Verifying the Upgrade

First Published: 2016-10-10
Last Updated: 2016-11-30

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

To verify the upgrade, complete the following tasks:

- Clearing the Browser Cache, page 39 (mandatory)
- Clearing Expired Flash SWZ Files From Browser, page 40 (required)
- Importing the Security Certificate, page 41 (required)
- Logging Into Cisco Vision Dynamic Signage Director, page 42 (required)
- Verifying the Control Panel and Other Menus, page 42 (required)
- Verifying that Services are Running, page 42 (required)
- Configuring the Media Player for VLAN Compliance Checking, page 43 (required)
- Upgrading the DMP Firmware, page 45 (required)
- Rebooting the DMPs, page 45 (required)
- Verifying Media Players, Groups, and Zones in the Management Dashboard, page 45 (required)
- Verifying the Multicast Configuration, page 46 (required)
- Setting Up the Quest Venue Manager to Send Updates to Cisco Vision Dynamic Signage Director Server, page 46 (required if using Quest for commerce integration)
- Completing the Post-Upgrade Checklist and Testing, page 49 (required)

Clearing the Browser Cache

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

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

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

   The Clear Recent History dialog box appears.

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

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

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

Clearing Expired Flash SWZ Files From Browser

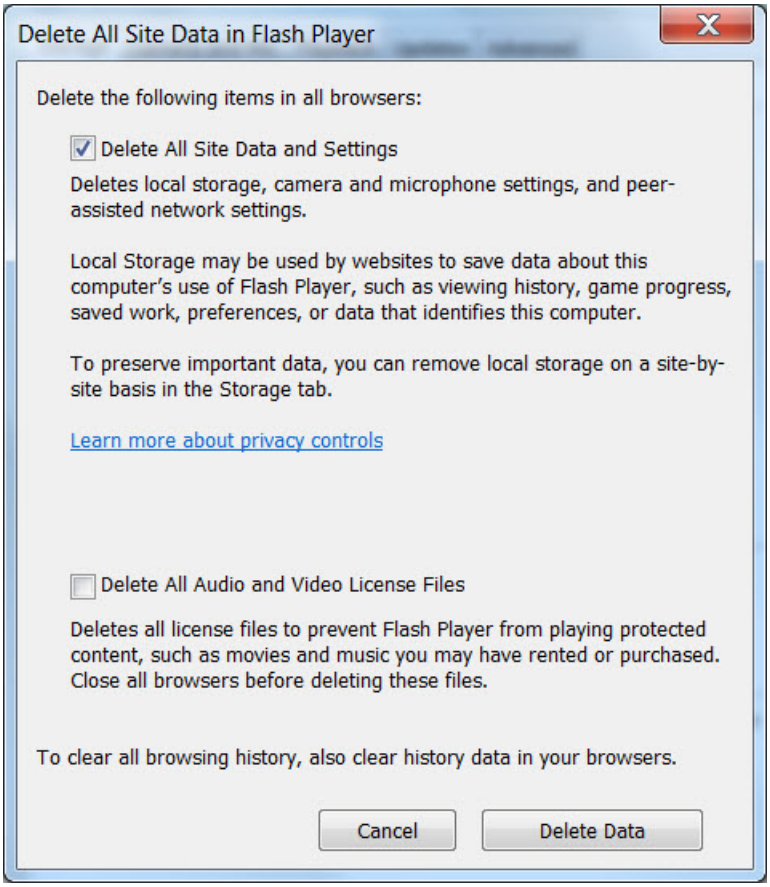
This section includes the following tasks:

Clearing the Flash Player Cache

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

1. Go to **Control Panel** > **Flash Player**.
2. In the Flash Player Manager Settings dialog box (Storage tab), click **Delete All**.
3. Select Delete All Site Data and Settings (Figure 1 on page 40).

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



4. Click **Delete Data**.

Deleting Other Cached Files From Flash

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

1. Close the browser window.
2. Delete cached files in the following paths for your browser application, and depending on your laptop client:

   From a Windows client:

   – For Chrome

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

   – For Mozilla Firefox

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

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

   From an Apple Mac OS X client:

   – For Chrome

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

   – For Mozilla Firefox

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

Importing the Security Certificate

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

Adding a Security Exception for Mozilla Firefox

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

1. When you see the warning page with the title “This Connection is Untrusted,” click the “**I Understand the Risks**” option.
2. Click **Add Exception...**.
3. In the Add Security Exception dialog box, click **Confirm Security Exception**.
4. Close all Mozilla Firefox windows.

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

Logging Into Cisco Vision Dynamic Signage Director

To verify that the upgrade was successful, and that Cisco Vision Dynamic Signage Director is up and operating, complete the following steps:

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

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

   or alternatively,

   http://*x.x.x.x*

   The Cisco Vision Dynamic Signage Director login screen appears.

2. Verify that the correct version is displayed.

   Note: If your window is not displaying the correct version, be sure that you have cleared the browser cache as described in Clearing the Browser Cache, page 39.

3. Type your Cisco Vision Dynamic Signage Director administrator login credentials and click **Log In**.

   Note: When you first log into Cisco Vision Dynamic Signage Director, the default administrator username and password is *admin*.

   The Cisco Vision Dynamic Signage Director Main Menu screen appears.

Verifying the Control Panel and Other Menus

To verify the control panel, complete the following steps:

1. From the Cisco Vision Dynamic Signage Director Main Menu, click **Control Panel**.

   After a few moments of loading resources, the Cisco Vision Dynamic Signage Director Control Panel Setup screen will open in a new window.

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

   Note: 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 Clearing the Browser Cache, page 39.

3. Verify that you can open the other Cisco Vision Dynamic Signage Director screens and menus.

Verifying that Services are Running

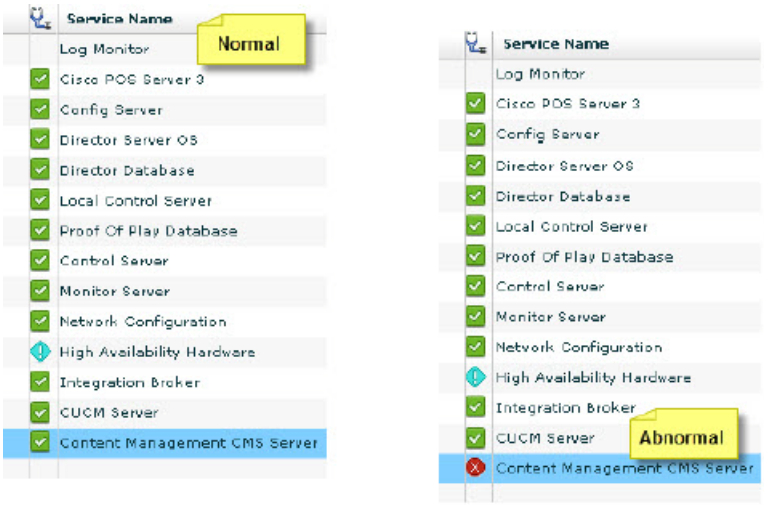
After you upgrade, go to the Management Dashboard to verify that all of the primary Cisco Vision Dynamic Signage Director services are running.

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

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

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

Figure 2 Verifying Normal Service States



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

Configuring the Media Player for VLAN Compliance Checking

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

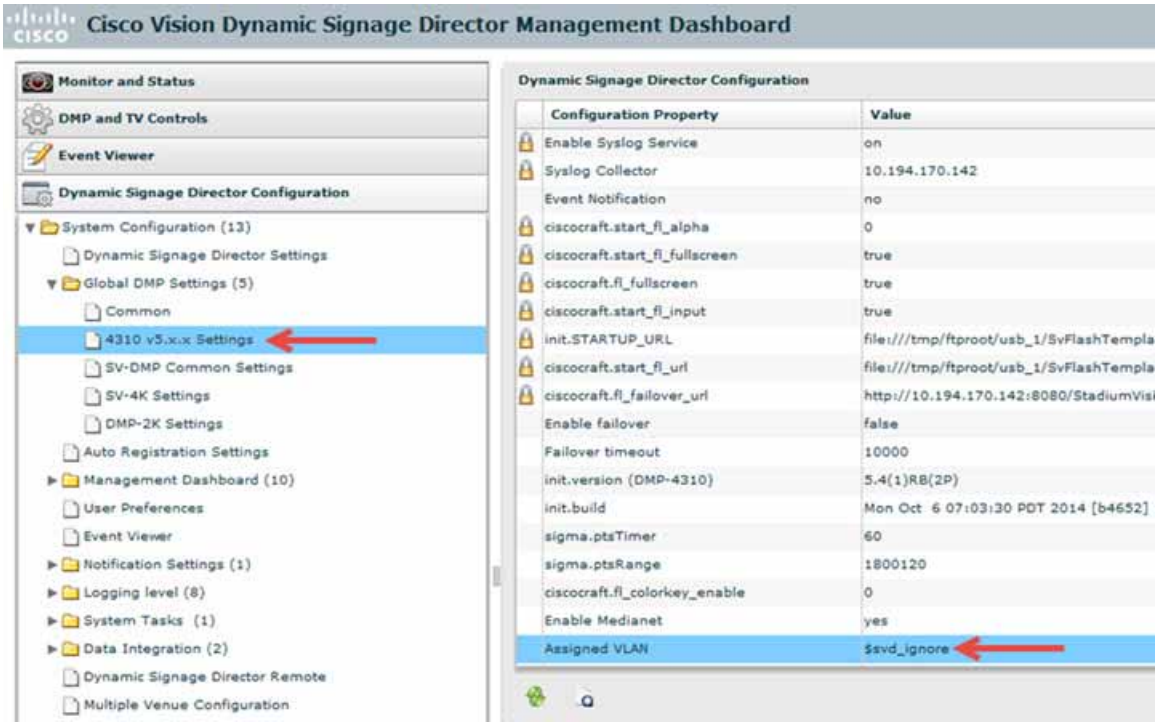
Note: Setting the assigned VLAN property for the media players is only recommended if all devices are located on the same VLAN. When a value is set, it is checked against what is being sent by the media player. Otherwise, you should configure **$svd_ignore**, which is the default.

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

1. From the Management Dashboard, go to **Dynamic Signage Director Configuration** > **System Configuration** > **Global DMP Settings**.
2. Do the following depending on your media player model:

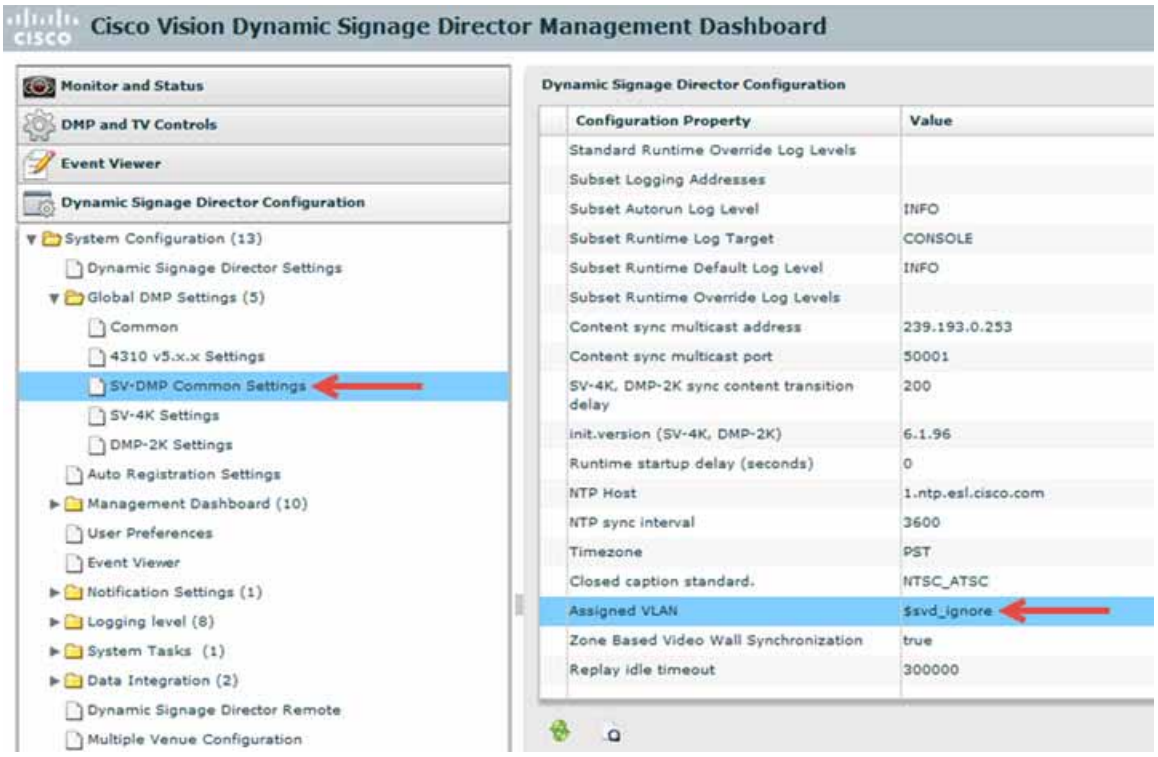
- For the DMP 4310G–Go to **4310 v5.x.x Settings** (Figure 3 on page 44).

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



- For the SV-4K and DMP-2K—Go to **SV-DMP Common Settings** (Figure 4 on page 44).

Figure 4 Assigned VLAN Property Configuration for the SV-4K and DMP-2K



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

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

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

4. Click the Save icon.

Upgrading the DMP Firmware

Verify whether your DMPs require a firmware upgrade and follow the steps in the corresponding modules of this guide to upload and install the required version(s) for your Cisco Vision Dynamic Signage Director release.

Note: If this is the initial upgrade of your system to Cisco Vision Dynamic Signage Director Release 5.0 software, a new firmware upgrade and configuration for the SV-4K and DMP-2K firmware is required. Follow the steps in Upgrading the SV-4K and DMP-2K Firmware, page 51.

Rebooting the DMPs

After an upgrade of the Cisco Vision Dynamic Signage Director software, the SV-4K and DMP-2K must be restarted to get the latest version of the runtime software.

- If this is the initial upgrade of your system to Release 5.0 and you have just performed a DMP firmware upgrade, then the DMPs have already rebooted and this step is not needed.
- If this an upgrade from Release 5.0 to another version of Release 5.0 without a DMP firmware upgrade, then you must reboot the SV-4K and DMP-2K to also update the DMP's runtime software.

To verify the system runtime on the DMP, see Verifying Media Players, Groups, and Zones in the Management Dashboard, page 45.

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

Note: Before you verify media player status, be sure that you have set the Assigned VLAN property so that the VLAN compliance check can be performed. For more information, see Configuring the Media Player for VLAN Compliance Checking, page 43.

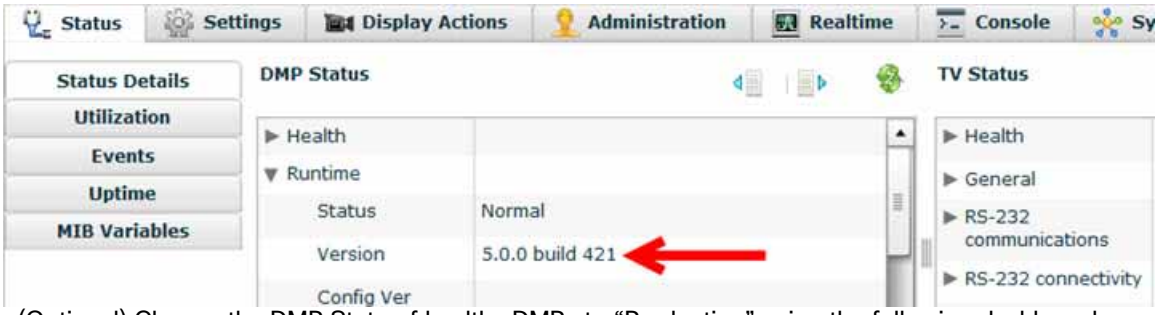
To check media players, groups, and zones after you upgrade your software, complete the following steps:

1. Go to the Management Dashboard and verify that all of your groups, zones and media players are present and in the green state.
2. From the DMP and TV Controls dashboard drawer, run the Get Status command on all devices to update Cisco Vision Dynamic Signage Director's record of MAC addresses:

   DMP and TV Controls > **Monitoring** > **Get Status**.
3. Run Get Status to confirm that all devices have successfully rebooted and are in good health.

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

4. Verify that the correct Cisco Vision Dynamic Signage Director runtime version is loaded on the DMP:
   a. Select the DMP(s) that you want to verify.
   b. Go to **Status** > **Status Details**.
   c. In the DMP Status panel, expand the Runtime status and verify the Version reported.



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

Verifying the Multicast Configuration

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

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

For more information about multicast configuration, see the “Configuring Multicast Ports for Cisco StadiumVision Director” topic in the “Configuring the Cisco StadiumVision Director Server System Settings” module of the Cisco Vision Server Administration Guide: Dynamic Signage Director.

To verify or configure the multicast addressing for Cisco Vision Dynamic Signage Director, complete the following steps:

1. From the Management Dashboard, select **Tools** > **Advanced** > **Registry**.
2. Scroll to the “MulticastHostPort” registry key in the Parameters list and confirm the entry for the registry.
3. To change the value, click on the value field and specify a multicast address in the range 239.193.0.0/24.

   Note: Be sure to use the value that is configured in your Cisco Connected Stadium network and include the **:***port*. The recommended default is **:50001**.
4. Click **Apply**.

Setting Up the Quest Venue Manager to Send Updates to Cisco Vision Dynamic Signage Director Server

Note: This task is only required if you are using the Quest Point of Sale system.

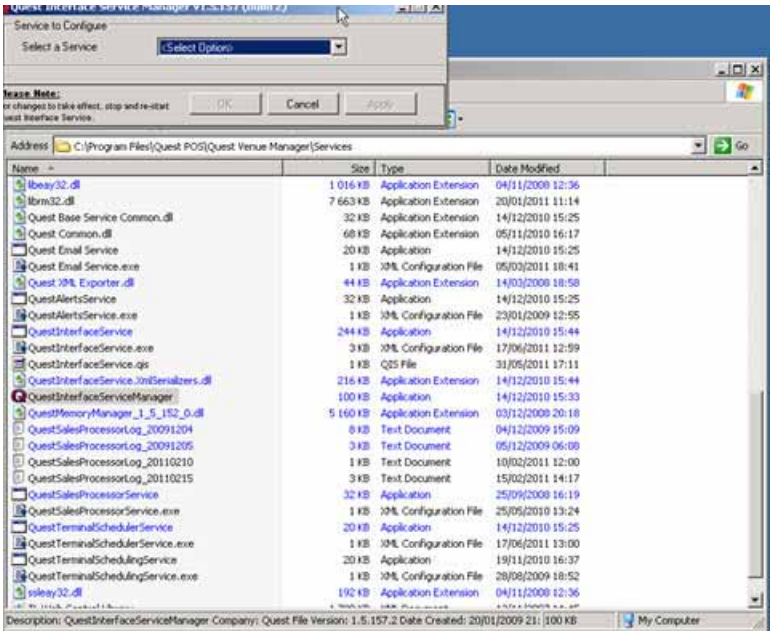
The steps described in this section assume that Quest has the notification service installed and enabled.

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

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

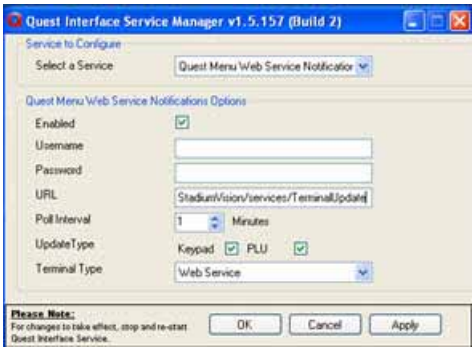
1. Access the Quest server.
2. Go to the C:\Program Files\Quest POS\Quest Venue Manager\Services directory.
3. Start the executable application program named “QuestInterfaceServiceManager” (Figure 5 on page 47).

Figure 5 QuestInterfaceServiceManager Application



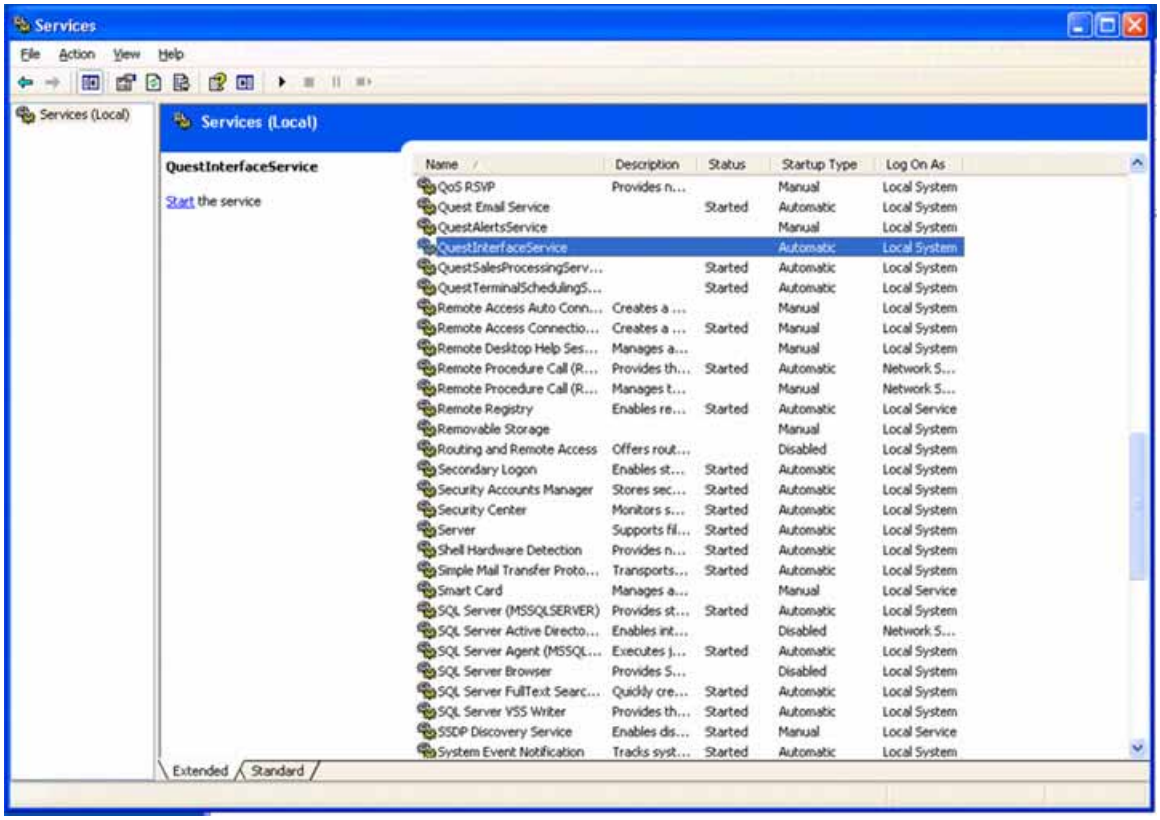
4. When the Quest Interface Service Manager application window opens, specify the following options (Figure 6 on page 48):
   a. In the Select a Service box, choose the **Quest Menu Web Service Notification**.
   b. Select the **Enabled** checkbox so a checkmark appears.
   c. In the URL box, enter “**http://svd:8080/StadiumVision/services/TerminalUpdate**”.
   d. In the Poll Interval box, select **1** minute.
   e. Select the **Keypad** and **PLU** update checkboxes so a checkmark appears.
   f. In the Terminal Type box, select **Web Service**.

Figure 6 Select a Service to Configure



5. Click **OK**.
6. Restart the windows service to implement the configuration by completing the following steps:
   a. From the Quest Server, click **Start** > **Run. . .**
   b. When the Run dialog box opens, type "**services.msc**".
   c. Find the Quest Interface Service and restart it (Figure 7 on page 49).

Figure 7 Restart the Quest Interface Service



Completing the Post-Upgrade Checklist and Testing

Use the Appendix A: Post-Upgrade Checklist, page 57 to be sure that you have completed the required verification steps.