enter**.

Step 4 At the confirm new password prompt, re-type the same password and press **Enter**.



Tip If the passwords do not match, you will be prompted to retry by typing Y, or N to cancel.

Step 5 Press any key to return to the System Accounts menu.



Tip If you have not yet configured the Admin user password, consider doing that now from the System Accounts menu before restarting the Cisco StadiumVision Remote software. The Admin user account must be configured to enable access to the Main Menu applications.

Step 6 Return to the Main Menu.

Step 7 Restart the Cisco StadiumVision Director Remote services by going to **StadiumVision Remote Server Administration > Restart StadiumVision Remote Software**.

Configuring the Admin Password

The admin system account password must be configured after you install Cisco StadiumVision Director Remote Release 3.2 for the first time. This credential is needed to authenticate access to the System State Report and Software Manager applications from the Main Menu.

To configure the admin password, complete the following steps:

Step 1 Log into the TUI as installer on the remote server using a directly-connected console or SSH client. The TUI Main Menu is displayed.

Step 2 From the Main Menu, go to **System Accounts > Change admin password**.



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

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

Step 3 At the new password prompt, type a password and press **Enter**.



Note To cancel the password configuration, do not enter any characters when prompted and simply press **Enter**.

Step 4 At the confirm new password prompt, re-type the same password and press **Enter**.



Tip If the passwords do not match, you will be prompted to retry by typing Y, or N to cancel.

Step 5 Press any key to return to the System Accounts menu.

Step 6 Return to the Main Menu.

Configuring the Date and Time Options on the Remote Server

When you install or upgrade the Cisco StadiumVision Director Remote servers, you need to configure the system date and time. This can be done in the TUI to either reference an NTP server (recommended), or manually set the date and time. You also need to configure the time zone.

For detailed information about how to configure the date and time options, see the [“Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers”](#) section on page 11 of the [“Configuring the Cisco StadiumVision Director Server System Settings”](#) module.

What To Do Next

After you have configured your Cisco StadiumVision Director remote servers, see the [“Configuring Cisco StadiumVision Director for Multiple Venue Support”](#) module on page 41 for information about how to set up Cisco StadiumVision Director for operation in multiple venues.



Configuring Cisco StadiumVision Director for Multiple Venue Support

First Published: April 21, 2014

Beginning in Cisco StadiumVision Director Release 3.1, a centralized server site can be deployed with multiple remote sites in a multi-venue architecture. This document is intended for Cisco StadiumVision Director administrators and describes how to enable and manage multiple venue support on Cisco StadiumVision Director Remote servers.

Contents

- [Prerequisites for Configuring Multiple Venue Support, page 41](#)
- [Restrictions for Configuring Multiple Venue Support, page 42](#)
- [Information About Configuring Multiple Venue Support, page 43](#)
- [How to Configure Multiple Venue Support, page 46](#)
- [How to Migrate Deployed Devices From a Single Venue to a Multiple Venue System, page 54](#)

Prerequisites for Configuring Multiple Venue Support

Before you configure Cisco StadiumVision Director remote servers for multiple venue support, be sure that the following requirements are met:

- You have read the [“Cisco StadiumVision Director Server Architecture” module on page 1](#).
- You understand the deployment of zones, groups and locations and the use of playlists and scripts in Cisco StadiumVision Director.
- The centralized Cisco StadiumVision Director server is installed with a minimum of Release 3.1.
- You have the following information for all installed Cisco StadiumVision Director Remote servers:
 - The names that you want to use for the remote sites.
 - The IP addresses for all installed Cisco StadiumVision Director Remote servers.



Note If you do not yet have the IP addresses for the remote server sites, you can continue to add the venues to Cisco StadiumVision Director without any IP address, and go back to configure the real IP addresses later.

- If you plan to override use of global remote server credentials, then you have the password that you want to use for each remote server. This will also require reconfiguration of these credentials using the Text Utility Interface (TUI) on the Cisco StadiumVision Director remote server. For more information, see the [“Configuring Cisco StadiumVision Director Remote Servers” module on page 31](#).
- You have planned the configuration for any new or changes to existing Locations. For existing Locations be sure that you are aware of current group/zone associations that will be disabled once you reassign an existing Location to a specific venue.

Restrictions for Configuring Multiple Venue Support

Before you configure Cisco StadiumVision Director remote servers for multiple venue support, be sure that you consider the following restrictions:

- Venue objects (such as locations, playlists, and scripts) are limited to a single-venue association, except for users who are assigned to the role of Venue Operator.



Caution

Once an existing Location is reassigned to a specific venue, any previous group/zone associations will be disabled and the Location will need to be reassigned to groups/zones.

- Only Venue Operators can be associated to one or more venues.
- Only certain areas of the Cisco StadiumVision Director software are *venue aware*, which means that certain roles can apply venue-specific scope of control using the venue selector. These areas include:
 - Control Panel > Control—Administrator, Event Operator, and Venue Operator
 - Control Panel > Content—Administrator and Content Manager
 - Control Panel > Schedule—Administrator and Content Manager
 - Management Dashboard—Administrator and Venue Operator



Note

The following areas of the Control Panel > Setup are not directly venue-aware using the venue selector, but objects defined there can have a venue-specific relationship:

- Users—You can define all Users under Control Panel > Setup, but you can only associate venues to Venue Operators under the Venues tab. Therefore, the Users interface is not venue aware.
- Zones & Groups—Zones and groups inherit their venue association through the Location. Locations are associated to venues under the Venues tab by the administrator.
- Triggers—Triggers can be applied to venue-associated scripts, but the Triggers interface itself is not venue aware, and all defined triggers in Cisco StadiumVision Director are global in scope.

- Playlists imported using the Media Planner Import API need to be manually assigned to venues after import into Cisco StadiumVision Director.

- Cisco StadiumVision Director does not support disabling of multiple venue support (set the “Multiple Venue Enabled?” property to false) after you have enabled it and associated objects.

Information About Configuring Multiple Venue Support

This section includes the following topics:

- [Cisco StadiumVision Director Remote Servers, page 43](#)
- [Role-Based Access Control for Hierarchical Management of Multiple Venues, page 43](#)
- [Understanding Venue Association, page 45](#)
- [Understanding Scripts and Staging Behavior in a Multi-Venue Environment, page 45](#)

Cisco StadiumVision Director Remote Servers

Cisco StadiumVision Director Remote Servers are installed at remote sites to provide a way of transferring venue-specific content in a distributed Cisco StadiumVision Director network environment, where primary management and control is performed on a centralized Cisco StadiumVision Director server.

The benefits of deploying remote servers include faster script staging due to WAN optimization, as well as multicast optimization which reduces the number of messages that remote DMPs receive.

The Cisco StadiumVision Director Remote servers support a limited set of administrative functions using a text utility interface (TUI) similar to the TUI support on Cisco StadiumVision Director. The remote servers are connected by a wide-area network (WAN) to the central Cisco StadiumVision Director server. The remote server connection to the central Cisco StadiumVision Director server is configured using the IP addresses of the servers. The IP address configuration must be completed on both the Cisco StadiumVision Director server, and on the Cisco StadiumVision Director Remote server using the remote server TUI.

The transmission of data is optimized over the WAN because the central Cisco StadiumVision Director server sends content only to the Cisco StadiumVision Director Remote server, rather than sending multiple transmissions to each remote DMP for that server. The remote server sends that content to each of the DMPs that it is configured to support on the local network.

For more information, see the [“Cisco StadiumVision Director Server Architecture” module on page 1](#).

Role-Based Access Control for Hierarchical Management of Multiple Venues

Cisco StadiumVision Director Release 3.1 introduces a new role of Venue Operator and adds new configuration management features to the Administrator role. All other legacy roles in Cisco StadiumVision Director retain their existing functionality.

For more information about user management and Role-Based Access Control (RBAC), see the [“User Management in Cisco StadiumVision Director” module on page 5](#).

Administrator

The Cisco StadiumVision Director administrator can perform all functions related to Cisco StadiumVision Director Remote server configuration and venue management.

Most of the configuration management for multiple venue support resides only with the Cisco StadiumVision Director administrator role, which includes the addition of the following functions:

- Enabling Cisco StadiumVision Director for multiple venue support.
- Creating venues in Cisco StadiumVision Director.
- Creating users with role of Venue Operator.
- Capability for associating any venues to users, locations, content, playlists, and scripts.

Content Manager

In a multi-venue architecture a Content Manager can perform all of the same functions as within a standard Cisco StadiumVision Director environment, with the addition of the following capabilities:

- Selecting the venue scope from the Content and Schedule screens in Control Panel.
- Importing content to be associated with one or more venues by using venue tags.
- Creating playlists and scripts to be associated with the currently selected venue scope or all venues.



Note

Content Managers can only create new objects with venue assignment based on the currently selected venue in the venue selector. To reassign an object to a different venue, the Content Manager must remove the object and add again.

Venue Operator

The Venue Operator is a new role introduced in Cisco StadiumVision Director Release 3.1 that is based on a subset of Event Operator and Help Desk roles, with the added functionality of venue-specific scope of control. The Venue Operator role supports the following capabilities:

- Changing the user password in Control Panel.
- Selecting venue scope for the venues for which permissions are granted.
- Viewing and monitoring information on the Management Dashboard with read-only access to the venues for which permissions are granted.
- Executing scripts and related state functions during an event at the venues for which permissions are granted.

Other Legacy RBAC Roles

Legacy RBAC roles (roles that were available in releases prior to Cisco StadiumVision Director Release 3.1) can perform all of the same functions as within earlier Cisco StadiumVision Director software releases.



Note

In a multi-venue architecture an Event Operator can perform all of the same functions as within a standard Cisco StadiumVision Director environment. The Event Operator role is not venue aware. To support venue-specific scope of control for scripts, use the new Venue Operator role.

Understanding Venue Association

A centralized Cisco StadiumVision Director site with multiple remote sites (venues) supports the following functionality:

- Association of venues to Users, Locations, Playlists, and Scripts (referred to collectively as *venue objects*).
- Inheritance of venue association from Locations for Groups, Zones, and Luxury Suites.



Tip

You can use the Bulk Administration Tool (BAT) to associate multiple locations to a venue.

Understanding Scripts and Staging Behavior in a Multi-Venue Environment

This section provides information about scripts that you should be aware of when implementing them in a multi-venue environment.

Script Best Practices

When configuring scripts in a multi-venue environment, consider the following best practices:

- Deploy remote servers to achieve faster script staging due to WAN optimization.
- Configure scripts to control only a single venue.
- When creating venue-specific scripts, use the following process:
 1. Create the script first without any actions—Name it and save it.
 2. Assign the script to the venue.
 3. Edit the script to assign it to zones/groups.
 4. Use playlists that belong to the same venue.
 5. Edit the script to further define states.
- Be sure that scripts that are intended to run at a remote site are not also being run on any non-site DMPs.
- For optimal operation, avoid running multiple event scripts to the same DMPs at a site.



Note

If you move a script assignment from one venue to another, be aware that the zones/groups/playlists might still be associated with the old venue until they are manually reassigned. If a script is part of one venue and zones/groups/playlists are part of another venue, then the script will not start.

Script Staging Behavior

In Cisco StadiumVision Director, script staging is always serialized. In the case of two venues where each is deployed with a different remote server, then when scripts are staged for each venue, one venue's script will be staged before the other. The scripts will not start at the same time.

In the case of content replacement, content staging happens right away. If current staging is going on, content replacement staging will go into the queue. The DMP will play old content until confirmation of successful staging occurs, so there could be some time delay.

How to Configure Multiple Venue Support

This section includes the following tasks:

- [Enabling Multiple Venue Support in Cisco StadiumVision Director, page 46](#) (required)
- [Adding Venues to Cisco StadiumVision Director, page 47](#) (required)
- [Associating Venues with Cisco StadiumVision Director Objects, page 48](#) (required)
- [Removing Venues From Cisco StadiumVision Director, page 51](#) (optional)
- [Selecting Venue Scope, page 52](#) (optional)
- [Monitoring Venues From the Management Dashboard, page 53](#) (optional)

Enabling Multiple Venue Support in Cisco StadiumVision Director

By default, Cisco StadiumVision Director is not configured for multi-venue deployment. To support Cisco StadiumVision Director with a centralized server and remote sites, you must configure the Multiple Venue Configuration property, which will set the corresponding registry key. Once this registry key is set, it will be preserved during an upgrade.



Caution

Cisco StadiumVision Director does not support disabling of multiple venue support (set the “Multiple Venue Enabled?” property to false) after you have previously enabled it and associated objects. In other words, do not toggle between enabling multiple venue support and disabling it.

To enable multiple venue support in Cisco StadiumVision Director, complete the following tasks:

- Step 1** Log into Cisco StadiumVision Director as an administrator.
- Step 2** From the main menu, click **Management Dashboard**.
- Step 3** Go to **SV Director Configuration > Multiple Venue Configuration**.
- Step 4** Set the **Multiple Venue Enabled?** property value to “true.”
- Step 5** Click the Refresh icon to update property values.

The multiple venue management functions are enabled in Cisco StadiumVision Director and the registry key named “**multiVenueDeployment**.”

- Step 6** Click **Save**.
- Step 7** Confirm that the “**Choose venue:**” control appears in the upper right corner of the Management Dashboard window.



- Step 8** Go to **Control Panel > Setup** and confirm that the Venues tab is available.

**Tip**

If you already had the Control Panel open before enabling multiple venue support, refresh the browser to display the Venues tab.

Adding Venues to Cisco StadiumVision Director

After you enable multiple venue support in Cisco StadiumVision Director, you can add remote sites as venues in the Control Panel.

To add venues in Cisco StadiumVision Director, complete the following tasks:

- Step 1** Log into Cisco StadiumVision Director as an administrator.
- Step 2** From the main menu, click **Control Panel**.
- Step 3** Go to **Setup > Venues**.
- Step 4** Click the plus (+) icon.

The Intro panel displays the remote server configuration options ([Figure 1](#)).

Figure 1 New Venue Intro Panel

- Step 5** (Required) In the Name box, type a unique and identifiable name for the venue. “new venue” is the default.
- Step 6** (Required) In the Time zone box, click the arrow to open the drop-down box and select the time zone for the remote site.

**Note**

This option is informational only and for proof-of-play reporting. The actual time zone for the venue is configured from the TUI on the remote server. For more information, see the [“Restrictions for Configuring Multiple Venue Support”](#) section on page 42.

- Step 7** (Required only when remote servers are deployed) In the IP address box, type the IPv4 address of the Cisco StadiumVision Director Remote server.

**Caution**

If you do not know the IP address of the remote server, do not type an invalid IP address as a placeholder for the real IP address due to certain backend processes that are started once an IP address is entered and that can interfere with normal operation. Simply leave the IP address box empty until you can confirm the valid IP address.

Step 8

(Optional) To specify a unique password for the remote server to enable monitoring from the Management Dashboard, type a Password.

**Tip**

When global credentials are configured, this field is automatically populated with the global password that is configured in the Cisco StadiumVision Director Management Dashboard. Before you modify this password, be sure that you understand the use and requirements for this password. For more information, see the [“Configuring Connectivity to the Cisco StadiumVision Director Server” section on page 33](#).

Associating Venues with Cisco StadiumVision Director Objects

You can associate venues with Locations, Playlists, Scripts, and Users in Cisco StadiumVision Director. Only the administrator can perform associations for all of these objects for all venues using the Venues tab in the Control Panel Setup screen.

After the initial multiple venue configuration and association is completed by the Cisco StadiumVision Director administrator, other roles (Content Manager and Venue Operator) can use the venue selector in Cisco StadiumVision Director for their authorized functional areas of the interface to select their venue scope of control. Any related tasks will be based on that selected venue scope (All Venues or a specific venue).

This section includes the following topics:

- [Guidelines for Associating Venues, page 48](#)
- [Venue Association Procedure, page 49](#)
- [Troubleshooting Venue Association Conflicts, page 50](#)

Guidelines for Associating Venues

Before you associate venues in Cisco StadiumVision Director, be sure that you understand the following guidelines:

- Each object is limited to a single-venue association, except for users.
- Only users with the assigned role of Venue Operator can be assigned to one or more venues by the administrator.
- Only the following roles can see the venue selector in the Cisco StadiumVision Director interface and use it to select the venue scope of control for their authorized areas:
 - Administrator
 - Content Manager
 - Event Operator

- Venue Operator



Note SSC users and the SSC portal are not venue aware. There is no venue selector available in SSC.



Caution

If a location is already in a group/zone configuration, it will be forcibly removed from those groups and zones when you either associate or disassociate the location from a venue. Scripts might fail to start on those endpoints because they are not part of the group anymore.

- Refer to the [“Script Best Practices” section on page 45](#) for guidelines on script creation and association.

Venue Association Procedure

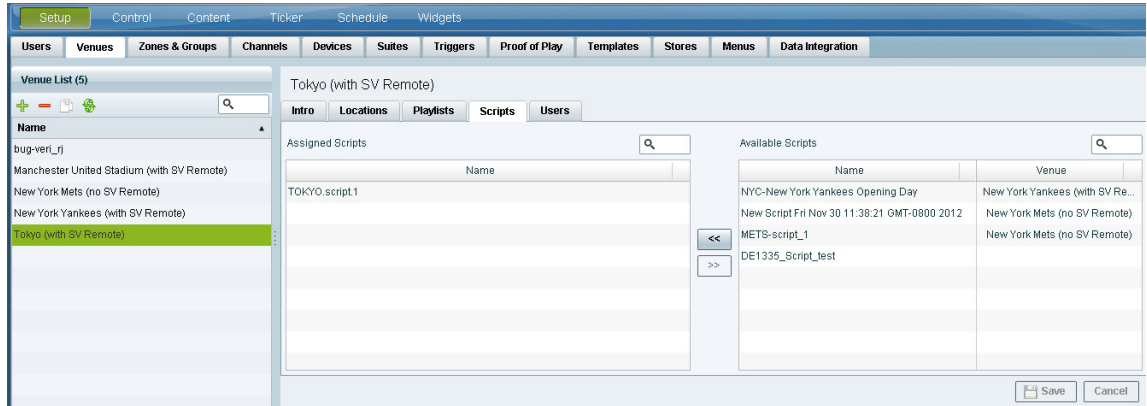
To associate venues with Cisco StadiumVision Director objects, complete the following steps:

- Step 1** Log into Cisco StadiumVision Director as an administrator.
- Step 2** From the main menu, click **Control Panel**.
- Step 3** Go to **Setup > Venues**.
- Step 4** In the Venue list, click the name of the venue that you want to associate.
- Step 5** Do the following to assign object types to the selected venue:
 - Click **Locations, Playlists, Scripts, or Users**.
 - In the “Available” box, select the name of the location, playlist, script, or user that you want to associate.



Tip You can multi-select objects. Click the checkbox and Ctrl+Click to select additional objects. In releases prior to Release 3.1 SP1, multi-selection was limited to Locations objects only.

- Click the << button.
The object name is added to the Assigned box.
- Repeat from Step [a.](#) or Step [b.](#) for as many objects as you need to associate.

Figure 2 Associate Scripts to Venue Example

Step 6 (Optional) To remove an assigned object, select the name of the object in the “Assigned” box and click the >> button.

Step 7 When associations are complete, click **Save**.

Troubleshooting Venue Association Conflicts

When you attempt to associate objects to venues, certain conditions can cause the system to provide you with a warning about objects that are not optimally configured to be associated to the venue, such as a Location already being associated to a group or zone in another venue. The warning message identifies the objects, which allows you to do one of two things:

- Click **Close** to go back to the Cisco StadiumVision Director configuration to confirm that the object best follows venue association guidelines and note or change the configuration.
- Click **Force** to permit the system to attempt to make the requested association for the objects in conflict.



Note

The Force button might not work for all associations. It is important to understand that an attempt is made by the system to force the specified user action but several factors influence its success. For best results, read the error message and see what objects are identified as being in conflict with the requested action and take corrective steps to avoid the conflict within Cisco StadiumVision Director.

[Figure 3](#) shows an example of an error message that can appear when you attempt to associate venue objects and there are conflicts within the Cisco StadiumVision Director configuration. Any other objects not in conflict will be associated to the venue as requested.

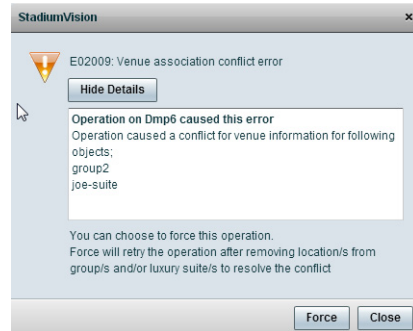
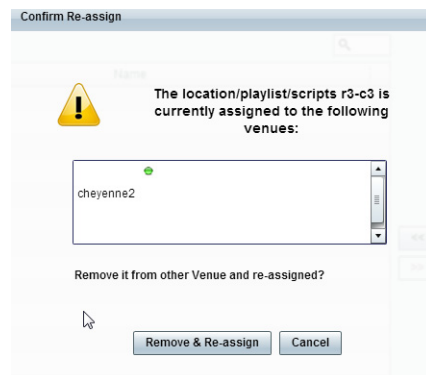
Figure 3 Venue Association Conflict Message Example

Figure 4 shows an example of a venue assignment conflict message where the location, playlist, or script that you tried to assign to a venue is identified as already assigned to another venue. The original venue assignment is displayed in the message (“Cheyenne2” in this example). You can do one of two things:

- Click **Remove & Re-assign** to proceed with the new venue assignment and remove the specified object from its current venue assignment.
- Click **Cancel** to retain the original venue assignment and return to Cisco StadiumVision Director.

Figure 4 Confirm Object Reassignment Message Example

Removing Venues From Cisco StadiumVision Director

To remove a venue from Cisco StadiumVision Director, complete the following steps:

-
- Step 1** Log into Cisco StadiumVision Director as an administrator.
 - Step 2** From the main menu, click **Control Panel**.
 - Step 3** Go to **Setup > Venues**.
 - Step 4** Dissociate all objects that are linked to the venue that you want to remove.
 - Step 5** In the Venue List box, select the venue that you want to remove.
 - Step 6** Click the delete icon (red dash).
-

Selecting Venue Scope

You can select venue scope in the Control Panel and in the Management Dashboard. However only certain areas of the Control Panel interface are venue aware. Once you have enabled the software for multiple venue support and added new venues in the Control Panel, you can use the venue selector in those areas that are venue aware.

Venue status is indicated in the venue selector using a radio button that is colored red to indicate that the venue is disabled and green to show that the venue is online.



Caution

Take note that the venue selector will show the last venue that you selected, but the scope will not be limited to the selected venue if you are not in a venue-aware area of the interface. The global scope will apply (All Venues). For more information, see the [“Understanding Venue Association”](#) section on page 45.

To select venue scope, complete the following tasks:

- Step 1** Log into Cisco StadiumVision Director as an administrator, content manager, or venue operator.
- Step 2** Go to the Control Panel (or Management Dashboard, as allowed by your role).
- Step 3** At the top of the window, look for the venue selector drop-down box.

Figure 5 shows an example of the venue selector in the Cisco StadiumVision Control Panel.

Figure 5 Venue Selector Drop-Down Box in the Control Panel



- Step 4** Do one of the following:
 - To apply the scope of operation to a specific venue, select the name of the venue in the drop-down box.
 - To apply the scope of operation to all venues, select All Venues.
- Step 5** Continue to the Control Panel area that you want to configure.

Monitoring Venues From the Management Dashboard

You can monitor the status of remote devices for selected venues from the Management Dashboard.

The red, green, or gray LED to the left of venue names in the venue selector represents the status of the Cisco StadiumVision Director remote server, but not whether the DMPs in the venue are accessible.

You also can see if there are connection issues for the Cisco StadiumVision Director remote server **Monitor and Status > Services** area of the Management Dashboard.

Traffic monitoring of remote DMPs in the Management Dashboard is performed using unicast messaging, so multicast optimization does not apply nor interfere with the multicast optimization for the Cisco StadiumVision Director Remote server processing.

To monitor venues from the Management Dashboard, complete the following steps:

- Step 1** Log into the Cisco StadiumVision Director server as an administrator.
- Step 2** Go to the Management Dashboard.
- Step 3** At the top of the window, select the venue whose devices you want to monitor.
- Step 4** Click **Monitor and Status**.
- Step 5** Select the area that you want to get information about. Go to **Services** to see the status of the Cisco StadiumVision Director remote server connection.

Figure 6 shows information about zones in the Tokyo venue.

Figure 6 Monitoring Devices for a Specific Venue in the Management Dashboard

The screenshot displays the Cisco StadiumVision Management Dashboard interface. The main content area is titled 'Monitor and Status' and shows a 'Device List' table with the following data:

Location	IP Address	MAC Address	Model	Firmware	Checked At
Off Rov_R-Cat2_C3R4	10.194.171.151	00:0F:44:01:5c:b5	DMP-4310	5.4	02/19/13 03:33:03 Af
Off Rov_R-Cat2_C1R4	10.194.171.154	00:0F:44:01:5d:a8	DMP-4310	5.4	02/19/13 03:33:03 Af
Off Rov_R-Cat2_C2R4	10.194.171.152	00:0F:44:01:5e:b1	DMP-4310	5.4	02/19/13 03:33:03 Af

Below the table, there are sections for 'Status Details' (DMP Status, TV Status), 'Utilization', 'Events', 'Uptime', and 'MIB Variables'. On the right side, there is a 'DMP Summary Feb 18, 6:23 PM' widget showing an overall status of 3 total devices (0 Critical, 3 Normal, 0 SD problems, 0 Flash problems, 0 Unreachable). Below that is a 'Service Alerts' widget showing a warning for 'SVD for Manchester United Stadium (with SV Remote)' and a green checkmark for 'Cisco POS Server 3'.

How to Migrate Deployed Devices From a Single Venue to a Multiple Venue System

This section describes the best practices for migrating a large number of deployed devices and locations from a single venue to a multiple venue system using the Bulk Administration Tool (BAT).

For more information about the tasks referenced here for exporting, editing, and importing TSV files using BAT, see the *Cisco StadiumVision Director Bulk Administration Tool* guide.

This section includes the following tasks:

- [Prerequisites, page 54](#) (required)
- [Exporting a Device List for the Original System Configuration, page 55](#) (required)
- [Creating New Venues, page 56](#) (required)
- [Removing All Locations From Existing Groups, page 56](#) (required)
- [Removing Locations From Existing Suites, page 56](#) (only required if DMPs are in suites)
- [Associating Initial Locations to Venues, page 57](#) (required)
- [Completing Venue-Specific Information and Association of Locations Using BAT, page 57](#) (required)
- [Populating Group Information in the New Device List, page 58](#) (required)

Prerequisites

Before you migrate deployed devices from Cisco StadiumVision Director, be sure that the following requirements are met:



Caution

Cisco StadiumVision Director does not support disabling of multiple venue support (set the “Multiple Venue Enabled?” property to false) after you have previously enabled it and associated objects. In other words, do not toggle between enabling multiple venue support and disabling it.

- You must be sure that the following object types are configured to be unique per venue: Groups, zones, locations, scripts, suites, and playlists.
- A recommended best practice is to use a naming convention that easily identifies the venue to which an object is associated by assigning a prefix to the object name. This can make it easier to find and track related objects.

For example, to name scripts, playlists, and locations that belong to a venue called “WEST-SIDE-VENUE” you could use the prefix “WE” such as WE-Script1, WE-Script2, WE-Playlist1, WE-Location1, and so on.

- If you have existing DMPs in a group that are targeted to be in multiple venues, they need to be split up so that each group contains DMPs *only for a single venue*.

For example, if there is a group (ALL-DMPs) that consists of all of the DMPs in Cisco StadiumVision Director, then the group needs to be sub-divided into smaller groups of DMPs by venue, such as “ALL-DMPs-Venue1,” “All-DMPs-Venue2,” “ALL-DMPs-No-Venue” and so on.

This same rule applies to other objects like zones, scripts, suites, and locations. If any of these have objects that are targeted to be in different venues or to be global (that is, objects that are not part of any venues) then they need to be sub-divided on a per-venue basis.

- (For DMPs in suites only) All suites must have a suite controller attached.

**Tip**

You can easily verify whether or not a controller is defined for a suite by looking at the original exported device list (See [“Exporting a Device List for the Original System Configuration” section on page 55.](#)) If Column N (Suite Name) has a value and Column M (Suite Control Type) does not have a corresponding value in the same row, then you know that the Suite named in Column N does not have a device list attached to it.

If a suite controller is not attached, then you must assign a suite controller to it. If there are not any available suite controllers, you can create an artificial one and assign it to the suite. These fake controllers can be deleted after the migration process has completed successfully:

1. Go to **Control Panel > Setup > Devices > IP Phones.**
2. Create artificial IP phone entries with fake, non-pingable IP addresses.
3. Go to **Suites.**
4. Select the suite that does not have a suite controller.
5. Click the **Phone & Remote** tab on the right panel that has suite properties.
6. Assign the artificial IP phone that you created to the suite by selecting the checkbox.

Exporting a Device List for the Original System Configuration

This task should be done to preserve initial single venue system configuration information and to aid re-population of that information to the new multi-venue device list created later.

For more information, see the “Exporting and Downloading a TSV File for Locations and DMPs” topic in the [Cisco StadiumVision Director Bulk Administration Tool](#) guide.

To export a device list for the original system configuration, complete the following steps:

-
- Step 1** Go to **Control Panel > Setup > Devices > Locations & DMPs.**
- Step 2** Click **Export.**
- Step 3** When the Export box displays, click **Download.**
- Step 4** When the “Select location for download” window appears, type the name of the .txt file that you want to save, or accept the default name and click **Save.**
- Step 5** **Be sure to save a master copy** of the originally exported device list.
-

Creating New Venues

This task describes how to create a new venue with basic information, which will be further updated in a later task using BAT.

To create new venues, complete the following steps:

-
- Step 1** Go to **Control Panel > Setup > Venues**.
 - Step 2** Specify the Name and Timezone for the venue.
 - Step 3** Click **Save**.
-

Removing All Locations From Existing Groups



Note

Before you remove locations from existing groups, be sure that you have completed the requirements in the Prerequisites section to place all objects in unique groups per venue.

Before associating Locations to the new venues, you need to remove them from existing groups.

To remove all Locations from Groups, complete the following steps:

-
- Step 1** Go to **Control Panel > Setup > Zones & Groups > Location<->Group**.
 - Step 2** Click **Groups**.
 - Step 3** Select an individual group.
 - Step 4** In the Locations panel on the right, select all Locations for the selected group.



Tip

You can use Ctrl+Click or Shift+Click key sequences to multi-select the Locations.

-
- Step 5** Click **Remove From Groups**.
 - Step 6** Repeat from [Step 3](#) for all groups that need locations removed.
 - Step 7** Refresh the browser to reload the UI so that the changes are updated.
-

Removing Locations From Existing Suites

To associate locations to a venue, they need to be removed from any existing suites. These locations will be added back to the configuration using the BAT tool using the original Device list that was exported.

To remove Locations from existing suites, complete the following steps:

-
- Step 1** Go to **Control Panel > Setup > Suites**.

- Step 2** Select any suites that contain locations that are targeted to be moved to venues.
- Step 3** Select each location and click the red '-' button on the top to delete it from the suite.



Tip Click the red '-' button rapidly to delete DMPs quickly from the suite.

- Step 4** After all DMPs are removed from the suite, be sure to click **Save**.
- Step 5** Repeat from [Step 2](#) for each suite from which you need to remove locations.

Associating Initial Locations to Venues


To establish the venue-specific fields when you export the new multi-venue device list, you need to associate at least one Location to each new venue that you created.

For more information, see the [Associating Venues with Cisco StadiumVision Director Objects, page 48](#).

Completing Venue-Specific Information and Association of Locations Using BAT

This task is performed to more easily complete configuration of any remaining venue-specific information and association of locations using BAT.

To complete venue-specific information and association of Locations, complete the following steps:

- Step 1** Export a new device list.
- After the association of at least one Location per venue, the newly exported device list file now contains the venue-specific field entries that can now be more easily populated with the remaining required configuration information.
- The venue-specific field entries in the BAT file are:
- Venue Name
 - Venue Timezone
 - Venue Remote Server IP
 - Venue JMX Password—The JMX password is saved in the venue information only when the system is disabled for global credentials.
-  **Note** The Venue JMX Username field is always ignored.
- Step 2** To complete association of Locations to venues, edit the TSV file using a spreadsheet application such as Microsoft Excel to:
- a. Complete the venue-specific information.
 - a. Copy (or auto-fill) to add rows for new Locations that you want to add to the venues.
- Step 3** Import the device list.

For more information, see the “Importing a TSV File” topic in the *Cisco StadiumVision Director Bulk Administration Tool* guide.

- Step 4** Go to **Control Panel > Setup > Venues** and confirm that the Locations are properly associated to their venues.
-

Populating Group Information in the New Device List

This step allows you to more easily re-populate the original system’s Group information to the new multi-venue device list.

To populate Group and other information from the original device list, complete the following steps:

- Step 1** Export a new device list and open the file in your spreadsheet application.
- Step 2** Excluding the first row, select all rows and columns.
- Step 3** Sort the spreadsheet by the Name field (column E).
- Step 4** Obtain the copy of the master device list that you exported in [Step 1](#). Also sort the master spreadsheet by the Name field.
- Step 5** From the original master file, copy the columns that have Group information (Z, AA, AB, AC, and so on) and paste them appropriately into your new device list.



Tip When working with certain rows and columns in Microsoft Excel, the hide/unhide columns or rows feature and freeze/unfreeze feature can be used to efficiently do this job. For information about these features, see the Microsoft support site.

- Step 6** From the original master file, also copy columns that have Suites and Suite Controller information (J–Y).
- Step 7** Save the new device list.
- Step 8** Import the new device list into Cisco StadiumVision Director.
- Step 9** After the import is complete, refresh the browser.
-



StadiumVision



PART 3

Cisco StadiumVision Director Account Management



System Accounts on the Cisco StadiumVision Director Servers

First Published: April 21, 2014

This module describes the default system accounts implemented by Cisco StadiumVision Director and Cisco StadiumVision Director Remote for access and control of certain server functions. Aside from the admin account, these system accounts are generally separate from the user accounts that secure access to the Cisco StadiumVision Director feature configuration and operation.

In addition, only a few of these accounts are intended for general modification after installation of the server. Other system accounts are reserved for special services or technical support and should not be modified unless you are instructed to do so, or you otherwise understand the impact to your server installation.

For information about user accounts and Role-Based Access Control (RBAC) in Cisco StadiumVision Director, see the [“User Management in Cisco StadiumVision Director” module on page 5](#).

Information About System Accounts

All of the system accounts are automatically implemented upon installation of the Cisco StadiumVision software.

This section provides an overview of the default system accounts in Cisco StadiumVision:

- [Common System Accounts, page 2](#)
- [Other System Accounts, page 3](#)

Common System Accounts

Table 1 describes the common system accounts in Cisco StadiumVision Director and Cisco StadiumVision Director Remote that are intended for you to modify after deployment of your server, and on which server platform they are supported. These common system accounts are automatically implemented upon installation of the Cisco StadiumVision software.

Table 1 Description of Common System Accounts

Account	Purpose	Server Platform
Admin	<p>Cisco StadiumVision Director</p> <p>Account that provides access to the administrator RBAC functions in the Cisco StadiumVision Director user interface(UI).¹ It is automatically implemented upon installation of the Cisco StadiumVision Director software.</p> <p>The username is: admin</p> <p>The default password is: admin</p> <p>Note Using the Text Utility Interface (TUI) to change the admin account password allows an installer to recover access to the Cisco StadiumVision Director UI. The password for the admin user account can also be changed in the Cisco StadiumVision Director Control Panel Setup or by setting the option to force a password change upon initial login with the admin account.</p> <p>Cisco StadiumVision Director Remote</p> <p>Account that provides access to the applications on the Cisco StadiumVision Director Remote Main Menu, such as System State Reports and the Software Manager.</p> <p>The username is: admin</p> <p>There is not a default password. You must configure the password after the Release 3.2 software is first installed.</p>	<p>Cisco StadiumVision Director</p> <p>Cisco StadiumVision Director Remote</p>

Table 1 Description of Common System Accounts

Account	Purpose	Server Platform
Installer	Account that provides access to the TUI using a directly-connected console or SSH client. The username is: installer The default password is: cisco!123 . ²	Cisco StadiumVision Director Cisco StadiumVision Director Remote
JMX	Global account that implements monitoring services of Cisco StadiumVision Director Remote servers in the Management Dashboard of the centralized Cisco StadiumVision Director server. There is no default password. The password must be configured on both the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers. Note To support monitoring, the Cisco StadiumVision Director Remote server JMX account must match what is configured in the centralized Cisco StadiumVision Director server. ³	Cisco StadiumVision Director Cisco StadiumVision Director Remote

1. For more information on the administrator role in Cisco StadiumVision Director, see the “[User Management in Cisco StadiumVision Director](#)” module on page 5.
2. For more information about the TUI, see the “[Cisco StadiumVision Director Server Text Utility Interface](#)” module on page 3
3. For more information, see the “[Configuring Cisco StadiumVision Director Remote Servers](#)” module on page 31.

Other System Accounts

Table 2 describes some other default system accounts that are reserved for use in Cisco StadiumVision troubleshooting or other specialized access.

Table 2 Description of Reserved System Accounts

Account	Purpose	Server Platform
admgr	Reserved for use by special agreement with Cisco Systems to support the Media Planner Import API. ¹	Cisco StadiumVision Director
MySQL	Reserved for internal use only to access the MySQL database account.	Cisco StadiumVision Director
TAC user	Reserved for troubleshooting with remote shell access. This account should remain disabled and only activated when instructed by Cisco Technical Support for troubleshooting.	Cisco StadiumVision Director Cisco StadiumVision Director Remote

1. For more information about the Media Planner Import API and other API support in Cisco StadiumVision Director, see the *Release Notes for Cisco StadiumVision Director Release 3.1*.

How to Change System Account Passwords

You can change system account passwords from the defaults on the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers using the TUI.

**Tip**

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

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

To change system account passwords, complete the following steps:

-
- Step 1** On the Cisco StadiumVision Director or Cisco StadiumVision Director Remote server, log into the TUI by doing the following:
- a. Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the primary Cisco StadiumVision Director server using the IP address for your server.
 - b. When the login prompt appears, enter the **installer** userid followed by the installer password at the password prompt.
- Step 2** From the Main Menu, go to **System Accounts**.
- Step 3** Select the system account whose password you want to change.
- Step 4** At the prompt, type the new password.
- Step 5** When prompted to confirm, retype the password.
- Step 6** Press any key to return to the System Accounts menu.
- Step 7** Return to the Main Menu and exit the TUI.
-



User Management in Cisco StadiumVision Director

First Published: April 21, 2014

Cisco StadiumVision Director deployments normally have a team of people who are responsible for different aspects of the site setup and event operation. For example, in addition to a system administrator, there is usually an event operator, a content manager, and a technical support person, among other personnel. Each person has different skills and needs for working with the Cisco StadiumVision Director software.

The Cisco StadiumVision Director software implements Role-Based Access Control (RBAC) to control permissions and user access to only the portions of the system for which they are trained and authorized to use. More than one user can be assigned to the same role in the software. However, only a single role can be assigned to each username.

Information About User Management

This section includes the following topics:

- [Administrator Role Overview, page 5](#)
- [RBAC Roles Overview, page 6](#)
- [Access Summary by Role, page 7](#)

Administrator Role Overview

The Administrator role has unrestricted access to the Cisco StadiumVision Director software, and is the only role that can add users and assign RBAC privileges to them. The Administrator role is pre-configured in Cisco StadiumVision Director and cannot be deleted. However, you can change the password.

The Cisco StadiumVision administrator is the person who is responsible for deploying the Cisco StadiumVision solution throughout the venue.

The administrator has sufficient permissions to do the following functions:

- Installing, upgrading, backing up, and restoring Cisco StadiumVision Director servers.
- Configuring multiple venue support and Cisco StadiumVision Director Remote servers.

- Associating objects to venues.
- Creating additional users and assigning roles.
- Adding devices to Cisco StadiumVision Director.
- Staging content.
- Configuring the channel lineup (Content Managers can also configure this area).
- Configuring local control areas such as luxury suites, back offices, and bars.
- Configuring Point of Sale (POS).
- Generating Proof of Play (PoP).
- Configuring the Dynamic Menu Board application.
- Configuring the TV Off custom application.

RBAC Roles Overview

Table 1 provides an overview of the roles that can be assigned by the Administrator in Cisco StadiumVision Director.

Table 1 Cisco StadiumVision Director Roles

Role	Description
Concessionaire	Concessionaires have access only to the Dynamic Menu Board application, which allows modification of certain text-based and graphics items, and the background graphic on menus. All content uploaded by the concessionaire is available to all users that have sufficient permissions based on the roles assigned to them. The concessionaire role does not have permissions in the Control Panel or the Management Dashboard, and they can only see the DMB themes that they create.
Content Manager	Content Managers are responsible for uploading content and ads provided by the creative services team. They create event scripts so that the correct content displays in the proper area of the venue and the proper area of the TV screen according to the specified schedule. The content manager role has permissions in Cisco StadiumVision Director to configure event states/scripts, zones, groups, screen templates, playlists, and tickers. Content managers can also assign gadgets for custom menus and create playlists for those menus.
Event Operator	Event Operators run the Cisco StadiumVision Director event scripts during an event. The event operator role has permissions to start and stop scripts and modify their states. They can change the transition of an event state from time-based to manual, move an event into one of the three ad hoc states (Inside Emergency, Outside Emergency, or Delay), and approve ticker content (legacy version). Additionally, the event operator keeps track of which break states have played and is responsible for performing the pre-game walk-through.
Facility Operator	Facility Operators have access only to the TV Off application. The facility operator must access this application directly using the <code>http://ipaddress:9090/web/sv/home</code> , where <i>ipaddress</i> is the IP Address of the Cisco StadiumVision Director server.

Table 1 Cisco StadiumVision Director Roles

Role	Description
Help Desk	Help Desk users have read-only permissions to view and monitor information on the Management Dashboard. This role does not have permissions in the Control Panel, except to change their own password. For more information on the tasks performed by the help desk role, see the StadiumVision Director Management Dashboard Guide.
SSC User	(Release 3.0 and later). Self-Service Content (SSC) users are given access only to the SSC portal area of Cisco StadiumVision Director, where they can upload content into albums and publish that content to authorized TVs. This user-specific workspace contains only the content explicitly uploaded by that user, and only that user can see the content. The administrator authorizes each SSC user for the suites and TVs on which they can display their content.
Support	Support users are responsible for first-level technical support. They have limited access to the Management Dashboard to monitor DMP status, troubleshoot, and manage the DMPs on the Cisco StadiumVision network. The support role does not have permissions in the Control Panel, except to change their own password. For more information on the tasks performed by the help desk role, see the StadiumVision Director Management Dashboard Guide.
Venue Operator	(Release 3.1 and later). Venue Operators have script control only, and only for venues authorized by the administrator for that user. In the Management Dashboard, venue operators can view and monitor information on the Management Dashboard with read-only access to the venues for which permissions are granted.

Access Summary by Role

Table 2 provides a summary of the areas of access in the Cisco StadiumVision Director software by each user role.



Note

“Yes” indicates that the user role has access to the corresponding functional area, and “—” means that the role does not have authorization there.

Table 2 Role Access Summary by Functional Area of Cisco StadiumVision Director

Functional Area	Admin	Concessionaire	Content Manager	Event Operator	Facility Operator	Help Desk	SSC User	Support	Venue Operator
Control Panel/ Setup									
Channels	Yes	—	Yes	—	—	—	—	—	—
Data Integration	Yes	—	Yes	—	—	—	—	—	—
Devices	Yes	—	—	—	—	—	—	—	—
Menus	Yes	—	Yes	—	—	—	—	—	—
My Profile	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Proof of Play	Yes	—	—	—	—	—	—	—	—

Table 2 Role Access Summary by Functional Area of Cisco StadiumVision Director (continued)

Functional Area	Admin	Concessionaire	Content Manager	Event Operator	Facility Operator	Help Desk	SSC User	Support	Venue Operator
Stores	Yes	—	—	—	—	—	—	—	—
Suites	Yes	—	—	—	—	—	—	Limited ¹	—
Templates	Yes	—	Yes	—	—	—	—	—	—
Triggers	Yes	—	—	—	—	—	—	—	—
Users	Yes	—	—	—	—	—	—	—	—
Venues	Yes	—	—	—	—	—	—	—	—
Zones & Groups	Yes	—	Yes	Yes	—	—	—	—	—
Control Panel									
Content	Yes	—	Yes	—	—	—	—	—	—
Control	Yes	—	—	Yes	—	—	—	—	Limited ²
Control/Staging	Yes	—	—	Yes	—	—	—	—	—
Schedule	Yes	—	Yes	—	—	—	—	—	—
Ticker (legacy)	Yes	—	Yes	Yes	—	—	—	—	—
Widgets	Yes	—	Yes	—	—	—	—	—	—
Dynamic Menu Boards	Yes	Yes	Yes	—	—	—	—	—	—
Management Dashboard	Yes	—	—	—	—	Limited ³	—	Yes ⁴	Limited ⁵
System State Reports	Yes	—	—	—	—	—	—	—	—
TV Off Application	Yes	—	—	—	Yes	—	—	—	—
SSC Portal ⁶	—	—	—	—	—	—	Yes	—	—

1. Support users can set up TV control PINs and channel guides for suites.
2. Venue operators have script control only, and only for venues authorized by the administrator for that user.
3. Help Desk users can issue Get Status, Ping, Display IP, and Ping Test commands in the Management Dashboard.
4. Support users can issue Get Status, Ping, Display IP, Ping Test, TV On/Off, Set Display Input, Set Display Banner, Set Closed Captions, Set Video Channel, Cabling Test using TDR, and Show TDR Test Results commands.
5. Venue operators can view and monitor information on the Management Dashboard with read-only access to the venues for which permissions are granted. They also can issue Get Status, Ping, Display IP, and Query Syslog commands in the Management Dashboard for the DMPs in their authorized venues.
6. The SSC portal cannot be accessed directly from the Cisco StadiumVision Director main menu or Control Panel. Access to the user-specific portal is opened only by logging into Cisco StadiumVision Director as an SSC user.



StadiumVision



PART 4

Cisco StadiumVision Director System Management



StadiumVision

Backing Up and Restoring Cisco StadiumVision Director Servers

First Published: April 21, 2014

Revised: June 13, 2014

This module describes how to setup and schedule backups between a primary and secondary server, and restore data between them.

Contents

- [Prerequisites for Backing Up and Restoring Cisco StadiumVision Director Servers](#), page 3
- [Restrictions for Backing Up and Restoring Cisco StadiumVision Director Servers](#), page 4
- [Information About Backing Up and Restoring Cisco StadiumVision Director Servers](#), page 4
- [How to Backup a Cisco StadiumVision Director Server](#), page 6
- [How to Restore a Cisco StadiumVision Director Server](#), page 13

Prerequisites for Backing Up and Restoring Cisco StadiumVision Director Servers

Before you backup or restore Cisco StadiumVision Director servers, be sure that the following requirements are met:

- You are familiar with using the Text Utility Interface (TUI) in Cisco StadiumVision Director.
For more information, see the [“Cisco StadiumVision Director Server Text Utility Interface”](#) module of the *Cisco StadiumVision Director Server Administration Guide*.
- You have a directly-connected console or an SSH client to access the primary active and secondary servers.
- You have the IP addresses of the active and secondary servers.
- You know the installer account credentials on the Cisco StadiumVision Director active and secondary servers.

- The IP address of the secondary server must be reachable on the network from the active server or the TUI backup configuration will fail.
- You have determined an appropriate time on the network to schedule automatic backups and restores.

Restrictions for Backing Up and Restoring Cisco StadiumVision Director Servers

Consider the following restrictions when backing up and restoring Cisco StadiumVision Director servers:



Caution

The tasks described in this document apply only to a redundant server environment where *both* Cisco StadiumVision Director servers are running version 3.2 or later software.

- If you have to fail over to your secondary Cisco StadiumVision Director server due to a problem on the primary, then your original backup configuration will be invalid.
Be aware that your scheduled backup process cannot fully operate by automatically transferring a copy of the backup to the secondary server until you use the TUI automatic backup configuration again to reset the backup configuration between the primary and secondary servers. However, a backup will continue to be saved on the primary server.
- When you fail back to the original primary server and are now using the original IP addressing configuration, you still will need to use the TUI automatic backup configuration again so that the backup directory can be re-established on the secondary server.
- A restore cannot run while an event script is running.

Information About Backing Up and Restoring Cisco StadiumVision Director Servers

This section includes the following topics:

- [Backup Environment, page 4](#)
- [What Cisco StadiumVision Director Data is Backed Up, page 5](#)
- [Disk Storage and Maintenance, page 5](#)
- [Restore Environment, page 6](#)

Backup Environment

While you can run a backup for a network environment where there is only a single Cisco StadiumVision Director server, the recommended environment that is described in this document is a redundant environment for either Platform 2 or Platform 3 servers or a virtualized environment. In a redundant environment, you are running Cisco StadiumVision Director on a primary server, with a secondary server connected to the same subnet where the backup data from the primary server is saved.

The backup process can be scheduled and also run manually.

For a disk space alert based on the disk critical threshold set for the server, look for “DEGRADED” in the Sub Type column for the “Service Monitor” in the Source column.

Restore Environment

As with backups, you can schedule the restore process or run it manually. When the manual restore screen is displayed, it lists backups from both the backup and restore directories, concatenated together. This allows you to run a manual restore on either the primary or the secondary server. An automated restore always uses the most recent backup file in the restore directory.

Also, the schedule of tasks to run in the primary database and the secondary database will be different, due to the existence of the backup and restore tasks. Therefore, the schedule itself is not automatically restored.

How to Backup a Cisco StadiumVision Director Server

This section includes the following tasks:

- [Enabling the Backup Account on the Secondary Server, page 6](#) (required)
- [Setting Up the Primary Server for Automatic Backup and Restore, page 7](#) (required)
- [Scheduling a Regular Backup, page 9](#) (required)
- [Starting a Backup Manually for Immediate Execution, page 10](#) (optional)
- [Verifying Backup Completion, page 11](#) (optional)
- [Modifying the Number of Days for Backup File Retention, page 11](#) (optional)

Enabling the Backup Account on the Secondary Server

Before you set up the primary Cisco StadiumVision Director server for automatic backup and restore with a redundant secondary server, you need to enable the backup account on the secondary server using the TUI.

For more information about using the TUI, see the “Cisco StadiumVision Director Server Text Utility Interface” module of the *Cisco StadiumVision Director Server Administration Guide*.

To enable the backup account on the secondary server, complete the following steps:

-
- Step 1** On the secondary server, 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 4** At the prompt, type the password for the installer account on the secondary backup server.
- Step 5** When accepted, the system generates the RSA keys and the public key is copied to the secondary server. Confirm that the keys are created without errors as shown in (Figure 5):

Figure 5 Generation of RSA Keys

```

Please enter the IP address of the currently inactive SVD server
Enter hostname (or press <ENTER> to cancel): 10.194.171.62
Please enter the password for installer @ 10.194.171.62:
Generating public/private rsa key pair.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
31:79:b0:1f:e4:c3:34:67:9a:38:3a:69:2e:65:98:0b root@gatemp34
The key's randomart image is:
+--[ RSA 2048 ]-----+
  . +.
  O.o
  .o#
  o o o
  o o .S .
  E o B
  . * .
  o
  +
-----+
Press any key to return to the menu.

```

- Step 6** Wait until the “Press any key” message appears (there can be a short delay before it is displayed).
- Step 7** Then, press any key to return to the StadiumVision Server Administration menu.
- Step 8** Continue to return to the Main Menu and exit the TUI.

Scheduling a Regular Backup

After you have configured the servers to support the backup process, you need to schedule backups using the Management Dashboard in the Cisco StadiumVision Director software.



Note

It is recommended that you schedule backups to occur while the Cisco StadiumVision Director servers are not actively running scripts or performing other event processing.

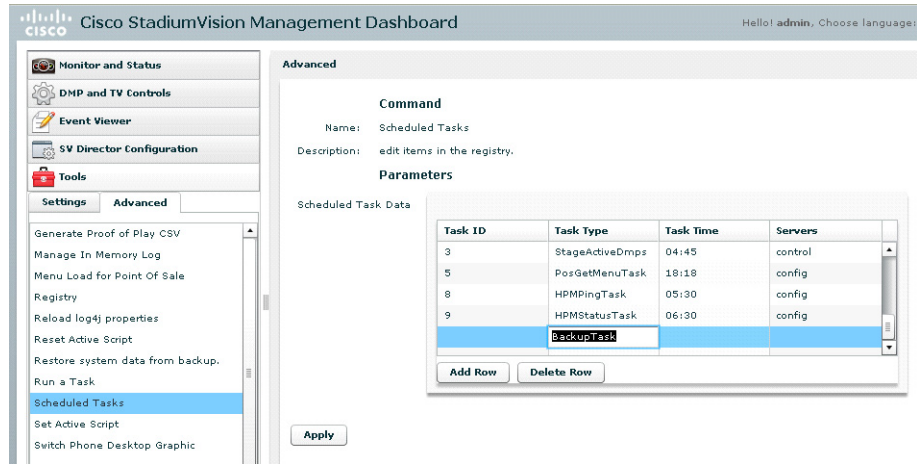
To configure a backup to run on a regular schedule, complete the following steps:

- Step 1** Log into the primary Cisco StadiumVision Director server as an administrator.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
The Cisco StadiumVision Management Dashboard opens in a new window.
- Step 3** Select **Tools > Advanced > Scheduled Tasks**.
- Step 4** Click **Add Row** and scroll to the new blank line.
- Step 5** Click in the Task Type column and type **BackupTask** (Figure 6).



Note

Be sure to type the name of the task exactly as shown with upper and lowercase characters.

Figure 6 Adding a Backup Task to Run on a Regular Schedule

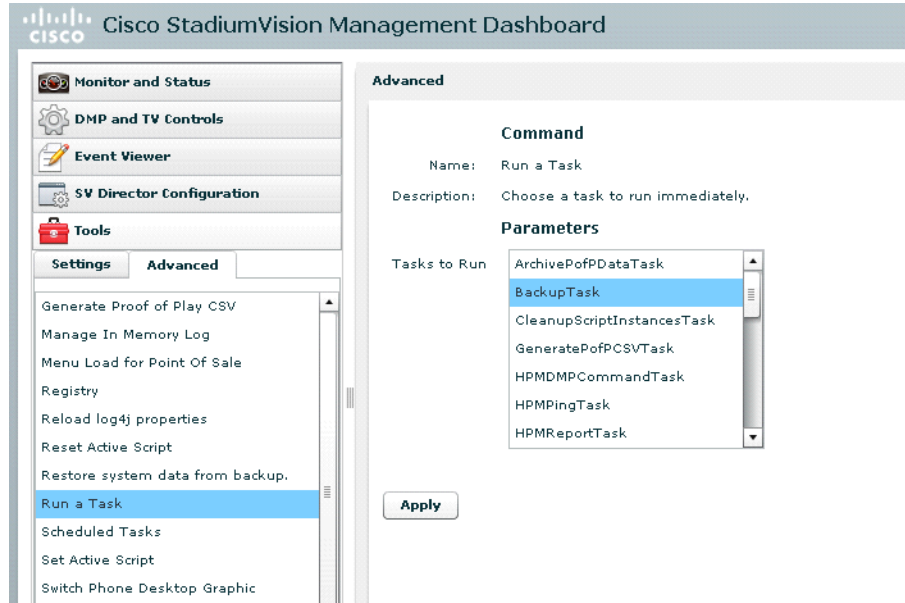
- Step 6** Click in the Task Time column and specify the time (in 24:00 format) when you want the backup to run.
- Step 7** Click in the Servers column and type **config**.
- Step 8** Click **Apply**.

Starting a Backup Manually for Immediate Execution

If you want to start a backup other than at the regularly scheduled time, the Cisco StadiumVision Director software also allows you to run a backup process immediately.

To start a backup manually for immediate execution, complete the following steps:

- Step 1** Log into Cisco StadiumVision Director as an administrator.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
The Cisco StadiumVision Management Dashboard is opened in a new window.
- Step 3** Select **Tools > Advanced > Run a Task**.
- Step 4** In the Tasks to Run box, select the **BackupTask** (Figure 7).

Figure 7 Running a Scheduled Backup Task Manually

- Step 5** Click **Apply**.
The backup begins immediately.



Note The “success” message that appears means that the backup task has started. It does not mean that the backup has completed.

Verifying Backup Completion

You can go to the **Management Dashboard > Tools > Advanced > Restore system data from backup** and verify that backup files with dates and times appear.



Note Messages from the backup process include the string “com.cisco.sv.backup” and are stored in the `/opt/sv/servers/config/logs/sv_dev_debug.log` file. However, be aware that the messages “Starting backup” and “Backup completed” will always appear in the log regardless of success.

The “Backup completed” message does *not* necessarily mean that the backup was successful. If a log message appears before the “Backup completed” message (and after the “Starting backup” message) that includes the “com.cisco.sv.backup” string and also “ERROR,” then there is a problem.

Modifying the Number of Days for Backup File Retention

If your site maintains a large volume of video content, you might want to modify the number of days that backup files are retained to reduce the amount of disk storage required in your system. The default retention period is 10 days.

**Note**

This task must be run on both the primary server and secondary backup server.

To modify the number of days for backup file retention, complete the following steps:

- Step 1** Log into the TUI by doing the following:
- Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the primary Cisco StadiumVision Director server using the IP address for your server.
 - 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 **StadiumVision Server Administration > Backup/restore Retention Policy**.
- A menu of policy options is displayed (Figure 8), where you can choose to retain files for 1, 2, 5, 7, or 10 (the default) days.

Figure 8 Backup/restore Retention Policy Menu

```
Main Menu > StadiumVision Server Administration > Backup/restore Retention Policy
Please choose one of the following menu options:
a) Keep backup/restore files newer than 1 day
b) Keep backup/restore files newer than 2 days
c) Keep backup/restore files newer than 5 days
d) Keep backup/restore files newer than 7 days
e) Keep backup/restore files newer than 10 days
R or < or ,) Return to prior menu
```

- Step 3** Type the letter that corresponds to the number of days that you want to retain files and press **Enter**.
- Step 4** When the change of policy confirmation message displays, press any key to return to the StadiumVision Server Administration menu.

Figure 9 Confirmation of Policy Change

```
Configured Backup/Restore Retention Policy.
Press any key to return to the menu.
```

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

How to Restore a Cisco StadiumVision Director Server

The Cisco StadiumVision Director software automatically copies backup files between the primary and secondary servers and when the restore process starts, verifies the MD5 checksum.

If you need to failover to the secondary server and do a restore, follow the procedures in the “[Configuring Failover Between Redundant Cisco StadiumVision Director Servers](#)” module on page 15.

**Note**

If for some reason you need to manually copy files between the servers, be sure that you copy both the .tar and .chksum files because the restore process automatically uses both files to verify the MD5 signature.

This section includes the following tasks:

- [Starting a Restore Manually for Immediate Execution, page 13](#) (optional)
- [Restarting the Cisco StadiumVision Director Software, page 14](#) (required after restore run)

Starting a Restore Manually for Immediate Execution

If you want to start a restore other than at the regularly scheduled time, the Cisco StadiumVision Director software also allows you to run a restore from backup to begin immediately.

**Caution**

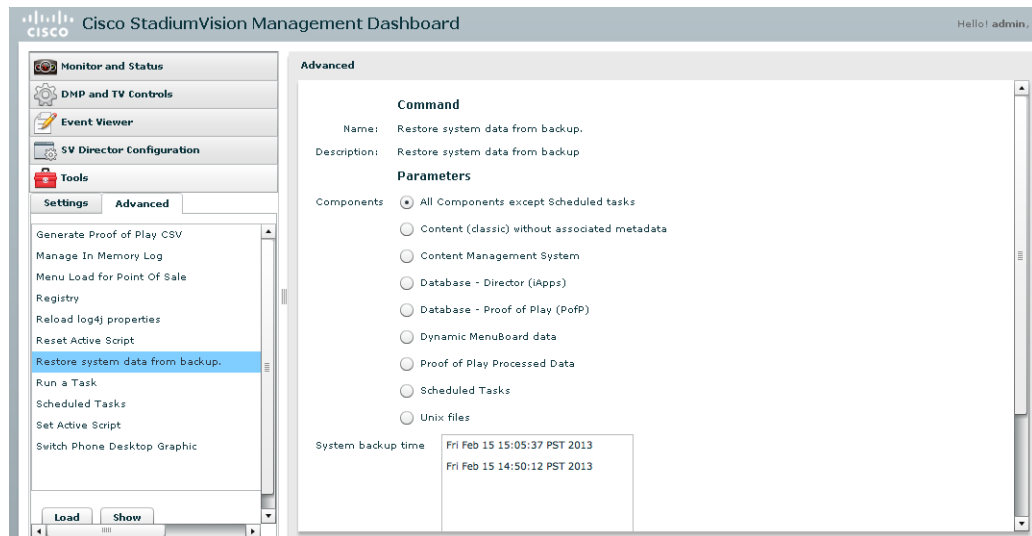
You cannot successfully run the restore process while an event script is running.

To start a restore manually for immediate execution, complete the following steps:

- Step 1** Log into Cisco StadiumVision Director as an administrator.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
The Cisco StadiumVision Management Dashboard is opened in a new window.
- Step 3** Select **Tools > Advanced > Restore system data from backup**.

Step 4 For Components, select the **All components except Scheduled tasks** (Figure 10).

Figure 10 Running a Restore Task Manually



Step 5 (Optional) If you do not want to restore the latest backup (the default), then in the System backup time box, select the date and time of the backup file that you want to restore (Figure 10).

Step 6 Click **Apply**.

The restore begins immediately.



Note

If you need to also restore the scheduled tasks, you can rerun the Restore system data from backup and for Components, select **Scheduled Tasks**.

Restarting the Cisco StadiumVision Director Software

After you perform any restore on a Cisco StadiumVision Director server, you must restart the Cisco StadiumVision Director software to resume normal operation of the services.

To restart the Cisco StadiumVision Director software, complete the following steps:

- Step 1** On the primary server, log into the TUI by doing the following:
- Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the primary Cisco StadiumVision Director server using the IP address for your server.
 - 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 **StadiumVision Server Administration > Restart StadiumVision Director Software**.

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



Configuring Failover Between Redundant Cisco StadiumVision Director Servers

First Published: April 21, 2014

Cisco StadiumVision Director supports an environment best described as *warm standby* between two servers that run the Cisco StadiumVision Director software—one of the servers operates as the primary active server, and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Contents

- [Prerequisites for Configuring Failover Between Redundant Cisco StadiumVision Director Servers, page 16](#)
- [Restrictions for Configuring Failover Between Redundant Cisco StadiumVision Director Servers, page 16](#)
- [Information About Failover Between Redundant Cisco StadiumVision Director Servers, page 16](#)
- [How to Promote a Standby Secondary Server to the Active Server, page 18](#)
- [How to Restore the Primary Server to Active, page 24](#)



Note

Restoring the primary server after failover to secondary requires a service interruption and should only be conducted during scheduled downtime. Be aware that until you change the IP address of the primary server to remove the addressing conflict with the newly active secondary server, you will be unable to schedule backups between the two servers. You will also need to reconfigure the backup/restore environment using the Text Utility Interface (TUI) after the restore. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.

Prerequisites for Configuring Failover Between Redundant Cisco StadiumVision Director Servers

Before you promote a secondary server to become the primary active server, be sure that the following requirements are met:

- You have either physical console access or an SSH client such as PuTTY to log into both Cisco StadiumVision Director servers.
- You understand how to use the Text Utility Interface (TUI). For more information, see the “[Cisco StadiumVision Director Server Text Utility Interface](#)” module. For simplicity in these tasks, the instruction to “select” a particular menu item implies that you type the character that corresponds to the menu option and press **Enter**.
- Verify that you have a successful backup of the primary server on the secondary server. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.
- The Cisco StadiumVision Director backup server is on the same subnet as the primary server.
- The servers are using the Eth0 interface for connection to the network.
- You have the IP addresses of the primary and secondary servers.



Tip

The IP address for the server is displayed on the screen when you log into the TUI. You also can view the `/etc/hosts` information on each server using the TUI **System Settings > System Information** menu option.

Restrictions for Configuring Failover Between Redundant Cisco StadiumVision Director Servers

The Cisco StadiumVision Director server redundancy architecture has the following restrictions:

- Redundancy, and therefore failover, is not supported for Cisco StadiumVision Director Remote servers.
- The Cisco StadiumVision Director server architecture does not support automatic failover when a failure occurs on the active server.
- Depending on your environment, 30 minutes or more is needed to complete the manual failover process.
- In addition, after the manual failover process is completed, a script push will be required if you are in an active event, which depending on your deployment and content size, can take anywhere from minutes to an hour. When pushing the script again, there will be a service interruption.

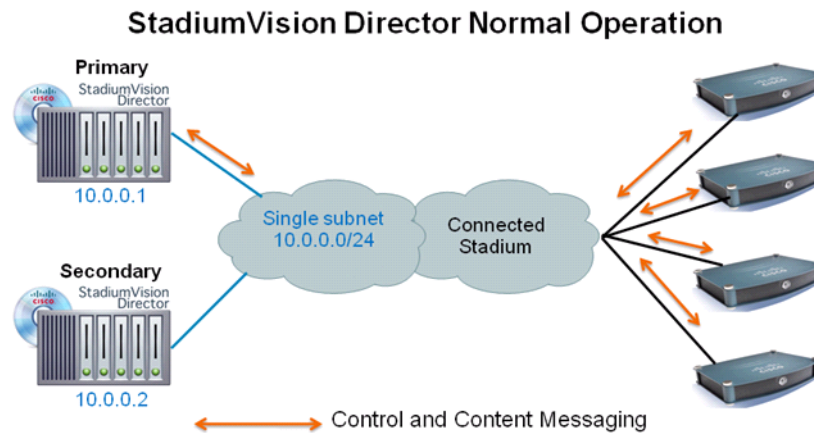
Information About Failover Between Redundant Cisco StadiumVision Director Servers

[Figure 1](#) shows the architecture of Cisco StadiumVision Director server redundancy under normal network conditions and operation. The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet in the Cisco Connected Stadium network.

While the secondary server is still connected to the network, notice that communication and control only occurs between the primary Cisco StadiumVision Director server and the rest of the network, including the Digital Media Players (DMPs).

The secondary server is only connected to the network to be made available as a backup to the primary should a failure occur. In addition, the secondary server can (and should) be configured to be backed up with data from the primary server on a scheduled basis.

Figure 1 Cisco StadiumVision Director Server Redundancy Under Normal Operation



[Figure 2](#) shows the redundancy environment when connectivity from the primary Cisco StadiumVision Director server fails. When the primary server fails, a manual process must take place to restore the secondary server from a backup, shut down the primary server, and activate the secondary server as the primary.

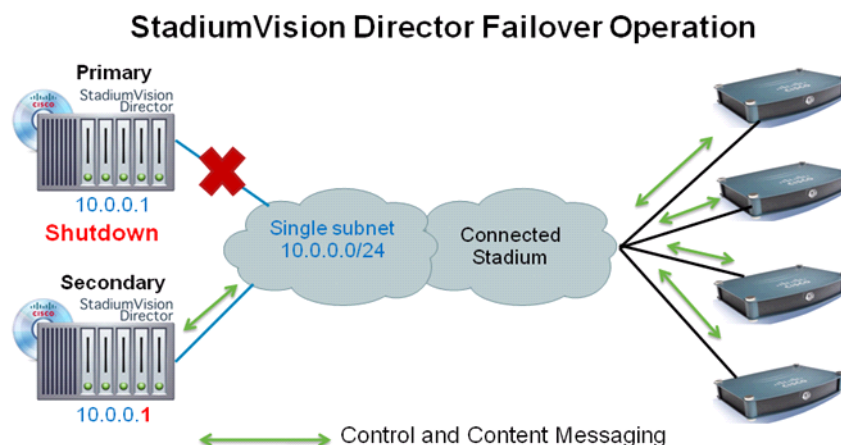
Notice that the secondary server must be reconfigured to use the same IP address the original primary server. In this example, the secondary server IP address is changed to 10.0.0.1 (from 10.0.0.2) to match the primary server address. When the process is complete, communication and control only occurs between the newly activated secondary server and the rest of the network.



Note

The word “failover” does not mean automatic activation of a secondary server. The failover process is manual.

Figure 2 Cisco StadiumVision Director Server Redundancy Under Failover Operation



How to Promote a Standby Secondary Server to the Active Server

This section describes the related tasks to perform when a primary Cisco StadiumVision Director server fails in a redundant server environment. It includes tasks to activate the secondary server to replace the functionality of the primary server for Cisco StadiumVision operation.



Note

For simplicity in these tasks, any instruction to *go to* or *select* a particular TUI menu item implies that you type the character that corresponds to the menu option and press **Enter**.

This section includes the following tasks:

- [Starting and Configuring the Services on the Secondary Server, page 19](#) (required)
- [Restoring the Secondary Server with System Data From a Backup File, page 19](#) (required)
- [Stopping Services and Auto-Restart, and Shutting Down the Primary Server, page 19](#) (required)
- [Shutting Down Services on the Secondary Server, page 20](#) (required)
- [Changing the IP Address on the Secondary Server, page 20](#) (required)
- [Restarting the Network Service on the Secondary Server, page 21](#) (required)
- [Verifying Network Connectivity to the Secondary Server, page 22](#) (required)
- [Clearing the ARP Cache on the Switch, page 22](#) (optional)
- [Restarting Cisco StadiumVision Director on the Secondary Server, page 23](#) (required)
- [Verifying the Cisco StadiumVision Director Configuration on the Secondary Server, page 23](#) (required)

Starting and Configuring the Services on the Secondary Server

To start and configure the services on the secondary server, complete the following steps:

-
- Step 1** Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client. The TUI Main Menu is displayed.
 - Step 2** Go to the **StadiumVision Server Administration > Failover** sub-menu.
 - Step 3** Select the **Promote as Primary/Active** option.
The Cisco StadiumVision Director services are started and also configured to start automatically when a reboot occurs.
-

Restoring the Secondary Server with System Data From a Backup File

To restore the secondary server with system data from a backup file, complete the following steps:

-
- Step 1** Log into Cisco StadiumVision Director on the *secondary* server using an administrator account.
 - Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
 - Step 3** From the Dashboard Drawers, select **Tools > Advanced > Restore system data from backup**.
 - Step 4** Select the components that you want to restore, and select the date of the backup file to use for the restore.
 - Step 5** Click **Apply**.
The restore begins. A dialog box appears notifying you when the restore process has successfully completed.
-

Stopping Services and Auto-Restart, and Shutting Down the Primary Server

**Note**

If the primary server has become unavailable for this task, be sure that you power down the server so that it will not conflict with the newly active secondary server.

To stop services and auto-restart, and shut down the primary server, complete the following steps:

-
- Step 1** Log into the TUI as installer on the *primary* server using a directly-connected console or SSH client. The TUI Main Menu is displayed.
 - Step 2** Go to the **StadiumVision Server Administration > Failover** sub-menu.
 - Step 3** Select the **Configure as Secondary/Inactive** option.
 - Step 4** Press any key to return to the Failover sub-menu.

- Step 5** Return to the **StadiumVision Server Administration** menu by typing **R** and pressing **Enter**.
- Step 6** Select the **Power Off** option.
The primary server is shut down.
-

Shutting Down Services on the Secondary Server

To shut down services on the secondary server, complete the following steps:

- Step 1** Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client.
The TUI Main Menu is displayed.
- Step 2** Go to the **StadiumVision Server Administration** sub-menu.
- Step 3** Select the **Shutdown StadiumVision Director software** option.
All Cisco StadiumVision Director services are stopped.
- Step 4** Return to the Main Menu by typing **R** and pressing **Enter**.
-

Changing the IP Address on the Secondary Server

Prerequisites

Before you change the IP address on the secondary server, be sure that the following requirements are met:

- You have the IP address of the primary server.
- You understand how to use the vi editor. For information about using the vi editor, see the [“Cisco StadiumVision Director Server Text Utility Interface” module on page 3](#)



Note

The system will run if the localhost entry exists but the hostname entry is missing in the /etc/hosts file. However, when the secondary hostname exists, the IP address of the secondary server must be changed to match the IP address of the primary server.

Procedure

To change the IP address on the secondary server, complete the following steps:

- Step 1** From the TUI Main Menu on the secondary server, go to the **System Settings** menu.
- Step 2** Select the **Network Settings** option.
The Network Settings sub-menu is displayed.
- Step 3** Select the **Setup Network Information** option.
- Step 4** At the Configure Network confirmation screen, press any key to continue.

The Select Action screen is displayed with the “Edit Devices” option highlighted.

Step 5 Press **Enter** to select.

The Select a Device screen is displayed with the “eth0” network interface highlighted.

Step 6 Press **Enter** to select.

The Ethernet Configuration screen is displayed.



Note The Linux screen is misspelled “Devernet Configuration.”

Step 7 Press the tab key until the cursor is positioned on the Static IP address line.

Step 8 Press the backspace key to go to the beginning of the line and type in the IP address of the primary server. In our example from [Figure 2](#), this would be 10.0.0.1. Be sure to use the actual IP address of your primary server.

Step 9 Press the tab key until the **Ok** button is highlighted and press **Enter**.
You return to the Select a Device screen.

Step 10 Press the tab key until the **Save** button is highlighted and press **Enter**.
You return to the Select Action screen.

Step 11 Press the tab key until the **Save&Quit** button is highlighted and press **Enter**.
You return to the TUI Configure Network screen.

Step 12 Press any key to return to the Network Settings sub-menu.

Step 13 Select the **Edit hosts file** option.

Step 14 Press any key to enter edit mode.

Step 15 Replace this server’s IP address with the IP address of the primary server.

Step 16 Save the configuration and exit vi using the following command:

```
:wq
```

Restarting the Network Service on the Secondary Server

To restart the network service on the secondary server, complete the following steps:

Step 1 From the TUI Main Menu on the secondary server, go to the **Services Control** sub-menu.

Step 2 Select the **Networking** option.
The Networking sub-menu is displayed.

Step 3 Select the **Restart networking** option.
The network daemon is restarted and the IP address change is put into effect on the secondary server.



Note If you are connected to the server through the network using SSH, your session is disconnected and you will need to reconnect using the IP address of the primary server.

Verifying Network Connectivity to the Secondary Server

To verify network connectivity to the secondary server, complete the following steps:

- Step 1** From the TUI Main Menu on the secondary server, go to the **Troubleshooting** sub-menu.
- Step 2** Select the **Ping a host** option.
- Step 3** At the “Enter hostname” prompt, type the hostname or IP address of the secondary server and press **Enter**.
- Step 4** Look for successful transmission and receipt of PING packets.



Note If you cannot reach the secondary server, go to the [“Clearing the ARP Cache on the Switch” section on page 22](#).

- Step 5** Press **Ctrl-C** to stop sending PING packets.
- Step 6** Press any key to return to the Troubleshooting menu.

Clearing the ARP Cache on the Switch

This task is optional, as the ARP cache on the switch will refresh in 5-10 minutes. However, if you cannot access the secondary server after changing its IP address, you can clear the ARP cache for that IP address on the switch using the **clear ip arp** privileged EXEC command.

To clear the ARP cache on the switch, complete the following steps:

- Step 1** Use a directly-connected console, or if you know the IP address of the switch, use Telnet to access the switch as shown in the following example, where *ip-address* is the address of your switch:


```
telnet ip-address
```
- Step 2** At the corresponding prompts, enter your login information as shown in the following example, where *yourname* and *yourpass* are your username and password:


```
Username: yourname
Password: yourpass
switch>
```
- Step 3** Enter privileged EXEC mode using the **enable** command and corresponding password:


```
switch> enable
Password: enablepassword
switch#
```

- Step 4** To clear the ARP cache of the newly-assigned IP address now used by the secondary server, use the **clear ip arp** command as shown in the following example:

```
clear ip arp 10.0.0.1
```

Restarting Cisco StadiumVision Director on the Secondary Server

To restart Cisco StadiumVision Director on the secondary server, complete the following steps:

- Step 1** Do one of the following on the *secondary* server:
- If still logged into the TUI, go to the Main Menu.
 - If not still logged into the TUI as installer on the secondary server, use the new IP address and log in again using a directly-connected console or SSH client.
- The TUI Main Menu is displayed.
- Step 2** Go to the **StadiumVision Server Administration** sub-menu.
- Step 3** Select the **Restart StadiumVision Director Software** option.
- All Cisco StadiumVision Director services are started.
- Step 4** Press any key to return to the StadiumVision Server Administration sub-menu.
- Step 5** Press **R** and **Enter** until you return to the Main menu.
- Step 6** Press **X** to exit the TUI.
-

Verifying the Cisco StadiumVision Director Configuration on the Secondary Server

To verify the Cisco StadiumVision Director configuration on the secondary server, complete the following steps:

- Step 1** Log in to Cisco StadiumVision Director on the *secondary* server using an administrator account.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
- Step 3** From the Dashboard Drawers, select **DMP and TV Controls > Monitoring > Get Status**.
- Confirm that you have successful communication between the DMPs and Cisco StadiumVision Director.
- Step 4** Verify that all of the content is on this server.
- Step 5** To establish control of the DMPs, start a script without any content and with the No Staging radio button selected. This should only require less than 10 minutes.



Note You can push a script with content, but this will result in a longer period of downtime.

How to Restore the Primary Server to Active


Note

This task requires a service interruption.

At a scheduled downtime, you should restore the primary server as the active server to re-establish your normal operating environment and clean up the original primary server from the failure, make IP addressing changes, and have regularly scheduled backups again between the two servers.


Note

For simplicity in these tasks, any instruction to *go to* or *select* a particular TUI menu item implies that you type the character that corresponds to the menu option and press **Enter**.

This section includes the following tasks:

- [Prerequisites, page 24](#)
- [Stopping Services and Auto-Restart on the Secondary Server, page 24](#) (required)
- [Changing the IP Address on the Secondary Server, page 25](#) (required)
- [Restarting Cisco StadiumVision Director on the Secondary Server, page 26](#) (required)
- [Verifying Network Connectivity on the Secondary Server, page 26](#)
- [Starting and Configuring the Services on the Original Primary Server, page 27](#) (required)
- [Restoring the Original Primary Server with System Data From a Backup File, page 27](#) (as required)
- [Restarting the Local Control Service on the Primary Server, page 28](#) (required after restore run)
- [Verifying Network Connectivity to the Primary Server, page 28](#) (required)
- [Verifying the Cisco StadiumVision Director Configuration on the Original Primary Server, page 29](#) (required)

Prerequisites

If you have made any administrative changes on the active secondary server, be sure that a successful backup has been run.

While the secondary server is still active, re-configure the backup environment and run a manual backup from the Management Dashboard. The latest backup will then be copied to the primary (inactive) server. For more information, see the [“Backing Up and Restoring Cisco StadiumVision Director Servers” module on page 3](#).

Stopping Services and Auto-Restart on the Secondary Server

To stop services and auto-restart of them on the secondary server, complete the following steps:

-
- Step 1** Log into the TUI as installer on the *secondary* server using a directly-connected console or SSH client. The TUI Main Menu is displayed.
- Step 2** Go to the **StadiumVision Server Administration > Failover** sub-menu.
- Step 3** Select the **Configure as Secondary/Inactive** option.

- Step 4** Press any key to return to the Failover sub-menu.
 - Step 5** Return to the **StadiumVision Server Administration** menu by typing **R** and pressing **Enter**.
 - Step 6** Select the **Shutdown StadiumVision Director Software** option.
-

Changing the IP Address on the Secondary Server


Prerequisites

Before you change the IP address on the secondary server, be sure that the following requirements are met:

- You have the IP address of the secondary server.
- You understand how to use the vi editor. For information about using the vi editor, see the [“Cisco StadiumVision Director Server Text Utility Interface” module on page 3](#)

Procedure

To change the IP address on the secondary server, complete the following steps:

- Step 1** From the TUI Main Menu on the *secondary* server, go to the **System Settings** menu.
- Step 2** Select the **Network Settings** option.
The Network Settings sub-menu is displayed.
- Step 3** Select the **Setup Network Information** option.
- Step 4** At the Configure Network confirmation screen, press any key to continue.
The Select Action screen is displayed with the “Edit Devices” option highlighted.
- Step 5** Press **Enter** to select.
The Select a Device screen is displayed with the “eth0” network interface highlighted.
- Step 6** Press **Enter** to select.
The Ethernet Configuration screen is displayed.

Note The Linux screen is misspelled “Devernet Configuration.”
- Step 7** Press the tab key until the cursor is positioned on the Static IP address line.
- Step 8** Press the backspace key to go to the beginning of the line and type in the IP address of the secondary server.
In our example from [Figure 1](#), this would be 10.0.0.2. Be sure to use the actual IP address of your secondary server.
- Step 9** Press the tab key until the **Ok** button is highlighted and press **Enter**.
You return to the Select a Device screen.
- Step 10** Press the tab key until the **Save** button is highlighted and press **Enter**.

You return to the Select Action screen.

Step 11 Press the tab key until the **Save&Quit** button is highlighted and press **Enter**.

You return to the TUI Configure Network screen.

Step 12 Press any key to return to the Network Settings sub-menu.

Step 13 Select the **Edit hosts file** option.

Step 14 Press any key to enter edit mode.

Step 15 Replace this server's IP address with the IP address of the secondary server.

Step 16 Save the configuration and exit vi using the following command:

```
:wq
```

Restarting Cisco StadiumVision Director on the Secondary Server

To restart Cisco StadiumVision Director on the secondary server, complete the following steps:

Step 1 Do one of the following on the *secondary* server:

- If still logged into the TUI, go to the Main Menu.
- If not still logged into the TUI as installer on the secondary server, use the new IP address and log in again using a directly-connected console or SSH client.

The TUI Main Menu is displayed.

Step 2 Go to the **StadiumVision Server Administration** sub-menu.

Step 3 Select the **Restart StadiumVision Director Software** option.

All Cisco StadiumVision Director services are started.

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

Step 5 Press **R** and **Enter** until you return to the Main menu.

Step 6 Press **X** to exit the TUI.

Verifying Network Connectivity on the Secondary Server

To verify network connectivity to the secondary server, complete the following steps:

Step 1 From the TUI Main Menu on the *secondary* server, go to the **Troubleshooting** sub-menu.

Step 2 Select the **Ping a host** option.

Step 3 At the “Enter hostname” prompt, type the hostname or IP address of the secondary server and press **Enter**.

Step 4 Look for successful transmission and receipt of PING packets.



Note If you cannot reach the secondary server, go to the [“Clearing the ARP Cache on the Switch” section on page 22.](#)

- Step 5** Press **Ctrl-C** to stop sending PING packets.
- Step 6** Press any key to return to the Troubleshooting menu.

Starting and Configuring the Services on the Original Primary Server

To start and configure the services on the original primary server, complete the following steps:

- Step 1** Power on the original *primary* server.



Note It might take a few minutes for SSH to be available as the server boots.

- Step 2** Log into the TUI as installer on the original *primary* server using a directly-connected console or SSH client.
- The TUI Main Menu is displayed.
- Step 3** Go to the **StadiumVision Server Administration > Failover** sub-menu.
- Step 4** Select the **Promote as Primary/Active** option.
- The Cisco StadiumVision Director services are started and also configured to start automatically when a reboot occurs.
- Step 5** Press any key to return to the Failover sub-menu.
- Step 6** Depending on the state of the server when it went down and what was done while the server was down, a script might be running on the original primary StadiumVision Director server. If a script is running, end the script in the Cisco StadiumVision Director software.

Restoring the Original Primary Server with System Data From a Backup File

If any administrative changes were made to the system while in failover to the other server, you should restore the backup from the secondary.



Note This step requires that a backup was run from the secondary server to the primary before reactivating the primary server.

To restore the original primary server with system data from a backup file, complete the following steps:

- Step 1** Log in to Cisco StadiumVision Director on the original *primary* server using an administrator account.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.

- Step 3** From the Dashboard Drawers, select **Tools > Advanced > Restore system data from backup**.
 - Step 4** Select the components that you want to restore, and select the date of the backup file to use for the restore.
 - Step 5** Click **Apply**.
The restore begins.
-

Restarting the Local Control Service on the Primary Server

After you perform a restore, you must stop and start the local control service (svd-localctl) to resume normal operation of the local control application programming interface (API).

To restart the local control service on the primary server, complete the following steps:

- Step 1** Log into the TUI as installer on the original *primary* server using a directly-connected console or SSH client.
The TUI Main Menu is displayed.
 - Step 2** Go to the **Services Control > StadiumVision Director Services > SVD Local Control** sub-menu.
 - Step 3** Select the **Stop service** option.
The svd-localctl service is stopped.
 - Step 4** When prompted, press any key to return to the SVD Local Control sub-menu.
 - Step 5** Select the **Start service** option.
The svd-localctl service is started. Look for the message that the command completed successfully.
 - Step 6** When prompted, press any key to return to the SVD Local Control sub-menu.
 - Step 7** Press **R** and **Enter** until you return to the Main menu.
 - Step 8** Press **X** to exit the TUI.
-

Verifying Network Connectivity to the Primary Server

To verify network connectivity to the primary server, complete the following steps:

- Step 1** From the TUI Main Menu on the original *primary* server, go to the **Troubleshooting** sub-menu.
- Step 2** Select the **Ping a host** option.
- Step 3** At the “Enter hostname” prompt, type the hostname or IP address of the primary server and press **Enter**.
- Step 4** Look for successful transmission and receipt of PING packets.



Note If you cannot reach the secondary server, go to the [“Clearing the ARP Cache on the Switch” section on page 22](#).

- Step 5** Press **Ctrl-C** to stop sending PING packets.
 - Step 6** Press any key to return to the Troubleshooting menu.
 - Step 7** Press **R** and **Enter** until you return to the Main menu.
 - Step 8** Press **X** to exit the TUI.
-

Verifying the Cisco StadiumVision Director Configuration on the Original Primary Server

To verify the Cisco StadiumVision Director configuration on the original primary server, complete the following steps:

- Step 1** Log in to Cisco StadiumVision Director on the original *primary* server using an administrator account.
 - Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
 - Step 3** From the Dashboard Drawers, select **DMP and TV Controls > Monitoring > Get Status**.
Confirm that you have successful communication between the DMPs and Cisco StadiumVision Director.
 - Step 4** Verify that all of the content is on this server.
 - Step 5** Test the system by looking at the status in the Management Dashboard and by running test scripts to verify operation of the system.
-

■ How to Restore the Primary Server to Active



StadiumVision



PART 5

Cisco StadiumVision Director System Tools



Cisco StadiumVision Director Server Text Utility Interface

First Published: April 21, 2014

The Text Utility Interface (TUI) provides a console-based interface for use by system installers, administrators, and troubleshooting personnel. The TUI replaces the requirement for any low-level system command line (shell) access and can be used to perform routine system tasks such as modifying system configurations, changing passwords, and checking system logs. Remote TAC access and troubleshooting can both be facilitated from the TUI in the event of an outage or failure.

The Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers both include a TUI interface. The remote server version of the TUI has a similar menu structure, but only provides a subset of the functions available in Cisco StadiumVision Director.

Contents

- [Information About the TUI, page 3](#)
- [How to Use the TUI, page 8](#)
- [Related Documentation, page 10](#)

Information About the TUI

This section includes the following topics:

- [Overview of the TUI Menus, page 4](#)
- [Working with the TUI Interface, page 7](#)

Overview of the TUI Menus

The TUI is a nested structure of menus with options that allow you to drill down to specific system tasks to be performed on the server. The primary menus are:

- Main Menu
- System Settings
- System Accounts
- Services Control
- StadiumVision Server Administration
- Troubleshooting

Table 1 provides a description of the primary menus included in the Cisco StadiumVision Director TUI.

Table 1 Description of the Primary TUI Menus

Menu Name	Use this menu to . . .
Main Menu	Access all other menus or exit the TUI.
System Settings	Change server network configuration, system date/time, or display system information.
System Accounts	Manage default system passwords. For more information about system accounts and modifying them, see the “System Accounts on the Cisco StadiumVision Director Servers” module of the <i>Cisco StadiumVision Director Server Administration Guide</i> .
Services Control	Access services running on the server to start, stop, or show status.
StadiumVision Server Administration	Manage the operation and software configuration of the server.
Troubleshooting	Run a ping command, monitor disk space usage, clean up files to free up disk space, display system logging information, or get NTP information.

Figure 1 shows a map of the new Cisco StadiumVision Director TUI menuing system and options.

In Cisco StadiumVision Director Release 3.1.0-797, the Cisco StadiumVision Director TUI was modified with the following changes to allow configuration of the log file retention policy for upgraded servers:

- The “Backup/restore Retention Policy” sub-menu from the StadiumVision Server Administration menu is renamed to “Retention Policy.”
- A new sub-menu named “Log Files” was added to the revised Retention Policy menu, with corresponding options to keep files newer than 5, 10, or 15 days.

Figure 1 TUI Map for Cisco StadiumVision Director Servers

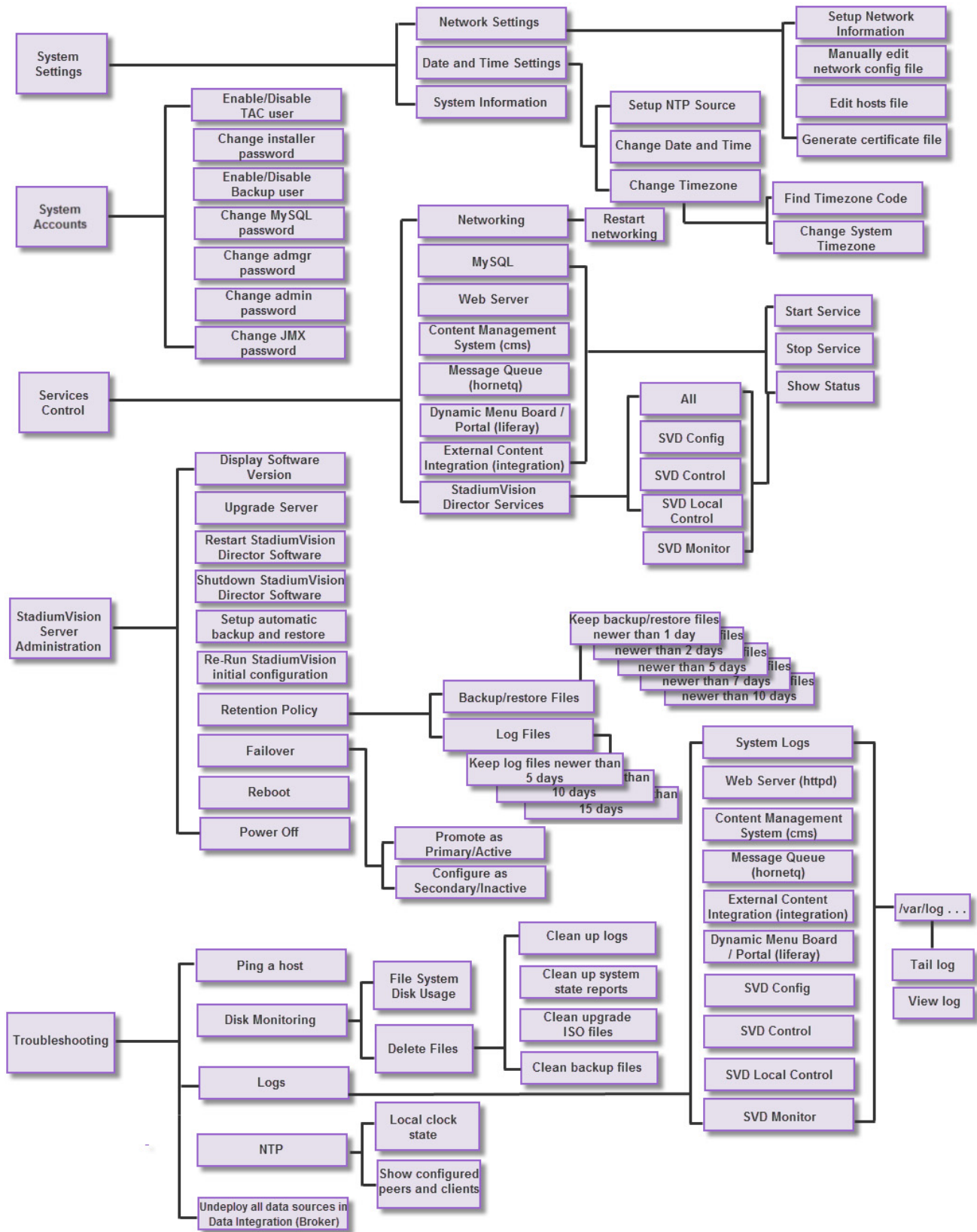
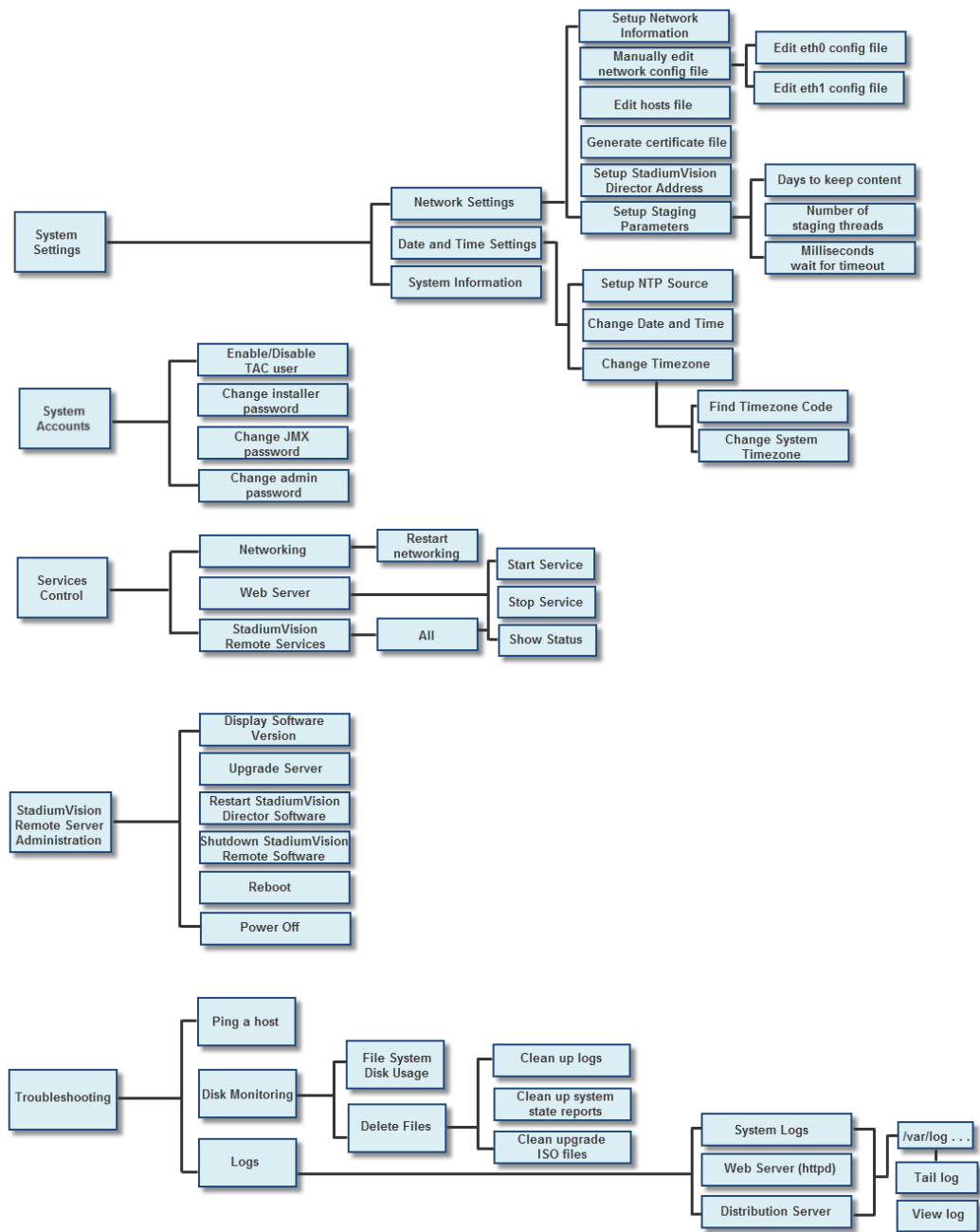


Figure 2 shows a map of the Cisco StadiumVision Director Remote TUI menuing system and options.

Figure 2 TUI Map for Cisco StadiumVision Director Remote Servers



Working with the TUI Interface

This section includes the following topics:

- [Menu Navigation, page 7](#)
- [File Editor, page 7](#)

Menu Navigation

The Main Menu is displayed when you log in. To navigate through the menus you must type the character that corresponds to the menu area where you want to go (**a**, **b**, **c**, and so on) and press **Enter**.

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



Caution

Avoid pressing Ctrl-c from the TUI. This immediately terminates the TUI session and if services were started during the session they might stop running. Use the TUI menu system to exit the interface.

File Editor

Several of the TUI options open server system files for you to modify using the Unix system vi editor. The following configuration files are editable from the TUI:

- DNS information—/etc/resolv.conf
- NTP server information—/etc/ntp.conf
- Server host information—/etc/hosts

Before modifying configuration files, you should be familiar with the simple editing techniques used within the vi editor. [Table 2](#) describes some of the more common vi Editor commands.

Table 2 Common vi Editor Commands

Command	Description
ZZ or :wq	Exit vi and save changes.
:q!	Exit vi without saving changes.
Esc key	Exit current mode and enter vi command mode.
Cursor Movement	
h	Move left (backspace).
j	Move down.
k	Move up.
l	Move right.
Enter key	Move to the beginning of the next line.
Inserting	
a	Append character after cursor.
i	Insert character before cursor. Enters INSERT mode.
r	Replace character under cursor with next character typed.

Table 2 Common vi Editor Commands

Command	Description
R	Keep replacing character until [Esc] is pressed.
Deleting	
db	Delete word before cursor.
dd	Delete line under cursor.
dw	Delete word under cursor.
x	Delete character under cursor.
Put	
P	Undo deletion of characters, words, or lines before cursor.
p	Undo deletion of characters, words, or lines after cursor.

How to Use the TUI

This section provides information about how to use some of the areas of the TUI interface. It includes the following topics:

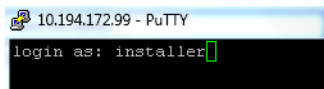
- [Logging Into the TUI, page 8](#)
- [Displaying System Information, page 9](#)
- [Exiting the TUI, page 10](#)

Logging Into the TUI

To access the TUI, you need either physical console access or an SSH client such as PuTTY.

To log into the TUI, complete the following steps:

-
- Step 1** Do one of the following:
- Access the server using a directly-attached console.
 - In the SSH client software, specify the IP address of the server that you want to access.
- Step 2** When the “login as:” prompt appears, type **installer** and press **Enter** (Figure 3):

Figure 3 TUI Login Prompt

- Step 3** At the password prompt, type the installer password and press **Enter**.



Note In a PuTTY terminal, the keystrokes for your password entry are not shown.

Exiting the TUI

**Caution**

Avoid pressing Ctrl-c from the TUI. This immediately terminates the TUI session and if services were started during the session they might stop running. Use the TUI menu system to exit the interface.

To exit the TUI, complete the following steps:

Step 1 Go to the TUI Main Menu.

**Tip**

If you are in a TUI submenu, you will have to type **R** or **<** or **,** and press **Enter** to navigate back to the Main Menu.

Step 2 Type **X** and press **Enter**.

Related Documentation

The following documents provide details about using some of the specific areas of the TUI:

- Other modules in this *Cisco StadiumVision Director Server Administration Guide*.
- [Cisco StadiumVision Director Software Installation and Upgrade Guide](#)



StadiumVision



PART 6

Cisco StadiumVision Director Server Troubleshooting



System State Reports

First Published: April 21, 2014

The System State Report feature enables easy capture and export of system state data for Cisco StadiumVision servers. This information can be sent to a remote support engineer to help troubleshoot any issues that occur with the system.

Information About System State Reports

Figure 1 shows the System State Report screen.

Figure 1 **System State Report Screen**



Table 1 describes the options provided on the System State Report screen.

Table 1 System State Report Screen Description

Category	Description
Report Destination	<p>Allows you to choose whether you want to download the report or view it in your browser window. If you check Download report, your browser will download the resulting report when the system state report is ready. You can save this file on your computer, view its contents, and mail it to support personnel.</p> <p>If you check View in browser, the resulting report is available for immediate viewing online via the link provided.</p>
Level	<p>Selects the level of detail you want in the report.</p> <ul style="list-style-type: none"> • Basic First Level: Provides detailed information of the system state, including information on configuration and current performance of the hardware, the operating system, the database, the Java VM, and the SV application. • Java Heap Dump: Displays a report indicating the internal activities of the selected Java Virtual Machine (JVM). Before running the report, you will see a selection screen showing the process ID, the name of the JVM, and its command line. Select one of the JVMs that you wish to get the head dump for, then click Get Heap Dump. The heap dump report will generate. <p>Exercise care in taking a heap dump, because while this is running, it can affect system performance.</p> <ul style="list-style-type: none"> • Full SVD Logs: Displays a list of system log files available for retrieving from the server and copying to your local drive or sending to Cisco Support. If you select View in Browser, then you can view the logs online as well.
Previous Reports	<p>Lists up to 15 of the most recent exports of the system state reports that were collected. The reports may have been collected from someone accessing this request page, or from a system scheduled task.</p> <p>You can select one of the links to download to your local drive to view or email to Cisco support.</p>

How to Run a System State Report

This section includes the following tasks:

- [Running a System State Report Manually, page 3](#)
- [Scheduling a System State Report, page 3](#)
- [Viewing Reports, page 3](#)

Running a System State Report Manually

To run a system state report manually, complete the following steps:

-
- Step 1** From the Cisco StadiumVision server or remote server Main Menu, click **System State Report**.
 - Step 2** Select one or both report destination types, **Download report** and/or **View in browser**.
 - Step 3** Under Level, select the type of report that you want to run.
 - Step 4** Click **Get System Status**.
A status bar is displayed while the report is generating.
-

Scheduling a System State Report

You can extract the system state data on a periodic basis through the **Tools > Advanced > Scheduled Tasks** function in the Management Dashboard. The reports generated can be viewed under **Previous Reports** on the main System State Report page.

To create a scheduled task, use the following procedure:

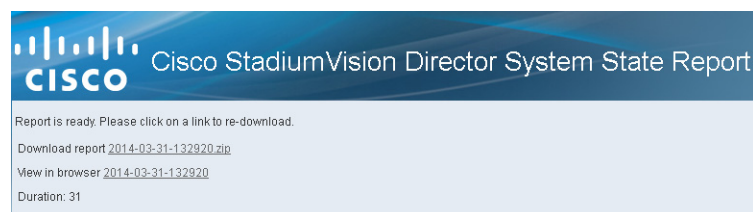
-
- Step 1** Open the Dashboard and select **Tools > Advanced > Scheduled Tasks**.
 - Step 2** Click **Add Row** and add a row with the task type being **SystemStateExtractorTask**.
 - Step 3** Enter a task time as desired.
 - Step 4** Click **Apply**.
-

The reports generated can be viewed under **Previous Reports** on the main System State Report page.

Viewing Reports

After manually running a report, the screen displays “Report is ready” as shown in [Figure 2](#).

Figure 2 *Report is Ready*



Depending on the option(s) that you selected before running the report, you can view the report in your browser by selecting the link provided.

If you downloaded the report, then depending on your browser and its settings, you will get a dialog box to save the report on your local machine. If the automatic download does not work, you can click on the link after the word **Download** to download the file again. The report is downloaded as a compressed file (.zip) containing multiple parts to the report.

**Note**

The heap dump report type is a compressed report file which you can save to your local drive and forward to support personnel for troubleshooting, and is packaged like the Basic Level report.

Viewing Scheduled Reports and Previous Reports

Scheduled reports can be viewed under **Previous Reports** on the System State Report screen. The format of the file name is the date and time that the report was run.

Click one of the timestamps under **Previous Reports** to download the report that ran at the scheduled time. You may get a dialog box to save the report on your local machine. If so, save it as desired. This is a compressed file containing multiple parts to the report.

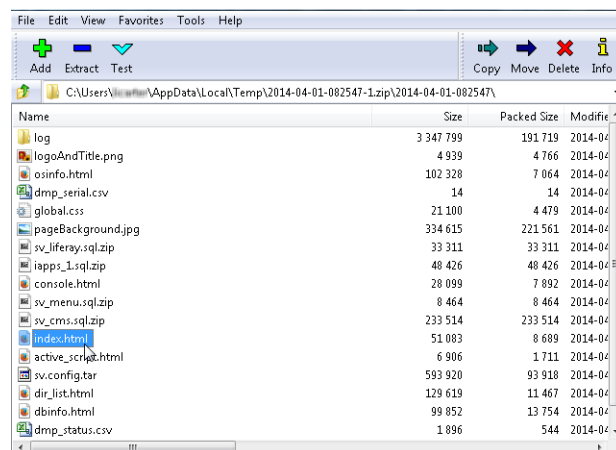
Viewing the Contents of the Zip File

Once you have downloaded the report file to your PC, you will have a .zip file. You can email it to Cisco support as is.

To view the contents of a downloaded file, complete the following steps:

- Step 1** Double-click the file to open the .zip file archive manager. The contents of this file depends on the file compression software program installed on your PC. [Figure 3](#) shows an example of a common Microsoft Windows compression file manager, where the .zip file has been opened to view the contents.

Figure 3 Windows Compression File Manager Example



- Step 2** Click **Extract** and load all of the files in the archive to a new directory on your local drive.
- Step 3** Navigate to the directory that you just created and locate a file named **index.html**. Double-click the file and it will open in your internet browser.
- Step 4** Click links from the browser page to view the rest of the report.

**Tip**

In the case of the heap dump and log file reports, there is not an “index.html” file. Simply navigate down the levels of folders until you see the log files of interest.
