Using the TUI Upgrade Utility

First Published: May 29, 2012

Note If you are upgrading an existing Cisco StadiumVision Director server from Release 2.4 to Release 3.0, see the "Upgrading a Cisco StadiumVision Director Server from Release 2.4 SP1 to Release 3.0" module first.

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

This module includes the following topics:

Best Practices

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

- Choose an appropriate down time to perform the upgrade on the Cisco StadiumVision Director server when there is adequate time to complete and verify the upgrade before any scheduled events and to allow time to resolve any unexpected issues that might occur.
- Refer to the *Release Notes for Cisco StadiumVision Director Release 3.0* for the latest information about hardware and software requirements, changes, important notes, and caveats for your software release.
- Pay particular attention to the required hardware and software versions for other devices supporting your Cisco StadiumVision solution and be sure that you upgrade those devices as needed. For example, generally only certain firmware versions are supported for the DMP hardware, or a new firmware version is needed to provide additional functionality supported by the Cisco StadiumVision Director software.

- Perform a backup and restore of the primary and secondary servers:
  - Perform a backup of the currently active primary server.
  - Restore the backup data onto the standby secondary server.
  - Promote the secondary server to primary.
  - Access the promoted secondary server to perform the upgrade.

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

Prerequisites

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

- Your server is running a minimum of Cisco StadiumVision Director Release 2.4.0-168 or higher.
- If you are upgrading your server from Release 2.4, you are following the requirements and tasks described in the "Upgrading a Cisco StadiumVision Director Server from Release 2.4 SP1 to Release 3.0" module in this guide.
- You have the IP address for the Cisco StadiumVision Director server where you want to upload the ISO upgrade image. You will need to use this information as part of the URL to access the ISO upload utility.
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the *Cisco StadiumVision Release Notes for Release 3.0*.
- You have an installer account on the Cisco StadiumVision Director server.

Information About Using the TUI Upgrade Utility to Update an Existing Release 3.0 Server

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

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

ISO Upgrade Files

The ISO upgrade files are stored in the following location:

/var/www/cgi-bin/ISOupload

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

Disk Maintenance

There is no automatic aging of ISO upgrade files or any utility to remove files from the Cisco StadiumVision Director server.

You should periodically maintain your disk storage by manually removing any ISO upgrade files that you no longer need.

Upgrade Tasks

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

- Downloading ISO Upgrade Files from Cisco.com, page 27 (required)
- Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server, page 28 (required)
- Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server, page 30 (required)
- Verifying the Upgrade, page 33 (required)

Downloading ISO Upgrade Files from Cisco.com

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

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

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

http://www.cisco.com/cisco/software/release.html?mdfid=283489263&flowid=31962&softwareid=283866237&release=3.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

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

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

Table 1 shows the filename conventions used for ISO upgrades.

Table 1 ISO Upgrade Filename Conventions

Hardware Product ID	Filename Convention[1]
64-bit Model SV-DIRECTOR-K9 or SV-PLATFORM2=	• SV-DIRECTOR-UPGRADE-3.0.0-*nnn*.x86_64.iso • SV-DIRECTOR-UPGRADE-3.0.0-*nnn*.x86_64.iso.md5sum

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

Table 2 shows the filename conventions used for service pack (SP) ISO upgrades.

Table 2 SP Filename Conventions [1]

Hardware Product ID	Filename Convention
64-bit Model SV-DIRECTOR-K9 or SV-PLATFORM2=	• SV-DIRECTOR-SPx-3.0.0.x86_64.iso • SV-DIRECTOR-SPx-3.0.0.x86_64.iso.md5sum

[1] "x' represents the ordered number of the service pack file. The first service pack is SP1.

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

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

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

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

Uploading an ISO Upgrade File to the Cisco StadiumVision Director Server

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

Prerequisites

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

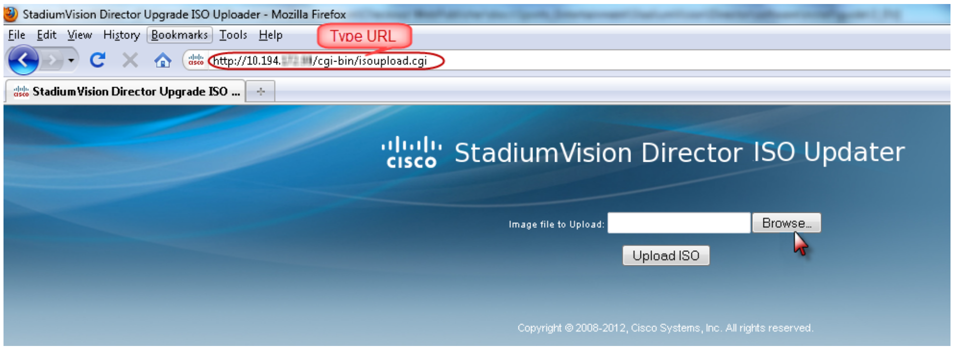
To upload an ISO upgrade file to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Log into Cisco StadiumVision Director as an administrator.

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

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

Figure 1 ISO Updater Utility



StadiumVision Director Upgrade ISO Uploader - Mozilla Firefox

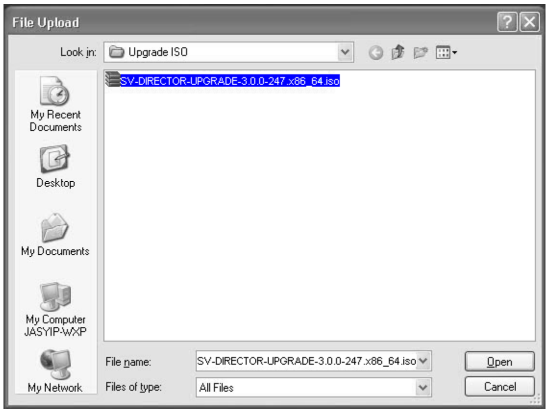
http://10.194.[redacted]/cgi-bin/isoupload.cgi

File Edit View History Bookmarks Tools Help
Type URL
StadiumVision Director Upgrade ISO ...
cisco StadiumVision Director ISO Updater
Image file to Upload:
Browse...
Upload ISO
Copyright © 2008-2012, Cisco Systems, Inc. All rights reserved.

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

Step 4 From the File Upload dialog box, navigate to the location of the ISO upgrade file that you downloaded from Cisco.com. Select the file that you want to upload and click **Open**. Figure 2 shows an example of selection of a 64-bit ISO upgrade file.

Figure 2 File Upload Dialog Box



File Upload

Look in: Upgrade ISO

SV-DIRECTOR-UPGRADE-3.0.0-247.x86_64.iso

File name: SV-DIRECTOR-UPGRADE-3.0.0-247.x86_64.iso

Files of type: All Files

Step 5 Click the **Upload ISO** button (Figure 3). The file is sent to the server.

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

Figure 3 ISO File Selection and Upload

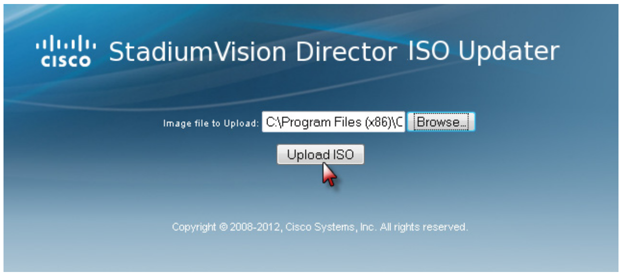


Image file to Upload: C:\Program Files (x86)\C

cisco StadiumVision Director ISO Updater
Browse...
Upload ISO
Copyright © 2008-2012, Cisco Systems, Inc. All rights reserved.

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

- Image integrity is verified before an image is stored on the server. When the image is validated and uploaded successfully, a message is displayed stating that the ISO image has been uploaded.
- The image upload failed for some reason and you will need to retry the upload again.

Installing the ISO Upgrade Image on the Cisco StadiumVision Director Server

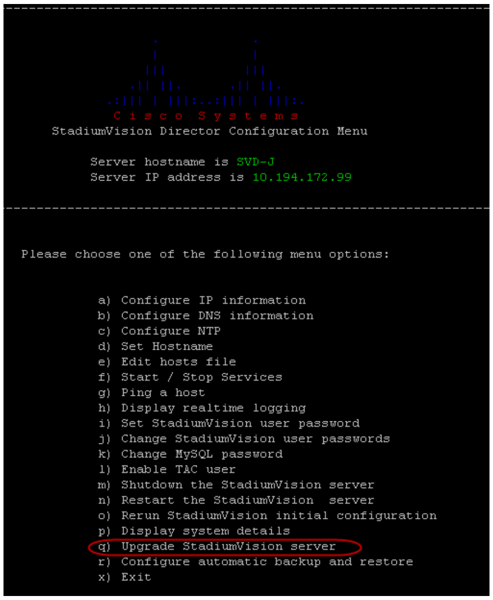
To install the ISO upgrade image on the Cisco StadiumVision Director server, complete the following steps:

Step 1 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 Cisco StadiumVision Director server using the IP address for your server.

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

Step 3 When the StadiumVision Director Configuration menu appears, type **q** and press Enter (Figure 4):

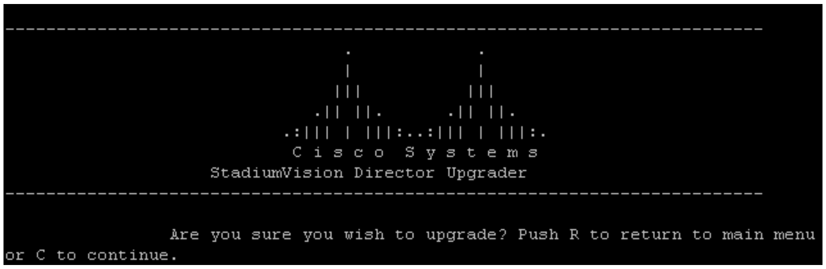
Figure 4 TUI Main Menu Option for Upgrade of Cisco StadiumVision Server



```
---------------------------------------------------------------

                  .            .
                  |            |
                 |||          |||
               .|| ||.      .|| ||.
            .:||| | |||:..:||| | |||:.
             C i s c o  S y s t e m s
      StadiumVision Director Configuration Menu

           Server hostname is SVD-J
           Server IP address is 10.194.172.99

---------------------------------------------------------------


  Please choose one of the following menu options:


            a) Configure IP information
            b) Configure DNS information
            c) Configure NTP
            d) Set Hostname
            e) Edit hosts file
            f) Start / Stop Services
            g) Ping a host
            h) Display realtime logging
            i) Set StadiumVision user password
            j) Change StadiumVision user passwords
            k) Change MySQL password
            l) Enable TAC user
            m) Shutdown the StadiumVision server
            n) Restart the StadiumVision  server
            o) Rerun StadiumVision initial configuration
            p) Display system details
            q) Upgrade StadiumVision server
            r) Configure automatic backup and restore
            x) Exit
```

Step 4 When the upgrade configuration confirmation prompt appears, type **c** to continue (Figure 5):

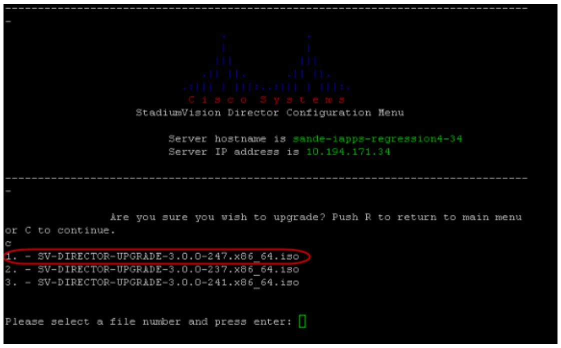
Figure 5 TUI Upgrade Configuration Confirmation



```
--------------------------------------------------------------------------
                                .            .
                                |            |
                               |||          |||
                             .|| ||.      .|| ||.
                          .:||| | |||:..:||| | |||:.
                           C i s c o  S y s t e m s
                    StadiumVision Director Upgrader
--------------------------------------------------------------------------

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

Step 5 All of the ISO upgrade files that you have uploaded are displayed with a sequence number and the image name. Type the sequence number that corresponds to the image that you want to install, and press **Enter**. Figure 6 shows an example of selection of a 64-bit ISO upgrade file for installation.

Figure 6 ISO Upgrade Image File List

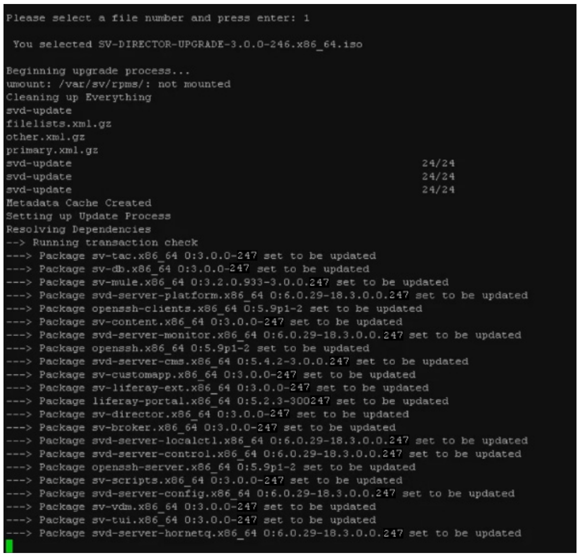


```
--------------------------------------------------------------------------------
-
                                .            .
                                |            |
                               |||          |||
                             .|| ||.      .|| ||.
                          .:||| | |||:..:||| | |||:.
                           C i s c o  S y s t e m s
                    StadiumVision Director Configuration Menu

                         Server hostname is sande-iapps-regression4-34
                         Server IP address is 10.194.171.34

--------------------------------------------------------------------------------
-

                Are you sure you wish to upgrade? Push R to return to main menu
or C to continue.
c
1. - SV-DIRECTOR-UPGRADE-3.0.0-247.x86_64.iso
2. - SV-DIRECTOR-UPGRADE-3.0.0-237.x86_64.iso
3. - SV-DIRECTOR-UPGRADE-3.0.0-241.x86_64.iso


Please select a file number and press enter:
```

The upgrade process begins (Figure 7).

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

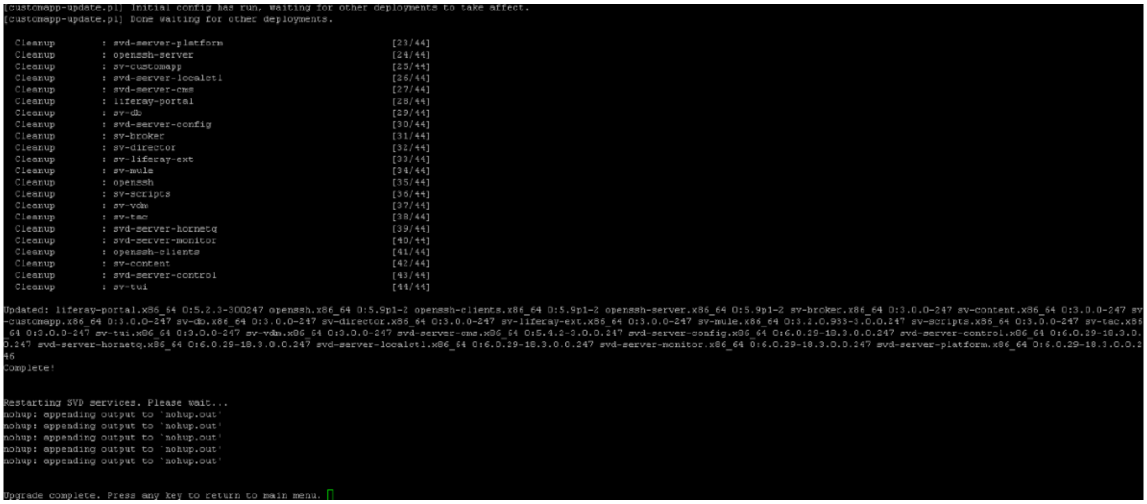
Figure 7 Start of ISO Upgrade Process



```
Please select a file number and press enter: 1

 You selected SV-DIRECTOR-UPGRADE-3.0.0-246.x86_64.iso

Beginning upgrade process...
umount: /var/sv/rpms/: not mounted
Cleaning up Everything
svd-update
filelists.xml.gz
other.xml.gz
primary.xml.gz
svd-update                                                    24/24
svd-update                                                    24/24
svd-update                                                    24/24
Metadata Cache Created
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package sv-tac.x86_64 0:3.0.0-247 set to be updated
---> Package sv-db.x86_64 0:3.0.0-247 set to be updated
---> Package sv-mule.x86_64 0:3.2.0.933-3.0.0.247 set to be updated
---> Package svd-server-platform.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
---> Package openssh-clients.x86_64 0:5.9p1-2 set to be updated
---> Package sv-content.x86_64 0:3.0.0-247 set to be updated
---> Package svd-server-monitor.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
---> Package openssh.x86_64 0:5.9p1-2 set to be updated
---> Package svd-server-cms.x86_64 0:5.4.2-3.0.0.247 set to be updated
---> Package sv-customapp.x86_64 0:3.0.0-247 set to be updated
---> Package sv-liferay-ext.x86_64 0:3.0.0-247 set to be updated
---> Package liferay-portal.x86_64 0:5.2.3-300247 set to be updated
---> Package sv-director.x86_64 0:3.0.0-247 set to be updated
---> Package sv-broker.x86_64 0:3.0.0-247 set to be updated
---> Package svd-server-localctl.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
---> Package svd-server-control.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
---> Package openssh-server.x86_64 0:5.9p1-2 set to be updated
---> Package sv-scripts.x86_64 0:3.0.0-247 set to be updated
---> Package svd-server-config.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
---> Package sv-vdm.x86_64 0:3.0.0-247 set to be updated
---> Package sv-tui.x86_64 0:3.0.0-247 set to be updated
---> Package svd-server-hornetq.x86_64 0:6.0.29-18.3.0.0.247 set to be updated
```

Step 6 When the “Upgrade complete” message appears, press any key. (Figure 8):

Figure 8 End of ISO Upgrade Process



```
[customapp-update.pl] Initial config has run, waiting for other deployments to take affect.
[customapp-update.pl] Done waiting for other deployments.

  Cleanup        : svd-server-platform                          [23/44]
  Cleanup        : openssh-server                               [24/44]
  Cleanup        : sv-customapp                                 [25/44]
  Cleanup        : svd-server-localctl                          [26/44]
  Cleanup        : svd-server-cms                               [27/44]
  Cleanup        : liferay-portal                               [28/44]
  Cleanup        : sv-db                                        [29/44]
  Cleanup        : svd-server-config                            [30/44]
  Cleanup        : sv-broker                                    [31/44]
  Cleanup        : sv-director                                  [32/44]
  Cleanup        : sv-liferay-ext                               [33/44]
  Cleanup        : sv-mule                                      [34/44]
  Cleanup        : openssh                                      [35/44]
  Cleanup        : sv-scripts                                   [36/44]
  Cleanup        : sv-vdm                                       [37/44]
  Cleanup        : sv-tac                                       [38/44]
  Cleanup        : svd-server-hornetq                           [39/44]
  Cleanup        : svd-server-monitor                           [40/44]
  Cleanup        : openssh-clients                              [41/44]
  Cleanup        : sv-content                                   [42/44]
  Cleanup        : svd-server-control                           [43/44]
  Cleanup        : sv-tui                                       [44/44]

Updated: liferay-portal.x86_64 0:5.2.3-300247 openssh.x86_64 0:5.9p1-2 openssh-clients.x86_64 0:5.9p1-2 openssh-server.x86_64 0:5.9p1-2 sv-broker.x86_64 0:3.0.0-247 sv-content.x86_64 0:3.0.0-247 sv
-customapp.x86_64 0:3.0.0-247 sv-db.x86_64 0:3.0.0-247 sv-director.x86_64 0:3.0.0-247 sv-liferay-ext.x86_64 0:3.0.0-247 sv-mule.x86_64 0:3.2.0.933-3.0.0.247 sv-scripts.x86_64 0:3.0.0-247 sv-tac.x86
_64 0:3.0.0-247 sv-tui.x86_64 0:3.0.0-247 sv-vdm.x86_64 0:3.0.0-247 svd-server-cms.x86_64 0:5.4.2-3.0.0.247 svd-server-config.x86_64 0:6.0.29-18.3.0.0.247 svd-server-control.x86_64 0:6.0.29-18.3.0.
0.247 svd-server-hornetq.x86_64 0:6.0.29-18.3.0.0.247 svd-server-localctl.x86_64 0:6.0.29-18.3.0.0.247 svd-server-monitor.x86_64 0:6.0.29-18.3.0.0.247 svd-server-platform.x86_64 0:6.0.29-18.3.0.0.2
46
Complete!


Restarting SVD services. Please wait...
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'


Upgrade complete. Press any key to return to main menu.
```

Note There is no need to reboot the Cisco StadiumVision Director server. The server is restarted automatically after the upgrade is complete.

Step 7 Exit the TUI and go on to the “Verifying the Upgrade” section on page 33.

Verifying the Upgrade

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 33 (required)
- Importing the Security Certificate, page 34 (required)
- Logging Into Cisco StadiumVision Director, page 35 (required)
- Verifying the Control Panel and Other Menus, page 36 (required)
- Checking for Duplicate MAC Address Entries, page 37 (required)
- Verifying that Services are Running, page 37 (required)
- Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check, page 38 (required)
- Verifying DMPs, Groups, and Zones in the Management Dashboard, page 39 (required)
- Verifying the Multicast Configuration, page 40 (required)
- Setting Up the Quest Venue Manager to Send Updates to Cisco StadiumVision Director Server, page 40 (required if using Quest for commerce integration)

Clearing the Browser Cache

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

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

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

The Clear Recent History dialog box appears.

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

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

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

Step 4 Click **Clear Now**.

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

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

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

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

Step 3 Click **Delete**.

Importing the Security Certificate

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

Importing the Security Certificate for Microsoft IE

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

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

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

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

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

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

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

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

Step 8 Click **Finish**.

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

Confirm that a dialog stating “The import was successful.” appears.

Step 10 Close all Microsoft IE windows.

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

Adding a Security Exception for Mozilla Firefox

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

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

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

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

Step 4 Close all Mozilla Firefox windows.

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

Logging Into Cisco StadiumVision Director

To verify that the upgrade to Cisco StadiumVision Director Release 2.4 was successful, and that Cisco StadiumVision Director is up and operating, complete the following steps:

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

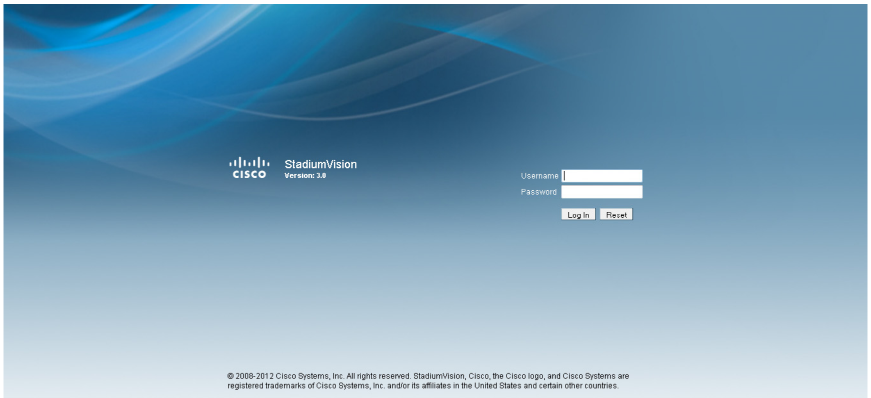
```
https://x.x.x.x/StadiumVision/login.jsp
```

or alternatively,

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

The Cisco StadiumVision Director login screen appears (Figure 9).

Figure 9 Cisco StadiumVision Director Login Screen



© 2008-2012 Cisco Systems, Inc. All rights reserved. StadiumVision, Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 2 Verify that the Version 3.0 is displayed.

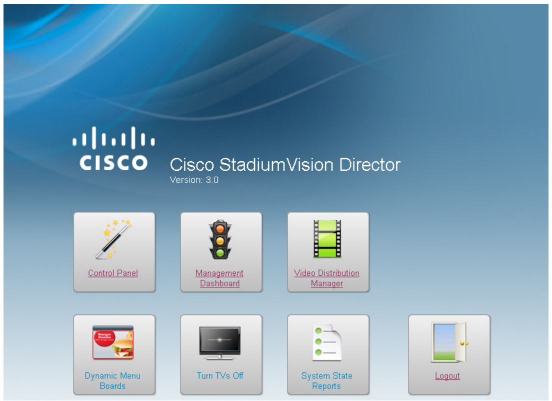
Tip If your window is not displaying Version 3.0, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 33.

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

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

The Cisco StadiumVision Director Main Menu screen appears (Figure 10).

Figure 10 Cisco StadiumVision Director Main Menu



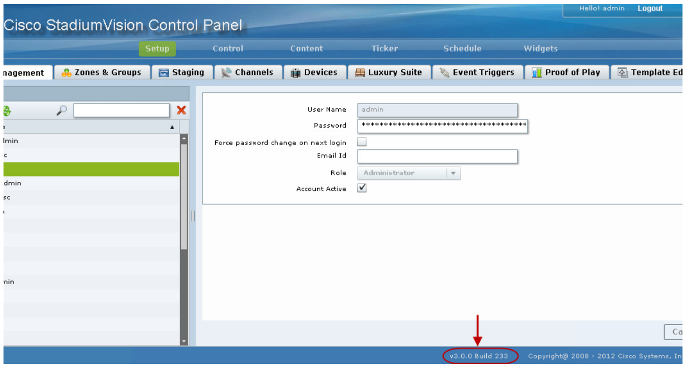
Verifying the Control Panel and Other Menus

To verify the control panel, complete the following steps:

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

After a few moments of loading resources, the Cisco StadiumVision Control Panel Setup screen will open in a new window (Figure 11).

Figure 11 Cisco StadiumVision Control Panel



User Name admin
Password ***********************************
Force password change on next login ☐
Email Id
Role Administrator
Account Active ☑

v3.0.0 Build 233 Copyright@ 2008 - 2012 Cisco Systems, In

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

Tip If your window is not displaying the appropriate version and build that you loaded, be sure that you have cleared the browser cache as describe in the "Clearing the Browser Cache" section on page 33.

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

Checking for Duplicate MAC Address Entries

Cisco StadiumVision Director does not support duplicate MAC addresses for the DMPs. After you have upgraded your software, check the following file for any duplicates:

/var/sv/db/mysql/upgrade-invalidmac.csv

Tip You can also run the GetStatus operation on selected DMPs in the Management Dashboard to update the MAC address for the selected DMPs in the Cisco StadiumVision Director database.

Verifying that Services are Running

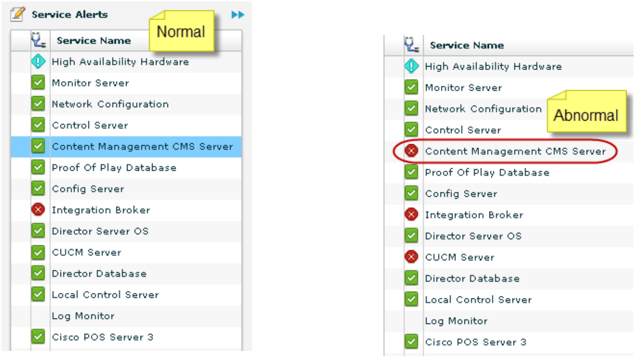
After you upgrade, go to the Management Dashboard to verify that all of the primary Cisco StadiumVision Director services are running.

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

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

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

Figure 12 Verifying Normal Service States



Service Alerts

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

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

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

Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check

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

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

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

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

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

Figure 13 shows how to configure the Assigned VLAN property under the 4310 Settings for DMPs that are not located on the same VLAN using the "$svd_ignore" string.

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

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

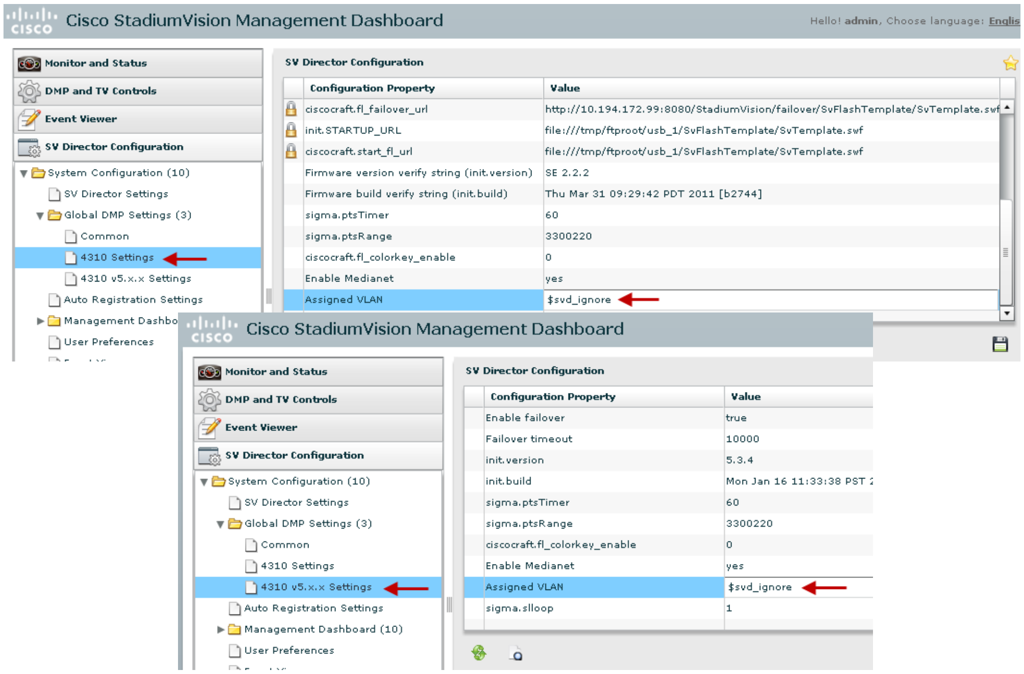
Step 1 Go to the Management Dashboard, and click **SV Director Configuration** > **System Configuration** > **Global DMP Settings**.

Step 2 Complete both of the following steps, as shown in Figure 13:

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

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

Figure 13 Assigned VLAN Property Configuration for DMPs



SV Director Configuration

Configuration Property	Value
ciscocraft.fl_failover_url	http://10.194.172.99:8080/StadiumVision/failover/SvFlashTemplate/SvTemplate.swf
init.STARTUP_URL	file:///tmp/ftproot/usb_1/SvFlashTemplate/SvTemplate.swf
ciscocraft.start_fl_url	file:///tmp/ftproot/usb_1/SvFlashTemplate/SvTemplate.swf
Firmware version verify string (init.version)	SE 2.2.2
Firmware build verify string (init.build)	Thu Mar 31 09:29:42 PDT 2011 [b2744]
sigma.ptsTimer	60
sigma.ptsRange	3300220
ciscocraft.fl_colorkey_enable	0
Enable Medianet	yes
Assigned VLAN	$svd_ignore

SV Director Configuration

Configuration Property	Value
Enable failover	true
Failover timeout	10000
init.version	5.3.4
init.build	Mon Jan 16 11:33:38 PST 2
sigma.ptsTimer	60
sigma.ptsRange	3300220
ciscocraft.fl_colorkey_enable	0
Enable Medianet	yes
Assigned VLAN	$svd_ignore
sigma.slloop	1

Step 3 Click the Save icon.

Verifying DMPs, Groups, and Zones in the Management Dashboard

Note Before you verify DMP status, be sure that you have set the Assigned VLAN property for your DMP 4310s so that the VLAN compliance check can be performed. For more information, see the "Configuring the DMP 4310 Assigned VLAN Property for VLAN Compliance Check" section on page 38.

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

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

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

Step 3 Run an Initial Config to enable the Video Distribution Manager (VDM) configuration using the following dashboard command path:
DMP and TV Controls > **DMP Install** > **Initial Config**.

Step 4 Run Get Status to confirm that all DMPs have successfully rebooted.

Step 5 Stage the Flash template using the following dashboard command path:
DMP and TV Controls > **DMP Install** > **Stage Template**.

Step 6 Send Global DMP Settings to the DMPs using the following dashboard command path:
DMP and TV Controls > **Global** > **Global DMP Settings**.

Note You must send the Global DMP Settings command twice to reboot the DMPs due to an issue with enabling Medianet services for the first time.

Step 7 Run Get Status to confirm that the DMPs are in good health.

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

Step 8 (Optional) Change the DMP State of healthy DMPs to "Production" using the following dashboard command path:
DMP and TV Controls > **Auto Registration** > **Change DMP State**.

Step 9 Run Get Status to check the DMP state after the change.

Step 10 Investigate any DMPs that are not in "Normal" state.

Verifying the Multicast Configuration

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

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

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

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

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

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

Step 4 Click **Apply**.

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

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

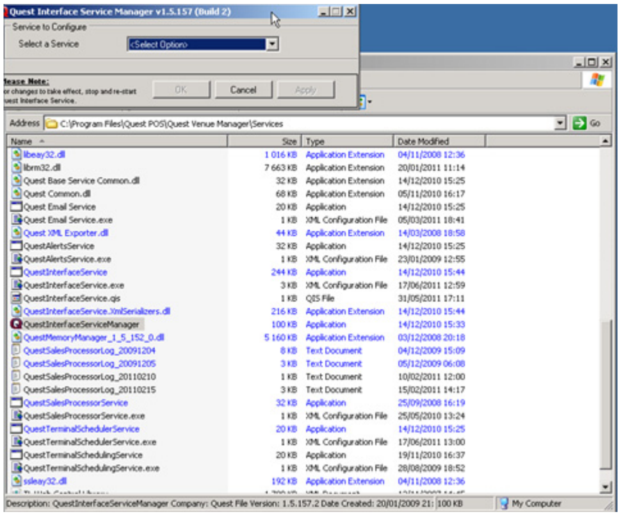
To set up the Quest Venue Manager to send updates to the Cisco StadiumVision Director server, complete the following steps:

Step 1 Access the Quest server.

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

Step 3 Start the executable application program named “QuestInterfaceServiceManager” (Figure 14).

Figure 14 QuestInterfaceServiceManager Application



Quest Interface Service Manager v1.5.157 (Build 2)

Service to Configure

Select a Service: <Select Option>

Please Note:
For changes to take effect, stop and re-start Quest Interface Service.

Address: C:\Program Files\Quest POS\Quest Venue Manager\Services

Name	Size	Type	Date Modified
libeay32.dll	1 016 KB	Application Extension	04/11/2008 12:36
librm32.dll	7 663 KB	Application Extension	20/01/2011 11:14
Quest Base Service Common.dll	32 KB	Application Extension	14/12/2010 15:25
Quest Common.dll	68 KB	Application Extension	05/11/2010 16:17
Quest Email Service	20 KB	Application	14/12/2010 15:25
Quest Email Service.exe	1 KB	XML Configuration File	05/03/2011 18:41
Quest XML Exporter.dll	44 KB	Application Extension	14/03/2008 18:58
QuestAlertsService	32 KB	Application	14/12/2010 15:25
QuestAlertsService.exe	1 KB	XML Configuration File	23/01/2009 12:55
QuestInterfaceService	244 KB	Application	14/12/2010 15:44
QuestInterfaceService.exe	3 KB	XML Configuration File	17/06/2011 12:59
QuestInterfaceService.qis	1 KB	QIS File	31/05/2011 17:11
QuestInterfaceService.XmlSerializers.dll	216 KB	Application Extension	14/12/2010 15:44
QuestInterfaceServiceManager	100 KB	Application	14/12/2010 15:33
QuestMemoryManager_1_5_152_0.dll	5 160 KB	Application Extension	03/12/2008 20:18
QuestSalesProcessorLog_20091204	8 KB	Text Document	04/12/2009 15:09
QuestSalesProcessorLog_20091205	3 KB	Text Document	05/12/2009 06:08
QuestSalesProcessorLog_20110210	1 KB	Text Document	10/02/2011 12:00
QuestSalesProcessorLog_20110215	3 KB	Text Document	15/02/2011 14:17
QuestSalesProcessorService	32 KB	Application	25/09/2008 16:19
QuestSalesProcessorService.exe	1 KB	XML Configuration File	25/05/2010 13:24
QuestTerminalSchedulerService	20 KB	Application	14/12/2010 15:25
QuestTerminalSchedulerService.exe	1 KB	XML Configuration File	17/06/2011 13:00
QuestTerminalSchedulingService	20 KB	Application	19/11/2010 16:37
QuestTerminalSchedulingService.exe	1 KB	XML Configuration File	28/08/2009 18:52
ssleay32.dll	192 KB	Application Extension	04/11/2008 12:36

Description: QuestInterfaceServiceManager Company: Quest File Version: 1.5.157.2 Date Created: 20/01/2009 21: 100 KB My Computer

Step 4 When the Quest Interface Service Manager application window opens, specify the following options (Figure 15):

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

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

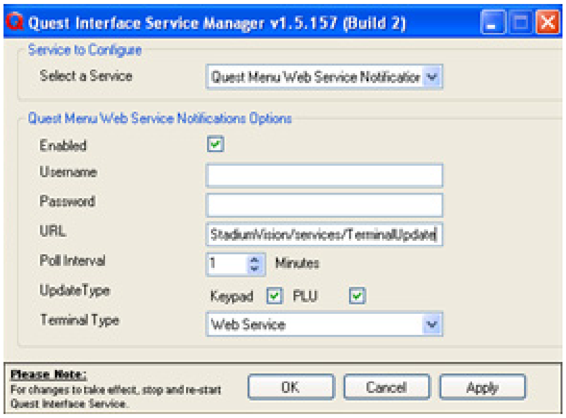
c. In the URL box, enter “**http://svd:8080/StadiumVision/services/TerminalUpdate**.”

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

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

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

Figure 15 Select a Service to Configure



Quest Interface Service Manager v1.5.157 (Build 2)

Service to Configure

Select a Service: Quest Menu Web Service Notificatior

Quest Menu Web Service Notifications Options

Enabled ☑

Username

Password

URL: StadiumVision/services/TerminalUpdate

Poll Interval: 1 Minutes

UpdateType: Keypad ☑ PLU ☑

Terminal Type: Web Service

Please Note:
For changes to take effect, stop and re-start Quest Interface Service.

Step 5 Click **OK**.

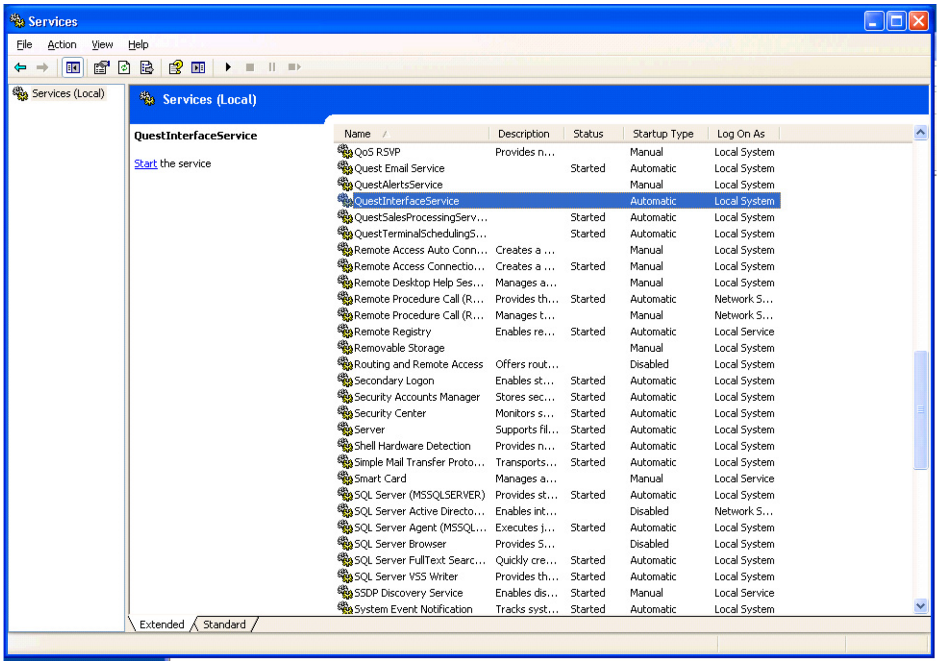
Step 6 Restart the windows service to implement the configuration by completing the following steps:

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

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

c. Find the Quest Interface Service and restart it (Figure 16).

Figure 16 Restart the Quest Interface Service



QuestInterfaceService

Start the service

Name	Description	Status	Startup Type	Log On As
QoS RSVP	Provides n…		Manual	Local System
Quest Email Service		Started	Automatic	Local System
QuestAlertsService			Manual	Local System
QuestInterfaceService			Automatic	Local System
QuestSalesProcessingServ…		Started	Automatic	Local System
QuestTerminalSchedulingS…		Started	Automatic	Local System
Remote Access Auto Conn…	Creates a …		Manual	Local System
Remote Access Connectio…	Creates a …	Started	Manual	Local System
Remote Desktop Help Ses…	Manages a…		Manual	Local System
Remote Procedure Call (R…	Provides th…	Started	Automatic	Network S…
Remote Procedure Call (R…	Manages t…		Manual	Network S…
Remote Registry	Enables re…	Started	Automatic	Local Service
Removable Storage			Manual	Local System
Routing and Remote Access	Offers rout…		Disabled	Local System
Secondary Logon	Enables st…	Started	Automatic	Local System
Security Accounts Manager	Stores sec…	Started	Automatic	Local System
Security Center	Monitors s…	Started	Automatic	Local System
Server	Supports fil…	Started	Automatic	Local System
Shell Hardware Detection	Provides n…	Started	Automatic	Local System
Simple Mail Transfer Proto…	Transports…	Started	Automatic	Local System
Smart Card	Manages a…		Manual	Local Service
SQL Server (MSSQLSERVER)	Provides st…	Started	Automatic	Local System
SQL Server Active Directo…	Enables int…		Disabled	Network S…
SQL Server Agent (MSSQL…	Executes j…	Started	Automatic	Local System
SQL Server Browser	Provides S…		Disabled	Local System
SQL Server FullText Searc…	Quickly cre…	Started	Automatic	Local System
SQL Server VSS Writer	Provides th…	Started	Automatic	Local System
SSDP Discovery Service	Enables dis…	Started	Manual	Local Service
System Event Notification	Tracks syst…	Started	Automatic	Local System

What to Do Next

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