

Installing Cisco StadiumVision Mobile Software for the First Time

First Published: May 26, 2015 Revised: June 12, 2015

This module provides instructions for installing Cisco StadiumVision Mobile Reporter or Cisco StadiumVision Mobile Streamer software on the Cisco UCS C220, as well as the requirements for installing Cisco StadiumVision Mobile software on a VM (virtual machine), and contains the following sections:

- Installation Tasks, page 9
- Configuring the Network Setup, page 13
- What To Do Next, page 16

Prerequisites

Refer to the release notes for Cisco StadiumVision Mobile for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.

Cisco UCS C220 Servers

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

• Your new server is installed in its production location. For more information, see the *Cisco UCS C220 Server Installation and Service Guide* available at:

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C220/install/C220.pdf

- You have completed the initial server setup and configured the Cisco UCS C-Series Integrated Management Controller (CIMC) interface.
- To configure the CIMC, you will need an additional IP address for the server and should be prepared to change the default login and password. Be sure that the server is configured for standalone mode with the following settings:
 - DHCP—Disabled
 - NIC redundancy-None
 - Boot order-Virtual CD/DVD, HDD

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

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



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

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

When using a Cisco UCS C220 server, observe the following guidelines before starting the installation:



Do not alter the RAID configuration prior to installation

• Verify the boot order in the BIOS (by pressing **F2** while booting) prior to installation



If you are doing a fresh installation on a previously configured system, a full install will erase the Cisco StadiumVision Mobile Streamer or Cisco StadiumVision Mobile Reporter configuration. Perform a backup prior to installing to preserve configuration data. See the *Cisco StadiumVision Mobile Streamer Administration Guide* or *Cisco StadiumVision Mobile Reporter Administration Guide* for instructions on performing a backup.

Virtualized Server Environment

Installing Cisco StadiumVision Mobile in a virtualized server environment includes setting up your server environment, running the full ISO for Cisco StadiumVision Mobile, and configuring the network. For more information see the "Hardware Prerequisites" section on page 2, the "Installing on a Virtual Server for the First Time" section on page 5, in the "Getting Started Installing or Upgrading Cisco StadiumVision Mobile Software" module.

Installation Tasks

This section provides a high-level overview of the installation process, and contains the following sections.

- Obtaining the ISO File, page 9
- Installing from the Hard Drive, page 9
- Installing using CIMC, page 10
- Installing on a Virtual Server with Release 2.1 for the First Time, page 13
- Configuring the Network Setup, page 13
- Logging into the TUI, page 16
- Setting the Server Time Zone, page 16
- Setting the Server Date and Time, page 17
- Configuring NTP, page 17
- Removing the Undisciplined Local Clock, page 17

Table 4 lists the platform, type of media, and file to use to perform a fresh installation.

Table 4 Cisco StadiumVision Mobile Fresh Installation Media and ISO File Type

Product	Platform	Media	File to Use
Cisco StadiumVision Mobile Streamer or Cisco	Cisco UCS C220	Hard drive	Full ISO
Stadiumvision Mobile Reporter	Cisco UCS C220	CIMC remote mount	

Obtaining the ISO File

Obtaining the Full ISO from stadiumvision-pm@cisco.com if you need the full install ISO file.

Installing from the Hard Drive

To install from the hard drive, complete the following steps:

- **Step 1** Be sure the CIMC firmware is up to date; configure CIMC (see "Appendix A: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server").
- **Step 2** Power on the server.
- **Step 3** When the server console shows a login prompt proceed to the "Configuring the Network Setup" section on page 13.



Cisco StadiumVision Mobile Reporter and Cisco StadiumVision Mobile Streamer come preinstalled with a released image of Cisco StadiumVision Mobile software. Depending on the timing of your hardware shipment with available software releases, this image might not be the latest released version. Therefore, after you install your hardware, it is important that you power on and access the Cisco StadiumVision Mobile software to verify the software version. As necessary, you can upgrade the software following the guidelines in this guide and in the Cisco StadiumVision Mobile Release Notes.

Installing using CIMC

To install using CIMC, complete the following steps:

- **Step 1** Verify that CIMC firmware and BIOS are up to date.
- **Step 2** Configure CIMC (see "Appendix A: CIMC Configuration and Firmware Upgrade Guidelines on the Cisco UCS C220 Server").



At this release, the CIMC 1.5.1 firmware version is the minimum tested version.

- Step 3 Connect a second Ethernet cable to the CIMC Ethernet port marked M.
- **Step 4** Power on the server.
- **Step 5** Start CIMC and perform a virtual DVD mount:
 - a. Access CIMC from a web browser: https://ip address/login.html
 - b. Click the Add Exception button.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified. What Should I Do? If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Getme out of here! Technical Details I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	You have asked Firefox to connect securely to 10.194.168.139 , but we can't confirm that your connectio is secure.
What Should I Do? If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Getme out of here! * Technical Details * I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Get me out of here Technical Details I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	What Should I Do?
Get me out of herel	If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Technical Details I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if yo trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	Get me out of here!
I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	Technical Details
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if yo trust the site, this error could mean that someone is tampering with your connection. Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	I Understand the Risks
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if yo trust the site, this error could mean that someone is tampering with your connection.

- c. Click Confirm Security Exception to get to the CIMC login page. The default login credentials are: user: admin password: password
- d. Click on the Launch KVM Console at the top of the CIMC interface to launch the KVM console.

erall Server Status 💦 💍 👌 🤳 🛛 🤅	C 3 3 📕 0 0				
Server Sun Launch K	VM Console				
erver Admin Immary ventory insors stem Event Log mote Presence OS wer Policies ult Summary Turn Off Locator LED	Server Projecteds Product Name: Serial Number: PID: UUID: BIOS Version: Description: Server Status Power Status: Overall Server Status: Temperature: Power Supplies: Fans: Locator LED:	UCS C220 M3S FCH1615V0FX UCSC-C220-M35 A778AA13-306C-4AC1-8843-28741EE2E147 C220M3.1.4.4c.0 (Build Date: 02/22/2012)			
	Cisco Integrated Manage Hostname: TE Address: Firmware Version: Concent Time (UTC):	ment Controller (CIMC) Information ucs-c220-m3 10.194.168.69 C4:64:1-39:86:54 1.4(4a) Mon-ect 10 22:15:15 2012			

The KVM tab provides a view of the system diagnostics or command prompt execution. The Virtual Media tab provides the virtual CD/DVD setup for ISO installation.

- e. Click on Add Image tab under the KVM Console Virtual Media tab.
- f. Navigate to the ISO file.

Note

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



ſ

If the installation seems to suspend operation on a Cisco UCS C220, you might need to restart the installation by remapping the ISO image, and power cycling the Cisco UCS C220 server.

- g. Click the check box for the Mapped option under Client View to select the ISO source.
- h. Confirm that the Virtual CD/DVD has been added under the Virtual Media tab, Virtual CD/DVD.

/M Virtual Med	lia				
Client View					
Mapped Re	ad Only Drive				Exit
	🔟 🏼 🛃 C:\Users\vatu)Desktop\SVM-pr	oject'ISO\SVM	-REPORT-FULL-1.2.0	
					Create Image
					Add Image
					Remove Image
					Details ±
•	1			•	Details ±
∢ Details				•	Details #
Cetails TargetDrive	MappedTo	ReadBytes	WriteBytes	Duration	Details *
	MappedTo	ReadBytes	WriteBytes 0	Duration 00:00:03	Details ±
	MappedTo C:Users'vatu'Deskto Not mapped	ReadBytes	WriteBytes 0	Duration	Details ±
	MappedTo C:Users'vatu'Deskte Not mapped Not mapped	ReadBytes	WriteBytes 0	Duration	Details ±

- i. Double click on **Virtual CD/DVD** and observe the read bytes counter increasing (this refreshes the read bytes).
- j. Close the KVM tab to start viewing the installation process.
- **k.** On the CIMC interface under Server Summary, click **Power Cycle Server** to start the installation process.



I. On the KVM Console/KVM terminal, confirm that the system is restarting and booting up from the Virtual CD/DVD.



Step 6 When the server console shows a login prompt proceed to the "Configuring the Network Setup" section on page 13.

Installing on a Virtual Server with Release 2.1 for the First Time

The installation process for a virtual server running Cisco StadiumVision Mobile software release 2.1 for the first time involves the following tasks:

- Verify that your virtual server meets the requirements listed in Table 1 and Table 2 in the "Getting Started Installing or Upgrading Cisco StadiumVision Mobile Software" module.
- Install VMWare ESX hypervisor software.

S, Note

I

Any VMware license that does not allow your virtual machine to be set to the minimum requirements described in Table 1 and Table 2 in the "Getting Started Installing or Upgrading Cisco StadiumVision Mobile Software" module is not supported.

- Load the Cisco StadiumVision Mobile Release 2.1 (full ISO).
- Run the installation.
- After installation, restart the Streamer Service or reboot by using the TUI.

Configuring the Network Setup

This part of the installation process is common to all platforms and all Cisco StadiumVision Mobile software, and should be done after the initial software installation.

1

To configure the network setup, complete the following steps:

Step 1 Select Network Configuration from the menu.

Note	

The network configuration window displays for approximately sixty minutes. If the window disappears, continue the network configuration using the TUI.

Step 2 Select Edit Devices and press Enter.

View Macros Tools Help Virtual Media
Select Action
Edit Devices
Save&Quit Quit
Tab>/ <alt-tab> between elements <space> selects <f12> next screen</f12></space></alt-tab>

Step 3 Select eth0 and press Enter.





The Linux screen is mislabeled "Devernet Configuration."

<u>Note</u>

The Cisco StadiumVision Mobile Streamer or Cisco StadiumVision Mobile Reporter must use a static IP address.

ſ	Deverne	t Configuration	_
	Name Device Use DHCP Static IP Netmask Default gateway	eth0 eth8 18.194.168.140 255.255.255.224 IP 10.194.168.129 Cance1	
<tab>∕<alt-tab> b</alt-tab></tab>	etween elements	¦ ⟨Space⟩ selects	; ⟨F12⟩ next screen

- **Step 5** Select **OK** and press the Enter key.
- **Step 6** Select **Edit DNS configuration** and press **Enter**.



Step 7 Enter DNS information. When done, select OK, and press Enter.

KVM Virtual Media	DNS configuration Hostname Primary DNS Secondary DNS Tertiary DNS Search Cancel
<tab>/<alt-tab> betwe</alt-tab></tab>	n elements <space> selects <f12> next screen</f12></space>

Note Do not use a period ('.') as part of the hostname.

- Step 8 Select Save & Quit and press Enter.
- **Step 9** Select **Exit** and press **Enter**.

I

After this step, the Cisco StadiumVision Mobile software installs and the system reboots. This process takes up to 30 minutes. The installation should be completed. Validate the installation by logging into the Cisco StadiumVision Mobile Streamer or Cisco StadiumVision Mobile Reporter.

What To Do Next

This section describes procedures to perform after successfully installing Cisco StadiumVision Mobile software, and contains the following topics:

- Logging into the TUI, page 16
- Setting the Server Time Zone, page 16
- Setting the Server Date and Time, page 17
- Configuring NTP, page 17 ٠
- Removing the Undisciplined Local Clock, page 17

Logging into the TUI

To access the TUI, you need either physical console access or an SSH client such as PUTTY. Log in from the console or over SSH with the following default credentials, using the IP address of the Cisco StadiumVision Mobile Reporter or Cisco StadiumVision Mobile Streamer:

username = installer password = cisco!123

Setting the Server Time Zone

To set the server time zone, complete the following tasks:

۵. Note

Set the time zone for both the Cisco StadiumVision Mobile Reporter and the Cisco StadiumVision Mobile Streamer. The default time zone is Eastern Standard Time (EST).

- Log into the TUI using the procedure in the "Logging into the TUI" section. Step 1
- Step 2 In the TUI, go to System Settings > Date and Time Settings > Change timezone as shown in the following figure.

S	StadiumVision Mobile F	eporter Configuration Menu
Hostname:	reporter	
IP address:	28, 284, 178, 285	
Software version:	2.0.1-1	Time: Fri May 22 13:41:46 PDT 201
Main Menu > Syste	em Settings > Date and	Time Settings
 Main Menu > Syste P	em Settings > Date and Please choose one of t	<pre>I Time Settings the following menu options:</pre>
Main Menu > Syste P	em Settings > Date and Please choose one of t a) Set syste	I Time Settings :he following menu options: :m date
Main Menu > Syste P	em Settings > Date and Please choose one of t a) Set syste b) Chance ti	I Time Settings The following menu options: The date The date
Main Menu > Syste P	em Settings > Date and Please choose one of t a) Set syste b) Change ti c) Set NTP s	I Time Settings the following menu options: tm date mezone erver address
Main Menu > Syste	em Settings > Date and Please choose one of t a) Set syste b) Change ti c) Set NTP s d) Modify NT	I Time Settings the following menu options: tm date mezone terver address P configuration file

Choose the appropriate timezone from the list and enter the corresponding number.

Setting the Server Date and Time

To set the server date and time, complete the following tasks:

Set	t the server date and time for both the Cisco StadiumVision Mobile Reporter and the
Cisco StadiumVision Mobile Streamer.	
Lo	g into the TUI using the procedure in the "Logging into the TUI" section.
Lo In	g into the TUI using the procedure in the "Logging into the TUI" section. the TUI, go to System Settings > Date and Time Settings > Set system date .

Configuring NTP

To configure the Network Time Protocol (NTP), complete the following tasks:

Note

ſ

Configure NTP for both the Cisco StadiumVision Mobile Reporter and the Cisco StadiumVision Mobile Streamer.

- Step 1 Log into the TUI using the procedure in the "Logging into the TUI" section.
- **Step 2** In the TUI, go to **System Settings > Date and Time Settings > Set NTP server address**.
- **Step 3** Set the NTP server address.



For the Cisco StadiumVision Mobile Reporter, it is critical that NTP be properly configured in order to provide accurate reports.

Removing the Undisciplined Local Clock

To remove the undisciplined local clock, complete the following tasks:

Note	Remove the undisciplined local clock for both the Cisco StadiumVision Mobile Reporter and the Cisco StadiumVision Mobile Streamer if you are running them as a leaf node in a NTP network.
Step 1	Log into the TUI using the procedure in the "Logging into the TUI" section.
Step 2	In the TUI, go to System Settings > Date and Time Settings > Modify NTP configuration file.
Step 3	Delete the following section to remove the undisciplined clock:

1

Undisciplined Local Clock. This is a fake driver intended for backup
and when no outside source of synchronized time is available.
server 127.127.1.0 # local clock
fudge 127.127.1.0 stratum 10

Step 4 Repeat the steps above to remove the undisciplined clock from both the Cisco StadiumVision Mobile

Reporter and the Cisco StadiumVision Mobile Streamer.



Remove the undisciplined local clock on any new installation or upgrade that sets an NTP server.