VBrick Enterprise Media System

VEMS v5.4 Portal Server Admin Guide

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 v5.4 Admin Guide

1. Introduction

2. Global Settings

3. Server Administration

4. Users and User Groups

Portal Server v5.4 Admin Guide

Preface

his *Portal Server Admin Guide* is written for anyone who will be using or evaluating the VBrick Enterprise Media System (VEMS) Portal Server. This includes system administrators, software developers, network technicians, and others. The VEMS Portal Server is a web-based portal for accessing and managing video assets including both live or stored audio and video files. The VEMS Portal Server is a key component in VBrick's Enterprise Media System. The VEMS Portal Server provides a simple, intuitive interface that auto-discovers available media assets in your network. Key components in VBrick's Enterprise Media System include:

- VEMS-VOD Video-on-Demand Servers – Provide all standard Video-on-Demand (VOD) features including support for MPEG, Windows Media, and H.264 for maximum flexibility.
- VBrick Hardware Encoders/Decoders – Rugged, reliable video appliances that can reside anywhere on your network to provide either distributed or high-density centralized encoding/decoding of MPEG-2, MPEG-4, WM (Windows Media), and H.264 video.
- VEMS IP Receivers – Leading-edge digital set top boxes that provide a low-cost standalone decoder for MPEG, Windows Media, and H.264 video assets.

Note The Amino STB is a compact set top box that plays MPEG-2 streams only. It is fully integrated with the Portal Server and provides access to *most* Portal Server viewer functionality. *It does not, however, support* Access Logging, Scheduling, Device Control, Emergency Broadcast, or Copyright Restrictions.

---

1. Introduction	provides an overview of the application including server and desktop requirements and an overview of features and functionality.
2. Global Settings	explains high-level configuration settings and parameters that apply to the entire system.
3. Server Administration	provides detailed explanations of all VEMS Portal Server global settings and configuration options, as well as diagnostics and status windows.
4. Users and User Groups	explains how to configure the system for access control. It explains how to create users and groups with specific permissions and access to resources.
5. Configuring for SSL	explains how to securely configure the system using the Secure Sockets Layer.
6. Configuring for Presentations	explains how to configure the Portal Server for encoder presentations and device presentations.

7. Network Video Recording	explains how to configure and use an NVR to offload recording tasks from the Portal Server to a separate "recorder server" machine.
8. Auto Content Ingestion	explains auto content ingestion. This is the process whereby video content is automatically populated on the portal server.
9. Automatic System Backup	explains how to automatically backup the MySQL database and other key directories if you purchased ETVBackup.
10. Manual System Backup	explains how to manually backup the MySQL database and other key directories if you did not purchase Enterprise Media System Backup.
11. AmiNET110 MPEG-2 STB	explains how to connect and use the Amino set top box to view MPEG-2 streams.
12. ACNS Configuration	explains how to configure the Portal Server and Cisco's Application and Content Networking System (ACNS) to work together.
13. NXG-to-VOD-W Content Migration	explains how to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG (Linux) VOD server to a VBrick VOD-W (Windows) VOD server.
14. Purchased Content Ingestion	explains how to mass ingest separately purchased video content to any or all configured VOD servers.
15. VBrick Internet Streaming	the VBrick Streaming Service is available for those users who wish to extend the ability to view live events to Internet clients.
16. Embedding a VBrick Player	explains how to add an embedded VBrick player to a web page or to Microsoft SharePoint so that it can display an embedded list of VOD content.
17. Configuring a DVB Gateway	explains how to configure a DVB-T gateway that will auto discover and play live broadcast channels in Europe.

Getting Help

If you need help, or more information about any topic, use the online help system. The online help is cross-referenced and searchable and can usually find the information in a few seconds. Use the tree controls in the left pane to open documents and the up and down arrows to page through them. Use the **Search** box to find specific information. Simply enter one or more words in the box and press Enter. The search results will return pages that have all of the words you entered—highlighted in yellow (Internet Explorer only). The **Search** box is not case-sensitive and does not recognize articles (a, an, the), operators (+ and –), or quotation marks. You can narrow the search by *adding* words.

If you can't find the information you need from the online help, or from your certified VBrick reseller, you can contact VBrick Support Services on the web. Support Services can usually answer your technical questions in 24 business hours or less. Also note that our

publications team is committed to accurate and reliable documentation and we appreciate your feedback. If you find errors or omissions in any of our documents, please send e-mail to documentation@vbrick.com and let us know. For more information about any VBrick products, all of our product documentation is available on the web. Go to www.vbrick.com/documentation to search or download VBrick product documentation.

Note	VBrick has made every effort to ensure that the information in this document is accurate at the time of publication. However if we find are errors or omissions, VBrick reserves the right to make changes without notice. To see the latest documentation for this product go to www.vbrick.com/documentation

Font Conventions

Arial bold is used to describe dialog boxes and menu choices, for example: **Start > All Programs > VBrick**

`Courier fixed-width font` is used for scripts, code examples, or keyboard commands.

`Courier bold fixed-width font` is used for user input in scripts, code examples, or keyboard commands.

This bold black font is used to strongly emphasize important words or phrases.

Folder names and user examples in text are displayed in this sans serif font.

User input in text is displayed in this bold sans serif font.

Italics are used in text to emphasize specific words or phrases.

Related Documents

VEMS Portal Server User Guide

VEMS Reporter User Guide

IPR Receiver Admin Guide

VOD-W Server Admin Guide

VOD-WM Server Admin Guide

Printer-Friendly

Click on the following link to print a hard copy of the document.

VEMS Portal Server User Guide

VEMS Portal Server Admin Guide

VEMS Portal Server Release Notes

▼   To save or print a PDF document:

1. Click once to open the PDF document in Acrobat Reader.

2. To save or print a PDF document, right-click and select **Save Target As** or **Print Target**.

Introduction

Topics in this section

Portal Server Overview

VBrick's Enterprise Media System (VEMS) consists of a group of products that includes the VEMS Portal Server, VEMS Encoders, the VEMS-VOD Video-on-Demand Server, VEMS IP Receivers and StreamPlayer software. This integrated system delivers both live and on-demand audio and video over an IP-based infrastructure. The VEMS Portal Server functions as a video portal, permitting end users to view live and on-demand MPEG, WM (Windows Media), and H.264 streams on a Window PC, a Macintosh, or a set top box. The VEMS Portal Server comes as software-only solution that can be installed on a Windows Server or as a pre-configured hardware/software combination.

Figure 1. VBrick Enterprise Media System

The VBrick Enterprise Media System Portal Server is a web-based portal for accessing Live and On-Demand audio and video files. A key component of VBrick's Enterprise Media System, the VEMS Portal Server provides a simple interface to easily locate available media assets on your network. Upon accessing the main portal page, users can navigate or search

for specific videos, select the video, and immediately begin viewing DVD quality video. For on-demand videos, users can **Fast Forward/Rewind** and **Seek** to specific points in the video. Standard access control functionality provides restriction of certain content to particular users, user groups, or IP receivers. An optional scheduling module allows users to schedule devices to send video, receive video, record video, or to initiate a two-way conference.

Server Requirements

The *minimum* server requirements include:

- Windows Server 2003 (Web Edition or Standard Edition).
- Windows Server 2008 (Web Edition or Enterprise Edition).
- Pentium IV or Xeon Processor 1.26 GHz Minimum (2 GHz or higher recommended).
- RAM 512 MB Minimum (1 GB or more recommended).
- Hard Drive 36 GB Minimum (larger for frequent recording).

Note VBrick has tested the VEMS Portal Server on Windows Web Server 2008. Note also that VEMS Portal Server also will not operate correctly on a server that is configured as a primary domain controller or with other network-related services and software.

Desktop Requirements

Windows-based PC and Macintosh users access the VEMS Portal Server through a web browser. For Windows-based PCs, on the first access to the server, VBrick StreamPlayer software is automatically downloaded to the PC. StreamPlayer software lets end users select a stream and view TV-quality video directly on a PC. Macintosh users view MPEG-4 video through the QuickTime player.

Table 1. Desktop Requirements

PC Type	Requirements
Windows PCs	• Windows XP, Vista, Windows 7. • 750 MHz Pentium III processor (Pentium IV required for H.264). • 512 MB RAM (1 GB recommended for H.264). • SVGA video card 1024x768, video card acceleration and 32 bit color recommended. • Minimum 250 MB hard disk space for installation. • Microsoft Internet Explorer 7.0 or higher. • Microsoft Windows Media Player 9.0 or higher. • Firefox 3.5 or higher. • DirectX Media Version 8.1 and higher.
Macintosh PCs	• Mac OS X 10.5 or higher for Intel-based PC. • Firefox for Macintosh 3.5 or higher. • Safari 3.1 or higher. • QuickTime Player 6.0 or higher. • Internet Explorer on a Macintosh is not supported.

Copyright Protection

The Portal Server uses copyright restrictions and content expiration to protect the rights of content owners and to enforce rules against unauthorized usage or distribution. Copyright

restrictions are specifically used to enforce license requirements. Content is often restricted to a limited number of viewers and you may need a license, for example, to view MPEG-2 content. In the Portal Server, **Max. Concurrent Viewers** is used to enforce copyright restrictions for any live, stored, or recorded video. If the number of concurrent viewers exceeds the configured value, the content will not play. (The **Max. Concurrent Users** restriction does not apply to viewers who tune in to a scheduled broadcast.)

Content expiration controls the length of time that specific content can be viewed. Content expiration is used for time-sensitive, copyrighted, or otherwise protected content that cannot be legally displayed after a specified date or a period of time. Users with appropriate permissions (see Copyright Restrictions & Expiration Privileges topic on page 141) can assign expiration dates or a viewing period when they use the **Add Video** feature. The viewing period starts at the time the content is added to the server. If desired, administrators can restrict expiration privileges to particular users or groups in which case only those specified users or groups (and administrators) can set content to expire.

Administrators can also assign an **Expiration Date** or **Viewing Period** for any stored video using the Modify VOD Content page. By default, recordings from live streams have no expiration date. However administrators can set default viewing periods for content recorded from specific live streams (see "Viewing Periods" in Stream Restrictions topic on page 33).

The VEMS Portal Server enforces content expiration by preventing the streaming or scheduling of content that is expired or will expire before the scheduled event. Once content has expired, administrators can set a new expiration date or viewing period. By default, expired content will remain in storage indefinitely unless you choose to delete it automatically using the **Set Expired VOD Content Treatment** option in Global Assignments.

The Portal Server writes to a log that tracks content expirations; administrators can view or purge this log as necessary (see Expired Content Log topic on page 117). In many installation an administrator is assigned to monitor and/or renew content that is about to expire. To facilitate this process, the Portal Server can be configured to automatically generate e-mail that notifies the designated administrator when content is about to expire by using the option in Global Assignments.
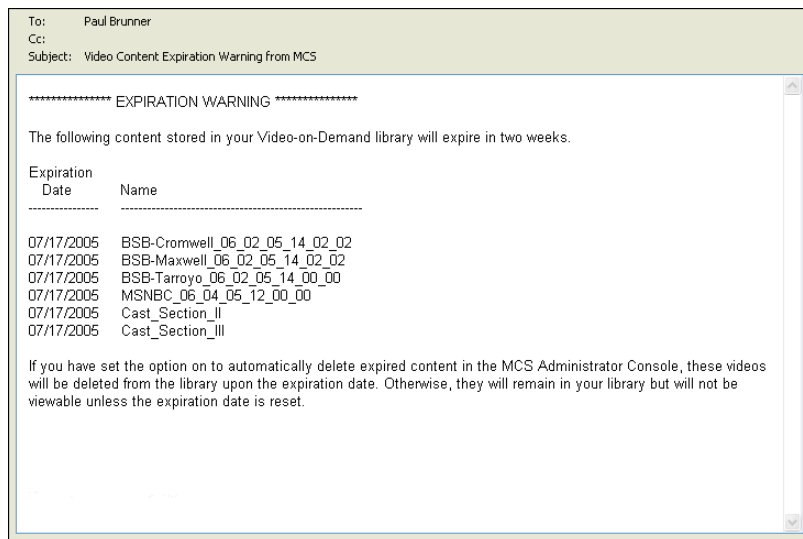
MySQL

The VEMS Portal Server is shipped with MySQL as the database. The MySQL database is installed as part of the Portal Server installation package. If the hardware/software combination was purchased from VBrick, MySQL will already be installed on your machine; the default user name is `root`. To protect the integrity of the database, you should change the default password (`vbrick_18`) after initial installation and periodically thereafter as explained below. To backup the MySQL database, see <u>Automatic System Backup</u> topic on page 185.

Note MySQL Query Browser is an Open Source front-end that provides a graphical interface to the MySQL database. MySQL Query Browser is available with the free software/open source GNU General Public License at to <u>http://www.mysql.com</u>

▼ To change the MySQL password:

1. Go to **Global Assignments > Change MySQL Password**.
2. Enter the Admin Username (**root**) and Admin Password (**vbrick_18**).
3. Enter the Username, the New Password (and confirm), and click **Submit**.

Microsoft Service Packs and Security Updates

It is standard VBrick policy to configure and ship our products with the recommended service packs and security updates available from Microsoft on the release date of the VBrick product. During product development, VBrick client and server applications are fully tested on the applicable operating system (Windows XP, Vista, Windows 7, Windows Server 2003, or Windows Server 2008) with the Microsoft service packs and updates available at that time. We also run limited regression tests when new service packs are released by Microsoft. Once installed at a customer site however, it becomes the customer's sole responsibility to continue installing security updates and patches as they become available. VBrick assumes no liability for damage resulting from the failure to patch your software. For best results, we recommend running Microsoft's "automatic updates" during off-peak hours when it will not affect users or impact performance.

Portal Server Features

End User Features

*   Windows-based PCs, Macintoshes, or IPRs (connected to televisions or display monitors) can all access the Portal Server.
*   Users can view video at **Full Screen** for a television-like user experience.
*   Users can view Video-On-Demand assets with full VCR/DVD control, including **Play**, **Pause**, **Stop**, **Fast Forward**, **Rewind**, and **Seek**.
*   Video can be viewed in a preview window or launched in multiple external, re-sizeable player windows (PC and Macintosh).
*   IP Receiver users can use familiar **Channel Up/Down** keys and other hot keys on the IR remote control to navigate through video listings.
*   Users can search through the list of Live or On-Demand videos by **Title**, **Tags**, **Description**, or other custom fields defined by an VEMS Portal Server administrator.
*   Users can record and store videos on the VEMS-VOD Video-on-Demand server via VEMS Portal Server.

- Users can publish pre-recorded content and thumbnails directly to the VOD server.
- Users can view closed caption text (Windows-based PCs and IP Receivers only).
- Users can launch pre-configured emergency broadcasts. (Optional. Requires Scheduling module.)
- Users can schedule recordings or broadcasts. (Optional. Requires Scheduling module.)
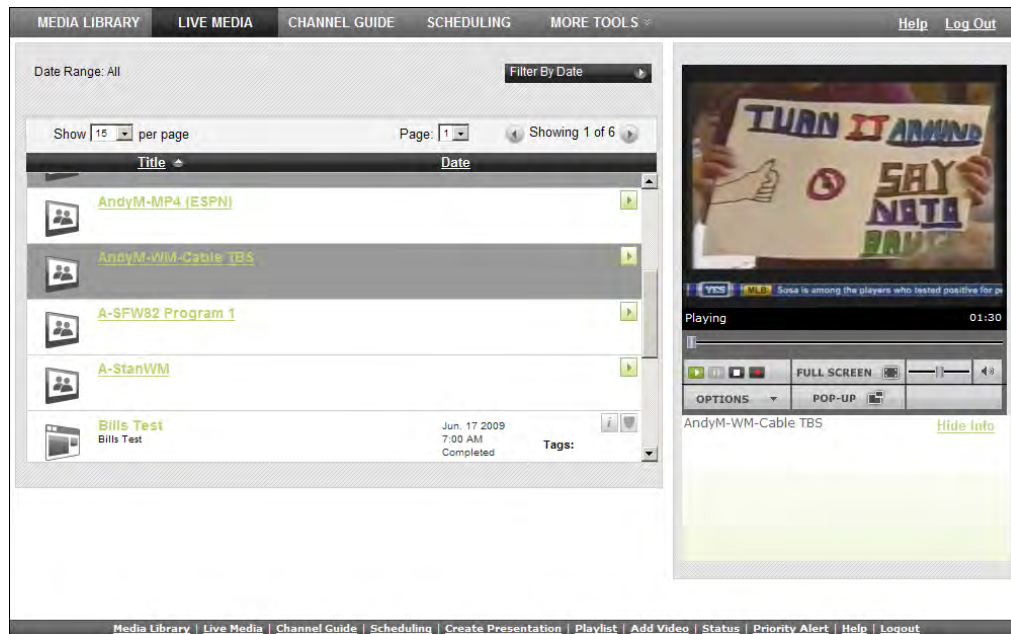
Figure 2. VEMS Portal Server Live Media

Administrative Features

- Access Control - allows administrators to allow/deny access to specific functions of the VEMS Portal Server server. Access control functionality can use the local VEMS Portal Server database or authenticate to an LDAP directory server.
- Clustering support – multiple VEMS-VOD Video-on-Demand servers can be clustered to increase total throughput. The VEMS Portal Server will automatically load balance all servers defined in VEMS Portal Server; no additional configuration is necessary. See Servers topic on page 33 for more.
- SSL/TLS security – the VEMS Portal Server can be set up to provide encrypted access to the Login pages and/or the Admin pages. See Configuring for SSL topic on page 147.
- Customer defined URLs – can be entered into the system and displayed in the VEMS Portal Server interface. The URLs can point to video assets or other assets such as PDFs or PowerPoint documents.
- Autoingestion to the VEMS-VOD server – content placed in autoingestion folders on the VEMS Portal Server will be automatically transferred and ingested into the VEMS-VOD server.
- Customized global messages can display on the VEMS Portal Server interface.
- Channel numbers can be assigned to live streams.
- Define a startup channel for IPRs – the IPR will automatically tune into this channel when users select the **Live TV** option.

- Emergency broadcasts – can define pre-configured emergency broadcast templates that can be launched instantaneously. See <u>Priority Alert</u> topic on page 85 for more.
- Status window – shows the status of videos being added, recorded, or ingested.
- Diagnostics window – displays a complete log of system events by source, time, and IP address.
- Custom fields and streams – the ability to add customized information and search parameters to live and stored streams.
- A Channel Guide Server can be configured to automatically provide third-party programming data for configured TV Stations.

Portal Server Components

VBrick Encoders/Decoders

VBrick's VB4000-5000-6000 Series MPEG-2 network video appliances provide DVD quality video and CD quality audio at 1–15 Mbps of bandwidth. MPEG-2 is the world's most popular digital compression technology and is used to encode DVDs as well as Digital Cable and Digital Satellite broadcasts. VBrick's VB4000-5000-6000 Series MPEG-4 encoders and decoders are versatile and reliable video appliances for one or two-way interactive communications over low or medium bandwidth IP networks. The VBrick MPEG-4 encoder/decoder can be used for webcasting, multicasting, transcoding, and two-way interactive video. Designed for streaming over the Internet at lower bit rates (56K, 128K, 384K) and over a LAN at higher rates (1Mbps and above). VBrick's WM (Windows Media) video appliances provide scalable quality at webcasting rates up to 2 Mbps. It features built-in live streaming server, automatic multicasting, and state-of-the-art reliability. A key benefit of the WM appliance is its compatibility with the Windows Media Player, thus eliminating the need for desktop player installation. VBrick H.264 appliances represent VBrick's newest networked video appliances. The new H.264 appliances can deliver vastly improved quality for a given bit rate, allowing organizations to deliver a better customer experience for any given bandwidth.

VEMS VOD Servers

VEMS Video on Demand (VOD) servers provide the VEMS Portal Server with a source of available video content organized in folders. The VOD content is displayed by name in the VEMS Portal Server user interface, along with the duration of the video, and associated descriptions, key words, and other custom information entered by an administrator. You play content from the VOD server by selecting the program name from the application interface (see the *Portal Server User Guide* for details). The VEMS Portal Server currently supports all of the VOD servers shown in Table 2. The configuration for each server is essentially the same (see <u>Servers</u> on page 33 for details) and there is little difference in functionality for end users.

VEMS servers can be LAN-based or Internet-based depending on how the range of Internet addresses is defined (see "Assign LAN/Internet Address Range" in <u>Global Assignments</u> topic on page 23). VOD servers accessible to Internet users are called Internet-zone servers; VOD servers assessable to LAN users only (within a secured corporate network and behind a firewall) are called LAN-zone servers.

Content added by users in the LAN zone will be ingested to all VOD servers for which they have permissions using the **Add Video** page. Users in the Internet zone have the **Add Video**

page available only if they have permissions for at least one VOD server that is also in the Internet zone. Content added by LAN users is added to all configured servers that can handle the content (for example you cannot add MPEG content to a Windows Media server) and for which you have permission. The content available for viewing may also be limited by the server type. For example, Internet users will see only MPEG-4 and Windows Media content on VOD-D and VOD-WM servers respectively. LAN users however will see all content on all servers.

Table 2. Supported VEMS VOD Servers

Server Type	Description	Zone
VOD-W	Windows-based VOD-W VOD server. Available in three versions depending on throughput: VOD-50W, VOD-125W, and VOD-300W	LAN only
VOD-WM-Standard	• Standard – Microsoft Windows Media Server (unicast only). Requires an FTP server. • Enterprise – Microsoft Windows Media Server (unicast or multicast). Requires an FTP server.	LAN or Internet
Wowza Flash Server	Supports Flash and H.264 files. Wowza is an alternative to the Adobe Flash Media Server.	LAN or Internet
Adobe Flash Media Server	A Flash Media Server (FMS) is a proprietary data and media server from Adobe Systems. The server can send data to clients with an FLV player installed.	LAN or Internet
VOD-D	Darwin Open Source server for Windows or Macintosh. Ingests and plays MPEG-4 content only. Requires an FTP server. Compatible but not sold or supported by VBrick.	LAN or Internet
QuickTime Streaming Server	A QTSS is a Unix-based device that runs on Mac OS X. QTSS is delivered as part of Mac OS X Server.	LAN or Internet
File Server	A Windows Media or H.264 VBStar encoder can be configured as a progressive download server.	LAN or Internet

VEMS Internet-Based Servers

VEMS Portal Server supports the installation of LAN-based servers and Internet-based servers. As part of an VEMS Server installation, you can configure a VOD server to run in the "zones" (LAN or Internet) specified in Table 2. Before server configuration, you assign a range of IP addresses that define the LAN domain, or vice versa, that define the Internet domain. Any IP address outside that range will assumed to be from an Internet source, or vice versa, from a LAN source. (See "Assign LAN/Internet Address Range" in <u>Global Assignments</u> topic on page 23.)

You can purchase an Internet-based VOD-W or VOD-WM server from VBrick (in which case they are configured by VBrick) or you can purchase and configure a VOD-WM yourself using the Microsoft documentation (not recommended). You can also install a Darwin Open Source server which is fully-compatible with VEMS Portal Server but is not sold or supported by VBrick. (For more about downloading, installing, and configuring a Darwin server, go to: <u>http://developer.apple.com/opensource/server/streaming/index.html</u>) As noted, VEMS users can be on the Internet or on a LAN; Internet users can only access MPEG-4, Windows Media. and H.264 content stored on Internet-based servers. LAN users

can access all content on all servers both inside and outside the firewall. To summarize, *Internet-based* servers and users are subject to the following limitations:

- Internet servers support MPEG-4 and Windows Media content only.
- Internet servers support unicast only (they do not support multicast).
- Internet VEMS users can add video only to VOD servers in the Internet zone.
- Internet users can only see MPEG-4, Windows Media, and H.264 content stored on Internet-based servers.
- Internet servers do not support VEMS scheduling features.

VEMS IP Receiver

VEMS-IPRs access the VEMS Portal Server through a web browser within the IP Receiver. Using the IP Receiver remote control, users can navigate and search for specific on-demand content or live video streams, select a stream, and begin viewing television-quality video. IP Receiver users can also record video directly on the VEMS Portal Server using the remote control or the wireless keyboard. See the IP Receiver documentation for more about how to configure and use an VEMS IP Receiver.

VEMS Network Video Recorder

The VEMS Network Video Recorder and the VEMS Live Portal Server are optional components that are purchased and installed separately. They have different license files that must be installed separately. See Install/Replace License Files topic on page 17. The VEMS Network Video Recorder lets you off-load all recording tasks from the VEMS Portal Server machine to one or more separate "recorder server" machines. This optimizes recording performance and improves VEMS Portal Server performance as well. The Network Video Recorder uses VEMS

Portal Server components and typically requires two machines: the VEMS Portal Server is installed on one machine; the Network Video Recorder software is installed on a different machine. Once installed, the NVR machine is used for all VEMS Portal Server recording tasks. See Network Video Recording topic on page 171 for more information.

Note A standard VEMS Portal Server permits two concurrent recording operations. If you purchase a Network Video Recorder, the number of concurrent recording operations (10 or 40) is fixed by the terms of your licensing agreement with VBrick.
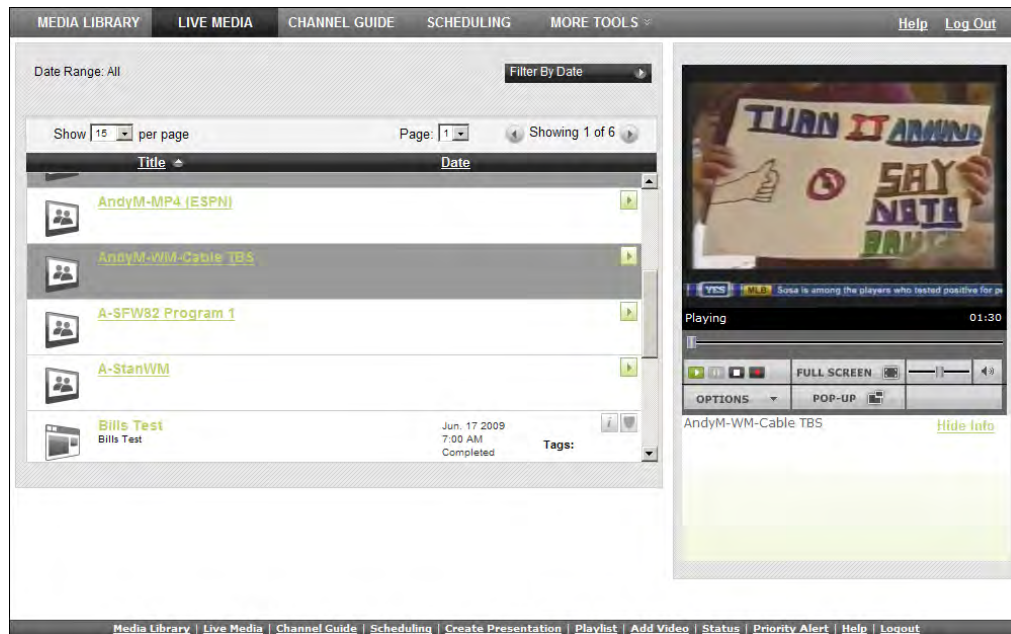
Figure 3. Live Portal Server User Interface

Distribution Servers

Distribution servers are used to load-balance the distribution of .jpg images and HTML pages when delivering large-scale presentations. After installing the Portal Server you will need to run DistributionServer.exe on each VEMS server present in your configuration. Distribution servers are used for "presentations" (live webinars) only and require a separate license. Auto-generated e-mail invitations from VEMS presentations will point to the load-balanced distribution servers if present.

Distribution servers can each handle approx. 5000 users. (For highest scalability, configure the webinar **Permission Mode** (on the Create Presentation > Permissions page) for "Everyone" and set a webinar password. See the *Portal Server User Guide* for more about presentations.) Distribution Servers serve Presentation/webinar HTML pages, PowerPoint Slides (converted and displayed as .jpg images), and reference material (Word documents, PDFs, etc. that been uploaded by a presentation creator). Distribution Servers also provide the following functionality.

Note The *Portal Server Release Notes* explain how to install and configure Distribution Servers and how to configure your system for presentations. The <u>Zones</u> topic in this document explains how to configure and use "zones" that point to specific servers.

- Zones (separately addressable internal and external "zones" for load-balancing and viewing video).
- Viewer questions (realtime questions from presentation viewers).
- Polling (view/respond to multiple-choice polls created by a presentation creator). Polling, viewer questions, and access log data are queued up and batched to the main Portal Server once every minute.
- Access logging (captures the IP address of each presentation viewer).

Amino Set Top Box

The AmiNet110 is a compact set top box for the Portal Server manufactured by Amino. It connects to a standard TV and only plays MPEG-2 streams; no other streams are selectable for viewing on the Portal Server interface. There is no software installation required. Simply connect and configure the device as explained in AmiNET110 MPEG-2 STB topic on page 201. The *Portal Server User Guide* explains how to use the Amino infrared remote control unit that comes with the device.

The AmiNet130 is a compact set top box that connects to a standard TV and plays H.264 Transport Streams only. There is no software installation required. Simply connect and configure the device as explained in H.264/MPEG-2 STB Quick Start Guide.

WM IP Receiver

VBrick's WM IP Receiver is similar to a conventional set top box but is significantly more stable, rugged, and reliable. It is designed for 24x7 operation, and built for enterprise networks that require a high degree of stability, security, and scalability. The WM IP Receiver is a robust, state-of-the-art device that meets the demanding requirements of VBrick's Enterprise Media System. The WM IPR plays Windows Media streams from VBrick WM appliances and Windows Media servers. The WM IPR is also a fully-featured VBrick VEMS client. This means that in addition to the ability to deliver video, subsequent WM IPR releases will provide scheduling, access logging, and device control from the Portal Server. For more information about the WM IPR, see the *IPR Admin Guide* in the Portal Server online help.

Portal Server Installation

Complete installation instructions for the Portal Server are provided in the *VEMS Portal Server Release Notes*. Once the Portal Server is installed, end users on Windows or Macintosh machines may be prompted for additional download components as explained below. This only happens the first time they access the Portal Server. The Portal Server supports a wide variety of clients and video formats. See Supported VBrick Clients and Video Formats for a complete list.

Download Components

Windows PCs

If configured with the appropriate components, Windows PCs (with Internet Explorer or Firefox) can play all stream types including MPEG, Windows Media, and H.264. For Windows-based PC users, the Portal Server uses VBrick StreamPlayer software-based components to decode video streams on user desktops. The Portal Server downloads these components to each client machine the first time you access the Portal Server (depending on the **Specify Components to Download to Clients** setting in Global Assignments). No download is necessary for subsequent access. If this is a new installation, end users must answer Yes to security requests to download these components. After a download, you don't have to restart your computer but must you must close the browser. These components are downloaded using .cab files.

In certain circumstances however, the use of .cabs is either not allowed or not feasible. In these cases, VBrick provides an `.msi` installer called `VBrickComponents.msi`. This installer installs the same components and allows end-users who cannot download .cabs to have full

Portal Server functionality. This installer is located in the `Program Files\VBrick\MCS\utils` folder.

Note The component download setting will not affect previously-installed components. For example if you have StreamPlayer installed, you will be able to play MPEG-2 streams regardless of what components you specify for download.

Firefox

With Firefox, users will also be prompted to install additional components the first time they launch a stream—if they are configured to receive these download components. Links for the appropriate stream types (MPEG, WM, or H.264) will be displayed in the area where the embedded player is normally displayed. These additional plugins *must* be installed. Firefox users will also be required to install an additional plugin when they use **Add Video** for the first time (again, if they are configured with this privilege). Also be aware that there is no automatic downloading of Firefox components during a VEMS upgrade. To be sure you have the latest VBrick components for Firefox, you will need to manually uninstall `VBPlayerMoz`, `VBWMPlayerMoz`, and `VBFTPMoz` using **Add or Remove Programs** in Windows—*on each client desktop.* The latest VEMS components for Firefox will be installed the next time the Firefox client launches a stream.

Table 3. Supported Windows Operating Systems and Browsers

Operating System	Browser †
Windows XP	Internet Explorer 7.0, Firefox 3.5
Windows Vista	Internet Explorer 7.0, Firefox 3.5
Windows 7	Internet Explorer 8.0, Firefox 3.5

† Use version shown or higher.

Locked-Down Windows PCs

As described above, the Portal Server automatically downloads components to client PCs depending on the Global Assignment setting. This download can be an issue in environments that have restrictions on client software installation. For playback of WM files, Portal Server uses the existing Windows Media Player components on the client PC and there is no need for the extra components to be downloaded. This means that Portal Server and WM can be used in some but not all restrictive or "locked-down" environments.

Even if downloads are configured, a client PC will still refuse to accept the component download if the Internet Explorer security feature **Download signed ActiveX controls** is disabled. When using Portal Server exclusively with WM streams and a WM VOD, the client PC can refuse to accept the downloaded components and all Portal Server features except **Add Video** will work. In this case you should uncheck the **Add Video Utility** in Global Assignments.

Some sites also require that their PCs be configured with certain Internet Explorer security settings. The Portal Server will not work on clients with Internet Explorer security set to **High**. The Portal Server *will* work at any level at or below **Medium**. If you start at **High**, the client will still work with Portal Server if you enable **Run ActiveX controls and plug-ins**, **Script ActiveX controls marked safe for scripting**, and **Active scripting**.

Since firewalls on LAN client PCs can also cause problems with Portal Server, it is recommended that firewalls be disabled on LAN clients. (In Windows XP with Service Pack

2, the firewall is enabled by default.) Portal Server's support for Internet clients is designed to work through firewalls. If you have Internet clients with firewalls see the description of LAN/Internet address ranges in <u>Global Assignments</u> topic on page 23.

Macintosh PCs

If configured with the appropriate components, Macintosh PCs (with Safari or Firefox) can play all stream types including MPEG, Windows Media, and H.264. In a Macintosh environment, if downloads are configured in Global Assignments, when you launch the VEMS Portal Server for the first time, the Home page (see Figure 2) displays a link prompting you to download components that are appropriate for your computer. If you agree, these components are automatically installed and no additional download is necessary for subsequent access. On Macintosh PCs, Portal Server functionality is the same as in Windows except that the **Add Video** feature is not available. Table 4 shows the stream types supported for each environment; Table 5 shows the operating systems that are tested and supported. Note that there are certain performance limitations in Macintosh environments; see the *VEMS Portal Server Release Notes* for information and recommendations.

Configuring a Macintosh for Tunneled Streams

You may need to perform certain configuration steps on a Macintosh before you can use QuickTime to view streams tunneled over HTTP from a VOD-W server.

▼   To configure QuickTime for tunneled streams:

1. Launch QuickTime on a Macintosh and click on the **Apple QuickTime** player to set focus on the task bar at the top of the screen.
2. Click **QuickTime Player** in the task bar and go to **QuickTime Preferences**.
3. On the **Advanced** tab, click on **Transport Setup** and then **Custom**.
4. Check the **Port ID** used for the HTTP **Transport Protocol**. The **Port ID** must match the **HTTP Tunneling Port** set on the Portal Server for the VOD-W server (default = 8000). If necessary, get this port number from your system administrator. See the *VOD-W Admin Guide* for more information.

Table 4. Supported Macintosh Stream Types

Environment	Supported Streams	Closed Captions †
Macintosh	Safari – MPEG-1, MPEG-2, MPEG-4, WM, H.264.	Supported for MPEG-1/MPEG-2 streams, and for MPEG-4 and WM with VBrick plugin.
	Firefox – MPEG-1, MPEG-2, MPEG-4, WM, H.264.	Supported for MPEG-1/MPEG-2 streams, and for MPEG-4 and WM with VBrick plugin.

† Closed captions are not currently supported on H.264 streams.

Table 5. Supported Macintosh Operating Systems and Browsers

Operating System	Browser †
Mac OS X 10.6 (Snow Leopard)	Safari 4.0.x, Firefox 3.5
Mac OS X 10.5 (Leopard)	Safari 3.1.1, Firefox 3.5

† Use version shown or higher.

Player Licenses

Most video compression technologies are protected by patents and their use requires obtaining a license from the technology owner. These licenses are granted after royalties have been paid to the owner. VBrick typically obtains licenses for specific video formats in advance from the technology owners and makes them freely available to Portal Server users. For viewing purposes, each license is equivalent to one "seat." This means if you have 100 MPEG-2 seats, for example, the number of concurrent users viewing an MPEG-2 stream (with any type of player) cannot exceed 100. The number of licenses initially available to Portal Server users is shown in Table 6. If you need additional licenses to comply with patent restrictions please contact the VBrick Sales team.

Table 6. Video Format Licenses

Video Format	Licenses Provided
MPEG-2	100
MPEG-4 Part 2	1000
Windows Media on a Macintosh	100
Windows Media on a PC	License not required
H.264 RTP	1000
H264 TS	100
MPEG-1	License not required
AAC (Advanced Audio Coding)	1000

Decoder Closed Captioning Support

The Portal Server supports live streams with closed captioning. It also supports closed captioning for MPEG-4 stored content as long as the content is recorded with closed captioning and stored on a VOD-W server. Closed captioning is not supported for NXG MPEG-4 stored content. The following table shows closed captioning support for VBrick decoders/IPRs, cross-referenced by live and stored content.

Table 7. Set Top Box/Decoder Closed Captioning Support

	Live Content	Stored Content		
Set Top Box/Decoder		VOD-W	VOD-WM	VOD-D
MPEG-2 Decoder	Yes	Yes	N/A	N/A
MPEG-4 Decoder	Yes	Yes	N/A	MPEG-4 only
MPEG Set Top Box	Yes	Yes	N/A	MPEG-4 only
WM-IP Receiver	No	N/A	No	N/A
AmiNET110 MPEG-2 Set Top Box	Yes	Yes	N/A	N/A
AmiNET130 H.264/MPEG-2 STB	Yes	Yes	N/A	N/A

Port Requirements

The drawing below, and the table that follows, show the required port configuration for various Portal Server devices. *All ports in the drawing are TCP except as noted.*
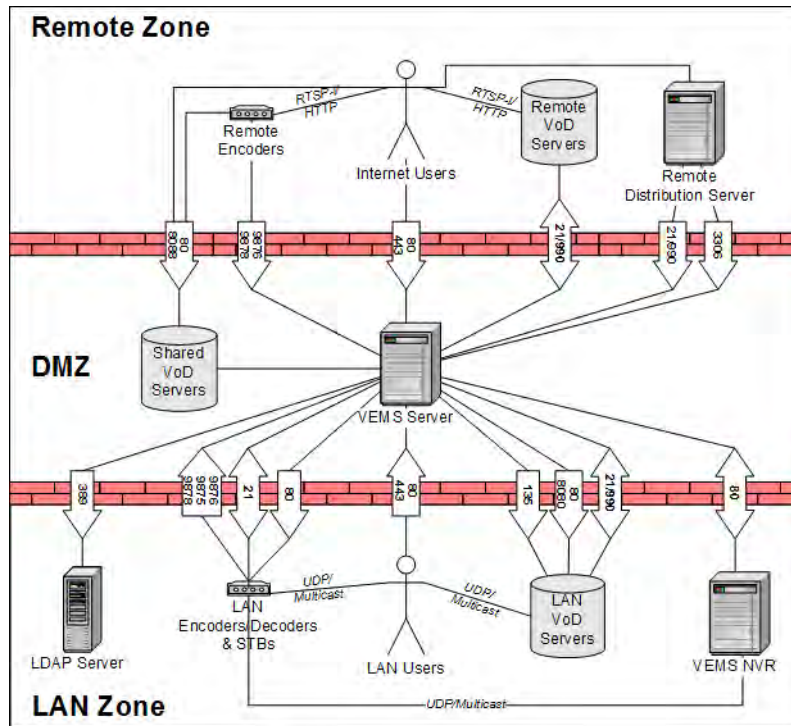
Table 8. Port Requirements

Zones	Port(s)	Description
Internet > DMZ	80/443 (TCP)	Web request from client to VEMS (http = 80, https = 443).
Internet > DMZ	80 (TCP)	RTSP-I/HTTP Tunneling from client to shared VOD server.
Internet > DMZ	80 (TCP)	HTTP Push from presentation VBStar to shared VOD Server.
Internet > DMZ	9876/9878 (UDP)	Management/RTSP SAP announce from VBrick to VEMS.
Internet > DMZ	21/990 (TCP)	FTP/FTPS from client to VEMS (to AutoIngest folder) (990 for ftps).
Internet > DMZ	3306 (TCP)	MySQL database request from remote distribution server to VEMS.
Internet > DMZ	21/990 (TCP)	FTP/FTPS from remote distribution server to VEMS (using FTP sync).
Internet > DMZ	139/445 (TCP), 137/138 (UDP)	File copy from remote distribution server to VEMS (using DFS sync).

Zones	Port(s)	Description
DMZ > Internet	21/990 (TCP)	FTP/FTPS from VEMS to VoD Server (Darwin/Windows Media/FTP).
LAN > DMZ	80/443 (TCP)	Web request from client to VEMS (http = 80, https = 443).
LAN > DMZ	9875/9876/9878 (UDP)	Multicast/Management/RTSP SAP announce from VBrick to VEMS.
LAN > DMZ	21 (TCP)	FTP from VBStar to VEMS (auto-FTP to VEMS Auto-Ingest directory).
DMZ > LAN	21 (TCP)	FTP from VEMS to VBStar (content discovery).
DMZ > LAN	80 (TCP)	Management command from VEMS to VBrick/STB. Used by the VEMS "Create Presentation" tool and to schedule some STBs for content playback.
DMZ > LAN	80/8080 (TCP)	Web service request from VEMS to VoD Server (Infovalue/NXG).
DMZ > LAN	54321 (TCP)	Used to control various Amino STBs.
DMZ > LAN	21/990 (TCP)	FTP/FTPS from VEMS to VoD Server (Darwin/Windows Media/FTP).
LAN > DMZ	21 (TCP)	FTP from VoD Server (NXG/Infovalue) to VEMS.
DMZ >LAN	135 (TCP)	Management command from VEMS to Windows Media (DCOM).
DMZ > LAN	80 (TCP)	Web service request from VEMS to Network Video Recorder (NVR).
LAN > DMZ	80 (TCP)	Web service request from Network Video Recorder (NVR) to VEMS.
DMZ > LAN	389 (TCP)	LDAP lookup from VEMS to LDAP Server (e.g., Active Directory).

Uninstall/Change Configuration
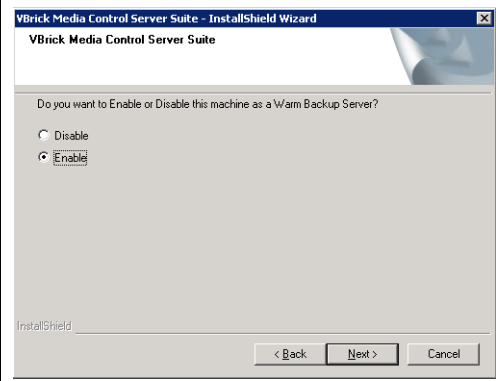
Use the following steps when you want to uninstall VEMS or change VEMS configuration options. For example you may need to enable/disable a warm backup server or modify the host name of the VEMS server.

▼   To uninstall or change the configuration:

1.   Go to **Start > Control Panel > Programs and Features > VBrick Enterprise Media System**.

2.   Click the **Uninstall/Change** button.
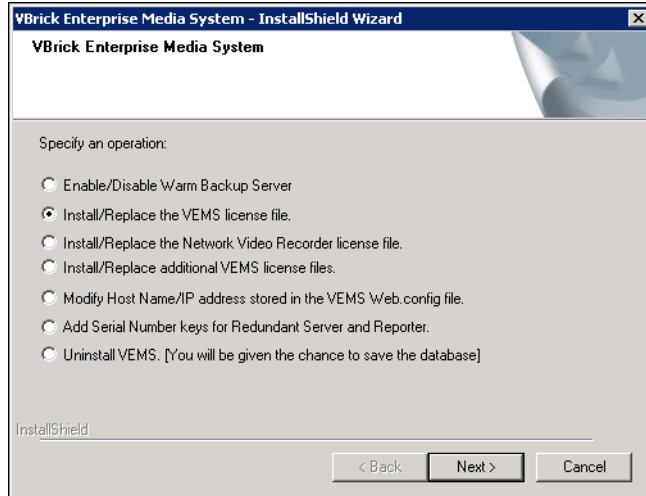
3. Select the operation you wish to perform and click **Next**. A description of each of the options is listed below.

Enable/Disable Warm Backup Server	If you purchased Enterprise Media System Backup, two Portal Servers will be present—one of which must be configured as a warm backup. Use this option (and the popup shown below) to enable or disable the backup server. If you enable one server, you must disable the other. Default = Disable. See <u>Automatic System Backup</u> topic on page 185 for more information.
Install/Replace the VEMS license file	Use this option, as directed, to install a Portal Server license file. If not installed you will not be able to run the Portal Server.
Install/Replace the Network Video Recorder license file	A Network Video Recorder is a standalone recorder option that can speed up recording operations and/or enhance Portal Server performance (see <u>VEMS Network Video Recorder</u> on page 8). If not installed there will be a "record" failure for more than two concurrent record requests.
Install/Replace Additional VEMS licenses	Use this option to install or replace any of the Portal Server licenses shown in Table 9 on page 19.

Modify Host Name/ IP address stored in VEMS Web.config file	Use this option to modify certain values in web.config.

• Auto-detect server Host Name – If you change the host machine name, use this option to auto-detect the Portal Server Host Name.

• Manually enter server Host Name or IP – If you change the host machine name, use this option to manually enter the Portal Server Host Name. This name must match the machine name on which Portal Server is installed.

• Enter external IP/Host Name – Used to configure an **Internet Link** for the "Share Media" feature in the client application (a **LAN Link** is configured by default and always present). Enter a valid external IP address for your VEMS server to display an "Internet" link on the client page; blank out the field to remove the link. When content sharing is enabled, Portal Server users can share any stored content or live streams by clicking the envelope icon to the right of the stream title.

The Share Media external **Internet Link** will only be displayed for content accessible to Internet users. Content not accessible by Internet users will only have the internal **LAN Link**. Internet users are defined in "Assign LAN/Internet Address Range(s)" on the Global Assignments page. If no Internet users are defined, the external IP link will not shown for any content.

Add Serial Number keys for Redundant Server and Reporter.	Required for optional VEMS Backup and VEMS Reporter components. If not installed, these applications will not run.
Uninstall VEMS	Remove all VEMS Portal Server components. You are prompted to save the database as desired.

Install/Replace License Files

You are prompted to install serial numbers and license files(`.lic`) as part of the Portal Server installation process. Different Portal Server functionality is available depending on the type of license you purchase and install. (For example if you do not install a Scheduler license, you will not see a **Scheduler** option in the Portal Server client application.) After initial

installation you can install a different license as necessary using **Programs and Features** functionality in Windows Web Server 2008. All of the different license files are explained in Table 9.
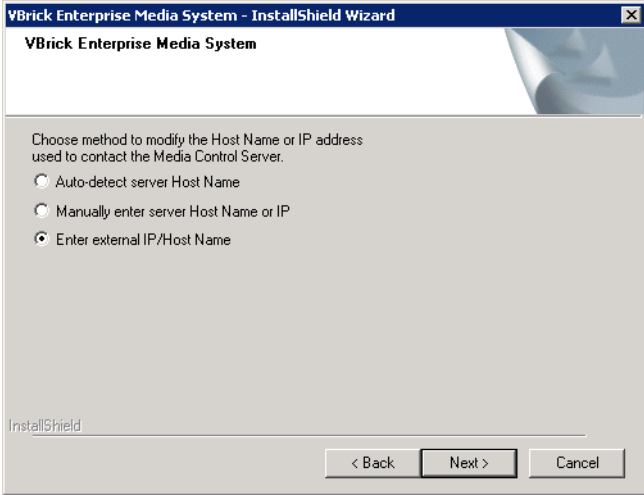
▼ To install or replace VEMS license files:

1. Go to **Start > Control Panel > Programs and Features > VBrick Enterprise Media System**.

2. Click the **Uninstall/Change** button.
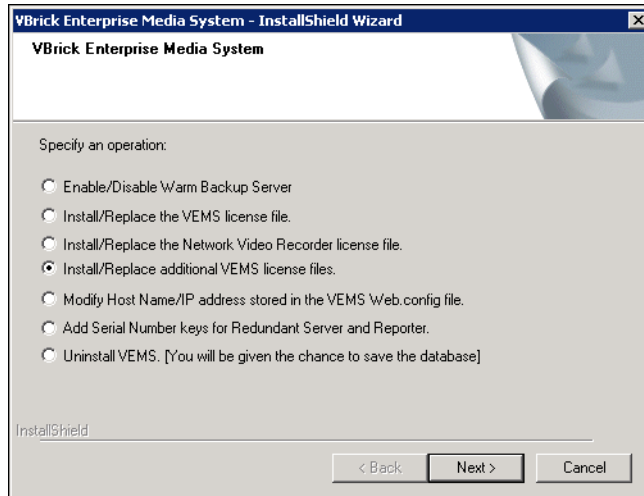
3. Select an option or click **Install/Replace additional VEMS license files** and click **Next** to see more license options. See Table 9 <u>Portal Server License Files</u> for a description of each license file.
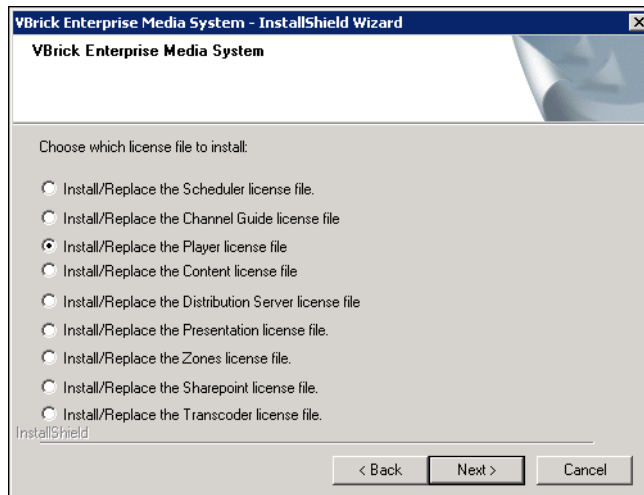
4. A serial number is required for some components (for example Redundant Server and Reporter). Enter a serial number and confirm if necessary. If the serial number window pops up and is already filled in, click **Next** to continue. If the serial number field is empty, enter the serial number you received from VBrick Support Services (or from the "License Activation Keys & Serial Numbers" card that was included with the VEMS Product CD), and click **Next**.
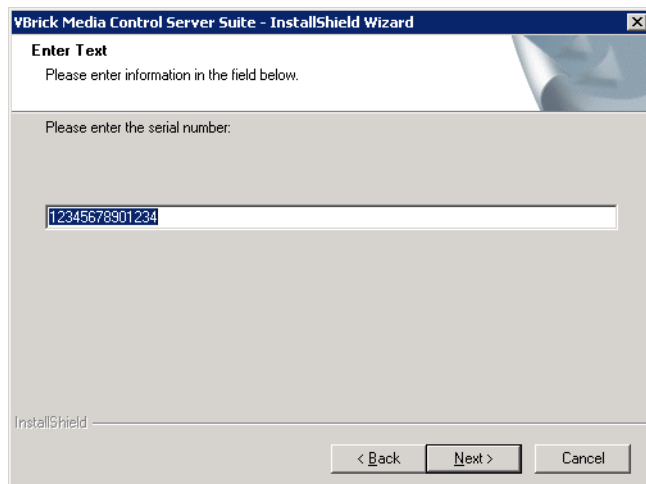
5. When prompted, navigate to the folder with your license (.lic) file. License files are obtained by using the "License Activation Keys & Serial Numbers" card included with the Product CD. The "Software License Activation" document, also included, explains how to activate your licenses using these keys. Note that multiple license files may be shown if you purchased optional VEMS components. *Select the appropriate license file.* (For more about license files, see "Installing Serial Numbers and License Files" in the *Portal Server Admin Guide.*)

6. **Repeat these steps for each VEMS component.** When done, manually close the window and launch the application. There is no need to restart the host machine.

Table 9. Portal Server License Files
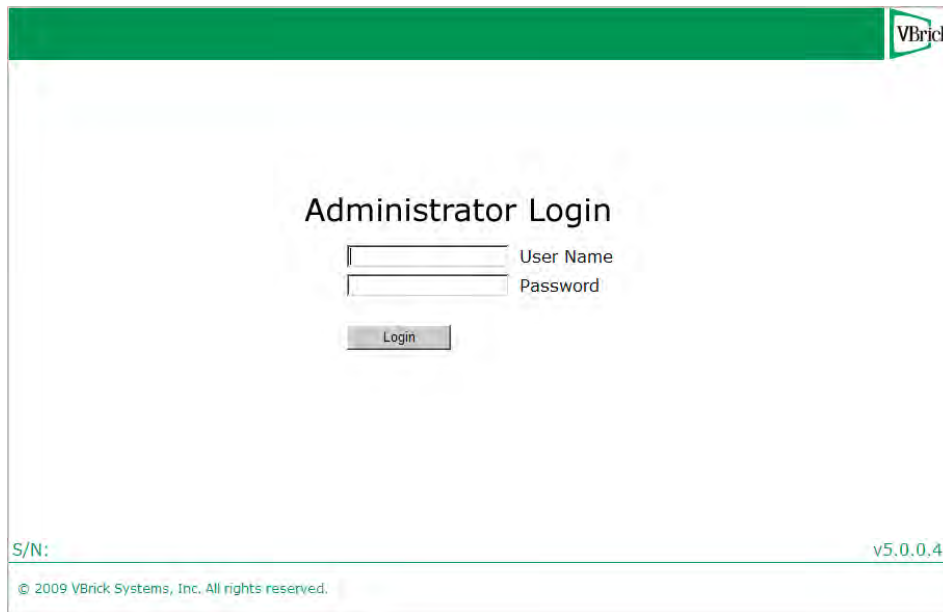
License File	Description	If not installed ...
Scheduler	Enables the broadcast or recording of future events. See the *VEMS Portal Server User Guide* for more information.	the **Add** option will not be shown Scheduler page in client application.
Channel Guide	Enables access to the Channel Guide Server for TV Stations that are typically provided by a third-part content provider.	there will be no TV Stations or access to the Channel Guide server.
Player	The embedded Windows Media Player has restrictions on the number of licensed users. Use this option to select a license file that modifies the number of allowed users for various MPEG-1/2/4 streams.	a popup message will be displayed when you try to launch a stream.
Content	Used to install third-party content purchased from VBrick.	the purchased content ingestion will fail.
Distribution Server	Use to install one or more Distribution Server license files. See Distribution Servers topic on page 9.	you will be unable to communicate with the distribution servers.
Presentation	Used to create rich media presentations with PowerPoint slides and a video stream.	the **Create Presentation** feature will not be available in client application.

License File	Description	If not installed ...
Zones	Determines how many <u>Zones</u> you can configure.	the **Add Zone** button will be greyed out once you configure the number of licensed zones.
SharePoint	Lets you display a list of a list of streams from a VEMS VOD server on a SharePoint page.	the configured SharePoint page will display an error message rather than a list of streams.
Transcoder	Used to transcode various file types to Windows Media or H.264.	the **Transcoding** feature will not be available on the **Add Video** page.

Admin Console Login

The VEMS Portal Server can be administered from Windows-based PCs using Internet Explorer 7.0 or higher only. The Admin Console pages are best viewed at 1024x768 resolution. The Admin Console is not supported on Macintoshes or IP Receiver, or with Firefox or other browsers. In order to access the administrative functions enter the following address in the Internet Explorer browser of the PC where `myserveraddress` is the host name or IP address of the VEMS Portal Server. The session will timeout after 20 minutes of inactivity. `admin` is both the default user name and password.

http://myserveraddress/admin/

Note As a standard best practice, VBrick recommends changing the default administrator User Name and Password. Go to **Global Settings > Global Assignments** on the Admin Console.

Admin Console Options

Login to the VEMS Portal Server Admin pages with a valid user name and password to display the following window. This window provides access to all admin configuration options.

Table 10. Admin Options

Option	Description
Getting Started	The VEMS Portal Server splash page shown above.
Global Settings	Provides system-wide configuration parameters to connect to VBrick encoders and VOD servers as well as to customize the look of the VEMS Portal Server pages.
Channels	Lets you define TV stations and custom stations that obtain programming data from a third-party provider.
Modify VOD Content	Provides the ability to Move, Rename, or Delete assets on the VEMS-VOD Video-on-Demand server. (Not supported on some legacy NXG servers.)
Diagnostics	Displays system log messages by source, time, and (generally) IP address.

Option	Description
Status	Shows the status of events in progress including recordings, Add Video commands, ingestion to the VOD server, and FTP downloads.
Expired Content Log	Shows all expired content still present on the Portal Server. Use Purge All to delete unwanted content.
Access Control	Provides the ability to limit access to the VEMS Portal Server system to different users or groups of users.
Users †	Used in conjunction with Access Control to limit access to the VEMS Portal Server system to different users.
User Groups †	Used in conjunction with Access Control to limit access to the VEMS Portal Server system to different groups of users.
Resource Groups †	Used in conjunction with Access Control to group resources which can then be provided to users or user groups.
Digital Signage ††	Used to combine video streaming and digital signage content into one delivery system.
Help	Displays the VEMS Portal Server online help system in a new window.
About	Displays the VEMS version number as well as the license and serial number status for each installed module.
Logout	Logs out the user who is currently logged in.

† Users, User Groups, and Resource Groups are only displayed if Access Control is enabled. See Users and User Groups topic on page 131 for a description of these functions.

†† VBrick Digital Signage is a standalone, web-based application. See Digital Signage on page 129 for more information.

Internet Explorer 7.0 Configuration

The Admin Console and the Portal Server user interface support the browsers shown in Table 3 and in Table 5. When using Internet Explorer 7.0, there are additional security settings required for compatibility with the Portal Server.

▼ To configure the Portal Server for Internet Explorer 7.0:

1. Go to **Tools > Internet Options > Security** and select **Custom level**.
2. Under **Active X controls and plugins** set the following parameters:

- **Allow previously unused ActiveX controls to run without prompt** – Enable
- **Automatic prompting for ActiveX controls** – Disable
- **Display video and animation on a webpage that does not use external media player** – Enable
- **Download signed ActiveX controls** – Prompt
- **Run ActiveX controls and plug-ins** – Enable
- **Script ActiveX controls marked as safe for scripting** – Enable

Global Settings

Global Settings include configuration settings and parameters that apply to the entire system. Global Settings include all of the following.

Topics in this section

Global Assignments

Global Assignment are listed below. Most are self-explanatory and consist of text boxes where you enter appropriate values.
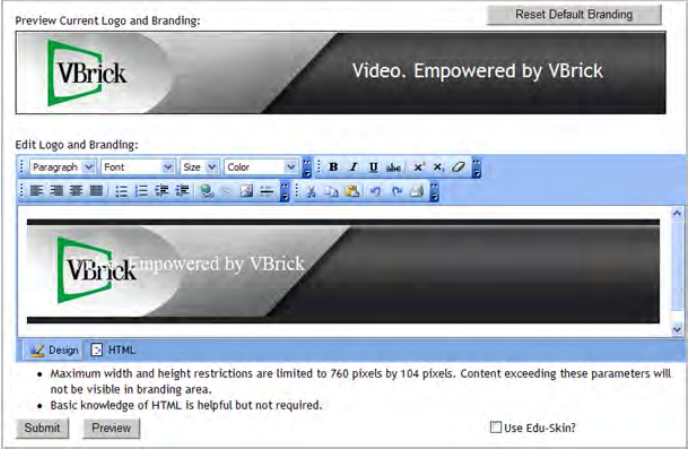
Figure 4. Global Assignments

Item	Description
Define IP Receiver Startup Channel	When an IP Receiver (in VEMS Portal Server Start mode) accesses the **Watch Live Media** page, it can be set to automatically play a defined channel in the Preview Window. Highlight that channel from the list and click Submit. If there are no channels listed, channels must first be defined as Customized Live Streams.
Change Admin User Name	Change the default admin user name of `admin`. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.
Change Admin Password	Change the default admin password of `admin`. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.

Item	Description
Define FTP User Name	VEMS Portal Server is defaulted for "anonymous" FTP access which is configured in Windows IIS Default FTP Site. If a more secure FTP access is desired, the User Name can be changed in IIS (see the Windows Server documentation for details). The same User Name should be entered here. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.
Define FTP User Password	VEMS Portal Server is defaulted to "vbrickuser" FTP access which is configured in Windows IIS Default FTP Site. If a more secure FTP access is desired, the Password can be changed in IIS (see the Windows Server documentation for details). The same Password should be entered here. Use any combination of alphanumeric and special characters *except* slashes, quotes, or commas.
Define a Record Duration	Applies to the on-demand **Record** pushbutton only (not to scheduled recording). Defines the maximum duration (default 120 minutes) allowed for a continuous recording. Maximum record duration limited only by size of hard drive.

Item	Description
Customize Logo and Branding	This feature let's you brand the Portal Server with a custom image and text of your choice. Use this built-in design editor to replace the default banner image (`vemsbranding.jpg`) and the customizable text that is superimposed on the banner. You can also check **Use Edu-Skin** to use a banner (`vemsbrandingEduSkin.jpg`) custom-designed for education environments. This image is in `C:\Program Files\VBrick\MCS\VemsImages`. Uncheck to use default VBrick image.

The editor has Submit, Preview, and Reset buttons. Use **Preview** to see how your changes will look; use **Reset Default Branding** to discard your changes and revert to the initial VEMS branding; use **Submit** to actually publish your changes to the Portal Server. The **Submit** button will save your changes to the database and update the live Portal Server page. *Always be sure to preview your changes in the Portal Server before and after a "submit."*

The editor has a **Design** view with extensive formatting controls like Microsoft Word and an **HTML** view for experienced HTML users. Use one or both editors to customize the Portal Server page that your end users will actually see. Experiment with the controls: you can add images, insert hyperlinks, and customize the style, color, and font of the text as necessary. You can also use an outside editor like Front Page and then paste and test the generated HTML code in the Portal Server editor. Experienced web developers are also free to add custom CSS and Javascript. See the *Portal Server Customization Guide* on the VBrick <u>Product Documentation</u> web page for more information. This document explains in detail how to add custom CSS and Javascript files to VEMS.

Item	Description
Change Announcement Addresses	*Changing these from the defaults is highly discouraged and should only be done if advised by a VBrick technician or Network Administrator.* Changes the Management, Multicast, and RTSP addresses on which Announcements (SAPs) are received. By default all VBrick devices are set to the same addresses and ports as the defaults in VEMS Portal Server. These have to match on all devices for proper functionality.
Change Announcement Filter	Filters SAP announcements so that only the specified IP addresses are shown on the Live Media page in VEMS Portal Server. Wildcards are allowed. For example 255.*.*.* displays only those addresses in the range 255.0.0.0 – 255.255.255.255.
Assign LAN/Internet Address Range(s)	Define the range(s) of IP addresses that define the LAN or the Internet domain for the first two zones available at your site. (See <u>Zones</u> on page 93 to configure any additional zones.) *Mixed or duplicate IPv4 and IPv6 addresses are supported.* Any IP addresses outside the range are assumed to be from the domain you did *not* select. Check one option and, if necessary, use the text box to enter the range(s) separated by a comma, a semicolon, or a new line. For more information, see <u>VEMS Internet-Based Servers</u> on page 7. Note: If your network has IPv6-enabled VEMS clients or VEMS servers, you must define IPv6-style ranges, and IPv4-style ranges, for all clients defined in the LAN/Internet zone. • All Users, Servers, and VBricks are in the LAN Domain (default). • All Users, Servers, and VBricks are in the Internet Domain. • Specify LAN Address Range(s); assume users/servers/VBricks outside this range(s) are in the Internet domain. • Specify Internet Address Range(s); assume users/servers/VBricks outside this range(s) are in the LAN domain. • Always use TCP protocol (HTTP Tunneling/RTMPT/RTSP Interleaving) for MPEG-4, H.264, Flash and Windows Media content – Use only with Internet-compatible (VOD-D, VOD-W, VOD-WM, Flash, and Wowza) servers. If checked, the Portal Server will always use HTTP tunneling or RTSP interleaving using the **HTTP Tunneling Port** defined for the server (see <u>Servers</u> on page 33 for more information). If checked, Flash media will always be played back using RTMPT. Note: Standard VBrick IP Receivers do not support HTTP tunneling and will not play MPEG-4 content if this option is selected.

Item	Description
Assign Multicast Address Range	Defines the current multicast IP address range and port range. The default multicast IP range is 225.1.1.0–239.128.255.255. The default port range is 1040–65534.
Assign VOD Polling Interval	Not generally changed. Defines the interval at which the Portal Server polls the VOD server(s) for new content (default 120 minutes). This is only used to poll for content added to the VOD from an interface *other than VEMS Portal Server*. When adding a server, use **Sync Now** to sync the program listings on the client Browse Video Library page with the content on the new server. Use **Hide content for VOD Servers experiencing connection problems** to prevent end users from seeing unavailable content and to enable rollover to the **Default Server Address(es)** specified on the **Zones** page (see <u>Zones</u> on page 93 for more information). Default = checked. If this option is unchecked, there will be no rollover to default servers in the event of a server failure.
Assign VoD Content Ingestion Maximum	Defines the maximum number of simultaneous video files that can be ingested to the VOD Video-on-Demand server. The default is set to 2. Increasing the default may increase the speed at which files will be transferred to the VOD server, but may result in playback issues from the Video-on-Demand server. VBrick recommends keeping the default of 2 for all supported VOD servers.
Assign Default Max. Concurrent Viewers	Defines the *default* maximum concurrent viewers allowed for new live or stored (VOD) content. An entry on the **Stream Restrictions** page or the **Modify VOD Content** page will override these value for live and stored streams respectively.
Set Expired VOD Content Treatment	Specifies whether expired content will be kept or automatically deleted at the expiration date.
Assign Content Expiration Warning Recipients	Enter one or more semicolon separated e-mail address for the person(s) responsible for renewing copyrighted or otherwise protected content. When you configure or change either the recipient or the mail server, the Portal Server will attempt to send a test message. Check that this message is successfully delivered. The Portal Server validates the e-mail address but cannot detect other mail delivery failures. If the user's mail box is full, for example, the message will not reach its intended recipient to warn of impending content expiration. For more about content expiration, see <u>Copyright Protection</u> on page 2.

Item	Description
Assign Mail Server	Required field. SMTP mail server name used for Content Expiration messages and Presentation invitations. (For an example go to Microsoft Exchange > Tools > E-mail Accounts > E-mail > Microsoft Exchange Server > servername.) An e-mail to the assigned Content Expiration Warning Recipient(s) is generated when you configure or change this field. If you enter a user name and password, these credentials will be used to send e-mail to external domains that require user authentication. If user name and password are blank, the default network credentials are used. Note that in some environments, the default credentials will not allow e-mail delivery to domains outside the specified mail server host.
Assign Time Zone of Admin Console	Most times shown in the client interface are converted to the user's local time zone. The times displayed for <u>Custom Programs</u> in the Channel Guide and <u>Diagnostics</u> on the Admin console however are displayed in the currently selected time zone for the Admin Console. Use the dropdown list box to select a time zone for the admin console.
Assign Presentations	The Presentations User is a user who will be given permission to publish presentations to specified folders and VOD servers. The Presentation User must have access to all VOD servers you will be publishing to and all Content Publishing folders. See the "Configuring for Presentations" topic in the *Portal Server Admin Guide* for more about presentations.
Select Player for H.264/ MPEG-4 Content	Select the player to use for H.264/MPEG-4 content on Windows/Macintosh clients: • VBrick Player – users will be prompted to install a VBrick plugin the first time they launch H.264/MPEG-4 content. • Apple QuickTime Player – VBrick plugin not required. Does not support access logging.
Assign AutoIngest	The current autoingest via XML user name that has access and publishing rights to a VOD server. See <u>AutoIngest Content via XML</u> on page 179 for more information.
Delete Recorded Files After Ingestion	Used with scheduled recording and push button recording. Specifies whether or not to delete the recorded file from the NVR after ingestion. Enabled by default.

Item	Description
Specify Components to Download to Clients	This setting defines whether the Portal Server will download additional components to client machines when the client first makes contact with the Portal Server—before any streams or assets are selected for playback (see Download Components on page 10 for more information.) *Any changes to these settings apply to new client machines only and will not affect previously configured machines.* The settings here apply to Internet and/or LAN users as defined in the **Assign LAN/ Internet Address Range(s)** in Global Assignments (see above). The default is to download all components to all clients. For Windows clients you can selectively choose any combination of settings; for Macintosh clients, any one selection will download all components for all clients. • MPEG-2 Video Support – makes both MPEG-2 files playable. • MPEG-4/H.264 – makes MPEG-4/H.264 files playable. • WM Video Support for Firefox on Windows PC – makes Windows Media files playable on Firefox. • 'Add Video' Utility – enables or disables the "add video" functionality on client machines.
MPEG-2 Packet Ordering at Schedule End	Network hardware infrastructure determines the order in which packets arrive at a destination. To improve video quality, VBrick MPEG-2 appliances reorder packets by default. Since this reordering can cause an increase in latency and affect applications like video conferencing, you can set packet ordering to disabled at schedule end.
Stored Schedule Mode	Used when creating a live broadcast schedule for stored content. Note that the following parameters are "sticky." They remain associated with the schedule even if the Stored Schedule Mode is subsequently changed. • Content Centric – content titles are shown; content servers are not shown. The content is downloaded from load-balanced servers. Use Content Centric when creating stored schedules in large-scale implementations where the system has multiple load-balanced VODs in the same LAN and the Portal Server is in the same domain. • Server Centric – content servers are shown with a tree control for selecting content. The content is downloaded from a specific server and is not load balanced. Use Server Centric in almost all implementations when stored schedules are being created by an LDAP-authenticated user.
External Player Mode	Windows only. Determines whether or not multiple streams can be displayed by launching external player windows. Default = Single. You can launch multiple windows but you can only record one stream at a time.

Item	Description
Client Multiple Monitor Setup	The Portal Server supports dual client monitors. However, if you experience problems when using a second monitor, disable the DirectX component VMR9.
Set Cisco ACNS Manifest Options	Check the box to enable generation of a Cisco ACNS Manifest File. (The Cisco ACNS server must be configured to point to this file.) Select the files (MPEG-4 and/or WM) to include in the file, and specify a Manifest Generation Interval (default = 10 minutes) that defines how often the file will be regenerated. Click Generate Now to create an "on demand" file. ACNS copies all MPEG-4 and WM video files to all (Windows Media, Darwin, and VOD-W) servers in your VEMS system. Additional configuration steps are required on the VOD-W server only. See <u>ACNS Configuration</u> on page 207 for more about ACNS.
Display VOD File Extensions	Check the box to display file extensions (for example .mp4 or .wmv) in the Portal Server Media Library.
VOD Server Storage Options for H.264 Content	Select from the following options depending on your site requirements. You will also need to reboot the VEMS server before any change takes effect. (Note that if you purchased AmiNET130 Set Top Boxes, they will only play H.264 Transport Stream files.) • Store H.264 Transport Stream Only • Store H.264 MP4 Only • Store H.264 Transport Stream and H.264 MP4 Files (default)
Change MySQL Password	This function lets you change the MySQL password for VEMS database users. Before you can change the MySQL password, you must enter the Admin Username (`root`) and Admin Password (`vbrick_18`). For more information, see <u>MySQL</u> on page 4. Note: A software upgrade reverts the user name and password to `root` and `vbrick_1`. If you previously changed the username and password, you will have to repeat your changes after an upgrade.
VBrick Distributed Media Engine	When playing files from a DME, set Playback Protocol for .MP4 to RTMP (default) or RTSP. This flag sets the protocol that VEMS will force when playing back H.264 files. Since VEMS can't differentiate between .mp4 and H.264 files, it will assume (by default) that .mp4 files are H.264 files, and if the RTMP flag is set, will play the file using the Flash player. As a result, when the Playback Protocol is set to the RTMP default, playback of .mp4p2 files will fail. Note that even if RTMP is selected, set top boxes, playlists, and presentations will still use RTSP for playback.

Custom Fields

Custom fields are used to add additional fields to the Info pages associated with stored videos and live broadcast streams. All stored videos, and those live streams that have been "customized," have an **Info** hyperlink. By default, the Info page has fields for **Description** and **Tags**. The Custom Fields functionality lets you add additional "custom" fields that are appropriate to your business or application. This lets you provide more information on the page and it also makes it easier to search for specific streams. (All defined fields are listed in the dropdown list box next to the **Search** button.)

When you add a custom field using this function, the field is available to administrators as a selection on the Modify Custom Station page (see <u>Add Custom Stations</u> on page 108). It is also available to end users as the **Modify Info** button on the Info pages associated with stored videos (if they have content publishing permissions).

▼   To create a Custom Field:

1.   Go to **Global Settings > Custom Fields**.
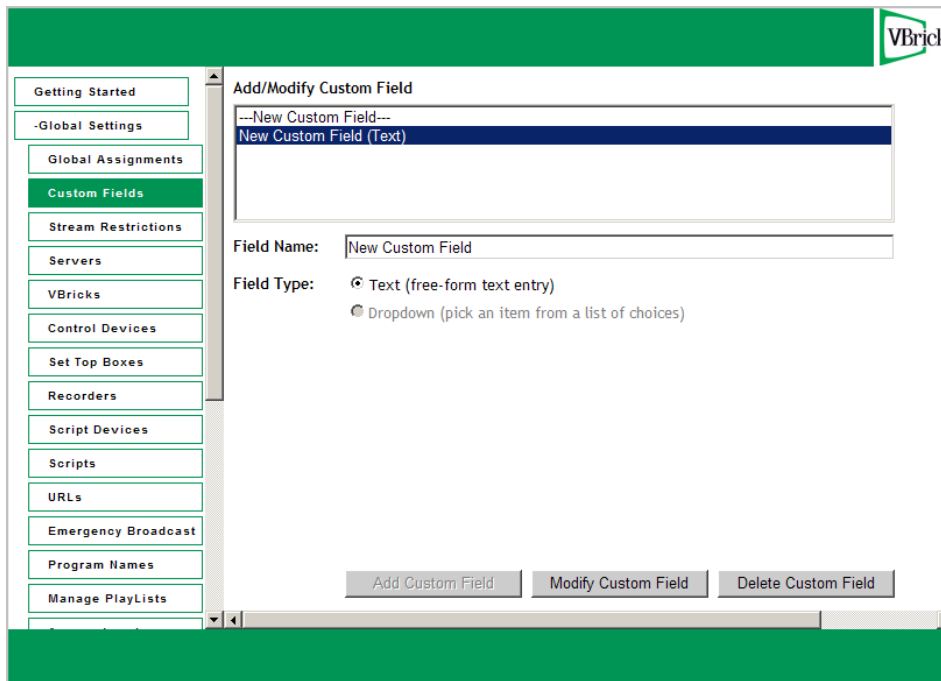
2.   Enter a **Field Name** and a **Field Type**. If you select **Dropdown**, you can add items one at a time followed by **Add Item**. These items will populate a dropdown list box on the <u>Add Custom Stations</u> page.

3.   When done, click **Add Custom Field**. The field will be added to the panel at the top of the window; it will also be available as an option when you are customizing a stream.

Add/Modify Custom Field	This panel shows the existing custom fields that have previously been defined.
Field Name	The field name you want to display on the Info page for this stream or video.
Field Type	This determines how the field will be displayed on the viewer Info page, either as a text field or as a dropdown list box.

Stream Restrictions

Use this page to set and the viewing period for live stream recordings and the maximum number of concurrent viewers. There are no default expiration dates for live streams when a recording is made but administrators can automatically set the content from a specific stream to expire by setting a viewing period. For more about content expiration see <u>Copyright Protection</u> on page 2.

Live Stream	Click on any live stream shown in the list to populate this field.
Max. Concurrent Viewers	Set the maximum number of concurrent viewers for this stream to unlimited or any number greater than zero.
Viewing Period of Stream Recordings	Set the length of the viewing period for a file recorded with this stream in hours, days, weeks, months, or years. The file will no longer be available for viewing at the end of the period and will be deleted or saved as configured in Global Assignments > Set Expired VOD Content Treatment.

Servers

Use the **Servers** page to add or modify VOD servers, FTP servers, and file servers. You can also add or modify VOD Content Folders associated with each VOD server. Note that you can cluster multiple servers to increase throughput: the VEMS Portal Server will automatically load balance all servers defined on the **Servers** page; no additional configuration is necessary. Note that content added by users in the Internet zone will only be ingested to VOD servers in the Internet zone for which they have permissions. Content added by users in the LAN zone will be ingested to all VOD servers for which they have permissions. See <u>VEMS VOD Servers</u> on page 6 for more about VEMS servers.

> **Note** After adding a server, it may take up to 20 minutes for new server content to be displayed in the VEMS Portal Server. To make content available immediately, go to **Global Settings > Global Assignments > Assign VOD Polling Interval** and click **Sync Now**.

The following window (Figure 5) shows an example of the Servers page. It shows the parameters that will be displayed if you choose to add a VOD-W server. The options on the page will vary depending on which type of server you select from the dropdown list. Most of the fields described below are common to all servers. For parameters that are unique to a specific server type, refer to the actual description of that server on the pages that follow.

Note that when defing a server, if your network supports Windows 98 users, you *must* use the IP address of the VOD server—not the host name. After selecting a **Server Type** VBrick recommends you keep the default settings for FTP Password, Publishing Local Path, Publishing Directory, etc. unless there is a compelling reason to change them. Nor is it necessary to create a Streaming Alias. Leave this parameter blank unless you are using HTTP Tunneling.

Figure 5. Add VOD-W Server

Number of Connection Licenses	Enter the number of VOD servers you purchased from VBrick. Default = 0. When purchasing a VOD server from VBrick, you are allowed one connection license per server. If you wish to use a VOD server purchased elsewhere, you must buy a connection license from VBrick for each connected server to comply with licensing requirements.
IP or Domain	This is the primary IP address or Host Name of the VOD server for LAN users (see also **Secondary Server Address** below). The Server Name or IP address entered into the VEMS Portal Server must be accessible by the VEMS Portal Server. (If the network supports Windows 98 users, you *must* use the IP address.)
Server Description	This allows the administrator to define a descriptor such as location.
FTP User Name	This is the FTP user name that the Portal Server uses when publishing content to the server. The default user name for NXG, VOD-D, VOD-WM, and FTP servers is vbrickuser. The default user name for VOD-W servers is anonymous. The FTP User Name refers to a user account that already exists on the server. If the FTP User Name is changed on any VOD server, it must be changed here as well. Use any combination of alphanumeric and special characters.

Server Type	To add a server to the VEMS configuration select one of the following options from the dropdown list: • **VOD-W** – Windows-based InfoValue VOD server. • **VOD-D** – Darwin Open Source server for Windows, or Macintosh. Ingests and plays MPEG4 content only. Requires an FTP server. • **VOD-WM-Enterprise** – Microsoft Windows Media Server (unicast or multicast). Requires an FTP server. • **VOD-WM-Standard** – Microsoft Windows Media Server (unicast only). Requires an FTP server. • **FTP** – Use FTP only if you want to copy from the Recorder server to another FTP server in which case it records to `ftp:\root`. • **File-Server** – Any Windows computer with an FTP server running can be configured as a progressive download file server. • **Wowza-Server** – Wowza Server 2 Flash Media Server supports H.264 and FLV files. • **Flash Media Server** – Adobe's proprietary media server works with the Flash player runtime environment. • **NXG** – Linux-based Kasenna VOD server. This legacy device is no longer supported. • **DME-Media Engine** – VBrick's Distributed Media Engine provides reflecting, media transformation, and VOD storage. • **Lifesize** – Provides access to live and stored streams on a Lifesize server.
FTP Password	The FTP password the Portal Server uses when publishing content to the server. The default FTP password for VOD-W, VOD-D, VOD-WM, and FTP servers is `vbrickuser`. If the FTP Password is changed on the server, it must be changed here as well. Use any combination of alphanumeric and special characters.
Publishing Local Path	Maps the Publishing Directory to the physical location on the VOD server.
Publishing Directory	Used for Add Video, FTP, or Record. The logical path to a folder under `FTP` root. This is the staging area on the VOD server from which files are ingested to the destination folder.
Streaming Alias (IP or Domain)	Some content hosts (PowerStream, Akamai, etc.) use one host name for FTPing and indexing content, and another host name for streaming content. If necessary, use this field to identify the host name alias for streaming content. *Be aware that if you specify a Streaming Alias here, it overrides all other addresses (LAN and Internet) that have been defined for streaming content.* In other words, one alias is used for all streaming for all users.

HTTP Tunneling Port	VOD-W, VOD-WM and VOD-D servers can stream to clients via the HTTP protocol. By default this uses port 80. If another process on the server (for example a web server) is also using the HTTP protocol, there will be a conflict on this port. This setting lets you select a different port (1–65535 with limitations) to be used when streaming via HTTP. This setting *must* correspond with the port setting on the server. See "Assign LAN/Internet Address Range > Always use TCP protocol for MPEG-4 content" in <u>Global Assignments</u> on page 23.
Secondary Server Address	A VOD server can have two addresses: one for Internet users and one for LAN users (see also **IP or Domain** name above). This is the secondary server address for Internet users. It is the IP address or domain name of a second NIC or a NAT.

Add VOD-W Server

A sample page for a VOD-W server is shown in Figure 5. The following parameters are unique to VOD-W servers.

Enable URL Password Protection	Check to enable an encryption key in the URL for added security. Default = unchecked.
Web Service Port (HTTP)	The Portal Server and the VOD-W communicate using a web service configured to use port 80 by default. If you choose to tunnel over port 80, you must use a different port for the web service communication using this parameter. You must configure the VOD-W to use this same port for the web service. See "Using HTTP Tunneling" in the *VOD-W Admin Guide* for more details.
Ingest H.264 Transport Files To This Server	Default = checked. If checked, and the input file is an H.264 transport file, it will be ingested to this server; if the input file is an H.264 MP4, it will be converted to an H.264 transport file and ingested to the server. If unchecked, no H.264 transport files will be ingested to this server.
Ingest H.264 MP4 Files To This Server	Default = checked. If checked, and the input file is an H.264 MP4, the file will be ingested to this server; if the input file is an H.264 transport file, it will be converted to an H.264 MP4 and ingested to the server. If unchecked, no H.264 MP4 files will be ingested to this server.
Support HTTP Tunneling?	*VOD-W only.* Determines whether or not the server supports HTTP tunneling. Default = checked. Go to Global Assignments to actually enable HTTP tunneling. See "Assign LAN/Internet Address Range > Always use TCP protocol for MPEG-4 content" in <u>Global Assignments</u> on page 23. Uncheck if you are using a VOD-W server installed *before* Portal Server v4.2.

Enable URL Password Protection	*VOD-W only.* Default = unchecked. To enable URL password protection, check the box and enter and confirm a password. *The password must match the password configured on the VOD-W server.* Default password = vbrickkey. If checked, all video requests sent to VOD-W servers by the VEMS Portal Server will have a security token embedded in the URL. The VOD-W server will validate and deny the request if the token is absent or invalid.

Add VOD-WM Server

Although the VOD-WM Enterprise server supports numerous multicast types, the Portal Server creates and displays only "File" multicasts which stream a single file. A Windows Media server administrator can create other multicast types using the Windows Media Services interface but these multicast types are not supported and may not be displayed in the Media Library. Note that the **Free Space** option (see below) is only available if you run the EnableQueryDiskSpace.reg utility.
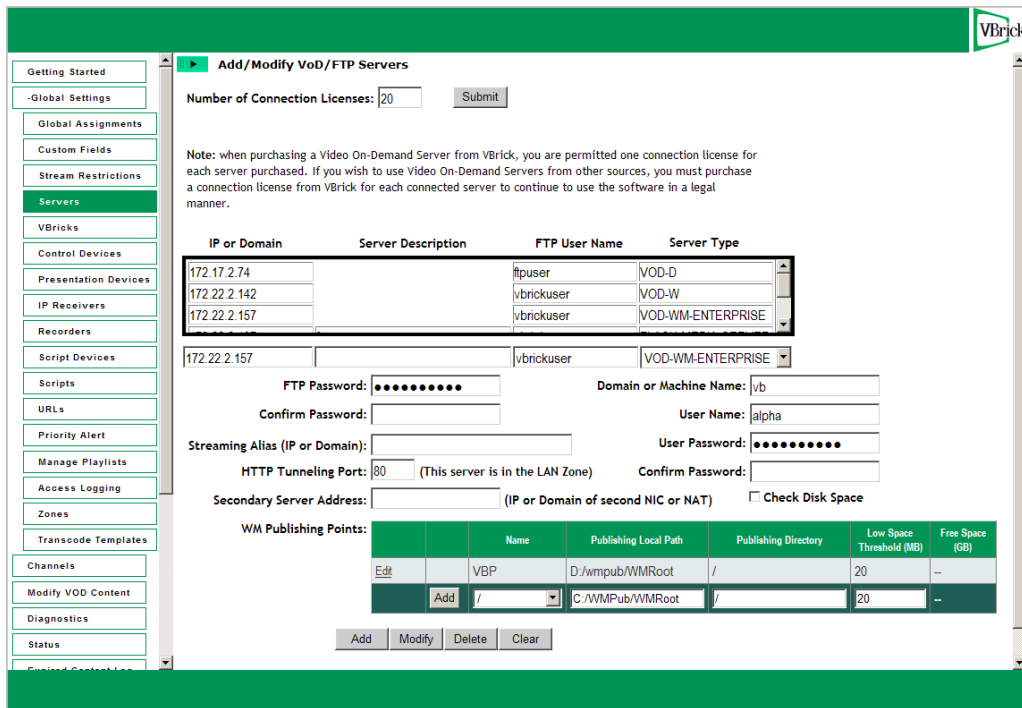

Figure 6. Add VOD-WM Server

Domain or Machine Name	When the VEMS Portal Server and the VOD-WM server reside in the same domain, this is the name of that domain. When workgroups are being used, this is the machine name of the VOD-WM server. Note: the machine name is *not* the IP address of the server.

User Name	The name of a valid user that has administration privileges on the VOD-WM server or the network domain. If the VOD-WM Server is within a domain, the name entered here will be a domain user. That domain user must have administration privileges on the VOD-WM Server. If the VOD-WM Server is part of a workgroup, the name entered here will be a local user with administration privileges on the VOD-WM Server. A local user with administrator privileges having the same name must also exist on the VEMS Portal Server.	
	Note: The VEMS Portal Server and VOD-WM Server(s) must all be within a domain or part of a workgroup. Any topology that mixes servers in domains and servers in workgroups will not work or will be extremely slow.	
User Password	The valid password of the user specified above.	
Check Disk Space	Default = unchecked. If checked, the Portal Server will periodically check the available disk space remaining on the server machine. Uncheck this box if the server is in the Internet zone, if there is a firewall between it and the Portal Server, or if the server is not a Windows server (the disk space check capability is only available to Windows servers and the Flash Media and Wowza servers can run on other platforms).	
WM Publishing Points	Name	The publishing point (default = VBP) on the VOD-WM server where content will be accessed and managed by the VEMS Portal Server. *Note: this setting must correspond to an existing, valid publishing point on the server.*
	Source	Local path to the publishing point. Default = `d:/wmpub/WMRoot`. Do not change for first publishing point.
	FTP Directory	Path to user-created FTP directory. See Creating a VOD-WM FTP Server.
	Low Space Threshold	Optional. Default = 20 MB. If the available disk space on this publishing point is less than the specified value, the publishing point with the largest amount of free space will be used.
	Free Space	Optional. This option automatically calculates the free space (in GB) available on disk when you add a new publishing point or refresh the publishing point list. This feature can consume server resources and is disabled by default. To enable (or disable) this option (on VOD-WM servers or File Servers), go to `<install_dir>\program files\VBrick\MCS\utils`, run `EnableQueryDiskSpace.reg` or `DisableQueryDiskSpace.reg` respectively, and reboot the server when done.

Adding Publishing Points to a VOD-WM Server

In a typical scenario, first you configure the publishing point on the Windows Media server, *then* you configure the publishing point on the Portal Server with matching values. Additional publishing points are required to make content available when you add disk space to a Windows Media server. As shown on the previous window, a Windows Media Server supports multiple publishing points. *In this context, publishing points are used to discover your content via FTP.* Use the following steps, **in the order shown**, to create a new publishing

point. Note that as explained below, you must create a virtual FTP directory in IIS for *each* publishing point on the WM Server.

▼ To add a publishing point:

1. Create an FTP server on the WM server. See <u>Creating a VOD-WM FTP Server</u> on page 40.

2. Create a publishing point on the WM Server.

   a. Go to **Start > Administrative Tools > Windows Media Services**.

   b. Right-click on the server_name and select **Add Publishing Point (Wizard)**.

   c. Add a meaningful publishing point name and click Next.

   d. Select **Files (digital media or playlists) in a directory** and click Next.

   e. Select **On-demand publishing point** and click Next.

   f. Specify the location of your content, for example d:\WMPub\WMRoot and click Next.

   g. Skip through the remaining steps and click **Finish** when done.

3. To create a virtual directory on the WM server for this publishing point:

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

   b. Navigate to the Default FTP Website. Right-click and select **New > Virtual Directory**.

   c. For **Alias**, use the Publishing Point name from Step 3 above and click Next.

   d. Enter the path to the content directory for this FTP site and click Next.

   e. Allow **Read** and **Write** permissions and click Next.

   f. Click **Finish** when done.

4. In the Portal Server, configure the publishing point **Name**, **Source**, and **FTP Directory** to match the values you used for the publishing point on the Windows Media server.

Note • The publishing point name within a server must be unique. You cannot add a publishing point that already exists in VEMS database.

• The publishing point FTP directory within a server must be unique.

• If free space information is available at the time a publishing point is added, it must be greater than the entered **Low Space Threshold**.

• Publishing points located within another publishing point are not supported although publishing points on the same drive are supported. For example, two publishing points with **Source** c:\pub1 and c:\pub2 are supported but two publishing points with **Source** c:\pub1 and c:\pub1\pub2 are not supported.

Creating a VOD-WM FTP Server

If you are using a VOD-WM-Enterprise or VOD-WM-Standard (Microsoft Windows Media) server, you must install and configure a standard FTP server on the VOD-WM server as explained below. (For more about Microsoft Windows Media servers see <u>VEMS VOD Servers</u> on page 6.)

▼ To create a Microsoft Windows Media FTP server:

On the Microsoft Windows Media Server:

1. Install the FTP server.

2. Set the default FTP directory to the Microsoft Windows Media Server's default Publishing Point directory.

3. Create and configure an FTP user account with full permissions (read/write, rename/delete etc.) on the directory specified above. If using the VBrick default, this account's

user name is vbrickuser and the password is vbrickuser. Hint: use the settings of the anonymous account as an example.

4. Verify that the directory specified in Step 2 above is set to allow the FTP user account full permissions.

On the Portal Server:

5. When the Microsoft Windows Media Server is created or modified, specify the user name and password created in Step 3 above in the **FTP User Name** and **FTP Password** fields on the **Add/Modify VOD/FTP Servers** page.

Add VOD-D Server

A Darwin Streaming Server runs on Windows Server and other platforms and is configured on the Portal Server Admin pages. A Darwin server is the open source version of Apple's QuickTime Streaming Server. It is supported by the open source community and not by Apple. Darwin servers are compatible with Windows and Macintosh desktops. They ingest and play MPEG-4 content only and require an FTP server (see Creating a VOD-D FTP Server on page 41.) For more about downloading, installing, and configuring a Darwin server, go to http://developer.apple.com/opensource/server/streaming/index.html

Creating a VOD-D FTP Server

If you are using a VOD-D (Darwin) server, you must install and configure a standard FTP server on the VOD-D server as explained below. (For more about Darwin servers see VEMS VOD Servers on page 6.)

▼ To create a Darwin FTP server:

On the Darwin Server:

1. Install a standard FTP server on port 21.
2. Set the default FTP directory to the Darwin Server's Media Folder directory (also called the Publishing Point) or create a virtual directory of the FTP root pointing to the Darwin server's Media Folder.
3. Create and configure an FTP user account with full permissions (read/write, rename/delete etc.) on the directory created above. If using the VBrick default, this account's user name is vbrickuser and the password is vbrickuser. Hint: use the settings of the anonymous account as an example.
4. Verify that the directory created in Step 2 above is set to allow the FTP user account full permissions.

On the Portal Server:

5. When the Darwin Server is created or modified, specify the user name and password created in Step 3 above in the **FTP User Name** and **FTP Password** fields on the **Add/Modify VOD/FTP Servers** page.

Add QuickTime Streaming Server

A QuickTime Streaming Server (QTSS) is a Unix-based device that runs on Mac OS X. QTSS is delivered as part of Mac OS X Server and provides enhanced administration and media management tools that are not available as part of the open source project. The following instructions explain how to configure a QuickTime Server so that it is fully compatible with the VBrick Portal Server. When properly configured, the Portal Server will recognize, display,

and play content stored on the QTSS and will record content to the QTSS. A QuickTime Streaming service is part of Mac OS X Server. It is not related to the Portal Server application and is configured separately. *This procedure has been tested on Mac OS X 10.5.* It may work on other Mac OS X versions but this has not been verified by VBrick.

Note This procedure explains how to configure the QTSS to work with the VEMS Portal Server. It assumes you have a working administrator knowledge of Mac OS X. You can use other methods but this is the only method used and tested by VBrick.


A typical installation of QuickTime Streaming Service (QTSS) under Mac OS X Server will set the default content to be served from `\Library\QuickTimeStreaming\Movies`. A typical installation of FTP service will set the default **Authenticated users see** to FTP Root And Share Points and the **FTP Root** to `/Library/FTPServer/FTPRoot`. These defaults must be modified as explained below.

▼   To configure a QuickTime Streaming Server:

On the Mac QuickTime Server

1. Create another user in the Mac OS X environment naming it for example `content` and set the home folder for this user to `/Users`.

2. Create a folder under `/Users/content` called `videos`.

3. Open a Terminal window in Mac OS X and login as the administrator e.g `su`

4. In the Terminal window, navigate to the content folder: `cd /Users/content`

5. In the Terminal window, set the permissions to allow the world to read/write to the videos folder: `chmod 777 videos`

6. In the Terminal window, navigate to the QuickTime Streaming Service publishing point: `cd /Library/QuickTimeStreaming/Movies`

7. In the Terminal window, create a link to the `videos` folder: `ln –s /Users/content/videos videos`

8. Open the Server Admin interface to manage the FTP service. Go to **Advanced**, set **Authenticated Users see** to Home Directory Only using the dropdown, and then click **Save**.
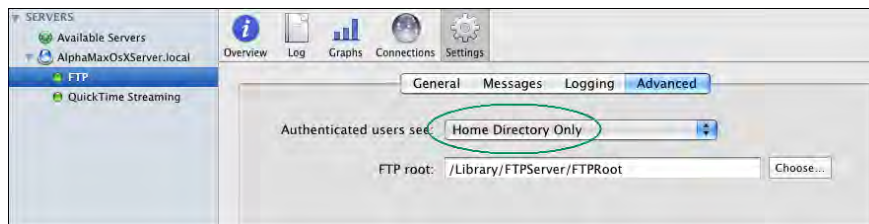
9. If you will be using this QuickTime Streaming server *exclusively* with the Portal Server click on **QuickTime Streaming** and append `videos` to **Media directory** path. If you will *not* be using this QuickTime server exclusively with the Portal Server, skip this step and add a Streaming Alias when configuring the Portal Server in Step 4 below.

10. Save and restart the server when done.
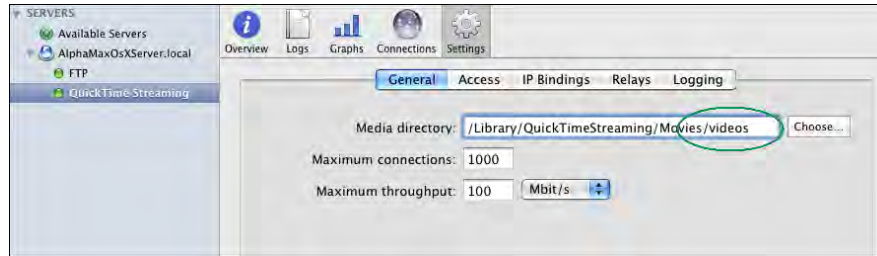
On the VBrick Portal Server

1. Open the Portal Server Admin Console and go to Global Settings > Servers.

2. Add a VOD-D server with the IP address, FTP User Name = `content`, and FTP Password.

3. Set the **Publishing Directory** folder to `/videos`.

4. If you skipped Step 9 above when configuring the QTSS, configure a **Streaming Alias** for `server_name/videos` or `ip_ address/videos`.

5. After successfully completing these steps you will be able to read and write content from the QuickTime server.

Add FTP Server

Use FTP only if you want to copy from the Recorder server to another FTP server in which case it records to `ftp:\root`.
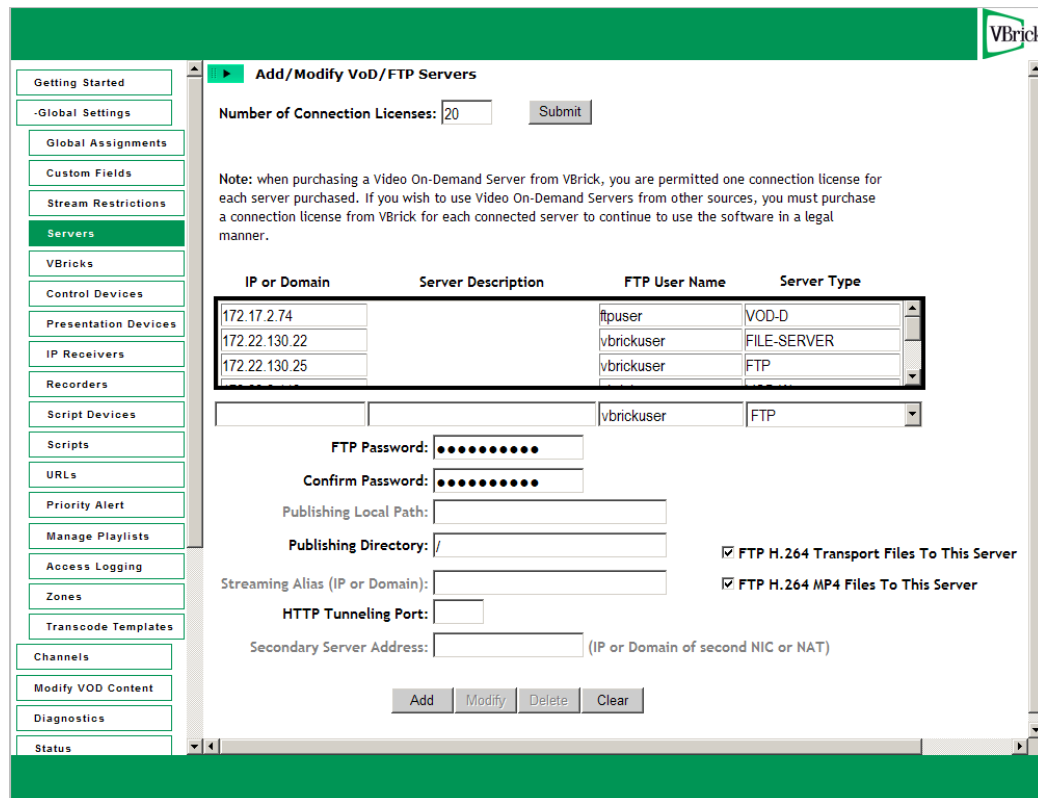

Figure 7. Add FTP Server

FTP H.264 Transport Files To This Server	Default = checked. If checked, and the input file is an H.264 transport file, it will be FTPed to this server; if the input file is an H.264 MP4, it will be converted to an H.264 transport file and FTPed to the server. If unchecked, no H.264 transport files will be FTPed to this server.
FTP H.264 MP4 Files To This Server	Default = checked. If checked, and the input file is an H.264 MP4, it will be FTPed to this server; if the input file is an H.264 transport file, it will be converted to an H.264 MP4 and FTPed to the server. If unchecked, no H.264 MP4 files will be FTPed to this server.

Using Secure FTP

VBrick's FTP client supports secure FTP connections from the end user (client), Portal Server and NVR to the VOD servers. This is accomplished using FTP over SSL (FTPS protocol). Having a client that supports FTPS however, is not enough to have secure FTP connections throughout the system. The FTP servers on all VOD servers also need to support FTPS for a secure connection to exist. If a secure connection cannot be established, the client will revert to the standard FTP protocol. The FTP server on Windows platforms (IIS) does not currently support FTPS. *Therefore, to have secure connections, you must install a third-party add-in on all Windows VOD servers.* Of the various solutions available, VBrick recommends FTP Guardian. FTP Guardian is a wrapper for IIS that serves as a proxy between a secure client and an unsecured IIS. You change the FTP port of IIS to an arbitrary port (10021 for example), then you start the FTP Guardian service. It binds to port 21 and all incoming FTP clients communicate using a secure front that proxies the calls to IIS on port 10021. Be aware that this add-on, for Windows servers only, is not sold or supported by VBrick. It requires a server wrapper and additional .dlls.

▼ To install FTP Guardian:

1. Go to http://www.tcpdata.com/ftpg_license.shtml
2. Click and run **Download ftp Guardian Server Wrapper - 600K** on the VOD server.
3. Click **Download SSL Libraries - 380K** on the VOD server.

Then open the .zip file and copy `libeay32.dll` and `ssleay32.dll` into `C:\Program Files\ftpgs`

Add File Server

Any Windows computer with an FTP server running can be configured as a progressive download file server. Progressive download is a method of delivering audio and video that involves caching and playing the downloaded portion of a file while a download is still in progress via FTP. Recorded WM files are automatically ingested to all VOD and file servers if the user has access rights and publishing permissions. A progressive download file server can provide secure (encrypted) playback if configured for SSL. (Note: You can also use a WM or H.264 encoder with a hard drive for progressive download. See VBrick Configuration on page 58 for more about progressive download.) Note that the **Free Space** option (see parameter description) is only available if you run the `EnableQueryDiskSpace.reg utility.`

Adding MIME Types

By default, Windows Server 2003/2008 does not set MIME types for .mp4, .f4v, .m4v, .flv, and .m4a extensions. This means that if the server is added as a File Server, and a VEMS client attempts to play these files using HTTP, the client will display a "Connection error." To

workaround this issue, you will need to add the MIME types for these extensions to IIS on the Windows Server 2003/2008 machine.

▼   To add the MIME types to IIS:

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

2.   In the navigation bar, go to Sites > Default Web Site > MIME types.

3.   On the MIME Types page click **Add**.

4.   Using the information below, enter the File name extension, the MIME type, and click **OK**. Repeat for each MIME type.

Extension	MIME Type
.mp4	video/mp4
.f4v	video/mp4
.m4v	video/mp4
.flv	video/x-flv (Windows Server 20003 only)
.m4a	audio/mp4

Figure 8. Add File Server

|	
Playback Protocol	• HTTP – Use HTTP if there is a web server running on the file server. For details, see <u>Using HTTP Playback</u> below. • FTP – Use FTP if there is no web server running on the file server. For details, see <u>Using FTP Playback</u> below. • Secure Playback – Use Secure Playback if the file server is configured for SSL. For details, see <u>Using Secure Playback</u> below.
HTTP Playback Port	• 80 – default port for HTTP playback. • 443 – default port for HTTPS playback. To use Secure Playback, the file server must be configured for SSL.
Domain or Machine Name	Displayed when **Free Space** option is enabled. When the Portal Server and the file server reside in the same domain, this is the name of that domain. When workgroups are being used, this is the machine name of the file server. Note: the machine name is *not* the IP address of the server.
User Name	Displayed when **Free Space** option is enabled. The name of a valid user that has administration privileges on the file server or the network domain. If the file server is within a domain, the name entered here will be a domain user. That domain user must have administration privileges on the file server. If the file server is part of a workgroup, the name entered here will be a local user with administration privileges on the file server. A local user with administrator privileges having the same name must also exist on the Portal Server. Note: The VEMS Portal Server and file server(s) must all be within a domain or part of a workgroup. Any topology that mixes servers in domains and servers in workgroups will not work or will be extremely slow.
User Password	Displayed when **Free Space** option is enabled. The valid password of the user specified above.

Content Location	HTTP Directory	Shown if playback protocol is HTTP. The virtual directory on the file server where content will be accessed and managed by the VEMS Portal Server.
	Source	The complete path to the physical location of the content on the file server.
	FTP Directory	Path to a user-created virtual FTP directory. See Add FTP Server on page 43 for more information.
	Low Space Threshold	Optional. Default = 20 MB. If the available disk space on this publishing point is less than the specified value, the publishing point with the largest amount of free space will be used.
	Free Space	Optional. This option automatically calculates the free space (in GB) available on disk when you add a new publishing point or refresh the publishing point list. This feature can consume server resources and is disabled by default. To enable (or disable) this option (on VOD-WM servers or File Servers), go to `<install_dir>\program files\VBrick\MCS\utils`, run `EnableQueryDiskSpace.reg` or `DisableQueryDiskSpace.reg` respectively, and reboot the server when done.

Using HTTP Playback

If you select HTTP for **Playback Protocol**, Figure 9 shows sample content location. The FTP server has three corresponding publishing directories that map to three local paths. These publishing directories are needed for the Portal Server to discover contents in the file server and to publish new content. The file server also has a web server running with three corresponding HTTP directories that map to those three local paths. The Portal Server constructs an HTTP URL for each file and the Portal Server client downloads the file from the web server inside the file server. By default, HTTP is played back over Port 80.
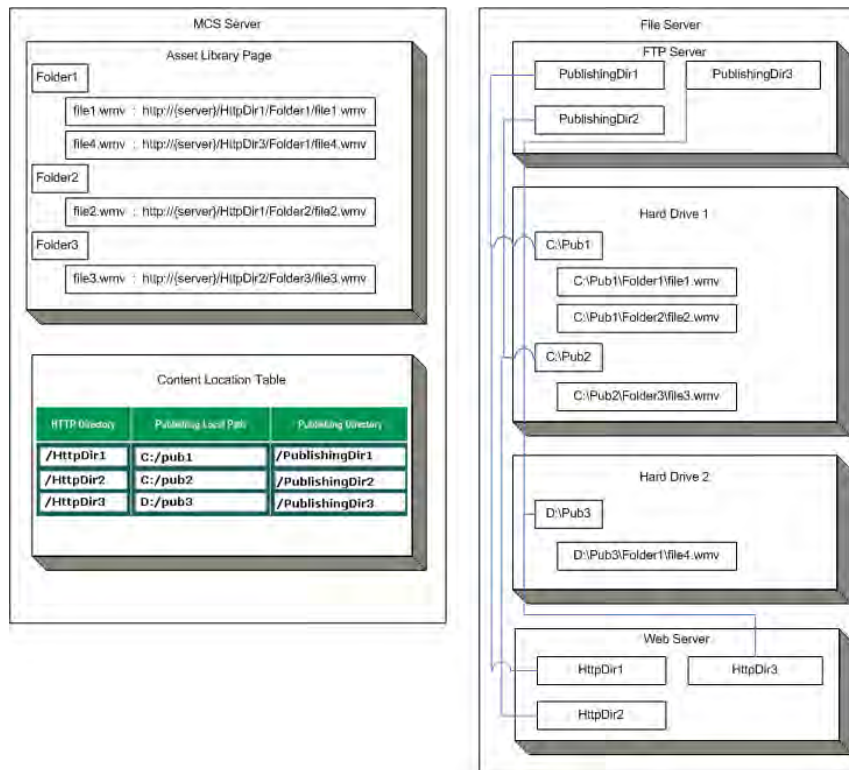
Figure 9. Content Location for HTTP Playback

Using FTP Playback

If you select FTP for **Playback Protocol**, Figure 10 shows sample content location. In the example there are three folders: `c:\Pub1`, `c:\Pub2` and `d:\Pub3`. The FTP server has three publishing directories that map to those three folders. (Note that only one publishing point is actually required.) The Portal Server constructs an FTP URL for each file and the Portal Server client downloads the file from the FTP server inside the file server. Multiple content locations can on the same hard drive. For example, `c:\pub1` and `c:\pub2` are on drive C. This is necessary to preserve the current file structure on the file server but you cannot create a content location inside another content location. Secure FTP playback is not supported. Note that Portal Server users cannot create thumbnails when **Playback Protocol** is set to FTP.
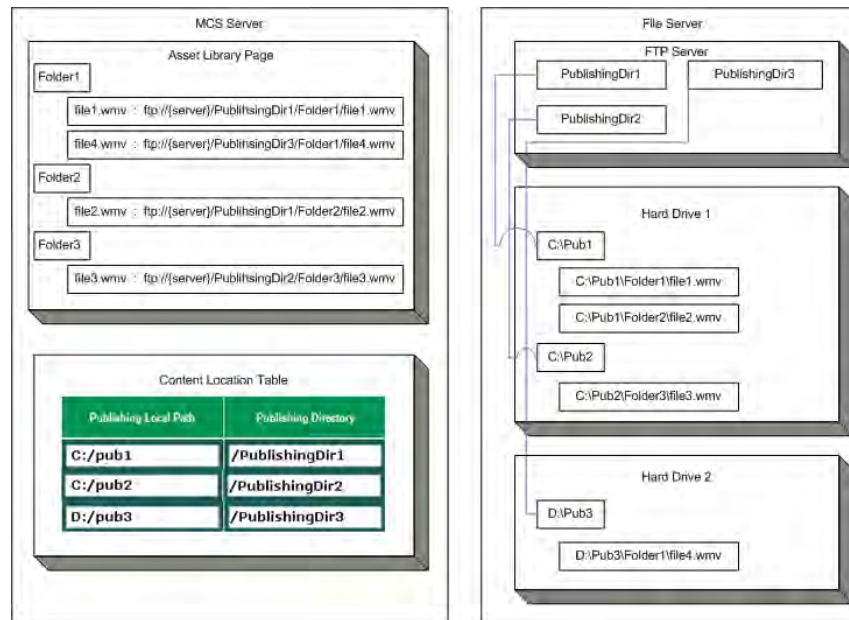
Figure 10. Content Location for FTP Playback

Using Secure Playback

If you select Secure Playback for **Playback Protocol**, the file is progressively downloaded *and* encrypted. In order to use secure playback, the *file server* must be configured for SSL with a digital X.509 certificate from a trusted certificate authority. Secure download is only valid for HTTPS. By default, HTTPS is played back over Port 443. Note that Portal Server users cannot create thumbnails when **Playback Protocol** is set to Secure Playback.

Note	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.

Add Wowza Server

Wowza Media Server 2 is a high-performance, extensible, and interactive Flash media server that also supports H.264 media. Wowza is an alternative to the Adobe Flash Media Server product. Wowza Media Server Pro is a powerful and extensible Java-based server. It unifies the multi-protocol, multi-player H.264 streaming into a single workflow, eliminating the need for multiple player-specific encoders and servers. Wowza Server 2 is a Java-based application that runs on any server platform that supports Java. It ingests and plays .mp3, .mp4, and .flv files. VEMS manages Wowza media content using an FTP server running on the Wowza server. You must define this FTP server as part of the installation. See Creating a Wowza FTP Server on page 51 for details.

The Wowza Media Server 2 includes the ability to share a single server using a "virtual host" configuration. Virtual hosts can be configured with their own system resource and streaming limitations. For example, a server has only one IP address but it can have two virtual hosts, each targeting a different group of users. You can add multiple Wowza server virtual hosts from the same physical server to VEMS as long as they can be uniquely identified by their IP address or domain host name. You can also add multiple applications belonging to the same

Wowza virtual host to the same Wowza server. Files added through VEMS will be added to the first application's storage directory. The Wowza server supports the following Flash content:

- Stored VOD files – can be manually added from the VEMS client interface or auto ingested by the server (see <u>AutoIngest Content</u> on page 177).
- Live VOD streams – an be added by configuring a live stream URL (see <u>Add/Modify a URL for a Live Video Stream</u> on page 81) from the Wowza server or by configuring the encoder to send SAPs to the Portal Server. See the *H.264 Appliance Admin Guide* for more about encoder SAPs.
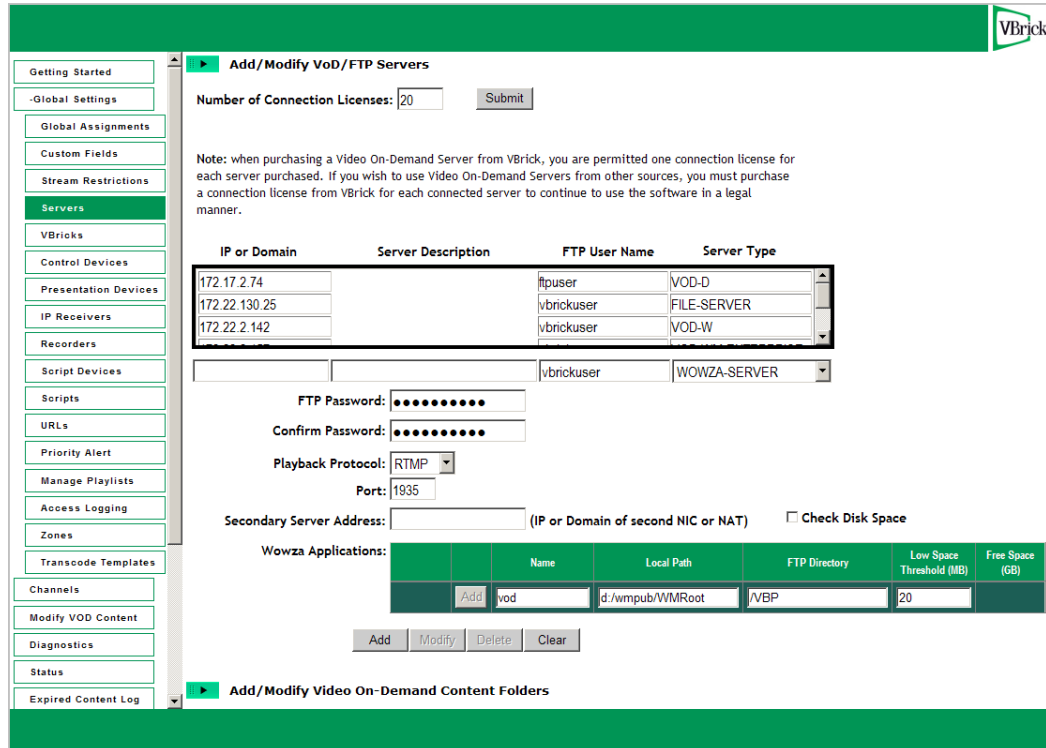
Figure 11. Add Wowza Server

| Playback Protocol | Select from the following. The same protocol will be used for all Wowza "applications" added to VEMS.
• RTMP – Standard, unencrypted Real Time Messaging Protocol.
• RTMPT – RTMP tunneled over HTTP.
• RTMPS – RTMP over SSL.
• RTMPE – Encrypted version of RTMP. RTMPE is faster than SSL and does not require certificate management. |
|---|---|
| Port | Default = 1935 for all protocols. The same port will be used for all Wowza "applications" added to VEMS. |
| Secondary Server Address | A VOD server can have two addresses: one for Internet users and one for LAN users (see also **IP or Domain** name above). This is the secondary server address for Internet users. It is the IP address or domain name of a second NIC or a NAT. |

Wozwa Applications	Name	The application name (default = vod) on the Wowza server where content will be accessed and managed by the VEMS Portal Server. The content path is `C:\Program Files\Wowza Media Systems\Wowza Media Server 2\applications\vod`
	Local Path	Maps the Publishing Directory to the physical location on the VOD server.
	FTP Directory	Path to user-created FTP directory. See <u>Creating a Wowza FTP Server</u>.
	Low Space Threshold	Optional. Default = 20 MB. If the available disk space on this publishing point is less than the specified value, the publishing point with the largest amount of free space will be used.
	Free Space	Optional. This option automatically calculates the free space (in GB) available on disk when you add a new publishing point or refresh the publishing point list. This feature can consume server resources and is disabled by default. To enable (or disable) this option (on VOD-WM servers or File Servers), go to `<install_dir>\program files\VBrick\MCS\utils`, run `EnableQueryDiskSpace.reg` or `DisableQueryDiskSpace.reg` respectively, and reboot the server when done.

Creating a Wowza FTP Server

To get started go to the <u>Wowza</u> website, download the Wowza Media Server application and sign up and obtain a development license. Before you run the Wowza installer you will also need to install the <u>Java</u> JRE and JDK on the server machine if not already present. When creating a Wowza server you need to setup an FTP server on the Wowza server and create an FTP virtual directory for each Wowza application storage directory. You also need to define the relationship between the Wowza application and the FTP virtual directory. Figure 12 shows the relationship between the VEMS server and the Wowza server. The Wowza server runs on a variety of operating system platforms; the following instructions explain how to set up an FTP server using IIS on Windows Server 2003.
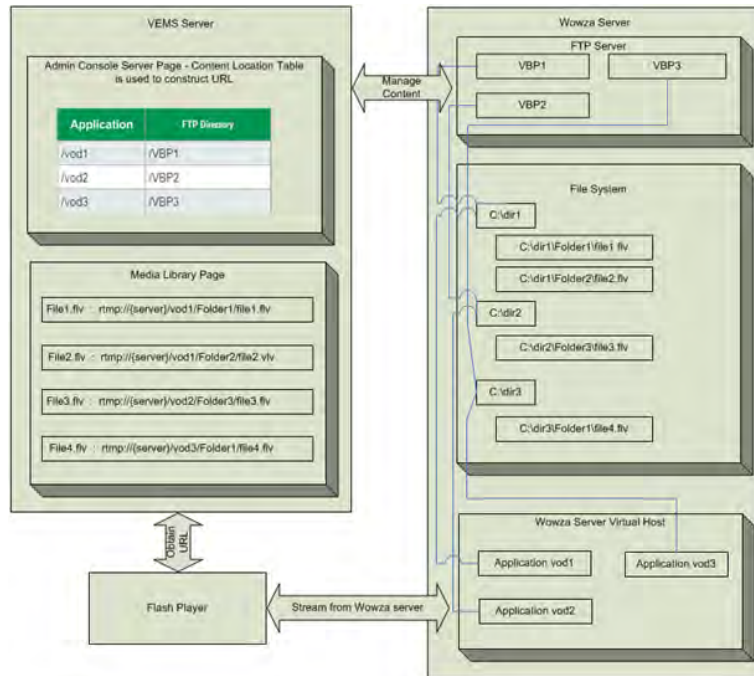
Figure 12. Wowza VOD Server File Structure

▼ To set up an FTP server:

1. Enable the FTP Service (if not already enabled):

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

   b. Click on **Add/Remove Windows Components**.

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

   d. Click on **Internet Information Services (IIS)** and then **Details**.

   e. Check the **File Transfer Protocol (FTP) Service** box and **OK**.

   f. Then complete the wizard and exit.

2. Optional. Configure FTP Server Security. This optional step disables anonymous connections so that only authenticated users can access the server.

   a. Go to **Start > Administrative Tools > Internet Information Services**.

   b. Go to **FTP Sites** and then right-click and select **Properties** on the **Default FTP Site**.

   c. Go to the **Security Accounts** tab and uncheck **Allow Anonymous Connections**.

3. Create a new FTP virtual directory mapped to the Wowza content folder.

   a. Go to **Start > Administrative Tools > Computer Management**.

   b. Go to **Services and Applications > Internet Information Services (IIS) Manager** > **FTP Sites**.

   c. Right click on the **Default FTP Site** and select **New > Virtual Directory**.

   d. Define the **Virtual Directory Alias** as **VBP** and click **Next**.
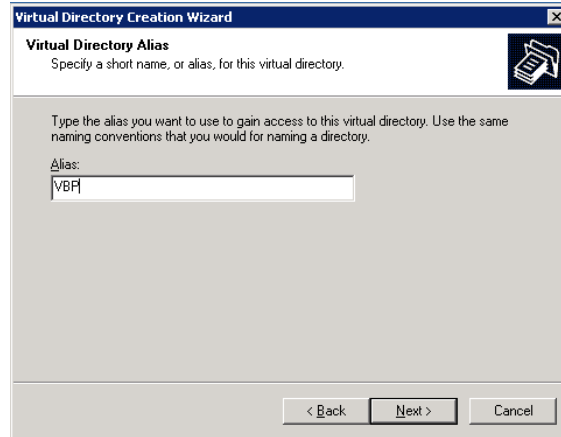
e. Browse to the Wowza default content folder: `C:\Program Files\Wowza Media Systems\Wowza Media Server 2\content`. If the Wowza server has multiple applications, you will need to create a FTP virtual directory for each application.
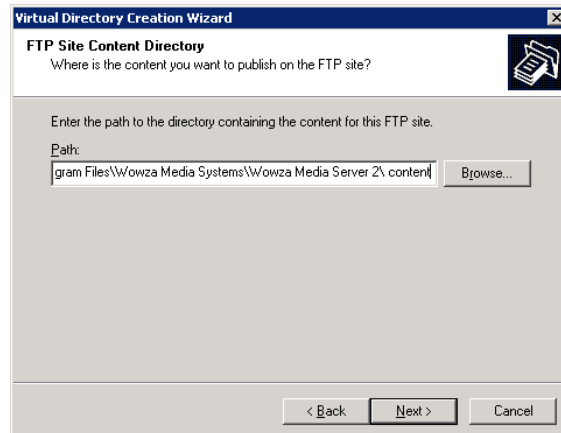
f. Check the **Write** box to enable adding content to the Wowza server.
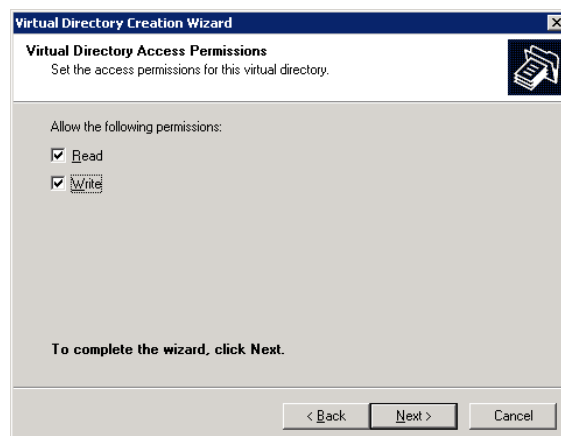
g. Click **Next** to complete the wizard.

4. Give the FTP user access the content folder.

a. In Windows Explorer, go to `C:\Program Files\Wowza Media Systems\Wowza Media Server 2\content`.

b. Right-click on the content folder and select **Properties**.

c. Go to the **Security** tab and give **Full Control** to the vbrickuser.

Starting the Wowza Server

▼ To start the Wowza Server via System Services:

1. Go to Start > Settings > Control Panel > Administrative Tools > Services > Wowza Media Server.

2. Change **Service** to **Automatic**.

Add Adobe Flash Server

A Flash Media Server (FMS) is a proprietary data and media server from Adobe Systems. This server works with the Flash Player runtime to create media driven, multiuser RIAs (Rich Internet Applications). A Flash Media Server is a hub; Flash-based applications connect to the hub using Real Time Messaging Protocol (RTMP). The server can send and receive data to and from the connected users with alive web FLV player installed. Adding an Adobe Flash Media Server is essentially the same as adding a Wowza Media Server. The Adobe server supports stored VOD files and live VOD streams. *The only significant difference is that the Wowza server supports multiple publishing points but the Adobe server supports only one publishing point.* To add an Adobe FMS, follow the steps in Add Wowza Server on page 49.

Add NXG Server

NXG VOD servers are legacy VEMS components. Existing NXG VOD servers are compatible with VEMS 5.3 but have not been tested and are no longer be supported by VBrick. This means you can use existing NXG servers if they work but VBrick assumes no responsibility for support if they do not work.

Add DME Media Engine

The VBrick H.264 Distributed Media Engine (DME) simplifies delivery of high definition video and other rich media content across multi-site enterprises and campus environments. The Distributed Media Engine, typically deployed at the network edge, is a single integrated platform which provides media redistribution, media transformation and video-on-demand content storage. The DME accepts a H.264 video stream from a central site and redistributes that content to diverse endpoints including PCs/MACs, mobile phones and televisions/monitors. This one integrated platform optimizes WAN bandwidth use, simplifies endpoint support and offers local storage of centrally managed content.

Figure 13. Add DME Media Engine

Playback Protocol	When playing files from a DME, you can set the Playback Protocol for .MP4 to RTMP or RTSP on the Global Settings > Global Assignments page. This setting shows what is selected on that page.
	• RTMP – Protocol playback is forced to standard, unencrypted Real Time Messaging Protocol.
Progressive Download	Enabled by default. over Port 80. Check Secure Playback to use Port 443.

Add LifeSize Server

A VEMS LifeSize server plays content that is sourced from a v1.2 or higher LifeSize Video Center. It provides access to live streams that are physically hosted on a remote LifeSize server. High Definition streams can originate at LifeSize (or be reflected from a DME) and play in the highly-scalable VEMS environment. VEMS polls the Lifesize server at the specified interval (see Set Polling Interval) and automatically populates the **Live Media** page with available Lifesize streams. Content can be added to LifeSize using the **Add Video** feature on the VEMS client, by auto ingesting content (see Auto Content Ingestion, or by scheduled or push button recording. For information about configuring the LifeSize server, see the *LiveSize Administrator Guide* that was shipped with the server.

Notes Content being added to the LifeSize server is subject to the following constraints:

- If a transcode is currently in progress on the **Add Video** page, content will not be added to LifeSize and a message will be displayed in the Windows **Event Viewer**.
- If a remote NVR is configured, and it is the only NVR, content will not be added to LifeSize and a message will be displayed in the Windows **Event Viewer**.
- If a remote NVR is configured, as well as a local NVR, content <u>may</u> be added to LifeSize if the local NVR is selected randomly by the NVR's load-balancing algorithm.
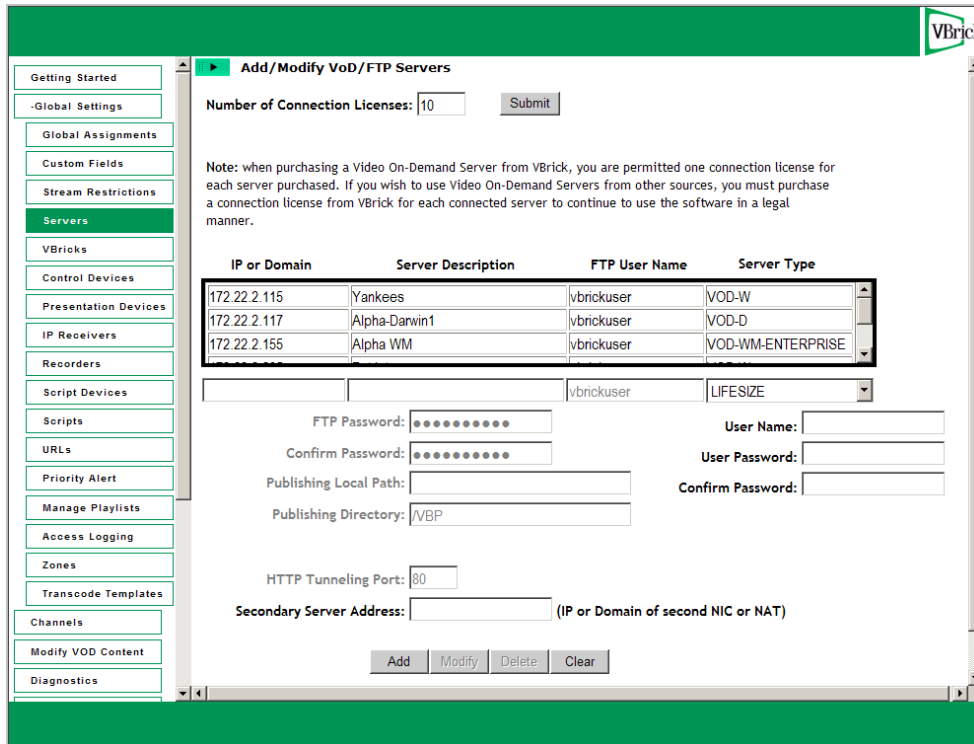
Figure 14. Add LifeSize Server

User Name	`administrator`
User Password	`admin123`

Set Polling Interval

You can set the interval at which VEMS polls the LifeSize server by adding the following keys to `VBUService.exe.config`. The first key is the interval for live content polling; the second key is a timeout after which the program is removed if no stream is detected. Both values are in seconds and the file is located in: `C:\Program Files\VBrick\MCS\Common\VBUService`

```
<add key="LifeSizePolling" value="30" />
<add key="LifeSizeContentTimeout" value="35" />
```

Add/Modify Video On Demand Content Folders

Add/Modify Video On Demand Content Folders can be used to organize content on a specific Video-on-Demand server. The Portal Server periodically polls certain folders for presence of content and if found ingests the content onto multiple VOD servers. Any files FTPed into a particular folder in the Autoingest folder will automatically be ingested into the corresponding folder on the VOD server(s). You must add these folders using the window shown below. (See Auto Content Ingestion on page 177 for more about autoingestion.) Existing folder structures on a VOD server will be mirrored in the Portal Server. However you will still need to associate those folders with other server(s) if the file is to be autoingested onto multiple servers.

This function is useful for VBrick VBStar appliances to easily transfer content from their hard drives to the VOD server. (It can also be helpful for users who acquire content outside of the VEMS Portal Server, for example from StreamPlayer Plus.) When a folder is created, you must check a box in **Add/Modify Folders on Selected Servers** to associate the folder with a server for autoingestion. VEMS Portal Server checks these folders every 5 minutes and ingests new content if present. This feature only applies to Autoingest; it does not apply to **Record** or **Add Video**.

Note that empty folders are not displayed on the Portal Server client interface. These folders are only displayed when they have content. As the folder structure is created in this section, autoingest folders will be created in the FTP root path. For example, if the FTP root path is `d:\inetpub\ftproot`, then folders that are created in the **Add/Modify On-Demand** content folders will also be created in the `d\inetpub\ftproot\mcs\autoingest` folder.

Autoingested content can go into any folder that has been associated with a server or servers using the **Add/Modify Folders on Selected Servers** check boxes shown above. If using a VBStar, be sure to associate a folder with a server for autoingest. This enables the folder that the VBStar will FTP files into. This function is not associated with a user or group

permission and is controlled only by the Administrator. See <u>Auto Content Ingestion on page 177</u> for a more detailed description of the Autoingestion functionality.

Note Use the **Delete** button to remove non-empty folders only. Use the **Modify** button to change AutoIngest settings in the **Add/Modify Folders on Selected Servers** pane.

Creating Subfolders

Use the following steps to create a subfolder in an existing folder.

▼ To create a subfolder:

1. Highlight any existing folder name, for example /Bill as shown in the previous window, and click **New**.

2. Type the new subfolder name in the text field, preceded by a forward slash, for example /Bill**/temp**, and click **Submit** when done.

VBricks

All VBricks must be configured in VEMS Portal Server before they can be managed and used for scheduled events. (VBrick configuration is only required if you are using the **Scheduling** feature. Once configured, all VBricks in the system are shown on the following window. In the VEMS Portal Server, SAP (Session Announcement Protocol) announcements are sent to the Portal Server by network-connected VBrick devices (encoders and/or decoders). The **Select VBrick** panel in the next screen shows VBrick appliances (encoders and decoders) that have announced their presence on the network but have not been configured for use in VEMS Portal Server. (Note that if you delete a VBrick from the **Currently Configured VBrick List**, it will not be shown as available until you logout and log back in to the Admin Console.)

VBrick Configuration

▼ To add a VBrick configuration:

1. Go to **Global Settings > VBricks**. The information in the panel indicates whether a VBrick can be used for multimedia or for progressive download (as a VOD server).

2. Select **Add VBricks** and click **Submit**.

3. In **Select VBrick**, select one or more existing VBricks for which a SAP has been received. If you select one VBrick, this populates the **VBrick Configuration** panel. (If you select multiple VBricks, it does not populate the panel; if you need to configure the VBricks, you must add them one at a time.)

4. Complete or modify the fields in **VBrick Configuration** as necessary. Note that you must enter a User Name and Password <u>and</u> confirm that Password or the configuration will fail.

5. Click **Submit** when done. This adds the new configuration to the list of configured VBricks shown on the previous page.

Note	The only time you will need to manually complete the VBrick Configuration fields is when you are defining the configuration for a VBrick that will be added to the network at a later time. In this case, you will need to know the following configuration data in advance. The only exception is the HTTP Port. The HTTP Port is required if you will be using the VBrick to support presentations.

Host Name	Required. Host name of VBrick.
IP Address	Required. IP address of VBrick.
User Name	Defaults to system-defined value if blank.
User Password	Defaults to system-defined value if blank.
Confirm Password	Defaults to system-defined value if blank. Must match User Password if entered above.
Software Revision	Optional. To get the Software Revision, use IWS (for MPEG and WM) or VBAdmin (for H.264).
HTTP Port	Optional (required for Presentations). To get the HTTP Port, use IWS (for MPEG and WM) or VBAdmin (for H.264).
VBrick Model	Select from the dropdown. Advanced settings are enabled if you select an encoder or a VBStar.
Progressive Download Server	Check this box to enable a WM VBStar (with v4.2.1 or higher software) or an H.264 VBStar (with v3.0 or higher software) as a progressive download server. A VBStar is a WM or H.264 encoder with a 60 GB hard drive (the H.264 encoder also supports an external USB drive). All .wmv and .flv files stored in the `D:\public` folder of the VBStar (or in `E:\public` for an H.264 encoder with and external USB hard drive) will be available in the Media Library for progressive download. (Note also that you can also use a File Server for progressive download. See <u>Add File Server</u> on page 44 for more information.)
Allow Content Publishing	All WM and H.264 recordings will be published to the VOD servers *and* to this VBStar if the user has access rights and publishing permissions. Note that ingestions to the VBStar will fail when the 60 GB hard drive is full.
Storage Location	*H.264 VBStar appliances only.* Select the 60 GB **Internal Drive** or a physically-attached **External USB** drive.

Advanced Settings

Advanced settings are enabled if you select a VBrick encoder or a VBStar. *Note that the Portal Server will attempt to retrieve and autofill the Multicast IP addresses and Port numbers.* You can modify these fields as necessary.

Note The following values are stored in the Portal Server database only. Depending on how a scheduled event is configured, they may be saved and written back to the VBrick device after the scheduled event runs.

Multicast IP	Destination multicast IP address.
Video Port	Destination video port.
Audio Port	MPEG-4 devices only. Destination audio port.
CC Port	MPEG-4 devices only. Closed captioning port.

Multimedia VBrick Configuration

These settings are only enabled when you add or modify a VBrick that has a WM encoder (with a hard drive) or an H.264 encoder (with internal or external storage) in at least one slot. By completing these fields you are defining the encoder as a **Multimedia VBrick** that can be used for presentations and in specialized end-user environments. For example, in some environments, the Portal Server can be configured to use a multimedia VBrick for rich media presentations. In this scenario, the settings (for **Resolution**, **Target Bit Rate**, and **Audio Bit Rate**) are used at presentation runtime and will override existing settings on the VBrick encoder.

A VBrick reflector model (with a WM VBStar hard drive) can also be configured as Multimedia VBrick and used for presentations. This setup can be used with VBrick's Rich Media Studio or with a Tandberg Content Server (TCS). Presentations configured with the reflector do not support slides, polls, share website, and text overlay features. The user interface for these features (on the VEMS client "Presenter" page) is disabled.

Slot 1 is a Multimedia Slot	Default = not checked. Lets you define the multimedia-specific fields listed below. Slot 2 (if present) can also be configured for multimedia.
Include CC and Metadata	Default = not checked. Include closed captions and metadata if available in the stream.
Description	Text field used for descriptive text.
E-Mail Template	This field, used with custom applications, adds the specified text to an auto-generated e-mail and ensures that the e-mail recipient can connect to the right VBrick encoder.
Add Viewing URL	To see this field, you must first "Add" the VBrick and then go back in and select "Modify." Typical examples are shown below. For Windows Media, enter a fully-qualified path to the Windows Media Server and Publishing Point that will be hosting the video. For example: • Windows Media – `http://www.WM_Server_IP_Address/Publishing_Point` • H.264—`vbricksys:\\<multicast_url>&port=<port_number>&<source_ip_address>` Note: If you are using Zones, you may need to add a reference IP address. See Adding a Reference IP Address for URLs on page 82.

Control Devices

 Control devices let you configure a video source device so that it can be controlled by end users from the Portal Server user interface. (An example of a video source device is a DVD or VCR directly connected to a VBrick encoder.) Once configured, a special icon on the **Live Media** page indicates you can control the stream using a "virtual" remote control

panel as shown in Figure 15 below. VBrick currently supports DVDs and VCRs from several different manufacturers as well as the VBrick VBIR remote controller that can be customized for use with a wide variety of source devices. See Add User-Defined VBIRs below for more about VBIRs.

Note In some cases you may be able to control a source device using the front panel or the handheld remote that came with the unit, but this is not always possible. For example, if the remote gets lost or the source DVD and/or VCRs are rack-mounted in an inaccessible metal enclosure, you *must* use the Portal Server interface or a VBIR.
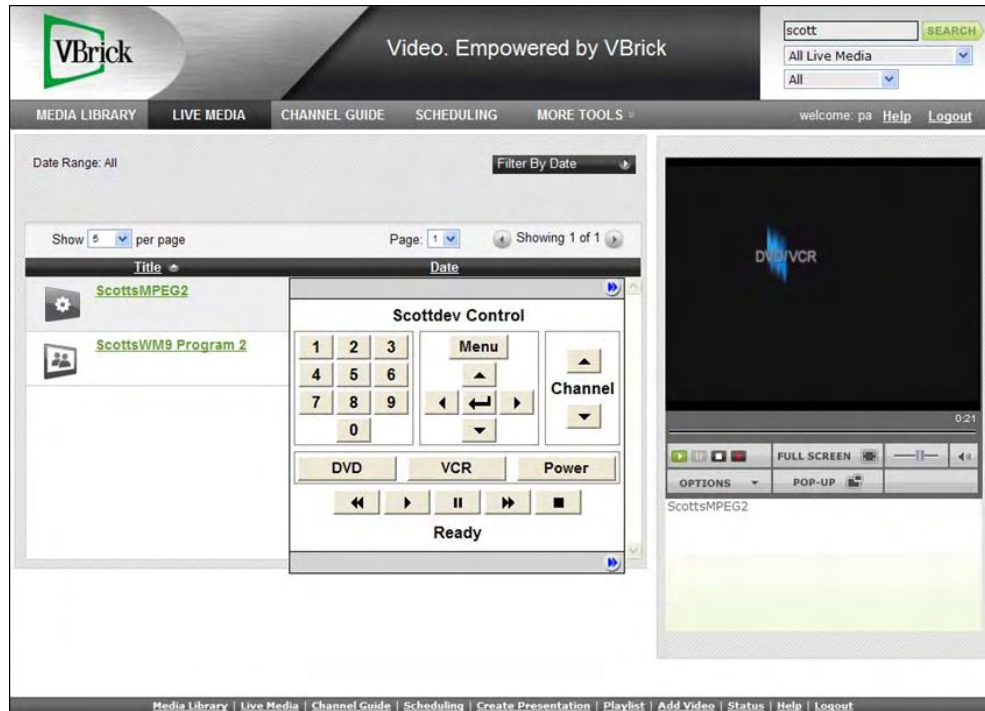
Figure 15. Virtual" Remote Control Panel on Live Media Page

As shown in Figure 16 below, the remote control panel will have a different graphical user interface depending on whether the source device is directly attached (via a serial port connection) or uses a VBIR. The control panel interface for direct-connect devices varies according to the specific device you select; the control panel interface for VBIR-connected devices is the same for all VBIR devices (unless manually changed as in Figure 17).
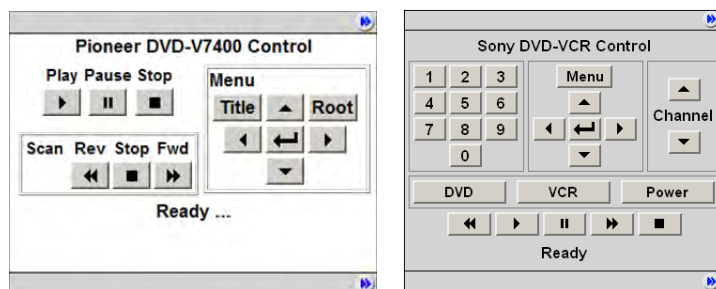
Figure 16. Control Panel for Direct-Connect Devices (left) and VBIR Devices (right)

Note The Amino set top box does not recognize "control devices." Any video source devices configured as **Control Devices** in the Portal Server will not display a "virtual" remote control panel on the Amino set top box.

Add Control Devices

Use the following windows to define or modify control devices. As noted, these devices will be displayed on the **Live Media** page with a special icon for any users with access to that encoder. *If the device is used as a source encoder for a scheduled broadcast, however, only the user who actually created the schedule will have access during the scheduled period.* This prevents other users from potentially interrupting the broadcast. If the Portal Server does not have a Scheduling license, all control devices are available at any time to any user with VBrick access and other permissions. See "Using the Scheduler" in the *Portal Server User Guide* for an explanation of how to schedule events for control devices.

▼   To define a control device:

1.   Go to **Global Settings > Control Devices** and select **Add Control Devices**.
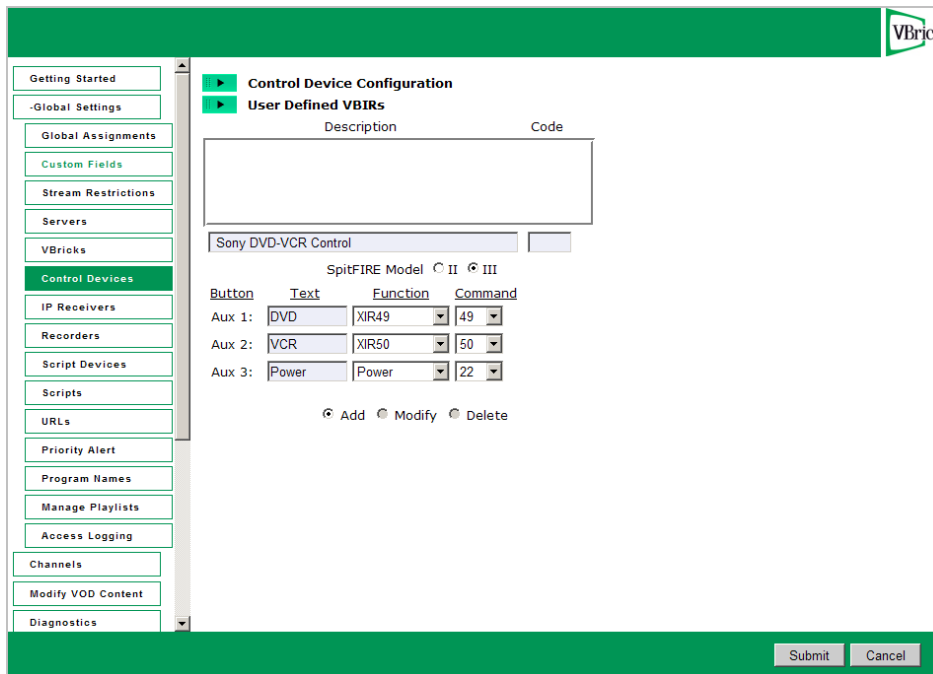
2.   Complete the fields on the next screen as explained below and click **Submit**.

Name	Enter a unique, descriptive name that will be displayed on the virtual remote. For example in Figure 15, "Sony DVD" is the configured name shown on the controller. No embedded spaces or special characters are allowed.
Device	Select a device from the dropdown list. The list shows serial port direct-connect devices and VBIR (SpitFire) commanded devices that are tested and supported by VBrick. It also shows any custom VBIR devices you have added. Creating User Defined VBIR custom devices is explained below. **You cannot create custom serial port direct-connect devices.** If the source device you wish to control does not have a serial port, you must use a VBIR for remote control.
Source	Select as the source either a VBrick encoder or a Live Video Stream URL (identified by URL) from the dropdown list. The Device that was selected above will be associated with the specified Source. Selecting a Live Video Stream URL requires that you specify an IP address and port. Enter these in the IP and Port fields that are displayed when you select a Live Video Stream URL.
User Defined VBIRs	Select the SpitFire version you have (SpitFire II or III) and enter a Description and a three-digit Code (see Add User-Defined VBIRs below).

Add User-Defined VBIRs

The VBrick VBIR is an external hardware device that uses the passthough port on a VBrick to send control commands *via an infrared link* to third-party devices like VCRs, DVDs, etc. (see Figure 18 for a visual schematic). You must use a VBIR if the target third-party device does not have a serial port that can directly connect to a VBrick encoder. The VBIR can be programmed with codes representing IR command sets that are compatible with devices from many manufacturers. Use the following window to create a custom **User Defined VBIR**. Enter a device description (20 characters or less), a three-digit code, and select the SpitFire model. When done, the new device is added to the **User Defined VBIRs** list as well as to the **Source Device** dropdown list. For a current list of VCR/ DVD device codes for SpitFire II models, go to http://innotech.com/spitfire-ii-device-codes.pdf For SpitFire III models, go to http://innotechsystems.com/Spitfire/SpitFire III.pdf Be aware that the device codes at this link are not tested or supported by VBrick. If you can't find the code you need, or have trouble controlling a non-supported device, check the product documentation or contact the manufacturer.

> **Note** The VBIR Model SpitFire III can be programmed to use IR commands much like a universal remote controller. These "learned" commands are stored in VBIR memory. See Update the VBIR Command Set on page 69 for details.

Adding a SpitFire Model III VBIR

The VBIR user interface on the Portal Server is designed for the Sony SLV-D380P DVD-VCR player (supported by VBrick). The default interface is shown on the left in Figure 17 but can be modified for use with other devices. You can add your own labels and functionality to the **Aux 1**, **Aux 2**, and **Aux 3** buttons as shown on the right in Figure 17.

© 2011 VBrick Systems, Inc.
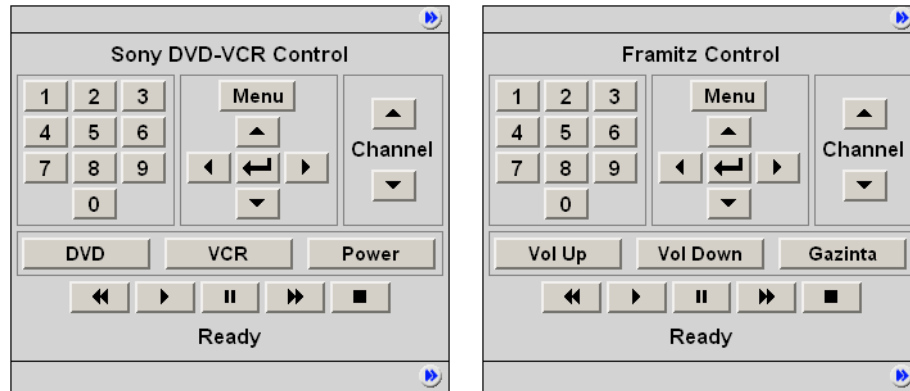
Figure 17. Modifying the SpitFire III Control Panel

In the default configuration there are three "auxiliary" buttons for toggling between **DVD** mode and **VCR** mode plus a **Power** button. The auxiliary buttons are configurable in that you can modify the button label and the associated instruction that will be sent to the VBIR. For example, suppose you want to support the Framitz device, and instead of buttons for DVD, VCR and Power, you want **Vol Up**, **Vol Down** and the special **Gazinta** function.

You can do this by selecting a SpitFire Model III. The auxiliary button definitions will initially display the default values (corresponding to the Sony SLV-D380P). You define the **Text**, **Function** and/or **Command** for each Aux button with an appropriate value—usually obtained in advance from the manufacturer. *It is the customer's responsibility to determine which functions and/or commands to specify for the buttons*. When done, The User Defined VBIR is saved and configured with a VBrick. The buttons will map properly and correctly perform the defined functions.

Connect Control Devices

To set up a device that can be remotely controlled from the Portal Server, you connect the serial interface on the source device (the DVD or VCR) to the passthrough port (COM1 or COM2 for Slots 1 and 2 respectively) on the VBrick encoder using an appropriate cable (see Table 11) from those shipped with the encoder. For more about Serial Port Passthrough, see the online help for the encoder. You can also control devices using VBrick's VBIR remote controller. To use the VBIR remote controller, you connect the VBIR SpitFire device to COM1 or COM2 on the VBrick encoder. The VBIR subsequently communicates with the DVD or VCR via infrared commands (see Figure 18) at the configured baud rate.

If necessary, connect one end of the XIR emitter cable to the SpitFire and the other to the DVD or VCR making sure the adhesive lead is securely attached to the device. The emitter is used when there is no direct line-of-sight to a control device (for example when the VCR is in a cabinet) and you can't use the remote control. On the back of the VBIR, be sure the SpitFire is in RS-232 mode.
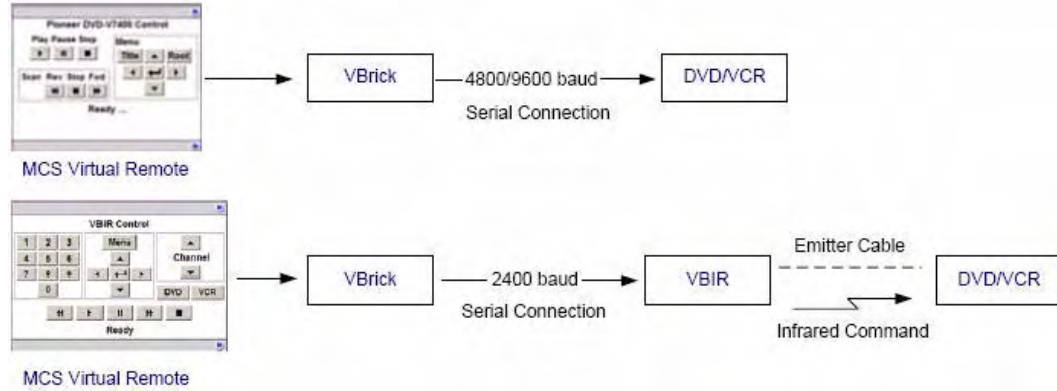
Figure 18. Connecting Control Devices

Table 11. Device Connectors

Device	Connector
VCR	DB-9 †
DVD	DB-15 †
MPEG-1 Encoder	DB-9
MPEG-2/4/WM Encoders	RJ-45

† Typical device connector.

Configure Control Devices

You also need to configure the baud rate and passthrough state of the VBrick associated with a control device. In VBAdmin, go to the **System Configuration > Advanced Configurations > Passthrough** page and set these values as follows:

Table 12. Baud Rate and Passthrough State

Device	Baud Rate	Passthrough State
DVD	4800	Responder
VCR	9600	Responder
VBIR	2400	Responder

Update the VBIR Command Set

VEMS Portal Server Control Devices use SpitFire model VBIRs to manipulate DVDs, VCRs or other devices controlled by IR commands. The VBIR contains an internal library of several hundred IR command sets stored in flash memory. The internal library is accessed by a three digit code. The VBIR internal library supports a wide range of devices from many, but not all, device manufacturers. If the IR command set for a particular device is not stored in the internal library there are two ways (as explained below) that the VBIR can be enhanced to control the device.

Learning IR Commands

The VBIR (Spitfire Model III only) can be set to learn and store IR commands like a universal remote controller. Learned commands are stored in VBIR memory areas called slots and are accessed by reserved three-digit codes. The six slots are available are: AUX (994), TV (995), VCR (996), DVD (997), AUD (998), and CBL/SAT (999). Once learned IR commands are stored on a VBIR they can be written as an external library file on a PC. The IR commands in an external library file can be learned by other VBIRs through the process of cloning. For more information, see the application note Learning IR Commands on the VBIR on the www.vbrick.com/documentation page.

Downloading External Libraries

The VBIR can be upgraded by downloading an external library file. External library files contain IR command sets for a specific device or devices. External library files are supplied by a third party or created using the SpitFire VBIR learning mode. For more information, see the application note Downloading External Libraries to the VBIR on the www.vbrick.com/documentation page.

Presentation Devices

VEMS supports two types of rich media presentations: (1) "encoder" presentations are sourced from VBrick encoders and support video and PowerPoint slides; and (2) "device" presentations are sourced from "presentation devices" you create with the Admin Console

and support video only. **Device presentations require a defined presentation device; encoder presentations do not.** This topic explains how to create Presentation Devices that are used with "device" presentations. See <u>Configuring for Presentations</u> on page 165 for detailed steps that explain how to configure both types of presentations. Once you have configured an encoder or a device for presentations, see the "Create Presentation" topic in the *Portal Server User Guide* for an explanation of how to actually create, schedule, and author live presentations from the client user interface.

A presentation device is simply a "virtual" entity that is used to display video from an external device using the VEMS presentation interface. It is used to create and publish presentations where the streaming video is sourced from any external viewing URL. For example this URL can be the stream from a VBrick Rich Media Studio (RMS), the stream from a Rich Media Desktop (RMD), or it can be the web page generated by a presentation device. There is no communication between VEMS and the presentation device but the device can be reserved (i.e. scheduled), and a presentation can be associated with the device, using the **Create Presentatio**n tool on the *client* user interface.

Presentation devices may also require user authentication. This means that when creating a presentation, you may not be able to access a Presentation Device if you don't have permission (see <u>Allow Presentation Device Access</u> on page 141 for more information). When creating a presentation from the client interface, as explained in the *User Guide*, you can choose a device, an encoder, or a reflector as the video source for the presentation. If you select a device as the source, you cannot download PowerPoint slides and the authoring page has limited functionality: you can basically edit, save, or author the presentation.

Host Name	Host Name used to identify the presentation device.
IP Address	IP Address used to identify the presentation device.
User Name	Unique user name associated with the device.
User Password	Unique password associated with the device.

Virtual Publishing Directory	Virtual directory where the recorded webinar and the slides are published. Default = `PDPresentations`. The files must be published to a unique subfolder (user-created by FTP or other means) inside the virtual directory.
Launch Browser for Viewing	Used when the Viewing URL for a presentation device is a web page rather than a video. If checked, the entire web page is displayed on the presentation page. If you are using <u>Zones</u> to direct Portal Server clients to specific servers, you may need to append a `refip` (reference IP address) parameter to the URL to identify a server that is outside the defined zones. See <u>Adding a Reference IP Address for URLs</u> on page 82 for details.
RMS Silverlight Presentation	If checked, the presentation will be played and viewed in the Silverlight Player. If not checked (default), the WM Player with VBrick plug-in will be used to render the presentation on a PC; the VBrick Player will be used to display presentation on a Macintosh.

Once you have defined the **Presentation Device**, use the **Advanced Configuration** page to define the parameters associated with the presentation device.

Slot 1 is a WM Slot	Read-only. Indicates you are defining all available Windows Media video Viewing URLs. Note that <u>Zones</u> logic will ensure that the connected client receives the correct viewing URL from the defined list. If you are using <u>Zones</u>, and have checked **Launch Browser for Viewing**, you may need to add a reference IP address to the URL. See <u>Adding a Reference IP Address for URLs</u> on page 82.

Slot 2 is an H264 Slot	Read-only. Indicates you are defining all available H.264 video Viewing URLs. Note that <u>Zones</u> logic will ensure that the connected client receives the correct viewing URL from the defined list. If you are using <u>Zones,</u> and have checked **Launch Browser for Viewing**, you may need to add a reference IP address to the URL. See <u>Adding a Reference IP Address for URLs</u> on page 82.
Include CC and Meta data	Not used. Do not check.
Description	Text field used for descriptive text.
E-Mail Template	This field adds the specified text to an auto-generated e-mail sent to presentation *authors*. Sometimes used with custom applications to add additional information or instructions.
Add Viewing URL	This URL defines all of the available viewing URLs for the video source or web page. Use any valid viewing URL for Windows Media or H.264 streams (see <u>Valid URL Examples</u> on page 83 for more information). To see this field, you must first click **Add Viewing URL**. You will subsequently need to click **Edit** and **Apply** when making changes. • RMS – If using RMS it will be a WM stream from a Windows Media server or a reflector. • RMD – If using RMD it will be the WM or H.264 stream from the available video source. • WM – enter a fully-qualified path to the Windows Media Server and Publishing Point that will be hosting the video. For example: `http://www.WM_Server_IP_Address/Publishing_Point` • Silverlight – same as WM above. Enter a fully-qualified path to the Windows Media Server and Publishing Point that will be hosting the video. Note: When viewing Silverlight presentations on a Macintosh client, at least one unicast viewing URL is required. • H.246 – See <u>Valid URL Examples</u> on page 83. Note: If you are using <u>Zones,</u> and have checked **Launch Browser for Viewing**, you may need to add a reference IP address to the URL. See <u>Adding a Reference IP Address for URLs</u> on page 82.

IP Receivers

Digital IP Receivers (also called STBs or Set Top Boxes) must be configured in VEMS Portal Server before they can be managed and used for scheduled events. (IP Receiver version must also be 3.7.1 or higher.) Once configured, all IP Receivers in the system are shown on the following window. The **Select IPR** panel in the next screen shows IPRs that have announced their presence on the network but have not been configured for use in the Portal Server.

▼   To add an IPR configuration:

1.   Go to **Global Settings > IP Receivers**.

2. Select **Add IPRs** and click **Submit**.

3. In **Select IPR**, select one or more existing IPR for which a SAP has been received. This populates the **IPR Configuration** panel. (If you select multiple IPRs, it does not populate the panel; if you need to configure the IPRs, you must add them one at a time.)

4. Complete or modify the fields in **IPR Configuration** as necessary and click **Submit**. This adds the new configuration to the list of configured IPRs shown on the previous page.

Note The only time you will manually complete the IPR Configuration fields is when you are defining the configuration for an IPR that will be added to the network at a later time. In this case, you will need to know the configuration data in advance.

Host Name	Required. Host name of IPR.
IP Address	Required. IP address of IPR.
User Name	Defaults to system-defined value if blank.
User Password	Defaults to system-defined value if blank.
Confirm Password	Defaults to system-defined value if blank. Must match User Password if entered above.
Software Revision	Optional.
IPR Model	Select from the dropdown.
Start Mode	Select from the dropdown: VEMS | Local | Local-Fullscreen

Configuring IP Receiver Timeout

Digital IP Receivers time out by default every two hours and display a popup message. This means that if a video exceeding two hours is playing and you do not interact with the system, the video will stop, the STB will display a popup message, and you will be redirected to the login page. The configurable timeout option described here lets you set the timeout interval to a higher value so a video can play all day for example without timing out. The STB requires a periodic timeout for cleanup but you can set the timeout value to a high number to minimize the potential disruption caused by timeouts.

Note The only requirement in configuring a timeout value is that the SDK timeout (configured in `VBUServer.exe.config`) must be set to a greater value than `SessionIPRTimeOut` (configured in `web.config`).

As explained below, you can configure the timeout interval on Digital IP Receivers (STBs) by changing two configuration values in the Portal Server installation files. One value is in `web.config`; the other is in `VBUService.exe.config`.

▼ To modify the STB timeout value:

1. Navigate to `<InstallDir>\Vbrick\MCS\`**`web.config`**

2. Find the key called `SessionTimeOutIPR` and set this value to the desired timeout. This value is in minutes, so if you want the STB to timeout every 8 hours, you would set this value to 480.

3. Go to `<InstallDir>\Vbrick\MCS\Common\VBUService\`**`VBUService.exe.config`**

4. Find the key called `MCSSDKTimeout` that handles SDK timeouts and make this value greater than the value set for `SessionTimeOutIPR`. This value is in milliseconds, so if you have set the `SessionTimeOutIPR` to 480 (8 hours), you would set the `MCSSDKTimeout` to 30600000 milliseconds (8.5 hours).

5. After making these changes, reboot the Portal Server and you are done.

Recorders

A Recorder server enables recording by Portal Server users. If a recorder server is not created here, any attempt to record a live stream or a stored video will fail. Once enabled, users must also be assigned the appropriate permissions (see <u>Allow Content Recording</u> on page 140). (Note: Do not confuse a Recorder server with a Network Video Recorder which is a a

separate product. See the *VEMS Network Video Recorder Release Notes* for more information.)

Note By installation default, all recordings are stored on the D: drive. If you install VEMS Portal Server on a system without a D: drive, you must subsequently go to **Global Settings > Recorders** and change the record path as necessary. Also, the **Max Recording** field shows the default number of concurrent recording sessions allowed. *If you need more than 2 concurrent recording sessions, you must purchase a Network Video Recorder.*

▼   To add a Recorder configuration:

1.   Go to **Global Settings > Recorders**.

2.   Select **Add Recorders** and click **Submit**.
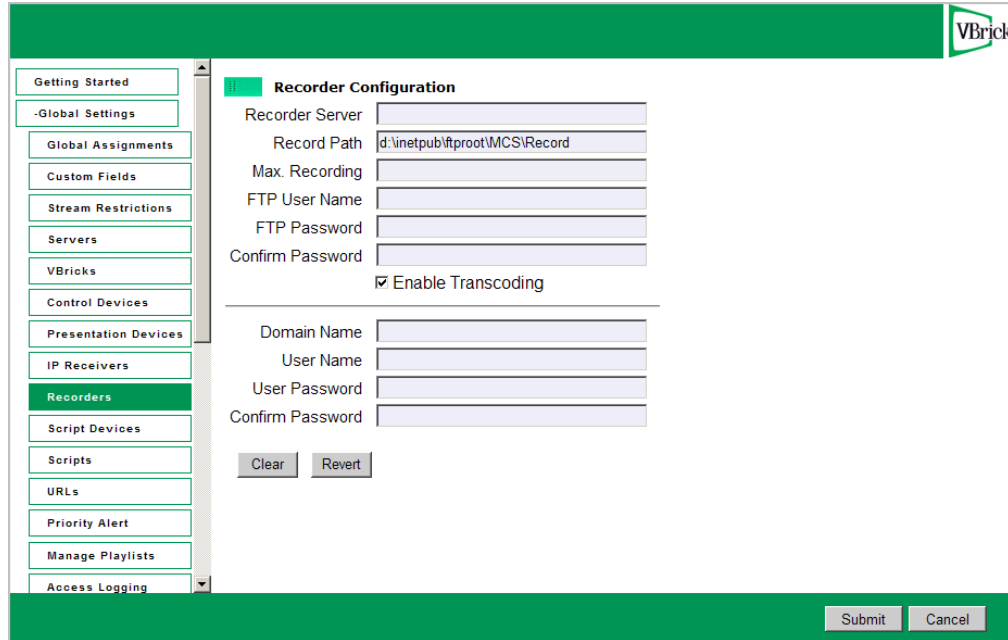
3. Complete the fields in **Recorder Configuration** window and click **Submit**. This adds the newly configured recorder to the previous window. If necessary see <u>Synchronizing the Portal Server and the NVR</u> below.

Recorder Server	IP address or host name of recorder server. Defaults to localhost if recorder server is on the same machine as VEMS Portal Server.
Record Path	Path and folder where all recording are stored. By default, recordings are stored on the D: drive. If you install VEMS Portal Server on a system without a D: drive, you must change the path. Also, in order to record multiple streams, the Record Path must be under FTP root. For example, if root is `C:\Inetpub\ftproot` the Record Path must be `C:\Inetpub\ftproot\<your_folder>`
Max. Recording	The default number of concurrent recording sessions allowed is 2. If you exceed 2, you must purchase a Network Video Recorder. Without an NVR, any attempt to record more than 2 concurrent sessions will fail.
FTP User Name	FTP user name in operating system of Recorder server.
FTP Password	FTP password in operating system of Recorder server.
Confirm Password	FTP password in operating system of Recorder server.
Domain Name	*This field is required only if the Recorder server is not on the local network.* Enter the domain name if the Record Path above points to a server in a different domain,
User Name	The user name who has access to the specified path.
User Password	The corresponding password for this user name.

Synchronizing the Portal Server and the NVR

The internal clocks on the Portal Server and the NVR must be synchronized for recording functionality to work properly. You can use the `Net time` command as explained below or you can use an external time server. In order to run the `Net time` command on *either* server, the server must be on the domain, and the user logged onto the server must have admin privileges *and* be part of the domain. To synchronize the Portal Server and the NVR use the following command:

- Windows Web Server 2008 – Open a command prompt on the *Portal Server* and type:
  `Net time \\{NVR IP Address} /SET`

Script Devices

Script devices work with scripts and can be used to control VBricks, or other devices attached to a VBrick via the serial port. In order to use a script, the device (a VBrick, IP Receiver, camera, VCR, etc.) must be defined in the Portal Server database as a script device. Once defined, they can be subsequently controlled by a script (see Scripts on page 78) launched from the Portal Server Scheduler. A script device must be physically connected to the network and must be available at the runtime of a scheduled event. For example, PTZ cameras respond to pan, tilt, and zoom commands. Once defined as a script device, pan, zoom, and tilt commands can be scripted and executed from VEMS Portal Server to control the movement of the camera at a specific date, time, and recurrence.

Note You can also write a script (launched from the Portal Server) that uses TCP/IP to communicate with any compatible device on the network. Contact VBrick Support Services for more information.

▼ To add a Script Device configuration:

1. Go to **Global Settings > Script Devices**.

2. Select **Add Script Devices** and click **Submit**.
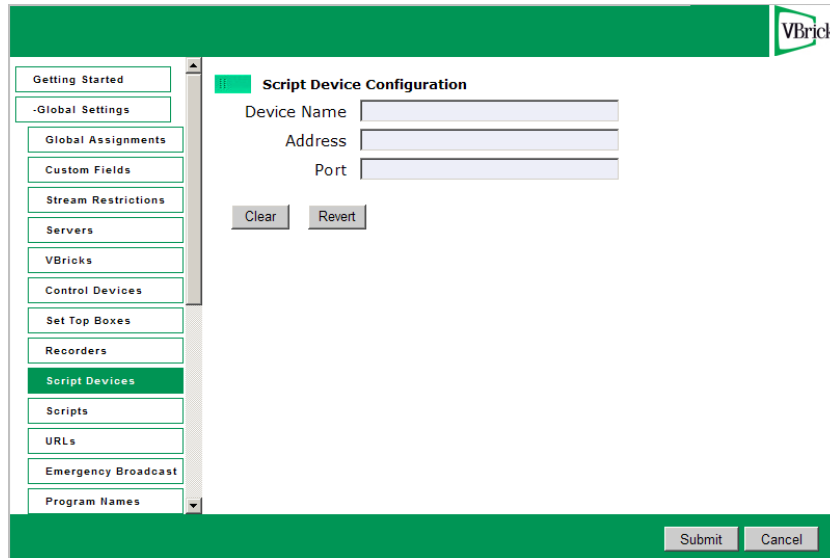
3. In **Script Device Configuration**, complete the following fields and click **Submit**. This adds the newly configured script device to the list of devices shown in the previous window. To modify a Script Device, first delete the device and then repeat these steps.

Device Name	Any user-defined name.
Address	Hard-coded device IP address. This is usually the address of the VBrick or the address of the VBrick to which a device is connected but it can be the address of any device.
Port	TCP/IP port number range = 1040–65534. If using serial port passthrough, use the VBrick's passthrough port number: 4439 for COM1, 4414 for COM2

Scripts

Scripts work with previously defined script devices such as VBricks, IP Receivers, or other devices attached to a VBrick. Scripts can be used to control any type of VBrick or to control other devices like cameras and VCRs that are attached to a VBrick. To script VBrick commands, you select the VBrick and build a script by choosing parameters from a dropdown list—the parameters vary depending on the type of VBrick you select (MPEG1, MPEG2, etc.). You can script commands to change any of the parameters (in the MIB database) that are available through IWS (MPEG and WM) or VBAdmin (H.264).

For non-VBrick (**Other**) devices, you write a script from scratch using the native language for that device. This scripting functionality is designed for advanced users and you must know the instruction set for the device in order to script commands that will control that device. You can use a text-based script or a binary script to control devices connected to the serial passthrough port (COM1 or COM2) on a VBrick encoder.
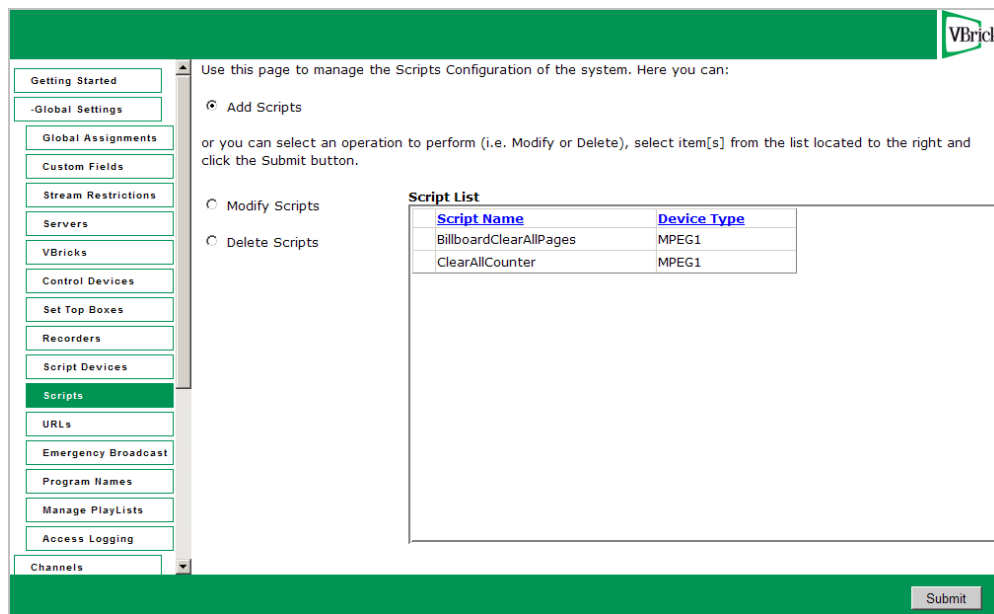
You can control devices that require binary input by pasting binary input into the **Script Content** text box. Binary scripts let you provide a sequence of commands for devices that require binary input. This type of script will pass binary input through the serial passthrough port on a VBrick to the specified device. You will typically connect your device to the serial passthrough port using the port number previously defined for the device (4439 for COM1, 4414 for COM2).

Note If you are scheduling an event, any device for which you write a script must be available to the network at runtime. If the device is not available the script will fail.

Creating a Script

▼ To create a script that can be executed from the Portal Server:

1. Go to **Global Settings > Scripts**.
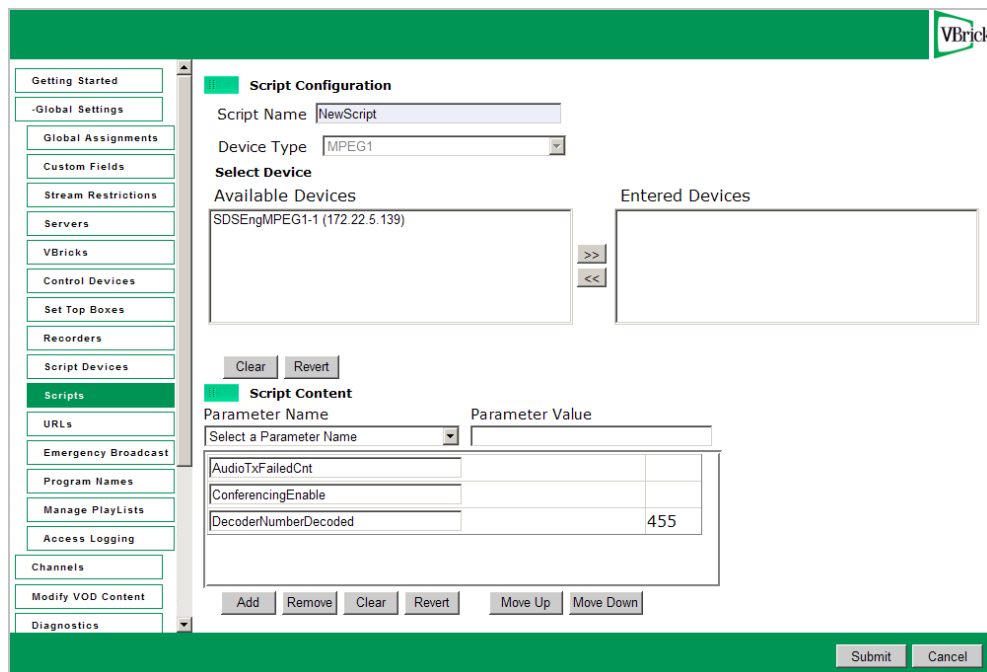
2. Select **Add Scripts** and click **Submit**.

3. In **Script Configuration**, enter a **Script Name** and select a **Device Type** (MPEG1, MPEG2/MPEG4/WM, H.264, or Other) from the dropdown list—and wait a few seconds for VEMS Portal Server to populate the panel with a list of devices.

4. In **Select Device**, highlight one or more devices and use the arrow buttons to populate the right panel.

5. Create the **Script Content**.

    a. For VBrick devices, select a **Parameter Name** from the dropdown list, enter a **Parameter Value**, and click **Add**. Repeat as many times as necessary and click **Submit** when done. Note that the order in which you add parameters is critical. This is the order in which the commands will be executed at runtime. (See <u>Finding VBrick Parameters and Values</u> for more information.

    b. For non-VBrick (**Other**) devices, write the script in a native language compatible with the device (or copy and paste binary input) and click **Submit** when done.

To run a previously created script, login to VEMS Portal Server and click **Scheduled Programs**. Then create a schedule by selecting a date, time, and (optionally) a recurrence pattern. When done, click **Script** and select the script you want to run on the schedule you just defined.

Example

The following example shows binary input for a VBrick VBIR device. In a typical scenario you will need to set the **Passthrough State** and other parameters on the encoder before you can run the script. See "Serial Port Passthrough" in the *VB4000-5000-6000 Admin Guide* for more information. The following example programs a VBrick VBIR device to device code 351 and sends the Play command. This is just a brief example. If you need help or want more information about using binary scripts, please contact VBrick <u>Support Services</u>.

Begin instruction set, program for following device code. This set of instructions is used in all scripts.

```
<-script->
<-send binary 0xc1 0x0d->
<-receive 2->
<-send binary 0xc0 0x0d->
<-receive 2->
```

Program three-digit device code. Here code is 351.

```
<-send binary 0x83 0x0d->
<-receive 2->
<-send binary 0x85 0x0d->
<-receive 2->
<-send binary 0x81 0x0d->
<-receive 2->
```

End device code programming, set for command. This set of instructions is used in all scripts.

```
<-send binary 0xc0 0x0d->
<-receive 2->
<-send binary 0xd3 0x0d->
<-receive 2->
```

Command. Here Play.

```
<-send binary 0x91 0x0d->
```

```
<-receive 2->
```

Finding VBrick Parameters and Values

In order to create scripts, you need to determine the correct parameters and values to use. The following procedures explain how to locate parameters from the VBAdmin page and how to find the value associated with that parameter using a standard MIB browser or text editor. These brief procedures simply outline the basic steps which are typically performed by a programmer or a system administrator. Contact VBrick Customer Service or see the *VBrick SDK User Guide* for more information.

▼ To locate a parameter name by viewing the source code:

1. Find the **Parameter Name** in the VBAdmin page.
2. Then locate the parameter name by viewing the source code of the page.

▼ To find the parameter value:

1. Locate the parameter name as described above.
2. Find the **Parameter Value** by examining the MIB file with either a standard MIB browser or a text editor.

URLs

Add/Modify a URL for a Live Video Stream

Administrators can manually enter URLs to live video streams that are not automatically displayed by the Portal Server. For example, the administrator may wish to have the Announcements (SAPs) disabled on the VBrick encoders for security purposes. Or the Administrator may want to enter the address of an off-network stream such as an MPEG-4 Stream from an Apple Darwin Server or a stream coming from a hosting provider. Additionally, this feature lets you enter the addresses of non-MPEG streams such as Windows Media and Real Networks. Note that the Access Control feature <u>Allow Viewing by Content Type</u> does not apply to manually added URLs. You can also filter and control which live streams are shown in the Portal Server by using a bit mask on the VBrick encoder. For more about this feature, refer to the Category parameter in the appropriate MPEG, WM, or H.264 encoder documentation.

Note   For any non-MPEG video, the correct player (such as Windows Media Player or QuickTime) must be present on the desktop for the client to be able to receive the stream.

▼ To add a URL for a live video stream:

1. Enter the URL or IP address in the **URL** field.
2. Enter the **Type** and **Title** and click **Add** to add the URL to the list of streams shown.
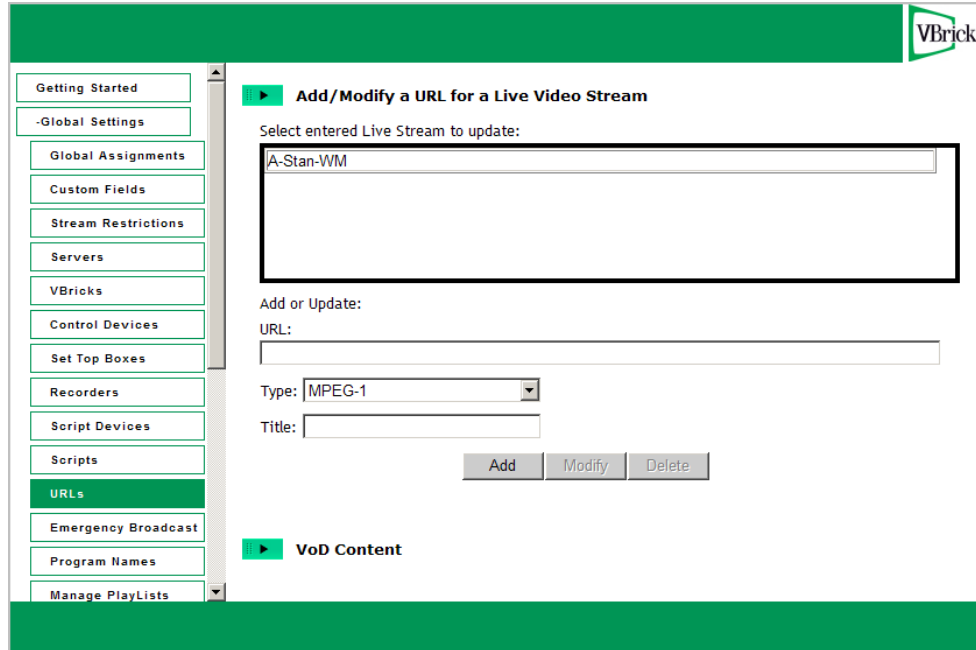
URL	Enter a valid URL or IP address. See examples below.
Type	Choose MPEG, WM, H.264, or Other. Select Other for most non-MPEG streams; select WM for .swf Flash streams.
Title	Title is what will display to clients in the VEMS Portal Server viewing pages.

Adding a Reference IP Address for URLs

When using **Zones** to direct Portal Server clients to specific servers, you may need to append a `refip` (reference IP address) parameter to the URL to identify a server that is outside the defined zones or uses a hostname exclusively. A `refip` may be necessary when (1) entering **Viewing URLs** for presentations that use Multimedia VBricks or Presentation Devices or (2) when manually entering URLs for live or stored streams. In a common scenario, a `refip` is required when users will need to fetch an sdp, nsc, or asx file from a web server, and where the file points to a video stream which will be accessed by users who are outside the zone identified by the server's IP address. A `refip` is also used in cases where the stream URL is identified by a host name. The `refip` parameter identifies the zone for the viewing URL; it can be any arbitrary address within the zone. When entering a live multicast URL, the `refip` parameter is always required even if you are not using zones. *The refip parameter is not necessary when the IP address of the URL itself can be identified as being in the zone.*

Format: `<valid_url_format>&refip=<IP_Address_of_Stream_Source>`

Example: `http://www.mycompany.com/multicast/file.asx&refip=192.99.999.999`

Note   To be displayed on the **Live Media** page, manually entered <u>URLs</u> for live streams must be appended with an `refip` tag if the stream source is not defined in the URL.

Valid URL Examples

The following examples show valid URL syntax for live video streams. All URLs are case sensitive and the syntax must be accurate because there is no internal validation of user input.

Stream Type	URL Syntax
MPEG-2	`vbricksys://ip=239.1.1.1&port=4444&refip=192.99.999.999` Where `239.1.1.1` is the multicast IP address and `4444` is the multicast port.

MPEG-4	`rtsp://172.1.1.1/vbrickvideo1`
	
	`vbrtsp://172.1.1.1/vbrickvideo1`
	
	Where `172.1.1.1` is the source IP address and `vbrickvideo1` is the program name.
	
	`vbhttp://172.1.1.1/vbs2d1.sdp`
	
	Where `172.1.1.1` is the source IP address and `vbs2d1.sdp` is the SDP file name.

WM	`http://172.22.2.147/vbs1http.asx`
	
	`http://172.22.2.147/vbrickvideo1`
	
	Where `172.22.2.147` is the source IP address and `vbrickvideo1` is the program name. *Note that the WM IPR does not support RTSP streams.*

H.264	<u>RTSP Streams</u>
	`vbrtsp2://172.1.1.1/vbStream1S1`
	
	Where `172.1.1.1` is the source IP address and `vbStream1S1` is the resource name.
	
	`vbhttp://172.1.1.1/vbStream1T1.sdp`
	
	Where `172.1.1.1` is the source IP address and `vbStream1T1.sdp` is the SDP file name.
	
	<u>Multicast Transport Streams</u>
	`vbricksys://`
	`ip=<multicast_ip_address>&port=<multicast_port>&license=http`
	`://<vems_server_ip_address>/licenses/playerlicense/`
	`CombinedLicensedUser.lic&refip=<encoder_ip_address>`

Flash	`rtmp://VOD/publishingpoint/file.flv`
	`rtmp://172.22.2.97/vod/sample1.flv`
	`rtmp://172.22.2.97/vod/mp4:sample2.f4v`
	`rtmp://172.22.2.97/vod/mp4:sample3.mp4`
	`rtmp://172.22.2.161/vod/folder1/folder1_2/mp4:sample4.m4v`
	`http://172.22.2.97/vod/sample5.flv`
	`http://172.22.2.97/vod/sample6.f4v`
	`http://172.22.2.97/vod/sample7.mp4`

Stream Type	URL Syntax

Other	ASX Files
	
	`http://172.1.1.1/file.asx`
	
	`http://myHost/file.asx`
	
	`http://www.myCompany.com/files/file.asx`
	
	MP3 and WMA Files
	
	`http://172.1.1.1/file.mp3`
	
	`http://myHost/file.mp3`
	
	`http://172.1.1.1/file.wma`
	
	`http://myHost/file.wma`
	
	WMV Files
	
	`http://www.myCompany.com/files/file.wmv`
	
	`mms://www.myCompany.com/files/file.wmv`

Add VOD Content

Administrators can manually enter URLs to VOD content that is not automatically displayed by the Portal Server. These URLs can be to content that is located on a non-NXG Video-on-Demand server, such as the QuickTime/Darwin server, a Windows Media server, or a Helix Real server. This is valuable feature if you want to enter an off-network stream such as an MPEG-4 Stream from an Apple Darwin Server or if there is Windows Media or Real Networks content that needs to be displayed through the Portal Server interface.

URL	Enter a valid URL or IP address. For example:
	
	`rtsp://ipaddress/programname`
	`mms://ipaddress/videoname.wmv`

© 2011 VBrick Systems, Inc.

Type	Choose MPEG-1, MPEG-2, MPEG-4, MPEG-4 NXG, Document, WM, H.264, or Other. If you are creating a URL for stored video that points to www.yahoo.com, for example, select Document in this field—not Other. Select WM for .swf Flash streams.
Title	This is what will display to clients in the VEMS Portal Server viewing pages
Folder	This is the folder on the VOD server in which the video will be displayed.
Tags	Enter keyword tags that can be searched from the user interface.
Max. Concurrent Viewers	Set the maximum number of concurrent viewers for this stream to unlimited or any number greater than zero.

Press **Add** to add the VOD content to the list. VOD content also can be Modified or Deleted. Simply select the VOD content, make modifications (if required), and click **Modify** or **Delete**.

Add Non-VOD Content

PC Users Only. In the **VoD Content** section, administrators can also link to external documents such as PDF files, PowerPoint files, web pages, or anything that can be displayed in a browser or other external program. For content that needs to run with a specific application (for example, PowerPoint slides), the application must be present on the desktop for that file to be viewed. Use the content **Type** field to identify the content. Select a stream type (MPEG-1, MPEG-2, etc.) to add video content from an outside source. Select type **Document** for PDFs or Word documents, or type **Other** for PowerPoint presentations, Flash demos, etc. Each content type has a different icon on the **Video Library** page.

The URL must point to a web server or a local drive. The Portal Server server can act as the web server for this content, if the content is placed in the `c:\program files\vbrick\mcs` directory on the VEMS Portal Server (or in any subdirectory you create, e.g. `... mcs\test_files\test.doc`). A local path or network shared path also can be entered. Content accessed from a local drive (or network shared path) needs to be entered in the format `c:/path/file` (it will fail if you use back slashes, for example `c:\path\file`). Also, this drive needs to be accessible by those that have access to the link.

Priority Alert

These pages are used to create priority alert templates that Portal Server users can subsequently use to launch a priority alert. *Priority alerts are launched from the Portal Server user interface—not from the Admin console.* A priority alert is a schedule that can be executed by Portal Server users with appropriate permissions. This schedule broadcasts a live or stored video to specified VBricks or IP Receivers in case of an emergency. The schedule is executed instantly, for a specified duration or indefinitely. When done (or manually stopped) all preempted schedules automatically resume.

A priority alert template pre-defines all parameters for the broadcast so that it can be launched immediately; it pre-empts all other broadcasts. Very simply, you define the source stream (live or stored) and the downstream targets (VBricks or IP Receivers) and then save the template for future use. It is important to note that priority alert streams are shown only on monitors or TVs attached to VBricks and IPRs respectively. *They are not shown on the Portal*

Server user interface. If you are watching a stream in the embedded player on the user interface browser, you will not see a priority alert.

Note Live and stored broadcasts, in this context, refer to content that is being streamed over your IP multicast-enabled network. This does not mean there is IP broadcasting to your entire network.

▼   To create a Priority Alert template:

1. Close any Portal Server client window(s) open on your PC.

2. Go to **Global Settings > Priority Alert**. This page shows a list of previously defined templates (if any).
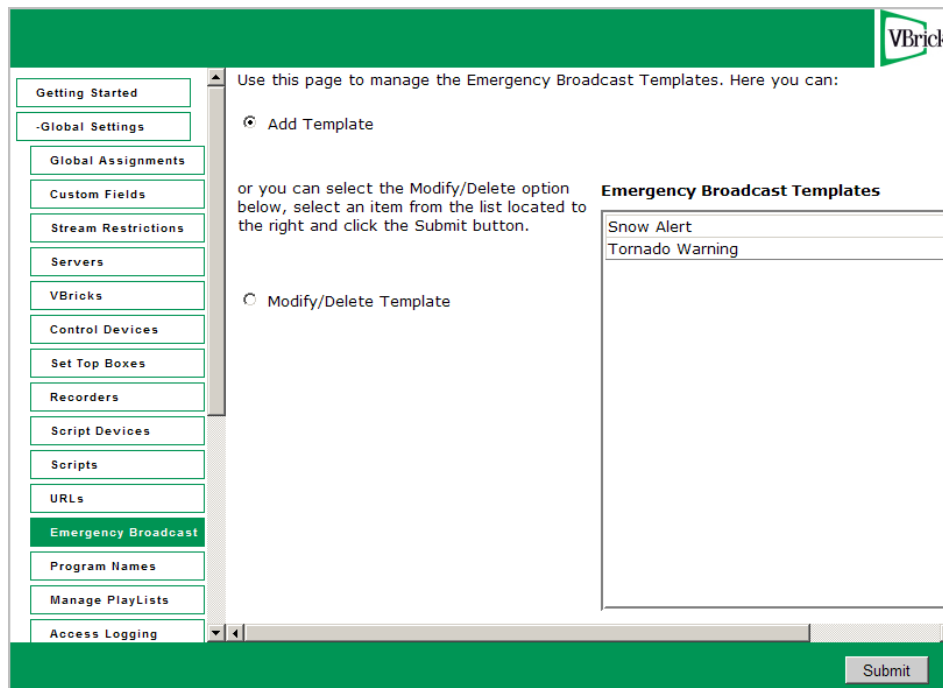
3. Select **Add Template** and click **Submit** to display the following window.
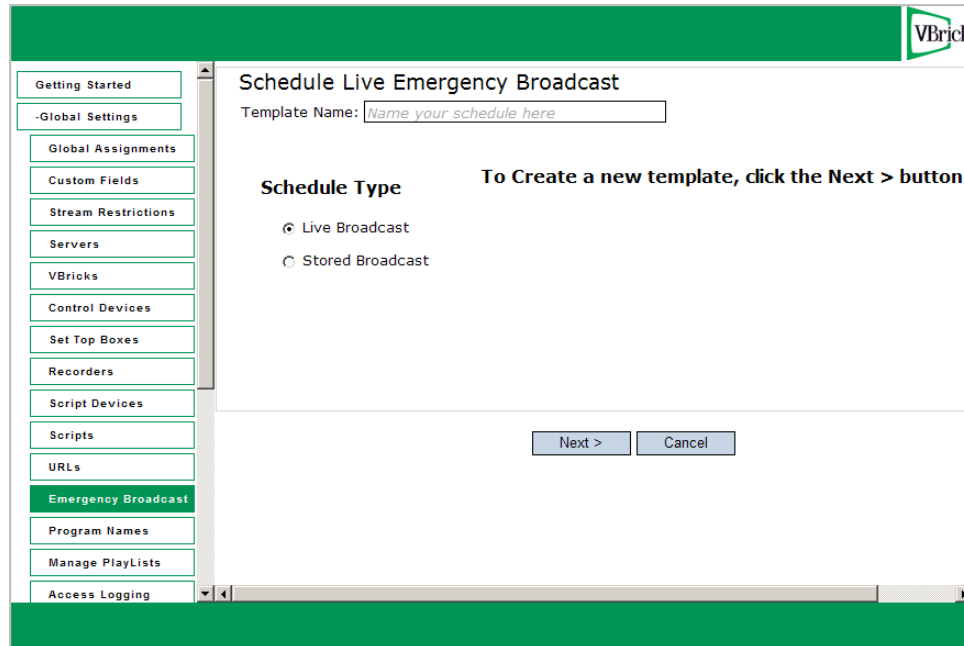
4. Enter a **Template Name**, select a **Schedule Type**, and click **Next**. (Duplicate template names are allowed but not recommended.)

   Each **Schedule Type** subsequently has a different wizard depending on the selections you make but basically, you select the video source (which can be a live or stored broadcast), the downstream targets (VBricks or IP Receivers) to which it will be broadcast, and configure any **Advanced Settings** (see note below) for the VBricks or IPRs. When done the template you created is available to authorized Portal Server users as a Priority Alert template. See the *VEMS Portal Server User Guide* for more information.

Note **Advanced Settings** are available to configure VBricks and IPRs with exceptional configuration parameters. It is unlikely you will ever need to change these settings. In all cases you can safely ignore the **Advanced Settings** and use the defaults provided by VEMS Portal Server.

Template name	Alphanumeric characters or spaces. No special characters.
Schedule Type	<u>Live Broadcast</u> • VBrick – Select a live stream by VBrick Name. Then select the destination VBricks or IPRs. • Program Name – Select a live stream by Program Name from all available. Then select the destination IPRs. • Enter Manually – Select an MPEG or WM source residing at a specified IP address. Then select the destination IPRs.
	<u>Stored Broadcast</u> • VoD Name – Select a VOD server and a source video. Then select the destination VBricks or IPRs. • VBrick Name – Select a VBrick (or VBStar) and a source video. Then select the destination VBricks or IPRs.

5. Configure **Advanced Settings** for VBricks and IPRs as necessary. As noted, it is unlikely you will ever need to change these settings. In all cases you can safely ignore these settings and use the defaults provided by the Portal Server.

   These settings generally set configuration options for source devices and destination devices (VBricks and IPRs) so that they are configured properly (e.g. transmit/receive enabled/disabled) at the beginning and end of a priority alert. All required devices must be present and enabled for a successful priority alert. The settings differ depending on the device (e.g. MPEG, WM, or H.264) you select and may include some or all of the fields explained below.
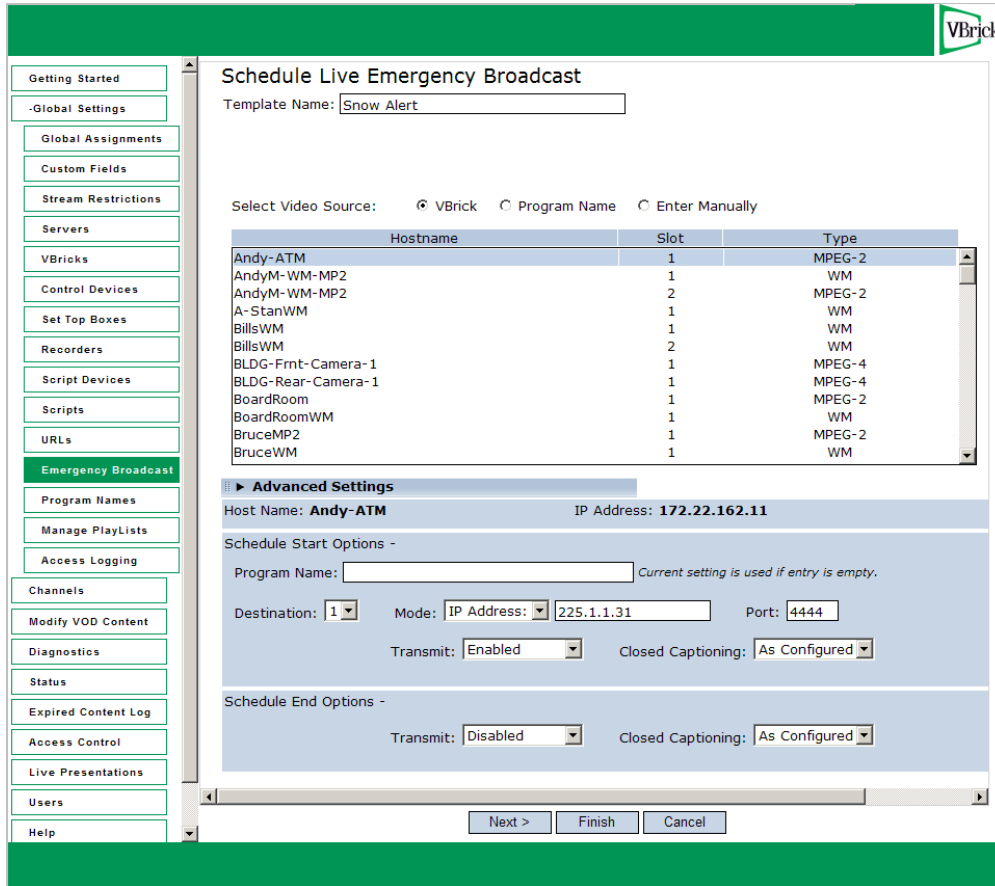
Schedule Start Options	Enter values that describe the device state at schedule start. • Program Name – Program name selected above. • Template – MPEG only. Screen varies for MPEG-1, 2, or 4. • Destination – Destination 1, Destination 2, RTSP Server. • Destination Address – Enter value. • Video Port – Enter value. • Audio Port – Enter value. • Closed Captioning Port – Enter value. • Video – Enabled, Disabled, As Configured. • Audio – Enabled, Disabled, As Configured. • Closed Captioning – Enabled, Disabled, As Configured.

Schedule End Options	Enter values that describe the device state at schedule end.
	• Video – Enabled, Disabled, As Configured.
	• Audio – Enabled, Disabled, As Configured.
	• Closed Captioning – Enabled, Disabled, As Configured.

6. Click **Next** to page through each wizard.

7. Click **Finish** when done.

8. Verify the information and click **Create Schedule** when prompted (or use the **Back** button to make changes). When finished, the template is added to the list of Priority Alert Templates available to VEMS Portal Server users from the Portal Server application. See the *VEMS Portal Server User Guide* for more information.
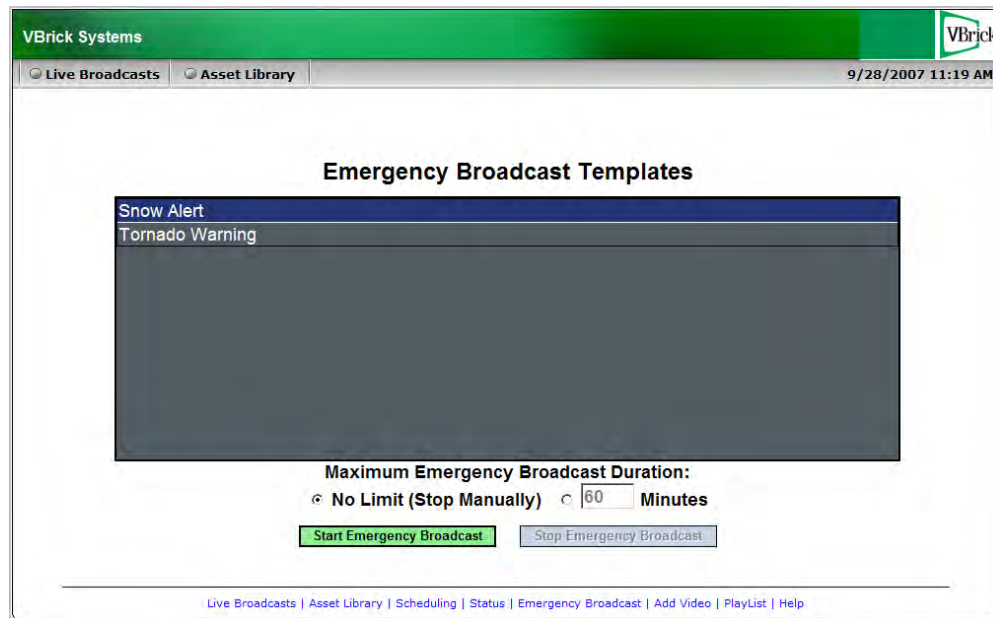
Manage Playlists

Use this window to change playlist attributes including **Folder**, **Title**, and **Owner**. If Access Control is not enabled, the owner for all playlists defaults to MCSClient. Note that if Access Control is subsequently enabled, any previously created playlists will not be available unless they are re-assigned from MCSClient to other valid users.
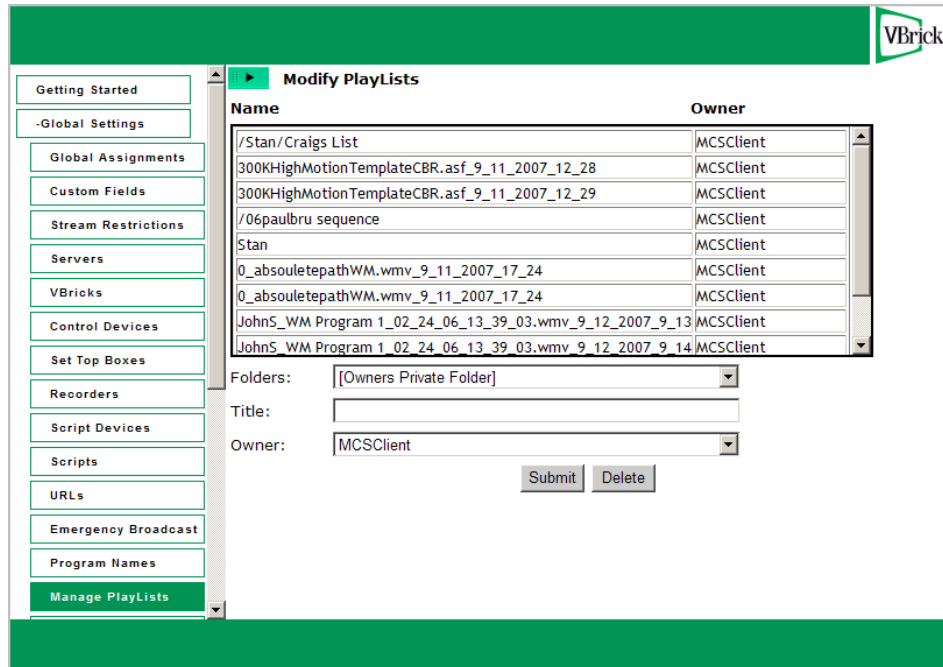
Folders	Select a folder location for the playlist. The default folder is the private `MyMedia` folder of the playlist owner.
Title	Use any alphanumeric characters *except* ' ^ : * ? | [ ] ( ) < > % #
Owner	The owner is the logged-in user who created the playlist.

Access Logging

Access logging tracks Portal Server usage. It creates logs that let you review who has watched what content, when, and for how long. Specifically, it logs access to live or VOD content, and to user-initiated recordings. **There are two output logs; one is used for live/VOD content and the other is for recordings.** The logs are created in a standard format and can be viewed with Enterprise Media System Reporter (VBrick's powerful log analysis tool or with a customized Excel spreadsheet. Use the various configuration options described below to save the logs to a different computer, set log time periods, etc. By default, access logging is set to off and the logs are saved in `Program Files\VBrick\MCS\Logs`. *Note that log entries are written to the log file only after viewing or recording is complete.* To see what is *currently* being viewed or recorded, open the Logged Programs table in VEMS using MySQL Query Browser or a similar tool. (MySQL Query Browser is available free of charge with the free software/open source GNU General Public License at http://www.mysql.com) Be aware that the access logger has certain constraints; for example, it:

- does not log web page access. This is an IIS function that can be set and controlled by system administrators.
- does not work with the Apple QuickTime player.
- does not have a built-in parser. The logs can be viewed as text files or can be managed and viewed using third-party reporting and analysis tools.

Enable Access Logging	Sets access logging on or off. Default = off. The log files are saved in `Program Files\VBrick\MCS\Logs`.
Log Cycle Time	New log files can be created daily, weekly, or when the file reaches a certain size. Old files are never deleted or written over.
Log File Directory	Specifies where the log files are saved. This can be on the same machine as the Portal Server or on a different machine in the same network.
Cycle Log File	Click **Cycle Now** to close the existing log files and create new files.
Logger Timeout Values	The timeout values (default two hours for stored content, four hours for live content) are typically used when a client machine crashes or hangs.

Using EthernetTV Reporter

You can use VBrick's powerful "Enterprise Media System Reporter" log analysis tool to examine the access logs. VEMS Reporter is a dedicated log file analysis tool. It reads individual log files generated by the Portal Server and generates a graphical statistical report based on the contents of the log data. Each log entry contains multiple fields, and VEMS Reporter extracts those field values from the log data and populates the report. VEMS Reporter is closely integrated with the Portal Server and has its own documentation. See the VEMS Reporter User Guide in the online help for more information. To launch EtherneTV Reporter, go to Start > All Programs > VBrick > EtherneTV Reporter.
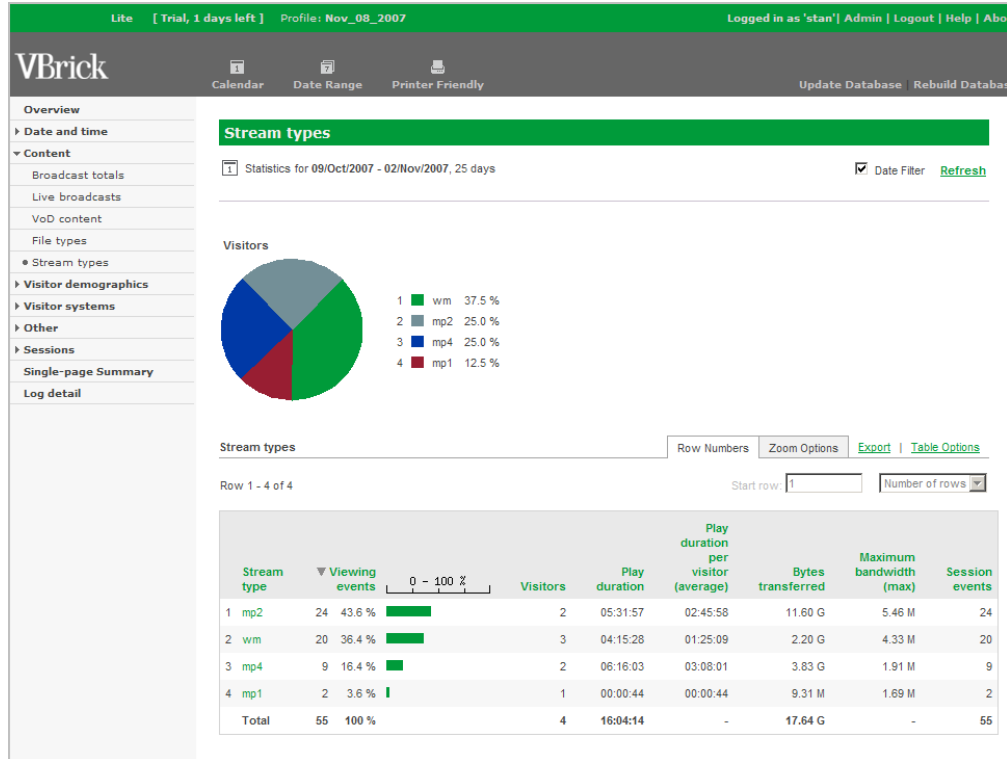
Figure 19. Sample Enterprise Media System Reporter Output

Using an Excel Spreadsheet

You can also use a standard editor like Notepad and the Excel spreadsheet template provided by VBrick to examine the logs. The `MCSS Access Log.xlt` template file makes to easy to view and sort log files. You can also use this template to build Pivot Tables to analyze the log data in greater detail. Pivot Tables are a powerful tool used to analyze multi-dimensional data. Pivot Tables are beyond the scope of this document and are not explained here. For an introduction to Pivot Tables, there are a variety of resources on the web including the Microsoft Office online demo at http://office.microsoft.com/en-us/assistance/HA011989031033.aspx

▼ To create a pivot table:

1. Navigate to `C:\Program Files\VBrick\MCS\Utils` and double-click `MCSS Access Log.xlt`
2. When prompted, select **Enable Macros**.
3. Click **Import Log(s)** and navigate to the log files in `Program Files\VBrick\MCS\Logs`
4. Select one or more log files by holding down the **Ctrl** or **Shift** keys while selecting files.
5. Once the window is populated with log data (Figure 20) you can view or sort any of the columns as necessary.
6. Click **Pivot Table Wizard** and follow the prompts to build a Pivot Table.

Figure 20. Imported Access Log

Zones

In a standard Portal Server configuration (with two zones), a client selecting a video is algorithmically directed to a load-balanced (Internet or LAN) server depending on the address ranges specified on the <u>Global Assignments</u> page (see "Assign LAN/Internet Address Range(s)." This is normal Portal Server behavior. The first two zones are configured in Global Assignments and the **Zones** page shown here is not used and is not even displayed. In a Professional or Enterprise configuration, the number of zones available for configuration depends on the licensing model (see Table 13) at your site. In a Professional or Enterprise model, the first two zones are also configured in Global Assignments and the next 10 or 100 zones (depending on what you purchased) are configured on the Zones page. You will only be able to configure the number of zones for which you are licensed.

The Zones page, *if shown*, directs Portal Server clients (or a range of clients) to *specific* servers (or a range of servers) within the address range(s) specified in Global Assignments. It associates each incoming network address with one or more server addresses. If using this page, you will typically create different named zones with different sets of client and server IP addresses. Note that if a client IP address is not included in the **Client Address(es)** list, that client is directed to the **Default Server/Encoder Address(es)**.

Table 13. Zones Licensing Models

Licensing Model	Zones Available
Standard	2
Professional	10
Enterprise	100

This page is also used to redirect clients when there is a server failure. The Portal Server polls all networked VOD servers at the polling interval specified in Global Settings. If the poll indicates a server failure, the specified Portal Server clients are automatically redirected to the failover server(s) only if the **Hide Content** option is checked on the **Assign VOD Polling Interval** page. *If unchecked, there will be no rollover to the specified default servers in the event of a server failure.*

Similarly, the Zones page is used to define Distribution Servers that are used to load-balance the distribution of .jpg images and HTML pages when delivering large-scale presentations (see the *Portal Server Release Notes* for more about installing and configuring Distribution Servers).
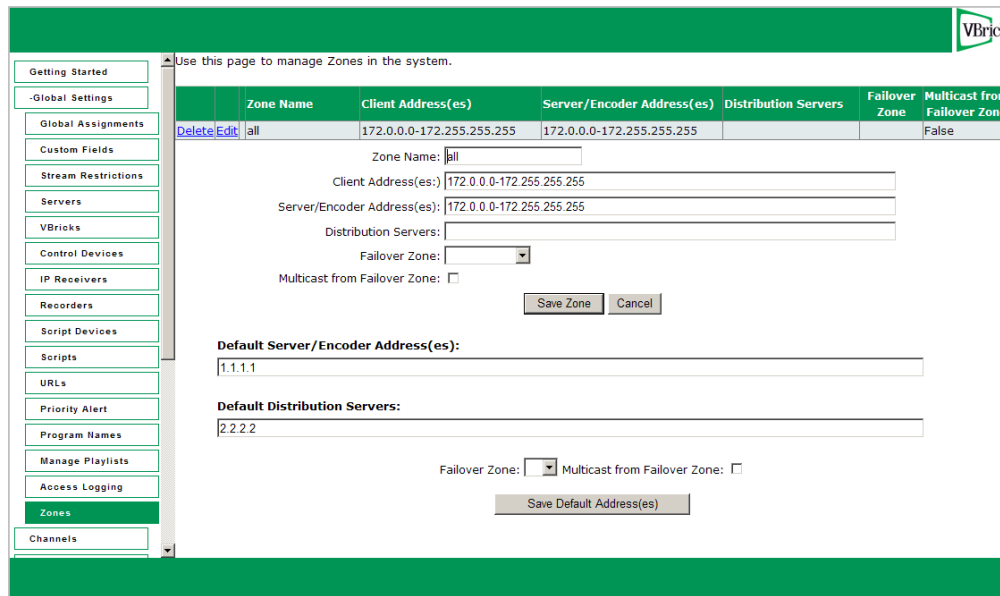
Zone Name	User-defined string that identifies the zone.
Client Address(es)	Enter individual, comma-separated client IP addresses and/or a range of client IP addresses. For example: **172.15.2.1**, **172.16.2.1-172.22.2.255**
Server/Encoder Address(es)	Enter individual, comma-separated server/encoder IP addresses and/or ranges of server/encoder IP addresses to which the specified client(s) will be directed.
Distribution Servers	Enter individual, comma-separated distribution server addresses to which a client will be directed for load-balanced presentations.
Failover Zone	If the requested content is not available locally or the local server is down, a content request will go to the defined Failover Zone (or to the Default Zone if selected).
Multicast from Failover Zone	Determines whether or not multicasting from the Failover Zone to clients is allowed if multicast content is available.
Save Zone	Saves zone information currently displayed in the upper panel.

Default Server/Encoder Address(es)	The server address(es) and/or range(s) to which a client is directed if the client IP address is not included in the **Client Address(es)** field. If the default address fails you can select a secondary Failover Zone (and a multicast setting) from the dropdown list of defined zones.
Default Distribution Servers	The distribution server address(es) to which a client will be directed for load-balanced presentations if the client IP address is not included in the **Client Address(es)** field.
Failover Zone	If the Default Address fails you can select a secondary Failover Zone (and multicast setting) from the dropdown list of zones.
Multicast from Failover Zone	Allow multicast from Failover Zone. Default = disabled.
Save Default Address(es)	Saves the default server information in the lower panel.

Configuring Zones

In a standard Portal Server configuration (with two zones), a client selecting a video is algorithmically directed to a load-balanced (Internet or LAN) server depending on the address ranges specified on the Global Assignments page. In a Professional or Enterprise model, the first two zones are also configured in Global Assignments and the remaining zones are configured here on the Zones page. When configuring zones, always take into account how the VEMS Server identifies a client. A client is identified to the Portal Server by its IP address. When WAN configurations are used, a network gateway can be entered as a Zone Client Address(es). This is because all clients in a network are viewed as this gateway address by an outside Host (for example the VEMS Portal Server).

Note   For Zones to work properly, manually entered URLs for live streams must be appended with an `refip` tag if the stream source is not defined in the URL.

Configuration Using Global Assignments

LAN and Internet Zones are defined on the Global Assignments page. Use these zones with a Standard VEMS Server.

LAN Zone Client	LAN Clients are allowed to view all content defined in the LAN address range and all Internet content which have addresses out of this range.
Internet Zone Client	Internet Clients are allowed to only view content not defined in the LAN address range.

Configuration Using Zones Page

Use the Zones page if you have a VEMS Professional or Enterprise Server. If you have a distributed environment with multiple independent LANs, you may not want to use the LAN/Internet Zones. Instead you can define the Internet Zone Address(es) using a separate Zone and enter all IP Addresses not defined in your other Zones. For example:

Zone 1 = Corporate Office Address Ranges
Zone 2 = Remote Office 1 Address Ranges

Zone 3 = Remote Office 2 Address Ranges
Zone 4 = Internet Zone (All IP's not in Zones 1–3)

If a Zone is defined and a default zone is not defined, clients inside the zone can only view content which is defined in the Zone range. Clients outside the zone can view all content available regardless of zone configuration. *If a Zone is defined and default zone is defined,* clients inside the zone can only view content which is defined in its Zone range. Clients outside the zone can only view content defined in Default Zone range.

Configuring Failover Zones

When a Zone is configured with a Failover Zone, the Zone's clients can view content from both its own zone <u>and</u> the failover zone. When the Zone's VOD server or encoder fails, clients will still have access to the failover zone's content. When configuring a Failover Zone that will reference NATed address(es), it is best practice to create a separate zone for the same client addresses which will be designated as another Zone's failover. In order for content to be available to a client the NATed address it must be entered in the client's Zone. But if a NATed failover VOD and primary VOD are both in the same zone the content will load balance to all clients in the zone. Therefore a separate zone should be created specifically for NATed failover addresses.

Configuring VOD Servers

When a VOD Server IP is defined in a Zone, all VOD Content from this server is available to the Zone's clients. All Scheduled Multicasts (via VEMS Scheduler page) from Zone's VOD will be available to Zone's clients.

Configuring Encoders, Viewing URLs, and Manual URLs

When an encoder IP is defined in a Zone, all enabled SAPs from this encoder are available to the Zone's clients with the exception of the encoder's External SAP. If the External SAP is configured, the URL IP entered in the External SAP will determine what Zone the SAP is directed to. The IP of the External SAP URL will have to be in the same IP Address Range of the Zone's assigned Server/Encoder Address(es) in order for the Zone's clients to view the video stream. When an encoder is used for Presentation feature (Multimedia VBrick), the encoder's Viewing URLs IP will determine what Zone the Viewing URL is directed to. The IP of the Viewing URL must be in the same IP Address Range of the Zone's assigned Server/Encoder Address(es) in order for the Zone's Clients to view the Presentations video stream. When a manual Live Video Stream URL is used (defined in VEMS Global Settings), the URL's IP address will determine what Zone the Viewing URL is directed to. The IP of the URL will have to be in the same IP Address Range of the Zone's assigned Server/ Encoder Address(es) in order for the Zone's clients to view the video stream.

Configuring Distribution Servers

If you are defining a Distribution Server for a Zone, the clients inside zone are directed to Presentation content from the Distribution Server(s) defined in its Zone range. Note: This is only true when using Presentation e-mail link to view a Presentation. *If you are defining a Distribution Server for the Default Zone,* all Clients outside defined zones are directed to Presentation content from the Distribution Server(s) defined in the Default Distribution Server range. Note: This is only true when using Presentation e-mail link to view a Presentation.

Transcode Templates

The VEMS transcoder is a tool that can be used with a Network Video Recorder (NVR) to "transcode" certain files to H.264 or Windows Media format. For example you may want to transcode all of your Windows Media files to H.264 files (or vice versa) or you may want downscale large MPEG-2 files to smaller Windows Media files. The use cases for the transcoder depend on the requirements and technologies available at your site. The **Transcode Templates** page is a licensed feature used to manage the preconfigured templates that are used for trancoding. If the Transcoding license is not installed, you will not see this feature in the Admin Console and the transcoding options will not be available on the **Add Video** page (Figure 21).

A Network Video Recorder (NVR) running on Windows Server 2008 is required for transcoding. Transcoding is computationally-intensive and runs on the NVR server. If multiple NVRs are present, the transcoding is algorithmically load-balanced. If no NVR is present, or if transcoding is not enabled on the NVR's Recorder Configuration page, the feature will not be available. When adding files to a VOD server from the **Add Video** page, you can select an **Output Format** (H.264 or Windows Media) and an encoding template with preconfigured settings. The templates closely match those available on the Windows Media and H.264 encoders but can be edited as necessary depending on your own requirements. The transcoder supports the input and output files shown in Table 14.

Figure 21. Add Video Page

Table 14. Supported Input/Output Files

Supported Input Files	• H.264 (transport stream or mp4) • WM (Windows Media) • MPEG-1, MPEG-2, MPEG-4 • mov • avi
Supported Output Files	• H.264 (transport stream or mp2) • WM

▼   To configure VEMS for transcoding:

1. Make sure you have purchased and installed an NVR. See <u>Network Video Recording</u> on page 171.

2. Make sure you have installed a transcoder license. See <u>Install/Replace License Files</u> on page 17.

3. On the VEMS server, go to **Global Settings > Recorders** and configure an existing NVR as a Recorder. See <u>Recorders</u> on page 74 for details.

4. Be sure to check **Enable Transcoding** on the Recorder Configuration page.

5. Go to **Global Settings > Transcode Templates** and edit the available templates as explained below. Note that you can edit templates; you cannot add or delete templates. As explained below (see <u>Editing H.264 Templates</u>) it is always a good idea to backup the template files before making changes.

Note If the input file and output file have the same file extension, or the converted file has the same extension as the input file, VEMS will create a new file name by appending the output file bitrate in kbps to the original file name. For example, `{original name}_500K.mp4`. Note that there is a 4GB limit on files encoded to MP4.
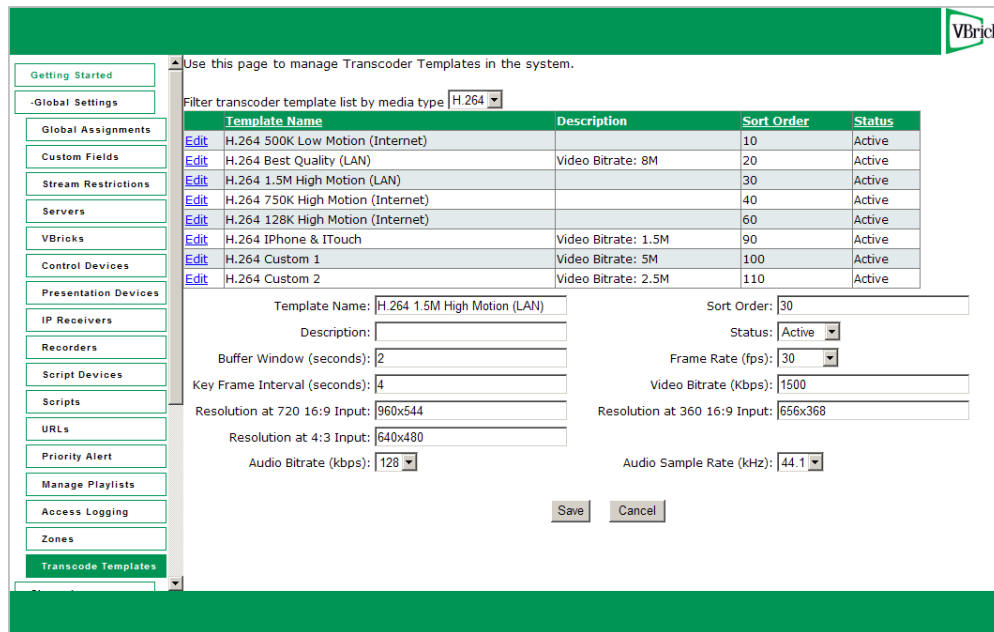
Template Name	This editable field shows the template currently selected.
Description	Optional. Add a user-friendly description.
Buffer Window	0.1 – 100 sec. Sets the rate control buffer depth in seconds. Larger buffer sizes may improve video quality and make the encoder's rate control more consistent.
Key Frame Interval	This interval allows a player to "sync up" with a video stream already in progress by providing basic anchoring and orienting data. If "key frames" are sent less frequently, it will take longer for the video to begin playing.
Resolution at 720 16:9 Input	If the input file has a 16:9 aspect ratio, and the input video height is greater than or equal to 720, the output file will have the value shown. Enter 0x0 to use the resolution of the source video file, otherwise enter [width]x[height].

Resolution at 4:3 Input	Enter `0x0` to use the resolution of the source video file, otherwise enter [`width`]x[`height`].
Audio Bitrate	This number represents how much data the VBrick will send out each second to carry audio to a player.
Sort Order	Determines the order in which the templates are displayed on the Add Video page. The template with the lowest value is displayed at the top of the list.
Status	Active | Inactive
Frame Rate	This number represents how many frames the VBrick will send out each second to carry the video to a player.
Video Bitrate	This number represents how much data the VBrick will send out each second to carry video to a player.
Resolution at 360 16:9 Input	If the input file has a 16:9 Aspect Ratio, and the input video height is less than 720, the output file will have the value shown. Enter `0x0` to use the resolution of the source video file, otherwise enter [`width`]x[`height`].
Sample Frequency	Select from dropdown. The frequency at which the audio is sampled at the encoder.

Editing H.264 Templates

You can edit the templates using the interface but you cannot add or delete templates. *If you are planning to edit the template files it is always a good idea to backup the original .xml files to a safe location for future use.* If necessary you can also edit the files in an .xml editor. The templates are located in: `C:\Program Files\VBrick\MCS\Transcoder Templates`

The output file resolution is based on the aspect ratio and resolution of the input file. For example, if the input file video is 16:9, and the video width is greater than or equal to 720px, the output file video resolution will be shown in the following table as 720 16:9. If the input file video is 16:9, and the video width is less than 720 px, the output file video resolution will be shown in the following table as 360 16:9. The following settings are common to all H.264 templates and can only be changed by editing the .xml file.

Audio codec	AAC-LC
Video encoding mode	CBR-1 pass
Resize mode	Letterbox
Audio channels	Stereo
Audio bits per sample	16

Table 15. H.264 Transcode Templates

Template	H.264 Best Quality (LAN)	H.264 1.5M High Motion (LAN)	H.264 750K High Motion (Internet)	H.264 500K Low Motion (Internet)	H.264 128K High Motion (Internet)	H.264 IPhone & ITouch	H.264 Custom 1	H.264 Custom 2
Video Bitrate	8M	1.5M	750K	500K	128K	1.5M	5M	2.5M
Resolution								

720 16:9	1280x720	960x544	656x368	656x368	256x144	480x272	0x0 †	640x360
360 16:9	656x368	656x368	656x368	656x368	256x144	480x272	0x0	640x360
480 4:3	640x480	640x480	400x300	640x480	320x240	480x360	0x0	640x480
Video Frame Rate	30	30	30	15	15	30	0	0 ††
Video Codec	H.264 Baseline	H.264 Main	H.264 Main	H.264 Main	H.264 Main	H.264 Baseline	H.264 Main	H.264 Main
Key Frame Interval	4	4	4	4	4	4	2	2
Video Buffer Window	2	2	2	3	3	4	5	5
Audio Sample Rate	48	44.1	44.1	44.1	44.1	48	44.1	44.1
Audio Bitrate	192	128	96	96	96	160	192	128

†   Resolution 0x0 means use resolution of input file.

††   Frame Rate 0 means use frame rate of input file.

Editing Windows Media Templates

You can edit the templates using the interface but you cannot add or delete templates. *If you are planning to edit the template files it is always a good idea to backup the original .xml files to a safe location for future use.* If necessary you can also edit the files in an .xml editor. The templates are located in: `C:\Program Files\VBrick\MCS\Transcoder Templates`

Output file resolution is based on the input file aspect ratio and resolution of the input file. The following settings are common to all Windows Media templates and can only be changed by editing the .xml file.

Video codec	VC-1 Main
Audio codec	WMA Professional
Video/audio encoding mode	CBR-1 pass
Resize mode	Letterbox
Audio Channels	Stereo
Audio bits per sample	16

Table 16. Windows Media Transcode Templates

Template	VC-1 Best Quality (LAN)	VC-1 1.2M (LAN)	VC-1 300K (Internet)	VC-1 128K (Internet)	VC-1 Windows Mobile	VC-1 Custom 1	VC-1 Custom 2
Video Bitrate	4.2M	1.2M	300K	128K	350K	4M	1M
Resolution							
16:9	640x360	384x216	256x144	160x92	240x136	0x0	384x216
4:3	640x480	320x240	240x180	160x120	240x180	0x0	364x272
Video Frame Rate	30	30	30	15	15	0	40
Key Frame Interval	3	3	5	6	8	4	4
Video Buffer Window	1	1	5	8	2	4	4
Audio Sample Rate	48	48	32	44.1	44.1	44.1	48
Audio Bitrate	192	128	32	32	48	192	128

Restricting Access

The **More Tools > Add Video** page makes transcoding options available to users. By default, the **Output Format** on the Transcoding window is set to **None** and transcoding is disabled. To enable transcoding, select an output format and a template. By default, if transcoding is enabled, both the original input file and the transcoded file are ingested. *The Transcoding options should be used with care.* A best practice is to restrict access to this feature so that transcoded files are not created inadvertently every you add a video. Access can be restricted by limiting access the NVR server(s) that perform the transcoding.
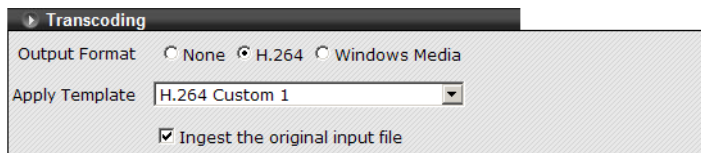
▼ To limit transcoding to specified users:

1. Open the Admin Console and go to **Users** (or **User Groups**) and click > **Allow Access to Specific Recorder Servers**.

2. To enable transcoding, check the box to make the NVR server(s) available. This will allow the selected user (or group) to access that server.

3. To disable transcoding, uncheck the box to make the NVR server(s) not available.

Server Administration

Topics in this section

Channels

Channel Guide

The Channel Guide configuration described here is used to display and populate the Channel Guide tab on the Portal Server user interface. The Channel Guide displays programming data from a VBrick channel server (Channel Guide Server 1) and/or it can display programming data from a second source (Channel Guide Server 2). The programming data shown in the Channel Guide can be updated periodically or on demand. This functionality requires a Channel Server license. If this license is not installed, the options for **Default URL** and **Default Password** are not shown on the Channel Guide configuration page.

Channel Guide Server 1

VBrick has partnered with a leading content provider, to provide news, information, and entertainment programming. This is an optional service that requires a license and may not be supported at your site. The program listing includes some 80+ television programs. These programs are generally all "network" listings, such as ABC, CBS, NBC, CNN, "National Geographic Channel, etc. The listing comes from a VBrick-maintained server. This server is a VBrick Apache machine that connect to our third-party content provider. In this scenario, the third-party provider provides the programming data shown on the Channel Guide user interface. Note that program data is only retrieved for defined TV stations (see Add TV Stations on page 109).

▼   To enable Channel Guide Server 1:

1.   Enable Channel Guide Server 1.

2. Define the TV Stations you want to appear in the Channel Guide.

3. Click **Update Now** to populate the defined TV stations with hourly programing data.

Channel Guide Server 2

You can use Channel Guide Server 2 to enable another source of program data. This is an optional service that requires a license and may not be supported at your site. There are two possible scenarios. The first option is to implement a web service that models the VBrick web service. This option requires the services of an experienced software developer. In the second option, you use VEMS as a Channel Guide Server host. There is a local VEMS channel web service that can be used for a second channel guide server. As explained below you point `web.config` of the web service to the local/virtual directory of the VEMS server which has the xml station and program data. Sample station and program data is located in the following VEMS folder:

`C:\Program Files\VBrick\MCS\Common\ChannelGuideWS\web.config`

You will need one programming file for each defined station. You can create this file manually or you can write a program to auto-generate the file.

▼ To configure VEMS as a Channel Guide Server host:

1. Enable Channel Guide Server 2.

2. Go to `C:\Program Files\VBrick\MCS\Common\ChannelGuideWS\web.config`

3. Create and add the following files to this folder and modify `web.config` to point to them.

   `stations.xml`

   `<stationid>.xml`

4. Modify `web.config` to point to the files you created.

   `... value="C:\Program Files\VBrick\MCS\Common\ChannelGuideWS\`**`stations.xml`**`"`

   `... value="C:\Program Files\VBrick\MCS\Common\ChannelGuideWS\`**`10003`**`"`

5. Each station defined in `stations.xml` (Figure 22) must have its own station id file named after the `<stationid>`, for example `10003.xml` (Figure 23).

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <allstations>
- <station>
  <stationid>10003</stationid>
  <stationname>American_Broadcasting_Company</stationname>
  </station>
- <station>
  <stationid>10142</stationid>
  <stationname>Cable_News_Network</stationname>
  </station>
- <station>
  <stationid>10149</stationid>
  <stationname>Comedy_Central</stationname>
  </station>
- <station>
  <stationid>11150</stationid>
  <stationname>The_Discovery_Channel</stationname>
  </station>
- <station>
  <stationid>11158</stationid>
  <stationname>The_Learning_Channel</stationname>
  </station>
- <station>
  <stationid>11207</stationid>
  <stationname>USA_Network</stationname>
  </station>
  </allstations>
```

Figure 22. `stations.xml`

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <completeguide>
- <program>
  <title>Wife Swap</title>
  <stationid>10003</stationid>
  <station>American_Broadcasting_Company</station>
  <description>A woman from a family obsessed with motorcycles trades places with a wor
  <reduceddesc1>A family passionate about their Irish heritage.</reduceddesc1>
  <reduceddesc2>A family passionate about their Irish heritage.</reduceddesc2>
  <reduceddesc3>A family obsessed with motorcycles.</reduceddesc3>
  <mpaarating />
  <starrating />
  <tvrating>TVPG</tvrating>
  <cc>Y</cc>
  <airdate>04/04/2009</airdate>
  <airtime>0000</airtime>
  <duration>0100</duration>
  </program>
- <program>
  <title>Supernanny</title>
  <stationid>10003</stationid>
  <station>American_Broadcasting_Company</station>
  <description>Jo helps a couple and their two children, ages 7 and 4, navigate the pa
  <reduceddesc1>Jo helps a couple and their two children navigate the painful process
  <reduceddesc2>Jo helps a family deal with divorce.</reduceddesc2>
  <reduceddesc3>Jo helps a family deal with divorce.</reduceddesc3>
  <mpaarating />
  <starrating />
  <tvrating>TVPG</tvrating>
  <cc>Y</cc>
```

Figure 23. `10003.xml`

Changing the Time Zone

The times for Channel Guide listings on the Portal Server are in UCT (Universal Coordinated Time). The program times are calculated by the Portal Server software using the time zone setting in Windows. For example, if a program is listed as beginning at 1800 hours UCT, and your time zone is U.S. Eastern, the "offset" from UCT is -5 and the program will be listed at 1300 hours. If your time zone is U.S. Pacific, the "offset" is -8 and the program will be listed at 1000 hours. To get accurate program listings, your local time zone must be properly configured in Windows. The Portal Server computer is shipped with U.S. Eastern time and should be reconfigured to match your own time zone. Use the following steps to set the time zone and verify that it was successfully changed.

▼ To change the time zone:

1. For reference purposes, note the currently scheduled time for any program in the Channel Guide.

2. Go to **Start > Control Panel > Date and Time** and select the Time Zone where the Portal Server is located.

3. When done reboot the Portal Server and open the Admin Console.

4. Go to **Channels > Channel Guide > Channel Guide Update** and click **Update Now**.

5. Wait approximately 20 minutes for the Channel Guide to update.

6. Verify that the time zone has been updated. Check the scheduled time for the program you noted in Step 1 and verify it has been updated to match your current time zone.

Channel Guide Server 1 Configuration	Use to define Channel Guide Server 1. Check to enable using the default web service URL.
	• Default URL – use the default VBrick web service. To enter a different URL location, uncheck the Default box and enter a web service URL.
	• Web Service URL – enter a valid web service URL.
	• Default Password – use the default password or uncheck, enter and confirm a new password.
Channel Guide Server 2/ DVB Gateway Configuration	• Channel Guide Server 2 – use to define a second source of programming data. The fields are the same as above.
	• Use DVB Gateway data – reserved for future use.
Channel Guide Update Time and Day	Select the time and day when the Portal Server will connect to the Channel Guide Server for program updates. This updates the Channel Guide on the user interface. When *TV Station* program data is updated, all expired *Custom Station* program data (more than 14 days old) is purged.

Channel Guide Update	Click **Update Now** to immediately retrieve programming from the Channel Guide Server and/or update the Channel Guide on the user interface. An update purges all outdated programming information from the database.

Stations

Use this page to add stations to the Channel Guide on the Portal Server "user" interface. There are two types of stations. **Custom Stations** are those for which *you* define program information and associate with a stream. **TV Stations** are those acquired through a third-party provider. **TV Stations** are also associated with a stream and already have program information provided by a Channel Guide Server. Note that the **Add TV Stations** option is not shown unless you have a Channel Guide Server license installed on the Portal Server (see Install/ Replace License Files on page 17 for more information). All currently defined stations are shown in the **Stations List**.

The Portal Server discovers all available live streams on the network. On a network with many live streams, the administrator can keep the stream list organized by assigning channel numbers. This also provides an environment for end users that is similar to television. When adding stations, you can assign or change the **Icon**, **Name**, **Channel** number etc. You can also enter a searchable **Description** that displays in the **Info** popup when you mouseover the channel number in the user interface. You can also enter **Tags** for searching, and values for any custom fields that have been defined (see Custom Fields on page 32).

Note For best viewing results after adding stations, click the **Live Media** button on the user interface to refresh the page and verify your changes. To avoid caching conflicts, do not use the browser refresh (F5) button.

Add Custom Stations

▼ To add a custom station:

1. Go to **Channels > Stations** and click **Add Custom Stations**.

2. Click on any *available* live stream to populate the window shown below. Note that only those streams not currently assigned to stations are displayed and available for use.

3. Select an existing icon or **Browse** to a file and select **Import** to make additional icons available.

4. Change the station **Name** (optional) and enter a **Channel** number (required).

5. Add a **Description** of the channel and **Tags**. These are displayed on the **Info** page shown when you mouseover the station icon. They are associated with the stream and make it easier to search for specific content.

6. When done click **Add Custom Station**. This creates the station, disables the **Add Custom Station** button, and enables the **Edit Programs** and **Add New Links** buttons.

7. Add custom programming information (see Custom Programs) and links (see Add New Links) as explained below.

8. Click **Modify Custom Station** when done to save your changes.

Available VBrick SAP Live Streams	Select an available live stream on your network. These were previously created and include VBrick SAPs (Session Announcements), multicasts from VOD servers, and URLs that were manually entered. See URLs on page 81 for more information about manually-entered URLs. *Note that only those streams not currently assigned to stations are displayed in this list.*
Icon Image	Navigate to any valid image file (.jpg, .gif, or .png, only). Use an image that will scale appropriately. All images are resized to 18x30 px.
Channel Name	Name assigned to the station that will display on the popup when you click an icon in the Channel Guide.
Channel #	Required. Unique number that will display on the popup when you mouseover the icon on the Live Media page
Description	Optional. Description that will display on the View Info page.
Tags	Optional. Enter searchable keyword tags(s) separated by commas or spaces that will display on the View Info page.
Custom Programs	Lets you add custom programming data. Note that you must add a Custom Station before creating programs for it.
Custom Fields	Any Custom Fields created on the Global Settings > Custom Fields page are shown here.
Links	Optional. Add hyperlinks that will display on the View Info page. See Add New Links below. Note that you must add a Custom Station before creating links for it.

Add TV Stations

This option is not shown unless you have a license for a Channel Guide Server. If you do have a license, certain content is being made available from a third-party provider. Adding a **TV Station** is the same as adding a **Custom Station** (see above) with two important distinctions. First, you must select a **Station Name** from the pre-populated list, an example of which is shown below. Second, there is no button that will allow you to create custom programming. The programming for TV Stations is automatically provided by the specified Channel Guide Server and updated at regular specified intervals (see Channel Guide on page 103 for details).
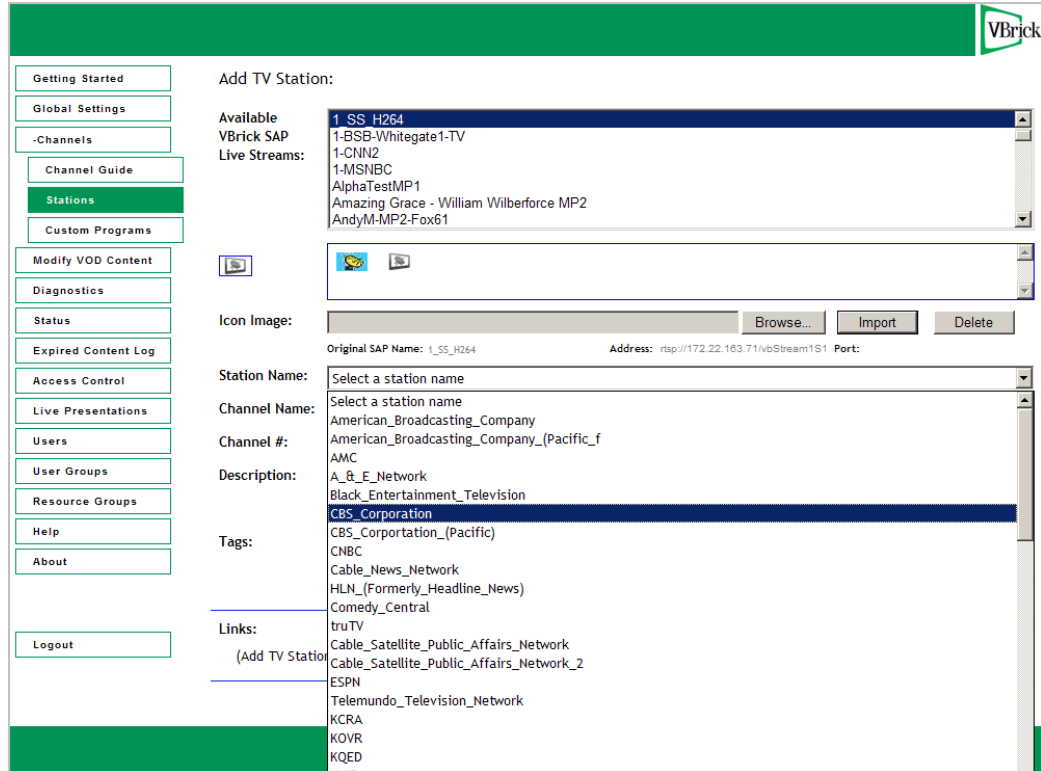
Station Name	Select a station from the pre-populated dropdown list.
Channel Name	Enter a searchable name (for example "CBS") so you can search **By Channel Name** in the Channel Guide.
Channel #	Enter a unique number that will identify the channel in the Channel Guide.

Add New Links

This feature lets you add a hyperlink to the page you get by clicking the **View Info** link that is associated with each live stream.

▼ To add a new link:

1. Click **Add New Link** and enter a **Link Title** and **Link Type**.

2. Enter a Web Page URL or navigate to an upload file (an image, a Microsoft Word document, etc.).

3. Click **Add Link** when done and repeat as many times as necessary.

© 2011 VBrick Systems, Inc.

Link Title	The title actually displayed on the View Info page, for example "Additional Information."
Link Type	• Web page URL – Enter a valid URL or copy and paste one from your web browser. • Uploaded File – Browse to select an upload file. This can be a PowerPoint, an image, or any file you want to make available to end users. The file is automatically uploaded to the Portal Server and the Portal Server creates a URL for end users to access it.

Custom Programs

This page is used to add programming information to an existing station. You can only program custom stations; TV stations (if present) are auto-programmed by a Channel Guide Server. You use the **Custom Programs** page to manually create programming data and associate it with a Custom Station. For example, you may want to modify the Channel Guide so that "Monday Night Football" is shown in the 8–10 P.M. time slot on Monday nights from September through January.

Note All times for custom programs are shown on this page in the currently selected time zone for the Admin Console—*not in local time*. When displayed in the Channel Guide however, the time is converted to viewer's local time zone. (The Admin Console time zone is displayed is configured in <u>Global Assignments</u>.)

Add Custom Programs

▼ To add custom programming to a custom station:

1. Click on **Custom Programs** to display the Custom Stations page.

2. The "Custom Station" dropdown list shows all currently defined *custom* stations. Select a Custom Station from this list and then click **Add New Custom Program**.

3. Use the fields explained below to create custom programming for the selected station. Click on the header titles as appropriate to sort the entries in the list.

4. Use the horizontal slider bar to display all fields. When done, click **Add**. The program will be added to the specified time slot and you will see a view similar to Figure 24 when you mouseover the item in the Channel Guide on the user interface.

Note When *TV Station* program data is updated from the Channel Guide Server, all expired *Custom Station* program data (more than 14 days old) is purged.
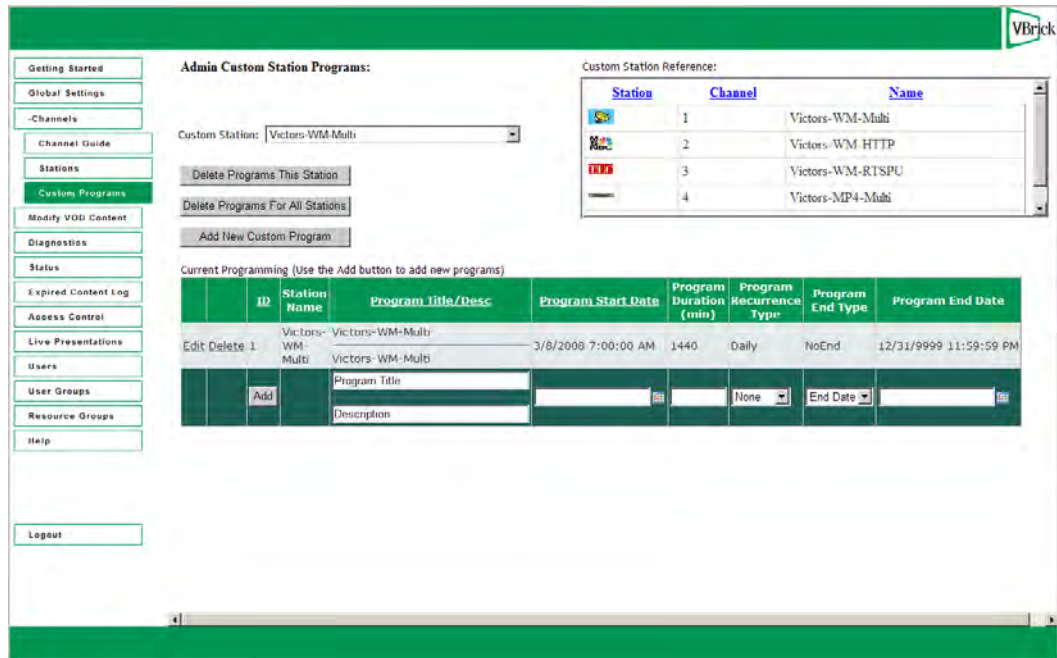
Custom Station	From the dropdown list, select a defined Custom Station for which you want to define a program.
Delete Programs This Station	Delete all programming data for the *selected* station.
Delete Programs For All Stations	Delete all programing data for *all* stations.
Add New Custom Program	Add a new line at the bottom of the "Current Programming" list for a new custom programming item.
ID	Program ID. Read only.
Station Name	Station Name. Read only.
Program Title/ Desc	Program Title – is shown in the Channel Guide, for example "Monday Night Football."
	Description – is shown on the popup (see Figure 24) when you mouseover the item in the Channel Guide and click Info.
Program Start Date	Use the calendar to select the start date and start time. Alternately, you can manually enter the values in the proper format: for example: 3/10/2009 5:30:00 PM
Program Duration	Required. Program length in minutes. Maximum = 1440 (24 hr.).
	To add a custom program that never ends, set **Program Duration** to "1440," with a "Daily" **Program Recurrence Type**, and a "NoEnd" **Program End Type**.
Program Recurrence Type	None | Daily | Weekly. If weekly, occurs on the same *day* as specified in Start Date.

Program End Type	Select NoEnd or EndDate and use calendar.
Program End Date	Use the calendar to select recurrence end date.
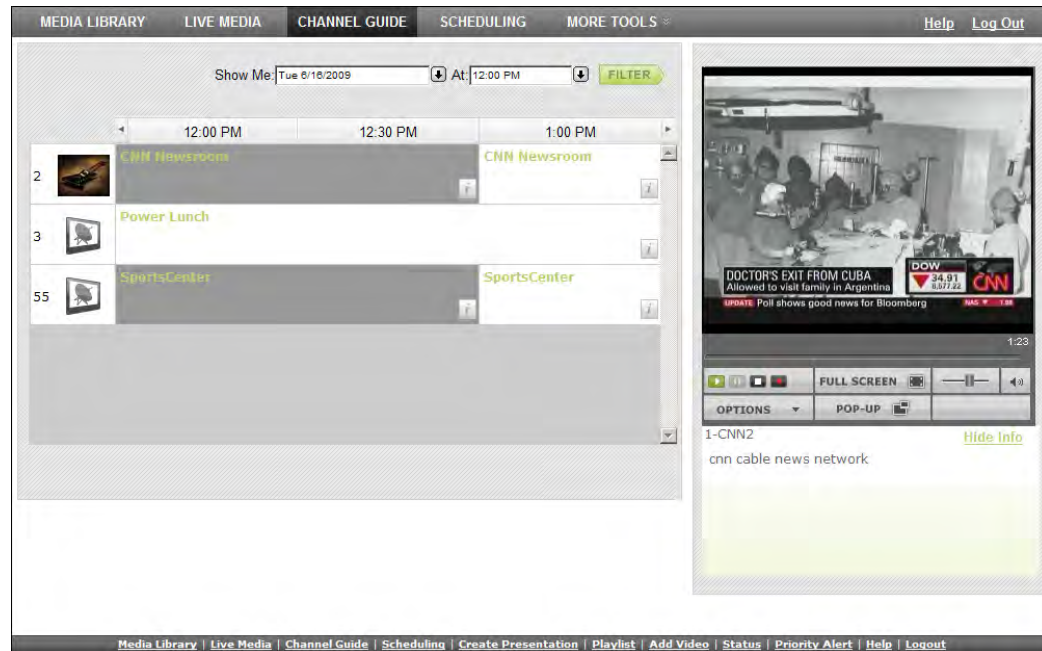
Figure 24. Custom Program Data

Note The message "Program Unavailable" in the Channel Guide means there is no programming data associated with the stream. *It does not mean the stream itself is unavailable.* You can still click on the stream to launch it in the preview window.

Edit Custom Programs

▼ To edit a Custom Program:

1. Navigate to the program you want to change and click **Edit**.

2. Manually edit any of the fields as necessary and click **Update** when done.

Modify VOD Content

Video on Demand Servers only. Administrators and authorized users can modify and delete content located on their video on-demand servers. (Note that you cannot delete or modify any content files that are currently in use.) Administrators can find or filter the displayed assets by clicking on **All**, **Tags**, **Title**, or **Expiration Date**. You can also use this window to set **Expiration**, define the maximum number of concurrent viewers, and update expiration dates for purchased content. Also, be aware that a user with publishing permissions can delete content by clicking the **Info** hyperlink and then **Delete Video**. To disable this user option, disable the user's content publishing permissions (see Allow Content Publishing on page 140).

Purchased Content Expiration

Purchased content is protected against theft, piracy, or copyright violation by means of an expiration date or viewing period. Each piece of content has an optional expiration date in the database. If the current date is later than this expiration date, the content cannot be viewed by a Portal Server user. When new content is added (for example using Add Video or autoingest), administrators can optionally enter an **Expiration Date** or **Viewing Period** and can limit the number of concurrent viewers. This data can be modified at anytime. The Expired Content Log shows all expired content on your system in chronological order with the oldest expiration date first. See Copyright Protection on page 2 for more information.

If third-party content is purchased from VBrick, however, the **Expiration Date** or **Viewing Period** are automatically populated with read-only data that cannot be changed without updating the license. (**Content Provider** and **Content Group** are only populated when you select purchased content.) If you purchased third-party content from VBrick, this content was installed on your VOD server(s) prior to shipment. If you purchased content later, this content can be mass-ingested into the Portal Server using a provided utility. See Purchased Content Ingestion on page 217 for more information.

Search box (All)	Search for specific assets by selecting All, Tags, Title, or Expiration Date. Then click Refresh.

Filter Pattern	Search for specific assets using a filter pattern. Type any text string and click Refresh. For example, type mp4 to search for assets with mp4 in the title. The filter does not recognize "wildcards" and is not case-sensitive.
Name	Video content name. Click on **Refresh** to re-paint the screen or **Purge** button to remove the artifacts of failed Delete operations.
Expiration	Expiration date if any.
Folders	Use to navigate to a specific folder.
Filename	Click once on any named content in the list to populate this field.
Expiration	• Expiration Date – set date in mm/dd/yyyy 12:00 AM format. • Viewing Period – set a value for viewing period in hours, days, weeks, months, or years.
Max. Concurrent Users	Defines the maximum number of users who can view this stream at the same time. Select Unlimited or enter a value greater than zero.
Content Provider	This read-only field is populated with information when you select a video that was included in content purchased from VBrick.
Content Group	This read-only field is populated with information when you select a video that was included in content purchased from VBrick.
Valid Licenses	This dropdown displays a list of all currently valid licenses for content purchased from VBrick. Select the license you wish to update.
Update all content expiration for the selected license	Use this field to update the expiration dates of purchased content. First install the license you receive from VBrick (see Install/Replace License Files on page 17). Then check this box and click Submit to update the content expiration data for the select license.

▼ To modify VOD Content:

1. Click on the content to be changed.
2. Enter a new filename and/or path for that file. Note that the file must be alphanumeric characters and cannot contain embedded spaces.
3. Set the **Expiration Date** or **Viewing Period** as necessary.
4. To delete a file, select the file and click **Delete**.

Note NXG1 only. You cannot rename or otherwise manage VOD files stored on some legacy NXG1 servers. This feature is supported on all NXG2 servers and on all other servers currently available with VEMS Portal Server.

Diagnostics

This window displays information about Scheduler events only. It displays system log messages by source and time and (generally) IP address. Use **Clear All** to empty the log. *Note that all times are shown in the currently selected time zone for the Admin Console—not in local time.* The Admin Console time zone is displayed near the bottom of the page and is configured in Global Assignments (see "Assign Time Zone of Admin Console.")

Status

This window shows the status of videos being added or recorded. Use **Refresh** and **Purge** as necessary. Use the tree controls on the left to expand (or contract) individual entries. Click the Cancel icon ⊠ to the left of each to cancel a recording or ingestion in progress. This also cancels the recording on the **Live Media** page.

Expired Content Log

This window shows all expired content in chronological order with the oldest expiration date first. Click **Purge All** to delete all records in the log. See <u>Modify VOD Content</u> on page 113 and <u>Stream Restrictions</u> on page 33 for more information.

Access Control

Under the Access Control section, administrators have the ability to enable Authentication and Authorization which requires users to login and be authenticated. By default **Enable Authentication and Authorization** is unchecked which allows everyone to access all content and all functions (recording, publishing, etc.). When Access Control is enabled, **User Groups**, and **Resource Groups** are shown on the navigation bar. Access control determines what

functionality is available to each user. For example some users may have unlimited access, while others can only view certain live channels and may not have permission to record live channels or add videos to the VOD server. Users and User Groups on page 131 explains in detail how configure users and groups.

Access control also lets you specify which folders are used when individual users record live media, add videos, or autoingest content. If you do not enable **Authentication and Authorization**, all of these actions default to the root folder (which can quickly get cluttered).

Note As soon as you check **Enable Authentication and Authorization**, users will be prompted for User Names and Passwords. VBrick recommends configuring the system prior to user access or during off hours when the network is idle.

Enable Authentication and Authorization	Enable authentication and authorization which requires users to login and be authenticated. If not checked, all users have access to all functionality and content.
Use VBrick database	Use the VBrick (non LDAP) database provided with VEMS Portal Server.
Use LDAP database	Use an LDAP database. VBrick supports several LDAP implementations including Microsoft Active Directory, Novell eDirectory, and Oracle (Sun) Enterprise Directory Server. These vendor implementations are tested and supported by VBrick.
Use RSA authentication	Use RSA authentication provided by RSA, the Security Division of EMC.

Use LDAP Database

Administrators have the option of using the onboard **VBrick database** for authentication, using an **LDAP database**, or using both. *VBrick supports major LDAP vendors such as Microsoft Active Directory, Novell eDirectory, and Oracle (Sun) Enterprise Directory Server.* These directory

services have been tested in some configurations but may not work with all structures and schemas. Apple OpenDirectory is not currently supported; Microsoft "Universal" type security groups are also not supported. In all cases, nested groups (groups within groups) are incompatible with VEMS. Contact Support Services for more information. Use the options on the following page to add or manage LDAP servers.

If authenticating against Microsoft's Active Directory, check the **LDAP Server is Microsoft Active Directory** check box and enter the path to the LDAP server in the **LDAP Path** box. If authenticating against a directory other than Microsoft Active Directory, do not check **LDAP Server is Microsoft Active Directory**. LDAP (Lightweight Directory Access Protocol) is a standardized method to access directories from multiple vendors. A complete discussion of LDAP is beyond the scope of this document.

LDAP Server is Microsoft Active Directory	Check only if using Microsoft Active Directory.
Use Integrated Windows Authentication	Use "single sign-on." This means that once you login to your local network, you can open VEMS Portal Server without re-entering your login credentials. See below <u>Use LDAP with Single Sign-On</u>.
Use Independent Group Entries	If unchecked (the default), the user's group memberships are stored as attributes of the user's directory entry identified by the **Attribute for Groups** field. If checked, VEMS will support LDAP models where group entries are independent of user entries. If checked, the Independent Group ObjectClass and Independent Group Identifier fields are required.
LDAP Path †	*Required by VEMS Portal Server.* Case sensitive. Must begin with `LDAP://` Points to a specific position in the LDAP tree and also includes the machine IP address (or Domain name) on which the server is running. For example use `LDAP://myLDAPServer` with Microsoft Active Directory; use `LDAP://myLDAPServer:636` with Novell eDirectory. For more information, see <u>Installing the Root Certificate</u> on page 125.
Attribute for Usernames †	*Required by VEMS Portal Server.* Attribute to identify a user. The following sample username attributes are widely used but refer to a specific LDAP schema: • Microsoft Active Directory: `sAMAccountName` • Novell eDirectory: `uid` • Oracle (Sun) LDAP: `uid`

Attribute for Groups †	*Required by VEMS Portal Server.* Attribute to identify the group to which a user belongs. The following sample group attributes are widely used but refer to a particular LDAP schema: • Microsoft Active Directory: `memberOf` • Novell eDirectory: `groupMembership` • Oracle (Sun) LDAP: `uniqueMember`
User Base DN	Base distinguishing name (DN) of user node and/or the Base DN for the Master Username.
Username Prefix	Used in non-Active Directory environments where the user name is prefixed with a specific string such as `uid=` or `cn=`. The following sample prefixes are widely used but refer to a specific LDAP schema: • `uid=` (Oracle ((Sun)) LDAP) • `cn=`
Master Username	Required for single-sign-on. User name that has admin permission to browse the LDAP tree. Used to browse the LDAP tree to get user groups.
Master Password	Required for single-sign-on. Password for Master Username.
Ind. GroupObjectClass	A group attribute in the LDAP database. Identifies which entries will be searched for user memberships. Oracle (Sun) LDAP uses `groupOfUniqueNames`
Ind. Group Identifier	The group attribute that uniquely identifies a group. VEMS will match the values returned for this attribute with group names entered on the **User Groups** page. Oracle (Sun) LDAP uses `cn`
Group Base DN	Base distinguishing name (DN) of user node.

† VEMS Portal Server required field. All others are optional.

Note The Softerra LDAP Browser 2.6 provides an Explorer-like LDAP client you can use to browse the LDAP tree. It is available for Windows only and can be downloaded free of charge from Softerra at http://www.ldapbrowser.com

Use LDAP with Single Sign-On

The following procedures explain how to set up single sign-on in Windows Server 2003 and in Windows Server 2008. To use single sign-on, go to **Access Control** and then check **Enable Authentication and Authorization** and **Use LDAP Database**. If the LDAP server is Microsoft Active Directory, you can select **Use Integrated Windows Authentication** to enable "VEMS Single Sign-on." This means that once you login to your local network with your assigned credentials, you can open VEMS Portal Server without re-entering your login credentials. VEMS Portal Server uses your assigned credentials to authenticate and authorize your defined permissions within the application. (If using an LDAP directory other than Microsoft's Active Directory, VBrick strongly recommends using SSL to encrypt the communication between the Portal Server server and the LDAP directory. Please consult

your LDAP vendor documentation for instructions on how to configure SSL.) When configuring for Integrated Windows Authentication, keep the following points in mind:

- Integrated Windows Authentication is only valid when using LDAP Authentication with Microsoft Active Directory.
- You must perform an additional configuration step in IIS as explained below in <u>Configuring IIS for Single Sign-On (Windows Server 2003)</u> or <u>Configuring IIS for Single Sign-On (Windows Server 2008)</u>.
- Integrated Windows Authentication only works seamlessly with Microsoft Internet Explorer browsers (Windows and Macintosh). When accessing VEMS Portal Server, you will get a popup login window *only* if you have not previously logged in to the network.
- When using Integrated Windows Authentication, all single-sign-on users must have an Active Directory account and the Portal Server must be part of the Windows domain.
- When using Integrated Windows Authentication, Microsoft Internet Explorer's default behavior is that it will *not* prompt for an ID/password when the server is in the **Local Intranet Zone**. (By default, Internet Explorer assumes a URL without a period (.). This means `http://yourserver/` is in the **Local Intranet Zone** while `http://yourserver.yourcompany.com` (or `http://199.88.7.11`)) is in the **Internet Zone**.

Note If single sign-on is enabled on multiple LDAP servers, when a user signs on for the first time, the system validates the login credentials against all servers configured for single sign-on. If you are validated by at least one server, you are automatically logged in. In most cases when single sign-on is enabled, the user will *not* be prompted for a **Domain** name at login.

Configuring IIS for Single Sign-On (Windows Server 2003)

Use the following steps to configure IIS for single sign-on. *If you do not perform these steps, the login page will likely be blank when you launch the Portal Server.*

▼ To configure IIS for single sign-on:

1. Go to **Start > Administrative Tools > Computer Management**.
2. Expand **Services and Applications** and expand **Internet Information Services (IIS) Manager**.
3. Expand **Web Sites** and then right-click on **Default Web Site** and select **Properties**.
4. Go to **Directory Security > Authentication and access control** and make sure that **Integrated Windows authentication** is checked on the following window.
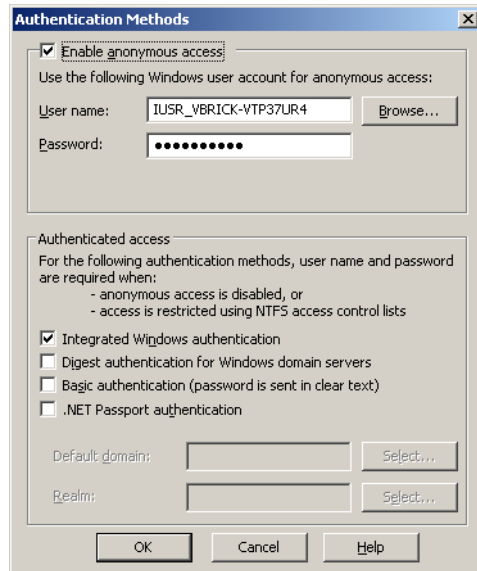
Configuring IIS for Single Sign-On (Windows Server 2008)

Use the following steps to configure IIS for single sign-on. *If you do not perform these steps, the login page will likely be blank when you launch the Portal Server.*

▼ To configure IIS for single sign-on:

1. Go to **Start > Administrative Tools > Server Management**.

2. Select Web Server (IIS) and click **Add Role Services**.
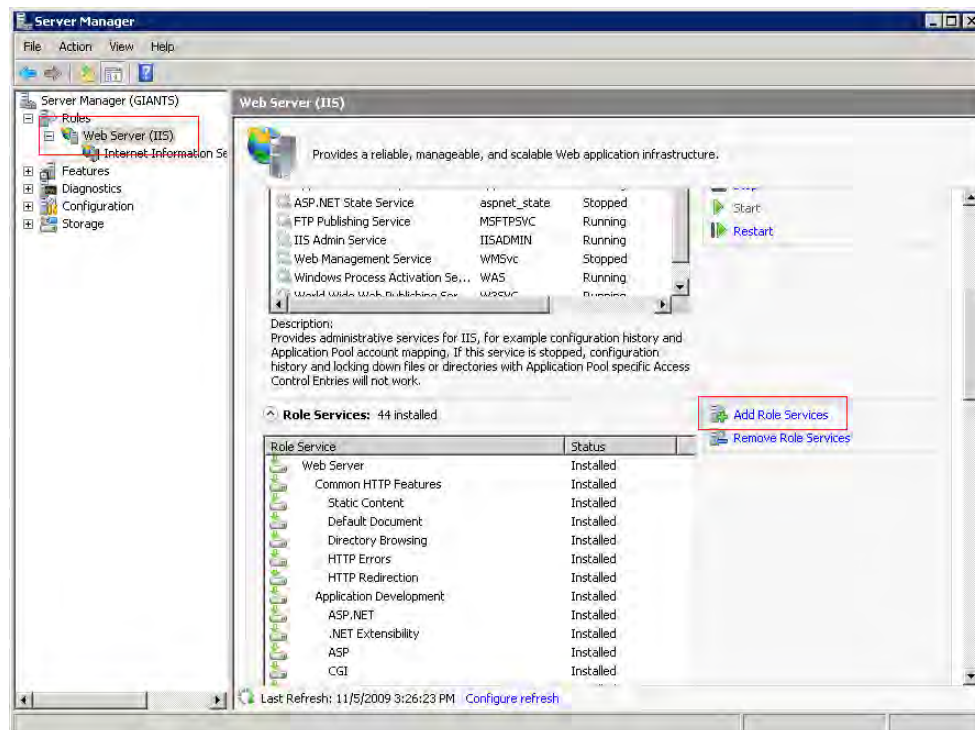
3. Enable the required roles (Basic Authentication and Windows Authentication).
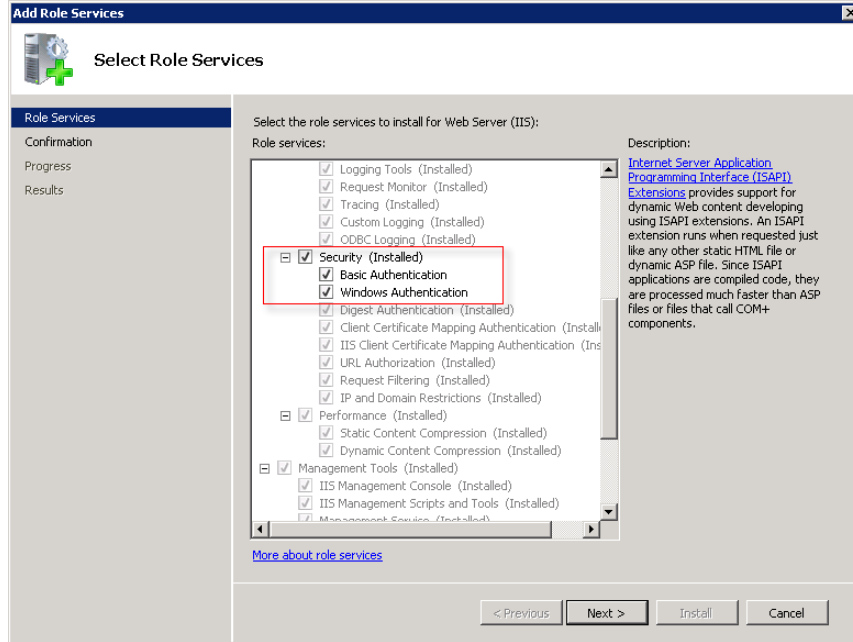
4. Restart IIS. Go to **Start > Administrative Tools > Internet Information Services (IIS) and** click on the Authentication option for the server.
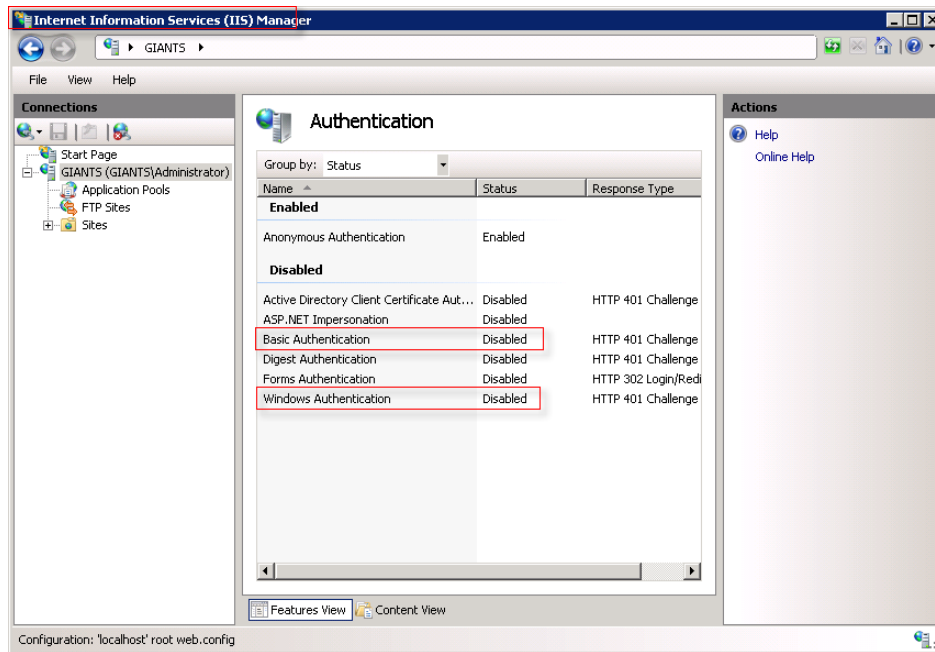
5. Right-click on Basic Authentication and Windows Authentication to **Enable**.

Use Single Sign-On

▼ To use single-sign-on (and avoid username/password prompts), you must do **one** of the following:

• Access the Portal Server by the *alphabetical name* (for example `http://yourserver`).

- Access the Portal Server by the *IP address* in which case you must also add the Portal Server to the **Local Intranet Zone** (**Internet Options > Security > Sites**). This setting can be pushed company-wide by an administrator using security policies.

- Change Internet Explorer's default settings to allow **Automatic logon with current username and password** (Go to **Internet Options > Security > Custom Level > User Authentication**).

Use LDAP with SSL

Installing the Root Certificate

If the LDAP server requires SSL (Secure Sockets Layer) for encryption and authentication, you will need to install the certificate locally on the VEMS Portal Server as a **Trusted Root Certificate Authority**.

▼ To install the root certificate locally on the VEMS Portal Server as Trusted Root Certificate Authority:

1. Open Internet Explorer.

2. In the address bar type `https://LDAPSERVER:636` where `LDAPSERVER` is the address of the LDAP Server associated with Certificate Authority (See <u>Resolving Other Security Alerts</u> on page 126) and `636` is the SSL port used to authenticate with the LDAP Server.

3. When Internet Explorer displays a Security Alert dialog (Internet Explorer 6) or certificate error screens (Internet Explorer 7), click **View Certificate**.

Note Internet Explorer 6 only. All three items in the Security Alert window below must be in compliance. The first item can easily be installed using these instructions; for the middle item, the local CA will need to create a new certificate if it is out of date; for the last item, the name of the certificate will need to match the address entered in the address bar of your browser.

---

4. A Certificate window will open, click on the **Certificate Path** tab.

5. If there is more than on certificate listed in the **Certificate Path** tab, choose the root certificate by selecting the top-most certificate and then clicking **View Certificate**.

6. Choose the **General** tab. and click **Install Certificate**.

7. Click **Next**.
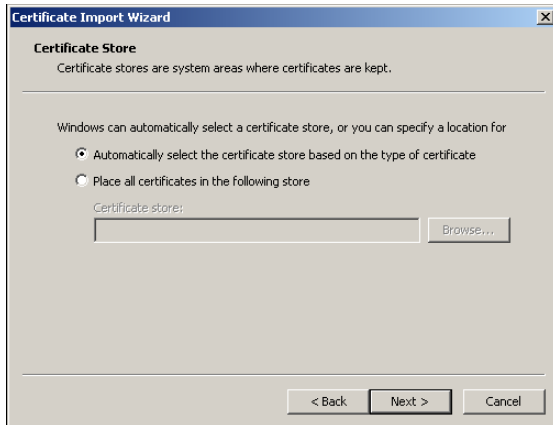
8. Click **Place all certificates in the following store**.
9. Click **Browse**.

10. Check **Show physical stores** check box.
11. Click the plus sign (+) next to **Trusted Root Certificate Authorities**.
12. Select **Local Computer** and click **OK**.
13. Click **Next** and **Finish** when done.

Resolving Other Security Alerts

If you are receiving any other Security Alerts you will need to identify the problem as either "out of date" or **The name on the security certificate is invalid.** If the certificate has an invalid name, follow the steps below to determine the valid name. If the certificate has an "out of date" error, a new certificate must be created.

© 2011 VBrick Systems, Inc.

▼ To determine the valid certificate name:

1. Click **View Certificate**.

2. The **General** tab shows who the Certificate is issued to; the address shown is the address that will need to be used in the browser address bar, as well as in the configuration of the LDAP Server.

For example: if the information is `edirldap.vb.loc` then the address bar should read `https://edirldap.vb.loc:636` and the LDAP Path should read `LDAP://edirldap.vb.loc:636` To find out if the address is accessible, ping the address given in a command prompt. If the address is not accessible you must create or add a DNS entry to the Host file on the local server or generate a new certificate with the correct information.

Use RSA Authentication

The VEMS Portal Server supports RSA Authentication. This feature works when there is an authentication and authorization plugin loaded on the VEMS IIS server. VBrick has tested this feature in an RSA-secured environment. Plugins from other vendors may also work if they can include HTTP headers similar to those explained below.

▼ To configure the Portal Server for RSA Authentication:

1. Launch the Portal Server Admin Console and click on **Access Control** in the left navigation panel. (Note that the following screen shows sample data.)

2. Check the **Use RSA authentication** option to enable RSA authentication.

3. Populate the User ID, E-Mail, and Group fields in the HTTP header as explained below.

User ID Field Name	Name of the HTTP header field that will store the unique User ID. For Vodafone, this may be the VDUID or the E-Mail address.
E-Mail Field Name	Name of the HTTP header field that will store the user's e-mail address.

Group Field Name	Name of the HTTP header field that will store the user's group/organization membership. For Vodafone, this will be the VfOpCoID.
Use Group ID	Check this box if the Group Field Name (above) returns a group ID rather than a group name. For Vodafone, this should be checked.

Configuring the Group ID

The **User Group ID** field (see below) will display only if the **Use Group ID** box is checked on the Access Control page. The **User Group ID** is a unique identifier for the group. To set the Group ID, go to **User Groups > Add User Groups > Add/Modify Group Information**.

"Default" Group	This is the default group used to define base permissions for all users.
User Group Name	A unique name for the group.
User Group ID	The User Group ID is a unique identifier for the group.

Users

See Configuring Users on page 135.

User Groups

See Configuring User Groups on page 142.

Resource Groups
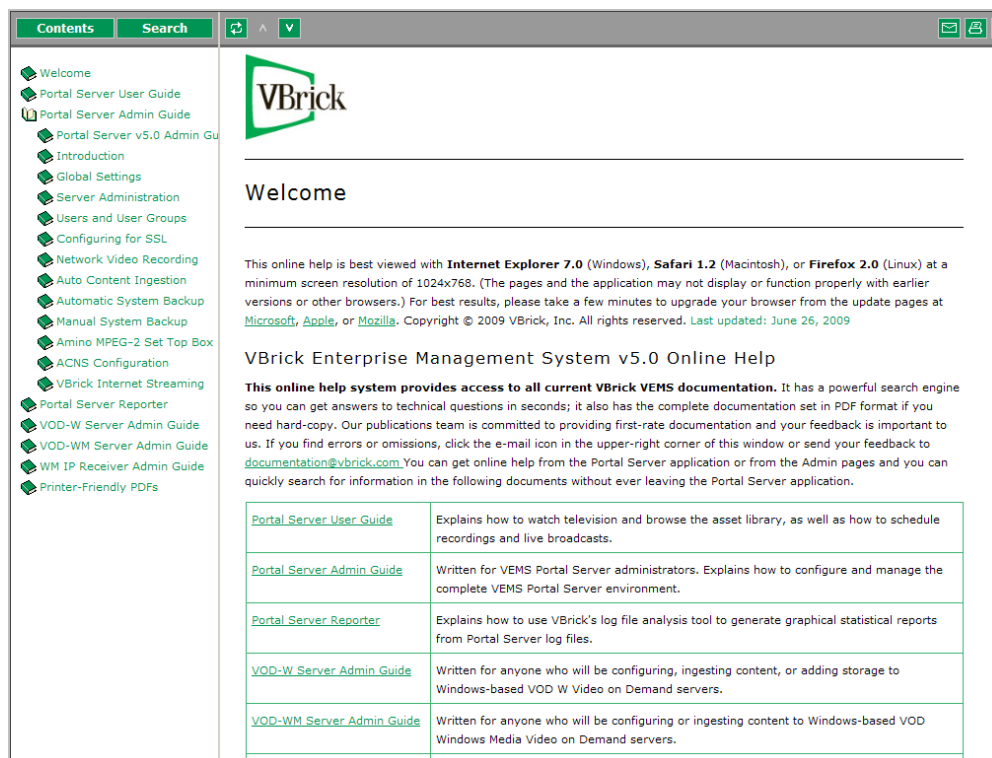
See Resource Groups on page 143.

Digital Signage

If you purchased the Digital Signage application, a **Digital Signage** button will display on the on the navigation bar launch a login page. Digital Signage is a standalone VBrick application that lets you use VBrick video appliances and VOD servers to configure and display dynamic video content on digital signage displays like LCDs, plasma screens, and other devices. In order to integrate video into a Digital Signage display, content creators simply add the URL of the live video from a VBrick appliance or the video on-demand URL from a VOD server. The VBrick Digital Signage player receives the video and displays it on a plasma or LCD screen. Output from the Digital Signage player can also be input to a VBrick encoder and delivered as one video stream over the network, allowing it to work with VEMS, VBrick reflectors, and VBoss (VBrick's Online Streaming Services). For more information see the *Digital Signage Quick Start Guide.*

Help

This command launches the VEMS Portal Server online help system in a new window. This online help system provide fast full-text search and makes it easy to find the information you need. To navigate in the help window, use the tree controls on the left to expand a topic and the navigation buttons at the top to move to a different page. Go to **About this Help > Using this Help** for information about how to Print pages and use the full text Search feature.

About

This page displays the Portal Server (VEMS) version number (for example 5.3) as well as license and serial number data for each installed module. The serial numbers provide warranty and tracking information. You may be asked for the module serial number when requesting help from VBrick Support Services.

License	Description	Serial Number
ETV VEMS	VEMS License Exists	12345678901234
ETV NVR	Record License Exists	12345678901234
ETV Schedule	Schedule License Exists	12345678901234
ETV Zones License	Zones License Exists	12345678901234
ETV Presentation License	Presentation License Exists	12345678901234
ETV Distribution Server	Distribution Server License Exists	12345678901234
ETV Channel Guide	Channel Guide License Exists	12345678901234
ETV Reporter		12345678901234
ETV Backup		12345678901234

Logout

This command logs you out of the application and lets you log back in as a different user. This may be necessary to gain access to certain functionality. For example, some users may not be allowed to create thumbnails and you may want to login as a user who has the permissions to do this.

Users and User Groups

Overview

Adding the Enterprise Media System to a network provides many benefits in the form of increasing access to rich media. However, because of the sensitive nature of some video assets, many customers want to limit access to different users or groups of users. VBrick's VEMS Portal Server allows Administrators to setup the system in just this manner. The VEMS Portal Server makes it easy to provide different Users or User Groups access to different resources. The VEMS Portal Server Access Control system allows administrators to allow/deny access to the Portal Server for Windows-based PCs, Macintoshes, and IP Receiver:

- Viewing of certain Live Channels
- Viewing of stored content from specific VOD folders
- Publishing content to specific VOD folders
- Recording content to a specific VOD folder
- Allow the viewing of content from only specific VOD servers on the network
- The ability to place bandwidth restrictions for viewing content
- The ability to limit certain users to only access Multicast or RTSP (unicast) content
- The ability to group content resources (Live Channels and/or VOD content) into Resource Groups, which allows the setup and modification of the Access Control functionality to take place much more easily.

The VEMS Portal Server is permissive by default, meaning, authentication is not enabled and access to the entire functionality of the server is allowed. However, to follow good security practices, once the Access Control functionality is enabled on the Portal Server, all resources are by default *not* available to any users. Administrators need to provide access to resources to different users or user groups.

User-Related Definitions

The ability to provide different users different access to resources on a network is typically referred to as access control, authentication and authorization, and/or access management. VBrick refers to this functionality as Access Control. In order to fully understand the range

of functionality of the VEMS Portal Server Access Control system, it is beneficial to define some of terms that are used in this section.

Authentication – Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization (see below), which is the process of providing individuals access to resources based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

The VEMS Portal Server Access Control system allows administrators to authenticate users against the VEMS Portal Server database or authenticate users against an LDAP directory. More details on the different authentication databases are given below.

Authorization – Authorization is the process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity. In the VEMS Portal Server, all authorization is done directly on the VEMS Portal Server, through the VEMS Portal Server database.

LDAP – LDAP (Lightweight Directory Access Protocol) is a set of protocols for accessing information directories. The LDAP standard defines both a network protocol for accessing information from the directory and an extensible structure for defining how the information is organized in the directory. The advantage of using an LDAP directory is centralized management of users. For example, a new user needs only to be entered once into the LDAP directory and all future modifications to that user can be done in the same central location. Different applications can authenticate and/or authorize users against the LDAP directory.

There are numerous LDAP directory products on the market today, but the most popular are Microsoft Active Directory, Novell eDirectory, Sun iPlanet, and OpenLDAP. *VBrick supports major LDAP vendors but only Microsoft Active Directory and Novell eDirectory are fully tested and supported.*

VBrick Database – The VEMS Portal Server server ships by default with the MySQL database, which is a fully ODBC-compliant database. (Open Database Connectivity is a standard database access method.) For those environments that have not migrated to an LDAP directory-based user management system, all of the authentication functionality can be done directly in the VEMS Portal Server database itself. Also, for those environments that are using LDAP directories for Authentication, all of the Authorization functionality also takes place in the VEMS Portal Server database. Additionally, to reduce the chance of system lockout, all Administrative Users are located in the VEMS Portal Server database.

Resources and Resource Groups – In the VEMS Portal Server, providing a user with Resources refers to providing them access to a particular functionality of the Enterprise Media System. These include the ability to view Live Channels, to view VOD content, to publish content to the VOD, and to record content or schedule a recording. A unique feature of the VEMS Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to specific Users or User Groups.

Configuring Users and User Groups

1. Setup and Configure VEMS Components

The following products need to be setup and properly configured prior to configuring Access Control.

VEMS Portal Server – The VEMS Portal Server needs to be properly setup and configured on the network. The following items should be configured in the Portal Server interface:

- If there is a VOD server(s) in the system, the proper addresses for these servers need to be entered into the Portal Server Administrative pages and connectivity to those servers should be ensured.

- The folder structure on the VOD server should be defined (even if there is no content in these folders) as folders are how the Access Control functionality provides access to end users to view VOD content, publish content, and record content. When setting up the folder structure, the Administrator should be thinking about how they plan to provide access to different groups of users. For example, if a corporation wanted to provide certain content to the Engineering group and certain content to the Marketing group, then they would want to set up an Engineering folder and a Marketing folder on their VOD server.

- If there are live streams on the network, then those streams should be provided a channel number if the Administrator wants to provide access to live streams via channel number.

- If security is a concern, SSL should be turned on between clients and the VEMS Portal Server server. This allows User Names and Passwords to be encrypted between the client and the server. See the section <u>Configuring for SSL</u> on page 147 for instructions on how to configure this.

VBrick – If there are VBricks in the network, they are auto-discovered but still need to be added to the Portal Server database.

VOD Server – If there are VOD servers in the network, again they need to have connectivity to the Portal Server and the folder structure needs to be configured.

IP Receivers – If there are IPRs to be deployed in the system, they should be configured with a Host Name, and should be configured to point to the VEMS Portal Server.

Additionally, if an LDAP server is going to be used to authenticate users, then the administrator should know the address of the server, the group structures on the LDAP server, and the Context (if the server is not Microsoft's Active Directory).

Note In order to scan the Groups available in Microsoft's Active Directory, in Windows Explorer, go to **Tools > Folder Options**. On the **General** tab, make sure that the **Show common tasks in folders** is selected. Then go to **Start > My Network Places** and select **Network Tasks > Search Active Directory**.

---

2. Choose an Authentication Method

Select one of the following methods:

VBrick Database	The native VEMS Portal Server user database provides local authentication for users and administrators.

LDAP Database	Enables the VEMS Portal Server to authenticate against, and retrieve user and group data from, an existing LDAP server.

Both methods can be used simultaneously. If LDAP authentication is enabled, the VEMS Portal Server will attempt to authenticate against the LDAP server first, and if this is unsuccessful, will attempt to authenticate against the local VEMS Portal Server User Database.

VBrick Database

If authentication is enabled, you must select a database (either VBrick or LDAP). The VBrick (VEMS Portal Server) user database contains user, group, and resource information that provides the Portal Server with information to allow it to provide the appropriate privileges to users and IP Receivers that are accessing the system. Administrators should authenticate users with the native Portal Server user database if:

- User authentication is required, but the organization does not have an LDAP server.
- For IPRs, the organization wishes to use User PINs. Since User PINs are not available in the LDAP directory, the users need to be created in the VEMS Portal Server database (Note: only those users that need PINs to access IPRs need to be created in the VEMS Portal Server database. PC or Mac users can still be authenticated against LDAP).

LDAP Directory Server

An LDAP directory server contains User and Group information which the VEMS Portal Server can authenticate against to verify User's identities. The Portal Server then uses this information to authorize users to access the system. Administrators should authenticate users with an LDAP Directory server if:

- The organization has an LDAP server that they actively manage to allow products to authenticate.
- The VEMS Portal Server administrator can obtain the necessary configuration information from the LDAP administrator to allow the authentication to occur.

Using LDAP reduces the amount of administrative time necessary to add and modify users from the VEMS Portal Server system. VBrick Systems encourages customers who have LDAP directories implemented to use them for authentication with the VEMS Portal Server.

3. Create User Groups on the Portal Server

Grouping users is common practice and makes administering access to the VEMS Portal Server less complicated than administering access by individual user. The VEMS Portal Server allows the administrator to create groups, specify group memberships for users, and set access privileges for the group. A user can be a member of one group or multiple groups. Group access privileges also can be set and modified on a per group basis. If an LDAP directory is being used for Authentication, the same group information that is available in the directory can be used to Authorize end users to access the VEMS Portal Server. For example, if the organization has three User Groups in its LDAP directory—Marketing, Engineering, and Sales—they can simply create these groups in the VEMS Portal Server system, and assign privileges to the groups.

4. Create Resource Groups on the Portal Server

In the Portal Server software, providing a user with Resources refers to providing them access to a particular functionality of the Enterprise Media System. These include the ability to:

• View Live Channels.

• View VOD content.

• Publish content to the VOD.

• Record content or schedule a recording.

• Launch a priority alert.

A unique feature of the Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to more than one User or User Groups. This also makes the ongoing management of this content for these Users or User Groups much easier. For example, if the organization has three User Groups—Marketing, Engineering, and Sales—they might create four resource groups. These Resource Groups would be Full Access, which are resources that everyone can see, and one Resource Group for each of the user groups. Full Access would be assigned to all user groups, and the Marketing Resource Group would be assigned to the Marketing User Group, the Engineering Resource Group to the Engineering User Group, and the Sales Resource Group to the Sales User Group.

Resource Groups provide the added bonus that they allow the Administrator to quickly provide access to new content to Users and User Groups. For example, if the organization originally had ten Live Channels on the network, and another Live Channel was added, the Administrator would simply need to add that Channel to the appropriate Resource Groups and the channel would be available.

5. Create Users on the VEMS Portal Server

Creating users is an optional step that can be completed for the following reasons.

• The organization needs to provide a single user with additional privileges above and beyond what is available to his or her User Group or Resource Group.

• The organization wants to authenticate IPR users using a PIN.

• Users can be assigned to multiple User Groups.

6. Assign Resources to Users or User Groups

The final step is to provide access to Resources to Users and/or User Groups. The administrator can assign individual resources to Users or User Groups, or can assign Resource Groups (if created) to Users or User Groups. Detailed information on the steps to configure access control and provide access to resources to Users and/or User Groups is provided in the following sections.

Configuring Users

There are several different ways to provide privileges to different User and User Groups with the VEMS Portal Server. The easiest way is to use the group structure of an existing LDAP database. LDAP User Groups can be added to the VEMS Portal Server system and assigned permissions (see User Groups below). All of the users in this group will have the same

permissions. For ease of implementation, VBrick recommends configuring User Groups and Resource Groups (see these sections below), prior to configuring users.

However, if further individual permissions need to be assigned, administrators can add them as a user. Under the users section, administrators have the ability to add, modify and delete users. Submit may be pressed at anytime during the process or can be done when everything has been added/modified. Users will have the permissions of the group as well as the additional permission that are assigned to them. The VEMS Portal Server is additive in its permissions, meaning that it takes all of the permissions that are provided to a particular user and provides all of these to the user.

Users can be added by using the VBrick Database if LDAP authentication is not available or desired. Finally, in order to assign user PINs to access IP Receivers, a user assignment is needed (see IPR Authentication section below). Note that IPR PIN access is dependent on the VBrick Database being enabled. See Access Control on page 117 for details.
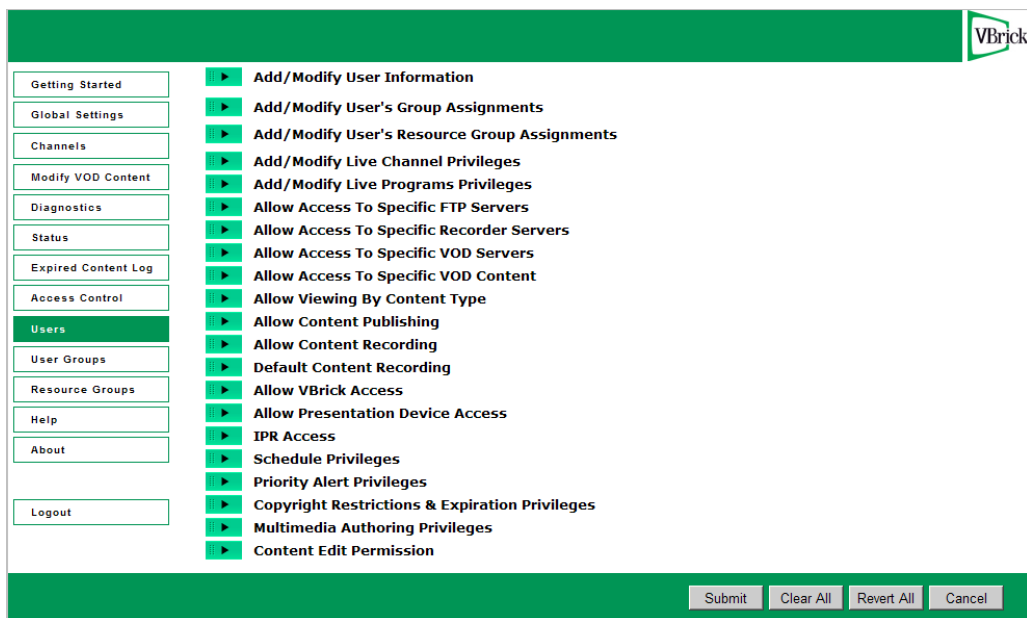
Submit	Save changes and/or navigate to the next window.
Add New	Takes the administrator to the Add New User, User Group, or Resource Group screen (depending on which section you are in)
Clear All	Clears any entries that have been entered in the individual sections.
Revert All	Returns all entries to the last state entered in the database. This selection is important if a mistake is made during entry.
Cancel	Cancels out of the page. Changes are not saved.
Clear	Clear eliminates or de-selects any entries in the particular section.
Revert	Returns the selection to the last state entered in the database. This selection is important if a mistake is made during entry.

Once all selections have been made, you can press **Submit** in the bottom right hand corner of the screen (or any of the other buttons shown above) to submit the information to the database. User privileges include the following options:

Add/Modify User Information

To add or modify users, select **Users** from the navigation bar on the left.

User	• User – Use this option if the Enterprise Media System will be accessed by a PC or Mac user, or if Users will be authenticated to IPRs via PIN numbers. This access is not limited to a specific PC or IPR. • IP Receiver – Use this option if the Enterprise Media System will be accessed via a IPR attached to a television or other video display. If IP Receiver is selected, then the privilege to the system will be on a per IPR basis. The authentication will take place automatically, so no end user interaction is required. When choosing IPR, the IPR's host name or IP address must be entered, as well as an optional location/description of the IPR.
Username	To authenticate using an LDAP database, the user name must match exactly what is in the LDAP database (the Portal Server is case sensitive). A new user can also be assigned (if using the VBrick database option) that does not exist in the LDAP database.
Password	For LDAP authentication a password is not needed (the user will use their normal network login password). If using the VBrick database a password must be entered (passwords are case sensitive). Passwords cannot exceed 31 characters.

IPR Pin	Optional. A PIN number can be assigned to a user that allows them to access their content from any IPR, regardless of the IPR's privilege level. This works well when an IPR is going to be a shared resource. Note: IPR PIN access is dependent on VBrick Database being enabled.
First Name	Optional. User first name.
Last Name	Optional. User last name.
E-mail address	Optional. User e-mail address.
Location	Optional. User location.

Assigning Privileges to Users

There are three ways to assign privileges to users:

- Assign the User to a User Group that has privileges assigned to it.
- Assign the User to a Resource Group that has privileges assigned to it.
- Individually assign resources to the User.

These methods all can be combined. For example, to provide a User with access to the resources provided to a User Group but also provide them access to additional resources, the administrator can a) Assign the User to that Resource Group and b) Individually assign the additional resources to that user. Each of these methods is discussed below.

Add/Modify User's Group Assignments

Users can be assigned to specific User Groups, and they will inherit the privileges of that group. If no User Groups appear, then none have been defined. Click User Groups in the main navigation to the left to create User Groups.

Add/Modify User's Resource Group Assignments

Users can be assigned to specific Resource Groups, and they will inherit the privileges of that Resource Group. If no Resource Groups appear, then none of been defined. Click Resource Groups in the main navigation to the left to create Resource Groups.

Add/Modify Live Channel Privileges

A "live channel" is a live stream that has been modified into a Custom station or a TV station and assigned a channel number. A list of available live channels will be displayed. A user can be provided access to all live channels or to individual live channels.

For live channels, both the Channel Number and the Station Name will appear in the Channel Guide. If the Channel number is selected, the VEMS Portal Server will always provide access to the particular channel (for example, Channel 1) even if the Program Name of that channel changes. If the Station Name is selected, the VEMS Portal Server will always provide access to the station (for example, CNN), even if the channel that it is associated with changes (for example, from Channel 2 to Channel 4).

Note The live streams shown in the Portal Server may also be restricted by a bit mask on a VBrick encoder. The Portal Server will parse the bitmask and send the live stream only to VEMS clients with a IP address that matches the masked IP of the source VBrick. You can use this feature in addition to the Portal Server authorization features. See the Category parameter in the MPEG, WM. or H.264 documentation for more information.

Add/Modify Live Program Privileges

"Live programs" are all live streams that are available. These are unmodified, unassociated streams. Use this option to restrict access to specific live streams.

Allow Access to Specific FTP Servers

Allow or deny access to defined FTP servers.

Allow Access to Specific Recorder Servers

Allow or deny access to defined recorder servers.

Allow Access to Specific VOD Servers

Choose from a list of available VOD server(s) to which a user has access. A user can have access to multiple servers. This feature is particularly useful when VOD servers are located in different physical locations that are separated by low bandwidth links. For example, if a company has offices and VOD servers in both New York and Chicago, and these offices are separated by a T-1 link, then they would want to limit the users in the Chicago office to the Chicago VOD server and those in New York to the New York VOD server.

Note When a user is provided access to particular VOD server(s), and they are given the privilege to Publish or Record to a particular folder, when they Publish or Record, the video will be Published or Recorded to each server that they have access to. This is important for clustering purposes.

Allow Access to Specific VOD Content

Choose from a list of folders to which a user can have access. A user can have access to multiple folders on multiple servers. If the user has access to multiple VOD servers, and the folder names are the same on both servers, only one folder name will show up in the list.

Allow Viewing by Content Type

The Administrator can limit the types of content that a user can view and/or limit the bandwidth that specific users can view. Note that this setting does not apply to URLs that were manually added by an administrator (see URLs on page 81).

Do Not Allow Multicast viewing	This will limit users that are on a non-multicast capable part of the network from trying to view multicast video.
Restrict Multicast to Kbps	This will limit users to only viewing multicast streams that are a certain size or smaller. This works well to maintain bandwidth utilization over a particular WAN port.

Do Not Allow RTSP viewing	This will limit users from viewing RTSP Unicast Streams from MPEG-4 Encoders and from accessing RTSP unicast streams from a Video-on-Demand server (MPEG-1, MPEG-2, or MPEG-4). This works well to maintain bandwidth utilization over a particular LAN or WAN port.
Restrict RSTP viewing to Kbps	This will limit users to only viewing RTSP streams that are a certain size or smaller. This works well to maintain bandwidth utilization over a particular LAN or WAN port.

Allow Content Publishing

Administrators can allow a user the ability to publish content to folder(s) on an VOD Video-On-Demand Server. This function allows the user access to the **Add Video** page, where users can add pre-recorded video content to a VOD. It also allows users to (1) create (and upload) **Thumbnails** for video files in the folders to which they can publish, to (2) delete video content from the VOD server, and (3) to add keyword tags and description data using the **Modify Info** button. To prevent users from deleting content, be sure this option is disabled.

Note If users are provided access to more than one VOD server, when they publish content, it will be published to each of the servers to which they have access. This is important for clustering purposes.

Allow Content Recording

Used for scheduled recording. Administrators can allow a user the ability to schedule the recording of live content to a specific folder(s) on a VOD Video-On-Demand Server. They cannot record content to any other folder(s). You must select a folder here to enable **Default Content Recording** below. If there is no schedule license, **Allow Content Recording** is not shown as an option and **Default Content Recording** lets you select any folder. If you add a schedule license later (using **Start > Control Panel > Add or Remove Programs)**, **Allow Content Recording** will be shown as an option with all folders selected. You may want to deselect specific folders in order to restrict recording privileges.

Default Content Recording

Used for on-demand recording. You must select a folder above for **Allow Content Recording** before you can make a folder selection here. Administrators can allow a user the ability to record live content to a specific default folder on an VOD Server by pressing the **Record** push button below the Preview Window. For ease of use, the Administrator can only assign one default folder where a particular user can record content. This allows one button recording on the VEMS Portal Server and is particularly important for IP Receiver users, who may not be able to enter a recording path with their IR remote control.

Allow VBrick Access

Administrators can allow a user the ability to access all VBricks or only specific VBricks when scheduling events. When scheduling an event, users will see only those VBricks for which they have been granted access.

Allow Presentation Device Access

Administrators can allow access to some or all defined presentation devices. Presentation devices are used to create live presentations using a variety of sources, for example VBrick's Rich Media Studio or a web-based presentation source.

IPR Access

Administrators can allow a user the ability to access all IPR or only specific IPR when scheduling events. When scheduling an event, users will see only those IPR for which they have been granted access.

Schedule Privileges

Users may have full, partial, or no permission to schedule VBrick event. Users with full privileges can modify all configuration parameters in a schedule. Users with partial privileges *cannot* modify **Advanced Settings**.

- Super – user can change all schedules.
- Full – user an change only "owned" schedules.
- Partial – user can change only "owned" schedules; no **Advanced** features.
- None – user cannot create schedules; no **Add** button shown on Scheduling page.

Priority Alert Privileges

Administrators can specify whether or not a user can launch Priority Alerts.

Copyright Restrictions & Expiration Privileges

Administrators can allow users to set Copyright Restrictions and Expiration Privileges when adding stored content or scheduling a recording. Note that copyright restrictions apply only to Portal Server-initiated playback sessions (and not, for example to direct RTSP requests to a VOD server).

Multimedia Authoring Privileges

"Presentations" is an optional module that requires a separate license and may not be available on your system. Even if you have this module, individual users may be restricted in the functions they can perform. 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.

- MultimediaAuthorSuper – user can create presentations and modify all presentations.
- MultimediaAuthorOn – user can create presentations and modify their own presentations.
- MultimediaAuthorOff – user cannot create or modify presentations.

Content Edit Permissions

In some specialized end-user environments, this option can be used to allow or deny access to certain administrative and content management features.

Configuring User Groups

Grouping users is common practice and makes administering access to the VEMS Portal Server less complicated than administering access by individual user. The VEMS Portal Server server allows the administrator to create User Groups, specify group memberships for users, and set access privileges for the group. A user can be a member of one group or multiple groups. Group access privileges also can be set and modified on a per group basis.

If an LDAP directory is being used for Authentication, the same group information that is available in the directory can be used to Authorize end users to access the VEMS Portal Server. For example, if the organization has three User Groups in its LDAP directory—Marketing, Engineering, and Sales—they can simply create these groups in the VEMS Portal Server system, and assign privileges to the groups.

Note Microsoft Active Directory. VEMS does not currently support "Primary Group" memberships (such as "Domain Users"). You must use a custom-defined Active Directory group.

Add/Modify Group Information

Use the "Default" group parameter to define base permissions for *all* Portal Server users. If checked, all defined Portal Server users will have the permissions defined by the remaining parameters on this page. If not checked, you can enter a specific group name, and all members of the specified group will have the permissions defined on this page.

If LDAP is being used for authentication, then the group name has to exactly match the group name in the LDAP directory. If LDAP is not being used, Group Names can be entered directly into the VEMS Portal Server database. If Microsoft's Active Directory is used, to find the available list of active groups in **Windows XP**, browse to **My Network Places** and click on the left-hand menu **Search Active Directory**. A new window will open. Click **Find now** to see all available groups. In **Windows 2000**, go to **My Network Places > Entire Network > Directory**, the domain, and **Users**.

Note Windows XP needs to be configured to **Show Common Tasks in Folders**. To configure this, in **My Network Places**, go to **Tools > Folder Options**. In the **General > Tasks** section, select the radio button called **Show common tasks in folders**.

Add/Modify Group's User Assignments

Users can be assigned to specific User Groups, and they will inherit the privileges of that group. If no Users appear, then none have been defined. However, if LDAP is being used for Authentication, no users need to be defined. When a user Authenticates to the system, the Authentication process will return the User's group information. The user will receive the privileges that are provided to that group.

Add/Modify Group's Resource Assignments

Resource groups can be assigned to User Groups, and the User Group will inherit the privileges of that Resource Group. If no Resource Groups appear, then none of been defined. Click **Resource Groups** in the main navigation to the left to create Resource Groups.

Note The remaining options for **User Groups** (beginning with **Add/Modify Live Channel Privileges**) are the same as those described earlier for individual <u>Configuring Users</u> on page 135. The only difference is that the descriptions will apply to groups of users rather than to individual users.

Resource Groups

In the VEMS Portal Server software, providing a user with Resources refers to providing them access to a particular functionality of the Enterprise Media System. These include the ability to view Live Channels, to view VOD content, to publish content to the VOD, and to record content. A unique feature of the VEMS Portal Server software is the ability to group Resources into Resource Groups. This allows the administrator to quickly and easily assign several resources at once to more than one User or User Groups. This also makes the ongoing management of this content for these Users or User Groups much easier.
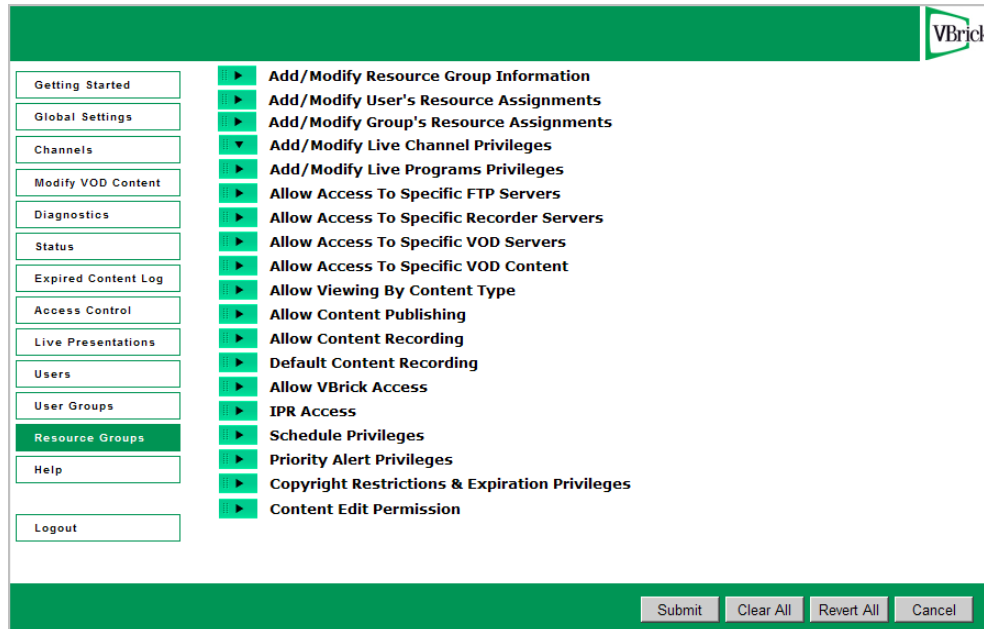
For example, if the organization has three User Groups—Marketing, Engineering, and Sales—they might create four resource groups. These Resource Groups would be Full Access, which are resources that everyone can see, and one Resource Group for each of the user groups. Full Access would be assigned to each user group, and the Marketing Resource Group would be assigned to the Marketing User Group, the Engineering Resource Group to the Engineering User Group, and the Sales Resource Group to the Sales User Group. Resource Groups provide the added bonus that they allow the Administrator to quickly provide access to new content to Users and User Groups. For example, if the organization originally had ten Live Channels on the network, and another Live Channel was added, the Administrator would simply need to add that Channel to the appropriate Resource Groups and the channel would be available.

Add/Modify Resource Group Information

Add the Resource Group Name that is relevant for the Resource Group being created.

Add/Modify User's Resource Assignments

Users can be assigned to specific Resource Groups, and they will inherit the privileges of that Resource Group. If no Users appear, then none have been defined. Click on the Users section to add Users.

Add/Modify Group's Resource Assignments

User Groups can be assigned to Resource Groups, and the User Group will inherit the privileges of that Resource Group. If no User Groups appear, then none have been defined. Click User Groups in the main navigation to the left to create User Groups.

Note   The remaining options for **Resource Groups** (beginning with **Add/Modify Live Channel Privileges**) are the same as those described earlier for individual Configuring Users on page 135. The only difference is that the descriptions will apply to resource groups rather than to individual users.

IPR Authentication

There are two ways (IPR IP address or user PIN) to authenticate and authorize IP Receivers in the VEMS Portal Server. IPR access control is slightly different from PC and Macintosh-based authentication (which uses the commonly employed User Name and Password mechanism). The two methods are outlined in the table below.

Table 17. Authentication Methods

Method	Description	User Interaction	Comment
User PIN	If Access Control is enabled, but the IPR is not defined in the system, then Access Control works based on a user PIN. This PIN is defined on a *per user* (not per IPR) basis, so that users need to be defined for this to work.	When the user logs into the system, they will be prompted for their PIN. The user simply enters the PIN with the remote control or the wireless keyboard, and can then access the video.	This implementation is appropriate for environments where multiple users with different privileges will be accessing the same IPR. An example of this would be a shared classroom where multiple teachers are accessing the IPR at different times.
IPR IP Address or Host Name	The VEMS Portal Server system determines the content that the IPR can view based on its IP Address or Host Name.	No user interaction is required. The user simply turns on the IPR and only the content that the IPR user can view id displayed.	This implementation is similar to a cable TV setup, e.g. if the cable plan does not include CNN, that channel cannot be viewed. This implementation is easiest for end users because you do not have to remember user names or PINs. It is appropriate for environments where one or a few people with the same privileges access the same IPR.

Authentication by PIN

When an end user accesses the VEMS Portal Server via a IPR, the Portal Server takes the following steps to authorize users.

1. It determines if there is Authentication/Authorization information associated with the Host Name of the IPR. If so, based on the IPR Host Name, the VEMS Portal Server will present the IPR with the information appropriate to its privileges. Note that the VEMS Portal Server uses the least restrictive settings when providing access to the system.

2. If there is no Authentication/Authorization information associated with the Host Name of the IPR, the user will be prompted for a PIN. A PIN is a user-based mechanism to log onto the IPR. When the user enters his or her PIN, the VEMS Portal Server authenticates the user against the Portal Server database.

3. Once the user is authenticated, the VEMS Portal Server will check the User Groups and/or Resource Groups that the User is associated with and the privileges associated with those groups.

4. After checking the Groups privileges, the VEMS Portal Server will check for any individual user privileges above the group privileges.

5. The user will be presented with the information appropriate to their privileges. Note that the VEMS Portal Server uses the least restrictive settings when providing access to the system.

If Authentication and Authorization is enabled, but the IPR is not defined in the system, then Access Management works based on a User PIN. This PIN is defined on a **per user** (not per IPR) basis, so Users need to be setup in the system for this to work. When the user accesses the VEMS Portal Server through the IPR, they will be prompted for their PIN. The user simply enters the PIN with the remote control or the wireless keyboard, and can then access the video for which they have privilege. This implementation is appropriate for environments where multiple users with different privileges will be accessing the same IPR. An example of this would be a shared classroom, where multiple teachers are accessing the IPR at different times.

Authentication by Host Name or IP Address

The VEMS Portal Server determines the content that the IPR can view based on its IP Address or Host Name. No user interaction is required. The user simply turns on the IPR, and only the content that the IPR user can view displays. This implementation is similar to a Cable Television setup—for example, if the plan does not include HBO, then that channel cannot be viewed. This implementation is easiest from the end user perspective because end users do not have to remember user names or PINs. This implementation is appropriate for environments where multiple people can access the same IPR.

Configuring for SSL

Overview

Secure Sockets Layer (SSL) provides endpoint authentication and communications privacy over the Internet using cryptography. Whenever there is a concern regarding confidentially and integrity of *management* data being sent between VEMS Portal Server and external clients, the VEMS Portal Server should be configured with a digital X.509 certificate to enable SSL encryption. When SSL encryption is enabled, the Portal Server encrypts either all pages in the Portal Server Admin and client applications (see Configure Hardened SSL) or all of the Portal Server Admin pages but only the Portal Server client *login page* (see Configure Non-Hardened SSL).

It is important to note that only the management data (for example user requests or configuration data) is encrypted. *The actual video streams are never encrypted.* When SSL is enabled, the following elements can be encrypted:

- MCS Admin Console – All MCS Admin Console pages can be encrypted to protect management information and other sensitive data.
- MCS User Portal – All Portal Server client pages can be encrypted (hardened SSL) or only the login page can be encrypted (non-hardened SSL).
- LDAP Server – If using LDAP authentication, communications between the Portal Server and the LDAP Server can be encrypted by enabling encryption on the LDAP server.
- VOD-W Server – Communication between the Portal Server and a VOD-W server can be encrypted by enabling SSL on the VOD-W server. See "Secure Communication" in the *VOD-W Server Release Notes*.

By convention, URLs that require an SSL connection start with `https` instead of `http`. The steps briefly listed here, and explained in detail on the following pages, explain how to set up and use SSL on the Portal Server.

▼   To set up SSL for client access to the VEMS Portal Server

1. Generate a Certificate Request.
2. Submit a Certificate Request.
3. Install the Certificate on the VEMS Portal Server.
4. Configure VEMS Resources for SSL.

SSL Prerequisites

- In order to use the Portal Server in secure (HTTPS) mode, you must have a signed and valid SSL certificate purchased from Verisign or another vendor. If the certificate is not signed, or if it is expired or otherwise invalid, video playback issues will occur.

- In an environment where the Portal Server is using SSL and a Network Video Recorder (NVR) is running on a separate server, the NVR server must also have an SSL Certificate installed in its IIS configuration or all NVR recording will fail.

- Be aware that hardened SSL encryption requires significant resources and can substantially impact performance. Use hardened SSL only when absolutely necessary in environments that require all pages to be encrypted.

- To use SSL, Amino set top box users must purchase a digital X.509 certificate from Verisign. Other certificates may work but Verisign is the only certificate currently tested and supported by VBrick.

Configuring SSL (Windows Server 2003)

1. Generate a Certificate Request

If your company does not have a X.509 certificate, or does not have one for the VEMS Portal Server, a new certificate request must first be created.

▼ To generate a certificate request:

1. From the VEMS Portal Server, start the Microsoft Internet Information Services (IIS) Manager.

2. Expand the server name and select the web site for which the certificate will be installed.

3. Right-click the web site, and then click **Properties**.

4. Select the **Directory Security** tab.

5. Select the **Server Certificate** button within **Secure** communications to launch the Web Server Certificate Wizard.

6. Select **Next** on the Welcome dialog box.

7. Select **Create a New Certificate** and then select **Next**. (If **Create a New Certificate** is unavailable, the certificate has probably been installed already. If that is the case, skip the rest of the steps, and go to Step 4. Configure Portal Server Resources for SSL. If you want to create new certificate for VEMS Portal Server, select **Remove the current certificate** to remove the certificate first, and then restart the procedure.)

8. Select **Prepare the request now, but send it later** and then select **Next**.

9. Type a descriptive name for the certificate in the **Name** field, type a bit length for the key in the **Bit length** field, and then select **Next**.

10. Type an organization name (e.g. VBrick) in the **Organization** field and type an organizational unit (such as Sales Department) in the **Organizational unit** field, and select **Next**. (This information will be placed in the certificate request, so make sure it is accurate. The Certificate Authority will verify this information and will place it in the certificate. A user browsing the VEMS Portal Server will want to see this information in order to decide if they should accept the certificate.)

11. In the **Common name** field, type a common name, and then select **Next**. (**Important:** The common name is one of the most significant pieces of information that ends up in the certificate.)

12. Enter the appropriate information in the **Country/Region**, **State/Province**, and **City/locality** fields, and then select **Next**.

13. Enter a file name for the certificate request. The file contains information similar to the following:

```
------BEGIN NEW CERTIFICATE REQUEST ------
MIIDZjCCAs………
------END NEW CERTIFICATE REQUEST ---------
```

This is a Base 64 encoded representation of the certificate request. The request contains the information entered into the wizard and also your public key and information signed with your private key.

14. Select **Next**. The wizard displays a summary of the information contained in the certificate request.

15. Select **Next** and select **Finish** to complete the request process.

2. Submit a Certificate Request

If a CA-signed Certificate from a trusted Certificate Authority (such as <u>VeriSign</u> or <u>Thawte</u>) is going to be purchased, the certificate can now be sent to a CA for verification and processing. After the certificate response is received from the CA, the installation process can continue on the VEMS Portal Server. Purchasing a CA-signed certificate will cause a security alert in the browser upon access to the server.

3. Install the Certificate

▼ To install the certificate on the VEMS Portal Server:

1. Start the Microsoft Internet Information Service (IIS) Manager.

2. Expand the server name and select the web site for which the certificate will be installed.

3. Right-click the web site and then select **Properties**.

4. Select the **Directory Security** tab

5. Select **Server Certificate** to launch the Web Server Certificate Wizard

6. Select **Process the pending request and install the certificate** and then click **Next**.

7. Enter the path and file name of the file that contains the response from the CA, and then click **Next**.

8. Examine the certificate overview, click **Next**, and then click **Finish**. A certificate is now installed on the VEMS Portal Server.

4. Configure Portal Server Resources for SSL

After installing the certificate on the VEMS Portal Server, the VEMS Portal Server can now be configured for SSL. As explained below, the Portal Server supports two different modes for SSL security:

- **Hardened SSL** – All pages in the Portal Server Admin and Portal Server client applications are secured with SSL. Users will see the padlock icon at the bottom of the screen on all pages.

- **Non-Hardened SSL** – All pages in the Portal Server Admin application; only the Portal Server client login page is secured.

Note You must select one and only one of these modes for configuring the Portal Server. The application cannot run with both modes enabled and attempting to do so will result in an application error.

Configure Hardened SSL

In hardened SSL mode, the Portal Server encrypts all pages in the Portal Server Admin application and all pages in the Portal Server client application. **Be aware that hardened SSL encryption requires significant resources and can substantially impact performance.** Use hardened SSL only when absolutely necessary in environments that require all pages to be encrypted.

Note If you are using the Portal Server in hardened SSL mode, your (Digital) Set Top Box(es) will not function unless you upgrade to STB v3.74b or greater. A popup window will alert you that an upgrade is available when first logging in. If you have Gold or Platinum warranty support, the upgrade is free: use the <u>Online Customer Service</u> page to contact Support Services. If you do not have warranty support, use the <u>Products</u> page to contact Sales representative. **If you are not using hardened SSL, there is no need to upgrade your Set Top Boxes.**

▼ To configure the Portal Server in Hardened SSL Mode:

1. Login to the Windows Server that is hosting the VEMS Portal Server application with a valid local Windows administrator account or domain account with local administrative permissions.

2. Launch the Internet Information Services Manager. Go to Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.

3. Locate your server name in the tree control on the left and click the plus sign (+) to expand the node.

4. Locate the node titled **Web Sites** and click the plus sign (+) next to it to expand the node. Your screen should look similar to this:
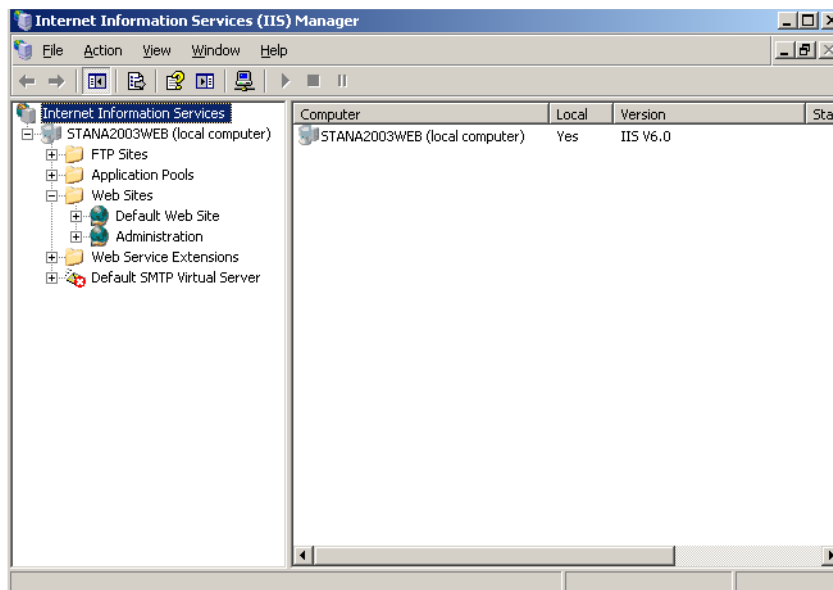
5. Right-click the **Default Web Site** node and click **Properties**.

6. Select the **Directory Security** tab. Your screen should look similar to this:
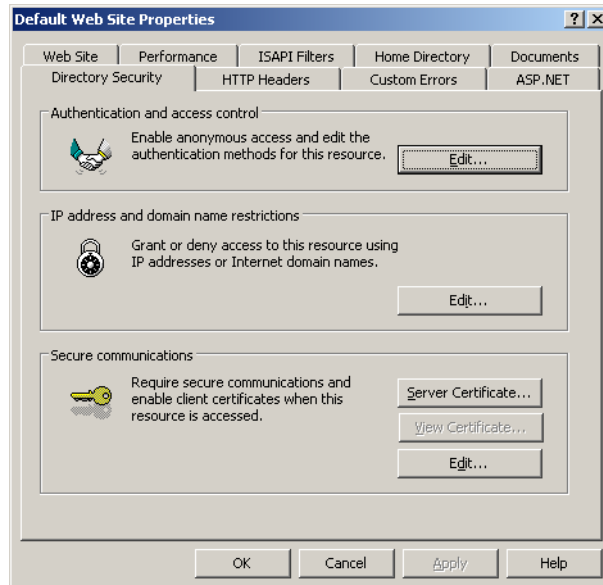
7. Go to **Secure communications** and click **Edit**.

8. Check the box marked **Require secure channel (SSL)** and click **OK**.
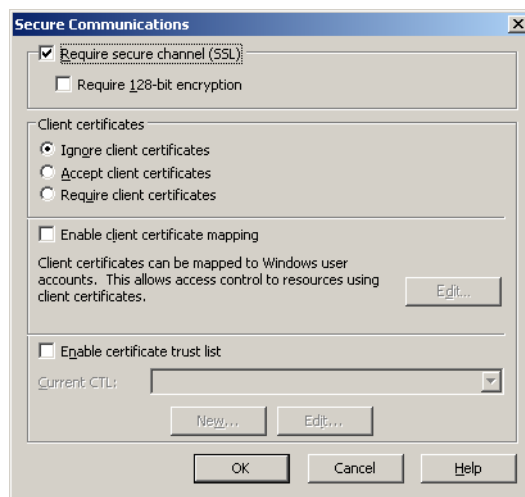
9. Click **OK** to close the **Default Web Site Properties** page.

10. Click the plus sign (+) in the tree next to **Default Web Site** to expand the node. Your screen should look similar to this:
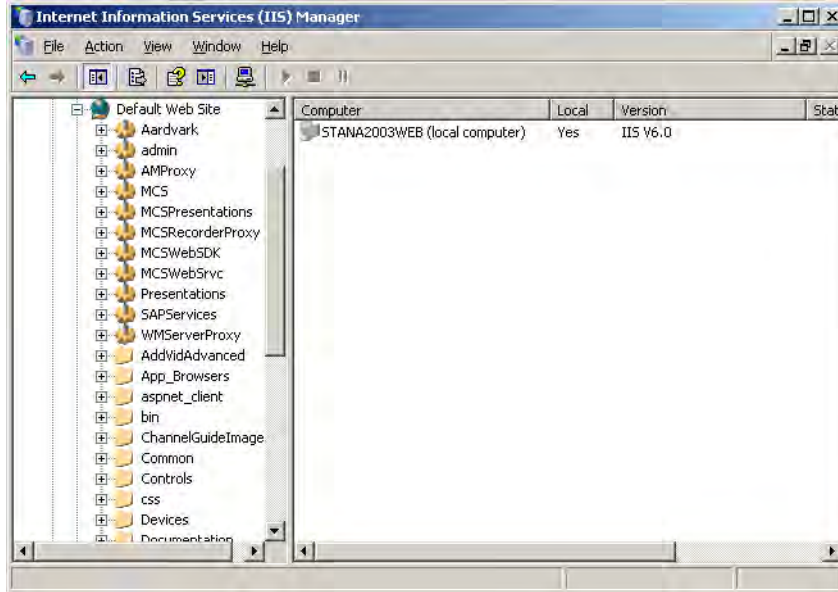
11. Right-click on **AMProxy** and select **Properties**.

12. Select the **Directory Security** tab, then go to **Secure communications** and click **Edit**.

13. Uncheck the box marked **Require secure channel (SSL)** and click **OK**.
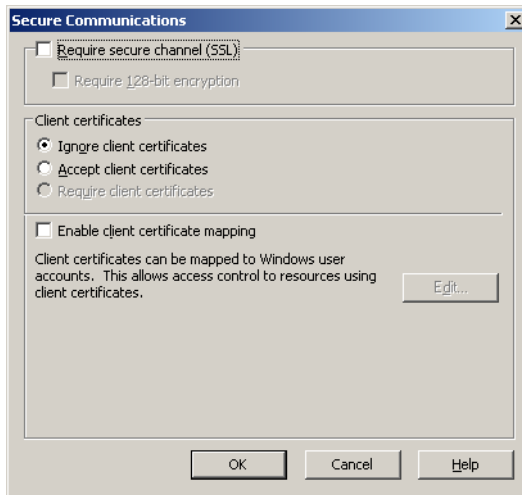
14. **Restart the Windows Server**.

After restarting the server, your users will be able to access the VEMS Portal Server application. From this point forward, users must use an **HTTPS** URL to access the application, for example: **https**://<server_ip_address>. Be sure to update all bookmarks and stored links to reflect this address change.

Configure Non-Hardened SSL

In non-hardened SSL mode, the Portal Server encrypts all of the Portal Server Admin pages but only the Portal Server client *login page*. Configuring non-hardened SSL is a two-step process: (1) first you configure the Portal Server user login page for SSL access, and (2) configure the Portal Server Admin pages for secure SSL access. This means that when a user attempts to access the Portal Server user pages it will automatically bring them to **https://**

`<ipaddressofserver>` for the user pages. Users will notice a padlock icon at the bottom of their screen while logging into the Portal Server, however the padlock will disappear once they login. When an administrator attempts to access the Administration pages it will also force them to use `https://<ipaddressofserver>/admin`. The padlock icon will be visible at the throughout the entire Admin site.

▼ **To secure the Portal Server User Pages:**

1. Go to the Portal Server install location, typically `C:\Program Files\VBrick\MCS` and open `web.config` in a text editor.

2. Uncomment the sections labeled Web Page Security 1, 2, and 3 **by deleting only the <!-- and --> characters shown below in red.**

Web Page Security 1

```
<!-- Web Page Security 1: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<section name="secureWebPages"
type="Hyper.Web.Security.SecureWebPageSectionHandler, WebPageSecurity"
allowLocation="false" />
-->
```

Web Page Security 2

```
<!-- Web Page Security 2: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<secureWebPages mode="On" maintainPath="False" warningBypassMode="AlwaysBypass"
bypassQueryParamName="BypassSecurityWarning">
<file path="login.aspx" /> <file path="login4.aspx" /> </secureWebPages>
-->
```

Web Page Security 3

```
<!-- Web Page Security 3: Remove comments around the following section to enable
SSL on the login page. -->
<!--
<add name="SecureWebPage" type="Hyper.Web.Security.SecureWebPageModule,
WebPageSecurity" />
-->
```

▼ **To secure the Portal Server Admin pages:**

1. Go the Admin Console location, typically `C:\Program Files\VBrick\MCS\Common\MCS Admin Console` and open `web.config` in a text editor.

2. Uncomment the sections labeled `Web Page Security 1` and `Web Page Security 2` **by deleting only the <!-- and --> characters shown below in red.**

Web Security 1

```
<!-- Web Page Security 1: Remove comments around the following section to enable
SSL on all Admin Console pages. -->
<!--
<section name="secureWebPages"
type="Hyper.Web.Security.SecureWebPageSectionHandler, WebPageSecurity"
allowLocation="false" />
-->
```

Web Security 2

```
<!-- Web Page Security 2: Remove comments around the following section to enable
SSL on all Admin Console pages. -->
<!--
<secureWebPages mode="On" maintainPath="False" warningBypassMode="AlwaysBypass"
bypassQueryParamName="BypassSecurityWarning">
<directory path="/" recurse="True" />
</secureWebPages>
-->
```

Configuring SSL (Windows Server 2008)

1. Generate a Certificate Request

If your company does not have a X.509 certificate, or does not have one for the Portal Server, a new certificate request must first be created.

▼ To generate a certificate request:

1. From the Portal Server, start the Microsoft Internet Information Services (IIS) Manager.
2. Click the server name and double click **Server Certificates** in the pane on the right side.
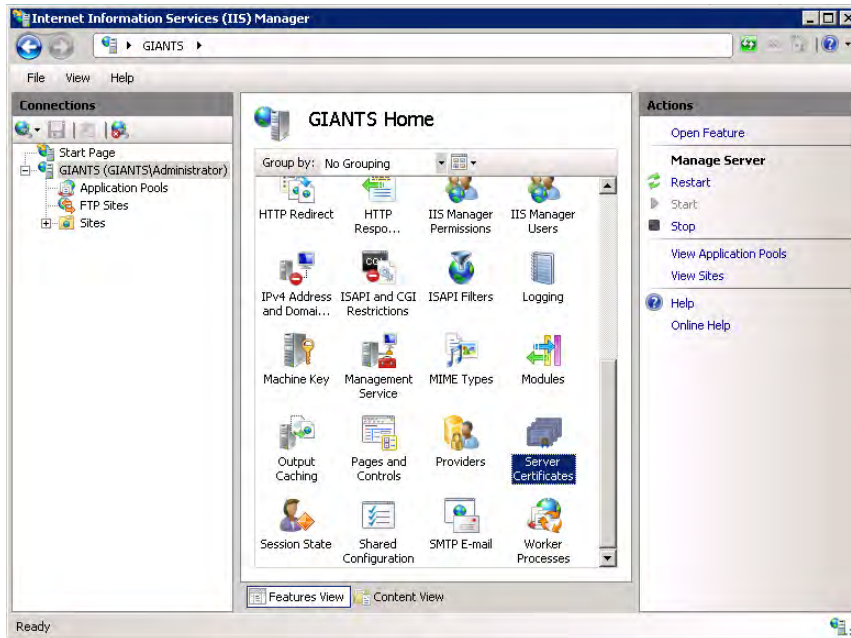
3. In the Actions column on the right, click **Create Certificate Request**.
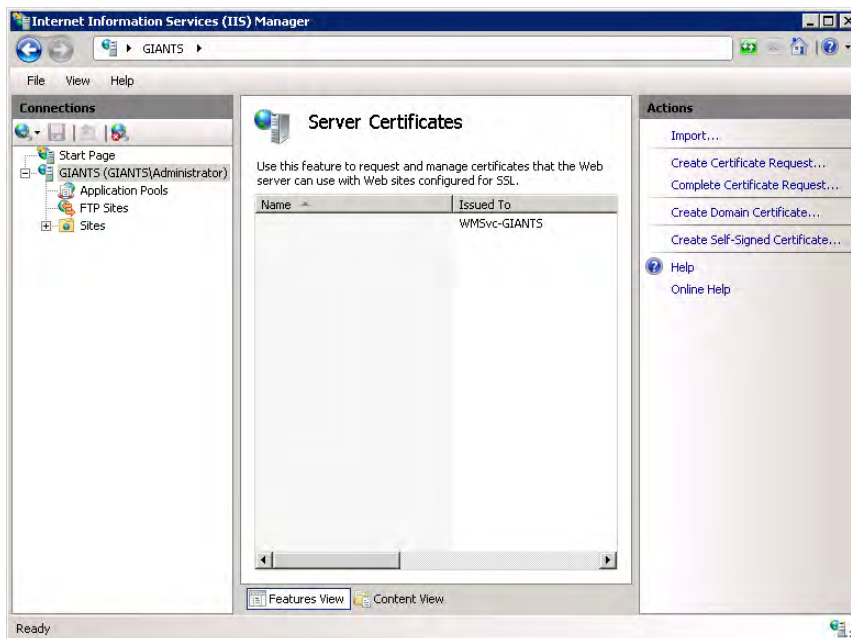
4. Type an organization name (e.g. VBrick) in the **Organization** field and type an organizational unit (such as Sales Department) in the **Organizational unit** field. (This information will be placed in the certificate request, so make sure it is accurate. The Certificate Authority will verify this information and will place it in the certificate. A user browsing the Portal Server will want to see this information in order to decide if they should accept the certificate.)

5. In the **Common name** field, type a common name, and then select **Next**. (**Important:** The common name is one of the most significant pieces of information that ends up in the certificate.)

6. Enter the appropriate information in the **Country/Region**, **State/Province**, and **City/locality** fields, and then select **Next**.

7. Select a **Cryptographic Service Provider** and **Bit Length** and click **Next**.

8. Enter a file name for the certificate request. The file contains information similar to the following:

```
------BEGIN NEW CERTIFICATE REQUEST ------
MIIDZjCCAs………
------END NEW CERTIFICATE REQUEST ---------
```

This is a Base 64 encoded representation of the certificate request. The request contains the information entered into the wizard and also your public key and information signed with your private key.
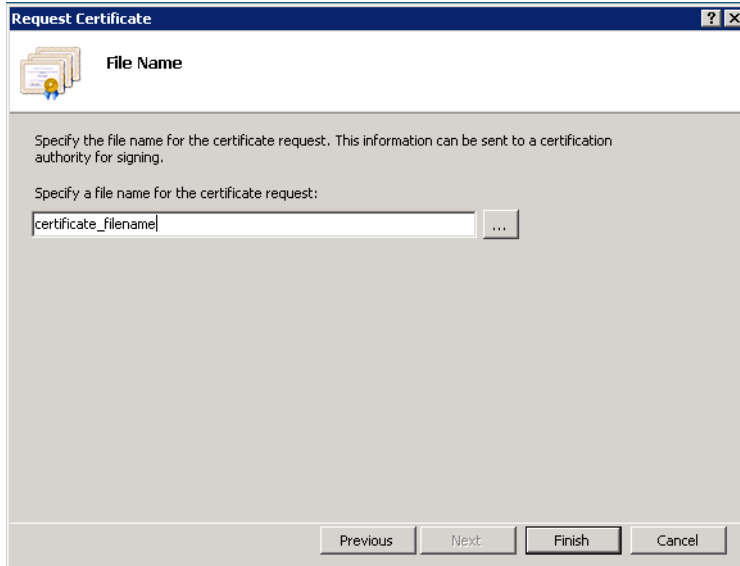
9. Select **Next**. The wizard displays a summary of the information contained in the certificate request.

10. Select **Next** and select **Finish** to complete the request process.

2. Submit a Certificate Request

If a CA-signed Certificate from a trusted Certificate Authority (such as <u>VeriSign</u> or <u>Thawte</u>) is going to be purchased, the certificate can now be sent to a CA for verification and processing. After the certificate response is received from the CA, the installation process can continue on the Portal Server. Purchasing a CA-signed certificate will cause a security alert in the browser upon access to the server.

3. Install the Certificate

▼   To install the certificate on the VEMS Portal Server:

1. Click on Start > Administrative Tools > Internet Information Services (IIS) Manager.

2. Click on the server name in the **Connections** column on the left. Double-click on **Server Certificates**.

© 2010 VBrick Systems, Inc.
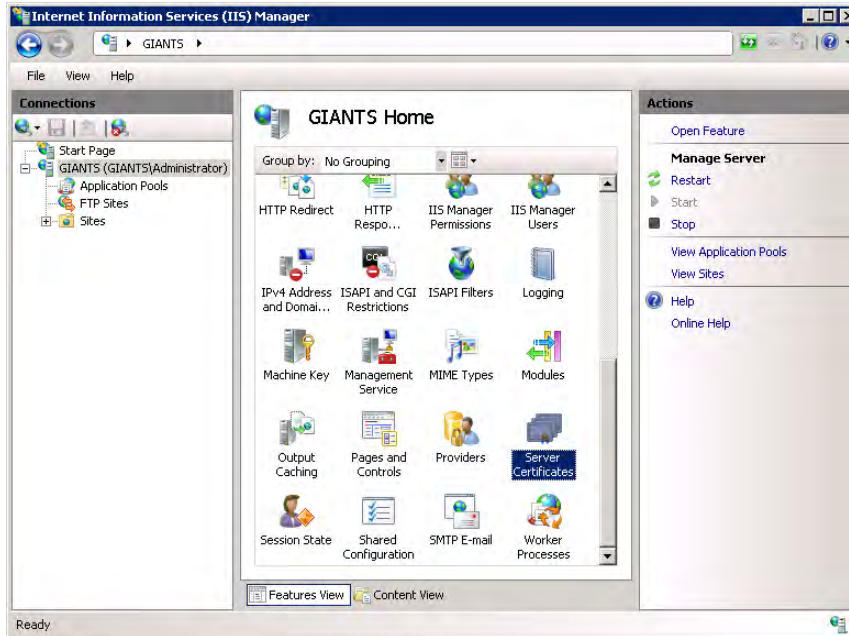
3. In the Actions column on the right, click on **Complete Certificate Request ...**
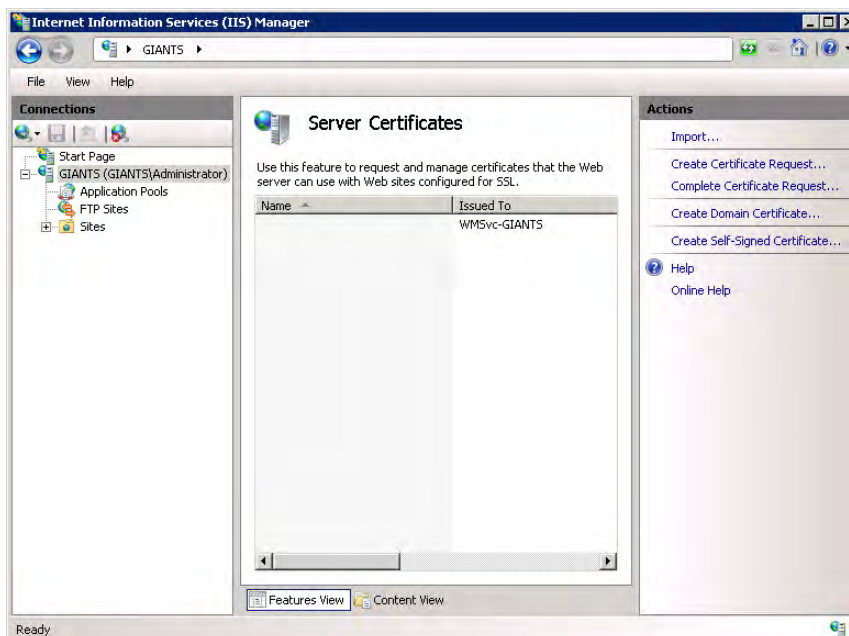
4. Click the button with the three dots and select the server certificate you received from the certificate authority. If the certificate does not have a .cer file extension, select to view all types. Enter a user-friendly name in order to track the certificate on this server. Click **OK** when done.
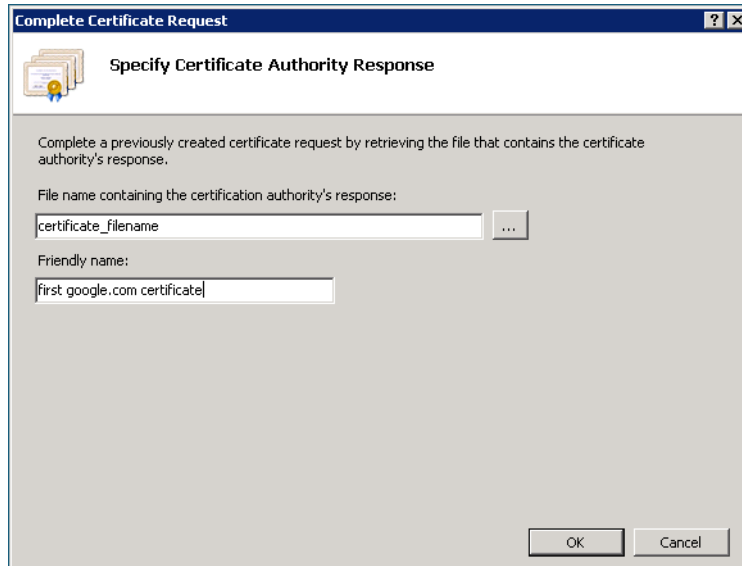
5. If successful, you will see your newly installed certificate in the list. If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate. Contact your certificate authority if you have problems.

6. Examine the certificate overview, click **Next**, and the click **Finish**. A certificate is now installed on the VEMS Portal Server.

4. Configure Portal Server Resources for SSL

After installing the certificate on the Portal Server, the Portal Server can now be configured for SSL. As explained below, the Portal Server supports two different modes for SSL security:

- **Hardened SSL** – All pages in the Portal Server Admin and Portal Server client applications are secured with SSL. Users will see the padlock icon at the bottom of the screen on all pages.
- **Non-Hardened SSL** – All pages in the Portal Server Admin application; only the Portal Server client login page is secured.

Note **You must select one and only one of these modes for configuring the Portal Server.** The application cannot run with both modes enabled and attempting to do so will result in an application error.

Configure Hardened SSL

In hardened SSL mode, the Portal Server encrypts all pages in the Portal Server Admin application and all pages in the Portal Server client application. **Be aware that hardened SSL encryption requires significant resources and can substantially impact performance.** Use hardened SSL only when absolutely necessary in environments that require all pages to be encrypted.

Note If you are using the Portal Server in hardened SSL mode, your (Digital) Set Top Box(es) will not function unless you upgrade to STB v3.74b or greater. A popup window will alert you that an upgrade is available when first logging in. If you have Gold or Platinum warranty support, the upgrade is free: use the Online Customer Service page to contact Support Services. If you do not have warranty support, use the Products page to contact Sales representative. **If you are not using hardened SSL, there is no need to upgrade your Set Top Boxes.**

▼ To configure the Portal Server in Hardened SSL Mode:

1. Login to the Windows Server that is hosting the VEMS Portal Server application with a valid local Windows administrator account or domain account with local administrative permissions.
2. Launch the Internet Information Services Manager. Go to Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
3. Locate your server name in the tree control on the left and click the plus sign (+) to expand the node.
4. Locate the node titled **Sites** and click the plus sign (+) to expand the node.
5. Select the **Default Web Site** node. Your screen should look similar to this:
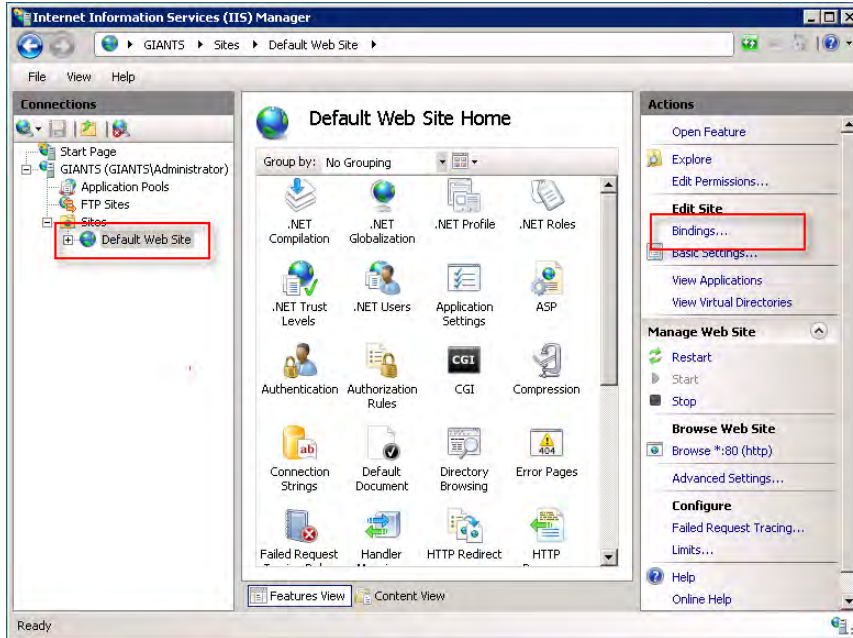
6. Click on **Bindings** in the right column and then click the **Add** button.
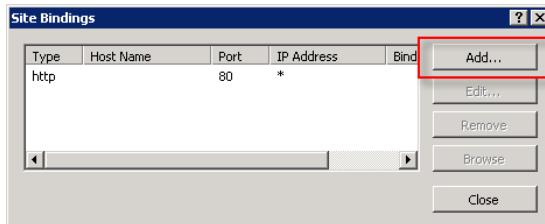
7. Change the **Type** to https. Then select the SSL certificate you just installed and click **OK**.
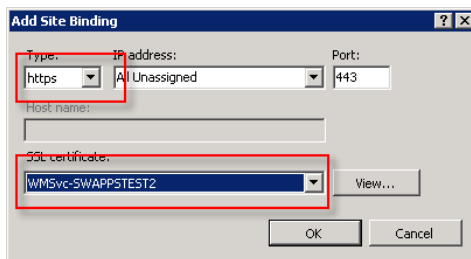
8. You will now see the binding for Port 443 listed. Click **Close**.
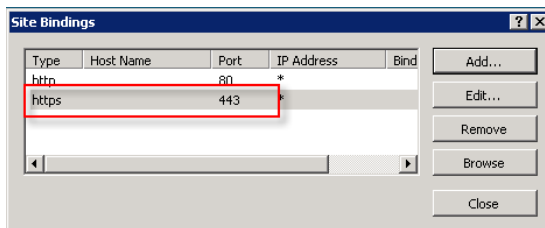
9. Double-click the **SSL Settings** button.
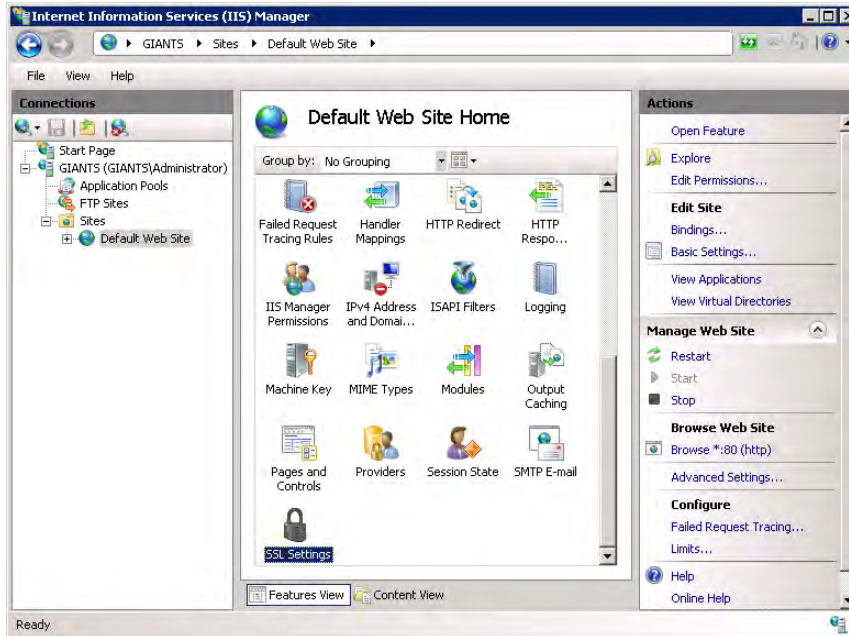
10. Select **Require SSL** and click **Apply**.
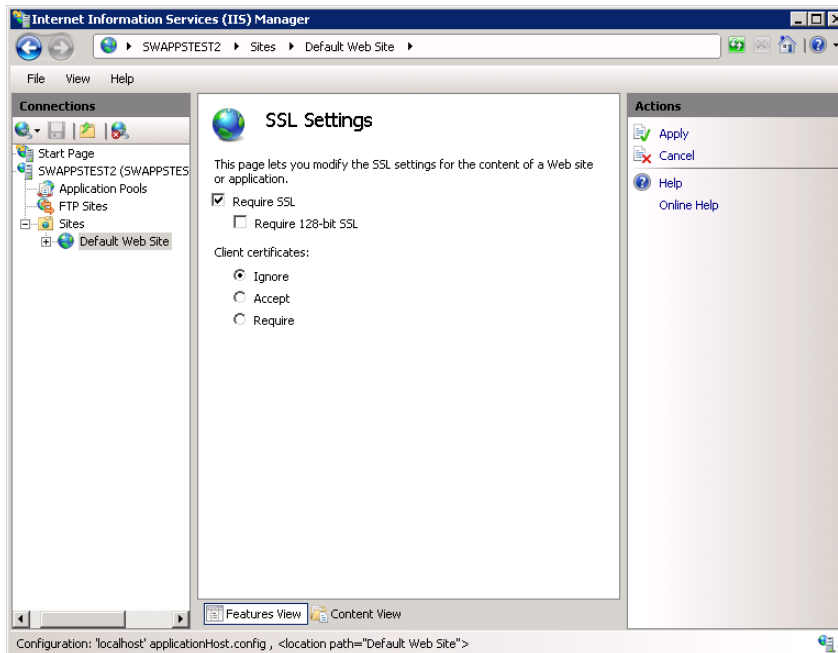
11. Click on **AMProxy** in the tree control on the left, and then double-click on **SSL Settings**.

12. Uncheck the box marked **Require SSL** and click **Apply**.
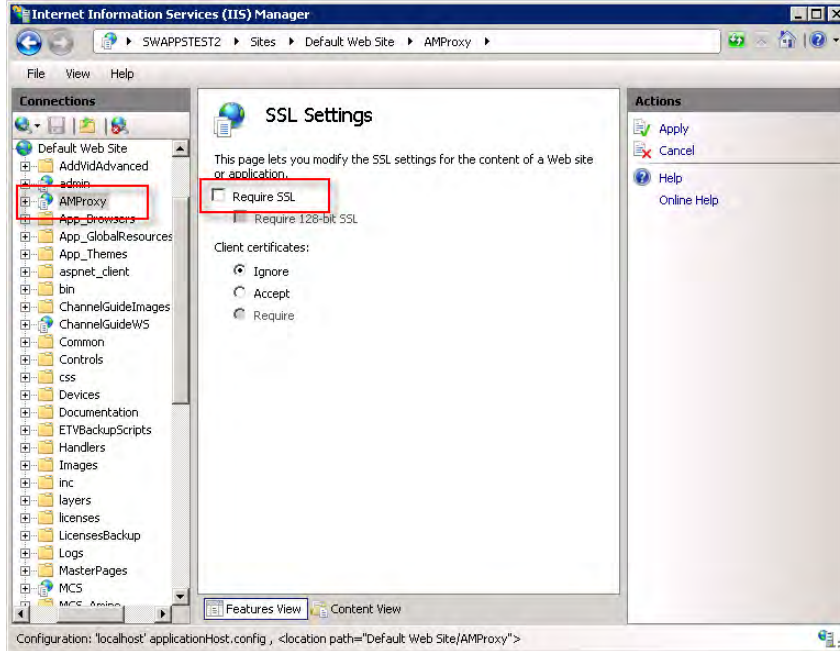
13. Restart the Windows Server.

After restarting the server, your users will be able to access the Portal Server application. From this point forward, users must use an **HTTPS** URL to access the application, for example: **https**://**<server_ip_address>**. Be sure to update all bookmarks and stored links to reflect this address change.

Configure Non-Hardened SSL

This procedure is the same for Windows Server 2003 and Windows Server 2008 with one exception. If you are configuring non-hardened SSL on Windows Server 2008, you will need to verify that the server is configured for HTTPS as explained below. When done go to Configure Non-Hardened SSL on page 152.

▼ To configure Windows Server 2008 for HTTPS:

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

2. Expand the left navigation tree on the left and highlight the **Default Website**.

3. Examine the **Browse Web Site** box on right side of page.

4. If **Browse *:443 (https)** is listed you are done. Go to Configure Non-Hardened SSL on page 152.
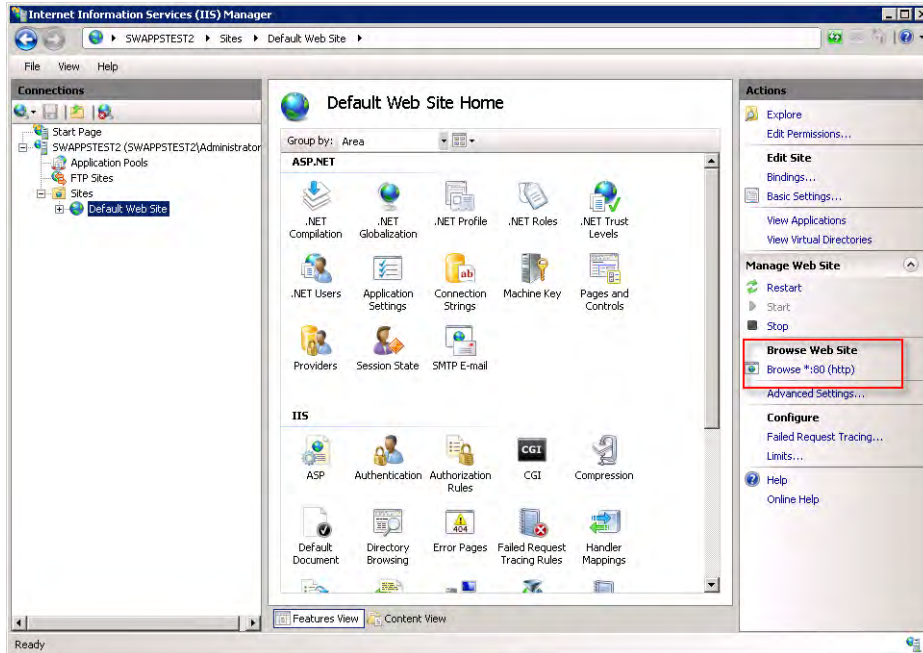
5. If **Browse *:443 (https)** is <u>not</u> listed, change to Content View at the bottom of the page and then click **Edit Bindings** on the right.
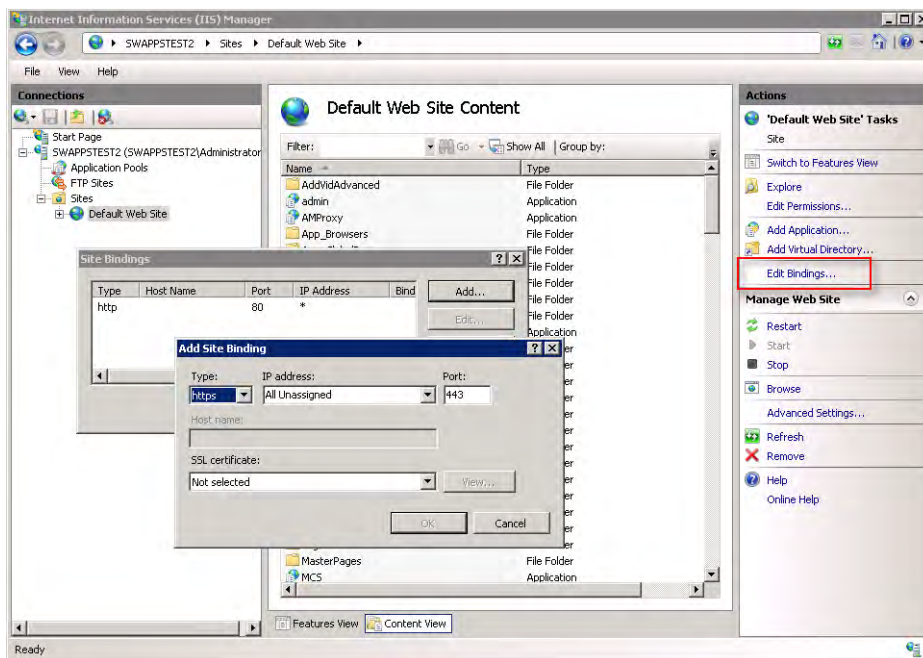
6. Add **https** in the popup window and click **OK**.

7. Verify that **https** is listed in the **Browse Web Site** box on the previous page (you may need to refresh the page) and then go to <u>Configure Non-Hardened SSL</u> on page 152.

Configuring for Presentations

Topics in this section

Overview

Multiple configuration steps are required before you can publish rich media presentations to the Portal Server. These steps are explained in more detail on the following pages. Also, be aware that in many cases a presentation will be pushed from a VBrick encoder 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 WM encoder or 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, the *Portal Server Release Notes* explains how to install them.

Note	Additional steps are also required if you will be using Distribution Servers to load-balance presentations. See "Installing Distribution Servers" in the *Portal Server Release Notes* for more about this; see the "Zones on page 93" for an explanation of how to configure and use zones that point to specific servers.

As noted, VEMS supports two types of presentations: (1) "encoder" presentations are sourced from VBrick encoders and support video and PowerPoint slides; and (2) "device" presentations are sourced from **Presentation Devices** that you create with the Admin Console and support video only. The configuration steps explained below are slightly different for encoder presentations or for device presentations. Once you have configured for presentations as explained here, see the "Create Presentation" topic in the *Portal Server User Guide* for an explanation of how to actually create, schedule, and author live presentations from the client user interface.

Encoder Presentations	Sourced from Multimedia WM and H.264 VBrick encoders. Encoder presentations support both video and PowerPoint slides. See Configuring for Encoder Presentations for more details.
Device Presentations	Sourced from "Viewing URLs" on Presentation Devices. Device presentations support video only. See Configuring for Device Presentations for more details. Used for RMS (Rich Media Studio) and RMD (Rich Media Desktop) presentations.

Configuring for Encoder Presentations

Use the following steps to configure a WM VBStar (with a hard drive) or an H.264 encoder (with internal or external storage) for presentations.

1. Configure a User with Multimedia Authoring Privileges

Do this on the Admin Console > Users page. 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 Multimedia VBrick Encoder

Using a WM VBStar as a Multimedia VBrick

1. 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.

2. You must configure a Windows Media (or reflector) VBStar as a "Multimedia VBrick' before it can be used for a presentation. See Multimedia VBrick Configuration on page 61 for more information. On the VEMS Global Settings > VBricks page in VEMS, enable the VBStar encoder in Slot 1 (or in Slot 2 of a dual encoder) as Multimedia and configure a **Viewing URL**. A **Viewing URL** is typically the path to a publishing point on a Windows Media Serve that points to the encoder, a web hosted NSC file from this encoder, or to a Windows Media Server Publishing Point which was created by a push/pull from this encoder.

3. You can also use a reflector-only model or the reflector on a single encoder in Slot 2 as a Multimedia device. (All multimedia models must be configured with a VBStar hard drive.) *Note that presentations configured with a reflector do not support slides, polls, share website, and text overlay features.*

Note   Be aware that when a presentation from a WM encoder is complete, the number of allowed clients on the appliance is set to zero. If you will be using the appliance for streaming or other purposes, it must be reconfigured: 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.

Using an H.264 Encoder as a Multimedia VBrick

You can also use an H.264 encoder (with internal or external storage) as a Multimedia VBrick. On the Global Settings > VBricks > Multimedia VBrick Config page, enable the VBStar encoder in Slot 1 (or in Slot 2 of a dual encoder) as Multimedia and configure a **Viewing URL**.

Note   When using an H.264 Multimedia VBrick for presentations, the PowerPoint slides will not cycle unless the Closed Caption parameter is disabled on the Program Configuration > Streams page in VBAdmin.

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

You configure a Mail Server and E-mail Address(es) for Presentations on the Admin Console > Global Assignments page and in the Portal Server `web.config` file or when configuring Distribution Servers. If you purchased the "Presentations" module with your VEMS Portal Server you will need to assign a mail server on the Global Assignments page. You will also

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.* The following instructions explain how to configure a mail server and e-mail addresses on your operating system: Windows Server 2008 or Windows Server 2009.

Note **If you will be installing one or more Distribution Servers, configure a mail server but ignore the rest of the steps.** You will configure the server IP addresses for e-mail invitations when you run the Distribution Sever installation tool. See "Installing Distribution Servers" in the *Portal Server Release Notes.*

Configuring a Mail Server and Addresses on Windows Server 2008

▼ To configure a mail server and IP addresses for e-mail invitations on Windows Server 2008:

1. Go to the machine on which on which the VEMS server is installed.

2. Open the Admin Console and go to **Global Settings > Global Assignments > Assign Mail Server.**

3. Enter the your **SMTP Mail Server Host Name**. If you will be generating e-mail for external users, you will also need to complete the User and Password Authentication fields.

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

5. Expand the tree control in the left navigation pane and select **Sites > Default Web Site**.

6. 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.

7. 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`

Configuring a Mail Server and Addresses on Windows Server 2003

▼ To configure a mail server and IP addresses for e-mail invitations on Windows Server 2003:

1. Go to the machine on which on which the VEMS server is installed.

2. Open the Admin Console and go to **Global Settings > Global Assignments > Assign Mail Server.**

3. Enter the your **SMTP Mail Server Host Name**. If you will be generating e-mail for external users, you will also need to complete the User and Password Authentication fields.

4. Go to **Start > Administrative Tools > IIS Manager**.

5. Expand the tree, right-click on the **Default Website**, and select **Properties**.

6. Go to the **ASP.NET** tab and click **Edit Configuration**.

7. On the **General** tab in the **Application Settings** table select the value to change and click **Edit**.

4. Assign a VEMS Presentation User

Do this on the Admin Console > Users page. 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 user who is associated with the authoring tool and has specific permissions on the Portal Server. This user must have access to all servers that presentations will be published to and all folders into which presentations can be published.

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

   b. **Allow Content Publishing** – check all 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**.

Configuring for Device Presentations

Use the following steps to configure a device presentation.

1. Configure a Mail Server and E-mail Address(es) for Presentations

This step is the same for encoder presentations. See Step 3. Configure a Mail Server and E-mail Address(es) for Presentations on page 166.

2. Assign a VEMS Presentation User

This step is the same for encoder presentations. See Step 4. Assign a VEMS Presentation User on page 169.

3. Create a Presentation Device

A "device" presentation needs a presentation device. A presentation device is simply a "virtual" entity that is used to create and publish presentations where the streaming video is sourced from an external viewing URL. See Global Settings > Presentation Devices for more about creating presentation devices.

4. Allow Presentation Device Access

Presentation authors using the client interface must have access to a previously created presentation device in order to create a device presentation. See Users > Allow Presentation Device Access on page 141 for more information.

Network Video Recording

NVR Overview

The Network Video Recorder (NVR) provides a dedicated platform to perform multiple simultaneous recordings of live streams coming from VBrick encoders. The NVR lets you off-load all recording tasks from the VEMS Portal Server machine to one or more separate "recorder server" machines. The NVR provides the ability to record live streams from the network, store these recorded video files on a specified location (a record server or other network location), transcode these streams from one format to another, and optionally automatically transfer the contents to selected locations, and/or ingest them to VOD servers.

 The NVR is available in two versions—one that supports 10 simultaneous records and one that supports 40—and is ideal for environments that require large scale recording on a robust and reliable platform. The NVR is tightly integrated with the Portal Server, the Scheduler, and VBrick's Video-on-Demand servers. The NVR provides these standard features.

- Dedicated platform – NVR servers are available on a dedicated hardware platform which eliminates resource contention and guarantees successful recording.
- Software only – NVR servers are available as a software-only option which you can install on your own server hardware. See the *NVR Release Notes* for server hardware recommendations.
- Redundant storage – both NVR servers offer RAID 5 for storage redundancy as well as dual power supplies.
- Large storage capacity – the NVR 10 provides 720 GB of storage; the NVR 40 provides 1492 GB.
- Load Balancing – Load balancing is used when multiple NVR servers are installed. Rather than recording to a specified server, the system records to a dynamically selected server based on a load balancing algorithm.
- Software Development Kit – VBrick provides an SDK to interface with the Portal Server or the NVR. In a typical security, surveillance, and monitoring applications application (without a complete Portal Server), you can write a custom application that will record streams directly to a standalone NVR.

In a basic Portal Server installation (without an NVR), the standard recording functionality allows a maximum of two concurrent recordings. In order to expand this recording capability, you can purchase a Network Video Recorder to offload recording tasks and improve overall

performance. The Portal Server and/or the NVRs are delivered with all software installed or as a software-only option. The NVR comes in standard and standalone versions as explained below. The only difference is in functionality. *Both record either 10 or 40 concurrent streams depending on the license you purchase.* Both versions can be expanded to include multiple, additional NVRs so that your recording capacity is virtually unlimited.
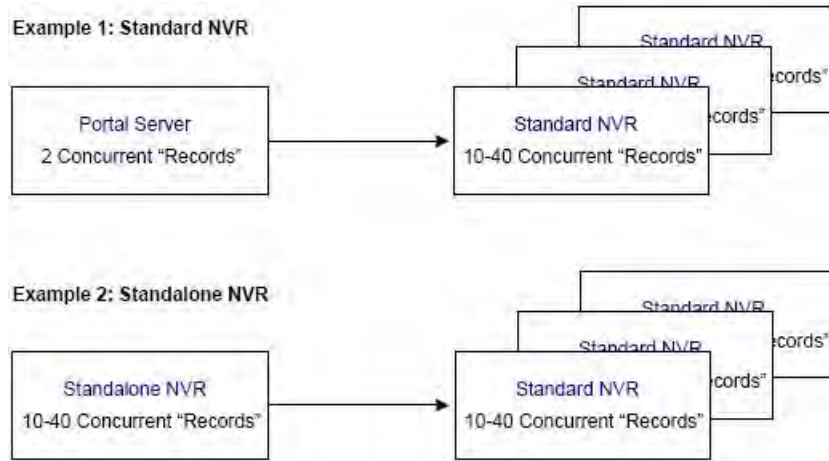
Figure 25. Standard and Standalone NVR Examples

NVR Hardware

The NVR is comprised of both hardware and software. If you purchased the hardware/software combination from VBrick, each platform (standard or standalone) comes fully loaded with NVR software. The following table shows the hardware configuration relative to the number of purchased licenses. The license file determines the total maximum concurrent recordings allowed. *In a standard NVR installation the NVR license file is stored on the Portal Server; in a standalone NVR installation the NVR license file is stored on the Standalone NVR.*

Table 18. NVR Hardware Specifications

NVR 10
Single Xeon Processor at 2.13 GHz, 2 GB memory, 4 x 73 (10 k, 2.5 in drives) configured as a RAID5, Redundant Power.
- PowerEdge R610 with Chassis for Up to Six 2.5-Inch Hard Drives   - E5506 Xeon Processor, 2.13GHz 4M Cache, 4.86 GT/s QPI, TurboHT   2GB Memory (2x1GB), 1066MHz Single Ranked UDIMMs for 1 Processor, Adv ECC   - Embedded Broadcom, GB Ethernet NICS with TOE   - PowerEdge R610 Heat Sink for 1Processor   (4) 73GB 10K RPM Serial-Attach SCSI 2.5" Hot Plug Hard Drive   - PERC 6/i SAS RAID Controller 2x4 Connectors, Internal, PCIe256MB Cache   - Windows Server 2008, Web Edition   - DVD ROM, SATA, Internal   - RAID 5 for PERC 6/i Controller   - Sliding Ready Rails Without Cable Management Arm   - Energy Smart Power Supply Redundant, 502W
NVR 40

Dual Xeon Processors at 2.8 GHz, 4 GB memory, 2 x 73 GB drives configured as RAID 1 for the OS, 2 x 146 GB drives configured as a RAID1 for recordings, Redundant Power.

* PowerEdge R610 with Chassis for Up to Six 2.5-Inch Hard Drives
* (2) X5560 Xeon Processor, 2.8GHz 8M Cache, 6.40 GT/s QPI, TurboHT
* 4GB Memory (4x1GB), 1066MHz Single Ranked UDIMMs for 2 Processors, Adv ECC
* Embedded Broadcom, GB Ethernet NICS with TOE
* PowerEdge R610 Heat Sinks for 2 Processors
* (2) 73GB 10K RPM Serial-Attach SCSI 2.5" Hot Plug Hard Drive
* (2) 146GB 10K RPM Serial-Attach SCSI 2.5" Hot Plug Hard Drive
* PERC 6/i SAS RAID Controller 2x4 Connectors, Internal, PCIe256MB Cache
* Power Saving BIOS Setting
* Windows Server 2008, Web Edition
* DVD ROM, SATA, Internal
* RAID 1/RAID 1 for PERC 6/i or SAS 6/iR Controllers
* Sliding Ready Rails Without Cable Management Arm
* Energy Smart Power Supply Redundant, 502W

NVR Performance Considerations

The NVR 40 lets you record any combination of up to 40 MPEG, WM, and H.264 streams at a time. There are however performance considerations when recording multiple, simultaneous, high-rate MPEG-2, WM, or H.264 streams. At MPEG-2 rates up to 5.5Mbps or WM rates up to 1.2Mbps 40 simultaneous recordings are supported. At higher rates however the full licensing capacity cannot be used. For example, when using the **Best Quality** WM template at 4.5Mbps, 10 simultaneous records are supported; when using MPEG-2 at 15Mbps, 15 simultaneous recordings are supported.

NVR Types

Standard NVR

A Standard NVR's record capability is managed by a Portal Server or Standalone NVR. In a standard NVR installation, the full Portal Server or Standalone NVR application is installed on one machine and the NVR application is installed on a separate machine. If you need to add recording capacity, you can add multiple NVRs as necessary. You use the Portal Server or a Standalone NVR application to configure the Standard NVR (see Configure a Standard NVR). A *standard* NVR has these characteristics:

* supports record only.
* records 10 or 40 concurrent streams depending on license.
* is configured with the standard Portal Server Admin Console *or* the Standalone NVR Console.
* records from the **Record** button *or* the **Scheduler** module.
* Supports "batch" recording where one large file is recorded into multiple smaller files.

Note When purchasing additional NVRs, VBrick provides a single combined license that includes recording capacity for all NVRs onsite.

Standalone NVR

A Standalone NVR manages the record capability of itself and any attached Standard NVRs. *A standalone NVR is typically used in security, surveillance, and monitoring applications or anywhere where full Portal Server functionality is not required.* In a standalone NVR installation, a subset of the Portal Server application is installed on one machine and the NVR application is installed on the same machine *or on a different machine.* If you need to add recording capacity, you can add multiple Standard NVRs necessary. You use the subset of the Portal Server application to configure the NVR (see Configure a Standalone NVR). A *standalone* NVR has these characteristics:

- supports record only.
- records 10 or 40 concurrent streams depending on license.
- is configured with a subset of the Portal Server Admin Console that has limited features—no VBricks, IPRs, etc.
- records from the **Scheduler** module only.
- has limited end user features. End users can see only the **Scheduler**, the **Status** page, and the **Help** system.
- supports "batch" recording where one large file is recorded into multiple smaller files.
- has an API interface that lets you write custom applications to control the NVR.

Note When purchasing additional NVRs, VBrick provides a single combined license that includes recording capacity for all NVRs onsite (Standard and/or Standalone).

NVR Installation

See the NVR Release Notes for complete installation instructions.

Synchronize the Portal Server and the NVR

The internal clocks on the Portal Server and the NVR must be synchronized for recording functionality to work properly. You can use the `Net time` command as explained below or you can use an external time server. In order to run the `Net time` command on *either* server, the server must be on the domain, and the user logged onto the server must have admin privileges *and* be part of the domain.

▼ To synchronize the Portal Server and the NVR:

1. Open a command prompt window on the Windows Web Server 2008 *Portal Server* machine.
2. Type: **Net time \\{NVR IP Address} /SET**

NVR Configuration

Configure a Standard NVR

A standard NVR is installed on a dedicated machine that comes fully loaded with all NVR software. However, you must still configure the NVR as explained below. NVR configuration is performed using the Recorders pages on the Portal Server's or Standalone NVR's Admin Console. See Recorders on page 43 for more information.

▼ To configure a standard NVR in a *Portal Server Installation*:

1. Login to the Portal Server Admin Console using *the host name or IP address of the Portal Server machine*. For example: http://myserveraddress/admin

2. Define a Record server.

   a. Set record **Path** if necessary. Set to local hard drive on NVR or to a network drive.

   b. Set **Max. Recording**.

3. Define VOD and FTP Servers (go to **Global Settings > Servers**).

   a. Record only – VOD server not required.

   b. Record and ingest – must define a VOD server.

   c. Record, ingest, and FTP – must define VOD and FTP servers.

   d. Record and FTP – must define an FTP server.

4. If Access Control is enabled, you must create a user and grant the following permissions on the **Users** page in the Admin Console. See Configuring Users on page 135 for more information.

   a. **Add/Modify Live Channel Privileges**

   b. **Allow Access To Specific FTP Servers**

   c. **Allow Access To Specific Recorder Servers**

   d. **Allow Access To Specific VOD Servers**

   e. **Allow Content Recording**

   f. **Schedule Privileges**

Configure a Standalone NVR

▼ To configure a standard NVR in a *Standalone NVR Installation*:

1. Login to the Standalone NVR Admin Console *using the host name or IP address of the Standalone NVR machine*. For example: http://myserveraddress/admin

2. Define a Record server.

   a. Set record **Path** if necessary. Set to local hard drive on NVR or to a network drive.

   b. Set **Max. Recording**.

3. Define VOD and FTP Servers (go to **Global Settings > Servers**).

   a. Record only – VOD server not required.

   b. Record and ingest – must define a VOD server.

   c. Record, ingest, and FTP – must define VOD and FTP servers.

   d. Record and FTP – must define an FTP server.

4. If Access Control is enabled, you must create a user and grant the following permissions on the **Users** page in the Admin Console. See Users on page 81 for more information.

   a. **Allow Access To Specific FTP Servers**

   b. **Allow Access To Specific Recorder Servers**

   c. **Allow Access To Specific VOD Servers**

   d. **Allow Content Recording**

   e. **Schedule Privileges**

Using an NVR

As noted, the Portal Server and the Network Video Recorder are installed on separate machines. Using the Admin Console, you configure the NVR by indicating where record files

will be stored, and defining the maximum number of simultaneous recording the NVR will support (which is less than or equal to the licensed number of recordings). The record **Path** can be set to local hard drive on the NVR machine or to a network drive. In a Portal Server installation, from PCs or IPRs, end users can access NVR record features (record start/ record stop) through using the Portal Server. When a recording is initiated using the **Record** button on the **Live Media** page of the Portal Server, the record file is be automatically ingested to available VOD servers, based on the stream type (e.g. MPEG2, MPEG4, etc.) and user's permissions. After ingestion, the record file can be automatically deleted from record server based on the Global Settings configuration.

When a record is initiated through Scheduler interface of Portal Server, end users can specify whether they want to FTP the recorded file to available FTP servers or to ingest the recorded file to available VOD servers. They can also specify whether or not to automatically delete the file after a successful FTP or ingestion. (These options are not available in "batch" mode. If you select **Enable Batch**, the files are not FTPed and ingested; they are saved to `D:\Inetpub\ftproot\MCS\Record` and all other options are disabled.)

In a *standard* NVR configuration, live streams can be recorded (1) by using the **Record** button on the embedded player or (2) by using the **Scheduler** module. In a *standalone* NVR installation, recording can *only* be initiated from the **Scheduler** module using the interface as shown below in Figure 26. For a complete description of the Scheduler, see "Using the Scheduler" in the *Portal Server User Guide.*

Note To use a standard NVR, the Portal Server and the NVR must be installed and running. To use a standalone NVR, only the NVR application must be running.
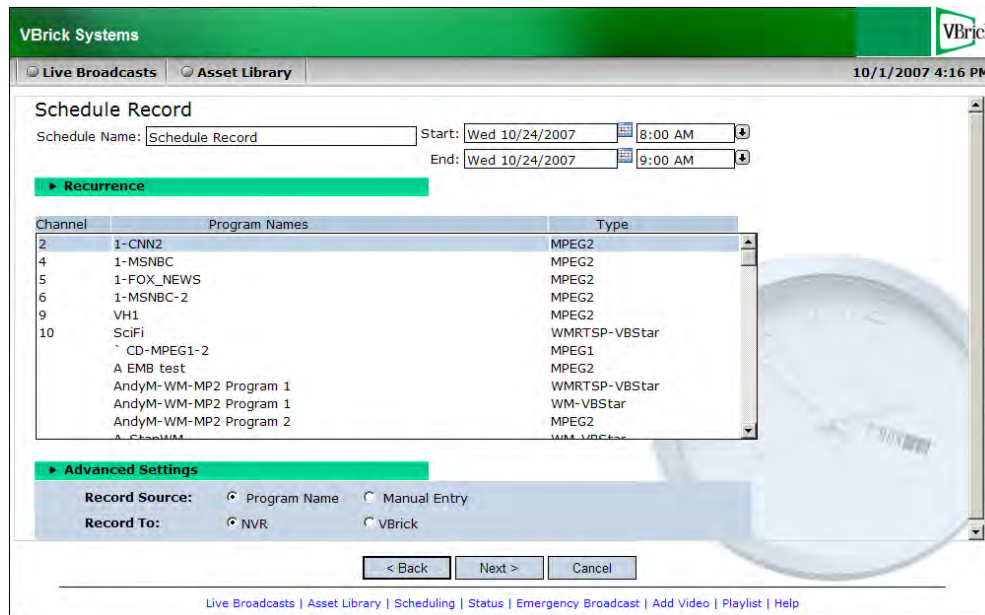
Figure 26. Portal Server "Schedule Record" Page

Auto Content Ingestion

As explained in this chapter, there are two ways to autoingest content depending on your requirements. One method is to FTP or copy your video content to predefined folders on the Portal Server. The folders are monitored and the content is automatically ingested (autoingested) at periodic intervals. The second method is to use .xml files for content stored at remote locations or on mass storage devices. This method also supports metadata for search, copyright protection, maximum viewers, etc. In either case this document assumes you are an experienced user who is familiar with IIS, FTP and similar technologies.

AutoIngest Content

You can FTP or copy prerecorded content to the VEMS Portal Server for easy ingestion to the VOD server(s). The VEMS Portal Server periodically (every 5 minutes) polls certain folders for presence of content and if found ingests the content onto multiple VOD servers. This process is called *Automatic Content Ingestion* or *Autoingestion*. The content can come from a pushbutton recording on the Portal Server, a VBrick VBStar, or a file recorded with StreamPlayer Plus.

Notes • You cannot auto ingest third-party presentations into the Portal Server. You must use the native FTP facilities in each application.

• File transcoding is not supported via AutoIngest.

The content should be placed in a pre-defined sub-folder (`mcs\autoingest`) under the FTP root folder. This pre-defined folder is called the *autoingest root folder*. For example, if the FTP root is at `c:\inetpub\ftproot`, the content could be placed anywhere under `c:\inetpub\ftproot\MCS\AutoIngest`. In this example the `autoingest` root is `c:\inetpub\ftproot\MCS\AutoIngest`.
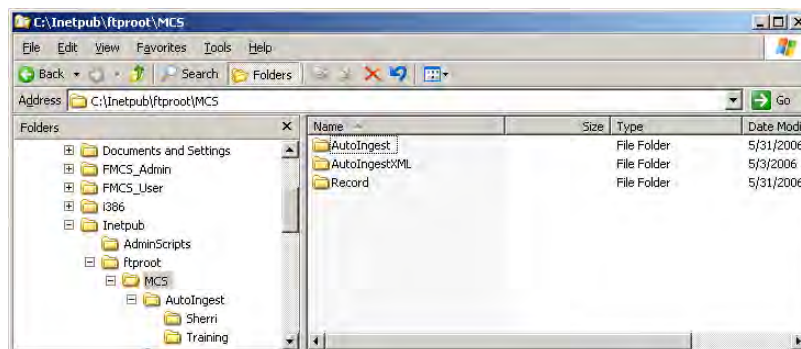
Note	An autoingest folder is not created until you record a program for the first time. If you want to autoingest before a recording, you must manually create the autoingest folder at `d:\inetput\ftproot\mcs\autoingest`.

The default FTP path may be on a different drive, refer to the IIS default FTP configuration to confirm. The default FTP path in IIS is automatically set via the installer, but, depending on your server'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**.

Note	When IIS installs the FTP service, a default FTP directory is created at `drive:\Inetpub\ftproot`. Also, in the Admin Console, 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**.

Content that is placed under the autoingest root folder on the VEMS Portal Server will be ingested into the root video folder on the VOD server provided that it is configured using the VEMS Portal Server Administrator interface. If you want to place content on a subfolder in the VOD server, that same folder would have to be created and configured using the VEMS Portal Server Admin interface as described below.

Go to **Global Settings > Servers > Add/Modify Video On-Demand Content Folders**. Here an existing or new folder can be associated with selected VOD servers for autoingestion. The folders are listed on the left with the path relative to autoingest root. The VOD servers are listed on the right inside the **Add/Modify Folders on Selected Servers** box. Select the desired folder and then select the target VOD servers to ingest content. Press **Submit**. The folder is now created under the autoingest root folder and configured. See <u>Add/Modify Video On Demand Content Folders</u> on page 57 for details.

Example

If under the root video folder on the VOD Server you had a folder (or want to create a folder) called `Training` and you wanted `trainingvideo.mpg` to be placed there,

FTP the file to the Portal Server into `<drive:>\inetpub\ftproot\mcs\autoingest\training\`
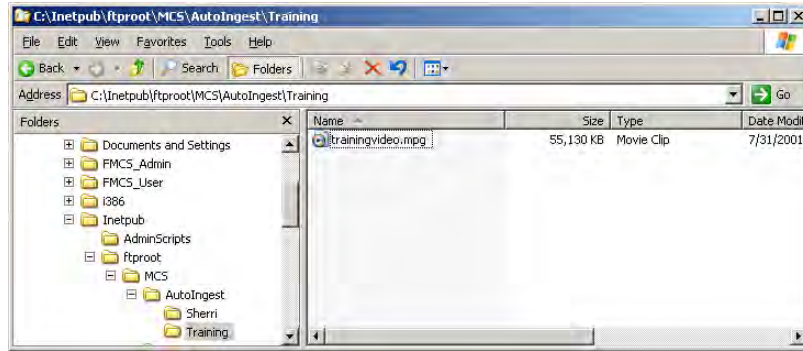
The VEMS Portal Server will then ingest the file automatically into the folder on the VOD server(s) that this folder is associated with. The file `trainingvideo.mpg` would be displayed on the VEMS Portal Server user interface in the Training folder.

AutoIngest Content via XML

This feature lets you autoingest video files by placing an .xml file in the `AutoIngestXML` folder on the Portal Server. It also lets you associate metadata with the video such as maximum number of viewers for copyright protection, keyword tags for searching, etc. As explained below there are three ways (see Table 19) to use this feature depending on where the source files are located. The Portal Server monitors this folder for .xml command files and autoingests any files at five-minute intervals. The `ingest` command, target video file name, target VOD folder, and metadata to associate with the video are contained in the .xml file. Autoingest permissions are associated with an autoingest user that is defined using the Admin Console.
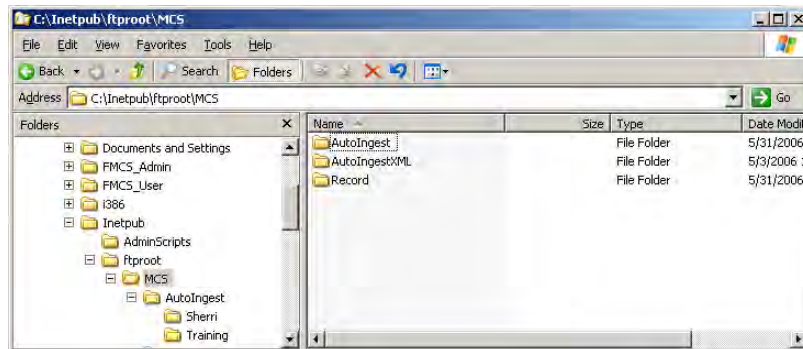
The Portal Server autoingest folder is under FTP root on the Portal Server at `/MCS/AutoIngestXML` The video file and the .xml file must be FTPed (or copied) to this directory and the target video title must contain the fully qualified path to the destination. The autoingest user name as configured in the Portal Server Admin Console will be used to access

available VOD servers. If the autoingest user does not have publishing rights for the VOD directory specified in the `MCSTitle`, the ingestion will fail.

Autoingest users must have VOD server access to at least one server capable of storing the video type (MPEG, WM, H.264). Only existing custom fields will be recognized and associated with the video (see <u>Custom Fields</u> on page 32 for more information). The Windows **Event Viewer** will log the ingest command, noting the full path and the .xml data contained in the command, and will also log the successful ingestion of the video.

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 a failed ingestion error.

▼   To create an autoingest user with publishing rights:

1.   Open the Admin Console, go to **Users > Add User**, and create an autoingest user, e.g. `AutoIngestUser`.

2.   On the same page, go to **Allow Access to Specific VOD Servers** and select the servers this user can access.

3.   On the same page, go to **Allow Content Publishing** and select the folders this user can publish to.

4.   Then go to **Global Settings > Global Assignments > Assign AutoIngest** and set the user you just defined as the **Current AutoIngest User**.

AutoIngestXML Modes

There are three modes of operation as shown in Table 19. The mode you use depends on *where* the source files are located.

Table 19. AutoIngest Modes

Mode	Description
Direct	The target source video file is FTPed to the `AutoIngestXML` folder. The video file and the .xml file must both be FTPed to this folder. In Direct mode, you must FTP the video file first or the ingestion will fail.
Absolute	WM files only. The target source video file resides in a folder on the Portal Server. Only the .xml file is FTPed to the `AutoIngestXML` folder. This is useful for mass storage devices because you do not have to copy the files to the `AutoIngestXML` folder on the Portal Server.
Remote FTP †	MPEG Files only. The target source video file resides on a remote FTP server. Only the .xml file is FTPed to the `AutoIngestXML` folder.

† Not available for VOD-D (Darwin) servers. Use Direct mode only to AutoIngest to VOD-D servers.

Using the XML Template

There are three named templates in the `VBrick\MCS\utils` folder for Direct, Absolute, and Remote FTP files. Use the appropriate template to manually create an .xml file for *each* video file. Use Notepad, TextPad, or a similar tool and then FTP this file (and the video in Direct mode) to the `AutoIngestXML` folder on the Portal Server. (In Direct mode, you must FTP the video file first or the ingestion will fail.) The filename can be any alphanumeric string with an

.xml extension. The following code shows a sample .xml file that uses the Direct mode template. **The template for each mode is the same except for the SourceFileName and SourceFileType tags**. Table 20 explains the required format for these tags.

```xml
<?xml version="1.0" encoding="utf-8"?>
<AutoIngestCmd version="1.0">
  <Command>ingest</Command>
  <Ingest>
    <MCSTitle>/VODFolder/Spiderman Returns</MCSTitle>
    <Keywords>Ingest001</Keywords>
    <Description>My ingested Video</Description>
    <Expiration>20060430-1130</Expiration>
    <SourceFileName>Ingest002.wmv</SourceFileName>
    <SourceFileType>WM</SourceFileType>
    <MaxViewers>-1</MaxViewers>
    <FileLink filename="myfile.ppt" url="http://www.google.com/" />
    <FileLink filename="myother.ppt" url="http://www.google.com/" />
    <CustomFields>
        <Field name="CustomTextField1" value="Value1" />
        <Field name="CustomTextField2" value="Value2" />
        <Field name="CustomDropField1" value="one" />
        <Field name="CustomDropField2" value="two" />
    </CustomFields>
  </Ingest>
</AutoIngestCmd>
```

Table 20. AutoIngestXML Tags

Tag	Description
Command	Required. Must be set to ingest.
MCSTitle	Required. Cannot be blank. Must begin with "/" and contains fully qualified path to destination VOD folder/title on the Portal Server. The autoingest user name must have publishing rights for VOD target folder.
Keywords	Optional. Keywords associated with this video. Used for search.
Description	Optional. Description of the video. Used for search.
Expiration	Optional. Content expiration specifier, e.g. 20060430-1130. Format: yyyymmdd-hhmm Used for copyright protection.

Tag	Description
SourceFileName	Required. Contains the source video file name to be ingested. The format of this data determines the mode of operation.
	• Direct – All files (see supported file types in Table 21). This file must reside in the `AutoIngestXML` directory (*it must be FTPed first*) on the Portal Server. This file will ultimately be copied to one or more VOD servers. The format is simply the filename for example: `ingest001.wmv`
	• Absolute – WM files only. This file must reside in a folder on the Portal Server. The format for this data is: `[absolutepath]` `<FullLocPath>` for example `[absolutepath]c:/Temp/ingest002.wmv`
	• Remote FTP – MPEG Files only. This file resides on a remote FTP server. The format for this data is:
	`ftp://username:password@FTPServerURL/subdirectory/Filename`
	For example: `ftp://videos:videos@172.22.2.1/videos/ingest0003.mpg` where the FTP protocol string, username, password, FTP URL, subdirectory, and file name are specified in the string in a fixed format.
SourceFileType	With Direct mode (see above) this parameter is automatically configured and not used. *This parameter is required for Absolute and FTP Remote modes.* Format type of the video files = `WM`, `H264`, `MPEG-1`, `MPEG-2`, and `MPEG-4`.
MaxViewers	Optional. Maximum number of concurrent viewers allowed. -1 = unlimited. If unspecified, -1 (unlimited) is assumed.
FileLink	Optional. 0–n file reference links to associate with this video. Each file link requires a filename (e.g. `"myfile.ppt"`) and a URL.
CustomFields	Optional. 0–n custom fields to associate with this video. See Custom Fields on page 32 for more information. Each custom field must contain:
	• name – must be already defined in Portal Server or field will be ignored.
	• value – dropdown list boxes only; must be already defined in Portal Server or field will be ignored.

Table 21. File Types Supported in Direct Mode

File Type	File Extension
MPEG-1	.mpg
MPEG-2	.mpg
MPEG-4	.mp4
H.264/MP4	.mp4
H.264/TS	.mpg
WM	.wmv, .wma, .mp3, .asf
FLV	.flv
SWF	.swf

File Type	File Extension
F4V	.f4v
MOV	.mov
M4V	.m4v
M4A	.m4a

Removing MPEG-4 Closed Captions

MPEG-4 files with closed captions cannot be added to NXG servers until the closed caption track is removed. The VEMS Portal Server will display an error message if you try to add such files. VBrick provides a utility to remove the closed captions track from an MPEG-4 file if necessary. It is installed with VEMS Portal Server in `c:\program files\vbrick\utils`

▼   To remove the closed captions track from MPEG-4 files:

1.   Go to `c:\program files\vbrick\MCS\utils` and double-click `CCTrackRemover.exe`

2.   Enter an **MPEG-4 File Name** and click **Remove CC Track**. Depending on the size of the file it may take a few moments to complete.

3.   When done, you can add or autoingest the video file as necessary.

Automatic System Backup

This chapter explains how to use ETVBackup to create a warm backup Portal Server. ETVBackup is an optional software application. If you did not purchase ETVBackup, you can backup key Portal Servers files and directories manually. See <u>Manual System Backup</u> **on page 199 for details.**

Overview

Enterprise Media System Backup is a highly-automated standalone application that backs up key directories on the Portal Server at periodic intervals. VEMS Backup requires two separate Portal Server machines: a "warm backup" Portal Server and a "live" Portal Server. *They must both have the same version of the Portal Server software installed.* During a scheduled backup, VEMS Backup copies new or changed files and ensures that the data on the warm backup always matches the data on the live Portal Server.
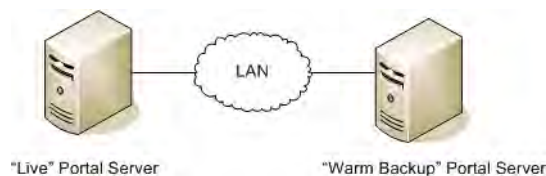
Warm backup is the process of copying key directories and files from a "live" (primary) Portal Server to a "warm backup" (secondary) server. These directories and files are backed up on a scheduled periodic basis (every 10 minutes) and a configurable number of archive versions are kept on the backup server. The warm backup will not function as a Portal Server while it is in warm backup mode. If the live Portal Server fails for any reason, you can quickly convert the backup server into the live server by performing a few simple steps. The warm backup then becomes the "live" primary server.

VEMS Backup is an optional Enterprise Media System component with its own license. *VEMS Backup does not provide a redundant "hot" standby server, nor does it backup video content.* VEMS Backup is designed to provide a "warm" backup server for key Portal Server data files and for the metadata describing your content. There is no installation procedure. VEMS Backup is automatically installed and requires only a license key. This document describes how to configure a warm backup and how to turn a warm backup server into a live server. Once it is properly configured, VEMS Backup will automatically run every ten minutes and no additional configuration or user action is required.

Note VEMS Backup is tightly integrated with the Portal Server and backs up key directories and files. VBrick does not support any user customization of this product or any non-VEMS Portal Server uses of the software.

VEMS Backup Profiles

The folders shown below are automatically backed up from the live server to the warm server. As shown in the window, each key Portal Server directory is preconfigured with a corresponding "profile." Note that Portal Server license files are specific to the server hardware on which they are installed. For this reason they are backed up on the warm server in an alternate location under the VEMS application directory so that they do not overwrite the warm backup server's own license files.

Table 22. Enterprise Media System Reporter Backup Profiles

Profile Name	Folder Location
VEMS Database Backup	C:\Program Files\MySQL\MySQL Server 5.1
VEMS Licenses Backup	C:\Program Files\VBrick\MCS\licenses
VEMS Live Presentations Backup	MCSPresentations (virtual directory)
VEMS Logs Backup	C:\Program Files\VBrick\MCS\Logs\
VEMS nsc Backup	C:\Program Files\VBrick\MCS\nsc
VEMS sdp Backup	C:\Program Files\VBrick\MCS\sdp
VEMS Station Icons Backup	StationIcons (virtual directory under MCS application)
VEMS Stored Presentations Backup	Presentations (virtual directory)
VEMS Thumbnails Backup	C:\Program Files\VBrick\MCS\Images\Thumbnails

Configuring VEMS Backup

▼   To configure Enterprise Media System Backup, you must perform all of the following steps in the exact sequence shown:

1. Enter License Key.

2. Set Profile IP Addresses.

3. Configure the Scheduler.

4. Reset Database Backup Versioning.

5. Enable the Warm Backup Server.

6. Test the Configuration.

1. Enter License Key

The first time you launch VEMS Backup, you will be prompted for a license key. This key is attached to the "Software Activation Keys" card shipped with the VEMS server.

▼   To enter the license key:

1. Find your license key on the "Software Activation Keys" card, type it into Notepad, and copy it to the clipboard (Ctrl-C).

2. Launch VEMS Backup: go to **Start > Programs > VBrick > ETV Backup**.

3. When the Serial Number window is displayed, paste the license key into the window (Ctrl-V) and the VEMS Backup application will automatically be launched.
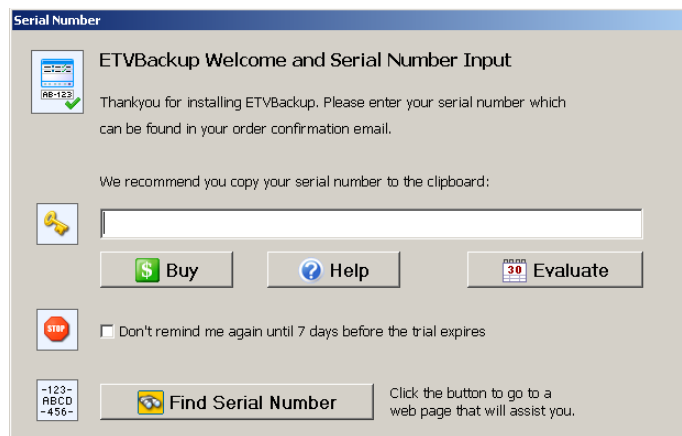
2. Set Profile IP Addresses

VEMS Backup is shipped with a preconfigured profile "group" called MCS Warm Backup Group. This group has individual profiles corresponding to all of the key Portal Server directories that need to be backed up. All VEMS Backup functions use this preconfigured group. Before you can run VEMS Backup you need to set the IP addresses for *each* of the individual profiles in MCS Warm Backup Group. These addresses must correspond to the actual IP address of your live Portal Server.

▼   To set the profile IP addresses:

1. Double-click on the first profile (or right-click and select **Modify**) in the group which is MCS Database Backup. (This should open the following window. If not check that **Preferences > Double-click Action** is set to **Modify the profile**.)
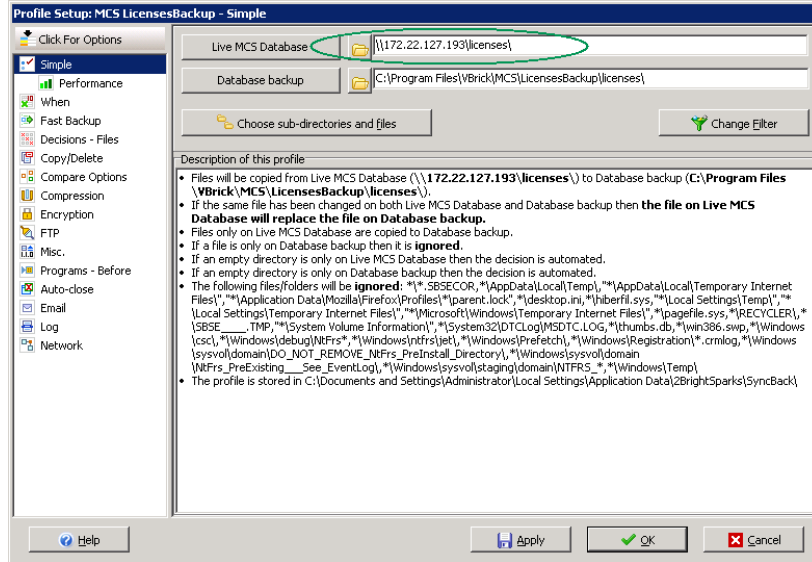
2. In the **Live MCS Database** field, replace the IP address shown with the IP address (or server machine name) of your live Portal Server. Do not change anything else in the path.

3. The **Database backup** field is populated automatically. Do not change anything in this field.

4. Click **OK** when done and repeat these steps for each of the other profiles.

3. Set MySQL Version

The preconfigured profile "group" called VEMS Database Backup must be modified to correspond to the MySQL version being used by VEMS (currently 5.1).

▼   To modify the MySQL profile setting:

1. Double-click on VEMS Database Backup (or right-click and select **Modify**.

2. In the **Live MCS Database** field, change MySQL Server 5.0 to MySQL Server 5.1. Do not change anything else in the path.

3. In the **Database backup** field change MySQL Server 5.0 to MySQL Server 5.1. Do not change anything in the path.

4. Click **OK** and ignore any messages when done.

4. Configure the Scheduler

The procedure for this step only varies depending on whether you are using Windows Server 2003 or Windows Server 2008. Use the instructions that are appropriate for your site. The remaining steps (5–7) are the same for both operating systems.

Windows Server 2003

▼   To configure the Scheduler on Windows Server 2003:

1. Right-click on MCS Warm Backup Group and select **Schedule**.

2. Click **Edit Schedule**.
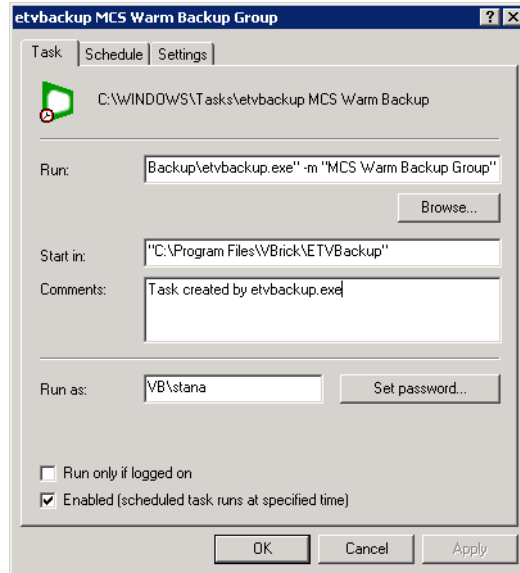
3. Be sure a user with administrative privileges on the server machine is shown in the **Run as** box. Press **Set Password** and enter the password associated with that user.
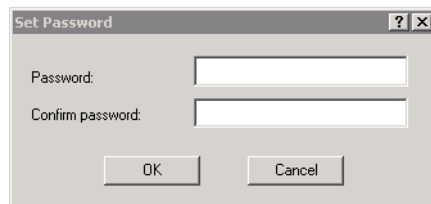
4. Press **OK** and **OK** and minimize the application—do not exit.

Windows Server 2008

▼ To configure the Scheduler on Windows Server 2008:

1. Right-click on MCS Warm Backup Group and select **Schedule**.

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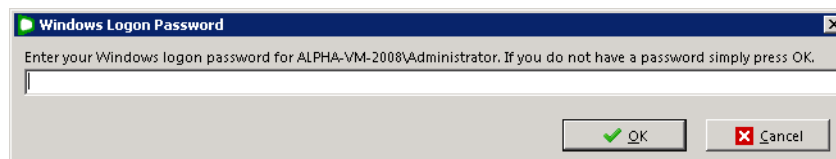
3. Be sure a user with administrative privileges on the server machine is shown in the **Run as** box. Then enter the password associated with that user and click **OK**.
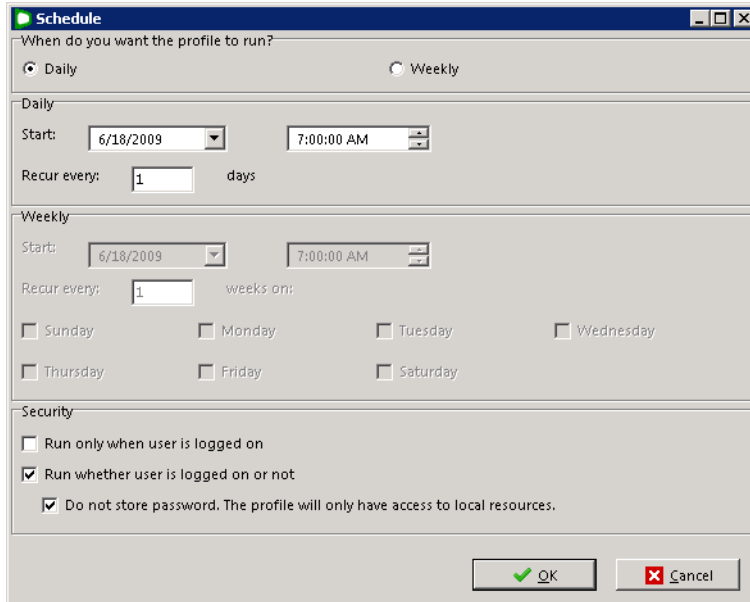
4. On the "Schedule" window, click **OK** and **OK** to exit.

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

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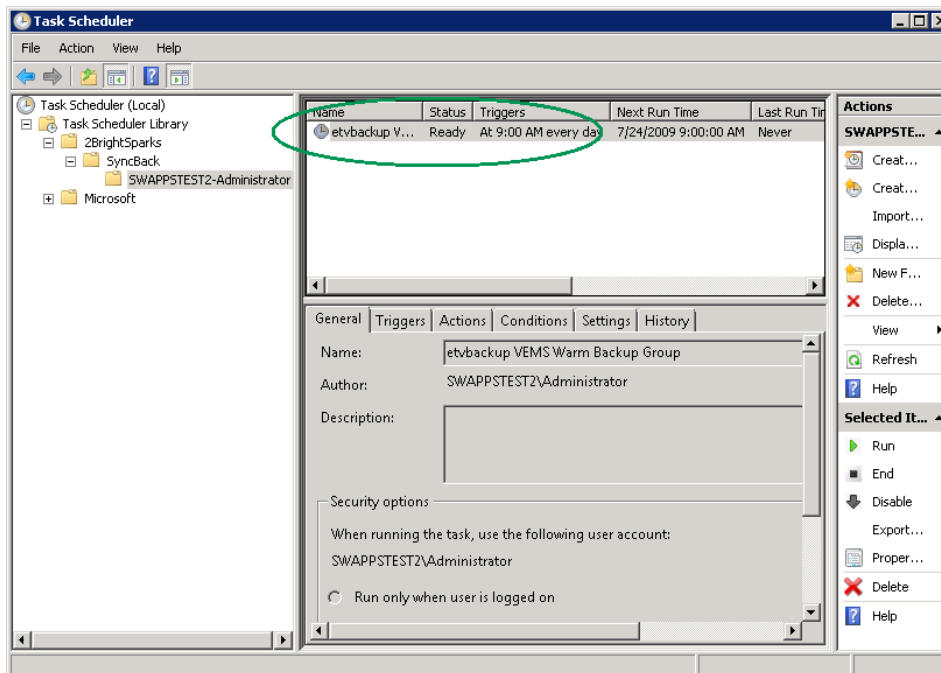
7. In the upper pane, double-click on **etvbackup VEMS Warm Backup Group** to display the properties page.
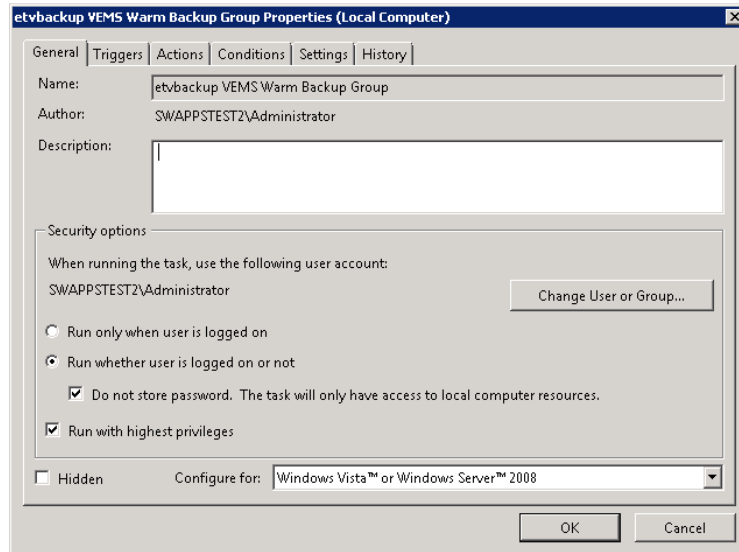
8. Click on the **Triggers** tab and click **Edit**.
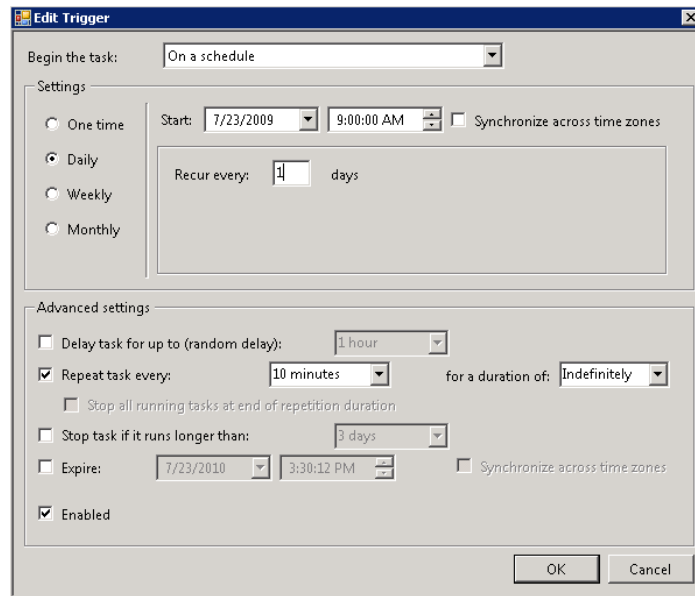
9. Select **Repeat task every** 10 minutes, set **for a duration of** Indefinitely, and click **OK**.

5. Reset Database Backup Versioning

This step is important. Do not omit this step.

▼ To reset database backup versioning:

1. Right-click on `VEMS Database Backup` and select **Modify**.

2. Then go to **Copy/Delete > Versioning** in the left navigation pane and set maximum versions to **5** and maximum days to **7**.
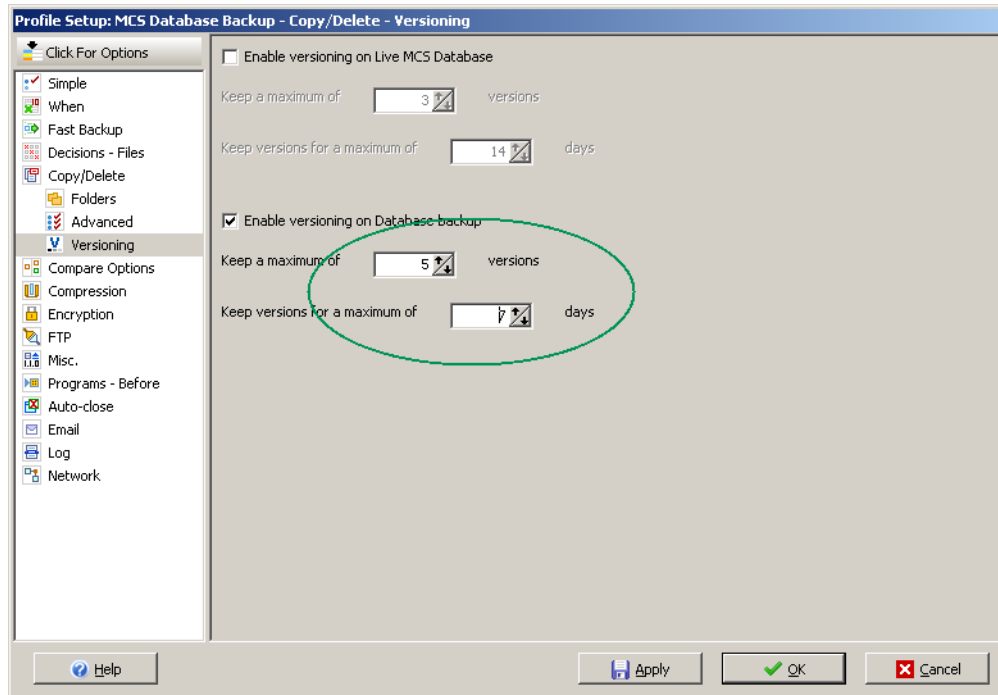
3. Click **OK** and minimize the application—do not exit.

6. Enable the Warm Backup Server

If you purchased VEMS Backup, two Portal Servers will be present at your site—one of which must be configured as a warm backup. *By default, the warm backup option is disabled on both servers.*

▼ To enable a warm backup server:

1. On the server machine that will be used as the warm backup, go to **Start > Control Panel > Programs and Features**.

2. Select **VBrick Enterprise Media System** and click **Uninstall/Change**. Then select **Enable/ Disable Warm Backup Server** and click **Next**.

© 2011 VBrick Systems, Inc.
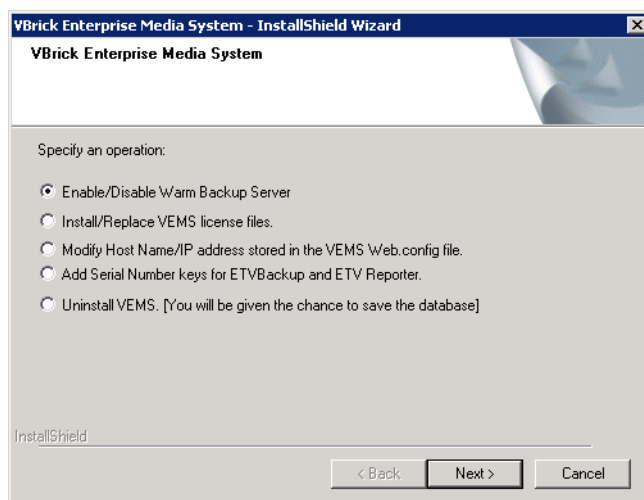
3. Then select **Enable** and click **Next**, then **OK** to exit. This will enable the machine as a warm backup. This will complete the configuration and there is no need to reboot the server.
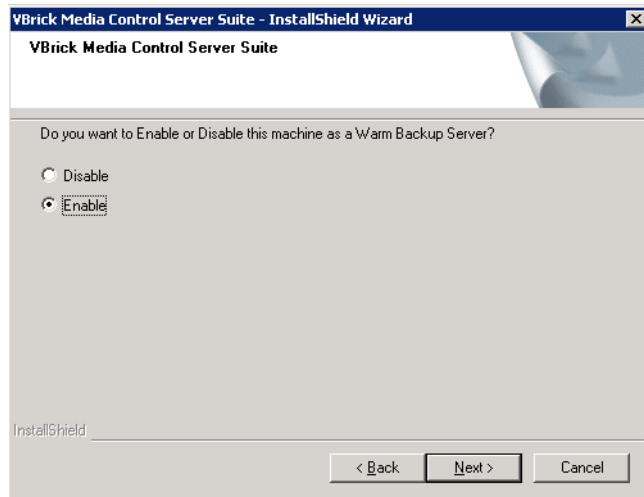
4. When finished, launch VEMS Backup using the desktop icon.

7. Test the Configuration

When you are finished configuring the IP addresses, click the **Run** icon in the navigation footer. All backup profiles should run without errors and a window similar to the one shown below will report a successful backup for each profile. If problems occur, for example if you entered an invalid IP address, the window will report any failures. Correct the problems using the information provided in the log window and try again.

▼ To test the configuration:

1. Highlight the MCS Warm Backup Group and click **Run**.
2. Click **Continue Run** for each Differences for profile: xxxxx window and then **OK**.
3. If no errors occur, a window similar to the one shown below will be displayed.
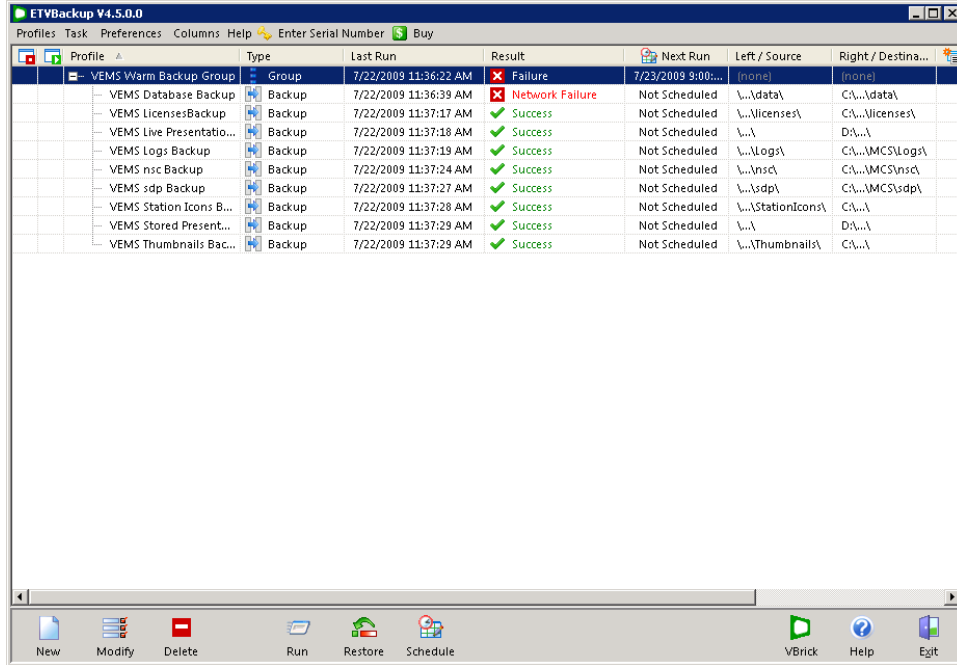
4. If errors occur, right-click on the failed profile and select **View Log > Newest**.
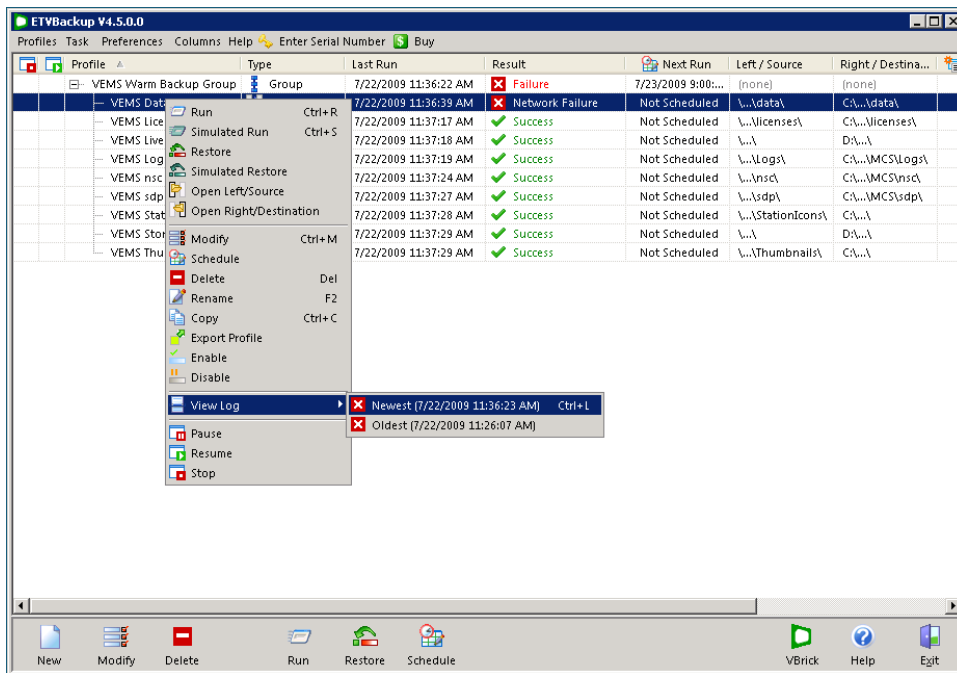
5. This will displayed detailed information (see below) that you can use to correct the error.
6. When done, highlight the failed profile and run again until successful.

ETVBackup Log
Main Page

Select a link below to view detailed information about the task you carried out:

| Copied, deleted, and changed (0) | Skipped (0) | Warnings (0) | Errors (0) | Non-Critical Errors (0) |

Log Report: Overview

Profile Name	MCS Database Backup		
Result	Scan Failure		
Unattended	No		
Username	VB\Stana	Computer Name	STANAXPNB05
Profile Start Time	3/4/2008 3:40:27 PM	Profile End Time	3/4/2008 3:40:50 PM (23 secs)

Log Report: Errors and Warnings

Critical Error	Failed to prepare Live MCS Database : Directory \\172.22.130.22\MySQL Server 5.0\data does not exist and cannot be created

Report produced by ETVBackup

Turning a Warm Backup Server into a Live Server

A Portal Server can experience a hardware failure for a variety of reasons. If the hardware fails, you may be unable to communicate with the server via a web browser, the Remote Desktop utility, or any other means. Since there will be no web access, end users may get a "404 page not found," server timeout, or similar message. If this happens, remove the server from service and turn the warm backup into the primary server as explained here. This procedure only takes a minute or two. *After fixing or replacing the failed primary server, you can then re-configure it as a warm backup or as the primary server.*

Note   In most cases, the changeover to a warm backup server will be totally transparent to end user (client) viewers. If they are watching a live or a stored VOD video when the changeover occurs, there will be no disruption to the video viewing.

▼   To turn a warm backup server into a live server:

1.   On the warm backup machine, open the **Add or Remove Programs** window on the **Control Panel** and click **Change/Remove** on the **VBrick Media Control Server Suite**.

2.   Then click **Disable** to disable the warm backup and make this machine your live server. *You will no longer have a warm backup server.*
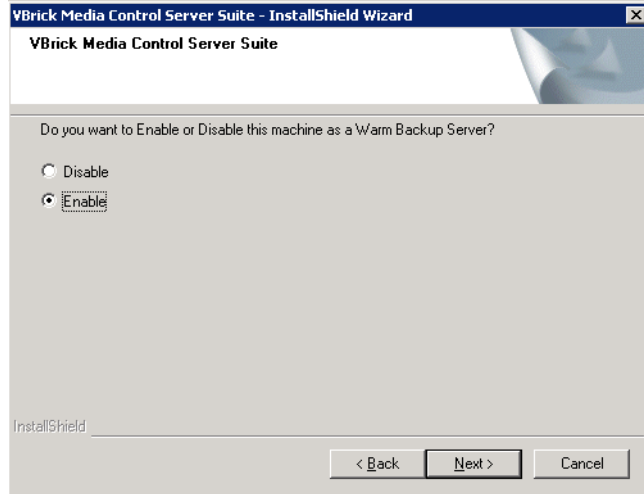
3. If you want viewers to use the same host name for the Portal Server after turning a warm backup into a live server, a network administrator will have to change the IP address or DNS entry to match the new address.

Bringing a Failed Machine Back Online

Bring a Failed Machine Back Online as a Warm Backup

▼ To bring a failed machine back online as a *warm backup* server:

1. Configure the fixed machine as a warm backup. Repeat *all* of the configuration steps described earlier (see Configuring VEMS Backup on page 187). Be sure to replace the profile IP addresses with the IP address (or server machine name) of the *new* live Portal Server. Make sure you don't put both the live server and the warm backup server online at the same time with the same IP address.

2. After fixing or replacing the failed server, go to **Add or Remove Programs** and **Enable** this machine as a warm backup—not as a live Portal Server. You can only have one Live Portal server configured at a time.

   (If you want viewers to use the same host name for the Portal Server after turning a fixed machine into a warm backup, a network administrator will have to change the IP address or DNS entry to match the new address.)

3. After performing these steps, the new primary server will acquire the backed up directories and files from the old primary server as soon as you test the configuration.

Bring a Failed Machine Back Online as a Primary Server

▼ To bring a failed machine back online as a *primary* server:

1. **Follow Steps 1–3 above to first bring a failed machine back online as a warm backup.** You must perform these steps first. *If you do not, you risk losing all existing backup data.*

2. Go to **Add or Remove Programs** and **Disable** this machine as a warm backup.

3. Go to **Add or Remove Programs** on the other server and **Enable** that machine as a warm back.

Software Installation and Upgrade

ETVBackup Installation

Enterprise Media System Backup requires a license key. If your VEMS purchase included VEMS Backup, the license key will be installed by VBrick prior to shipment. If you ever need to re-install the software, the license key is attached to the "Software Activation Keys" card that is included with the server. If you purchase VEMS Backup separately, VBrick will send a "Software Activation Keys" card with the new license key attached. Launch VEMS Backup and enter this license key, when prompted, to activate the software.

VEMS Upgrade

There is no upgrade for ETVBackup. This topic explains how to upgrade the VEMS software on a warm backup server.

▼ To upgrade the VEMS software on a warm back up server:

1. Manually save all of your data on the backup server. For details see Manual System Backup on page 199.

2. Close the ETVBackup application. Right-click on the icon in the system tray and select **Exit**.

3. On the warm backup server, go to **Start > Control Panel > Programs and Features**.

4. Select **VBrick Enterprise Media System** and click the **Uninstall/Change** button.
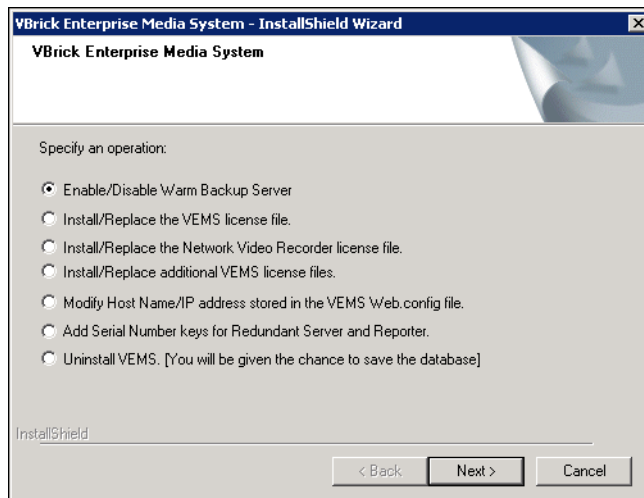
5. **Disable** the Warm Backup Server. See Uninstall/Change Configuration on page 15 for details.

6. Upgrade the Portal Server software as explained in the *Portal Server Release Notes*.

7. When done start with Step 3 above and **Enable** the Warm Backup Server.

8. When done reboot the server and ETVBackup will automatically start.

Manual System Backup

This chapter explains how to manually backup key system files and directories on the Portal Server. If you purchased Enterprise Media System Backup, this process is automatic. See <u>Automatic System Backup</u> on page 185 for details.

The Enterprise Media System Portal Server uses MySQL to manage the database of users and groups, and also the video *information* related to content on the VOD Servers. Note that this procedure backs up information in the MySQL database and key directories only. *It does not back up any video content you may have stored on attached VOD servers.* (To back up video content, you will likely need a backup strategy and a robust storage capability.) Use this procedure when removing the VOD server for troubleshooting purposes, or when upgrading the software, in order to avoid the loss of this content information. This procedure can also be helpful for load balancing and failover. It can simplify the task of maintaining multiple servers with the same information.Note that *In order to backup database files, you will need administrative access to the VEMS Portal Server and a safe location to store the backup database and files.*

Topics in this section

System Backup

To ensure a successful system backup, you must follow the exact sequence of steps shown below. Also, since this process will interrupt any streaming video, you may want to schedule this procedure at night or during non-business hours.

▼   To back up the system:

1. Log into the Portal Server as the Administrator.
2. The MySQL Service will need to be stopped in order to have a clean copy of the database. Go to **Start > Control Panel > Administrative Tools > Services**.
3. Right-click on **MySQL** in the right pane and select **Stop**. There will be a list of other services that will stop. Take note of these other services and select **Yes**.
4. The Service Control window will show the progress of the Services being stopped. After the services have stopped minimize the Services window.
5. Open **My Computer** and save copies of the following directories in a safe backup location.

   C:\Program Files\MySQL\MySQL Server x.x\data
   C:\Program Files\VBrick\MCS\licenses
   C: \Program Files\VBrick\MCS\MCSPresentations
       <u>or</u> D:\VBrick\MCSPresentations
   C: \Program Files\VBrick\MCS\Presentations
       <u>or</u> D:\VBrick\Presentations
   C:\Program Files\VBrick\MCS\Logs\

```
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
```

6. To restart the **Services**, maximize the **Services** window.

7. Right-click on the **VBrick Object Starter** and select **Start**. This will start the **MySQL** services. If the VEMS Scheduler Module or other services were stopped in Step 3 above they will need to be started as well.

System Restore

To ensure a successful system restore, it is critical that you follow the exact sequence of steps shown below. Also, since this process will interrupt any streaming video, you may want to schedule this procedure at night or during non-business hours.

Note The database cannot be restored from a different version number of VEMS Portal Server or from the same version number after additional features (for example VEMS Scheduler) have been installed. To ensure a successful restore, always perform a backup after an upgrade or after installing new features. Restore the database only to an VEMS Portal Server instance with the same version number and with the same features installed.

▼ To restore the system:

1. Log into the Portal Server as the Administrator.

2. The MySQL Service will need to be stopped in order to have a clean recovery of the database. Go to **Start > Control Panel > Administrative Tools > Services**.

3. Right-click on **MySQL** in the right pane and select **Stop**. There will be a list of other services that will stop. Take note of these other services and select **Yes**.

4. A Service Control window will show the progress of the Services that will be stopped. After the services have stopped, minimize the **Services** window.

5. Open **My Computer** and restore the following directories from the backup location.

```
C:\Program Files\MySQL\MySQL Server x.x\data
C:\Program Files\VBrick\MCS\licenses
C: \Program Files\VBrick\MCS\MCSPresentations
    or D:\VBrick\MCSPresentations
C: \Program Files\VBrick\MCS\Presentations
    or D:\VBrick\Presentations
C:\Program Files\VBrick\MCS\Logs\
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
```

6. To start the Services, maximize the **Services** window.

7. Right-click on the **VBrick Object Starter** and select **Start**. This will start the **MySQL** services. If the VEMS Scheduler module or other services were stopped in Step 3 above they will need to be started as well.

AmiNET110 MPEG-2 STB

Overview

The AmiNet110 is a compact set top box for the Portal Server manufactured by <u>Amino</u> Systems. It connects to a standard TV and plays MPEG-2 streams only—no other streams are selectable for viewing or adding. These pages explain how to connect and configure the Amino set top box. There is no software installation required: simply connect and configure the device as explained below and you are done. The *Portal Server User Guide* explains how to use the Amino remote control unit to select streams and navigate Portal Server pages *after* the Amino is configured and running as explained here. The Amino *does not* support the following Portal Server functionality:

- Access Logging
- Scheduling
- Custom Fields
- Device Control
- Priority Alert
- Copyright Restrictions

Connecting the AmiNET110

Connect the Amino STB to a standard TV and to your Ethernet network as explained below. If necessary, refer to the illustrations in the *AmiNet110 User Guide* that came with the device. Check the components for damage as you unpack the device. The AmiNet110 includes a power supply, a mounting stand, a remote control, and an A/V cable.

▼   To setup and connect the Amino

1. Mount the Amino either vertically or horizontally as explained in the *AmiNet110 User Guide.*

2. Connect the Amino to your network using a standard Ethernet cable (not supplied) with an RJ-45 connector.

3. Connect the Amino to the TV as follows.

    a. Connect one end of the Amino A/V lead to the composite connector on the Amino.

    b. Connect the other end to either the S-Video connector on the TV or to the red, white, and yellow audio and video connectors.

4. Connect the power supply and install three AAA batteries in the remote control.

Configuring the AmiNET110

The Amino STB is shipped with a handheld IR remote control and an optional wireless keyboard. **You must use the Amino wireless keyboard to configure the set top box**.

▼ To configure the Amino using the wireless keyboard

1. Connect the Amino, the network, and the TV as explained above and power on the STB.

2. When the Amino splash page is displayed, press **Alt-m** on the keyboard.

3. Enter the read management password (default = **leaves**).

Note When the Amino Admin pages are displayed, you must use Shift + Arrow Up/ Arrow Down to navigate through the menus.

---

4. If a DHCP server is present, the Amino IP address is automatically obtained from the DHCP server.

5. If a DHCP server is not present, and you want to set a static IP address, select **Network Configuration**, set **DHCP Info** to **Do not use**, and enter the new IP address and other network data.

6. Select **Trusted Domains** and add the Portal Server IP address or host name to the list of trusted domains in the format: <**ip_address**> or <**hostname**> (do not use http://). Also verify that **Macrovision** and **JavaScript** are enabled.

7. Save changes and enter the write management password (default = **snake**).

8. Return to main menu and select **Browser Setup**.

9. In the **Home Page** field, enter the Portal Server URL as **http://<PortalServerIPaddress>**

10. Save your changes and push the **Home** button on the keyboard to launch the Amino MCS home page (Figure 27).
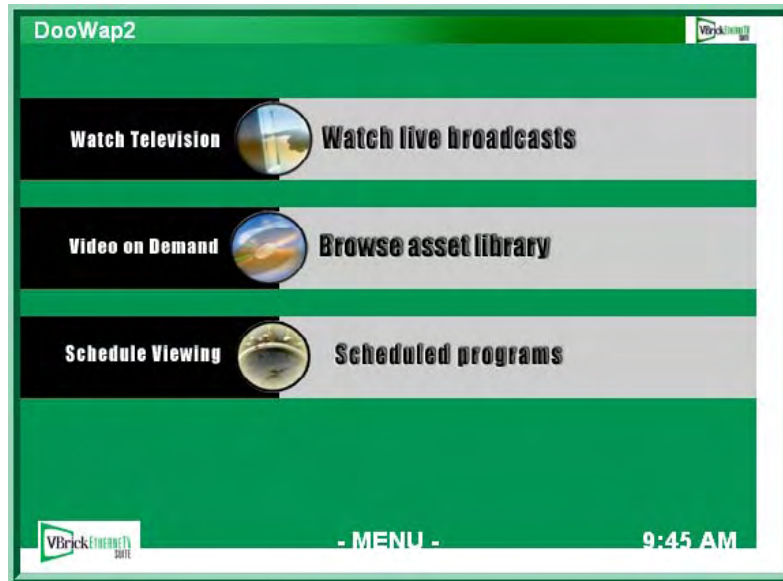
Figure 27. Amino MCS Home Page

11. Click on **Watch live media**, for example, to display the Live Media page (Figure 28). You can use this page to select any available MPEG-2 stream.
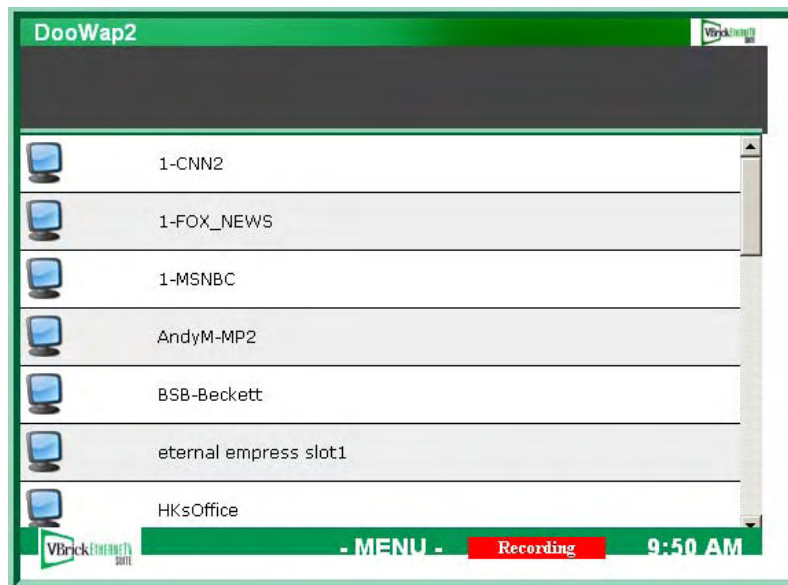
Figure 28. Live Media Page

Change the IP Address

Once the Amino is initially configured as explained above, you can change the IP address as necessary using the wireless keyboard.

▼ To change the IP address

1. Go to the Amino MCS home page (Figure 27) and press **Ctrl** on the keyboard.

2. Click **OK** to toggle the **Default Amino Keys** to **On**.

3. Press **Alt-m** on the keyboard and use the steps listed above in Configuring the AmiNET110 to set a new IP address.

4. Press **Ctrl** again to toggle off the **Default Amino Keys** and resume normal operation.

Configure a Direct Connection

In some cases you may wish to connect the Amino directly to a VBrick MPEG-2 appliance without using the Portal Server. In this case the attached monitor will display the single stream from the appliance in full screen mode. Note that when configured in this manner, the cursor will be displayed on the screen and cannot be removed. If necessary, use the arrow keys on the IR remote control to reposition the cursor.

▼ To connect an Amino directly to an MPEG-2 appliance

1. Open the management interface on the Amino (**Alt-m**).

2. Navigate to **Browser Setup > Home Page**.

3. In the **Home Page** field, enter the IP address of the VBrick appliance in the following format: **igmp://<vbrick_ipaddress>:port**

4. Reboot the Amino to display the MPEG-2 stream from the VBrick in full screen mode on the monitor.

Configuring the Remote Control for a TV

The Amino handheld IR remote control is designed to work with the Amino set top box. During normal operation, the **STB/TV** button (see the *Portal Server User Guide*) should be set for **STB**. It can, however, be configured to work with a standard TV. In order for the remote to transmit the correct signals to control the TV, it must be programmed with a 3-digit code that matches the TV. See the Amino Remote Controls User Guide for more information.

Configuring the AmiNET110 for a Widescreen

This procedure explains how to configure an Amino Set Top Box for MPEG-2 output to a widescreen (16:9) TV. Use one of the following methods depending on whether you are using the handheld remote control or the wireless keyboard. *When done, repeat these steps if necessary for each Amino set top box.*

▼ To configure for widescreen with the wireless keyboard

1. Press **Ctrl** to get into Amino keyboard mode.

2. Press **Alt-p** to get to **Preferences**.

3. On the **Preferences** menu select **TV system and Audio Settings**.

4. Change the **TV Display Format** to **Widescreen TV**.

5. Save changes, exit **Preferences**, and power cycle the STB.

6. Be sure to set the widescreen TV monitor to **Full** mode.

▼ To configure for widescreen using the remote control

1. Select the **Menu** button on the Remote Control to get to **Preferences**.

2. On the **Preferences** menu select **TV system and Audio Settings**.

3. Change the **TV Display Format** to **Widescreen TV**.

4. Save changes, exit **Preferences**, and power cycle the STB.

5. Be sure to set the widescreen TV monitor to **Full** mode.

Set the TV Display Format

As noted, you can change the **TV Display Format** from the **Preferences** menu. The following tables show the output from normal and widescreen TVs depending on how the **TV Display Format** is set. Be sure to power cycle the STB to implement any changes you make.

Table 23. Video Output with a Normal (4:3) TV

TV Display Format	Video Output
Standard (4:3) Mode	Normal (4:3) video plays normally and 16:9 video has the left and right sides cropped off (center cutout).
Letterbox Mode	Normal (4:3) video plays normally and 16:9 video has all the picture viewable with black bars on the top and bottom (letterbox).
Widescreen TV	Normal (4:3) video plays normally and 16:9 video displays all the picture but it is squashed in.

Table 24. Video Output with a Widescreen (16:9) TV

TV Display Format	Video Output
Widescreen TV	16:9 video plays normally and 4:3 video has black bars left and right (pillar box). This relies on the TV responding to aspect ratio switching signals on VBI line 23 (PAL only). On TVs that don't respond to this signal, you must set the TV aspect ratio manually to avoid a stretched or squashed picture.

ACNS Configuration

Overview

The Cisco Application and Content Networking System (ACNS) is a digital media delivery solution that reduces redundant digital media streaming traffic traversing a WAN from the data center to branch offices over satellite and terrestrial networks. Cisco ACNS offers a comprehensive set of streaming-media features that let you stream high-quality and long-playing digital videos live and simultaneously to thousands of users and media players and provide access on demand at a later time. By caching on-demand content, or prepositioning frequently accessed content, ACNS minimizes the need for the same digital media content to traverse WAN links from the data center to branch offices.

VBrick has partnered with Cisco to integrate VBrick's product line with Cisco's ACNS content distribution system. Integrated VBrick products include encoders, Video on Demand (VOD) servers, IP Receiver, PC and Mac clients, and the Enterprise Media System. The integration of these two industry-leading products means that customers with legacy networks can retain their existing network infrastructure and still deploy the latest in video delivery systems. The benefits of this product integration include unlimited geographic reach for video, reduced network circuit costs, higher quality video, and improved system performance. Cisco ACNS also provides a flexible management system for efficient operation, automation, and central management of the digital media delivery network.

Note The integrated Portal Server and ACNS Server solution handles MPEG-4 and Windows Media video files residing on Darwin, Windows Media, and VOD-W servers only. MPEG-1, MPEG-2, and H.264 files are not supported; VBrick's NXG (Linux) servers are not supported.

ACNS Configuration

To configure the Portal Server to work with ACNS you need to perform certain steps on the Portal Server and on the ACNS server. **If you have a VBrick VOD-W server, you will need to create a virtual directory in IIS before you configure the Portal Server or the ACNS server.** If you have a Darwin server or a Windows Media server, no additional configuration is required.

VOD-W Server Configuration

ACNS copies all MPEG-4 and WM video files from all (Windows Media, Darwin, and VOD-W) servers in your Enterprise Media System. (ACNS does not support NXG servers;

the Windows Media and Darwin servers require no additional configuration.) Use the following steps to configure a VOD-W server to work with ACNS.

▼ To configure a VOD-W server to work with ACNS:

1. Login the VOD-W server.
2. Go to **Start > Windows Explorer**.
3. Expand the tree in the left pane under the drive labeled (C:).
4. Expand Program Files under C: and then expand InfoValue under that.
5. Click on **QuickVideo OnDemand Server**.
6. Double-click on the file QvcsConfig.ini. The system should use Notepad to open the file.
7. Locate the line that reads "[Ingest]".
8. Locate the lines beginning with StoragePathN= shortly after the "[Ingest]" line where N is a number. Leave the Notepad window open.
9. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager.**
10. Expand the tree in the left pane and expand **FTP Sites**.
11. For each StoragePath line found in step 8, configure a virtual directory for it as follows:
    a. Right-click on the **Default FTP Site** and then select **New > Virtual Directory**.
    b. Click **Next** in the Welcome to the Wizard window.
    c. For **Virtual Directory Alias**, enter the text after the first backslash (\) from the StoragePath line whose data is being setup. For example, if the line reads StoragePath1=D:\Content, enter **Content** for the Alias. Click **Next**.
    d. For **FTP Site Content Directory**, click **Browse** and navigate to the directory specified in the StoragePath line whose data is being setup. Click **OK** then **Next**.
    e. In the **Access Permissions** window, click **Next** to select the default permission of Read.
    f. Click **Finish** to complete creation of the new Virtual Directory.
12. You will also need to configure the VOD-W Server to allow anonymous connections.

▼ To allow anonymous connections:

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager.**
2. Expand the tree in the left pane and expand **FTP Sites**.
3. Right-click on the **Default FTP Site** and select **Properties**.
4. Go to the **Security Accounts** tab, check **Allow Anonymous Connections**, and click **OK**.

Portal Server Configuration

Portal Server integration with Cisco's ACNS Server is available with Portal Server v4.0.1 or later software. The following procedures explain (1) how to configure a manifest file on the Portal Server that will be used by the ACNS server to ensure that the content on the ACNS Server matches the content on the Portal Server; and (2) how to verify that forced use of TCP for MPEG-4 content is disabled.

▼ To create a manifest file on the Portal Server:

1. Install VEMS v4.0.1 or later from the VEMS Product CD See the *VEMS Portal Server Release Notes* for detailed instructions.
2. After installing the Portal Server, open the Portal Server Admin Console and go to **Global Settings > Global Assignments > Set Cisco ACNS Manifest Options**.

3. Check **Enable manifest generation**, select the files (MPEG-4 and/or WM) to include, and specify an interval (default = 10 minutes) that defines how often the file will be regenerated.

4. Click **Submit** when done.

5. Click **Generate Now** to create an "on demand" manifest file. The Portal Server will create (and periodically overwrite) a manifest file called `ACNSManifest.xml` in the `Program Files\VBrick\MCS\Cisco` folder. The `Cisco` subdirectory is automatically created.

When a Portal Server is configured to integrate with an ACNS network, content playback is redirected to stream from ACNS nodes only if RTSP is used for video transmission. To use RTSP, verify that the Portal Server option to "Always use TCP" is unchecked (this is the default).

▼ To verify that TCP is off:

1. Go to **Global Settings > Global Assignments > Assign LAN/Internet Address Range(s)**.

2. Verify that **Always use TCP protocol (HTTP Tunneling/RTSP Interleaving) for MPEG-4 and Windows Media content?** is unchecked.

ACNS Server Configuration

Note that installation, configuration, and support for ACNS must be provided by Cisco and/or their representatives. Use the following steps to point to the Portal Server manifest file and set other configuration options.

▼ To set configuration options and identify the manifest file:

1. Be sure the ACNS Server is running and launch an Internet Explorer browser.

2. Go to the ACNS Management URL, for example `https://<ipaddress>:8443`.

3. Log into the ACNS Management Tool.

   Username: `admin`

   Password: `default`

4. Click on the **Services** tab at top of page.

5. Create a **Content Channel** for the VOD server.

6. Click on **Channel Content** on the left.

7. Near the top of the screen, set the **content acquisition method** to **specify external manifest file**.

8. In the **Manifest URL** field enter the Portal Server URL in the following format:

   `http://<MCSipaddress>/Cisco/ACNSManifest.xml`

9. Set the **Check manifest every** field to desired interval (60 minutes is recommended).

10. To check the manifest file, click **Validate** to open a pop-up that will show the manifest. The last message should indicate the manifest is correct.

11. Click **Fetch manifest now** to start content replication.

12. To check the status of the content replication click on **Replication Status** on the left side of page. The system is ready when the following is true:

    `Acquisition status` is `Completed`.

    `Device states` at the screen bottom are `Completed`, and the `In Process` counts are zero.

Verify Installation

▼ To verify the VEMS/ACNS integration is successful:

1. Be sure that the VEMS Portal Server and ACNS are configured as explained above.

2. Go into the ACNS management system and verify that the video content added via the VEMS Portal Server has been pushed to the ACNS remote content engine's disk storage.

3. Open a browser and launch a Portal Server client.

4. Launch a stored MPEG-4 or WM video from the Portal Server user interface. The MPEG-4 or WM content should run and play successfully to conclusion.

5. If you run a packet sniffer on the VEMS client, a trace will show that the client was redirected to play the content from a Cisco node and not from a VBrick VOD server.

NXG-to-VOD-W Content Migration

This chapter explains how to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG (Linux) VOD server to a VBrick VOD-W (Windows) VOD server. This migration is a two-step process:

▼ To migrate NXG files

1. First run the Linux script `VBListAssets.sh` on the NXG VOD server to create an asset list that identifies all video files present on the server.

2. Then run the migration tool to replicate these files on the VOD-W server.

Creating an Asset List

Use the steps listed below to run a script that will create an asset list (see Sample Asset List) of all video files on the NXG server. **The script requires that the following files be FTPed to the NXG server.** These files are located in the Portal Server utilities folder at: `C:\Program Files\Vbrick\MCS\utils\NXGtoVODWMigrationTools`

`VBListAssets.awk`

`VBListAssets.sh`

▼ To FTP the files and run the script

1. Open a Command Prompt on your PC and change directories to the folder with the files listed above.

   `FTP <NXG_ip_address>`

2. Login as user = **vbrickuser**; password = **vbrickuser**

   `ftp>` **bin** to transfer the files in binary mode.

   `ftp>` **mput VBL*** to transfer the script to the server. When prompted, answer **y** to allow the file transfer.

   `ftp>` **quit** to exit FTP.

3. Telnet to the NXG server to run the script.

   `telnet <NXG_ip_address>`

4. Login as user = **vbrickuser**; password = **vbrickuser**

   `chmod 777 VBL*` to make the script files executable (FTP will not do this).

   `./VBListAssets.sh` to run the script.

5. Wait approximately two minutes until the script completes. When prompted for password, type the root password (default = **omnibase**) and press **Enter**. The file `nxg_asset_list` will be created in the current directory. The script should not generate any output. If it does, note the output for analysis by VBrick Support Services.

6. Copy `nxg_asset_list` to the Portal Server machine or use an FTP URL in the **Assets** field of the Migration Tool. For example:

`ftp://vbrickuser:vbrickuser@<server_ip_address>/nxg_asset_list`

Sample Asset List

This snippet shows sample assets included in the file `nxg_asset_list`. Each asset is described by name and location.

```
<assets>
   <asset>
      <name>/demo/TestAutoIngest4.mpg</name>
      <location>/vbrick/content_links/20071005113535_1</location>
   </asset>
   <asset>
      <name>/1_MSNBC_05_16_07_16_12_41.mpg</name>
      <location>/vbrick/content_links/20071005113535_2</location>
   </asset>
   <asset>
      <name>/Rec9.mpg</name>
      <location>/vbrick/content_links/20071005113535_3</location>
    </asset>
 </assets>
```

Using the Migration Tool

The Migration Tool is used to migrate MPEG-1 and MPEG-2 video files from a VBrick NXG VOD server to a VBrick VOD-W VOD server. The original content remains on the NXG server and is not affected. The Migration Tool is a Windows-based application that is installed with the Portal Server installation and should be run on the Portal Server machine. Once you have created an asset file, use the following steps to actually migrate files to the VOD-W server. Note that the ingestion process on the VOD-W server is CPU and bandwidth intensive. You may want to run the migration during off-peak hours and increase the ingestion rate as explained below. Be sure to read the following important notes.

Note • Both the **Source** and **Destination** VOD servers must be defined in MCS and must be running.

• You must create an MCS user (or configure MCSClient, the default user) that can access the **Destination** VOD-W server but *cannot* access the **Source** NXG server. See Configuring Users on page 135 for details. The MCS user must be configured as follows.

   • Allow Access to Specific VOD Servers – select only the destination VOD-W.

   • Allow Access to Specific VOD Content – select all VOD Folders.

   • Allow Content Publishing – select all Available Folders.

• The Migration Tool will not run if SSL is enabled on the Portal Server. To disable SSL, re-comment the `web.config` file for Portal Server User pages *and* the Portal Server Admin pages. See Configuring for SSL on page 147 for details.

Increase the Ingestion Rate

You can make the migration process substantially faster by increasing the rate at which files are ingested on the VOD-W server.

▼ To increase the ingestion rate

1. On the VOD-W server, go to **Start > Control Panel > InfoValue QuickVideo > QVCS > Advanced**.
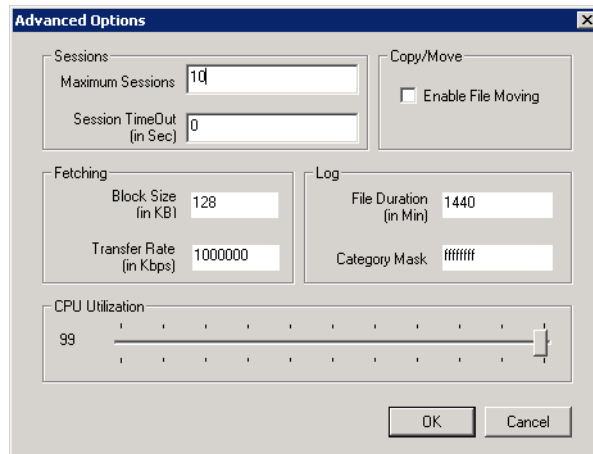
2. Set the **Transfer Rate** to **1000000** and click **OK**. Click **OK** again to exit.

3. When the content migration is complete, reset the **Transfer Rate** to the default (**10000**).

Run the Migration Tool

▼ To migrate video files to the VOD-W

1. Launch the Migration Tool. Go to C:\Program Files\Vbrick\MCS\utils\ NXGtoVODWMigrationTools and double-click on VBMCSReplicateContent.exe

2. Complete all required fields as explained below.

3. Select **Save to File** to create a status file that will show which files were ingested successfully.

4. Click **Start** to begin the migration immediately, or use the scheduling options to run later.

5. If necessary, when the content migration is complete, reset the **Transfer Rate** to the default (**10000**).
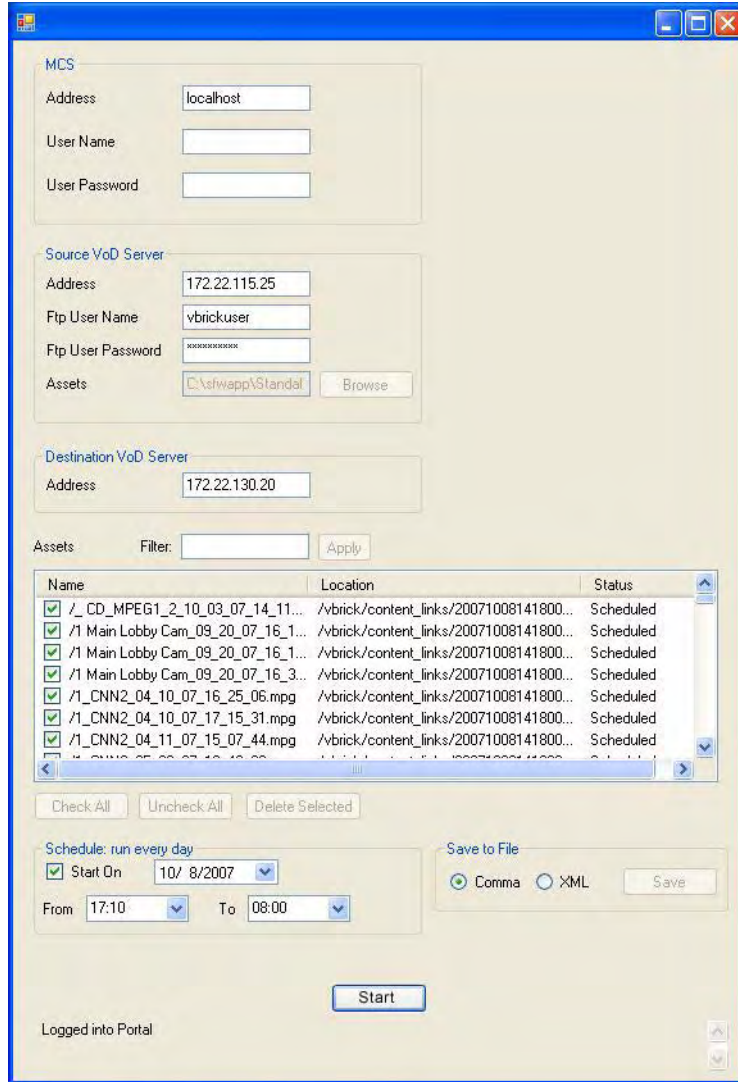
MCS	
Address	IP address of VBrick Portal Server.
User Name	User name for Portal Server.
User Password	User password for Portal Server.
Source VoD Server	
Address	IP address of source NXG server.
Ftp User Name	FTP user name of NXG server. Default = `vbrickuser`
Ftp User Password	FTP password of NXG server. Default = `vbrickuser`
Assets	Browse to the file `nxg_asset_list` or use an FTP URL in the following format: `ftp://vbrickuser:vbrickuser@<server_ip_address>/nxg_asset_list`
Destination VoD Server	
Address	IP address of destination VOD-W server.

Assets	
Filter	Optional. Enter an alphabetic substring to search for matching files and click **Apply**.
File Names	Select the video files to be migrated from the complete list of files in the asset list. Use **Check All**, **Uncheck All**, or **Delete Selected** as appropriate. Note that **Delete Selected** works with selected (i.e. highlighted) files and *not* checked files.
Schedule	
Start On	Start date. Default = unchecked. The tool will migrate files every day beginning at the specified hour.
From/To	The migration will run during the specified time period.
Save to File	This option saves a `status.xml` file that shows migration results. If some files fail to ingest during migration, you can point to this file in the **Assets** field and repeat the migration. • Comma – save the status file as comma separated values. This can be displayed in a spreadsheet or an editor. • XML – save status file as an .xml file. This file is identical in format to the asset list (see <u>Sample Asset List</u>) and can be used to repeat the migration.
Start/Stop	Start a migration; stop a migration currently in progress. You may want to stop the migration and correct a problem if multiple failures are shown in the Status column. See <u>Recover from Migration Errors</u> below.

Recover from Migration Errors

Migration errors are shown in the **Status** column. Once started, the migration will continue until each ingestion reports either success or failure. If you stop the migration, all queued ingestions are removed (click yes on the popup) from the Portal Server and you can correct the errors and restart the migration when ready.

If you ignore the popup window (click no on the popup), you will have to either remove queued ingestions manually from the Portal Server or wait until all ingestions are complete with either failure or success. Then you can fix the errors and restart. You may see duplicate asset file errors in the migration **Status** column. These errors indicate that the asset already exists on VOD-W and the Portal Server and can be safely ignored.

Verifying the Migration

Use the **Save to File** (XML) option to create a `status.xml` file which lists the video files that failed to ingest. If some files fail to ingest during migration, you can point to this file in the **Assets** field and repeat the migration.

Purchased Content Ingestion

Overview

Enterprise Media System users have the option of purchasing pre-packaged content from VBrick. If content was included on your original order, this purchased content is installed on your VOD servers prior to shipment. If content was not included with your original order, you will need to install this content on your VOD servers as explained here. *This procedure is highly technical and should be performed by a knowledgeable system administrator with suitable IT experience.* Note that VBrick does not support the ingestion of third-party content not purchased directly from VBrick.

The content package you purchased is shipped on a LaCie USB drive. If you open the USB drive in Windows Explorer, you will see that each content package is named by part number and text description. Each package has a corresponding Excel metadata spreadsheet describing the content in the package and a license file that contains content expiration data. The spreadsheet and license are used during the ingestion procedure. The Excel metadata spreadsheet for the package is inside the package folder with a name like `8000-0120 Clearvue HS MPEG Gold 7-17-08.xls`. You must copy this spreadsheet to your local C: drive. The license file has a name like `content_34294950443.lic`. You must install the license using the Windows **Add or Remove Programs** utility. The Mass Ingestion Utility is installed with the Portal Server and is located in `C:\Program Files\VBrick\MCS\bin\MassIngestionUtils.exe`

Note Content Ingestion to an SSL-enabled VOD-W is not supported. To ingest content to an SSL-enabled VOD-W, first disable SSL and run the ingestion; then re-enable SSL when done. See <u>Configuring for SSL</u> on page 147 for more information.

Configuring IIS

The following procedures explain how to ingest content to your VOD-W and/or VOD-WM servers. First you need to configure certain settings in IIS.

▼ To configure IIS for mass ingestion

1. Shutdown the Portal Server and attach the appropriate LaCie drive to a USB port.

   a. Restart the server.

   b. Copy `MassIngestionUtils.exe` and `MassIngestionUtils.exe.config` from the `\Utilities` directory on the LaCie drive to `C:\Program Files\VBrick\MCS\bin\` directory.

   c. Copy `xlviewer.exe` from the `\Utilities` directory on the LaCie drive to the desktop. Then double click on `xlviewer.exe` to install Microsoft Office Excel Viewer 2003.

2. Open IIS Manager.

   a. Expand the Local server and then the FTP server.
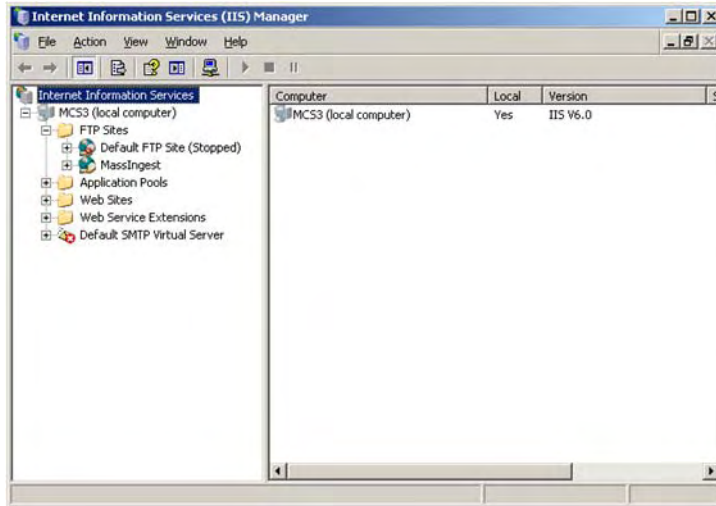
   b. Add an FTP site called **MassIngest**.
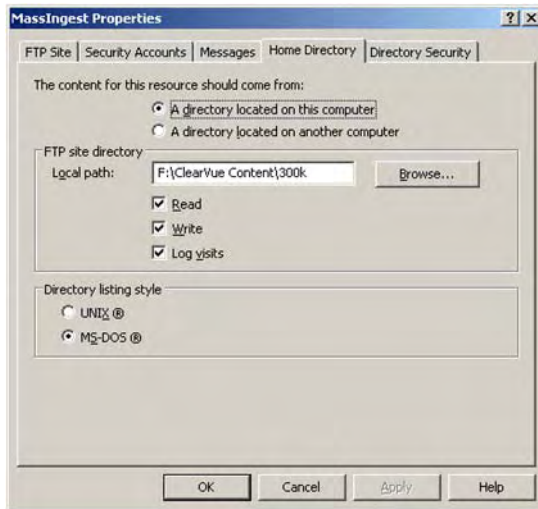
   c. Map the FTP site to the directory on the LaCie USB drive that has the video to be ingested.
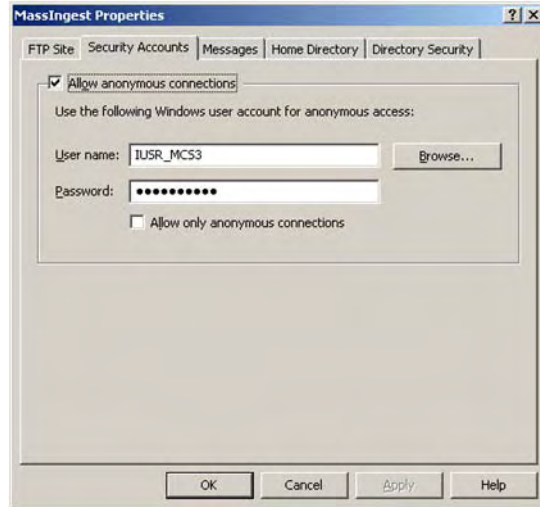
      d.   Set permissions to allow for anonymous FTP and close IIS.

3.   Copy the Excel spreadsheet from the flash drive to your C:\ drive.

4.   Install the license file (for example content_34294950443.lic) using the Windows **Add or Remove Programs** utility.

      a.   Go to **Start > Control Panel > Add or Remove Programs > VBrick Media Control Server Suite**.

      b.   Click **Change/Remove** and select **Install/Replace the EtherneTV Content license file**.

      c.   Click **Next**, then browse to the file and click **Open**.

5.   Manually close the window when done. See <u>Install/Replace License Files</u> on page 17 for more information.

Ingesting Content

Configure a VOD-W Server

VOD-W only. Use the following steps, prior to ingestion, to change the **Transfer Rate** from 10,000 to 1,000,000 Kbps. Make sure to change the ingestion limit back to 10,000 after all content has been ingested.

▼   To change the ingestion limit on a VOD-W

1.   Go to **Start > Control Panel**.

2.   Click on **VOD-W QuickVideo**.
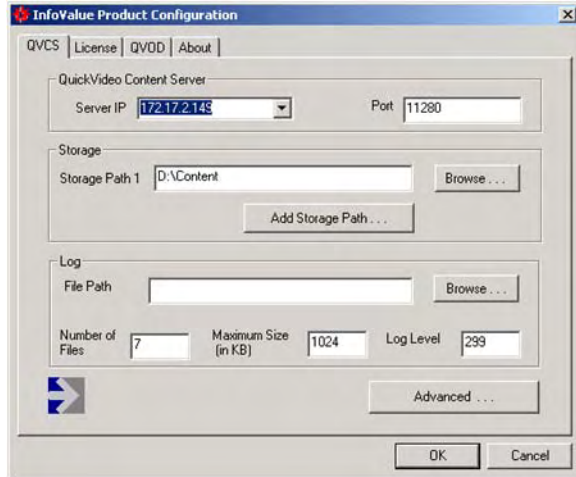
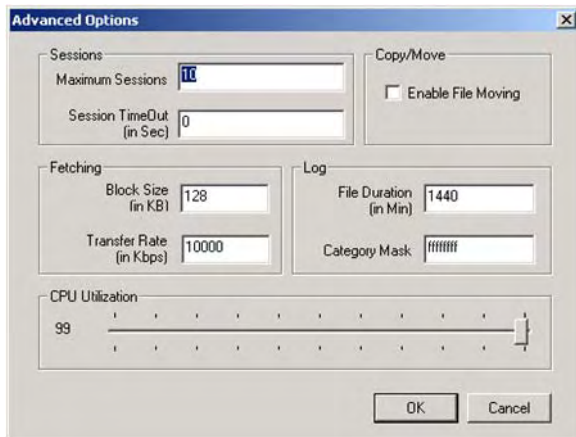3. Click on the **Advanced** button.

4. Change **Transfer Rate** from 10,000 to 1,000,000, click **OK** and **OK** again.
5. Reboot the VOD-W Server for the changes to take effect.

Ingest Purchased Content

▼ To ingest purchased content to your VOD servers

1. Run the C:\Program Files\VBrick\MCS\bin\MassIngestionUtils.exe program.
2. When the window opens, go to **Options > Initiate Mass Ingestion**.
3. When the Mass Ingestion utility starts:
   a. Set **Local Video Content Path** to the actual path.
   b. The **Ingest Source Directory** is ftp://[Portal Server IP Address]/MassIngest.
   c. Set the **Metadata File Path** to the location of the Excel spreadsheet.
   d. The **Sheet Name** should be Sheet1.
   e. The **MCS Server IP** is the address of the Portal Server.
   f. Select the **VoD Servers** to receive the content.
   g. Press the **Validate** button.
   h. Then press **Continue** and wait for the ingestion to complete. This may take from 2–8 hours.

4. After mass ingestion is complete, review the total results displayed on the Mass Ingestion utility. (The total results cannot be saved.) On the Portal Server, open Microsoft Office Excel Viewer 2003, view the Excel spreadsheet from the MCS `C:\` drive and check for failures on columns A, C and E. The columns should be populated with True and if False is shown, a failure has occurred. This means that the video file with the False failed to ingest. Contact VBrick Support Services if any failures occur. Note: the .xls file will now contain failure information only and was modified during the ingestion process. **Be careful not to overwrite the original .xls file.**

5. When done, change the **Transfer Rate** on your VOD-W back to 10,000 Kbps. (See Configure a VOD-W Server on page 219.)
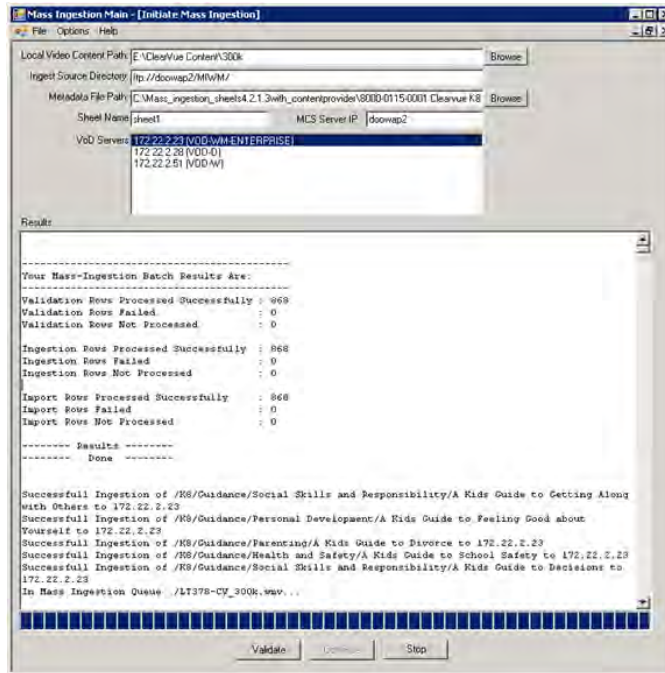
Note When a large ingestion completes, the utility may not respond to mouse commands for a few minutes. This is normal and for best results, wait a few minutes for it to recover.

Backing Up the Database

Once Mass Ingestion is complete, it is recommended that you perform a full database backup. To ensure a successful database backup, you must follow the exact sequence of steps shown below. Also, since this process will interrupt any streaming video, you may want to schedule this procedure at night or during non-business hours.

Note If you purchased Enterprise Media System Backup, all key directories are backed up every ten minutes. With VEMS Backup there is no need to perform a manual database backup.

▼ To backup the database

1. Log into the Portal Server as the Administrator.

2. The MySQL Service will need to be stopped in order to have a clean copy of the database. Go to **Start > Control Panel > Administrative Tools > Services**.

   a. Right-click on **MySQL** in the right pane and select **Stop**. There will be a list of other services that will stop. Take note of these other services and select **Yes**.

   b. The Service Control window will show the progress of the Services being stopped. After the services have stopped minimize the Services window.

3. Open **My Computer** and save copies of the following directories (and the Metadata file) in C:\VBrick Backup.

   C:\Program Files\MySQL\MySQL Server x.x\data

   C:\Program Files\VBrick\MCS\Images\Thumbnails

   C:\Program Files\VBrick\MCS\licenses

4. Copy the entire contents of the VBrick Backup directory to a flash drive and later burn a CD of these files.

5. To restart the **Services**, maximize the **Services** window. Then right-click on **VBrick Object Starter** and select **Start**. This will start the **MySQL** services. If the VEMS Scheduler Module or other services were stopped above they will need to be started as well.

VBrick Internet Streaming

Overview

The VBrick Internet Streaming is available for those users who wish to extend the ability to view live events to Internet clients. This document concentrates on users who intend to use the Internet Streaming service to provide additional services in Portal Server installations. In all cases, the basic scenario is that a user wants to schedule an event via the Portal Server, and wants the event to be made available to Internet users via a hosted service. VBrick Internet Streaming capabilities allow customers to extend the reach of their video to the Internet. In order to do this, the customer needs to do the following:

1. Choose whether they want end users to view the video through the Portal Server or via a different external web page (for example their external web site or VBrick's VBOSS site).
2. Purchase streaming bandwidth from a Content Distribution Network (CDN). VBrick offers this through our VBOSS service or the customer can purchase their own.
3. Configure the VBrick to send the stream to the CDN

Potential viewers fall into two categories as follows:

*   Authenticated Internet-based Portal Server clients – In this option, streams are viewed via the Portal Server interface (multicast or unicast) and all viewers can be authenticated. In this mode, the Portal Server must be in the DMZ to allow access to the Portal Server web pages from the Internet.
*   Non-Portal Server Internet web page viewers – These viewers are notified via e-mail that a stream is available. VBrick's Internet Streaming solution includes a bandwidth allowance and a hosted URL for live viewing. The service is available with a Windows Media (WM) VBrick appliance included or may be utilized by Portal Server customers who have purchased WM VBrick appliances. The viewing screen is configured as part of the VBOSS (VBrick Online Streaming Server) interface. Access to this interface may be limited via a password. For more information about customizing and using VBOSS, see the *VBOSS Broadcast Publisher Guide*.

Streaming Service Workflow

The following information is required in order to properly configure the VBrick WM appliance. For customers who purchase the VBOSS service, this information will be provided to you when you order the service. Other customers need to obtain this information from their CDN. When you purchase the VBrick Online Streaming Service, the VBrick administrator will provide the following host configuration information:

    a.   Server Name/IP and Port

     b.   Publishing Point Name

     c.   Publishing Point User Name

     d.   Publishing Point Password

     e.   Publishing Point Viewing URL

     f.   Hosted Page Viewing URL

The information labelled a–c above is entered on the VBrick appliance Push configuration page. When the event is initiated (via the Scheduler), the Portal Server turns on the Push transmit and streams to the remote publishing point. Internal authenticated users are directed to view the multicast/unicast directly from the VBrick encoder appliance. **You can only initiate the push via a Portal Server "schedule" that turns on a local multicast or unicast server.** External viewers are directed to the publishing point of the service provider. If the event presenter wishes to provide event access to non-authenticated viewers via an e-mail, he would e-mail the interested viewers the hosted page viewing URL (f). This mode does not require access to the Portal Server and the video will be launched using a Windows Media Player.

Portal Server Hosting

VBrick Configuration

VBrick Push Configuration

Regardless of whether you are serving remote Portal Server clients or non-Portal Server Internet web page viewers, the VBrick must be configured to push the stream to the provided destination hosting URL. The information in a–c should be entered in the appropriate fields as shown below. See the *WM Appliance Admin Guide* for more information.

Figure 29. VBrick Push Configuration Page

Maximum Push Destinations	One push destination is required for this application.
Enable	Use to enable HTTP Push. Normally this is left as Disabled for this application. The Scheduler will set this field to enabled when the schedule starts.
Server:Port	Enter the information from (a) Server Name/IP and Port from above.
Publishing/Mount Point	Enter the information from (b) Publishing Point Name
Copy From Publishing Point	Leave blank.
Auto Remove	Leave blank.
User Name	Enter the information from (c) Publishing Point User Name
Password	Enter the information from (d) Publishing Point Password
Domain Name	Leave blank.

VBrick Announce Configuration

▼   To configure the VBrick announce:

1.   Launch IWS, then go to Configuration: Encoder > Server and scroll to bottom of page.

2.   Set the **Stream Advertisement** to **Push to Microsoft Reflector** as shown below.

3.   Enter the Portal Server IP Address in the **IP Address or Host Name** field.

4.   If you wish to provide viewing to remote Portal Server clients, enter (e) in **URL** field.

Figure 30. Configuration: Encoder > Server > Announce(SAP)

IP Address or Host Name	The Portal Server IP address or broadcast IP.
URL	Enter (e) the Publishing Point URL.

Portal Server Configuration

Portal Server Admin Configuration

▼   To configure the Portal Server:

1.   Go to Global Settings > Global Assignments > Assign LAN/Internet Address Range(s).

2. Click on **Specify LAN Address Range(s)** and enter the address range of your local LAN. Internal users are identified by this range. Note: the VBrick encoder IP Address must be in this range.

Portal Server User Configuration

If authentication is enabled on the Portal Server, users must be authenticated and given Live Channel Privileges. See the *Portal Server Admin Guide* for more information.

Portal Server Scheduler Configuration

A live broadcast can only be initiated using the Portal Server Scheduler component. A stream will be pushed to the configured destination, from your VBrick appliance, at the configured date and time. You will also need to enable **Ext. SAP** and **HTTP Push** as explained below.

▼ To push the stream via the scheduler:

1. Launch the Scheduler and go to Schedule: **Live Broadcast**
2. For **Video Source** select **VBrick**.
3. Highlight your WM VBrick network appliance in the list of VBrick Host Names.
4. If the local LAN is multicast-enabled select a multicast destination, otherwise select unicast destination.
5. Go to **Advanced Settings** and enable **HTTP Push**.
6. If you wish to allow access to remote Portal Server clients, Enable the **EXT SAP**, otherwise leave this disabled.
7. Schedule End options should be left as **Disabled**.

Figure 31. Portal Server Scheduler Page – Advanced Options

Embedding a VBrick Player

Overview

A VBrick embedded player for streaming video is available for applications that require a standalone player that can access VEMS content. Depending on the application, the embedded player can access live content, stored content, or both live and stored content. The embedded player is designed for a wide variety of applications and two of the most common scenarios (1) embedding a player in a web page and (2) embedding a player in Microsoft SharePoint are described below. Note the required Required Browser Settings explained below.

Required Browser Settings

If you are using the embedded player <u>or</u> the SharePoint web part interface, the VEMS server must be configured in your browser as a "trusted site." If not configured as a trusted site, a VEMS client may not be able to login, or the custom settings for the viewer pages may be lost.

▼ To add the VEMS server as a trusted site:

1. In Internet Explorer go to **Tools > Internet Options > Security**.

    In Firefox go to **Tools > Options > Privacy > Exceptions**.

2. Click on **Trusted sites** and **Sites**.

3. Enter the URL of the VEMS server. If you are <u>not</u> using https be sure to uncheck "Require server verification (https) for all sites in this zone."

4. Then click **Add**, **Close**, and **OK**. Once the VEMS server is added as a trusted site it will be able to pass session cookies to the end user (i.e. client) PCs.

Embedding a Player in a Web Page

The VBrick player (Figure 32) can be embedded in a web page and used to access live and stored content on a VEMS server. All of the controls, including fullscreen and the pop-up player window, are fully functional. If authentication is enabled on the server, each viewer will need to login with valid user credentials before viewing content. Note that the embedded player streams live and stored video. If your page has links to "presentations," they will play in a separate pop-up window. The best practice is to host the page with an embedded player on VEMS. Because of the security settings in Internet Explorer, if you do not host the embedded player web page on VEMS, you will need to disable script debugging to prevent "access denied" errors. To disable script debugging in Internet Explorer go to Tools >

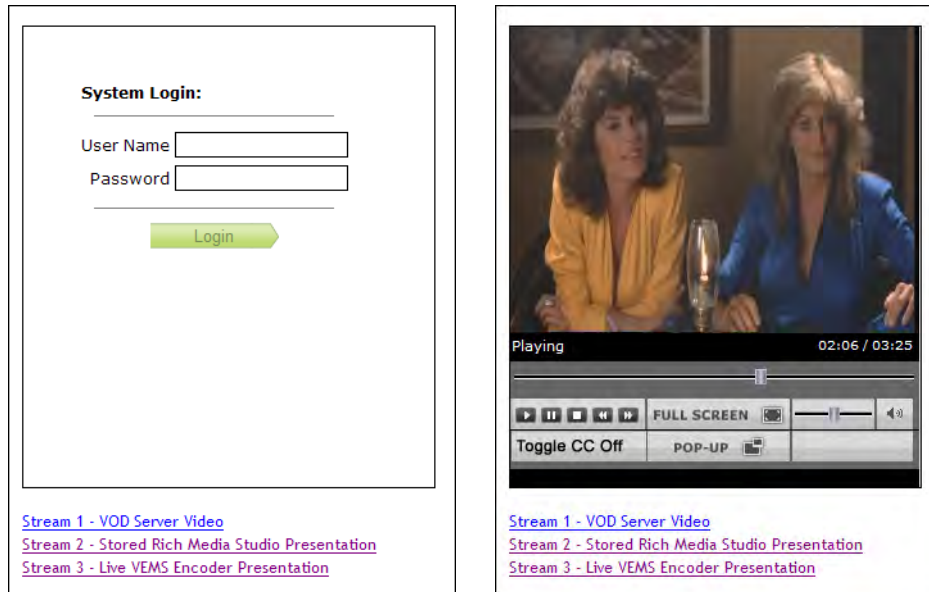Internet Options > Advanced. Navigate to "Browsing" and check Disable script debugging (Internet Explorer).

Figure 32. Embedded VBrick Player

Embedding a VBrick Player

The following steps explain how to embed links in a web page (see Figure 32) using the embed code from the **Share Media** feature in the client interface. Note that **Share Media** pop-up window may vary slightly depending on how your system is configured. It may have a local link and/or an Internet link. The local link let's you share content with users on your local area network. The Internet link let's you share content with users on the outside Internet. Note that the Internet link must be configured by an administrator and may not be displayed on your system. It let's you share content with users on the outside Internet. For more information about these links, see the "Sharing Media" topic in the *Portal Server User Guide*.

▼   To embed a VBrick player in a web page:

1.   In VEMS go to the **Media Library** or the **Live Media** page.

2.   To select a stream, click on the **Share Media** icon ✉ and then and click **Embed Player** (you don't have to launch the stream).
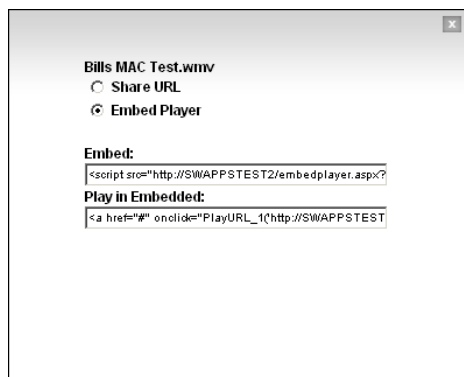
3. Copy and paste the **Embed** code <u>and</u> the **Play in Embedded** code into a web page (see <u>Sample Web Page Code</u> below.

4. To add additional URL links, add only the **Play in Embedded** code to the existing web page.

5. Be sure to add the VEMS server as a trusted site and disable script debugging (if necessary) as explained above.

Note Presentations do not play in the embedded player. To have a link open a live or stored presentation, use the **Share Media** feature on the Live Media or Media Library page in the client interface.

Sample Web Page Code

The following code shows an example for a simple HTML web page. It shows the **Embed** code within the `script` tags followed by three **Play in Embedded** (`HREF`) links. The last link launches a presentation and the URL was copied from the e-mail auto-generated by the presentation tool in the VEMS client.

```
<body>

<div>

<script src="http://SWAPPSTEST2/
embedplayer.aspx?embed_id=1&template=embeddedplayertemplate1.htm&gpgid=4d435353656
17263684c6f6769632e5341504275636b6574103233392e32322e3137332e3130207661633a3434343
420766163&gptitle=A-StanWM%20Program%201">

</script>

<p><span class="style1">

<a href="#" onclick="PlayURL_1('http://SWAPPSTEST2/
GeneralPlayer.aspx?embed_id=1&gpgid=4d43535365617263684c6f6769632e5341504275636b65
74103233392e32322e3137332e3130207661633a3434343420766163&gptitle=A-
StanWM%20Program%201');">Stream 1 - VOD Server Video</a></span><span
class="style1"><br/>

<a href="#" onclick="PlayURL_1('http://SWAPPSTEST2/
GeneralPlayer.aspx?embed_id=1&gpgid=4d43535365617263684c6f6769632e566f44436f6e7465
6e744275636b6574102f43687269735f574d204f666669636520537061636555f31325f30315f30395f
31355f33375f31372e776d76&gptitle=Chris_WM%20Office%20Space_12_01_09_15_37_17.wmv')
;">Stream 2 - Stored Rich Media Studio Presentation</a></span><span
class="style1"><br/>

<a href="http://SWAPPSTEST2/Present/Launch_Detail_View.aspx?ScheduleID=9&type=3
">Stream 3 - Live VEMS Encoder Presentation</a></span></p>

</div>

</body>
```

Using the VBrick Templates

For experienced web developers, VBrick also provides three templates you can use to customize the embedded player associated with the **Share Media** feature in the VEMS client. These templates are located in `C:\Program Files\VBrick\MCS\` and are named `embeddedplayertemplate1.htm`, `2`, and `3` respectively. The embedded players defined in templates 1, 2, and 3 are shown below from left to right. *By default, the Share Media feature uses embeddedplayertemplate1.htm.* You should be an experienced web developer if you are planning to modify these files. In all cases you should backup the originals before making any changes.

Figure 33. Embedded Player Templates

▼   To modify the embedded player template:

1. Open the template file in your development environment.

2. Make any appropriate changes and save the file back into VEMS as `C:\Program Files\MCS\embeddedplayertemplate1.htm`

Embedding a Player in SharePoint

The VEMS SharePoint Interface lets you integrate a chronological list of VEMS VOD content into Microsoft SharePoint as a Web Part. If you have rights to view the content you can click on any item in the embedded list to play that content in a VEMS popup window. Figure 34 shows a sample embedded list that uses the default color values. The VEMS SharePoint interface requires VEMS 5.2 or higher and Microsoft SharePoint 2007 or higher.

|	
Notes	• The configuration procedures described on the following pages must be performed by a SharePoint administrator with appropriate site privileges. A typical user will not be allowed to administer the SharePoint site.
	• Be sure that client viewers have added the VEMS server as a trusted site. See <u>Required Browser Settings</u> on page 227 for details.
	• You can only embed one list of VOD content per HTML page. You can embed a list on multiple pages in SharePoint but only once per page.
	• Macintosh (Safari) clients must adjust the default cookies behavior or the SharePoint interface will not work. In Safari go to Preferences > Security > Accept Cookies and set to "Always."
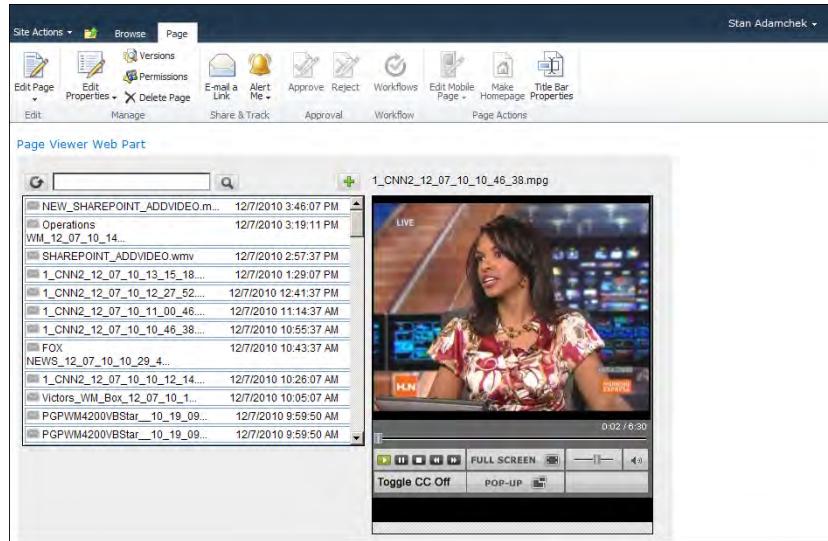
Figure 34. SharePoint Page with VEMS Interface

Note The Microsoft SharePoint interface to VEMS supports stored content on a VOD server. **It does not display or play live streams.**


The VEMS SharePoint Interface is used to expose specified VOD items in SharePoint. For example an organization may have a Microsoft SharePoint system and each department is assigned its own SharePoint area. In this scenario Human Resources has a SharePoint area and can display a list of all VEMS content in the "HR" folder on the VEMS system. The embedding procedure sets the appropriate query string values in the URL (for example `spfolder=/HR`) and the list will now be embedded for all users who have access to the HR page. The VEMS SharePoint Interface supports multiple VEMS authentication methods including:

• No authentication
• VBrick Authentication
• LDAP Authentication
• LDAP Authentication with Microsoft Integrated Authentication (SSO)

In the event that authentication is enabled and it is not single-signon (SSO), the user will be prompted for a user ID and password before they can view the VEMS SharePoint Interface list. SharePoint users will not see video content they have no rights to view. The list is compiled based on the users rights.

Adding and Sharing Video

If the corresponding query string variables are enabled in the <u>Base Interface URL</u> users can also share video via an e-mail message using the envelope icon ✉ or add stored video using the plus icon ➕ (displayed only if the user has **Add Video** privileges in VEMS). If desired, you can also embed a standalone Add Video interface (Figure 35) rather than the standard VEMS interface. Again, users will only see this page if they have **Add Video** privileges in VEMS. The steps for embedding the standalone Add Video interface are the same as those for embedding the VEMS interface except you replace `SPStoredMedia.aspx` in the base interface URL with `SPAddVideo.aspx`. All of the same query string variables used for the VEMS interface can be used with the Add Video interface.
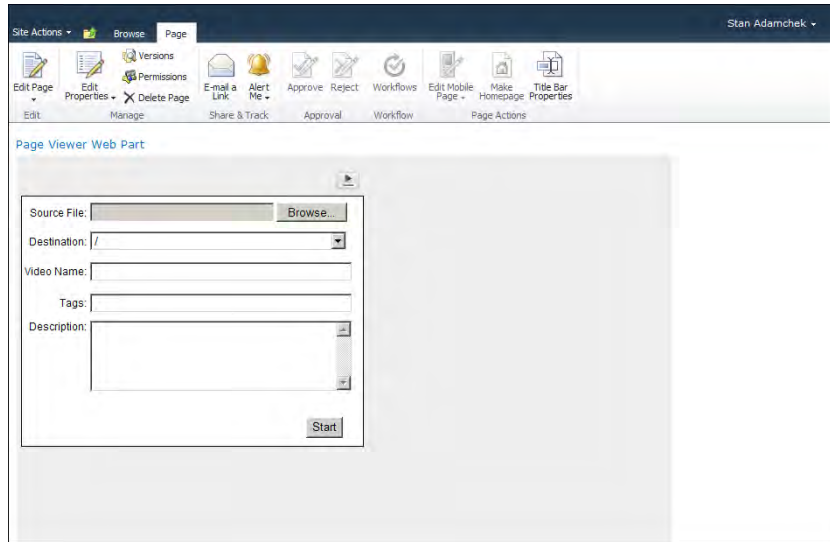
Figure 35. SharePoint "Standalone" Add Video Page

## *Embedding the Interface in SharePoint Server 2010*

The following steps explain how to embed the VEMS interface in SharePoint if you are using SharePoint Server 2010. *For more information, or if you are using a different version of SharePoint, see the Web Parts topic in the SharePoint online help of the version you are using.*
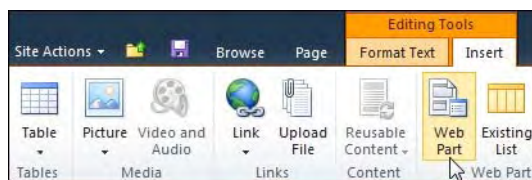
Add a Page Viewer Web Part to a Page

To edit a page you must have at least the permissions obtained by being added to the default Designer SharePoint group for the site.

▼   To add a Web Part to a Page:

1.   From a page, in the ribbon, click the **Page** tab, and then click the **Edit** command. If the Edit command is disabled, you may not have the permissions to edit the page. Contact your administrator for help.)
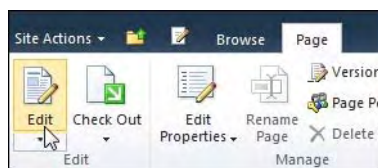
2.   Click on the page where you want to add a Web Part, click the **Insert** tab, and then click **Web Part**.
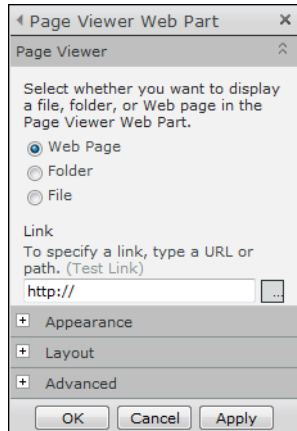

3.   Under **Categories**, select **Miscellaneous > Page Viewer Web Part**, and then click **Add**.
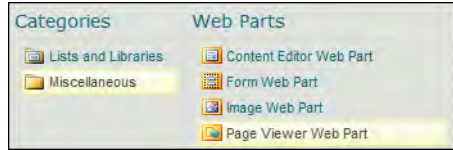
Enter the VEMS Interface URL

▼ To enter the VEMS interface URL:

1. Point to the **Page Viewer Web Part**, click the down arrow (on far right), and then click **Edit Web Part**. The Web Part properties display in the tool pane.

2. In **Page Viewer Web Part** select the **Web Page** radio button. This option automatically enters the `http://` string in the **Link** text box.

3. Enter the VEMS SharePoint URL (see <u>Configuring the VEMS Interface URL</u>) in the **Link** field and click **Apply**.

4. This will display the SharePoint page with an embedded VEMS interface (see Figure 34 on page 231). The next section provides a description of the URL and explains how to customize the look-and-feel.

Configuring the VEMS Interface URL

The URL to the VEMS SharePoint Interface contains all of the details about the look, feel and functionality of the interface. This URL has two parts:

• Base URL – points to the interface file itself
• Query string variables – define the look, feel and functionality of the interface

Base Interface URL

The Base URL to the VEMS SharePoint Interface is always:

`http://`**`<VEMS_Host_Name_or_IP Address>`**`/SharePoint/SPStoredMedia.aspx`

Query String Variables

The query string variables shown in Table 25 are appended to the base URL. They are not required, and if not appended, the interface will use default values. They can be inserted in any order but the first query string variable must be preceded by a "?" character and any subsequent variables must be proceeded by a "&" character. See the following example.

Sample URL

```
http://172.17.164.20/SharePoint/SPStoredMedia.aspx?spfolder=/VBrick/CEO
Broadcasts&spheight=325&spborderc=7F9DB9&sptablebgc=FFFFFF&sptextc=000000&spbodybg
c=EEEEEE&spmaxnum=100&spwidth=390&spsharing=true&spaddvideo=true&spuploadfolder=us
ername&spshowstoredicon=true
```

Table 25. SharePoint Interface Query String Variables

Variable	Description	Example
spaddvideo	Display the Add Video icon on the Stored Video interface. This provides a link to the Add Video feature. This link will only display if the user has rights to upload video. Default = false	spaddvideo=true
SPAddVideo.aspx	Use to embed the standalone Add Video interface (Figure 35) in a SharePoint page.	SPAddVideo.aspx
spbodybgc	Background color of the entire SharePoint web part. Default = FFFFFF.	spbodybgc=44CCFF
spborderc	Border color of the items in the list of titles. Default = 000000.	spborderc=44CCFF
spembedded	Do you wish to use the embedded player or a popup player. (False for popup. Default = false).	spembedded=true
spfolder	Root folder from where all items in the list will be drawn. Default = /.	spfolder=/videos/test
spgeneralfont	Font used for the list of titles. Limited by what fonts are available on the client. Default = Arial.	spgeneralfont=times
spgeneralfontsize	Font size, in pixels, of the list of titles. Default = 12.	spgeneralfontsize=14px
spheight	Height of the list of titles in pixels. Default = 315.	spheight=500
spmaxnum	Maximum number of titles which are allowed to be listed. Default = 25.	spmaxnum=50
spmaxtitlesize	Maximum number of characters a returned title may be before it is truncated. Default = 25.	spmaxtitlesize=50
spsearch	Search string to look for in the returned list of titles. Default = empty.	spsearch=education
spsharing	Enable the ability to e-mail a link to a video asset. Default = false	spsharing=true
spshowfileextension	Display the file extension of the video files in the list. Default=true.	spshowfileextension=true

Variable	Description	Example
spshowstoredicon	Display the Stored Media icon ✚ on the Add Video interface. This allows the user to navigate to the Stored Video interface. Default = true	spshowstoredicon=true
spsorttype	Sort by title or by creation date. (alternatively you may choose 'title.' Default = date).	spsorttype=date
SPStoredMedia.aspx	Use to embed the VEMS interface (Figure 34) in a SharePoint page.	SPStoredMedia.aspx
sptablebgc	Background color, in hex, of the table of returned titles. Default = FFFFCC.	sptablebgc=44CCFF
sptextc	Color of the text. Default = 00000.	sptextc=44CCFF
spuploadfolder	Specify an upload folder for the Add Video feature. If no folder is specified all folders the user has access to for uploading will appear in the **Destination** dropdown on the Add Video interface. Default = blank (no folder specified).	spuploadfolder=username
spwborderc	Border color of the outside of the list of titles. Default = 000000.	spwborderc=44CCFF
spwidth	Width of the list of titles in pixels. Default = 390.	spwidth=250

Configuring a DVB Gateway

Topics in this chapter

Overview

VBrick has partnered with Breeze Technologies to deliver a DVD-T (Digital Video Broadcasting-Terrestrial) Gateway that lets you auto discover and play live European digital broadcast channels from the VEMS user interface. The TVium DVB-T Gateway lets you distribute up to 125 channels of live digital broadcast TV and radio over your existing IP network. The TVium DVB-T Gateway appliance lets you distribute the full complement of DVB-T channels to desktop screens and displays across your LAN, WAN or IP network—all through a single appliance. When powered by VEMS, the DVB-T Gateway enables easy, network-wide distribution and management of content from one central location. Channels can be auto-scanned and configured, allowing end-users to stream individual channels to their desktops, digital displays, or set top boxes.

Table 26. TVium Features and Specifications

Feature	Specification
RF Input	Single 75 ohm DVB-T RF input supporting eight tuners and demodulators.
Network Input	10/100 Base-T Ethernet for management
Network Output	10/100/1000 Base-T Ethernet for streaming
Setup and Management	• Infrared remote control • Front panel keypad • Web Management Interface
Conditional Access	2 x Conditional Access Modules (CAM) supporting Mediaguard, Viaccess, Irdeto, Conax
Connectivity	USB2.0, SATA, HDMI

Feature	Specification
Video Output	Built-in LCD or HDMI
Audio Output	Unbalanced audio jack or built-in front panel speaker
Video Decoding	• MPEG-4 AVC/H.264 high profile level 4 • MPEG-1 and MPEG-2 main/high profile
Audio Decoding	MPEG-1 layer I and II
Demultiplexing	Transport Stream
Power Consumption	100-240V AC 30W via external adaptor
Standards Compliance	• CE and FCC approved • ISO /IEC 14496 and ISO/IEC 13818 compatible

Gateway Installation

Locate and read the *TVium TR1-100 User Manual* shipped with the product. This document explains how to setup the appliance and how to auto discover available live channels. You will need power, access to a terrestrial aerial connection, and two network cables.

▼   To install the DVB-T Gateway:

1. Connect the TV antenna cable to the **RF IN** socket on the appliance.
2. Connect a network Ethernet to the Ethernet port.
3. Optional. Connect a monitor to the HDMI port using an HDMI cable.
4. Connect AC power and power-on the unit.

Gateway Configuration

▼   To configure the gateway:

1. Start by plugging in all of the cables as explained in the *User Guide*. This will power up the Gateway and display a menu page.
2. Use the handheld Remote Control (or the keypad on front of unit) to navigate to **Auto Install** on the **Easy Setup** menu.
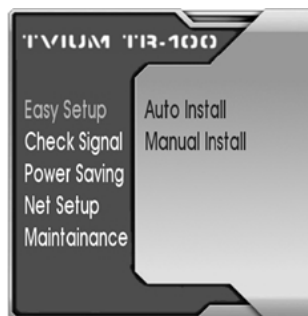
3. Click **Auto Install**, click **OK**, and the select **Start Automatic Search**.
4. If the aerial cable is plugged in correctly and acquires a signal it will scan and auto discover any available TV channels that can be streamed. During this process it will show the completion percentage, the number of channels found, and the channel names. (*If the number of channels discovered is less than you would expect, use the Check Signal option to test the connection.*)

5. When the auto discover process is complete, a **Stream Setup** option is added to the menu and the appliance displays all of the discovered channels and their multicast addresses. You will need these multicast addresses to configure the channels in VEMS. (*If necessary you can change the multicast address as explained in the TVium TR1-100 User Manual.*)

> **Note** All streams are enabled by default. Use the **Stream Setup** option to disable streams or to change the multicast address or port number.
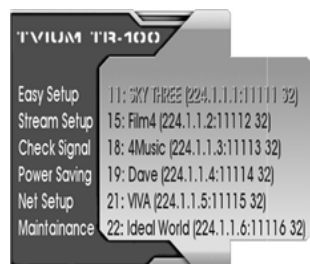
6. The next step is to configure the network settings for your site using the **Net Setup** option. For example you may want to configure two static addresses within your subnet—one for the multicast data to stream on and another for managing the gateway.
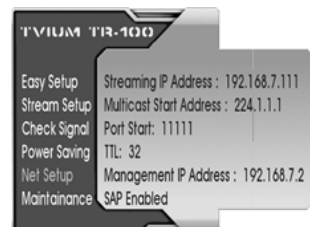
7. When done the gateway is configured and ready to go. The next step is to configure the discovered multicast addresses in VEMS.
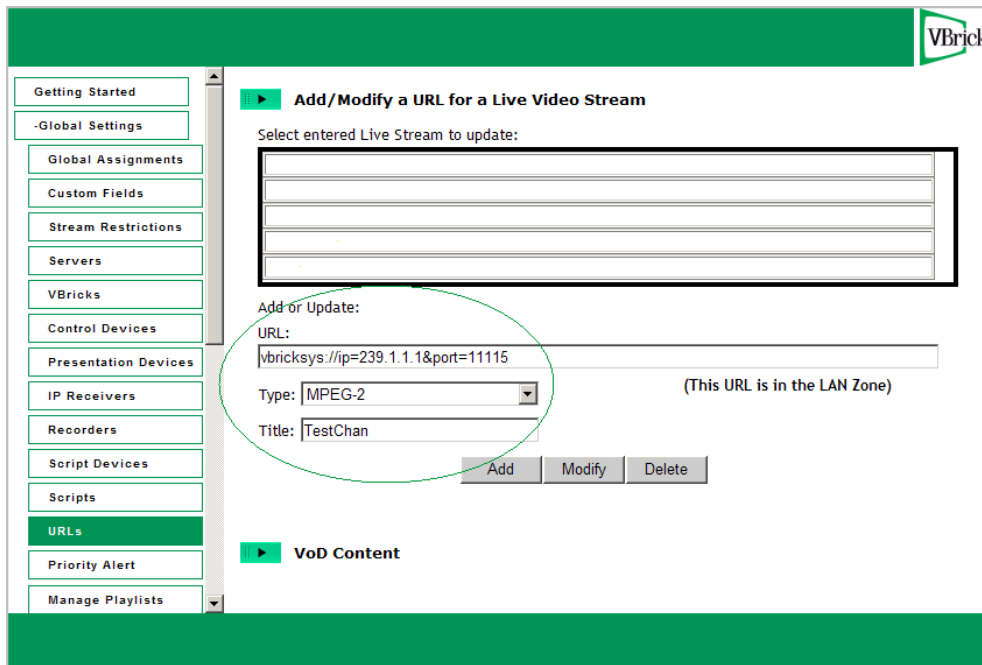
VEMS Configuration

Once you have auto discovered the multicast IP addresses, the next step is to configure them in VEMS as live URLs. For more detailed information see

▼   To add a URL for a live multicast stream:

1. Launch the VEMS admin console and go to Global Settings > URLs.

2. Enter the auto discovered multicast URL in the **URL** field using the exact format and syntax shown below.

3. For **Type** select MPEG-2; for **Title** enter a user-friendly name for the stream. Then click **Add** and this title will be shown on the **Live Media** page in VEMS.

4. Repeat these steps for each multicast URL you wish to add to VEMS.

URL	Enter the auto discovered multicast address and port as shown in the following example:
	`vbricksys://ip=239.1.1.1&port=11115 [&refip=192.99.999.999]`
	Where `239.1.1.1` is the multicast IP address and `11115` is the multicast port number.
	Note: If using Zones, the `refip` parameter is needed if the source IP address does not indicate which zone the DVB gateway is in. The `refip` can be the IP address of any component in the subnet where the gateway is actually located. For more details see Adding a Reference IP Address for URLs on page 82.
Type	Always select **MPEG-2** when using the DVB-T Gateway.
Title	The title is what will display to clients on the **Live Media** page in VEMS.

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