VBrick
Enterprise Media System

VEMS v5.0.1 Portal Server
Release Notes

Copyright

About VBrick Systems

Founded in 1997, VBrick Systems, an ISO 9001 certified vendor, is a privately held company that has enjoyed rapid growth by helping our customers successfully introduce mission critical video applications across their enterprise networks. Since our founding, VBrick has been setting the standard for quality, performance and innovation in the delivery of live and stored video over IP networks—LANs, WANs and the Internet. With thousands of video appliances installed world-wide, VBrick is the recognized leader in reliable, high-performance, easy-to-use networked video solutions.

VBrick is an active participant in the development of industry standards and continues to play an influential role in the Internet Streaming Media Alliance (ISMA), the MPEG Industry Forum, and Internet2. In 1998 VBrick invented and shipped the world's first MPEG Video Network Appliance designed to provide affordable DVD-quality video across the network. Since then, VBrick's video solutions have grown to include Video on Demand, Management, Security and Access Control, Scheduling, and Rich Media Integration. VBrick solutions are successfully supporting a broad variety of applications including distance learning and training, conferencing and remote office communications, security, process monitoring, traffic monitoring, business and news feeds to the desktop, webcasting, corporate communications, collaboration, command and control, and telemedicine. VBrick serves customers in education, government, healthcare, and financial services markets among others.

Contents

Portal Server v5.0.1 Release Notes

Portal Server v5.0.1 Release Notes

These *Release Notes* have important information about v5.0.1 of the Enterprise Media System Portal Server. The Portal Server allows you to manage your video activities seamlessly with device, system and user management, a scheduling interface, and viewing portal. You can access all live IP Video channels and on-demand servers—at any time or from any place. More information can be found in the VEMS Portal Server user documentation. The setup file on the Product CD installs the necessary VEMS Portal Server components to a target VEMS Portal Server machine. VEMS Portal Server v5.0.1 requires the installation of a license file, normally supplied by e-mail or CD-ROM. *Note that the VEMS Portal Server will not operate correctly on a server that is configured as a primary domain controller.* **VBrick tests and supports the VEMS Portal Server on the platforms listed below.** These are the only supported platforms—VBrick does not test or support the Portal Server on any other platforms.

- Windows Server 2003 (Web Edition or Standard Edition)
- Windows Server 2008 (Web Edition or Enterprise Edition)

Topics in this document

What's New in VEMS v5.0.1

- Support for Windows Server 2003 (Web Edition or Standard Edition)
- VEMS Plug-in for IBM Sametime (Sametime v8.0.2 or higher required). For more information see the *VEMS Plug-in for Sametime Quick Start Guide*.
- Support for video-only VEMS presentations (Q & A and polling but no PowerPoint slides). For more information see the *VEMS Portal Server User Guide*.
- Automated upgrade options:

Automated Upgrade	Where Explained:
Portal Server v3.1/3.2/4.x/5.x to v5.0.1	Upgrading from Portal Server v3.1/3.2/4.x/5.x to v5.0.1 on page 7
Portal Server v3.0 to v5.0.1	Upgrading from Portal Server v3.0 on page 7
Windows Server 2003 to 2008	Upgrading from Windows Server 2003 to 2008 on page 8

> **Note** Legacy PowerPC G3/4/5 Macs are no longer supported by VBrick and may not play 5.0.1 streams. If you have PowerPC Macs at your site , VBrick recommends you do not upgrade to v5.0.1.

Features not Supported in this Release

- Windows PC support only on XP (Internet Explorer 7 or 8, FireFox 3, and Vista
- WM and H.264 support only for live and stored content (no MPEG-2/MPEG-4)
- WM IPR support only (MPEG set top boxes are not supported)
- Control Devices are not supported
- PC Remote is not supported
- NXG server is not supported
- Mass Ingestion is not supported

Important Note

VEMS v5.0.1 supports Windows Media and H.264 technology (content, encoders and VOD servers). Existing MPEG-2 and MPEG-4 devices and content are compatible with VEMS 5.0.1 but have not been tested and will not be initially supported by VBrick. This means you can use existing MPEG content and devices at your own risk and that some VEMS functionality (e.g. video conferencing) that requires MPEG devices will not be available in VEMS v5.0.1 unless you have existing MPEG encoder/decoder assets. VBrick will provide full support for MPEG-2 and MPEG-4 in VEMS v5.1.

Similarly, the Portal Server client has not been tested and will not be initially supported on Macintosh PCs. Macintosh PCs will be supported in VEMS 5.1. Note that VBrick support for Linux PCs has been discontinued entirely. See Features not Supported in this Release on page 2 for more information.

System Prerequisites

Windows 2003/2008 Server

- The Windows Server 2003 or Windows Server 2008 installation disks are required for the install.
- A minimum of 700 MB free disk space. Substantial additional disk space will likely be needed when ingesting or recording video.
- IIS Web Server and IIS FTP Server functionality must be enabled. The installer will determine if this needs to be installed.

Installing the Portal Server

If you ordered a Hardware/Software combination, the software will be pre-installed, your licenses will be activated on your server, and no additional installation is required. The *Portal Server Admin Guide* will instruct you on how to configure the software. The *User Guide* will instruct you and your end users on how to access and view video from the Portal Server and how to schedule and view events with the Scheduler (if you purchased the Scheduler module).

For software only orders, it is strongly recommended that you read the *Release Notes*, which contain the installation instructions, and the *Admin Guide* prior to installing the software. The first step you should take is to Activate your software license. See the detailed instructions on the VEMS Product CD and on the "Software License Activation" document that was shipped

with your system. *Be aware that if you purchased a server-based "software-only" product from VBrick, you will need to install the software on a fully-dedicated server.* There is no support or warranty coverage for Portal Server, Distribution Server, VOD, or NVR software installed on a non-dedicated server. VBrick also recommends that you do not use anti-virus, spyware detection, or similar software. If you purchased a Network Video Recorder, see the *NVR Release Notes* for installation instructions.

Note **Windows Server 2003 or Windows Server 2008?** The installation steps for certain procedures vary slightly depending on whether you are using Windows Server 2003 or Windows Server 2008. For example, in Windows Server 2003 you use Control Panel > Add or Remove Programs for certain steps. In Windows Server 2008 you use Control Panel > Programs > Programs and Features. *This document explains how to perform installation steps if you are using Windows Server 2008.* If you are using Windows Server 2003, the steps will be slightly different.

Also, if you will be installing VEMS on a system with Windows Server 2003 *Standard* Edition installed, you will need to perform certain configuration steps *before* installing the Portal Server. These steps are explained below in <u>Configuring for Windows 2003 Server Standard Edition</u>.

Configuring for Windows 2003 Server Standard Edition

The Portal Server runs on Windows Server 2003 Web Edition or on Windows Server 2003 Standard Edition. If you are using a server with Windows Server 2003 Standard Edition installed, you must modify the installation as explained below *before* installing the Portal Server. **If you are using Windows Server 2003 Web Edition or Windows Server 2008, ignore these steps and go to <u>Installing the Portal Server (Windows Server 2003 or 2008)</u> on page 4.**

▼ To modify the Windows Server 2003 Standard Edition configuration

1. Install IIS (Internet Information Services).

   a. Go **Start > Control Panel > Add or Remove Programs**.

   b. Click on **Add/Remove Windows Components** in the left navigation panel of the window.

   c. Click on **Application Server** and select **Details**.

   d. Make sure the following subcomponents are selected:
      - Application Server Console
      - ASP.NET
      - Enable network COM+ access
      - Internet Information Services (IIS)

   e. Then select **Internet Information Services (IIS)** and click **Details**.

   f. Make sure the following subcomponents are selected:
      - Common Files
      - File Transfer Protocol (FTP) Service
      - Internet Information Services Manager
      - World Wide Web Service

   g. Then select **World Wide Web Service** and click **Details**.

   h. Make sure the following subcomponents are selected:
      - Active Server Pages
      - World Wide Web Service

2. If you install .NET 2.0 before installing IIS, the Network Service user is not added correctly to the .NET framework folder. Use these steps to verify or add the Network Service user:

   a. Go to C:\WINDOWS\Microsoft.NET\Framework.

   b. Right-click on the Framework folder, click **Properties**, and select the **Security** tab. If the Network Service user is present, exit the window and you are done.

   c. If the Network Service user is not present, click the **Add** button, type Network Service, and then **OK**.

   d. Give the Network Service user the following permissions and click **OK**:
      • Modify
      • Read & Execute
      • List folder Contents
      • Read and Write

3. When done, reboot the server, and install the Portal Server as explained below.

Installing the Portal Server (Windows Server 2003 or 2008)

The VEMS Portal Server installation (for Windows Server 2003 or 2008) is a two-step process. First you install the VEMS Portal Server program files; then you configure the IIS web site. *The appropriate Windows Server installation disk may be required for this install.*

When installing the Portal Server, the VEMS Portal Server host name or IP address must match the host name or IP address of the computer on which it is installed. If the computer's host name or IP address is different, change these values in VEMS Portal Server *after* you install the VEMS Portal Server software. Go to **Control Panel > Programs > Programs and Features**. Then select **VBrick Enterprise Media System** and click **Uninstall/Change**. Then click **Modify Host Name/IP address stored in the VEMS Web.config file** and modify these values as necessary. It is also good practice to check that the **Date & Time** and **Time Zone** are set accurately on the server. See "Synchronizing the Portal Server and the NVR" in the *Portal Server Admin Guide* for more information.

▼ To install the Portal Server:

1. Note the server name or IP address where the VEMS Portal Server server will be installed.

2. Go to the "Software" page on the VEMS Product CD and run the VBrick Enterprise Media System setup file. The InstallShield Wizard will extract the files, start Portal Server Setup, and verify the necessary prerequisites are installed. (Note: you may be prompted to reboot after prerequisites are installed. If so reboot the machine and then double-click on the installer again to continue the installation process.)

3. When prompted, use the "License Activation Keys & Serial Numbers" card that was included with the VEMS Product CD to enter serial numbers for each purchased component. Click **Next** when done.
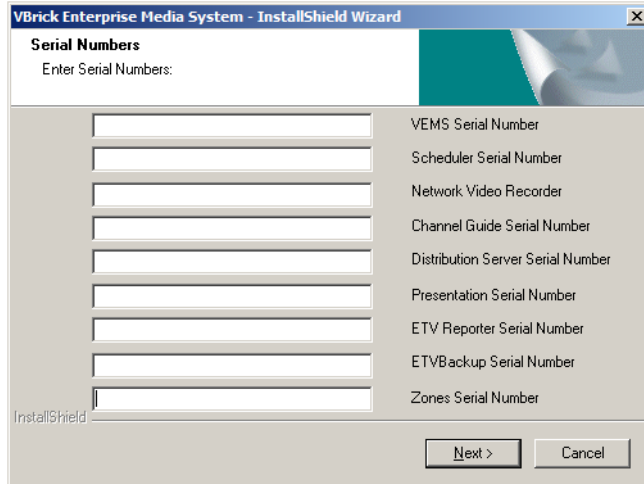
4. <u>Windows Server 2003 only.</u> When prompted, be sure **IIS** and **MySql** are checked for installation and click **Next** to continue. (If you choose not to install these pre-requisites, the install will end.)

5. If prompted, insert the original **Windows 2003 Server** installation disk and click **Next**.

6. A Welcome page is displayed after the prerequisites are installed. Click **Next** to continue.

7. Read the End-User License Agreement (EULA) and click **Yes** to continue.

8. A dialog box shows the default Portal Server directory path: `c:\program files\vbrick`. Select **Next** to continue or **Browse** to select a different path.

9. When prompted, navigate to the folder with your license (`.lic`) files. License files are obtained by using the "License Activation Keys & Serial Numbers" card included with the Product CD. The "Software License Activation" document, also included, explains how to activate your licenses using these keys. Note that multiple license files may be shown if you purchased optional VEMS components. *Select all available license files in the folder.* (For more about license files, see "Installing Serial Numbers and License Files" in the *Portal Server Admin Guide.*)

10. The Portal Server installation will then run to completion without additional input. This may take several minutes.

11. When the installation is complete, press **Finish** to exit setup. This completes the VEMS Portal Server installation. The VEMS Portal Server runs in the background and will auto-start if you re-boot the server machine. If you experience problems or need to start or stop VEMS Portal Server for any reason, you can or stop VEMS Portal Server as explained in <u>Launching the Portal Server</u>.

Note If you need to add or change a license file after initial installation, go to **Control Panel > Programs > Programs and Features**. Then select **VBrick Enterprise Media System** and click **Uninstall/Change**. Then use the radio buttons to install or replace the required license(s).

Reinstalling the Portal Server

Use the following steps in the unlikely event that you need to reinstall the VEMS Portal Server software.

▼ To reinstall VEMS Portal Server:

1. First uninstall the software. Go to **Control Panel > Programs > Programs and Features**.

2. Then select **VBrick Enterprise Media System** and click **Uninstall/Change**.

3. When prompted, be sure to *keep* the database.

4. When finished, restart the machine.

5. Reinstall VEMS Portal Server (see <u>Installing the Portal Server (Windows Server 2003 or 2008)</u> on page 4). You *do not* need to re-configure the web site.

6. Restart the machine and you are done.

Launching the Portal Server

As noted, VEMS Portal Server runs in the background and will autostart if you reboot the machine. If you experience problems or need to start or stop VEMS Portal Server for any reason, you must start or stop the default web site. Note also that this is a web server installation that runs continuously. No desktop icons are present to show run status.

▼ To start or stop the VEMS Portal Server Web Site:

1. Go to **Administrative Tools > Internet Information Services (IIS) Manager**.

2. Expand the tree under the **server_name** and click **Sites**.

3. Right-click **Default Web Site**, select **Manage Web Site**, and select **Start** or **Stop** as appropriate.

▼ To launch VEMS Portal Server from the server host machine:

1. Open a web browser.

2. Enter `http://localhost` to launch the client application.

3. Enter `http://localhost/admin` to launch the admin application.

▼ To launch VEMS Portal Server from a client machine:

1. Open a web browser.

2. Enter `http://<ip_addr|server_name>` to launch the *client* application where `<ip_addr|server_name>` is the IP address or server name of the VEMS Portal Server. (If using Integrated Windows Authentication, use the server_name.)

3. Enter `http://<ip_addr|server_name>/admin>` to launch the *admin* application where `<ip_addr|server_name>` is the IP address or server name of the VEMS Portal Server. (If using Integrated Windows Authentication, use the server_name.)

Uninstalling the Portal Server

Use the following procedure to uninstall the Portal Server for any reason. (Do not uninstall the Portal Server before performing an upgrade. **Before uninstalling the Portal Server be sure to take it off the network and reboot the machine.** If you fail to do so it may be necessary to reinstall the application and *then* uninstall again as explained below. If you have Distribution Servers configured for presentation load-balancing, run the `DistributionServer.exe` tool on each server and click **Revert** and **Start** before uninstalling the application (see <u>Installing Distribution Servers</u> on page 9 for more information).

▼ To uninstall the Portal Server:

1. Revert any defined Distribution Servers if present (see previous paragraph).

2. Go to **Control Panel > Programs > Programs and Features**. Then select **VBrick Enterprise Media System** and click **Uninstall/Change**.

3. When the following window is displayed, select **Uninstall VEMS** and click Next.
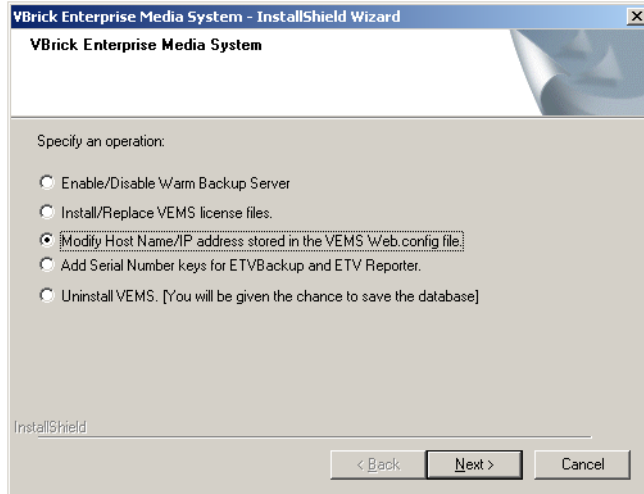
4. Respond appropriately when prompted to save the database.
5. After the uninstall, reboot the machine when prompted.

Upgrading the Portal Server

Upgrading from Portal Server v3.1/3.2/4.x/5.x to v5.0.1

Version 5.0.1 supports upgrades from all 3.x/4.x/5.x versions. The upgrade to VEMS v5.0.1 is highly automated with little user interaction. *Be sure to read the following note if there are Distribution Servers present.*

▼ To upgrade from Portal Server v3.1/3.2/4.x/5.x to v5.0.1:

1. Before runnning the upgrade, take the server off the network and reboot the machine.
2. Install the Portal Server. Run `setup_VBrick_Enterprise_Media_System_5_0_1.exe` and click **OK** when prompted. The installer will run automatically and prompt for a reboot.
3. When done select any license(s) when prompted.

Note If you have one or more Distribution Servers defined in your configuration, run the Distribution Server tool and select **Revert** on the Portal Server and on each Distribution Server <u>before</u> performing an upgrade. Then run the Distribution Server tool and select **Start** on the Portal Server and on each Distribution Server <u>after</u> the upgrade. See <u>Installing Distribution Servers</u> on page 9 for more information.

Upgrading from Portal Server v3.0

The upgrade from MCS v3.0 to VEMS v5.0.1 is a two-step process. First you install a patch file (`SetupMCSS_3_0_0_Patch.exe`) and then you run the v5.0.1 setup program (`Setup_VBrick_Enterprise_Media_System_5_0_1.exe`).

▼ To upgrade from MCS v3.0:

1. Before installing the upgrade, first take the server off the network and reboot the machine.
2. Run the patch file `SetupMCSS_3_0_0_Patch.exe`, follow the prompts, and reboot when done.
3. After the reboot run `Setup_VBrick_Enterprise_Media_System_5_0_1.exe` and follow the prompts. The installation is highly automated and requires little interaction.

4. Click **OK** when finished and the installer will prompt for a reboot.

5. Reboot the machine and you are done.

Upgrading from Windows Server 2003 to 2008

The v5.0.1 release has a "Cross-O/S Upgrade" option that lets you upgrade your server machine from Windows Server 2003 to Windows Server 2008. (Note that if MySQL is present on your 2008 computer, please uninstall before continuing.)

▼ To upgrade the server machine from Windows Server 2003 to Windows Server 2008:

1. Prior to the upgrade, on the 2003 Portal Server, run the `SetupVBDatabaseExporter.exe` from the Product CD to install the VBDatabaseExporter program. A shortcut will be installed on the desktop called VBDatabaseExporter. Double-click on it to bring up the program. If you haven't changed the root password for MySQL simply press **Export** (otherwise enter the current password and press **Export**). This will create a file called `ExportedDB.sql` on the desktop. Save this file and any custom user data in the `VBrick\MCS` directory to a safe and convenient location.
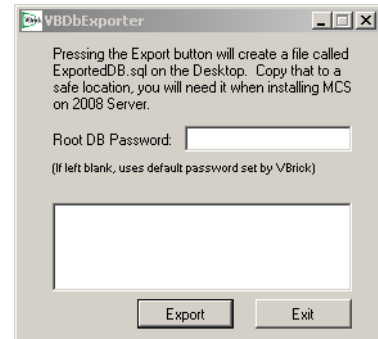
2. Custom user data can be found in the following directories:
   - D:\VBrick\Presentations\ or C:\Program Files\VBrick\MCS\Presentations if no D: drive is present on the system.
   - D:\VBrick\MCSPresentations\ or C:\Program Files\VBrick\MCS\MCSPresentations if no D: drive is present on the system.
   - C:\Program Files\VBrick\MCS\Logs\, or if the default directories are not used, the files located in the directory determined by MCS Admin Console > Global Settings > Access Logging > General Logging Properties > Log File Directory.
   - C:\Program Files\VBrick\MCS\nsc\
   - C:\Program Files\VBrick\MCS\sdp\
   - C:\Program Files\VBrick\MCS\StationIcons\
   - C:\Program Files\VBrick\MCS\Images\Thumbnails\

   Copy these folders into the same location you put the `ExportedDB.sql` file in Step 1. If you installed MCS in a non-default directory, change C:\Program Files to the appropriate directory in the file paths described in above in Step 2.

3. If you purchased our pre-packaged content, you will need to save the appropriate license files. Go to: C:\Program Files\VBrick\MCS\licenses\ and save the `contentlicense` folder. After you install VEMS 5.0.1 you will need to take these license files and add them using the Portal Server "Install/Replace License Files" function. See the *Portal Server Admin Guide* for instructions on how to do this.

4. When done, wipe the drive and install Server 2008 (either Web or Enterprise Edition).

5. When done, install the Portal Server. See <u>Installing the Portal Server</u> on page 2 for instructions. Near the beginning of the installation process, you will be asked if this is a Cross-OS upgrade. If **Yes**, a dialog box will let you browse to the `ExportedDB.sql` file you saved in Step 1 above.

6. Follow the prompts and reboot the server when prompted. If you saved any directories from your previous version of MCS you can now copy them back into the appropriate directories in VEMS v5.0.1. The file locations will be the same as they were in your

previous version of MCS unless you chose a different directory; if so the locations will be the same once you get to [InstallDir]\MCS.

7. Reboot the server.

Installing Distribution Servers

## *Installing Distribution Servers*

Distribution servers are used to load-balance the distribution of .jpg images and HTML pages when delivering large-scale presentations. In order to use Distribution Servers in a VEMS environment, you must configure "zones" and define a Distribution Server for each zone. See the "Distribution Servers" topic in the *Portal Server Admin Guide* for more about distribution servers. See the "Zones" topic in the *Portal Server Admin Guide* for an explanation of how to configure and use zones that point to specific servers. (Also see Configuring for Presentations on page 17.) Use the following steps to install a distribution server:

1. Go to the "Distribution Server" page on the VEMS Product CD and run the Distribution Server setup file on each distribution server. (See Installing the Portal Server on page 2. The steps are identical except that you only use the Distribution Server license file.)

2. Run the Distribution Server tool (DistributionServer.exe) on the Portal Server and on each distribution server to configure your site's IP addresses. The distribution server tool (DistributionServer.exe) is located in:
   C:\Program Files\VBrick\MCS\utils\DistributionServer

▼ To run the Distribution Server tool on the Portal Server or a Distribution Server:

1. Launch the tool to display the following window.
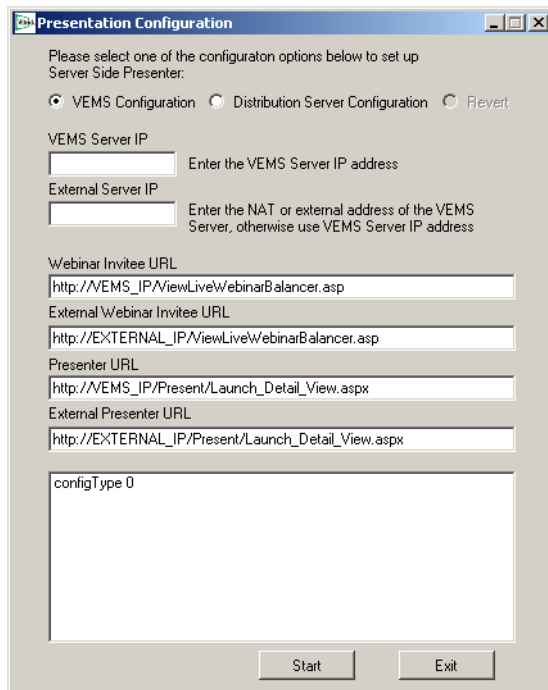
2. Enter the internal and external IP addresses for your VEMS server. As shown in the following window, the remaining fields are automatically populated with the appropriate IP addresses. For the **VEMS Server IP** enter the Portal Server's actual IP address. For **External Server IP** enter the NAT or external address of the Portal Server.
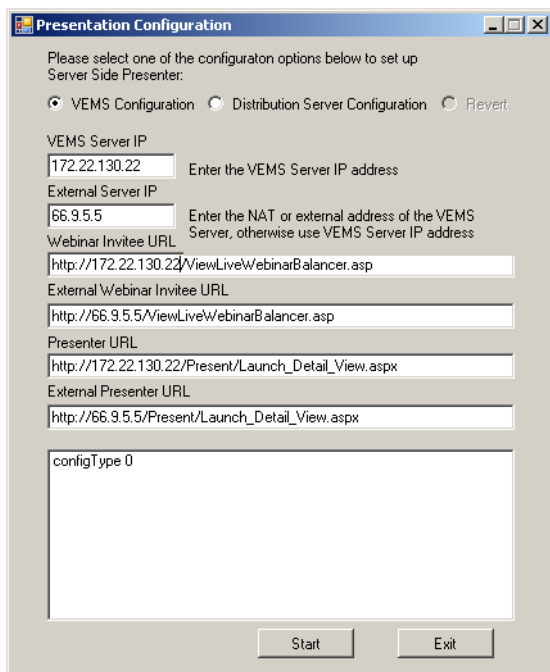
3. Click **Start** to run the tool. When done the following window is displayed. If there are errors or you need to change the values for any reason, use the **Revert** button.
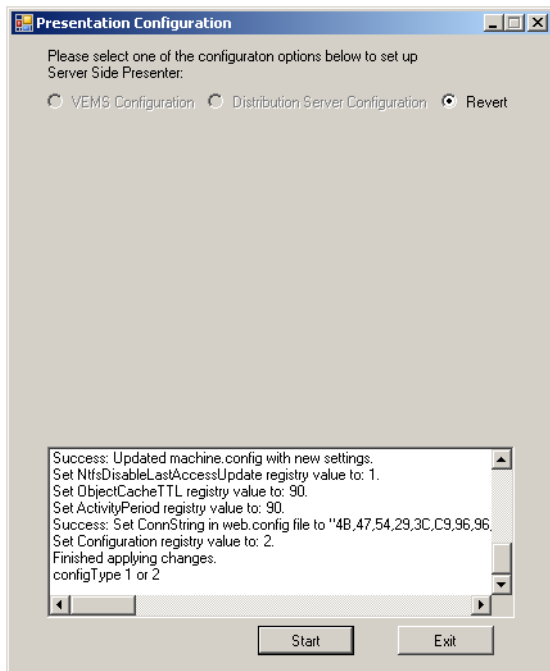
▼ To install the distribution server software on a Distribution Server:

1. Launch the tool as explained above.

2. Select **Distribution Server Configuration**, enter the VEMS Server IP Address and click **Start**. (If the Distribution Server is on the same network as the main Portal Server, enter

the **VEMS Server IP**. If the Distribution Server is on a different network (for example if the Distribution Server accesses the Portal Server via the Internet—not an intranet—enter the NAT or external address of the Portal Server.) Always take into account how the Distribution Server identifies the Portal Server via IP when configuring this tool.
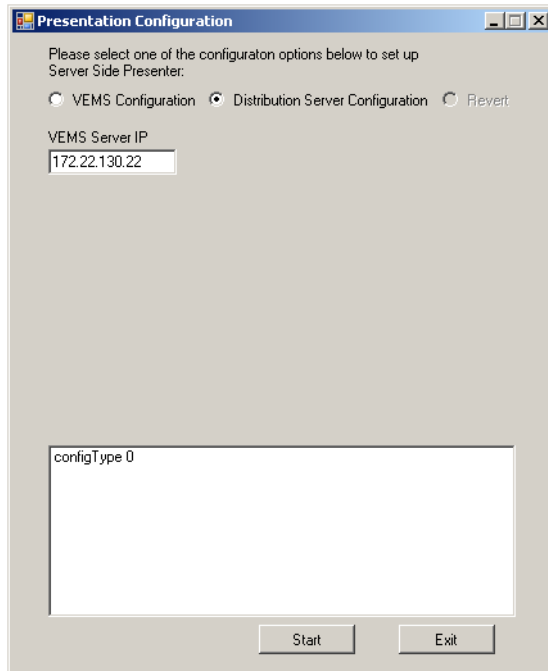
Configuring Distribution Servers

Note This step explains how to configure ETVBackup on each Distribution Server. **This step is not optional.** If you have installed distribution server(s) this configuration step is required. Repeat this procedure on each Distribution Server. Note that the user logged onto the Distribution Server must be a user with Administrator rights.

Configuring a Local Distribution Server

Use this configuration procedure when the Distribution Server is on the same network as the VEMS Portal Server and there is no firewall between them.

▼ To configure a local Distribution Server:

1. Set up VEMS Backup.

Note In order to configure the ETV Backup Profiles as explained in this section, you must be logged in to the Distribution Server as administrative user

   a. Start VEMS Backup and enter a valid serial number for the license. If you copied the serial number to the Windows Clipboard, ETV Backup will automatically put the serial number in the serial number text box.

   b. Add two new profiles, they are located in the `C:\Program Files\VBrick\MCS\ETVBackupScripts` folder.

      i. Double-click on the ETVBackup shortcut on the desktop, if you get a message asking to visit a web page, click No

      ii. Enter in the serial number if you haven't already registered the product.

      iii. Go to the **Profiles** menu item and select **Import Profile** and browse to Distribution Server Presentations.sps and Distribution Server Thumbnails.sps and import each one.

  c. Right-click on the Distribution Server Webinar data profile and select **Modify**.

      i. Next to "Live MCS Database" type in the following value: \\<name_of_server>\Presentations\. The [name of server] value is the VEMS server.

      ii. Next to **Database backup** browse to the following directory: D:\VBrick\Presentations.

  d. Right-click on the Distribution Server Webinar Thumbnails profile and select **Modify**.

      i. Next to **Live MCS Database** type in the following value: \\<name_of_server>\Thumbnails\. The <name of server> value is the VEMS server.

      ii. Next to **Database backup** browse to the following directory: C:\Program Files\VBrick\MCS\Images\Thumbnails

  e. In the main ETVBackup screen right-click on the VEMS Warm Backup Group, choose the Schedule menu item, then select **Delete Schedule**.

  f. In the main ETVBackup screen add a group profile named DistributionServer Group. Select Profiles > New > Enter "DistributionServer Group" and **Next**. Check the "Group" radio button. Select "Done", then "OK". The main profile setup window will now appear.

    Select the following two profiles (Distribution Server Webinar data and Distribution Server Webinar Thumbnails) and add them to the group by highlighting them and pressing the ">" button, followed by **OK**. The program will ask if you would like to perform a simulated run—select **No**.

2. Create a schedule for ETVBackup.

▼ To create a schedule:

1. In ETVBackup, right-click on Distribution Server Group and select **Schedule**.

2. When the popup window is displayed, click **Yes** to create a schedule.
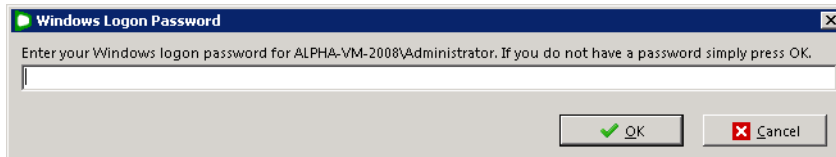
3. Be sure a user with administrative privileges on the server machine is shown in the **Run as** box. Then enter the password associated with that user and click **OK**.
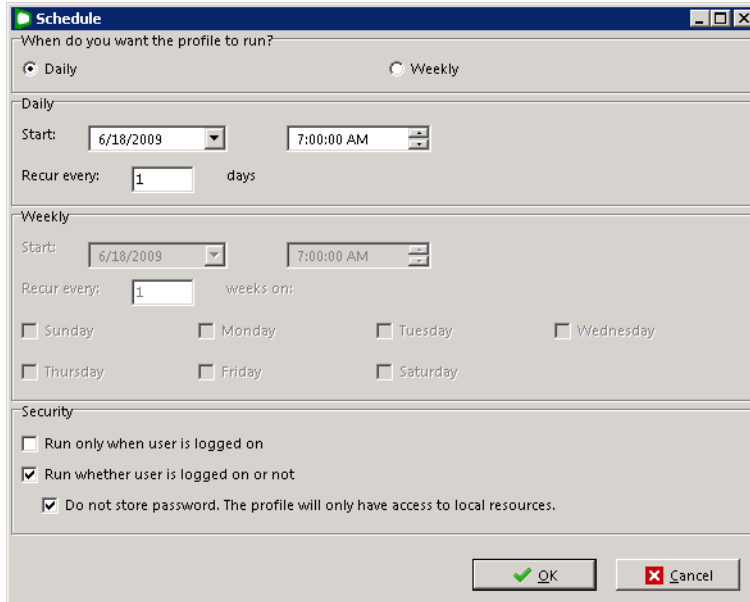
4. On the "Schedule" window, click **OK** and **OK** to exit.

5. On the Windows Web Server 2008 desktop, go to **Start > Administrative Tools > Task Scheduler**.

6. Expand **Task Scheduler Library > 2BrightSparks > SyncBack** and double-click on **ServerName-Administrator**.
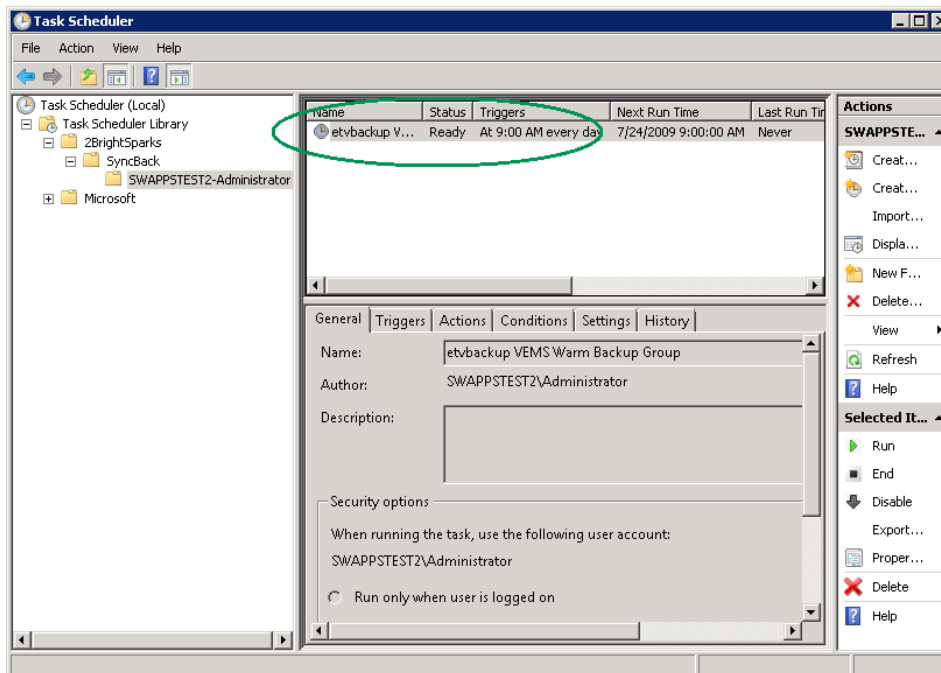
7. In the upper pane, double-click on **etvbackup VEMS Warm Backup Group** to display the properties page.
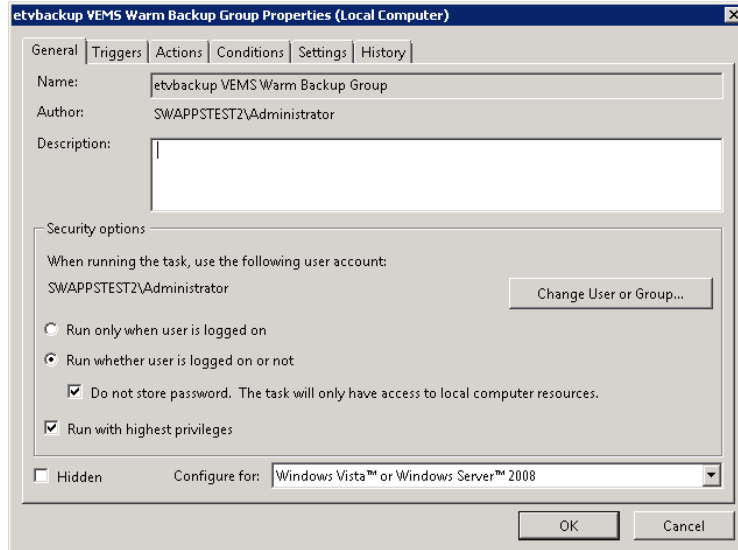
8. Click on the **Triggers** tab and click **Edit**.
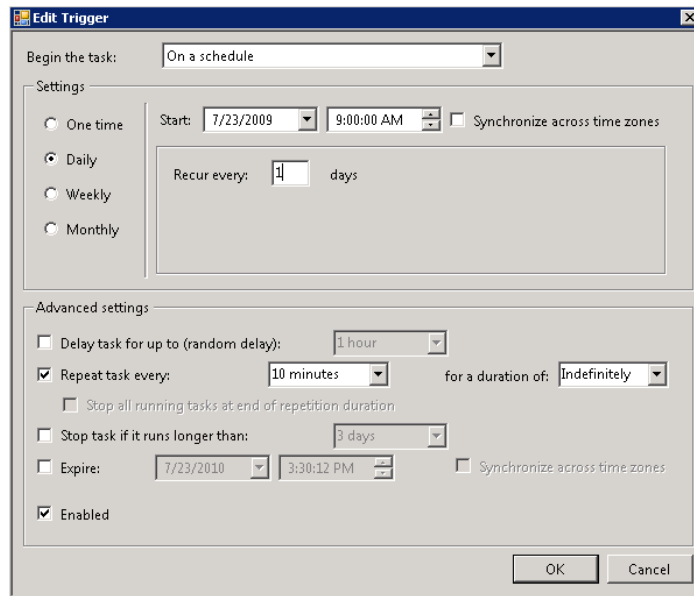
9. Select **Repeat task every** 10 minutes, set **for a duration of** Indefinitely and click **OK**.

Configuring a Remote Distribution Server

Use this configuration procedure when the Distribution Server is on a different network than the VEMS Portal Server or there is a firewall between them. You must open Port 21 (FTP Port) between the VEMS Portal and the Remote Distribution Server.

▼ To configure a remote Distribution Server:

1. Set up VEMS Backup.

Note In order to configure the ETV Backup Profiles as explained in this section, you must be logged in to the Distribution Server as administrative user

a. Start VEMS Backup and enter a valid serial number for the license. If you copied the serial number to the Windows Clipboard, ETV Backup will automatically put the serial number in the serial number text box.

b. Add two new profiles, they are located in the `C:\Program Files\VBrick\MCS\ETVBackupScripts` folder.

    i. Double-click on the ETVBackup shortcut on the desktop, if you get a message asking to visit a web page, click No.

    ii. Enter in the serial number if you haven't already registered the product.

    iii. Go to the **Profiles** menu item and select **Import Profile** and browse to `Remote FTP Distribution Live Presentation Data.sps` and `Remote FTP Distribution Live Presentation Thumbs.sps` and import each one.

c. Right-click on the `Remote FTP Distribution Live Presentation Data` profile and select **Modify**.

    i. Next to "Live Presentation Data" type in the following value: `D:\VBrick\Presentations\`

    ii. Next to **127.0.0.1** (double-click and change name to Remote Distribution Server IP for labeling) browse to the following directory: `\presentations\`

d. Select **FTP** on left hand pane. Enter IP Address of Remote Distribution Server in Hostname filled (This most likely will be Public address of Remote Distribution Server). Press **Test FTP Settings** to test connection. If ftp fails, check Firewall settings the FTP Username and password are both `Presentations` and are automatically created by VEMS installer.

e. Select **OK** to exit Modify Profile Setup.
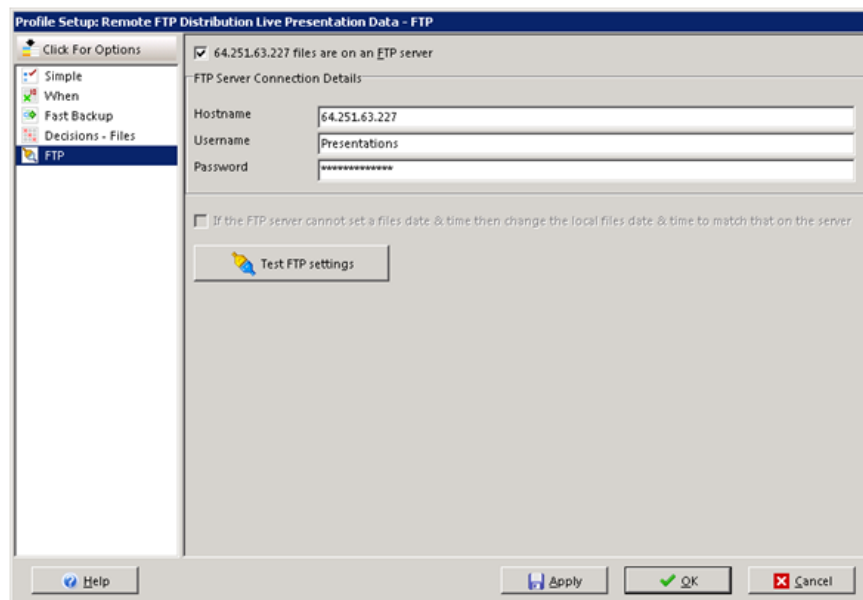
f. Right-click on the `Remote FTP Distribution Live Presentation Thumbs` profile and select **Modify**.

    i. Next to **Live Presentation Thumbs** type in the following value: `C:\Program Files\VBrick\MCS\Images\Thumbnails\`

    ii. Next to **127.0.0.1** (Double Click and change name to Remote Distribution Server IP for labeling) browse to the following directory: `\Thumbnails\`

iii. Select **FTP** on left hand pane. Enter IP Address of Remote Distribution Server in Hostname field (This most likely will be Public address of Remote Distribution Server). Press **Test FTP Settings** to test connection. If ftp fails check Firewall settings, the FTP Username and password are both Thumbnail and are automatically created by VEMS installer.

iv. Select **OK** to exit Modify Profile Setup.
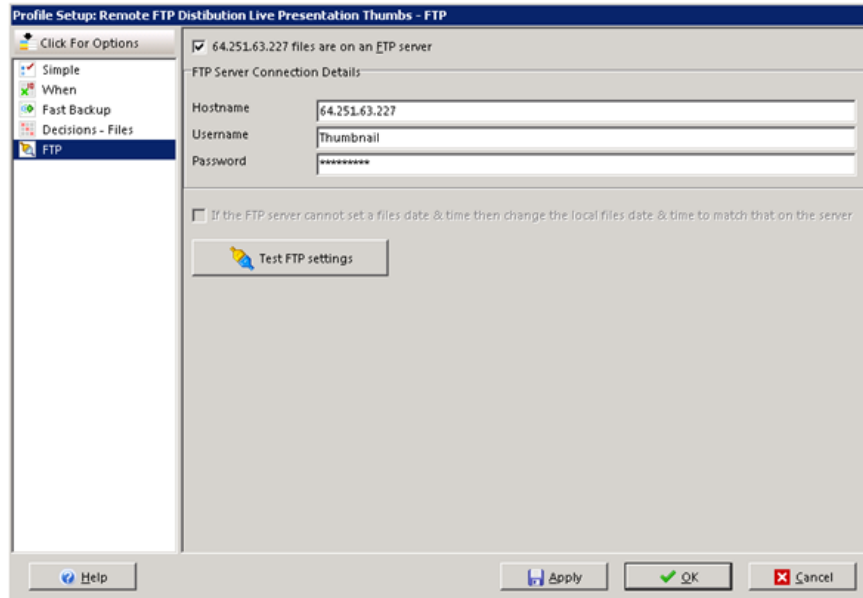
g. In the main ETVBackup screen right-click on the VEMS Warm Backup Group, choose the Schedule menu item, then select **Delete Schedule**.

h. In the main ETVBackup screen add a group profile named DistributionServer Group. Select Profiles > New > Enter "DistributionServer Group" and **Next**. Check the "Group" radio button. Select **Done**, then **OK**. The main profile setup window will now appear.

i. Select the following two profiles (Remote FTP Distribution Live Presentation Data and Remote FTP Distribution Live Presentation Thumbs) and add them to the group by highlighting them and pressing the ">" button, followed by **OK**. The program will ask if you would like to perform a simulated run—select **No**.

2. Create a schedule for ETVBackup. Go to Step 2 in <u>Configuring a Local Distribution Server</u> on page 11 and repeat the procedure to create a schedule using the Windows Task Scheduler.

Uninstalling Distribution Servers

The steps to uninstall a Distribution Server are the same as for uninstalling a Portal Server. See <u>Uninstalling the Portal Server</u> on page 6 for details. If you have Distribution Servers configured for presentation load-balancing, run the DistributionServer.exe tool on each server and click **Revert** and **Start** before uninstalling the application (see <u>Installing Distribution Servers</u> on page 9 for more information).

Configuring for Presentations

Several configuration steps are required before you can publish rich media presentations to the Portal Server. These steps are briefly listed below and explained in more detail in the following paragraphs. Also, be aware that in many cases a presentation will be pushed from a VBrick appliance to a Windows Media VOD server and/or to a VBrick Reflector. If so you will need to configure these devices as well: the *WM Appliance Admin Guide* explains how to configure a reflector; the *VOD-WM Server Admin Guide* explains how to configure publishing points on a Windows Media VOD server. If you will using distribution servers for load-balancing, see <u>Installing Distribution Servers</u> on page 9.

> **Note** Additional steps are also required if you will be using Distribution Servers to load-balance presentations. See <u>Installing Distribution Servers</u> on page 9 for more about this; see the "Zones" topic in the *Portal Server Admin Guide* for an explanation of how to configure and use zones that point to specific servers.

▼ To configure your environment for presentations:

1. **Configure a User with Multimedia Authoring Privileges** – do this on the Admin Console User pages.
2. **Configure a WM VBStar as Multimedia VBrick Encoder** – on the VBrick appliance IWS management pages, enable 25 Push Destinations, and enable Closed Captions and Metadata on the encoder, the archiver, and on all encoder destinations. On the VEMS Admin Console, enable the VBStar encoder Slot 1 as Multimedia and configure a Viewing URL.
3. **Configure Server E-mail Address(es) for Presentations** – do this on the Portal Server `web.config` file or when configuring Distribution Servers.
4. **Assign a VEMS Presentation User** – do this on the Admin Console Users page.

> **Note** When a presentation is complete, the number of allowed clients on the appliance is set to zero. To reconfigure an appliance for streaming or other purposes, open the IWS admin pages, go to Configuration: Encoder > Server, and set Max. Allowed Clients to a desirable number less than or equal to 50.

1. Configure a User with Multimedia Authoring Privileges

If Authorization and Authorization is enabled for your VEMS Environment, you must configure a user with presentation authoring privileges. For example some users may not be authorized to create presentations in which case this feature will not be displayed. Other users may only be authorized to edit or delete their own presentations. Super users can create and modify all presentations. See "Multimedia Authoring Privileges" in the Users pages in the *Portal Server Admin Guide* for more information.

2. Configure a WM VBStar as a Multimedia VBrick Encoder

You must configure a Windows Media VBStar as a "Multimedia VBrick' before it can be used for a presentation. The *Portal Server Admin Guide* explains how to configure the **Viewing URL** and other options; go to Global Settings > VBricks for more information. A **Viewing URL** is typically the path to a publishing point in a Windows Media Server. Viewing URLs are configured on the Global Assignments > VBricks page. Viewing URLs are urls which either point to the encoder, a web hosted NSC file from this encoder, or point to a Windows Media Server Publishing Point which was created by a push/pull from this encoder.

Also be aware that in many cases a presentation will be pushed from a VBrick appliance to a Windows Media VOD server and/or to a VBrick Reflector. If so you will need to configure these devices as well: the *WM Appliance Admin Guide* explains how to configure a reflector; the *VOD-WM Server Admin Guide* explains how to configure publishing points on a Windows Media VOD server.

3. Configure Server E-mail Address(es) for Presentations

If you purchased the "Presentations" module with your VEMS Portal Server you will need to configure the internal and external IP addresses of your server. These addresses are used to deliver automated e-mail invitations and must be configured using IIS. *If you do not configure these settings, you will not be able to send valid automated invitations.*

Note If you will be installing one or more Distribution Servers, ignore this section. You will configure the server IP addresses for e-mail invitations when you run the Distribution Sever installation tool. See Installing Distribution Servers on page 9.

▼ To configure the IP addresses for e-mail invitations:

1. Go to the machine on which on which the VEMS server is installed.
2. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. Expand the tree control in the left navigation pane and select **Sites > Default Web Site**.
4. Double-click on **Default Web Site** and then double-click again on **Application Settings** on the right side of the page. The following screenshot shows the settings you will need to modify.
5. Double-click on each setting, enter an appropriate internal or external value for IP address, and click **OK** when done.
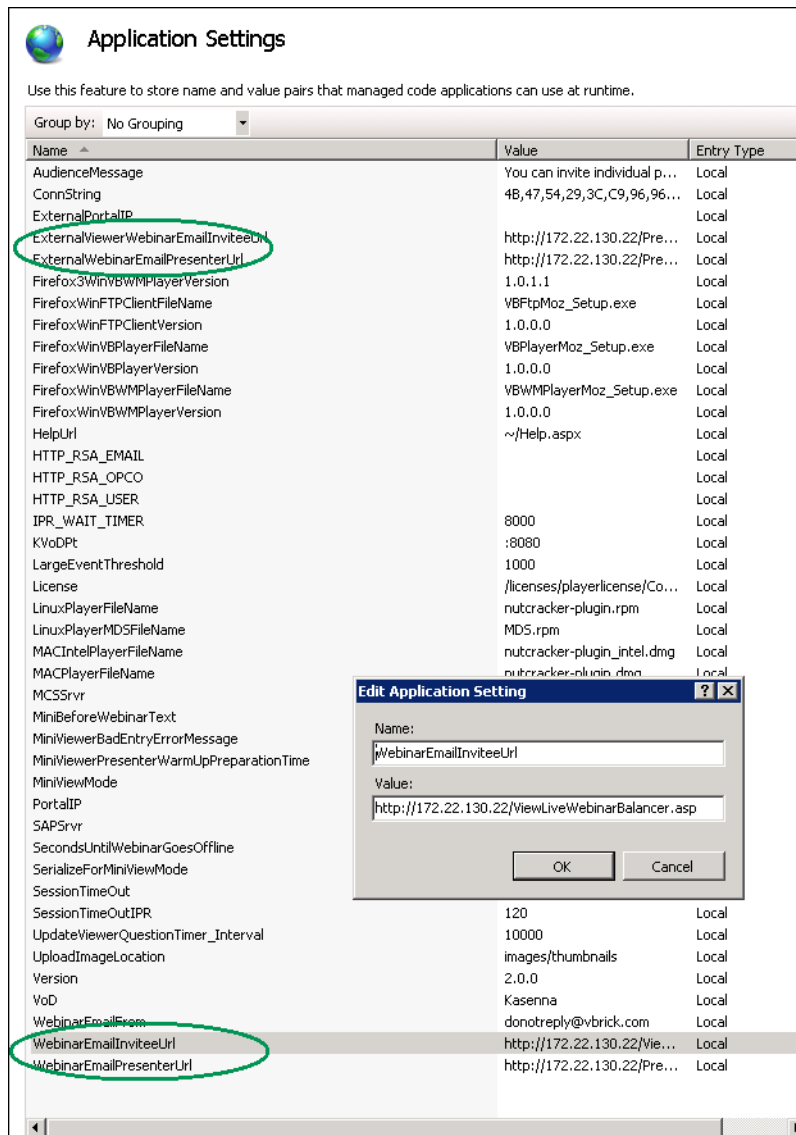
ExternalViewerWebinarEmailInviteeUrl	http://<external_IP_address>/Present/Launch_Detail_View.aspx
ExternalWebinarEmailPresenterUrl	http://<external_IP_address>/Present/Launch_Detail_View.aspx
WebinarEmailInviteeUrl	http://<internal_IP_address>/Present/Launch_Detail_View.aspx
WebinarEmailPresenterUrl	http://<internal_IP_address>/Present/Launch_Detail_View.aspx

4. Assign a VEMS Presentation User

Perform the following configuration *one time only* so that the Create Presentation tool in the client application can access the Portal Server. These steps will create a pseudo VBPresenter user who is associated with the authoring tool and has specific permissions on the Portal Server.

▼   To create a presentation user

1.   Open the Admin Console and go to **Users**.

2.   Add a user name (for example `PresentationUser`) and give this user the following permissions:

a. **Add/Modify Live Channel Privileges** – check the appropriate channels.

b. **Add/Modify Live Programs Privileges** – check the appropriate programs.

a. **Allow Access to Specific VOD Servers** – check the appropriate servers.

b. **Allow Access to Specific VOD Content** – check the appropriate folders.

c. **Allow Content Publishing** – check the appropriate folders.

3. Go to **Global Settings > Global Assignments > Assign Presentations** and select the user you created above (for example PresentationUser) as the **New Presentation User**.

Macintosh Configuration

Configuring Safari

If you use Safari as your web browser on any Macintosh computer, it will block pop-up windows by default. This prevents the Portal Server from creating an external player and also prevents full-screen mode from functioning properly.

▼ To configure Safari for Portal Server operation:

1. From the **Safari** dropdown menu, deselect **Block Pop-Up Windows**:
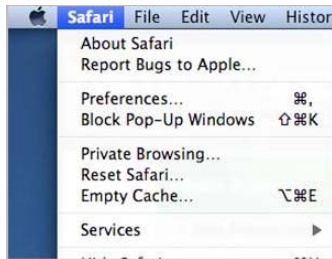
2. Then configure incoming connections as explained below. In order to view certain types of networked video streams, you must configure your Macintosh firewall to allow inbound UDP connections. This is configured differently depending on whether you are using Snow Leopard, Leopard or Tiger.

Configuring Snow Leopard

If accessing the Portal Server from a Mac OS X Snow Leopard machine with Safari, no streams will play unless you change the default 64 bit mode to 32 bit.

▼ To change Safari to 32 bit mode:

1. On the Macintosh desktop, go to **Finder > Macintosh HD > Applications > Safari**.

2. Right-click on the **Safari** icon and select **Get Info**.

3. Check **Open in 32-bit mode** and close the window.

Configuring Leopard

▼ To configure Macintosh OS/X 10.5 (Leopard):

1. Go to **System Preferences > Security**, then select the **Firewall** tab. You will see a window that looks like this:
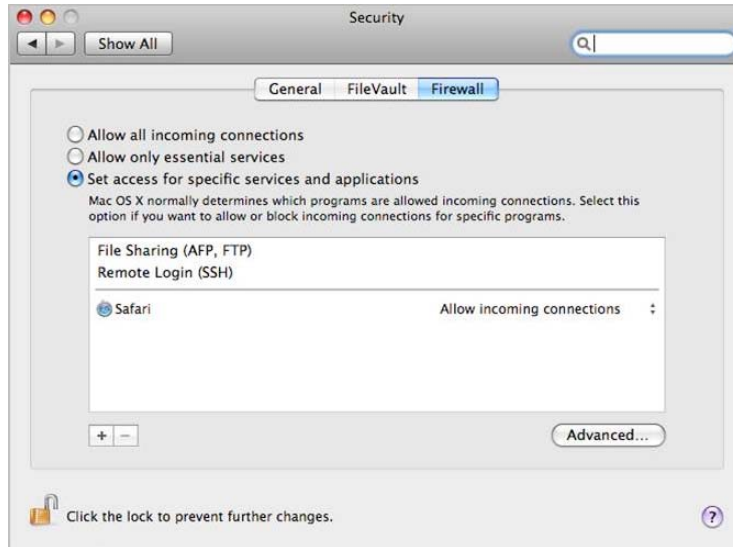
2. Set the Firewall either to **Allow all incoming connections** (not secure) or to **Set access for specific services and applications** (recommended). If you select the latter item, you must then click the **+** icon at the bottom of the window and add your web browser (Safari or Firefox) to the list. Note that the system will not work if you set the firewall to **Allow only essential services** because UDP packets will be blocked.

Configuring Tiger

▼ To configure Macintosh OS/X 10.4 (Tiger):

1. Go to **System Preferences > Sharing** and select the **Firewall** tab:
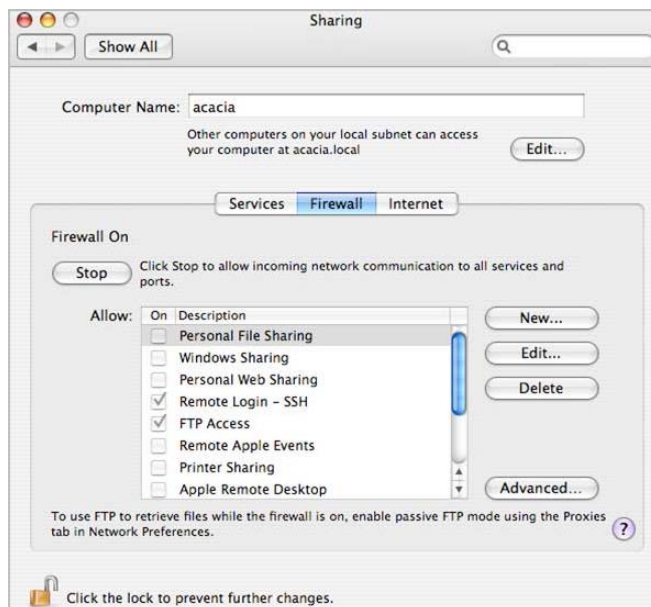
2. Then click the **Advanced** button and make sure that **Block UDP Traffic** is off as shown below.

Installing Macintosh Components

Depending on the **Specify Components to Download to Clients** setting on the Portal Server Global Assignments page, Macintosh users may be prompted to download VBrick player components the first time they launch a stream. These components must be installed to view all stream types (MPEG-1/2/4, Windows Media, H.264) and a separate download may be required for each.

▼   To download and install Macintosh components

1. Click on the link to download the VBrick Macintosh video player plugin. This will display the following window.
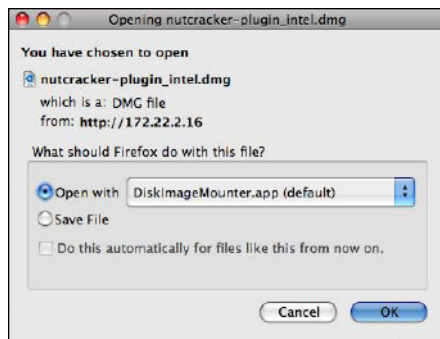
2. Select **Open with** and click **OK** and double-click on the `nutcracker-plugin-x86.pkg` to install the plugin. Follow the prompts and accept the defaults.
3. An administrator-level account is required to install the plugin. **Contact your system administrator and enter an appropriate administrator password when prompted.**
4. When done, restart your computer to complete finish the installation.
5. Verify the plugin is successfully installed.
    a. Open a Portal Server client window and launch a video.
    b. Ctrl-click on the video and select **About** from the popup menu. Verify that `Plugin 3.2.12` is installed.

Cardinal Peak Nutcracker(tm) Plugin 3.2.12

Copyright (c) Cardinal Peak, LLC. 2003-2008. All rights reserved. Portions based on open-source code, including the libraries libmpeg2, libmad, libfaad2, mp4v2, and ffmpeg. Source code for these modules is available at www.cardinalpeak.com.

Build 090111-1716 from bents-fort.cardinalpeak.com, using libcornet 3.2.12.
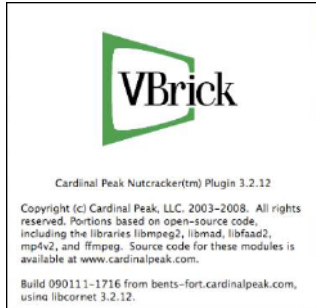
Upgrading Macintosh Components

If a Portal Server client machine has an older version of VBrick components installed, you must manually upgrade the player as explained below. **The Portal Server will not alert you that an update player plugin is available or required.**

Note If you do not upgrade the player on your Macintosh client machines to the latest version, older video content will continue to play as before but new features such as H.264 and Firefox 3 support will not be available.

▼ To upgrade an existing Portal Server client machine

1. Open the Portal Server in a web browser on the client machine requiring an update, launch a video, and check the *current* player version using the steps outlined above.

2. Ctrl-click on the video and select **About** from the popup menu. If the version number is less than 3.2.12 continue to the next step to perform an upgrade.

3. In the browser address bar, type the following URL:
   - Power PC Macs – **http(s)://<<Portal Server IP or Host Name>>/nutcracker-plugin.dmg**
   - Intel Macs – **http(s)://<<Portal Server IP or Host Name>>/nutcracker-plugin_intel.dmg**

4. When prompted, open the file, follow the prompts, and enter a password as explained above.

5. When done, restart your computer and verify the plugin is successfully installed as explained above.

Security Policy and Recommendations

VBrick has fully tested the all of its server-based software products on Windows Server 2003 and Windows Server 2008 with all current Microsoft security updates installed. It is standard VBrick policy to configure and ship our servers with all current service packs and security updates as of the shipping date of the product. We also run limited regression tests when new service packs are released by Microsoft. Once VBrick software is installed at a customer site however, it becomes the customer's sole responsibility to install security updates and software patches as they become available. To protect against imminent threats, VBrick recommends you install and/or test all Microsoft security updates as soon as they become available.

▼ To see what security (and other) updates are installed:

1. Go to **Start > Windows Update**.

> **Note** To avoid impacting server operation or performance, VBrick recommends you set "Automatic Updates" to **Check for updates but let me choose whether to download and install them**. This way you can install updates during off-peak hours without affecting viewers.

2. In the right navigation pane, click **View update history** to display the history of all installed updates.

3. If necessary, go to **Start > Control Panel > Add or Remove Programs** to remove an unwanted update.

Security Recommendations for Internet Explorer 8

Microsoft Internet Explorer 8 has standard security options that may prevent the Portal Server "Add Video" function from working properly. In order to successfully ingest recorded video to a VOD server you may have to configure one or more of the following options in Internet Explorer depending on whether the Portal Server is in an internet or an *intra*net "zone." Depending on your local environment, you may also need to add the Portal Server to the list of trusted sites.

Add to Internet Zone

▼ To use the Portal Server in the Internet zone:

1. Go to **Tools > Internet Options > Security**.
2. Select the **Internet** zone and **Custom Level**.
3. Enable **Include local directory path when uploading files to a server**.
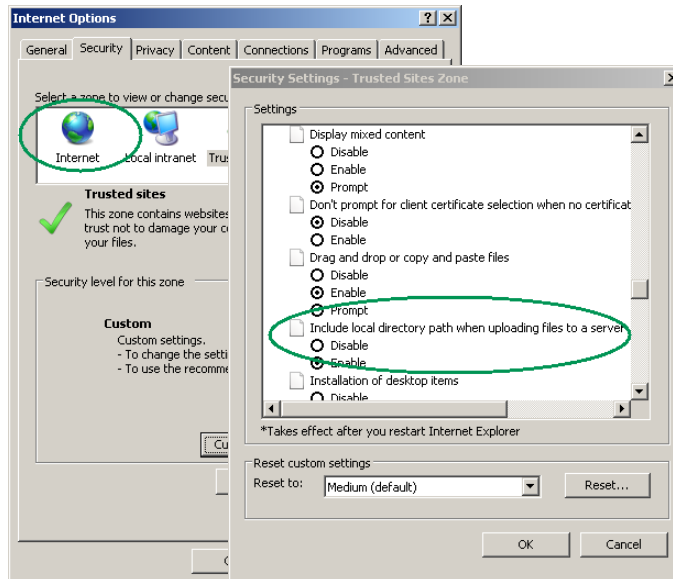
Add to Intranet Zone

▼ To use the Portal Server in the Intranet zone:

1. Go to **Tools > Internet Options > Security**.
2. Go to **Local intranet** > **Sites > Advanced.**
3. Add the Portal Server IP address to the zone.
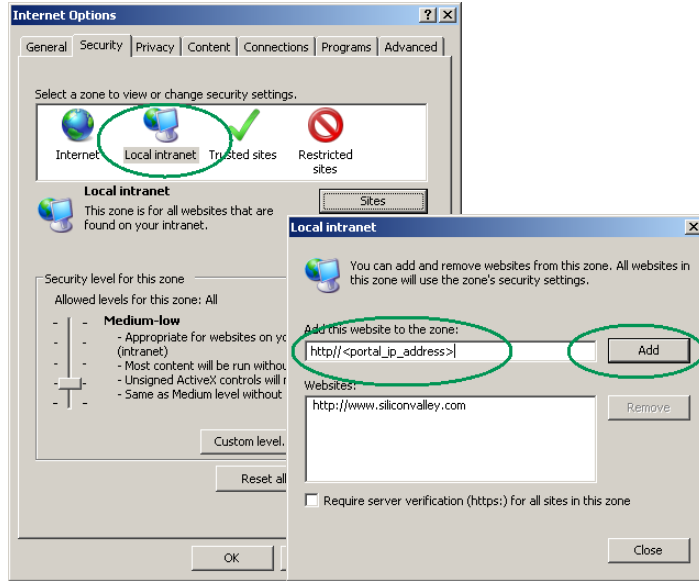
Add to Trusted Sites

▼ To add the Portal Server as a trusted site:

1. Go to **Tools > Internet Options > Security**.
2. Go to **Trusted sites** > **Sites > Advanced.**
3. Add the Portal Server IP address to the zone.
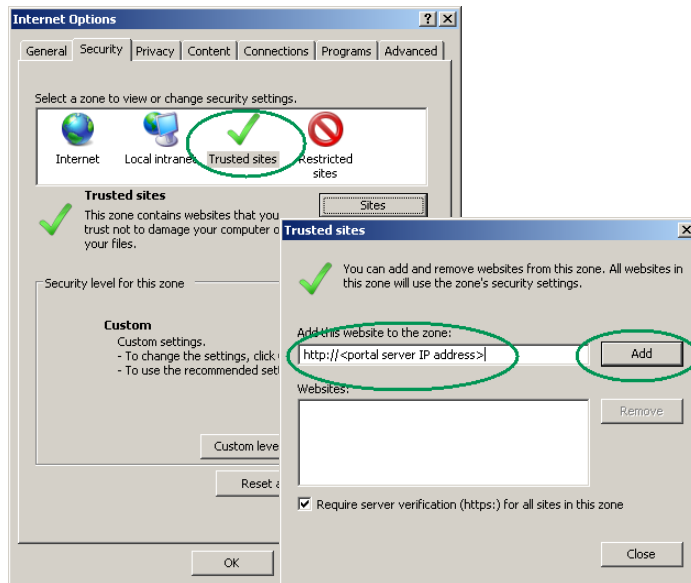
Caveats

This section addresses known issues, most of which have an easy workaround. For more information about any item, or help with an issue not listed here, contact your reseller or VBrick Support Services. The caveats below are arranged into categories as follows. *Note that the VEMS category includes the Portal Server, NVR, VBrick encoders, etc.*

VEMS

- To avoid conflicts when recording a presentation, always wait until the first presentation has been completely FTPed and ingested (check the **More Tools > Status** page) before starting another recording.

- CaptureID is not found. This error indicates there was a problem with a recording. When a recording fails, VBRecordService sends the status to VBUservice on VEMS server and removes the VBASR object from the list it maintains. VBScheduleEngine sends a StopCapture at the end of scheduled time interval but VBRecordService returns the error CaptureID is not found because the corresponding VBASR object has already been removed. To resolve this issue, check the **Status** page or the **Live Media** page to see if there are other errors returned by VBRecordService via VBUService. For more detailed information, enable logging for some of the recording components. (7303)

- VBrick appliances use Programs Names that are associated with a Session Announcement Protocol to identify encoded streams. This SAP text is displayed in the Portal Server Scheduler and in other places. Be aware that duplicate Program Names may cause unpredictable results when playing or scheduling streams.

- When modifying a scheduled, private conference (between MPEG-4 appliances only) to run again at a later date, you may get an Invalid IP Address error on the **Advanced Settings** page. To work around this error, select a different Destination in Advanced Settings, and then select Destination 1 again.

- If **URL Password Protection** is enabled for a VOD-W server, the length of the VOD content URL (rtsp://ServerIP/Folder and Filepath/Password Key) may exceed the maximum character length (100 chars) and the video will not play. To work around this issue, you can reduce the number of characters in the VOD asset name.

- When recording H.264/MPEG-4 files there is a "hinting" phase at the end of the recording phase designed to reduce CPU overhead and preprocessing. In extreme cases, the hinting may take over an hour depending on number of recordings, bit rate, and duration. When the Portal Server "Status" page shows "Recording in progress" and 100% done, it means the recording is done but the hinting is still in progress. When the hinting completes, the file can be FTPed to the VOD servers.

- MPEG-4 and H.264 appliances only. If you change the appliance's management port (default = 80), and the appliance is <u>not</u> in the Portal Server database, the Portal Server will not discover and play *multicast* streams from these appliances. To workaround this issue, manually add the appliance(s) to the Portal Server database.

- There is a known issue with the number of H.264 streams an NVR server can presently record. NVR H.264 recording capacity depends on the length of the recording, the bandwidth used, and the extent to which the recordings end at the same time. For short time frames and low bit rates, the system provides the specified number of recordings. In extreme cases of long recordings at high bit rates (for example 2 hour, 4 MB streams ending at the same time), an NVR 10 and an NVR 40 may be limited to 2 streams and 3 streams respectively. This issues applies to H.264 streams only and a patch is currently under development.

- A file server using secure playback can be configured with an IP address or a host name. If the server certificate is issued for an IP address, you must use the IP address; if issued for a host name, you must use the host name. Otherwise, the video will not play and a message will indicate the security certificate was issued for a different website.

- If two clients each try to record a stream at the same time, and the bandwidth required for both exceeds what is available on the VBrick (default = 20 mbps), the connection to the VBrick will be refused and one of the recording will fail with a message in the Status window. This is expected behavior.

- When creating playlists, the popup Javascript window that lets you set Start and End times will not function unless the Portal Server has been added to the list of trusted websites. Go to **Tools > Internet Options > Security** and add the Portal Server host name or IP address to the list of **Trusted sites**.

- The Portal Server supports Flash (.swf) streams on Windows-compatible machines only. When adding URLs to live and stored Flash files, set the Type to WM and these files will play in the Portal Server. Flash URLs are not currently supported on Mac or Linux machines.

- When recording from a WM encoder to a Network Video Recorder (NVR) 40 machine, and using the **Best Quality** template, the NVR's maximum recording capacity is reduced to approximately 10 streams. Other WM templates are not affected.

- When scheduling a recording from a WM Appliance, RTSP and HTTP streams are both displayed in the Scheduler as RTSP.

- When recording a stream from the WM IPR in Portal Server mode, a rectangular red box is displayed in the lower-right area of the window to show that a recording is in progress. If you never leave the page, you can stop the recording by simply pressing the **Record** again. If you leave the page however (e.g. if you choose **MENU** and select another option), you must reselect the stream (and *then* press **Record**) to stop the recording and close the box.

- If the **Receive Address Mode** of an MPEG-2 decoder is configured for **Program Name**, and the Portal Server is scheduled to stream to this VBrick, the video will not play as scheduled. There is no workaround. This is a known bug and was fixed in VBDNA v4.2 firmware.

- When scheduling a live or a stored broadcast from a VBrick appliance that has multiple bit rate (MBR) enabled, the scheduled broadcast will use the VBrick's configured bit rate regardless of the template setting in the Scheduler. In this scenario, the Scheduler may generate error messages similar to the following on both the Portal Server's **Diagnostics** page and the VBrick's **System Log**. These messages can be safely ignored and the schedule will execute properly.

  Failed to Set<vbrickSlot1EncoderNetwork TransmitEnable=1>
  Slot1EncoderTemplateApplySet set to applySet failed

- When creating a stored broadcast schedule, the schedule will fail to create if the schedule **Start** date and **End** date are different (for example if it starts on one day and ends on the next). The end date and time in the schedule are adjusted to the duration of the stored file (except for Windows Media or Darwin files) but **Create Schedule** returns an error message. To work around this issue, simply click **Modify** and then click **Finish**.

- When playing a stored video on the external player, if you upload an image for a thumbnail, and then switch streams while the **Update Image** panel is still open, any subsequent thumbnail you upload will be applied to the first stream for which you originally uploaded a thumbnail.

- Depending on the order in which they were originally installed, video streams may not run in the embedded player after you uninstall Internet Explorer ActiveX controls or Firefox plugins. To work around this issue in Internet Explorer, go to **Start > Control Panel > Internet Options > Settings > View Objects** and remove the following objects (if present) with Internet Explorer closed: CVBUI, CFtpClientMgr Object, VBrick Streamplayer Components, VBrick MPEG4 Components. Then go to VEMS and re-install them when prompted. To work around this issue in Firefox, simply download and install the browser from Mozilla.

- When switching between streams and/or switching between the integrated player and an external player, the embedded Windows Media Player will sometimes lose its ability to go fullscreen. This is a documented Microsoft problem with a patch available from: http://support.microsoft.com/?kbid=912452&SD=tech

- If you are FTPing non-English file names in IIS (for example when using the Portal Server SDK), there may be issues with Unicode support. If file names are not correctly displayed, go to **Control Panel > Regional and Language Options > Languages** and select **Install Files for East Asian Languages**. After rebooting go to **Control Panel > Regional and Language Options > Advanced** and select a language in the **Language for non-Unicode programs** control box. After a reboot the file names will display in the selected language on the FTP site using a command prompt window (on a Windows XP machine) or the Internet Explorer browser.

- When creating a Live Emergency Broadcast template from a WM appliance, if you set **Advanced Settings > Schedule Start Options > HTTP Push** to **Enabled** the existing Encoder Server settings will be used. Therefore, you also need to configure the WM appliance for the push. In IWS, go to go to **Configuration: Encoder > Server** and configure the Server Name or IP Address and Publishing/Mount Point. See "Creating Publishing Points" in the *WM Appliance Admin Guide* for more information.

- If you configure an MPEG-4 appliance with Audio and Video disabled and Closed Captions *enabled* (in extremely low bandwidth applications, for example), you must have **CC ON** set in the embedded Portal Server player or no stream (from any appliance) will play. If this happens, set closed captions to **On**, then close the browser and restart.

- When configuring the Portal Server to use LDAP database for access control, be aware that an LDAP user for **Auto Ingest via XML** is not supported. You must create and select a VBrick user in **Global Assignments** or the Event Viewer will display: `Failed to update ingestion status: Input string was not in correct format.`

- On Portal Server v3.2 or higher, an autoingest folder is not created until you record a program for the first time. If you want to autoingest before a recording, you must manually create the autoingest folder at `d:\inetput\ftproot\mcs\autoingest`. If you don't have a `d:` drive, use `c:\inetpub\ftproot\mcs\autoingest`.

- In some cases, because of a naming resolution issue, a LAN Network Video Recorder (NVR) does not record when the VEMS Portal Server server is in a DMZ. As shown on the status page, the recording will either fail or run indefinitely (without actually recording). To work around this issue, modify (or create) a `hosts` file on the VEMS Portal Server as shown below. Go to `c:\windows\system32\drivers\etc\hosts`. Open the `hosts` file in an editor and add the IP address and computer name of the NVR as shown below. (If the `hosts` file is not present, you must create one by saving a `txt` file with no extension.)

```
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
```

```
# space. Additionally, comments (such as these) may be inserted on
# individual lines or following the machine name denoted by a '#' symbol.
# For example:
# 102.54.94.97     rhino.acme.com # source server
# 38.25.63.10      x.acme.com     # x client host

127.0.0.1         localhost
nvr ip address    nvr computer name
```

- Use care when configuring virus scanning software. To avoid problems when recording on the VEMS Portal Server, do not scan any folders into which recorded files are being saved. This is typically: `D:\Inetpub\ftproot\MCS\Record`.

- When creating an Emergency Broadcast template for a live broadcast and *manually selecting* **MPEG-4** and **Program Name**, the destinations available page shows only VBricks—it does not show IPRs. Manual entry of Program Name does not apply to IPRs.

- If an ingestion fails after a record and you wish to use the auto-ingest feature, be sure to purge the failed ingestion on the Status page before attempting the auto-ingestion.

- The VEMS Portal Server and the Network Video Recorder (NVR) must be in the same time zone. Also, in order to record successfully, the system time on VEMS Portal server and the NVR must be synchronized. You can synchronize the machines, for example, by running the Service for Windows Time on both machines.

- When scheduling a broadcast of MPEG-4 content from an InfoValue server to a VBrick decoder, v3.3 or higher software must be installed on the VBrick or the video will not play. Also the MPEG-4 file must be "hinted" or it will not play properly on the VBrick decoder. Hinted files contain reorganized data that facilitates streaming, fast forward, rewind, etc.

- When IIS installs the FTP service, a default FTP directory is created at `drive:\Inetpub\ftproot`. In MSC 4.2 or higher the **Record Path** must be in the FTP path of the Record server, for example: `C:\Inetpub\ftproot\MCS\Record`. To set **Record Path** in VEMS Portal Server, go to **Global Settings > Recorders > Modify Recorders > Record Path**.

- You cannot create or upload thumbnails for Live Video streams that were added using the VEMS Portal Server **Global Settings > URLs** functionality. Any attempt to create thumbnails for these URLs will fail.

- VOD Polling interval requires a restart before changes take effect. On Admin page, go to **Global Settings > Global Assignments > Assign VOD Polling Interval**. If you change the value, you must restart Vbrick Object Starter Service on the VEMS Portal Server for this parameter to take effect.

- There is an issue with Admin settings for **Allow Access to Specific VOD Content** and **Allow Content Publishing**. If you check a parent directory, the sub-directories are also checked to indicate that the user has access to all sub-directories. However, at present there is no way to keep the user from unchecking a subdirectory. Regardless whether the user unchecks a sub-directory whose parent directory is checked, VEMS Portal Server will still allow access to the sub-directory.

- The installer now changes the default root password for the MySQL database from no password to `vbrick_18`.

- For one-click login, if you type in the IP Address, rather than the name of the machine, you will be prompted for a username/password box. This is intended behavior as IE sees the IP Address and believes the user is in the Internet Zone. If you click on **Remember my password** you will not see the box again.

- If a user has defined a default IPR channel, and then removes that particular customized channel in the **Customize Streams** page, that default IPR channel is still listed as the current channel, even though it no longer exists.

VOD Servers

- Darwin VOD Servers – Some Darwin Open Source VOD Servers have a 2 GB limitation for H.264/MPEG-4 files. Video files greater than 2 GB from a Darwin server, may not play on any player or platform. Check with the Darwin open source community (`http://developer.apple.com/opensource/`) for updates.
- When using dual NICs on any Windows VOD server, communication between the NICs may fail if there is no path in the routing table from one NIC to the default gateway. To work around this issue, add a path to the default gateway as explained in the Windows Server documentation.
- When ingesting content to a VOD-W Server, all content titles must begin with a forward slash (/) and apostrophes are not allowed.
- The VOD W server supports streaming of MPEG-4 closed captions; the NXG server does not. This means that if you have access to two servers (a VOD W and an NXG), and you perform a pushbutton recording of an MPEG-4 stream with closed captions, the closed captions track is stripped from the recording.
- Depending on user requirements, VOD users can be restricted to viewing RTSP streams at a specified bandwidth in Kbps. This feature is not currently supported for Darwin and VOD-WM video-on-demand servers.
- The duration of Darwin and WM video assets is not extracted in this release. As a result, the duration of a stored broadcast *schedule* for a Darwin or WM asset will not be automatically adjusted to the actual length of the clip. This means that the video asset plays until file end but the multicast continues until the end of the scheduled time.
- Multicast streaming from the VOD-D (Darwin) server is not supported.\

Internet Explorer

- When installing download components (FTP .cab) from the **Add Video** page using Internet Explorer 8, an error page may be displayed. This will only happen after the first download. If this error occurs, exit the browser and restart.
- Web page errors can occur in Internet Explorer 7 when running the Admin console and the Scheduler on separate tabs in the same browser instance. For example, if you modify an Emergency Broadcast template on one tab and then try to modify a schedule on a different tab, Internet Explorer will report a web page error.

FireFox

- Firefox only. When playing a stored WM stream on a Windows 2000 machine, the Pause control will black out the player window when you pause and then play. Do not use Pause. This is a known issue with no workaround.
- Firefox only. When viewing a playlist in an external player window, the external window does not stay on top when the clip changes. To change this behavior, Go to **Tools > Options > Content**. Click the **Advanced** button to the right of the **Enable JavaScript** checkbox, then check **Raise or lower windows**.

- The controls for some Portal Server features (for example Presentations and Playlists) will simply refresh the page. For these controls and features to work properly in Firefox, you must set Javascript options as shown here. Go to Tools > Options > Content > Enable Javascript > Advanced and check Raise or lower windows.
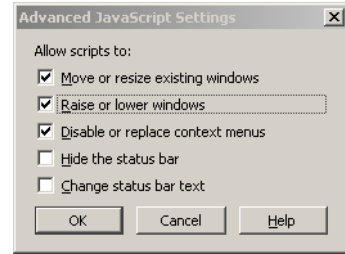
Windows

- Windows Web Server 2008 only. The Portal Server typically runs behind a firewall and is installed by default with Windows Firewall set to **Off**. If necessary, you can use the following steps to configure the Portal Server to run with Windows Firewall set to **On**.

    1. Go to **Start > > Control Panel > Windows Firewall**. Check that the Firewall is **On** and click **Allow a program through Windows firewall**.
    2. To allow client access to the web server, go **Add port** and add Port 80 (TCP) to the Exceptions list.
    3. To enable FTP, go to **Add port** and add Port 21 (TCP).
    4. To enable live streams, go to **Add program** and navigate to
       C:\Program Files\Common Files\VBrick\VBSapSrv
    5. To enable recording, go to **Add program** and navigate to
       C:\Program Files\VBrick\Asr\VBASR.exe
    6. To enable thumbnails, go to **Add program** and navigate to
       C:\Program Files\VBrick\MCS\ThumbNailCreator.exe

- With Windows Web 2008 (and Automatic Updates selected), warning messages can be generated by the Data Execution Prevention (DEP) software. To workaround these messages go to **Start > Control Panel > System > Advanced system settings >** (Performance) **Settings > Data Execution Prevention** and add the flagged VBrick module as an exception.

- Windows Vista only. Live streams and stored streams will not work properly in fullscreen mode if you have the **Color scheme** set to **Windows Aero**. If this Vista option is selected, go to **Appearance and Personalization** and select a different color scheme.

- To avoid problems when recording content, the Windows Firewall must be set to **Off**. Go to **Start > All Programs > Windows Firewall** to turn it off.

- The default FTP path in IIS is automatically set via the installer, but, depending on the particular machine's configuration, it may need to be changed. The installer sets the default FTP path to d:\inetpub\ftproot in IIS, if a D: drive is detected. Otherwise it sets the path to c:\inetpub\ftproot. If you have a machine with an E: drive and you want to set the FTP path to E:, you need to do the following: Go to IIS and use the right mouse button to select on the Default FTP Site, select **Properties** from the popup menu. The Default FTP Site Properties dialog box will appear. Select the **Home Directory** tab. In the **Local Path** edit box, change the value to e:\inetpub\ftproot and hit **OK**.

Macintosh

- Macintosh (Safari) and Linux (Firefox) clients may not play live or stored video after a Portal Server upgrade. Clearing the browser cache will usually resolve this issue.

- Macintosh (Safari and Firefox) and Linux (Firefox). MPEG-4 content encoded using the 56K template will not display closed captions.

- Macintosh only (Safari 3.0 or higher). If Apple QuickTime is enabled in Global Settings as the default Macintosh Player for MPEG-4 Content, the QuickTime player will freeze the first time you click on any item. Click again to unfreeze and continue.
- Macintosh only. Safari 3.0 or higher. If Apple QuickTime is enabled in Global Settings as the default Macintosh Player for MPEG-4 Content, and the browser becomes unresponsive, click anywhere on the QuickTime player to recover.
- Macintosh only. When multiple external windows are enabled, recording is disabled and you can only record the stream shown in the preview window. In some cases the **Record** button may be displayed on external windows even though it is non-functional.
- When using a Macintosh with Safari, you cannot always launch a stored stream from the Scheduler page by clicking on the TV icon. To work around this issue, launch the stream from the **Live Media** page instead.
- Macintosh only. The mute button is not "sticky" and works for the selected (live or stored) stream only . If you select a different stream, it will not be muted.
- QuickTime 7.6 only – To play H.264 streams, you must set Direct3D video acceleration to off in QuickTime Preferences. (This option is enabled by default.) Go to Edit > Preferences > QuickTime Preferences > Advanced > Video > DirectX and uncheck **Enable Direct3D video acceleration**.
- On Windows PCs, you must have Apple QuickTime 7.5.5 installed to play MPEG-4 and H.264 streams with QuickTime.
- QuickTime (using Firefox or Safari) does not support Fast Forward or Rewind when playing a stored MPEG-4 stream. The FF and RW buttons on the QuickTime player simply pause the stream.

VBrick Systems, Inc.
12 Beaumont Road
Wallingford, Connecticut 06492, USA