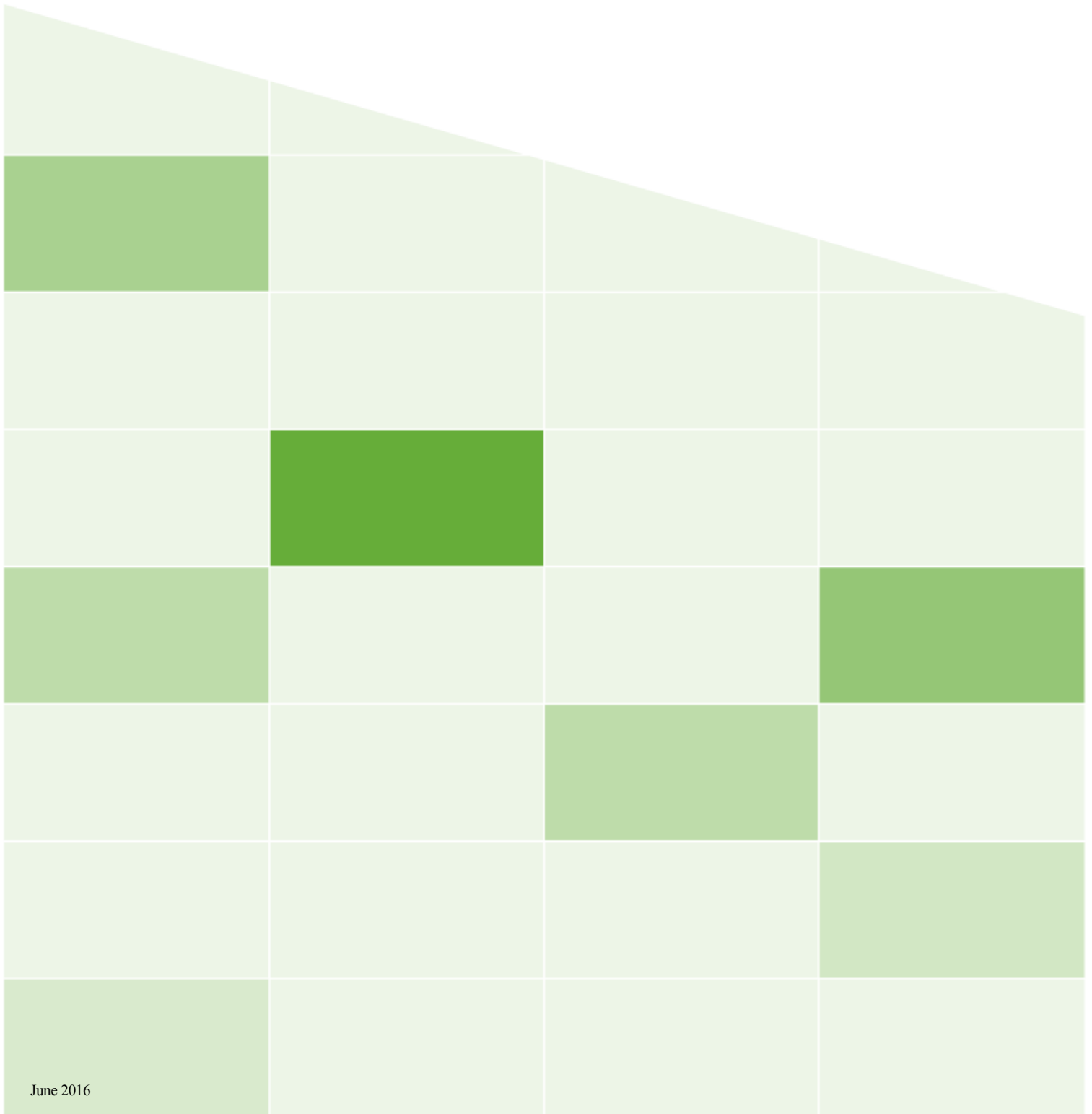




VBrick Enterprise Media System

VEMS Mystro Portal Server v6.3.17

Admin Guide



Copyright

© 2016 VBrick Systems, Inc. All rights reserved.
2121 Cooperative Way, Suite 100
Herndon, VA 20171, USA

This publication contains confidential, proprietary, and trade secret information. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any machine-readable or electronic format without prior written permission from VBrick Systems, Inc. Information in this document is subject to change without notice and VBrick assumes no responsibility or liability for any errors or inaccuracies. VBrick, VBrick Systems, the VBrick logo, VEMS Mysterio, StreamPlayer, and StreamPlayer Plus are trademarks or registered trademarks of VBrick Systems, Inc. in the United States and other countries. Windows Media, SharePoint, OCS and Lync are trademarked names of Microsoft Corporation in the United States and other countries. All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries should be made directly to those companies. This document may also have links to third-party web pages that are beyond the control of VBrick. The presence of such links does not imply that VBrick endorses or recommends the content of any third-party web pages. VBrick acknowledges the use of third-party open source software and licenses in some VBrick products. This freely available source code is posted at <http://www.vbrick.com/opensource>

About VBrick Systems

Founded in 1998, VBrick Systems 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. VBrick products are manufactured in an ISO certified manufacturing facility.

Contents

Portal Server v6.3.17 Admin Guide

Preface	ix
Getting Help	x
Font Conventions	x

1. Introduction

Portal Server Overview	1
Server Requirements	2
Desktop Requirements	2
Microsoft Service Packs and Security Updates	3
System Description	3
Portal Server Prerequisites	3
Portal Server Hardware Specifications	4
Software Installation	5
Supported File Types	5
Supported Network Configurations	6
Portal Server Components	7
Master and Redundant Servers	7
VEMS Database	7
VBrick Encoders	8
VEMS VOD Servers	8
VBOSS	10
DME	10
Digital Signage	10
iPhone/Android Mobile Device Support	10
Migration Support	11
Portal Server Installation	12
Download Components	12
Player Licenses	14
MPEG2TS Transport Stream Licenses	15
Port Requirements	15
Transcoder Licensing	16
Software Upgrade	16
Portal Server Configuration Changes	16
Install/Replace License Files	17
Login	19
Logout	21

2. Dashboard

Dashboard	23
Help	24
About	25

3. Access Control

Groups	27
Create New Group	28
Import Groups from LDAP	33
Users	35
Create New User	36
Inactive Users	37
User Announcements	37

4. Content Management

Category Management	39
Add New Category	40
Edit a Category	40
Delete a Category	41
Delete Multiple Categories	41
Custom Fields	42
Add New Custom Field	43
Live Entered URLs	43
Add New Live URL	45
Stored Entered URLs	46
Add New Stored URL	47
Content Workflow	48
Configuring Content Approval	49
Creating a Workflow Template	50
Recommended Videos	54
Required Videos	55
Report Permissions	55

5. Advanced Content Distribution

Overview	57
Ingesting Video to an Offline Stored Server	57
Enabling Offline Stored Server Ingestion	57
Ingesting Video to a Specific Stored Server	59
Redistributing Existing Content Based on Category Assignment	67

6. Devices

Application Servers	69
Add Server	70
Load Balancer	73
Channel Guide Servers	74
VBrick Channel Guide Server	74
User-Defined Channel Server	75
LDAP Servers	76
Add New LDAP Server	78
Using LDAP with Single Sign-On	79

Using LDAP with SSL.....	81
Presentation Devices	83
STB	86
Manually Add STB	89
Auto-Discover STB.....	91
Adding a VEMS User	91
Stored Servers	92
Add a New Server.....	94
Edit a Server	95
VOD-W.....	97
VOD-WM.....	98
VOD-D.....	102
VOD-FMS.....	103
VOD-Wowza	104
File Server-HTTP	107
File Server-FTP.....	110
Publishing FTP Server	110
DME	111
Cloud.....	114
Learn360	117
Discovery Education.....	118
VBricks (Encoders)	120
Manually Add VBrick	120
Auto-Discover VBricks	122
Define Slots/Channels	122
Define Viewing URLs.....	124
Script Devices	125
Control Devices	127
Add Control Devices.....	129
User Defined VBIRs	131
Modifying the Control Panel.....	132
Connecting Control Devices.....	133
Configuring Control Devices	134
Updating the VBIR Command Set	135

7. Zones

Overview	137
Define Default Zone	138
Define LAN/Internet	139
Define Zone.....	139
Configuring Zones	141

8. UI Customizations

Define Themes.....	143
Create New Theme	144
Preview Theme	147

Customize UI Text	147
Modifying Existing CSS and JS Files	149
9. System Settings	
Global Settings	151
YouTube Content Delivery Configuration	162
Password Complexity	165
Edit Password	166
Test Password	167
Player Preference	167
SAP Configuration	169
Task Scheduler	170
Edit Task	172
Cisco Content Delivery	172
Transcoding Presets	174
Best Practices	176
Configuring Transcoding Presets	177
Transcoding Profiles	180
Configuring HLS/HDS VOD Servers	181
Add New Profile	182
Define Default Profile	182
Transcoding Existing Content	183
Scripts	184
Add Script	184
Finding VBrick Parameters and Values	186
10. Reporting	
Export to Excel	187
Global Recording Status	191
Content Approval Status	192
11. SharePoint 2013 Integration	
Overview	195
Embedding a VEMS Interface	195
Creating a Page in SharePoint 2010	196
Client Side Settings	198
Setting Page Properties	198
Configuring an "Add Video" Widget	201
VEMS Configuration	201
SharePoint Configuration	203
12. VEMS Blackboard Integration	
Overview	207
Blackboard Administrative Setup	207
VEMS Mystro LMS Configuration and Settings	209

Define VEMS Mystro Global Settings	209
Configure VEMS Mystro Custom Fields	211
13. VEMS Lync Integration	
Overview	215
Add the DME Lync as a Presentation Device	216
Schedule a Lync Meeting Event Type	218
Start a Video Conference in Lync with a DME User	219
14. Configuring for SSL	
Overview	223
SSL Prerequisites	224
Configuring SSL	224
Disabling SSL for the Poodle Vulnerability	232
Configuring Secure FTP	232
15. Network Video Recording	
NVR Overview	235
Using an NVR	236
NVR Performance Considerations	236
16. Auto Content Ingestion	
Auto Content Ingestion	237
Auto Content Ingestion by Category	238
Auto Content Ingestion via XML	239
Using the XML Template	239
17. Using Mystro with a DME	
Understanding Instances	243
Player Preference and Instance Selection	243
Player Preference Example	244
Corrupted Files and Exceptions	244
Multiple Allow Players	245
Failover	245
18. STB Users Utility	
STB Users Utility	247
Installation	247
1. Create Groups	247
2. Add STBs to VEMS	248
3. Run STB Users Utility	249
19. Command Line Interface	
Command Line Interface	253

SDK Message Structure	253
Configuring Mystro for CLI	253
CLI Structure	253
Login	254
Logout	254
List Live	254
Start Record (uses NVR)	254
Start Encoder Record (uses VBStar)	255
Stop Record (uses either NVR or VBStar)	255
Get Channel Guide	255
Get List of STBs	256
Tune STB	256
List STB Schedules	256
XML Structure	257
Login	257
Logout	257
List Live	258
Start Record (uses NVR)	258
Start Encoder Record (uses VBStar)	259
Stop Record (uses either NVR or VBStar)	260
Get Channel Guide	261
Get List of STBS	262
Tune STB	262
List STB Schedules	263

Portal Server v6.3.17 Admin Guide

Preface

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

<u>Introduction</u>	Provides an overview of the application and describes major components, desktop requirements, and server requirements.
<u>Dashboard</u>	Explains how to use the dashboard, how to get online help, and how to check on the licenses you have installed.
<u>Access Control</u>	Explains how to create users and groups, how to import from LDAP, and how to create system announcements.
<u>Content Management</u>	Explains how to create custom fields and categories, how to add live and stored content URLs, and how to enable a Content Approval Workflow.
<u>Advanced Content Distribution</u>	Details advanced content distribution in VEMS and how to configure video ingestion to offline VOD servers and to specific VoD servers based on an assigned category.
<u>Devices</u>	Explains how to add VOD servers, DME servers and LDAP servers, and how to add or auto-discover VBrick appliances (encoders).
<u>Zones</u>	Explains how to use zones to direct Portal Server clients to specific servers for load-balancing and scalability.
<u>UI Customizations</u>	Explains how to create themes and customize colors and logo, also explains how to access labels and customize
<u>System Settings</u>	Explains the Global Settings used throughout the system as well as the Task Scheduler, password complexity options, SAP configuration, transcoding presets, content delivery, and player preference. This is also where you find Cisco ACNS and Cisco ACDS manifest file generation.
<u>Reporting</u>	Explains how to create Excel reports for content related, group, user, and system configuration reporting. Also provides information on global reporting status, content approval status, and real-time system diagnostics.
<u>SharePoint 2013 Integration</u>	Explains how the Portal Server is closely integrated with Microsoft SharePoint.
<u>VEMS Blackboard Integration</u>	Explains how to set-up the VEMS Mystro Blackboard integration so content may be synchronized to Blackboard.

<u>VEMS Lync Integration</u>	Details how to configure and set up Microsoft Lync so that you can broadcast a Lync Meeting event in VEMS to several simultaneous users.
<u>Configuring for SSL</u>	Explains how to configure SSL to safeguard management data sent between the Portal Server and external clients.
<u>Network Video Recording</u>	Explains how to maximize your recording capabilities by recording streams to an NVR.
<u>Auto Content Ingestion</u>	Explains auto content ingestion. This is the process whereby video content is automatically populated on the portal server.
<u>Using Mystro with a DME</u>	Explains how to use VEMS Mystro with VBrick's Distributed Media Engine.
<u>STB Users Utility</u>	Explains how to automatically create and associate set top box users in large-scale environments.
<u>Command Line Interface</u>	Explains how to use the CLI to interact with the Portal Server SDK from third-party control systems.

Getting Help

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.

Introduction

Portal Server Overview	1
Portal Server Components.....	7
Portal Server Installation	12
Portal Server Configuration Changes.....	16
Login	19

Portal Server Overview

VEMS Mystro® (pronounced my-stroh) delivers a fundamentally different IP video user experience that promises to change the way people use video to accomplish their day-to-day work and to reach their academic goals. By incorporating video into all applications, VEMS Mystro serves as the intersection point for video broadcasting, video conferencing, collaboration tools and social media, unlocking the power of video to amplify important messages throughout an organization and beyond. VEMS Mystro is the core of the VBrick Enterprise Video Architecture which spans video capture, distribution, play out and video content management.

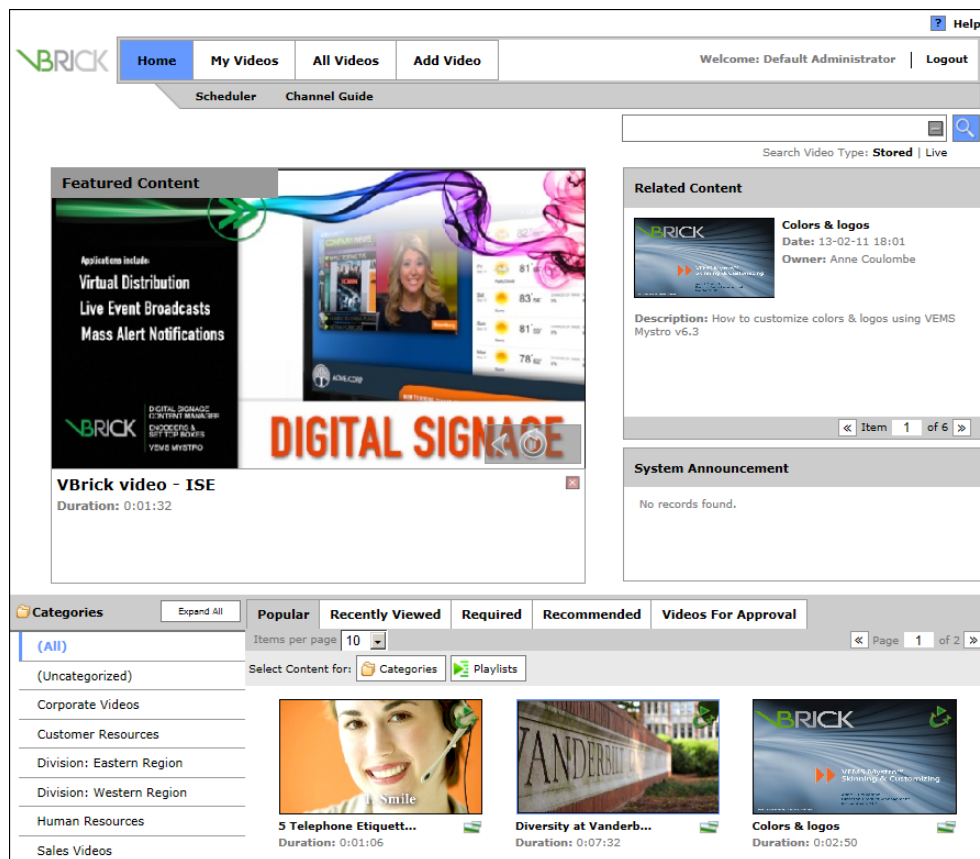


Figure 1. VEMS Mystro Home Page

The VBrick Enterprise Media System (VEMS Mystro) consists of a group of products that includes the VEMS Portal Server, VBrick Encoders, VEMS supported VOD servers (onsite and iCloud-based), Distributed Media Engine, and StreamPlayer software. This integrated system delivers live and on-demand video and audio over an IP-based infrastructure. The VEMS Portal Server functions as a video portal, permitting end users to view live and on-demand MPEG-2, WM (Windows Media), and H.264 content on Windows or Macintosh desktops and extends HLS and HDS content to mobile devices. 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 supplied by VBrick.

Note VEMS Mystro ships with the user and admin interfaces available in English (US), French (CA), and Spanish (ES). The administrative language of the system is set in the [Global Settings](#) page. End users can also choose their language using the dropdown menu in the footer of each page on the user interface.

Server Requirements

The *minimum* server requirements are shown in Table 1:

Table 1. Minimum Server Requirements – VEMS Mystro Standard Edition

Operating System	Windows Server 2008 R2 (Standard Edition) 64-bit, and Windows Server 2012 †
Software Framework	.NET Framework 4
Database	SQL Server 2008 R2, 2012 (Express, Workgroup, Standard, or Professional)
RAM	4–16 GB
Hard Drive	72 GB minimum (larger for frequent recording).
Disk Space	800 MB minimum for installation.

† with supported hardware.

Note SSL support requires a trusted third-party certificate. VBrick does not support self-signed/self-generated SSL certificates. You must purchase a valid certificate from a reliable vendor such as [GoDaddy](#), [Verisign](#), etc.

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.

Table 2. Desktop Requirements

PC Type	Requirements
Windows PCs	<ul style="list-style-type: none"> • Windows XP (SP3), Vista (SP2), Windows 7, Windows 8 ¹ • 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 Windows Media Player 9.0 or higher. • DirectX Media Version 8.1 or higher. • Microsoft Internet Explorer 8.0 or higher. • Firefox 9 or higher. • Chrome 19 or higher.
Macintosh PCs ²	<ul style="list-style-type: none"> • Mac OS X 10.5 or higher for Intel-based Macs. ² • Firefox 9.0 or higher. • Safari 5.0 or higher. • QuickTime Player 6.0 or higher.

¹ with supported hardware.

² Internet Explorer for Macintosh is not supported.

³ The release of Safari 7 included with Mac OS X has a new plug-in The Java applet should be set to **Allow Always** under **Safari Preferences > Security** for VEMS to allow file upload.

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 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.

System Description

Portal Server Prerequisites

Windows 2008 R2 Server Requirements

- Windows Server 2008 R2 Standard Edition (64-bit) is supported. 32-bit VEMS Mystro support was discontinued with version 6.3.
- Minimum 16 GB RAM per hardware configuration, application may run in less. See detailed specifications below for more information.
- Minimum 800MB free disk space. Substantial additional disk space will likely be needed when ingesting or recording video.

- IIS Web Server and IIS FTP Server functionality must be enabled. The installer will determine if this needs to be installed.

Portal Server Hardware Specifications

The Portal Server can be purchased from VBrick as a hardware/software combination and the core software [not including client download components] may be installed prior to hardware shipment. Refer to the *Portal Server Getting Started Guide* for core software installation and update instructions.

The Portal Server may also be purchased as a software-only product in which case the customer provides the hardware and installs the software. The software is then typically provided through the VBrick Support Downloads page on the [VBrick Website](#).

Note VEMS Mystro servers use the latest Power Edge 620 hardware from Dell. When purchasing hardware, use server hardware that meets or exceeds the recommendations for the 620 models used by VBrick as shown in Table 3 and Table 4. See the [PowerEdge 620 Technical Guide](#) for more information.

Table 3. VEMS Mystro Standard Edition

Item	Description
Base Unit	PowerEdge R620 XL,TPM
Network Interface	Broadcom 5720 QP 1Gb Network Daughter Card
RAID Type	RAID 1 for H710P/H710/H310 (2 HDDs)
RAID Controller	PERC H310 Integrated RAID Controller
Processor	Intel Xeon E5-2603 1.80GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4-Core, 80W, Max Mem 1066MHz - Quantity 1
Memory	4GB RDIMM, 1600 MHz, Standard Volt, Dual Rank, x8 - Quantity 4
Hard Drive	500GB 7.2K RPM Near-Line SAS 6Gbps 2.5in HotPlug Hard Drive - Quantity 2
Operating System	<ul style="list-style-type: none"> • Windows Server 2008 R2 SP1, x86 • Windows Server 2008 SP2 x86 on 5.x products

Table 4. VEMS Mystro Professional/Enterprise Edition

Item	Description
Base Unit	PowerEdge R620 XL,TPM
Network Interface	Broadcom 5720 QP 1Gb Network Daughter Card
RAID Type	RAID 1 for H710P/H710/H310 (2 HDDs)
RAID Controller	PERC H310 Integrated RAID Controller
Processor	Intel Xeon E5-2667 2.90GHz, 20M Cache, 8.0GT/s QPI, Turbo, 6-Core, 115W, Max Mem 1600MHz - Quantity 2
Memory	4GB RDIMM, 1600 MHz, Standard Volt, Dual Rank, x8 - Quantity 8
Hard Drive	500GB 7.2K RPM Near-Line SAS 6Gbps 2.5in HotPlug Hard Drive - Quantity 2
Operating System	Windows Server 2008 R2 SP1, x64

Software Installation

See the *Portal Server Getting Started Guide* for software installation and update instructions.

Supported File Types

Table 5. Supported Live Streams by Codec, Protocol and Media Player

		QuickTime	VBrick Player	VBrick Mac Player	Flash	Windows Media	iOS	Android 1	MF STB	Amino
	Protocol	RTP	RTP, TS/UDP	RTP, WM/ASF HTTP TS/UDP	RTMP, HDS	WM ASF		RTP	RTP, TS/UDP, WM ASF	TS/UDP
Codec	H.264/AAC	x	x	x	x		x	x	x	x
	MPEG-4 Pt 2/AAC	x	x	x					x	
	WMV/WMA			x		x			x	
	VP6				x ²					
	MPEG-2		x	x					x	x

¹ Requires Android OS version 2.1 or higher excluding Android OS versions 2.3.0–2.3.3.

² RTMP only

Table 6. Supported File Types by Protocol and VOD Server

		VOD-W	VOD-D	VOD-WM	DME	File Server	File Server	FMS	Wowza
	Protocol	RTP, TS/ UDP	RTP	WM/ASF	RTP, HTTP Progressive Download, RTMP	HTTP Progressive Download	FTP	RTMP, HDS	RTMP
File Type	mp4/mov (H.264) ²	x ¹	x ¹		x ¹	x		x	x
	mp4/mov (MPEG-4P2)	x ¹	x ¹		x ¹	x			
	wmv, wma, asf			x	x	x	x		
	flv, f4v, m4v				x	x		x	x
	mpg (H.264 in TS)	x							
	mpg (MPEG-2 in TS)	x							
	HLS (m3u8, ts)				x	x			
	HDS (f4m, f4f)				x	x ³			

¹ Hinting required for mp4 and mov files for RTP delivery. Hinting is added during Mystro 6.2 ingestion for mp4 with H.264/AAC.

² File is always transmuxed from mov to mp4 if it's H.264/AAC.

³ Some progressive download servers require additional software to support HDS download.

Table 7. Supported File Types by Protocol and Media Player

		QuickTime	VBrick Player	VBrick Mac Player	Flash	Windows Media	iOS	Android 1	MF STB	Amino
	Protocol	RTP, Progressive Download, HLS	RTP, TS/UDP	RTP, WM/ASF, HTTP Progressive Download, TS/UDP	RTMP, Progressive Download, HDS	WM ASF, HTTP Progressive Download	HTTP Progressive Download, RTP, HLS	HTTP Progressive Download, RTP ²	RTP, TS/UDP, WM ASF	
File Type	mp4 (H.264/AAC)	x	x	x ³	x		x	x	x	
	mp4 (MPEG-4 Pt 2/AAC)	x	x	x ³			x		x	
	mov (H.264/uncompressed)	x					x			
	mov (MPEG4 Pt2/AAC)	x					x		x	
	wmv, wma			x		x			x	
	flv, m4v, f4v				x					
	mpg (H.264 in TS)		x	x ³					x	x
	mpg (MPEG-2 in TS)		x	x ³					x	x
	HLS (m3u8, ts)						x			
	HDS (f4m, f4f)				x					

¹ Requires Android OS version 2.1 or higher.

² Not supported in Android OS versions 2.3.0–2.3.3.

³ Not supported for progressive download

Supported Network Configurations

Configuration	Description
Simple	In this configuration all VEMS Mystro elements (master server, SQL Server, NVR, Transcoder, etc.) are located on a single server machine.
Centralized with Redundant Services	This configuration consists of a master server and a redundant server (with an optional load-balancer) that provide redundant VEMS Mystro services.
Multi-Independent	In this configuration there are multiple, independent, load-balanced server machines, each with a fully independent subset of VEMS services and components.
Separate Servers	In this configuration there are separate systems that can typically connect to same or different LDAP servers. They can share VOD server(s) for stored content and the metadata (categories, keywords, etc.) is stored in the database—not on the VOD server. If desired, live events can be streamed programmatically between the systems. Note: SAP announcements do not cross systems.

Portal Server Components

Master and Redundant Servers

The VEMS Mystro solution is highly redundant and scalable. A standard configuration (see Figure 2) consists of a master server with an internal database. The standard configuration can be expanded to include one or more redundant servers, all of which communicate in realtime with an external database server. The master server runs all VEMS services; the redundant servers are identical but run a subset of VEMS services. Each server can support numerous, simultaneous client users. To support more users, you simply add optional redundant servers and implement a load balancer (not provided by VBrick). When using a load balancer all client requests are routed to the master (or redundant server) via the load balancer.

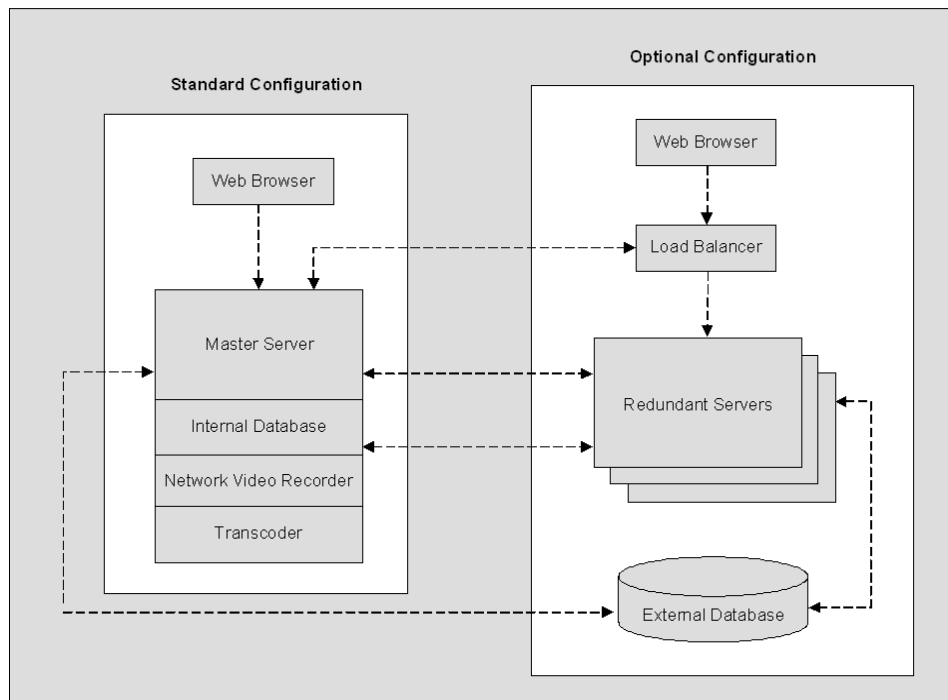


Figure 2. VEMS Mystro Architecture Schematic

VEMS Database

In a typical VEMS installation, Microsoft SQL Server Express (the default internal database) is installed on the same machine as the Portal Server. This database is shared by the master servers and all redundant servers (if present). Optionally, the master and redundant servers can connect to a user-installed and configured external database. If necessary, you can change the location of a configured external database or you can point to an entirely different database (see [Portal Server Configuration Changes](#) on page 16 for more about this). The Portal Server *Getting Started Guide* explains in detail how to create and move databases.

VBrick Encoders

VBrick H.264 appliances represent VBrick's newest networked video appliances. H.264 appliances deliver vastly improved quality for a given bit rate, allowing organizations to deliver a better customer experience for any given bandwidth. VBrick's MPEG-2 appliances are used for delivering low delay, DVD quality video over high bandwidth networks. VBrick's WM (Windows Media) appliances provide scalable quality at webcasting rates up to 4 Mbps. They feature 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.

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 8. The configuration for each server is similar (see [Stored Servers](#) on page 92 for details) and there is little difference in functionality for end users.

VEMS servers can be LAN-based and/or Internet-based depending on how the range of Internet addresses is defined (see [Define LAN/Internet](#) on page 139). 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 (that support the content) if they have permissions (roles and permissions are described in [Access Control](#) on page 27.) Content added by LAN users is added to all configured servers that can support that content type (for example you cannot add MPEG content to a Windows Media server) and for which you have permission. Internet users will only see content on Internet servers; LAN users will see content on both the Internet and on the LAN.

Table 8. Supported VEMS VOD Servers

Server Type	Description	Zone
VOD-WM-Standard	Standard – Microsoft Windows Media Server Standard Edition (unicast only). Requires an FTP server.	LAN or Internet
VOD-WM-Enterprise	Enterprise – Microsoft Windows Media Server Enterprise Edition (unicast or multicast). Requires an FTP server.	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
VOD-W	Windows-based VOD-W VOD server. Available in three versions depending on throughput: VOD-50W, VOD-125W, and VOD-300W. Supports MPEG-4 and H.264 content.	LAN only

Server Type	Description	Zone
VOD-FMS	An Adobe 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-Wowza	An Wowza Flash Server supports Flash and H.264 files. Wowza is an alternative to the Adobe Flash Media Server.	LAN or Internet
File Server-HTTP	A Windows Media or H.264 VBStar encoder can be configured as a progressive download server.	LAN or Internet
File Server-FTP	Plays content (via progressive download) and stores content in repository.	LAN or Internet
Publishing FTP Server	Stores content in repository only.	LAN or Internet
DME	VBrick Distributed Media Engine can be used as a VOD server for H.264 and WM (Windows Media) streams.	LAN or Internet
Cloud	This content is available to users with an Internet connection and an account.	Internet
Learn360	VEMS Mystro imports Learn360 educational content video content available in the cloud for playback from VEMS.	Internet
Discovery Education	VEMS Mystro imports Discovery Education™ educational content metadata available for playback in the My DE environment	Internet

VEEMS Internet-Based Servers

VEEMS Portal Server supports the installation of LAN-based servers and Internet-based servers. As part of an VEEMS Server installation, you can configure a VOD server to run in the "zones" (LAN or Internet) specified in Table 8. 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 [Define LAN/Internet](#) topic on page 139.)

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 VEEMS Portal Server but is not sold or supported by VBrick. (For more about downloading, installing, and configuring a Darwin server, go to: <http://developer.apple.com/opensource/server/streaming/index.html>) As noted, VEEMS users can be on the Internet or on a LAN; Internet users can only access 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 unicast only (they do not support multicast).

-
- Internet users can only see Windows Media and H.264 content stored on Internet-based servers.

VBOSS

VBrick's Online Streaming Service (VBOSS) is a cloud-based streaming server for live broadcast streaming, often as a unicast-to-multicast reflector service. It can also be used by VEMS Mystro as a Video On-Demand (VOD) Server. Content can be stored on VBOSS and then played back as requested by authorized VEMS users.

DME

VBrick's Distributed Media Engine is a versatile video processing and distribution platform. As part of the VBrick ecosystem, VEMS can manage the DME for numerous operations. In addition to acting as a VOD server, it can *transcode* (change the video compression method), *transmux* (change the video transmission method/protocol), and *transrate* (change the video transmission bit rate (e.g. for lower quality networks) with out sacrificing resolution. The DME can also cache content for local serving to significantly reduce bandwidth requirements and host VBrick's Video Conferencing Gateway.

Digital Signage

If you purchased VBrick's Digital Signage application, a Digital Signage button will display on the navigation bar when a Digital Signage server is configured on the System Settings > [Global Settings](#) page in Mystro. *This button simply launches the Digital Signage application.* 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*.



iPhone/Android Mobile Device Support

Mobile devices are increasingly used to view video either within the corporation's network or outside the firewall, based on the VEMS Mystro configuration. VBrick supports both live streaming and stored video content based on the mobile device operating systems and native

browser environments (iOS devices and Android phones). Moving forward, VBrick will develop mobile applications to increase functionality beyond the searching and playback functionality available today, as well as to expand the reach of the mobile devices beyond phones and tablets.

Table 9. Supported Android and iOS Devices

Device	Supported Content
Android Phones 1, 2, 3	<ul style="list-style-type: none"> • Live H.264 streamed via RTSP/RTP from devices such as 7000 or 9000 Series encoders. • Stored MPEG-4 files via Progressive Download over HTTP from Progressive Download servers including Cloud Servers. • Stored MPEG-4 files streamed via RTSP/RTP from VOD-W, VOD-D, and DME servers. • MPEG-4 files available in VBOSS.⁴
iOS Devices (iPad, iPhone, iPod) ^{3, 4, 5}	<ul style="list-style-type: none"> • Live HLS streams including streams from a DME. Live HLS content is only listed in VEMS when added as a Live Entered URL. Live SAP "announcements" from VBrick encoders are not displayed. • MPEG-4 files via Progressive Download over HTTP from Progressive Download Servers including Cloud Servers. • MPEG-4 files available in VBOSS.⁴

- ¹ VEMS Mystro supports Android phones running OS v2.3.x and OS v2.4.x. VEMS does not support v3.x Android tablets. Android devices do not support LDAP Single Sign-On. This will be resolved with the pending delivery of the VBrick Android App.
- ² For best results with Android streams, use the onscreen navigation controls in VEMS rather than the "back" button on the device. Note: the "seek" slider (for FF and RW) is not supported.
- ³ Live video reflected from RMS/RMD devices does not play on Android or iOS devices.
- ⁴ When initiating a Cloud Server account, make sure that all content you want to be accessible to iPad/Android devices is in MPEG-4 format. For example .flv files (Flash) and .mov files (QuickTime) will not play.
- ⁵ iOS 5 devices must have cookies enabled to work with VEMS Mystro. In iOS 5 they are disabled by default with the behavior set to "Never Accept Cookies." To enable cookies, go to Settings > Safari > Accept Cookies and change to "From visited" or "Always."

Migration Support

VEMS Mystro 6.3.1 provides a migration tool for customers wishing to migrate existing VEMS 5.4.2 systems to VEMS Mystro 6.3.1 (customers wishing to upgrade from earlier VEMS releases will first have to upgrade to 5.4.2). Be aware that not all 5.4.2 configuration data will be migrated to 6.3.1. VEMS Mystro 6.3.1 has new features and functions that were not present in 5.4.2, and 5.4.2 has legacy features that are not replicated in 6.3.1. Although new software versions may be available under your Service or Maintenance agreement, migration between versions is not covered and Professional Services fees will apply.

A successful migration requires a technical professional who is familiar with architectural differences between 5.4.2 and 6.3.1. **For these reasons a migration can only be performed by VBrick Professional Services or a certified reseller.** For a detailed overview that explains how it works, see the VEMS Mystro *Getting Started Guide* in the Portal Server [online help](#). To schedule a migration, contact your reseller or VBrick Support Services via the On-Line Support page: www.vbrick.com/support/online_support.asp

Portal Server Installation

Complete installation instructions for the Portal Server are provided in the *VEMS Portal Getting Started Guide*. 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 play the content. The Portal Server supports a wide variety of clients and video formats.

Download Components

Windows PCs

If configured with the appropriate components, Windows PCs (with Internet Explorer or Firefox) can play 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 a user clicks on the content. 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 from the Portal Server. After a download, you don't have to restart your computer but must you must close the browser.

In certain circumstances however, the use of downloaded components 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 component .cab files to have full Portal Server functionality. Contact VBrick Support Services about obtaining this file or if you have limited download functionality and cannot access the VBrick Download site.

Note Flash player components are not pushed to client desktops and must be manually downloaded from the [Adobe](#) website.

Firefox

With Firefox, users will also be prompted to install additional components the first time they launch a stream. Links for the appropriate stream types (WM or H.264) will be displayed in the area where the embedded player is normally displayed. These additional plugins *must* be installed. 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` and `VBWMPPlayerMoz` using **Programs and Features** in Windows Server 2008—*on each client desktop*. The latest VEMS components for Firefox will be installed the next time the Firefox client launches a stream.

Table 10. Supported Windows Operating Systems and Browsers (VEMS 6.x) ¹

Operating System	Supported Browser ²
Windows (Windows XP, Vista, 7, 8)	<ul style="list-style-type: none">• Internet Explorer 8 ³• Firefox 9• Chrome 19

¹ In VEMS 6.x the same browsers are supported for the client interface and the admin interface.

² Use version(s) shown or higher.

- 3 Internet Explorer 10 is supported with minor compatibility issues; live and stored streams will play as expected but you may experience minor visual artifacts or screen refresh issues.

Locked-Down Windows PCs

As described above, the Portal Server automatically downloads components to client PCs. 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.

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**.

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 [Zones](#).

Macintosh PCs

If configured with the appropriate components, Macintosh PCs (with Safari or Firefox) can play Windows Media, H.264, and Flash streams. In a Macintosh environment, when you click on a video for the first time, the Home page (see Figure 1) 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. Table 11 shows the stream types supported for each environment; Table 12 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. Note that the Macintosh StreamPlayer application supports both 32 and 64-bit environments.

Table 11. Supported Macintosh Stream Types

Environment	Supported Streams	Closed Captions ¹
Macintosh	Safari – WM, H.264, Flash	Supported for WM with VBrick plugin.
	Firefox – WM, H.264, Flash	Supported for WM with VBrick plugin.

¹ Closed captions are not currently supported on H.264 or Flash streams.

Table 12. Supported Macintosh Operating Systems and Browsers ¹

Operating System	Supported Browser ²
Mac OS X	<ul style="list-style-type: none">• Firefox 9• Chrome 19
Mac OS X 10.8 (Mountain Lion)	Safari 6
Mac OS X 10.7 (Lion)	Safari 5.1
Mac OS X 10.6 (Snow Leopard)	Safari 5.0.6

¹ In VEMS 6.x the same browsers are supported for the client interface and the admin interface.

² Use version(s) shown or higher.

Table 13. Supported iOS Browsers

Device	Browser
iPad 4.2.1	Safari Mobile
iPad Touch	Safari Mobile
iPhone	Safari Mobile

Table 14. Supported Android Browsers

Device	Browser
Chrome	Safari Mobile
iPad Touch	Safari Mobile
iPhone	Safari Mobile

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 Windows Media seats, for example, the number of concurrent users viewing a Windows Media stream (with any type of player) cannot exceed 100. The number of licenses initially available to Portal Server users is shown in Table 15. If you need additional licenses to comply with patent restrictions please contact the VBrick [Sales](#) team.

Table 15. Video Format Licenses

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

MPEG2TS Transport Stream Licenses

If you will be distributing transport streams (from a VBrick H.264 encoder) you will need a license for the MPEG2TS protocol to legally play these streams. This is a license for MPEG2TS—not a license for the MPEG-2 video codec which has a separate license. This requirement is typically satisfied by the fact that many PCs (with Windows 7) and set top boxes already have an MPEG2TS license. This license will already be present because the MPEG-2 video codec license also includes an MPEG2TS license. This means if you have a DVD player on your PC, your PC will already have a legal MPEG2TS transport license. As a general rule, the only devices which require an MPEG2TS license are legacy Macs without a QuickTime player and legacy (pre-Windows 7) PCs without a DVD player. Published MPEG2TS limits typically apply only to those devices that do not have MPEG2TS licenses.

Port Requirements

Table 16 shows the required port configuration for various Portal Server functions. **All ports are TCP except as noted**

Table 16. Port Requirements

Inbound Port	Description
80/443	Web request from client to VEMS.
9875/9876/9878 (UDP)	Multicast, Management, RTSP SAP announce from VBrick to VEMS. Note: These ports are configurable in the VEMS user interface.
21/990	FTP/FTPS from client to VEMS (Add Video, Upload Thumbnails).
80/443	Web Service requests between multiple VEMS servers.
1433 †	SQL Server listener port (default).
1434 (UDP) †	SQL Server handler port (default).
XXXX (UDP)	Multicast port of programs to record. For example, to record CNN (with a multicast IP of 239.22.2.2 and port of 4444), you would have to open port 4444 on the VEMS/recording server for the record to work.
Outbound Port	Description
21/990	FTP/FTPS from VEMS to VOD Servers (DME, Darwin, Windows Media, FTP) for content discovery and ingest.
80	VEMS to Multi-Format STB for scheduling.
80/443	Web Service request from VEMS to InfoValue VOD for content discovery.
54321	VEMS to AmiNET130 STB for scheduling.
80/443	Web Service requests between multiple VEMS servers.
554	Recording of RTSP (non-tunneled) H.264 and MPEG-4 streams.
135	Management command from VEMS to Windows Media (DCOM).
389	LDAP lookup from VEMS to LDAP Server.
636	LDAPS (LDAP over TLS)

† These are the default dynamic ports for a named instance. These ports are not guaranteed and therefore use of admin-defined static ports is strongly recommended for a firewall.

Configuring Ports for an External Firewall

If the entire VEMS system (the VEMS server, the LDAP server, and the database) is behind an external firewall, and client viewers will access VEMS from outside that external firewall, the three ports shown Table 17 must be open. Note that by default, the VEMS installer disables the Windows Firewall on the server machine.

Table 17. Required External Firewall Ports

Functionality	TCP Port
HTTP	80
HTTPS	443
Add Video	21

Transcoder Licensing

The transcoding feature requires a specific license if you are using a version of VEMS prior to v6.3.8. Transcoding is not a standard feature of the VEMS/DME environment until v6.3.8 and you must install the license using the proper procedure. See [Install/Replace License Files](#) on page 17 for more information. If you are using v6.3.8 and beyond, you do not have to follow this step.

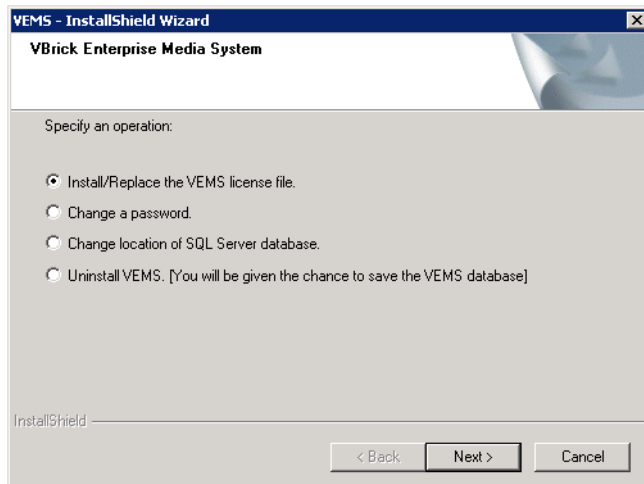
Software Upgrade

VBrick periodically releases upgrade to the VEMS Mystro software. You can visit our [website](#) or contact your certified reseller to see if an upgrade is available. For detailed upgrade instructions, see the *Portal Server Release Notes*.

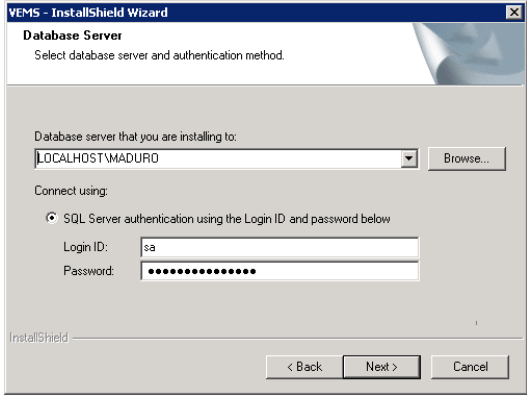
Portal Server Configuration Changes

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 > VEMS**.
 2. Click the **Change** button.



3. Select the operation you wish to perform and click **Next**. A description of each of the options is listed below.

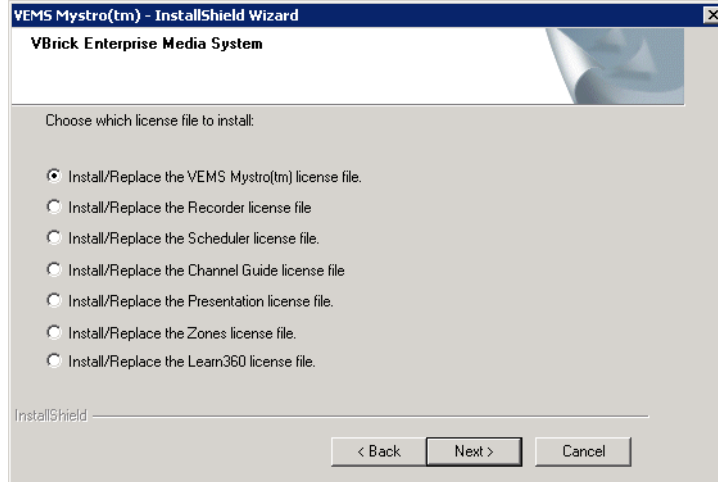
Install/Replace the VEMS license file	Use this option to install or replace any of the Portal Server licenses shown in Table 18 on page 18.
Change a password	Change the password (<code>VBrick_User</code>) for the database user. This changes a value in a configuration file on this server which VEMS uses to connect to the database. The database administrator must separately change the <code>VBrick_User</code> password on the database server to match this password.
Change location of SQL Server database	Change database location or vendor. 
Uninstall VEMS	Remove all VEMS Portal Server components. You are prompted to save the database as desired.

Install/Replace License Files

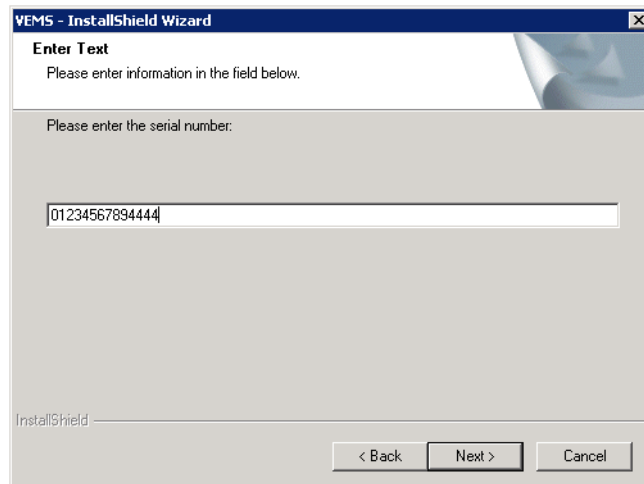
You are prompted to install serial numbers and license files (`.lic`) as part of the Portal Server installation process. Different Portal Server functionality is available depending on the type of license you purchase and install. (For example if you do not install a Scheduler license, you will not see 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 18. To see what licenses are currently installed, go to the [About](#) page on the VEMS admin interface.

▼ To install or replace VEMS license files:

1. Go to **Start > Control Panel > Programs and Features > VEMS**.
2. Click the **Change** button.
3. Select **Install/Replace the VEMS license file** and click **Next** to see more license options. See Table 18 [Portal Server License Files](#) for a description of each license file.



4. A serial number is required for some components. 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 your product), 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 your product. 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.

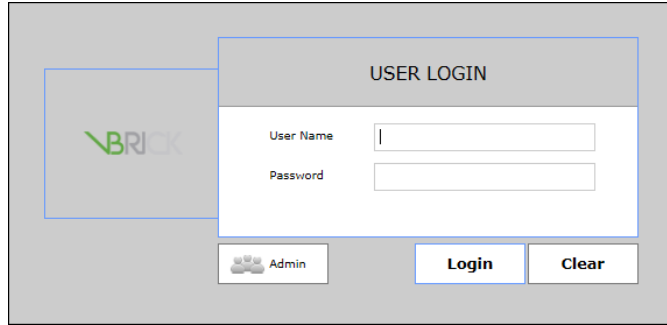
Table 18. Portal Server License Files

License File	Description	If not installed ...
VEMS Mystro	This is the basic license for VEMS Mystro.	The application will not run.

License File	Description	If not installed ...
Recorder	Network Video Recorder. Records two concurrent streams (or can add 10 or 40 with an additional license).	The number of concurrent recording will be limited by the license.
Scheduler	Enables the broadcast or recording of future events. See the <i>Portal Server User Guide</i> for more information.	The Add option will not be shown Scheduler page in client application.
Channel Guide	Enables the Channel Guide functionality described in the <i>Portal Server User Guide</i> .	The Channel Guide tab will not be shown on the user interface.
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.
Transcoder	One license on each VEMS Mystro and NVR server. Can be combined to permit concurrent transcoding during content ingestion. This step is only applicable if you are using a version of VEMS prior to v6.3.8. See: Transcoder Licensing .	Transcoder will not run.
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.
Learn360	Enables VEMS to import and play Learn360 educational content from the cloud.	The Stored Servers pages will not let you add a Learn360 server.
Discovery Education	VEMS Mystro imports Discovery Education educational content metadata available for playback within the My DE environment.	The Stored Servers pages will not let you add a Discovery Education 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-2/4 streams.	A popup message will be displayed when you try to launch a stream.

Login

The "Dashboard" page is automatically displayed when you login with a valid **User Name** and **Password**. All VEMS Portal Server functionality and commands are available from this page but you may not have access to all features and functions depending on your user privileges. For example, you may not be able to access certain VOD servers. *Note that after a configurable number of unsuccessful login attempts, you will need to close the window and start again.* Contact an administrator if you have trouble logging in.



- ▼ To launch the Portal Server Dashboard page:
1. Open a browser that is appropriate for your operating system.
 2. Enter the Portal Server *hostname* or *IP address* (e.g. `http:// <vems_servername>`) in the address bar. (If your system is configured with additional security you may need to enter `https`. Contact your system administrator if necessary.)
 3. If necessary select the **Admin** interface.
 4. Log in with a valid **User Name** and **Password** to launch the Dashboard page (Figure 3).
 Default User Name = `admin`
 Default Password = `adminadmin`

Note If you have multiple LDAP servers used for authentication you will need to select your server from the dropdown that is automatically displayed. If you are not sure which server to select, contact your system administrator.

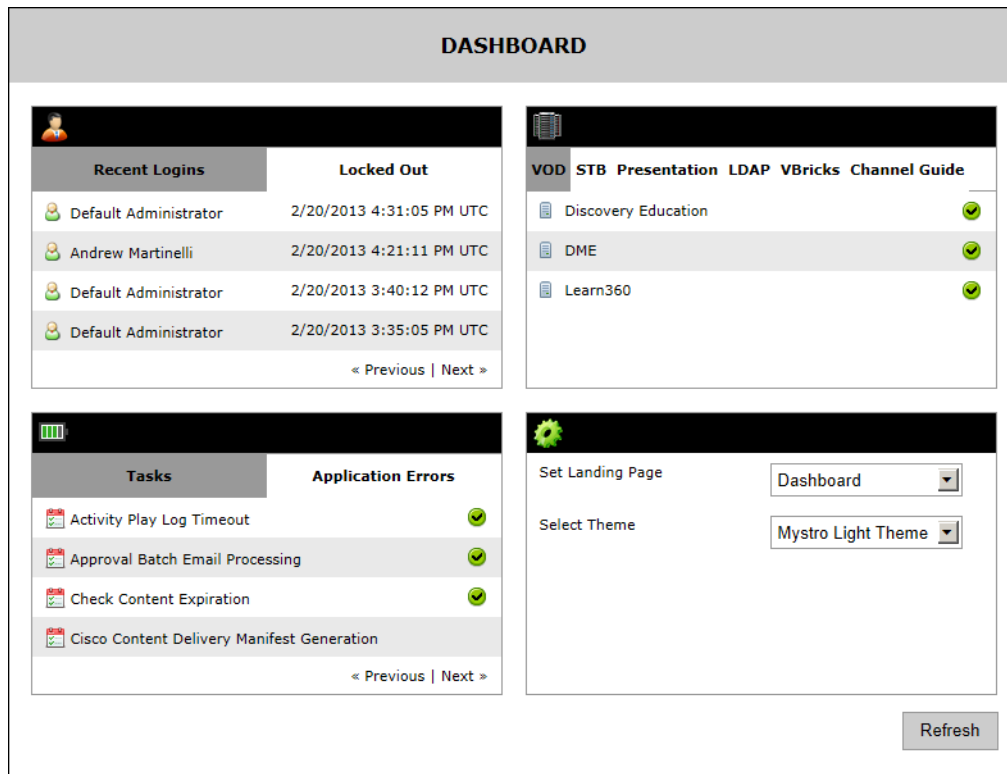


Figure 3. Portal Server Management Interface

Logout

The **Logout** 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.



Dashboard

Dashboard	23
Help	24
About	25

Dashboard

The "dashboard" page provides a quick snapshot, with color-coded icons, that shows the health status of all critical system functions. You can see who logged in recently as well as who was locked out because of configurable login policies. You can also see the online or offline status of all configured servers and VBrick appliances. If a server is reported offline, for example, you can click on the server name to launch the configuration pages for that server in order to troubleshoot the problem. You can also use the dashboard to set the landing page and color theme for the web pages. These are configurable preferences that are saved for each individual user.

DASHBOARD

Recent Logins	Locked Out
Default Administrator	2/20/2013 4:31:05 PM UTC
Andrew Martinelli	2/20/2013 4:21:11 PM UTC
Default Administrator	2/20/2013 3:40:12 PM UTC
Default Administrator	2/20/2013 3:35:05 PM UTC

<< Previous | Next >>

VOD	STB	Presentation	LDAP	VBricks	Channel Guide
Discovery Education					✓
DME					✓
Learn360					✓

Tasks	Application Errors
Activity Play Log Timeout	✓
Approval Batch Email Processing	✓
Check Content Expiration	✓
Cisco Content Delivery Manifest Generation	

<< Previous | Next >>

Set Landing Page: Dashboard

Select Theme: Mystro Light Theme

Refresh

Users	Recent Logins	Displays all recently logged in users. Click on any entry to display complete User Info.
	Locked Out	Displays all users in non-compliance with System Settings > Login Policies.
System Health	Tasks	Displays status of currently scheduled tasks. Click on a task name to modify the Interval or Schedule; go to System Settings > Task Scheduler to run the task now.
	Application Errors	Use for troubleshooting, Shows all application errors in the current session. Mouseover the error message to see the complete message text.
Devices	VOD Servers	Displays status of currently configured VOD servers. Click on any server name to open the configuration page for that server.
	STBs	Displays the status of any currently connected Set Top Boxes.
	Presentations	Displays the status of any currently connected Presentation Devices that may be used for webcasts.
	LDAP Servers	Displays status of currently configured LDAP servers. Click on any server name to open the configuration page for that server.
	VBricks	Displays status of currently configured VBrick encoders. Click on any VBrick name to open the configuration page for that device.
Preferences	Set Landing Page	Select the page (e.g. Dashboard, Access Control, etc.) that will display at login. This is an individual preference saved for each user.
	Select Theme	Select the theme (Light, Dark, Grey, or a user-created) that will be used for the user interface. This is an individual preference (saved in a cookie) for each user.

Help

This page displays the Portal Server 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.

Portal Server v6.3.1 User Guide

Preface

This *Portal Server User Guide* is written for anyone who will be using or evaluating the VEMS Mystro Portal Server. This includes system administrators, software developers, network technicians, and end users in a variety of business environments. 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 VEMS Mystro, the VBrick Enterprise Media System. The VEMS Portal Server provides a simple, intuitive interface that easily discovers available media assets in your network. The information in this document is arranged as follows:

Introduction	Provides an overview of the Portal Server. It explains desktop requirements and explains how to login, logout, and get help.
Home	Describes the functional elements on the home page and explains how to search for live and stored video assets.
My Videos	Describes the personalized content page that is different for each user. It has tabs for Favorites, Recently Viewed, and My Recordings.
All Videos	Explains how to find, play, and share any available live or stored streams. It also explains content recording and content metadata.
Add Video	Explains how to add live and stored video from a variety of internal and external sources, including YouTube.
Scheduler	Explains how to use the scheduler to create live broadcasts or webcasts, and how to rebroadcast or record stored content.
Channel Guide	Explains how to configure and use the Channel Guide which displays live channels and associated programming data.

Figure 4. Portal Server Online Help

About

This page displays the Portal Server **Version** number (for example 6.x) 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. Use the **Refresh Cache** button to update this page if you add VOD servers, change licenses, upload a new language file, or make other significant changes to the configuration. The **Diagnostic** information on this page provides important data about system response times. You may be asked to provide this information to VBrick Support Services when troubleshooting problems.

About

VEMS Mystro®

Version: 6.3.1.2

Number of VOD Connection Licenses:

License	Serial #	Expiration
VEMS Enterprise	12345678901234	Permanent
VEMS Record, maximum 10	12345678901234	Permanent
VEMS Schedule	12345678901234	Permanent
VEMS Zones	12345678901234	Permanent
VEMS Presentation	12345678901234	Permanent
VEMS Channel Guide	12345678901234	Permanent
VEMS Learn360 Content	12345678901234	Permanent
VEMS Discovery Education Content	12345678901234	Permanent
VEMS Transcode, maximum 3		Permanent

Refresh Cache

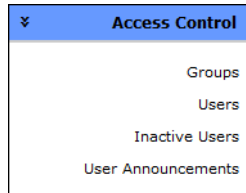
Diagnostic	Min	Avg	Max
Response Time from VEMS Server (milliseconds)	29	32	48
Response Time from DB Server (milliseconds)	< 1	< 1	< 1
Response Time from LDAP Server (milliseconds)	N/A	N/A	N/A

License	Description
VEMS Mystro	Standard, Professional, or Enterprise
VEMS Record	Enables 2 concurrent recordings (10 or 40 license, or combination with an NVR).
VEMS Schedule	Enables the Scheduler.
VEMS Transcoder	Enables one transcoding license per server. Additional concurrent licenses available. This step is only applicable if you are using a version of VEMS prior to v6.3.8. See: Transcoder Licensing .
VEMS Zones	Enables 2 (Standard), 10 (Professional), or 100 (Enterprise) zones, or a custom number of zones.
VEMS Presentation	Enables live webcasts.
VEMS Channel Guide	Enables the Channel Guide with live programming data.
VEMS SharePoint	Enables VEMS integration with Microsoft SharePoint.
Learn360	Enables VEMS integration with Learn360 content that customer has licensed from Learn360.
Discovery Education	Enables VEMS integration with Discovery Education content and the My Discovery Education portal (My DE) that customer has licensed from Discovery Education.

Access Control

The ability to provide different users different access to resources on a network is typically referred to as access control. Access control is used to define users and groups of users and to define the roles and permissions for each. Users are basically a subset of groups. You can assign roles and permissions to groups or to individuals. Users do not have to belong to a group. By default all resources are *not* available to any users or groups. You need to explicitly provide access to resources to different users or user groups.

Roles are predefined; you cannot create roles. Roles describe the functionality a user or group is allowed to perform. For example only a System Administrator can mark videos as **Featured** or **Required**. Table 19 on page 30 shows all roles and the access rights of each role. Permissions give users or groups access to different resources. They define the categories or individual videos a user or group is allowed to access. They also define whether a user can edit or delete content.



Groups	27
Users.	35
Inactive Users.	37
User Announcements.	37

Groups

Grouping users is common practice and makes administering access to the Portal Server less complicated than administering access by individual user. The Portal Server lets you create groups, specify the group members, 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, you can import a portion or all existing groups and privileges. See [Import Groups from LDAP](#) on page 33. The following screenshot shows all currently defined groups. Use the controls at the top of the page to search for named groups; to set the number of groups shown on each page; or use the arrows to navigate through the pages. Click on the group name to see the roles assigned to the group. Click on the **Duplicate** button to create another group with the same Roles and Permissions. Click on the **Edit** button to modify existing Roles or Permissions.













-
- Notes**
- The functionality for creating and managing groups is as explained here is basically the same for creating individual users. See [Users](#) on page 35 for more about this.
 - The paging controls near the top of the page are not functional if the number of users or groups is less than or equal to the value in the dropdown (default = 100).
-

Groups Administration

Groups Administration Q

Import Groups from LDAP
Create New Group

Current Groups: Items per page: 100 ▼

Groups List	Duplicate	Edit	Delete
1. Administrators			
2. Public			
3. Publishers			
4. Viewers			

Create New Group

Add Group Users

Use this page to create a new group from scratch. First enter a **Group Name** and **Description**. Then select the users that will be in the group. The list of all defined users is shown on the left; the list of users currently assigned to the group is shown on the right. Use the **Add** or **Remove** buttons as necessary. Note that if the number of users or groups exceeds 1000, you can click the **Load More** button to append additional users or groups to the bottom of the list.

Groups Administration

Group Information

Group Name

Description

Group Users

All Users

Admin
andy
ContentAdministrator
ContentPublisher
ContentViewer
Guest
Scheduler
SystemAdministrator
UserAdministrator
VBrickAdministrator

Assigned Users

Edit Group Roles

After creating a new group, the next step is to go back to the Groups Administration page and "edit" (i.e. assign) the Roles and Permissions available to the group you just created. To assign roles to a group, click all the checkboxes on the left that will apply to the group. **When you mouseover a group role on the left, the features associated with that role are shown in bold on the right.** When you click on one of the features on the right, you can see an explanation of the operational details associated with that feature. *Be sure to click Save before continuing to the Permissions page.*

Note You can assign multiple roles to a group but the roles themselves (see Table 19) are fixed. You cannot change the functionality associated with a role.

User Administration

» **User Info**
» **Roles**
» **Permissions**

User Roles

Select Roles for User - andy:

System Administrator
 User Administrator
 Content Administrator
 Scheduler
 Content Publisher
 Content Editors
 Content Viewers
 Content Approver
 Content Approver Manager
 Channel Guide Administrator

Features for: **Channel Guide Administrator**

- Admin Services
- Broadcast Administration
- **Channel Guide Administration**
- **Content Administration**
- Content Approval
- **Featured Content Administration**
- **PublisherServices**
- **Required Content Administration**
- Root Services
- SchedulePrivilegeFull
- SchedulePrivilegeSuper
- **User Services**

Back to List
Save Clear

Table 19. Group/User Roles

Role	Admin Application	User Application	Scheduler Application
System Admin	Complete access to system including ability to assign roles and permissions, however user should be added to the Content Approver list.	View access including: <ul style="list-style-type: none"> • Mark videos as Featured or Required. • Grant administrative privileges on specific content items. • Add and Edit content metadata. • Perform Broadcast Administration. • Add Video. 	Complete access including: <ul style="list-style-type: none"> • View main scheduling page. • Create and Edit schedules. • Modify own schedules as well as other user schedules.
User Admin	Complete access, and should be added to the Content Approver list.	Same access as System Administrator.	Same access as System Administrator.
Scheduler	No access.	Same access as System Administrator except this role cannot perform Broadcast Administration.	Same access as System Administrator except cannot modify other user schedules.

Role	Admin Application	User Application	Scheduler Application
Channel Guide Admin	No access	<ul style="list-style-type: none"> • Channel Guide Admin • Content Admin • Featured Content Admin • Publisher Services • Required Content Admin • User Services 	View main schedule page only.
Content Admin	No access.	Same access as System Administrator.	Same access as System Administrator.
Content Publisher	No access.	Same access as System Administrator except this role cannot: <ul style="list-style-type: none"> • Mark videos as Featured or Required. • Perform Broadcast Administration. 	Same access as System Administrator except cannot modify the schedules of others.
Content Editors	No access.	Same access as System Administrator except this role cannot: <ul style="list-style-type: none"> • Mark videos as Featured or Required. • Perform Broadcast Administration. • Add Video 	View main schedule page only.
Content Approver	No access.	<ul style="list-style-type: none"> • Content Approval • User Services 	View main schedule page only.
Content Approver Manager	No access	<ul style="list-style-type: none"> • Content Approval and ability to move content between approval templates and push content to next approval step, or override approvals. • User Services. 	View main schedule page only.
Content Viewer	No access.	Same access as System Administrator except cannot: <ul style="list-style-type: none"> • Add or Edit any content metadata. • Mark videos as Featured or Required. • Perform Broadcast Administration. • Add Video. 	View main schedule page only.
Content Download	No access.	Same access as Content Viewer except this role can: <ul style="list-style-type: none"> • Download content. 	View main schedule page only.

Edit Group Permissions

Use this page to define the categories (i.e. folders) the members of the group are permitted to access. Use the first row at the top of the list (All) to grant access to all categories and content in the column immediately below.

User Administration

» **User Info** »
Roles »
Permissions

Advanced View | **Collapse All**

Select Permissions For User - andy Cascade child category

Grant Access	Category/Content	Access Type				
<input type="checkbox"/>	📁 All	<input type="checkbox"/> Add	<input type="checkbox"/> View	<input type="checkbox"/> Edit	<input type="checkbox"/> Delete	<input type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Uncategorized	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Arts	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 HDS	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Health and Guidance	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 HLS	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Language Arts	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Mathematics	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Recordings	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Science and Technology	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Social Studies	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 UploadedVideos	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 Vocational Guidance	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 WebcastVideos	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin
<input checked="" type="checkbox"/>	📁 World Languages	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Admin

Back to List
Save Clear

Advanced View	Show or hide individual "Access Type" options. These include the ability to Add, View, Edit, or Delete content. The Admin option permits changes to content metadata (e.g. Comments, Keywords, etc.). By default, these options will reflect the default permissions defined by the roles with which the user or group is associated.
Cascade child category	When checked, any child categories automatically inherit the permissions of the parent <u>plus</u> any additional right that have been assigned individually to the content.
Grant Access	Use to grant access to all categories and content. Default = No access.
Category/Content	Use to grant access to specific categories and content.
Access Type	Use to grant specific access rights (for example add, delete, or view) to specified categories and content. Admin rights allow you to manage content belonging to other users.

Import Groups from LDAP

When you use this page to import groups from an existing LDAP server, the group members and privileges are automatically recreated in the VEMS database. 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. VEMS supports multiple LDAP servers and if your site has more than one LDAP server used for authentication, you will need to select your server from the dropdown that is automatically displayed on the login page.

The list of LDAP groups shown on the page is generated automatically by a Scheduled Task called "Refresh LDAP Groups." This task runs automatically when an LDAP server is successfully configured in the system and runs (by default) once each. When an LDAP server is first added to the system it may take some time before the list of groups on this page is available. The system will warn you if the job has not finished running. If this happens, wait a few minutes and try again.

There are numerous LDAP directory products on the market today, but the most popular are Microsoft Active Directory, Novell eDirectory, OpenLDAP, and Oracle (Sun) Enterprise Directory Server. *VBrick supports these popular vendors but only Microsoft Active Directory and Novell eDirectory are fully tested.*

▼ To import LDAP groups:

1. Go to Access Control > Groups and click on **Import Groups from LDAP**.

Groups Administration

Import LDAP Groups

Starts With

LDAP Server:

Group Name	Server Name

To optimize system performance, import only the groups you will actively grant permissions to.

2. Using the dropdown, select the individual LDAP server (or all servers) from which you want to import LDAP groups.
3. Enter a comma-separated list of LDAP groups to search for and click the search button. This will auto-discover LDAP groups on the selected LDAP server(s).
Since there may be tens of thousands of LDAP groups, the LDAP administrator will know which groups are relevant for VEMS and can use the search box and the **Starts With** or **Exact Match** controls. For example you can use **Starts With "exc"** to get a list of all LDAP groups beginning with those letters.
4. Check the individual groups you want to import and click **Submit**.
5. The selected groups will be removed from the **Import LDAP Groups** page and added to the **Groups Administration** page.

Note Be aware that after importing groups of users, the individual users in a group will not be displayed on the User Administration page until each user actually logs in to the Portal Server application.

Group Name	Server Name
<input type="checkbox"/> Exchange All Hosted Organizations	Microsoft Test
<input type="checkbox"/> Exchange Domain Servers	Microsoft Test
<input type="checkbox"/> Exchange Enterprise Servers	Microsoft Test
<input type="checkbox"/> Exchange Install Domain Servers	Microsoft Test
<input type="checkbox"/> Exchange Servers	Microsoft Test
<input type="checkbox"/> Exchange Trusted Subsystem	Microsoft Test
<input type="checkbox"/> Exchange Windows Permissions	Microsoft Test
<input type="checkbox"/> ExchangeLegacyInterop	Microsoft Test

LDAP Server	Select one LDAP server from those defined on the Devices > LDAP Servers page or All.
Page n of n	Shows which page you are on in the complete list of groups. Use the right and left arrow icons to go to the next or previous page.
<number of groups per page>	Select the number of groups to display on a page: 100, 500, 1000, 5000.
Select All	Select all discovered groups.

Clear All	Clear all selected groups.
-----------	----------------------------































Users

Creating users is an optional step that can be completed when you need to provide a single user with additional privileges above and beyond what is available in the group(s) to which they are assigned. Users can be assigned to multiple groups. Creating users (and assigning roles and permissions) is basically the same as creating [Groups](#) except that the user information is slightly more detailed. Individual users can be added or deleted. Deleted users are moved to the [Inactive Users](#) page where they will remain until re-activated.

User Administration

User Administration

Current Users:
Items per page:

User List	Duplicate	Edit	Delete
1. Admin			
2. andy			
3. ContentAdministrator			
4. ContentPublisher			
5. ContentViewer			
6. Guest			
7. Scheduler			
8. SystemAdministrator			
9. UserAdministrator			
10. VBrickAdministrator			

Create New User

User Administration

User Information

User Status:

First Name: User Name:

Last Name: Password:

Email Address: Retype Password:

PIN:

User Groups

All Groups:

Administrators
Public
Publishers
Viewers

Assigned Groups:

User Status	<ul style="list-style-type: none"> • Active – user is active. • TempLock – user is temporarily locked out. • PermLock – user is permanently locked out. • Inactive – user is inactive.
First Name	Used for information only.
Last Name	Used for information only.
Email Address	Used for information only and to send webcast invitations.
PIN	Used to login to a set top box. You will need to enter a PIN to login to a set top box that is not entered in the system, or to allow multiple different users to access the same set top box.
User Name	Used to login to VEMS.
Password	Used to login to VEMS.
Failed Logins	Read-only. The total number of failed logins by this user.
Last Failed Login	Read-only. The date and time of last failed login by this user.

Inactive Users


This page shows all users who have been "deleted." They will remain on this page until re-activated.

User Administration

User Administration

Current Inactive Users:

Items per page :

User List	Activate
1. Zoe	

User Announcements

User announcements are displayed in a text area on the client interface Home page. Keep in mind that the announcements are constrained by the size of the window and should not exceed a few sentences. To create an announcement, simply click in the User Announcements window, start typing, and click **Save** when done.

System Announcement

There will be a CFO webcast at 3:00 PM this afternoon.
Please make every effort to attend.

User Announcements

The current active user/system announcement is:

There will be a CFO webcast at 3:00 PM this afternoon. Please make every effort to attend.

Save

Delete

Content Management

Content Management includes features used to define content metadata (Custom Fields) and to save videos in meaningful, related folders (Category Management). Custom fields are used to add additional fields to the Additional Info pages associated with live and stored streams. This lets you provide more information on the page and makes it easier to search for specific keywords. Category Management lets you create, edit, and delete the "categories" with which all videos are associated. Live and Stored URLs provide the administrator with the ability to add Live URL streams and Stored URL streams. This functionality is identical to the Add Video feature in the user interface.

Note Support for entering HLS and HDS content was added in VEMS Mystro 6.3.

Content Management	Category Management	39
Category Management	Edit a Category	40
Custom Fields	Live Entered URLs	43
Live Entered URLs	Stored Entered URLs	46
Stored Entered URLs	Content Workflow	48
Content Workflow	Recommended Videos	54
Recommended Videos	Required Videos	55
Required Videos	Report Permissions	55
Report Permissions		

Category Management

One or more categories can be associated with each piece of video content. These categories are determined by the administrator of the system when first configured and they can be added to, changed or deleted. If you are migrating from a previous version then categories are typically derived from the folder structure of the content on a VOD server but can also be created manually. When working with categories, check the box to select the category you wish to edit or add subcategories to.

Category Administration

List of Categories :

Delete Multiple Categories

<input type="checkbox"/>	<input type="checkbox"/> Arts
<input type="checkbox"/>	<input type="checkbox"/> HDS
<input type="checkbox"/>	<input type="checkbox"/> Health and Guidance
<input type="checkbox"/>	<input type="checkbox"/> HLS
<input type="checkbox"/>	<input type="checkbox"/> Language Arts
<input type="checkbox"/>	<input type="checkbox"/> Mathematics
<input type="checkbox"/>	<input type="checkbox"/> Recordings
<input type="checkbox"/>	<input type="checkbox"/> Science and Technology
<input type="checkbox"/>	<input type="checkbox"/> Social Studies
<input type="checkbox"/>	<input type="checkbox"/> Uploaded Videos
<input type="checkbox"/>	<input type="checkbox"/> Vocational Guidance
<input type="checkbox"/>	<input type="checkbox"/> Webcast Videos
<input type="checkbox"/>	<input type="checkbox"/> World Languages

Add New Category

Edit Category

Delete

Add New Category

Click the **Add New Category** button and use this page to add a new category. There are no restrictions on Category Names. Use any combination of alphanumeric and special characters.

Categories	
Add New Category	
Add Category To	/
Category Name	<input type="text"/>

Edit a Category

Click the **Edit Category** button and use this page to edit a category. You must first select a category checkbox that you want to edit before clicking the button.

Categories

Edit Category

Current Category: Language Arts/

Category Name:

Delete a Category

Click the **Delete** button to delete a category. You must first select the category checkbox that you want to delete before clicking the button. If the category has sub-categories, they will be deleted as well.

Category Administration

Delete Multiple Categories

List of Categories :

Arts
 HDS
 Health and Guidance
 HLS
 Language Arts
 Mathematics
 Recordings
 Science and Te
 Social Studies
 Uploaded Vide
 Vocational Gui
 Webcast Video
 World Languages

VBrick

!

Are you sure you want to delete
Mathematics?
 Category Full Path:
Mathematics?

Delete Multiple Categories

Click the **Delete Multiple Categories** checkbox to delete several categories at once. You must first select a category checkbox from the **List of Categories** that you want to delete before clicking the **Delete** button. If the category has sub-categories, they will be deleted as well. You may also choose to expand a Category and delete several sub-categories at once.

Category Administration





List of Categories : Delete Multiple Categories

- Arts
- HDS
- Health and Guidance
- HLS
- Language Arts
- Mathematics
- Recordings
- Science and Technology
- Social Studies
- Uploaded Videos
- Vocational Guidance
- Webcast Videos
- World Languages

Custom Fields

Custom fields are used to create additional keywords for content metadata (on the **Additional Info** tab) and additional keywords you can search on in the Search box. Custom fields are used with stored videos and with live videos. The Custom Fields functionality lets you add additional "custom" fields that are appropriate to your business or application. This lets you provide more content metadata and also makes it easier to search for specific streams. (All defined fields are listed in the dropdown list box next to the **Search** button.)

Custom Field Administration

Field Name	Type	Edit	Delete
1. Biology	Text		
2. Sociology	Option		

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 Additional Info tab in Content Metadata (either as a text field or as a dropdown list box).





Add New Custom Field

Custom Field Administration

Add/Edit Fields:

Select Field Type:

Field Name:

Option Value	Edit	Delete
1. Political		
2. Scientific		
3. <input style="width: 100px;" type="text"/>	<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>

▼ To create a Custom Field:

1. Enter a **Field Type** and a **Field Name**. If you select **Option**, you can add items one at a time followed by **Submit**. These items will populate a dropdown list in the search box on the All Video page.
2. When done, click **Add Custom Field**. The field will be added as keyword in the Search box and as an Additional Info option on all Content Metadata pages.

Note If you will be adding numerous custom fields, such as Education State Standards, you can use the VEMS Mystro Custom Field Import Tool to simplify this process. You can get this tool from the VBrick website at www.vbrick.com/support/downloads

Live Entered URLs

This functionality is typically used to enter a live URL that is not sourced from a VBrick device. Administrators can manually enter URLs to live video streams that are not automatically displayed by the Portal Server. For example, you may wish to have the Announcements (SAPs) disabled on the VBrick encoders for security purposes. Or you may want to enter the address of an off-network stream such a stream coming from a hosting provider.

VEMS considers all live URLs associated with the same program name to be instances of the same stream. VEMS uses the information provided by either a Live Entered URL or by an "announcement" from a VBrick appliance to determine the appropriate destination of the stream based on the administrator's configuration of zones and preferred players. The advantage of using announcements (either standard Announcements or External Announcements) is that the live URL will only be displayed in VEMS when the stream is active and present. **When using a Live Entered URL, the stream is always displayed, regardless of whether it is active or not.**

Standard Announcements are typically used to announce the stream to other VBrick devices or applications. External Announcements are typically used to provide information about streams which are initially sourced from the appliance but ultimately sourced from outside the appliance. For example these might be streams sent from an appliance to a reflecting device (e.g. DME or) for redistribution to VEMS clients. For Live Entered URLs, this information is provided by using the **Source IP** parameter as explained below. (There is no comparable support for External Announcements.)

Live Entered URLs

Live Entered URL Administration

List of Live Entered URL :

Content Title	Edit	Delete
1. Live Entered URL (http://172.22.130.24 - HLS)		

Note The correct player, for example the Windows Media Player for .wmv files or the QuickTime player for .mp4 files, must be present on the client desktop for users to receive and play live streams.

Add New Live URL

Live Entered URLs

Live Entered URL Administration

Content Title:

URL:

Bit Rate:

Source IP:

Encoding Type:

Multicast?:

Categories

- (Uncategorized)
- Arts
 - Music
 - Children's Songs
 - History
 - Musical Instruments
 - Musicians
 - Theatre
 - Dramatists
 - General
 - Visual Arts
 - Architecture
 - Artists

Content Title	Title is what will display to clients in the VEMS Portal Server viewing pages.
URL	Enter a valid URL or IP address. See examples below.
Bit Rate	Enter bit rate if available.
Source IP	This parameter is used to filter entered URLs for Zones. When using Zones to direct Portal Server clients to specific servers, you may need to define a source IP address to identify a server that is outside the defined zones or uses a hostname exclusively. A Source IP may be necessary when manually entering URLs for live or stored streams. In a common scenario, a Source IP 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 Source IP is also used in cases where the stream URL is identified by a host name. The Source IP identifies the zone for the viewing URL; it can be any arbitrary address within the zone. When entering a live multicast URL, the Source IP is always required even if you are not using zones. <i>The Source IP is not necessary when the IP address of the URL itself can be identified as being in the zone.</i>
Encoding Type	Select one: WM, MP2, MP4, H264, H264TS, FLASH, FlashMulticast, SilverlightRMS, HLS, HDS, Other.

Categories	Optional. Select one or more categories for the live 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
WM	<pre>http://172.22.2.147/vbs1http.asx</pre> <pre>http://172.22.2.147/vbrickvideo1</pre> <p>Where 172.22.2.147 is the source IP address and vbrickvideo1 is the program name.</p>
H.264	<p><u>RTSP Streams</u></p> <pre>vbrtsp://172.1.1.1/vbStream1S1</pre> <p>Where 172.1.1.1 is the source IP address and vbStream1S1 is the resource name.</p> <pre>vbhttp://172.1.1.1/vbStream1T1.sdp</pre> <p>Where 172.1.1.1 is the source IP address and vbStream1T1.sdp is the SDP file name.</p> <p><u>Multicast Transport Streams</u></p> <pre>vbricksys://ip=239.16.120.3&port=4444&cc=off&license=http://172.22.130.23/License/CombinedLicensedUser.lic</pre>
Flash	<pre>rtmp://VOD/publishingpoint/file.flv</pre> <pre>rtmp://172.22.2.97/vod/sample1.flv</pre> <pre>rtmp://172.22.2.97/vod/mp4:sample2.f4v</pre> <pre>rtmp://172.22.2.97/vod/mp4:sample3.mp4</pre> <pre>rtmp://172.22.2.161/vod/mp4:folder1/folder1_2/sample.m4v</pre> <pre>http://172.22.2.97/vod/sample5.flv</pre> <pre>http://172.22.2.97/vod/sample6.f4v</pre> <pre>http://172.22.2.97/vod/sample7.mp4</pre>
HLS	<pre>http://172.16.2.182/HLS/videos/playlist.m3u8</pre> <pre>http://192.168.25.165/HLS/A1/playlist.m3u8</pre>



Stored Entered URLs

Administrators can manually enter URLs to VOD or DME content that is not automatically displayed by the Portal Server. For example these URLs can point to content located on a QuickTime/Darwin server or a Windows Media server. This is valuable feature if you want to enter an off-network stream from an Apple Darwin Server or if there is Windows Media content that needs to be displayed through the Portal Server interface.

Stored Entered URLs

Stored Entered URL Administration Q

List of Stored Entered URL :

Content Title	Edit	Delete
1. Non YouTube Video (http://cnn.com/video/world/2013/04/18/truck.overturns - FLASH - FLASH)		

Add New Stored URL

Stored Entered URLs

Stored Entered URL Administration

Content Title:

URL:

Bit Rate:

Encoding Type: ▼

Categories

- (Uncategorized)
- Arts
 - Music
 - Children's Songs
 - History
 - Musical Instruments
 - Musicians
 - Theatre
 - Dramatists
 - General
 - Visual Arts
 - Architecture
 - Artists
 - Criticism

Content Title	This is what will display to clients in the VEMS Portal Server viewing pages
URL	Enter a valid URL or IP address. For example: rtsp://ipaddress/programname mms://ipaddress/videoname.wmv
Encoding Type	Select from dropdown.
Categories	Select the categories in which the video will be included.

Content Workflow

Content workflow determines whether or not there is an "approval" process associated with stored content being added to the system, and if so, exactly what steps are required before the content is "approved" and made available to viewers. The content workflow process is typically used in environments which require complex legal and procedural rules for content publishing. Content workflow is enforced by "templates" that describe the workflow steps in detail. There is also end-to-end tracking and history of actions taken during content approval cycle. The Reporting > [Content Approval Status](#) page shows the status of all content waiting for approval or content that has been approved, rejected, or deleted. As explained below, Content Approval is configured on the System Settings > [Global Settings](#) page.

Workflows are associated with groups. When content is added to the system, it checks the logged-in user's group membership and the content is assigned to a workflow based on the group this user belongs to. This is the "workflow entry condition." Every workflow has an entry condition which defines the groups that will be allowed to approve content. There are three basic scenarios that then come into play: (1) If User1 belongs to Group1, any content added by User1 is associated with Workflow1. (2) If User2 belongs to Group1 and Group2, the system cannot assign a workflow and the content will appear on the approver's **Videos for Approval** tab (on the user interface) with an **Awaiting Workflow Assignment** button. (3) If User3 belongs to no groups, the content is assigned to the **Default** workflow in the **List of Workflow Templates** (see below).

Content Workflow Template			
Workflow Template Administration			
List Of Workflow Templates :	Items per page: 5	Add Workflow Template	
Name	Default	Edit	Delete
Default Content Approval Workflow	<input type="radio"/>		
Marketing Workflow	<input checked="" type="radio"/>		

Table 20. Content Workflow Components

Component	Description
User Groups	Defines the user groups that will be required to use this template when adding content. For example there may be different workflow templates for different groups within an organization.

Component	Description
Approvers	Defines the specific user or group of users who are responsible for approving content during each step of the workflow.
Steps	Defines the sequence of steps in the linear approval process as a piece of content moves from one individual or group to another for approval. For example, the content may need a manager review and then a director review.





Content Workflow Template				
Workflow	Steps	Email Templates		
List Of Workflow Steps :		Add Workflow Step		
Name	Order	Edit	Delete	
Step 1	1			
Step 2	2			

Figure 5. Workflow Templates List

As explained in the "Content Approval" topic in the Portal Server *User Guide*, content approvers will see a **Videos for Approval** tab on their home page in the user interface. This pane will show all content waiting for approval along with various buttons that will let them approve, reject, or otherwise manage the approval process. Content approvers may also be alerted via email notification if this is configured as part of the process.

- Notes**
- If content approval is enabled, the default workflow applies to any content added using (1) Add Video, (2) push-button recording, and (3) Scheduled recording. Auto-discovered content and webcasts are automatically approved.
 - You can only edit or delete a workflow when there is no unapproved content in that workflow.
 - A content approver must have "edit" rights to the categorie(s) in which the approved content will be saved.

Configuring Content Approval

Content approval must be enabled on the System Settings > [Global Settings](#) page. Content Approval Email Notifications can also be enabled on this page. If Approval Email Notifications are enabled, make sure that the SMTP mail server (also on the Global Settings page) is configured correctly. Use the **Send a test email** feature to verify the email is working properly.

▼ To enable a content approval workflow:

1. Optional. On the Mystro Admin interface, go to System Settings > Global Settings and check **Enable Content Approval Workflow**. Configure e-mail notifications that will be auto-generated when content needs approval. Email notifications will be sent to all users with "content approval" privileges who have a valid e-mail address configured on the **User Info** page.

Off	Default. No emails generated
Individual	One email is generated for each video (or clip) that requires approval
Digest	Once daily (by default) when the Approval Batch Email Processing task runs in the Task Scheduler. Administrators can override the Task Scheduler setting and run the task on demand from the Task Scheduler. This will run the task immediately and send email notifications alerting content approvers that there is content waiting for approval.

2. Configure a user (or a group of users) who will be responsible for approving content. If necessary, go to **Access Control > Users** and use the **Roles** tab to configure a user with "content approval" privileges. Each content approver will be asked to approve only content that exists in categories to which they have been granted access. Only the following user roles have content approval privileges:
 - System Administrator
 - User Administrator
 - Content Administrator
 - Content Approver
 - Content Approver Manager

Creating a Workflow Template

Use the following pages to create a workflow template. The Workflow Entry page is used to define the user groups that will be required to use this template when adding content.

- ▼ To create a workflow template:
 1. Go to Content Management > Content Workflow and "edit" the default workflow which you will save with a new **Workflow Name**.

Content Workflow Template

» Workflow
» Steps
» Email Templates

Workflow Template

Workflow Name:

Workflow Entry Condition

User Groups

All Groups:

Administrators

Public

Publishers

Viewers

Assigned Groups:

2. Enter a unique **Workflow Name** and configure the groups of users who will be adding content. (The individual users who will be adding content must belong to a group.) Move these group(s) to the **Assigned Groups** box on the right.
3. Click **Save** and go to **Steps**. Use this page to define the sequence of steps in the linear approval process as a piece of content moves through multiple approval steps from one individual or group to another for approval.

Content Workflow Template

» Workflow
» Steps
» Email Templates

Step Information

Step Name:

Description:

Instructions:

Approver Groups for this step

User Groups

All Groups:

- Administrators
- Public
- Publishers
- Viewers

Assigned Groups:

Approver Users for this step

Users

All Users:

- Admin
- Admin (Dup1)
- ContentAdministrator
- ContentPublisher
- ContentViewer
- Guest
- nick
- Scheduler
- Stan
- SystemAdministrator

Assigned Users:

4. Give each step a meaningful name and description and then add the groups or users who will be assigned as "approvers" to the **Assigned Groups** or **Assigned Users** box on the right.
5. Click **Save**, click **Back to List**, and click **Add Workflow Step**. Repeat the previous step as many times as desired to create a multi-step approval process.
6. When done go to **Email Templates**. The templates on this page will let you modify the email messages (and language) that are sent to content approvers during the different steps in the workflow. You can modify the existing templates but you cannot add templates. Note that `<$WorkflowName$>`, `<$WorkflowAction$>`, and `<$ContentTitle$>` are wildcards that will be dynamically replaced by Workflow Name, Action and Content Title respectively (in the selected language) when the actual email is sent to users. Use these wildcards in the email title or message body to refer to the Workflow Name, Action or Content Title. Use the wildcards exactly as shown—do not make any changes to these wildcards.

7. To modify an email template:
 - a. Select the email template you want to modify.
 - b. Select the language (English, French, or Spanish).
 - c. Click the **Lookup Template** button.
 - d. Modify the email title or body text, click **Submit**, and you are done.

Content Workflow Template

» Workflow
» Steps
» Email Templates

Select the type of email template:

Enter Workflow ▾

Select Language:

English (United States) ▾

Lookup Template

Email title:

New content in <\${WorkflowName}>

Message body:

New content named "<\${ContentTitle}>" has entered "<\${WorkflowName}>" workflow and requires your approval. The link below will allow you to view the upcoming action for this content.

Submit

Clear

Email Template	<ul style="list-style-type: none"> Enter Workflow Notify manager Workflow Action - Approvers Workflow Action - Owner Exit Workflow Reminder Email Digest Email Awaiting Workflow Assignment
Language	<ul style="list-style-type: none"> English (United States) French (Canada) Spanish (Spain)
Email Title	<p>The email title associated with the selected template. For example:</p> <p>Reminder - you must take action on content in <\${WorkflowName}></p>

Message Body	The message body associated with the selected template. For example: <pre>Content named "<\$ContentTitle\$>" in "<\$WorkflowName\$>" workflow still requires the following action : <\$WorkflowAction\$> and requires your attention. The link below will allow you to take action on this content.</pre>
--------------	--

Recommended Videos

This page lets an admin user "unrecommend" content that has been tagged as "recommended" by any other users. (Note that the user interface lets people unrecommend only content they themselves have recommended.)

▼ To uncommend content:

1. Go to Content Management > Recommended Videos.
2. Click on the button associated with the content you want to unrecommend.

Recommended Videos

Recommended Videos Administration

Currently Recommended Videos:
Items per page:

	Title	Recommended By Unrecommend
1.	10 minute HD_51193FD6	victor silva
2.	AndyWM_13_03_22_16_14_51	victor silva
3.	BMW 335i	victor silva
4.	Victors_H264_TS_13_02_13_14_22_25	victor silva

3. Uncheck the users and groups for whom this content is recommended (by default all users and groups are checked) and click **Submit**.

Users Recommended For

Default Administrator

Groups Recommended For

Administrators
 Viewers
 Publishers
 Public

Required Videos

This page lets an admin user "unrequire" content that has been tagged as "required" by any other users. (Note that the user interface lets people unrequire only content they themselves have required.)

▼ To unrequire content:

1. Go to Content Management > Required Videos.
2. Click on the button associated with the content you want to unrequire.

Required Videos Administration		Items per page: 20
Currently Required Videos		
Title	Unrequire	Required By
1. 10 minute HD_51193FD6		victor silva
2. AndyWM_13_03_22_16_14_51		victor silva
3. Victors_H264_TS_13_02_13_14_22_25		victor silva

3. Uncheck the users and groups for whom this content is required (by default all users and groups are checked) and click **Submit**.

Users Required For

Default Administrator
 Default Scheduler

Groups Required For

Administrators
 Viewers
 Publishers
 Public

Report Permissions

VEMS Mystro has a robust reporting capability that provides a variety of reports and reporting options. In a typical scenario an administrator will run VEMS Mystro reports from the *admin* interface to check on login activity, content inventory, and other metrics. This functionality is explained in detail in [Reporting](#) on page 187. The functionality described here explains how to configure specific end users who will be allowed to run those same reports

from the *user* interface. As explained below, each designated user will be associated with specific reports. After these Report Permissions are configured, that user will be able to access these reports from the **Reporting** tab on the user interface.

- ▼ To configure a user to run reports from the user interface:
 1. Go to Content Management > Report Permissions.
 2. When the following page is displayed, select one report (e.g. Content Inventory) from the dropdown listing all reports.
 3. In the right-hand column select a **User Group** or an individual **User** and click **Add**. (These groups and users must be configured in advance using the [Access Control](#) pages.)
 4. Click **Save** and a message will indicate that permission was granted successfully.

The screenshot shows a web interface for configuring report permissions. It is divided into three main sections:

- Select a report:** A dropdown menu is set to "Content Inventory".
- Select a Group:** This section has two columns. The left column, "User Groups", lists "Administrators", "Public", "Publishers", and "Viewers". The right column, "Assigned Groups", is currently empty. There are "Add" and "Remove" buttons between the columns.
- Select a User:** This section also has two columns. The left column, "Users", lists various roles: "Admin", "ContentAdministrator", "ContentPublisher", "ContentViewer", "Guest", "Scheduler", "SystemAdministrator", "UserAdministrator", "VBrickAdministrator", and "WebcastAnonymousViewer". The right column, "Assigned Users", has "stan" selected. There are "Add" and "Remove" buttons between the columns.

At the bottom of the interface, there are three buttons: "Clear All", "Save", and "Clear".

5. **Repeat these steps for each report.** When done the configured user will see a **Reporting** tab on the user interface and the page will have a dropdown menu showing all of the reports that this user is allowed to run.

Advanced Content Distribution

Overview	57
Ingesting Video to an Offline Stored Server	57
Ingesting Video to a Specific Stored Server	59
Redistributing Existing Content Based on Category Assignment	67

Overview

VEMS Mystro offers “advanced content distribution” solutions that enable organizations to dictate that their Stored Servers (Video on Demand Servers) ingest video when offline, specify which servers to send content to and, further, to redistribute existing content to various stored servers based on a designated category.

Advanced content distribution methods may be configured during content ingestion in VEMS through several different methods including when:

- Adding Video
- Recording Video
- Scheduling Video
- AutoIngest
- AutoIngestXML
- Webcast Recording and Publishing
- Transcoding Existing Content


Ingesting Video to an Offline Stored Server

Prior to VEMS 6.3.6, if a video was uploaded, recorded or auto ingested, the system attempted to upload that content to all stored servers that are Online. If one or more stored servers was offline during that period, the content would *not* be available to those stored servers even after they were back Online later.

Advanced content distribution now makes it possible for those stored servers to ingest this content once they are back Online.

Enabling Offline Stored Server Ingestion









- ▼ To support video ingestion to all offline stored servers, complete the following steps:
 1. Access **System Settings > Global Settings**.
 2. In the **Ingestion Options** section, seen below, make sure that the **Ingest to Offline Stored Server** checkbox is selected. By default, this checkbox is *not* selected. When it is not selected, *all* offline stored servers will be skipped during ingestion.

Ingestion Options	
Ingest to Offline Stored Server:	<input checked="" type="checkbox"/> 
Enable Advanced Content Distribution:	<input checked="" type="checkbox"/>
Content Storage Path:	<input type="text" value="Z:\VBrick\Archive"/>
Enable Transmux on H.264 Content:	<input checked="" type="checkbox"/>
Ingest H.264 Transport Stream and MP4 Files:	<input checked="" type="radio"/>
Ingest H.264 Transport Stream Files Only:	<input type="radio"/>
Ingest H.264 MP4 Files Only:	<input type="radio"/>

Note the following when stored server offline server ingestion is *enabled* by selecting this checkbox:

- When enabled, VEMS will attempt to ingest video to *all* stored servers.
- If a stored server is offline at the time of the ingestion process, the entire ingestion process will be marked as a failure.
- The failure status will be displayed on various status pages (this is current functionality).
- You may choose to purge the status if you do *not* want to ingest the file to the offline stored server(s).
- Conversely, you may also choose to fix the offline stored server(s) and wait for VEMS to re-initiate the ingestion process.

A new scheduled task termed **Restart Failed Ingestions** has been added to the **Task Scheduler (System Settings > Task Scheduler)**. This task will be scheduled to run every day at 5 o'clock AM by default.

13. Refresh Stored Content	Ready	2/10/2014 8:02 AM	Success	2/10/2014 10:02 AM		
14. Restart Failed Ingestions	Ready	2/10/2014 5:00 AM	Success	2/11/2014 5:00 AM		
15. Start Auto Ingest	Ready	2/10/2014 8:59 AM	Success	2/10/2014 9:14 AM		
16. State Cleanup	Ready	2/10/2014 1:51 AM	Success	2/11/2014 1:51 AM		

At the scheduled task time, VEMS will attempt to retry ingestion of the *offline* stored servers only.

Task Information	
Edit Features: Restart Failed Ingestions	
<input type="radio"/> Interval: Every: <input type="text"/> Minutes	
<input checked="" type="radio"/> Scheduled: Run at: <input type="text" value="5:00 am"/> <input type="button" value="v"/> Every: <input checked="" type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday	
<input checked="" type="checkbox"/> Enabled	

Note: A stored server *must* have at least one stored server publishing point and one stored server entry point defined. The ingestion process will skip the server without this info defined.

Ingesting Video to a Specific Stored Server

Prior to VEMS 6.3.6, when videos are uploaded, recorded or auto ingested, the system uploads that content to *all* stored servers that are configured. This may not be the most efficient use of resources for enterprises who have global locations and want content specified for particular locations pushed *only* to those geographically located stored servers to avoid using the storage and bandwidth of other geographically located stored servers.

This may also be the case, for example, for a school district that has implemented a centralized VEMS server for the district but desires individual school-based stored servers and doesn't want one school's content to go to another school's stored server. Advanced content distribution makes this possible.

Enabling Video Ingestion to a Specific Stored Server

There are three specific steps that must occur to push content to a *specific* stored server. They are:


1. Enable advanced content distribution
2. Assign stored servers to a category
3. Assign those categories when adding new content so that the content is then distributed to the assigned server. Keep in mind that if advanced content distribution is enabled, category assignment will be *required* when ingesting new content. This includes:
 - a. Adding new video
 - b. Recording or scheduling video
 - c. Publishing a Webcast
 - d. Transcoding existing content
 - e. AutoIngestion of content

Enabling Advanced Content Distribution

To push video to a specific stored server, you must first enable advanced content distribution. This is accomplished in **Global Settings**.

- ▼ To enable advanced content distribution, complete the following steps:
- 1. Access **System Settings > Global Settings**.
- 2. In the **Ingestion Options** section, seen below, make sure that the **Enable Advanced Content Distribution** checkbox is selected. By default, this checkbox is *not* selected. When it is not selected, published content will be distributed to *all* stored servers. When selected, VEMS will ingest content to specific stored servers based upon the category assigned to that server and content which is the next step.

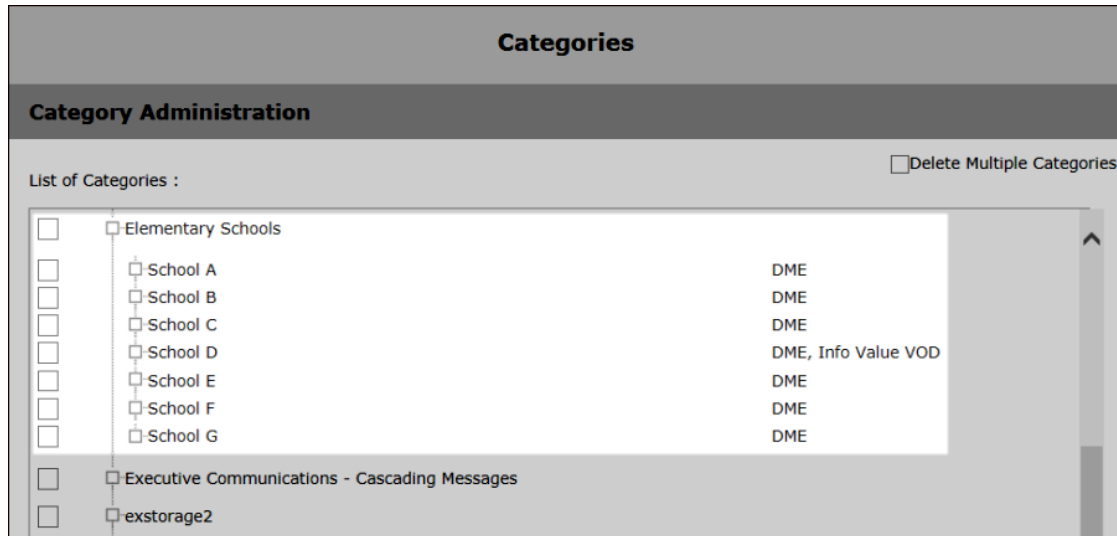
Ingestion Options	
Ingest to Offline Stored Server:	<input type="checkbox"/>
Enable Advanced Content Distribution:	<input checked="" type="checkbox"/>
Content Storage Path:	<input type="text" value="Z:\VBrick\Archive"/>
Enable Transmux on H.264 Content:	<input checked="" type="checkbox"/>
Ingest H.264 Transport Stream and MP4 Files:	<input checked="" type="radio"/>
Ingest H.264 Transport Stream Files Only:	<input type="radio"/>
Ingest H.264 MP4 Files Only:	<input type="radio"/>



- 3. The **Content Storage Path** field is also required once advanced content distribution is enabled. Note the following:
 - a. The Content Storage Path field may not be null if advanced content distribution is enabled as noted.
 - b. The path/folder specified in the Content Storage Path must exist/be correct.
 - c. VEMS servers must have read/write/delete access to the folder specified in the Content Storage Path or it will not be able to be saved.
 - d. The log on user of the Maduro Content Manager Service and the Identity of the IIS Application Pool where the Web App "MaduroSSL" is running must also have read/write/delete access to the folder specified in the Content Storage Path. (This is required for all VEMS servers)
 - e. All new content will be stored in the folder specified by the Content Storage Path. Every format is saved; only the highest bitrate is saved if a format has multiple bitrate instances.
 - f. The scheduled task **Purge Deleted Content** will scan the Content Storage Path periodically to delete any lingering file/folders that may remain when content is deleted by the system.
 - g. It is the Admin's responsibility to configure this field and folder securely.

Assigning Stored Servers to a Category

Once the **Enable Advanced Content Distribution** checkbox is selected, all stored servers will be listed on the **Category Administration, List of Categories** page, if assigned to a category. (**Content Management > Category Management**) You may need to expand a category to view the stored servers assigned as seen in the image below for the Elementary Schools category.



Keep in mind that *all* stored servers will be listed when you edit a category; including those offline servers and servers that have no entry or publishing point defined. (Select the **Edit** checkbox next to the category and then click the **Edit Category** button on the **List of Categories** page to edit a category)

When new content is assigned a category, *only* those servers that have been assigned to that category on the **Edit Category** page will have that content ingested.

For example, the image below depicts that all content assigned to the category Elementary School/School A will have it pushed to the School A DME only. That said, more than one server may be assigned a category if needed and, as a result, content assigned to that category will be pushed to all servers assigned. (School D, in the image above, is an example of this)

Note: When adding a new category, stored servers will also be able to be assigned as well (if advanced content distribution has been enabled).

Keep in mind the following for *new* content:

- Any newly created content must have a category assigned.
- If assigned categories are not associated with any stored server either directly or indirectly (rather, the category parent has the association), the content assigned will be ingested to *all* stored servers.
- If there is at least *one* assigned category that has an associated stored server either directly or indirectly, the assigned content will be ingested to the stored servers accordingly. The set of target stored servers is the union of the stored servers across categories.

To illustrate the above rules:

Stored-1 is assigned to category Elementary Schools. Stored-2 is assigned to category Elementary Schools/School A.

- A video in category Elementary Schools/School A will be uploaded to Stored-1 and Stored-2.
- A video in category Elementary Schools will be uploaded to Stored-1.
- A video in category Elementary Schools/School B will be uploaded to Stored-1.
- A video in category Science will be uploaded to Stored-1 and Stored-2.
- A video in category Elementary Schools and Science will be uploaded to Stored-1 and Stored-2.

Assigning Categories when Adding Video with Advanced Content

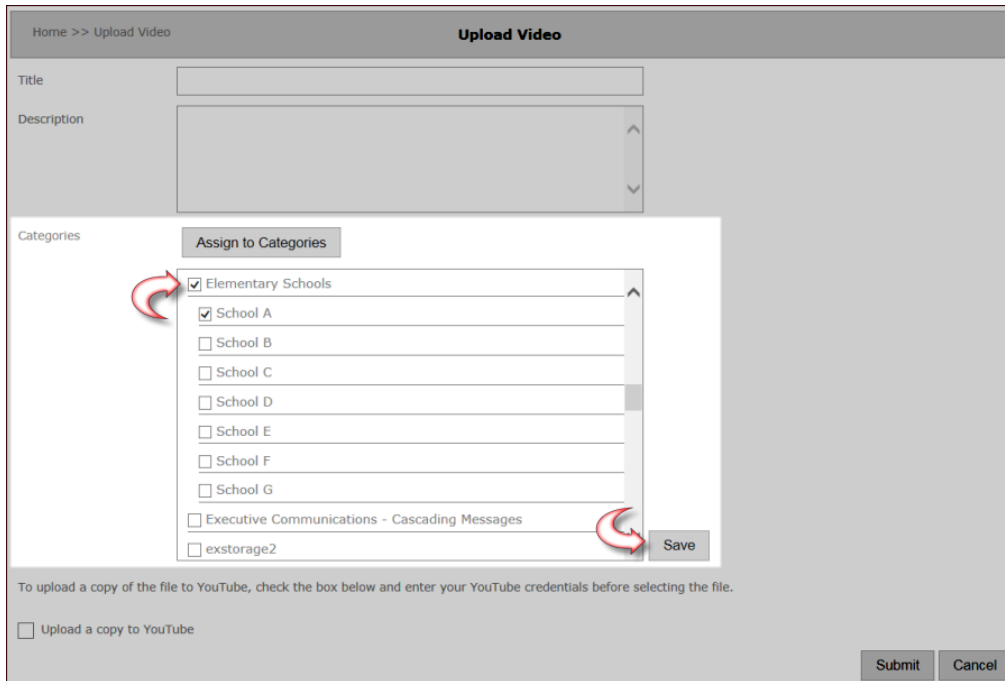
Distribution Enabled

If advanced content distribution is enabled, you must click the **Assign to Categories** button to assign a stored server category when uploading new video (for both upload video and upload multi-bitrate files). This is to ensure that content is pushed to the correct stored server. If advanced content distribution is not enabled, clicking this button is optional.

Until at least one category is assigned, valid file extensions are empty and a file may not be uploaded. This is seen in the image below.

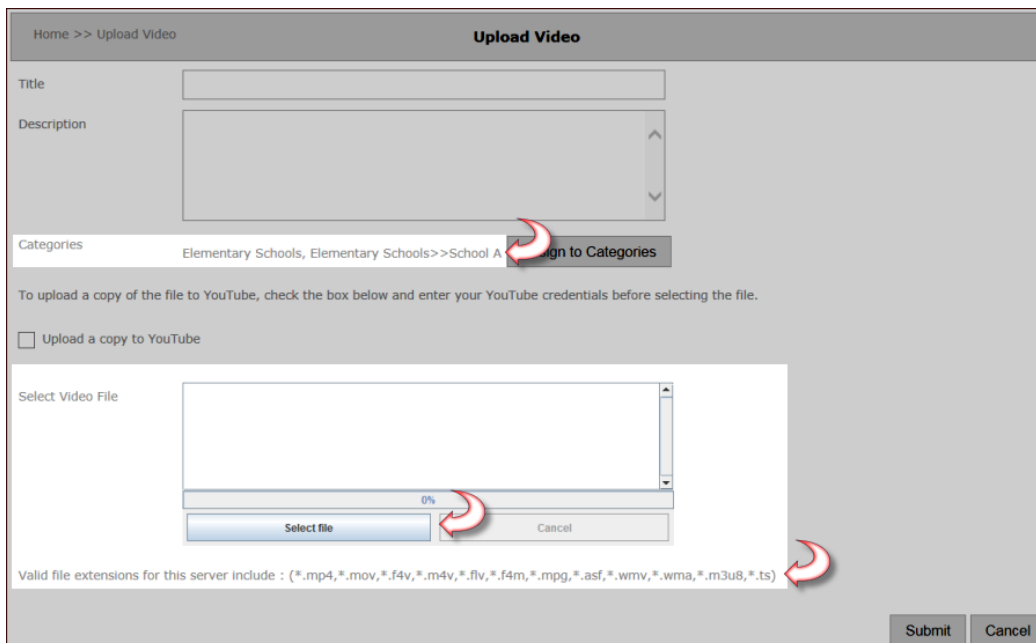
The screenshot shows the VBRICK web interface for uploading a video. The top navigation bar includes 'Home', 'My Videos', 'All Videos', and 'Add Video' (which is highlighted). A search bar is visible on the right. The main content area is titled 'Upload Video' and contains a 'Title' field, a 'Description' text area, and a 'Categories' section. In the 'Categories' section, there is an 'Assign to Categories' button and a red warning message: 'Until a category (and subsequent stored server) is assigned to the new content...'. Below this, there is a checkbox for 'Upload a copy to YouTube' and 'Submit' and 'Cancel' buttons. At the bottom, there is a copyright notice and options for 'Preferred Language' (set to English (United States)) and 'Change Theme' (set to Mystro Light Theme).

When the **Assign to Categories** button is clicked, the category edit list box will display, seen below. Category edit will list all the categories the user may assign to the video. Note that these categories will have been assigned to one or more stored servers as well so that the content will be uploaded to that specific server.



Once the video is added to one or more categories, the **Save** button is clicked and the edit category list box will be removed. The selected categories will then be listed horizontally, separated by commas, next to the **Assign to Categories** button as seen in the image below.

Further, notice that the valid file extension list will now be updated and the ability to now select a file to upload. At this point, a file with the appropriate extension may be uploaded and it will be pushed to the stored server assigned to the category selected.



Assigning Categories when Recording with Advanced Content Distribution Enabled

If advanced content distribution is enabled, you *must* assign at least one category when using push-button recording in the **Channel Guide** (seen below) or on the Live Video Viewing Page, or when using the **Scheduler** to schedule a recording and completing the **Content Metadata** information. If a category is not assigned when using these features, and advanced content distribution is enabled, an error message will be displayed.

Enter New Recorded Content Information:

Title:

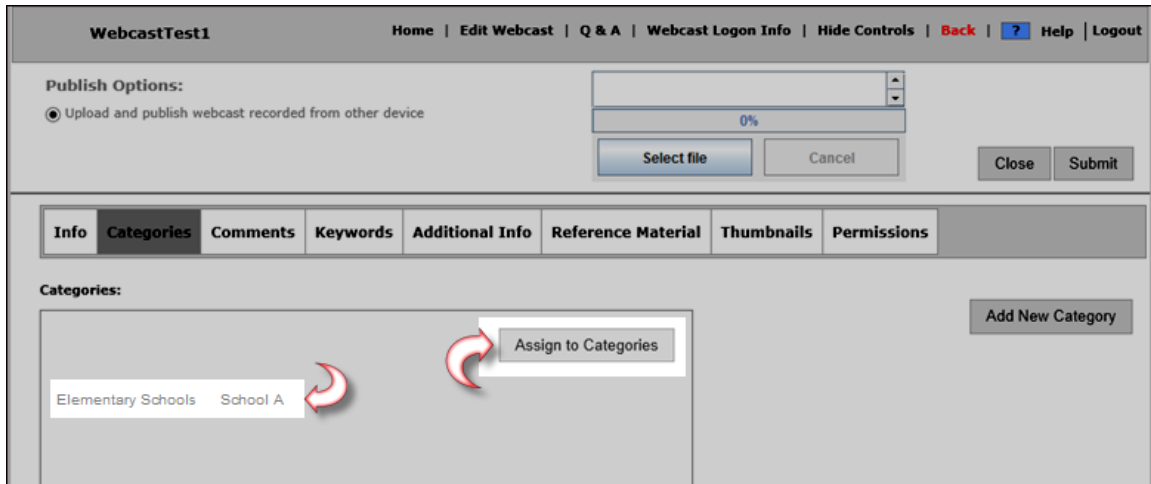
Description:

Categories:

- Elementary Schools
- School A
- School B
- School C
- School D
- School E
- School F
- High School
- School I
- Middle Schools
- School G
- School H

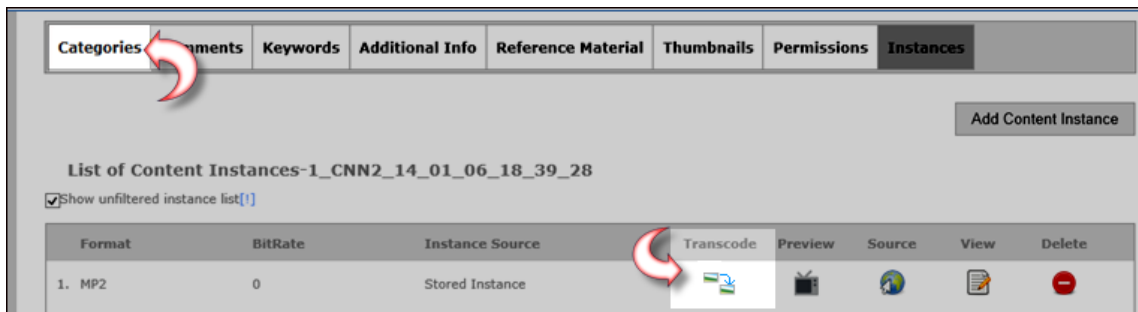
Assigning Categories when Scheduling and Publishing Live Webcasts with Advanced Content Distribution Enabled

If advanced content distribution is enabled, you *must* assign at least one category when scheduling and publishing a live **Webcast** to a stored server. If a category is not assigned when using these features, and advanced content distribution is enabled, an error message will be displayed.



Assigning Categories when Transcoding Existing Content with Advanced Content Distribution Enabled

If advanced content distribution is enabled, you *must* assign at least one category before clicking the **Transcode** icon to transcode existing content and create new instance streams. (**All Videos > Instances > Transcode** icon). If a category is not assigned when using this feature, and advanced content distribution is enabled, an error message will be displayed.



AutoIngestion Categories with Advanced Content Distribution Enabled

If advanced content distribution is enabled, VEMS Mistro Auto Content Ingestion and Auto Content Ingestion via XML features will follow very specific rules for categories.

AutoIngest Advanced Content Distribution Category Rules

Files put in the normal **AutoIngest** folder will be assigned to the **AutoIngestedVideos** category. You can then control the distribution to stored servers based on that category. Files can also be put into the category specific sub-folder.

If the **AutoIngestedVideos** category is not yet created, VEMS will create it.

AutoIngestXML Advanced Content Distribution Category Rules

File ingested via **AutoIngestXML** will be assigned to the **AutoIngestedVideos** category automatically in addition to other categories specified in the XML file.

Redistributing Existing Content Based on Category Assignment

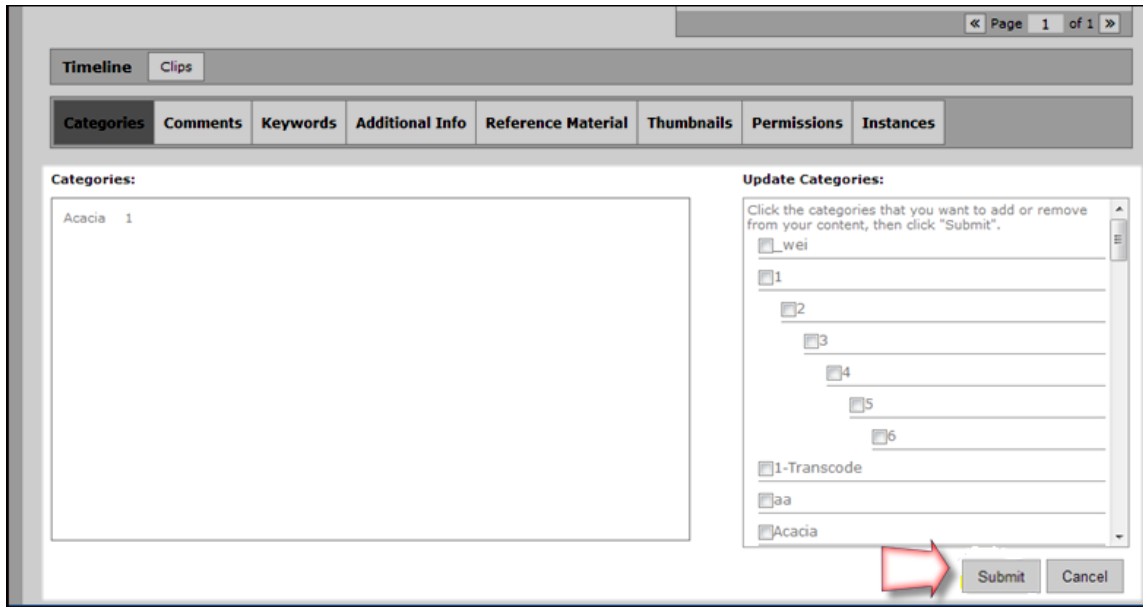
With advanced content distribution enabled, administrators will have the ability to move videos from one stored server to another stored server based on category assignment. If new categories are added after a video has been uploaded and the video is assigned to a new category, the video will be redistributed to the stored servers assigned to the category. Similarly, if a video is removed from a category, it will be removed from the associated stored server as well unless there are other categories that use the same stored server.

Keep in mind the following:

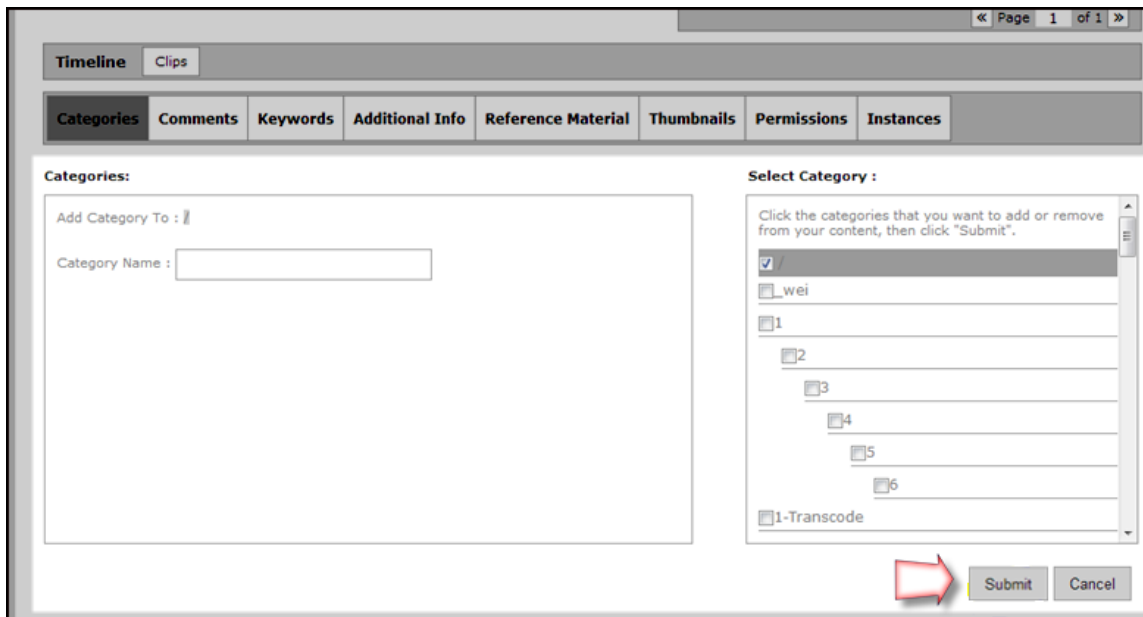
- This feature will only work on newly ingested content.
- There is no mass content copying or deleting.
- If a new stored server is added to the system and is assigned to a category that has associated content, it must be pre-populated by an Admin with this content.
- If an existing stored server is assigned to a category that has associated content, the system will not copy or sync content on that stored server with content in the folder specified by the Content Storage Path.
- If a category is deleted, the content on the stored server that is associated with the deleted category will not be deleted.
- When an earlier version of VEMS is upgraded to a version that has advanced content distribution, there is not content redistribution performed during the upgrade.
- Auto content copying/deleting only happens when a specific content is assigned to a new category or is removed from a category.

Content redistribution is only triggered in two places.

Content redistribution is triggered when the **Submit** button is clicked to assign categories to specific content.



Content redistribution is also triggered when the **Submit** button is clicked to create new categories that are assigned to specific content.



Devices

The Devices pages let you add, configure, and manage the hardware devices in your system. These include VBrick encoders, STBs, VOD servers, LDAP servers, etc.

Devices	
Application Servers	Application Servers 69
Channel Guide Servers	Channel Guide Servers 74
LDAP Servers	LDAP Servers 76
Presentation Devices	Presentation Devices 83
STB	STB 86
Stored Servers	Stored Servers 92
VBricks	VBricks (Encoders) 120
Script Devices	Script Devices 125
Control Devices	Control Devices 127
User Defined VBIRs	User Defined VBIRs 131

Application Servers

Application servers include Master servers, Redundant servers and NVRs. The Master application server is created when VEMS Mystro is installed. There can only be one "master" server. It can be edited; it cannot be deleted. The maximum number of simultaneous recording and transcodings allowed by license are shown in the page header. Both license types are the amalgam of all licenses in the system. VEMS Mystro automatically load balances the use of the slots by these license processes.

Application Server Administration

Server Administration

The maximum number of simultaneous recordings allowed by license: 10

Server List	Type	Max. Recordings	Edit	Delete
1. MEGATRON (TestApp Server Description)	Master	2		

Add Server

Depending on the environment at your location, you may have multiple Redundant servers or NVRs (in addition to the Master server) for scalability in large enterprises. The servers you configure on this page are initially defined during VEMS Mystro software installation.

Application Server Administration

Server Information

Type: Server Name:

Description:

FTP

User Name: Virtual Path:

Password: Local Path:

Record

Max. Recordings: Max. Bandwidth (kbps):

Recording Path:

AutoIngest

AutoIngest Path: Waiting List Size:

Active List Size:

Transcode

Max. Transcodings: Transcoder Priority: Low High

Type	Redundant or NVR.
Server Name	Enter a user-friendly display name for the server.
Description	Use to add descriptive information such as server 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 VOD-D, VOD-WM, and FTP servers is <code>vbrickuser</code> . The default user name for VOD-W servers is <code>anonymous</code> . 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.
	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 <code>vbrickuser</code> . If the FTP Password is changed on the server, it must be changed here as well. Use any combination of alphanumeric and special characters.
	Virtual Path	The virtual path that points to the content for playback.
	Local Path	Maps the publishing directory to the physical location on the VOD server.
Record	Recording Path	The virtual directory that points to the video for playback.
	Max. Recordings	The maximum number of concurrent recordings allowed.
	Max. Bandwidth	The maximum bandwidth of concurrent recordings allowed.
AutoIngest	AutoIngest Path	The content to be ingested can be placed in any named folder and will be ingested into the <code>AutoIngestedVideos</code> folder on each VOD server.
	Waiting List Size	The number of files that will be grabbed from the autoingest folder at a time and put into the autoingest queue waiting for ingestion. Default = 10.
	Active List Size	The number of files that will be actively ingested at a time. Default = 2.
Transcode	Max. Transcodings	Defines the max. number of concurrent transcodings allowed on this particular application server. The default is zero which disables transcoding on this server. If the maximum number of transcodings defined by the license file has been reached, an error message will be displayed if you try to increase the Max. Transcodings number. Note: This is only applicable if you are using a version of VEMS prior to v6.3.8. See: Transcoder Licensing .
	Transcoder Priority	Use the slider to defines the priority of the selected Application Server. If the priority is low, the server is less likely to be selected in the transcoder load balancing logic.

Application Server Administration

» **Server Info**
» **Entry Points**

Entry Points for Server: MEGATRON (TestApp Server Description)

Hostname or IP Address:

Port:

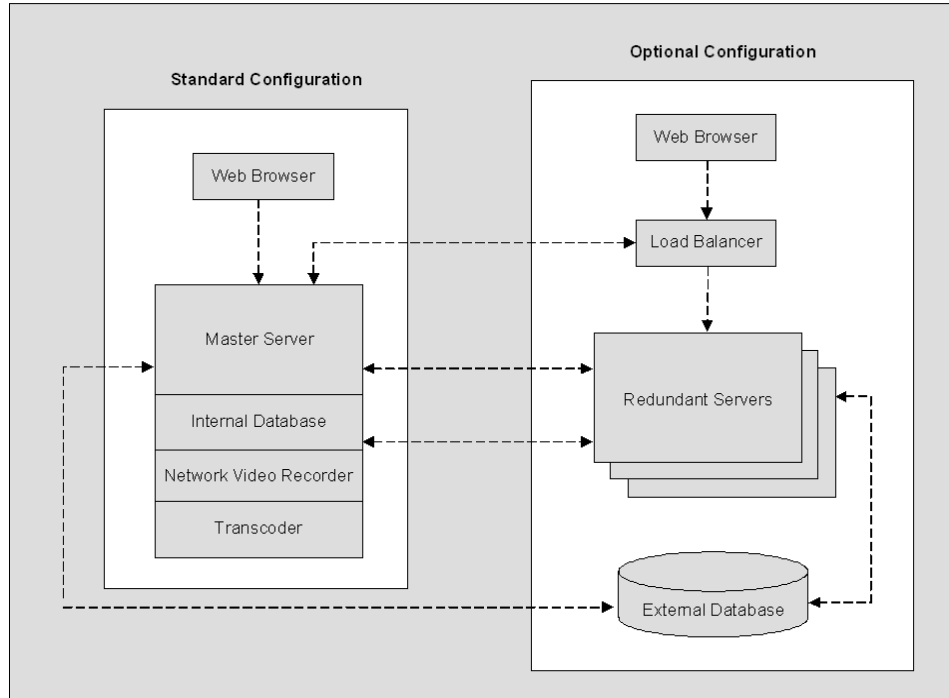
Requires HTTPS

Host Name	Host name used to identify the server.
IP Address	IP address used to identify the server.
Requires HTTPS	All application servers (including the master server) can be configured for HTTPS (for details see Configuring SSL on page 224). Once configured, this box must be checked to enable secure communication with the server. If SSL is not configured on the server, or this box is not checked, the system will use HTTP.

Load Balancer

If you have a redundant server in addition to the master server, you may implement a load balancer. This is optional and not provided by VBrick. When using a load balancer, all client requests are routed to the master or redundant server via the load balancer.

Keep in mind that “Client Affinity” will need to be set for the load balancer if a STB is configured to access VEMS Mistro servers via a PIN. VBrick recommends to associate each STB with a VEMS user instead of a PIN if a load balancer is used.



Channel Guide Servers

The Channel Guide is an optional feature that requires a license. To check whether a Channel Guide license is installed, go to the [About](#) page on the admin interface. Use this page to enable or disable the VBrick Channel Guide server or a third-party Channel Guide server. To refresh the Channel Guide content, go to System Settings > [Task Scheduler](#) and run the [Refresh Channel Guide](#) task.

VBrick Channel Guide Server

Use the following page if you will be enabling and using the VBrick-supplied Channel Server.

Channel Guide Server Administration

Add / Edit Channel Guide Server

Server Enabled

Server Type:

Server Name:

Description:

Server Enabled	Use to enable disable the Channel Guide server.
Server Type	Only the <code>VBrickSupportedWebService</code> is supported at this time.
Server Name	Descriptive name that will be shown on the user interface.
Description	Descriptive text for information only.

User-Defined Channel Server

Use this page to define the web service from which channel guide data is obtained. Only the `VBrickSupportedWebService` is supported at this time.

Channel Guide Server Administration

Add / Edit Channel Guide Server

Server Enabled

Server Type:

Server Name:

Description:

Web Service URL:

Password:

Confirm Password:

LDAP Servers

LDAP (Lightweight Directory Access Protocol) is a standardized method to access directories from multiple vendors. *VBrick supports major LDAP vendors including as Microsoft Active Directory, Novell eDirectory, OpenLDAP, 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. Contact Support Services for more information. Use the options on the following page to add or manage LDAP servers.

LDAP Server Administration

Select an LDAP Server:

Server Name	Edit	Delete

Add New LDAP Server

LDAP Server Administration

If you plan on using an LDAP directory other than Microsoft's Active Directory, VBrick strongly recommends using SSL to encrypt the communication between the Mistro server and the LDAP directory. Please consult your LDAP directory vendor for instructions on how to configure SSL.

LDAP Server Type:

Server Name:

Description:

Host:

Enable Server

This server requires credentials

Master User Name:

Master Password:

Retype Password:

[Advanced Settings](#)

[Back to List](#)

LDAP Server Type	Select from dropdown: Microsoft, Novell, OpenLDAP, or Sun. This automatically populates the page with the factory defaults for the selected server type.
Server Name	Enter a user-friendly display name for the server.
Description	Use to add descriptive information such as server location.
Host	Enter a Hostname or IP address.
Enable Server	Check to Enable Disable the server.
This server requires credentials	If checked, enter Master User Name and Password.
Use Single Sign-On	Microsoft Active Directory only. If checked, enter Master User Name and Password.
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.

Advanced Settings

If you plan on using an LDAP directory other than Microsoft Active Directory, VBrick strongly recommends using SSL to encrypt the communication between the VEMS server and the LDAP directory. Please consult your LDAP directory vendor for instructions on how to configure SSL. Advanced Settings are for use by experienced LDAP administrators. Use the scroll bar to see specific settings for the selected server. For a description of these settings, see the LDAP vendor documentation.

Advanced Settings

LDAP Protocol:

LDAP

LDAPS Sockets Layer

Port:

Users

Scope:

Class ID:

Class:

Name Attribute ID:

Name Attribute:

User First Name:

User Last Name:

User Email:

Groups Attribute:

Using LDAP with Single Sign-On

Active Directory and Internet Explorer only. The following procedures explain how to set up single sign-on Windows Server 2008. To use single sign-on, go to the configuration page for the LDAP server and check **Use 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.
- To enable Single Sign-On (and HTTPS) you must perform an additional configuration step as explained below in [Enable/Disable Single Sign-On and HTTPS/FTPS](#).

-
- Integrated Windows Authentication only works seamlessly with Microsoft Internet Explorer browsers (Windows only). 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-signon. If validated by at least one server, you are automatically logged in.

Enable/Disable Single Sign-On and HTTPS/FTPS

Note You must set up HTTPS and FTPS (see [Configuring SSL](#) on page 224) and verify proper operation before enabling single sign-on. Once HTTPS and FTPS are working properly with manual LDAP authentication, then you can configure and test single sign-on.

`MaduroSSLSettings.exe` is a console application that determines whether Single Sign-On and HTTPS (SSL) and FTPS are enabled or disabled. This application stops all VEMS services, edits certain configuration files for the services, and then restarts the VEMS services. **By default Single Sign-On and HTTPS/FTPS are both off.** *After enabling or disabling HTTPS/FTPS as explained below, an additional manual step is required only for HTTPS.*

`MaduroSSLSettings.exe` is located in: `C:\Program Files (x86)\VBrick\Maduro\Utils\MaduroSSLSettings.exe`

The complete usage of the command is:

```
MaduroSSLSettings.exe /[HTTP/HTTPS/] /[SSO/NoSSO] /[FTP/FTPS]
```

To enable/disable `HTTP/HTTPS`, `FTP/FTPS` and single sign-on, open a Command Prompt, navigate to the `Utils` folder, and run the command.

For example, the following command will disable HTTPS, FTPS and enable Single Sign-On:

```
MaduroSSLSettings.exe /HTTP /SSO /FTP
```

Note When prompted for the `HTTPS certificate domain name` (default = `jeremylaptop.vb.loc`) be sure that this address resolves directly to the server you are running the tool on and that it matches exactly the name the certificate is registered to.

Enable/Disable HTTPS in IIS

To enable or disable HTTPS, an additional manual step is required in IIS.

▼ To enable HTTPS in IIS:

1. After running the console application, go to Start Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
2. In the Connections tree view on the left, select Sites > Default Web Site/**MaduroSSL**.
3. In the Features view on the right select **SSL Settings**.

4. In SSL Settings, check **Require SSL** and **Ignore** client certificates. Then click **Apply** in the Actions pane on the right.
 5. Repeat this process for Sites > Default Web Site > **VEMSWeb**.
- ▼ To disable HTTPS:
1. Repeat the steps listed above for both MaduroSSL and VEMSWeb.
 2. In **SSL Settings**, uncheck **Require SSL**.

Using 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**).
 - Change Firefox's default settings to allow **Automatic logon with current username and password**.
 - Open a new tab with URL `about:config`
 - Bypass the warranty disclaimer
 - Enter NTLM in the **Search** field
 - Double click `network.automatic-ntlm-auth.trusted.uris` to edit
 - Add your VEMS server to the field and click **OK**.

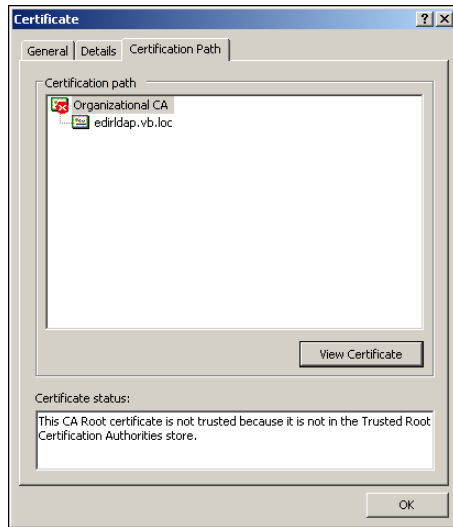
Using LDAP with SSL

When using TLS encryption, a VEMS client is effectively an LDAP client for an encrypted LDAP server. This VEMS client must be able to trust the certificate on the server. This is generally accomplished by using a trusted root certificate that recognizes the server certificate as valid.

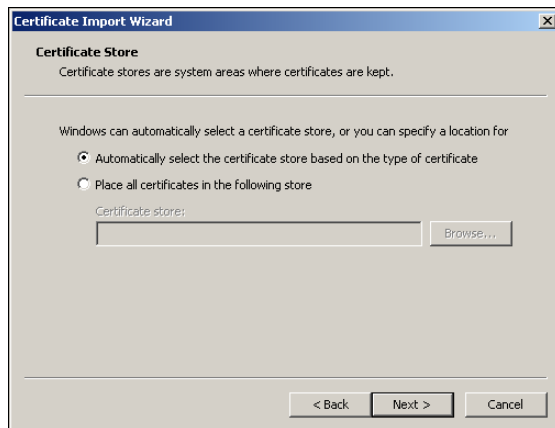
Installing the Root Certificate

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 [Resolving Other Security Alerts](#) on page 83) and `636` is the SSL port used to authenticate with the LDAP Server.
 3. When Internet Explorer displays a certificate error screen, click **View Certificate**.
 4. A Certificate window will open, click on the **Certificate Path** tab.
 5. If there is more than one 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 Certification 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.

▼ 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.

Presentation Devices

Use this page to define Presentation Devices that will be available in the Scheduler when configuring a Live Webcast. You will need to define a presentation device when the source stream is RMS (Rich Media Studio), RMD (Rich Media Desktop), or DME (Distributed Media Engine). You do not need a presentation device when the stream is sourced from a VBrick encoder, or from a VBrick encoder and a DME used as a reflector. (In other words if you have a standalone DME, you need a presentation device. If you have a DME used in conjunction with an encoder, you don't need a presentation device because you can specify a Viewing URL as an attribute of a VBrick encoder.)

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 an external viewing URL. For example an external URL can be the stream from RMS, RMD, DME, or it can be a 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 **Scheduler** functionality on the *client* user interface.

▼ To create a presentation device:

1. Go to **Devices > Presentation Devices** and click **Add Presentation Device**.
2. Enter the **Host Name** and **IP Address** of the RMS/RMD/DME machine.
3. Select a **Presentation Device Model** from the dropdown and click **Save**.

Presentation Device Administration

Presentation Device Information

HostName: IP Address:

Model
Presentation Device Model:

▼

RMS

RMD

DME

Generic

Software Revision:

Back to List

Save

Clear

Host Name	Host name used to identify the presentation device.
IP Address	IP address used to identify the physical presentation device.
Presentation Device Model	<ul style="list-style-type: none">• RMS – Rich Media Studio.• RMD – Rich Media Desktop.• DME – Distributed Media Engine.• Generic – used when the Viewing URL is any compatible URL/ direct stream, for example a web page (or a third-party encoder)
Software Revision	Reserved for future use.

4. On the Streams tab, click **Add Presentation Device Stream**.

Presentation Device Administration	
» Presentation Devices	Streams » Viewing URLs
Stream for: Euclid	
Stream Information	
Stream Number: 1	Stream Name: <input type="text" value="RMS Stream Name"/>
Email Template (Used for Webcasts)	
<input type="text" value="Please joins us for an RMS presentation."/>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

5. Enter a **Stream Name** corresponding to an available output on the source device, a message that will appear in the auto-generated email to each invitee in the presentation audience, and click **Submit**. Repeat this process for each additional slot.
6. On the Viewing URLs tab, click **Add New Viewing URL**.

Presentation Device Administration	
» Presentation Devices	Streams » Viewing URLs
Viewing URLs for: Euclid	
Stream Name:	<input type="text"/>
URL:	<input type="text"/>
Source IP:	<input type="text"/>
Bit Rate:	<input type="text" value="0"/>
Encoding Type:	<input type="text"/>
<input type="checkbox"/> Is Multicast URL	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Stream Name	Select a previously defined stream on the source device.
-------------	--

URL	Enter the Viewing URL of the stream (sourced from a presentation device). You can define multiple Viewing URLs. At the time of playback, VEMS selects the most appropriate instance of the stream for each viewer based on client capabilities, zones, etc.
Source IP	Used for <u>Zones</u> logic. If the stream is being reflected, enter the IP address of the reflector.
Bit Rate	Select a bit rate if available.
Encoding Type	Select the encoding type of the source stream, for example an H264 or SilverlightRMS stream coming from an RMS device.
Is Multicast URL	Check box if the source stream is defined as multicast.

7. Click **Submit** when finished configuring the Viewing URL and you are done.
8. Go to the **Scheduler** tab on the client interface and configure a **Live Webcast**. See "Authoring an RMS/RMD/DME Webcast" in the *Portal Server User Guide*. Then, at the configured date and time, the live webcast will stream from the configured RMS/RMD/DME device.

STB

VBrick set top boxes are designed for 24x7 operation. They play live or stored streams on TVs, plasmas, LCDs, projectors and other large format displays. The user-friendly STBs are controlled through an infrared (IR) remote. They can also be used to access live streams or request stored content from VOD servers. VBrick set top boxes can be deployed either as stand-alone devices (with a VBrick encoder) or with the VEMS Portal Server for enhanced functionality. As explained on the following pages, before you can use a set top box, you will need to (1) configure it in VEMS and (2) create a VEMS user for that set top box. VEMS Mystro currently supports the set top box shown in Table 21.

Table 21. Supported Set Top Boxes

Set Top Box	Description
Multi-Format STB	Plays live and stored H.264, Windows Media, MPEG-2, and MPEG-4 streams sourced from VBrick WM or H.264 encoding appliances or from VBrick VOD-W (MPEG), VOD-WM (Windows Media), VOD-D (Darwin), and DME VOD servers.
AmiNET130 STB	Compact set top box manufactured by Amino Systems and reconfigured with a VBrick user interface. It plays live or stored H.264 and MPEG-2 streams. No other streams are selectable for viewing or adding. It does not record streams.

Table 22. VEMS Mystro v6.3 Set Top Box Comparison

	Amino 130	MF STB v1.0	MF STB v2.0	WM IPR †
Minimum Video/Audio Bitrates				
H.264 TS	Any	1.5M/160K	Any	N/A
H.264 RTP	N/A	1.5M/160K	Any	N/A
WM	N/A	1M/128K	Any	Any
MPEG-4 part 2	N/A	1.2M/128K	Any	N/A

	Amino 130	MF STB v1.0	MF STB v2.0	WM IPR †
MPEG2	Any	Any	Any	N/A
Trick Mode (FF/RW, Pause)				
H.264 TS	Y	N	Y	N/A
H.264 RTP	N	N	N	N/A
WM	N/A	N	N	Yes
MPEG-4 part 2	N/A	N	N	N/A
MPEG2	Y	N	Y	N/A
Closed Captioning				
H.264	TS only	N	TS only	N/A
WM	N/A	N	N	N
MPEG-4 part 2	N/A	N	N	N/A
MPEG2	Y	Y	Y	N/A
Composite Video	Y	Y	Y	N
S-Video	Y	Y	Y	N
SD Component Video	Overlay	N	N	N
HD Component Video	Overlay	N	N	N
SD HDMI	Overlay	N	N	N
HD HDMI	Overlay	N	N	N

† Not supported on VEMS Mystro.

Table 23. VEMS Mystro 6.3: STB Functionality by VOD Server and Trick File Functionality

	VOD-W				DME				VOD-WM			
	FF	RW	Pause/Play	Stop	FF	RW	Pause/Play	Stop	FF	RW	Pause/Play	Stop
H.264 RTP	N	N	Y	Yes	N	N	Y	Y	N/A	N/A	N/A	N/A
H.264 TS	Y	Y	Y	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MPEG-4	N	N	Y	Yes	N	N	Y	Y	N/A	N/A	N/A	N/A
MPEG-2	Y	Y	Y	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
WM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N	N	Y	Y

Note For complete details that explain how to configure, manage, and use the set top boxes, see the Multi-Format and AmiNET130 documentation in the online help.

STB Device Administration

STB Administration Q

Select a STB:

	HostName	IP Address	Part Number	Edit	Delete
1.	A172016020171 Amino130 STB	172.16.2.171 Amino130 STB	8000-1555-000X		
2.	AlphaAmino130 Amino130 STB	172.22.2.180 Amino130 STB	8000-1555-000X		
3.	MAC000138ecda18 Multi Format STB	172.22.226.16 Multi Format STB	8000-0188-000X		

Manually Add STB
Auto-Discover STB

Host Name	STB host name.
IP Address	STB IP address.
Part Number	VBrick part number.
Manually Add STB	Lets you manually add a set top box to the VEMS. See below.
Auto-Discover STB	Lets you auto-discover any VBrick set top boxes on your network.

Manually Add STB

STB Device Administration

STB Information

HostName: <input style="width: 95%;" type="text" value="A172016020171"/>	IP Address: <input style="width: 95%;" type="text" value="172.16.2.171"/>
---	--

Model

STB Model:	<input style="width: 95%;" type="text" value="Amino130 STB"/>
Software Revision:	<input style="width: 95%;" type="text" value="V1.2.3"/>
Screen Adjustment%:	<input style="width: 95%;" type="text" value="10"/>
Default Language:	<input style="width: 95%;" type="text" value="EN-US"/>
STB Mode After Schedule:	<input style="width: 95%;" type="text" value="Local Channel Guide"/>

Part Number: 8000-1555-000X

Management

User Name:	<input style="width: 95%;" type="text" value="root"/>
Password:	<input style="width: 95%;" type="password" value="....."/>

VEMS Login

<input type="button" value="Edit"/>	VEMS User: <input style="width: 95%;" type="text" value="-- None --"/>	Please note that each VEMS User can only be associated with one STB. Selecting a VEMS User with a STB already associated will clear the previous STB association.
-------------------------------------	--	---

STB Information	Host Name	Host name of STB.
	IP Address	IP address of STB.

Model	STB Model	Select from dropdown: Multi-Format STB.
	Software Revision	Enter known software revision or leave blank.
	Screen Adjustment	<i>Multi-Format STB only.</i> Range 0–20. Default = 10. You can shrink the display area on a monitor connected to this set top box so that the entire output is shown on the monitor. For example, set to 5 to shrink the display area by 5%. †
	Default Language	Select from the dropdown. Default = EN-US. †
	STB Mode After Schedule	Determines which "start mode" the STB reverts to after a schedule with a STB destination ends. <ul style="list-style-type: none"> Local Channel Guide – The STB gets the channel guide from the local set top box. This is the default when a STB is added via Auto-Discovery. VEMS Mystro Channel Guide – The STB gets the channel guide from the VEMS Mystro Server.
	Part Number	Read-only.
	View Management UI for the device	Launches the password-protected management pages for the set top box.
Management	User Name	Default = <code>iptv</code>
	Password	Default = <code>settopbox</code>
	Allow the Management UI Access in Scheduling?	Default = checked. Provides access to the STB management user interface from the Scheduler pages.
VEMS Login	VEMS User	Click "edit" button and select from list; use paging controls if necessary. This user (with a PIN) must be created in advance (see Adding a VEMS User on page 91). Each configured set top box requires a unique VEMS user. Note that a VEMS user can only be associated with one STB; selecting a VEMS user that is already associated with a STB will clear the previous STB association. Note: Keep in mind that “Client Affinity” will need to be set for the load balancer if a STB is configured to access VEMS Mystro servers via a PIN. VBrick recommends to associate each STB with a VEMS user instead of a PIN if a load balancer is used. See: Load Balancer
Auto-Discovery Check	When manually adding a set top box, use this button to verify the set top box is actually available on the network. For example, if you enter a host name (or IP address), and click Auto-Discovery Check , the IP address (or host name) and other fields will be auto-populated with the correct data if the device is on the network. If not, an error will be displayed.	

Clear	Use to close selection pane after choosing a VEMS Login user.
-------	---

† This is the only way to modify this parameter in VEMS Mistro.

Auto-Discover STB

An auto-discover will automatically find any set top boxes on your network that are not already configured in VEMS. To add STBs to the configuration, simply select the auto-discovered STBs you wish to add and click **Save**. They will be added to the list of configured set top boxes on the STB Administration page.

STB Device Administration				
STB Administration – Auto Discovery				
Select the STBs to add:				
HostName	IP Address	Part Number	Software Revision	Select
1. (none)	172.22.2.90 Multi Format STB	8000-0188-000X	1251.1501.0126.655 1-5814	<input type="checkbox"/>
2. MACe0915309d9b7	172.17.2.102 Multi Format STB	8000-0188-000X	0026.8066_2.0.1	<input type="checkbox"/>
3. MACe0915309d9b8	172.16.2.74 Multi Format STB	8000-0188-000X	0026.8066- 8738_2.1.0	<input type="checkbox"/>
4. MACe0915309d9bb	172.22.2.47 Multi Format STB	8000-0188-000X	0026.8066_2.0.1	<input type="checkbox"/>
5. MACe0915309da60	172.22.2.102 Multi Format STB	8000-0188-000X	0026.8066_2.0.0	<input type="checkbox"/>

Adding a VEMS User

Before you can play streams from a set top box, an STB user must be associated with a VEMS user. When set top box client connects to the VEMS Mistro server to play a stream, the server will re-direct the client to the STB login page for the PIN number of the STB user. You must create this user on the Access Control > [Users](#) page as shown below. A PIN (see below) is typically four numeric characters. In large-scale deployments with numerous set top boxes, creating individual users for each set top box is a time-consuming manual process. If you have a large number of STBs, you can use the **STB Users Utility** to automatically create users and assign them to each STB. See the [2. Add STBs to VEMS](#) on page 248 for more about this. Further, keep in mind that “Client Affinity” will need to be set for the load balancer if a STB is configured to access VEMS Mistro servers via a PIN. VBrick recommends to associate each STB with a VEMS user instead of a PIN if a load balancer is used. See: [Load Balancer](#)

-
- Notes**
- Once you associate a user with a STB, the STB will skip the login page and auto-login to that user account when powered-on.
 - A VEMS user can only be associated with one STB. Selecting a VEMS user that is already associated with a STB will clear the previous STB association.
-

STB Device Administration

STB Information

HostName: <input style="width: 95%;" type="text" value="AlphaAmino130"/>	IP Address: <input style="width: 95%;" type="text" value="172.22.2.180"/>
---	--

Model
 STB Model:

Software Revision: <input style="width: 95%;" type="text" value="V1.2.3"/>	Part Number: 8000-1555-000X
Screen Adjustment%: <input style="width: 95%;" type="text" value="10"/>	
Default Language: <input style="width: 95%;" type="text" value="EN-US"/>	
STB Mode After Schedule: <input style="width: 95%;" type="text" value="Local Channel Guide"/>	

Management
 User Name:
 Password:
 Allow the Management UI Access in Scheduling?

VEMS Login
 VEMS User:

-- None --

1

Admin

andy

ContentAdministrator

ContentPublisher

ContentViewer

Guest

Scheduler

SystemAdministrator

Page: Of 2

Please note that each VEMS User can only be associated with one STB. Selecting a VEMS User with a STB already associated will clear the previous STB association.

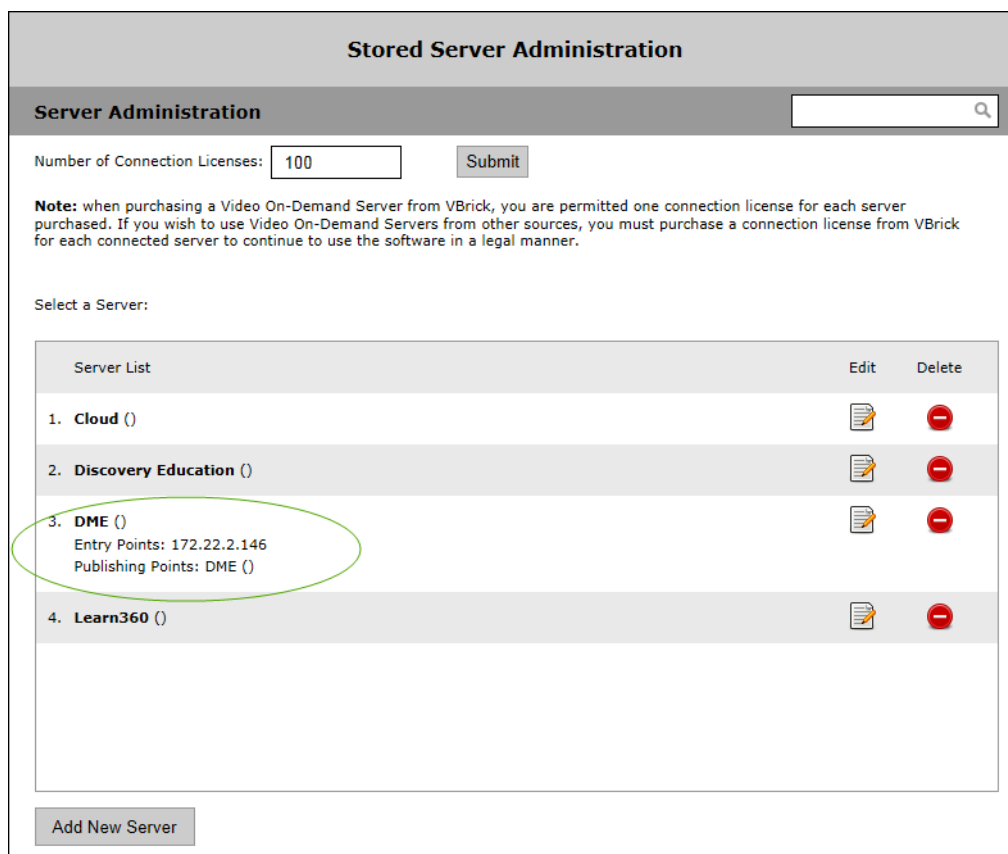
Stored Servers

Use the Stored Server Administration page to add or modify VOD servers, FTP servers, and file servers. Note that you can cluster multiple servers to increase throughput: the VEMS Portal Server will automatically load balance all defined servers; no additional configuration is necessary. Note that content added by users in the Internet zone will only be ingested to VOD and DME servers in the Internet zone for which they have permissions. Content added by users in the LAN zone will be ingested to all VOD and DME servers. See [Supported VEMS VOD Servers](#) on page 8 for a description of all supported servers.

The following window shows an example of the Server Administration page. It shows all currently defined servers. Click on the **Edit** button to drill down into the details (for example IP address and publishing points) associated with the server. The options on the **Server Info** and **Entry Points** pages are basically the same for all servers. The **Server Name** and **IP Address** (or Hostname) are always required. The **Publishing Points** pages are the same for all server types but the required parameters will vary depending on which type of server you select. **On the following pages the required fields for each server type are circled in green.** Refer to the description of each server for the details of each parameter.

VOD-W97

VOD-WM98
 VOD-D102
 VOD-FMS103
 VOD-Wowza104
 File Server-HTTP107
 File Server-FTP110
 Publishing FTP Server110
 DME111
 Cloud114
 Learn360114
 Discovery Education118



<p>Number of Connection Licenses</p>	<p>Required. To add a server, you must enter, or increment, the value in this field. When purchasing a VOD server VBrick, you are permitted one connection license for each purchased server. If you wish to use VOD servers from other sources, you must purchase a connection license from VBrick for each connected server. Enter the total number of purchased licenses and click Submit.</p>
--------------------------------------	---

Add a New Server

Server Information

Stored Server Administration

Server Information

Server Name:

Description:

Timezone:

Ingestion Schedule:

- 1) Select a time range by clicking and dragging areas on the grid.
- 2) Enter a bandwidth limit for the selected time range or choose the No Limit option.
- 3) Click the Apply button.

Bandwidth limit values must be between 10 and 999 or zero (which prevents ingestion).

Ingestion Times (24-hour notation)																								
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Tuesday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Wednesday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Thursday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Friday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Saturday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
Sunday	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞

KBPS Limit
 No Limit (∞)

Server Name	Enter a user-friendly display name for the server.
Description	Use to add descriptive information such as server location.
Timezone	Use the dropdown to select the timezone where the server is located.

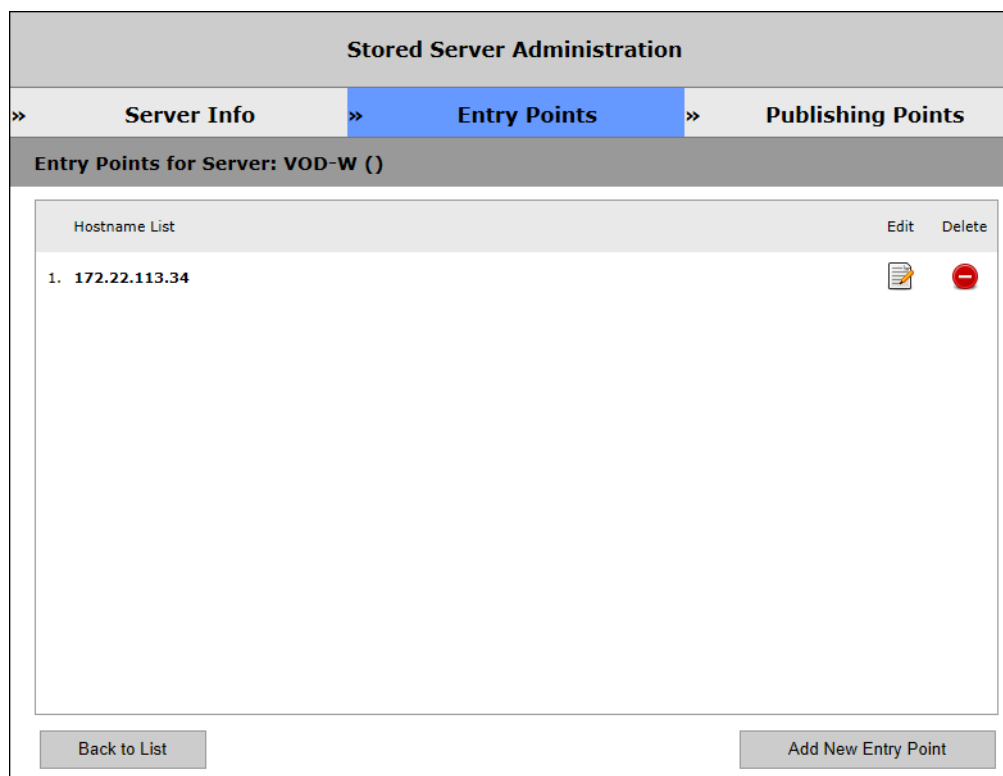
Ingestion Schedule	<p>To minimize the impact of video ingestion on system performance, you can create an "ingestion schedule" so that the FTP bandwidth needed for ingestion is limited (or entirely prevented) during peak viewing hours. This schedule is typically created by a system administrator who is familiar with bandwidth usage and availability.</p> <p>Note that video content added by Portal Server users is not available for viewing until it has been ingested.</p> <p>▼ To create an ingestion schedule:</p> <ol style="list-style-type: none"> 1. Select a time range by clicking and dragging areas on the grid. Use Ctrl-click and Shft-click as desired. 2. Enter a bandwidth limit in KBps for the selected time range. Bandwidth limit values must be in the range 10–999 or zero. 999 sets the bandwidth limit to approx 1 MB; zero completely prevents ingestion; No Limit uses all available bandwidth. 3. Click Apply to view your changes and then Submit to save and add your server. 4. Edit your server from the Stored Server Administration page next to create Entry and Publishing Points.
--------------------	---

Edit a Server

Once a server has been added, click the **Edit** icon from the **Stored Server Administration** page to begin adding specific **Entry** and **Publishing Point** parameters as needed.

Entry Points

Use this page to define your server's IP address. The only time you will have multiple entry points is if you have multiple NICs installed.



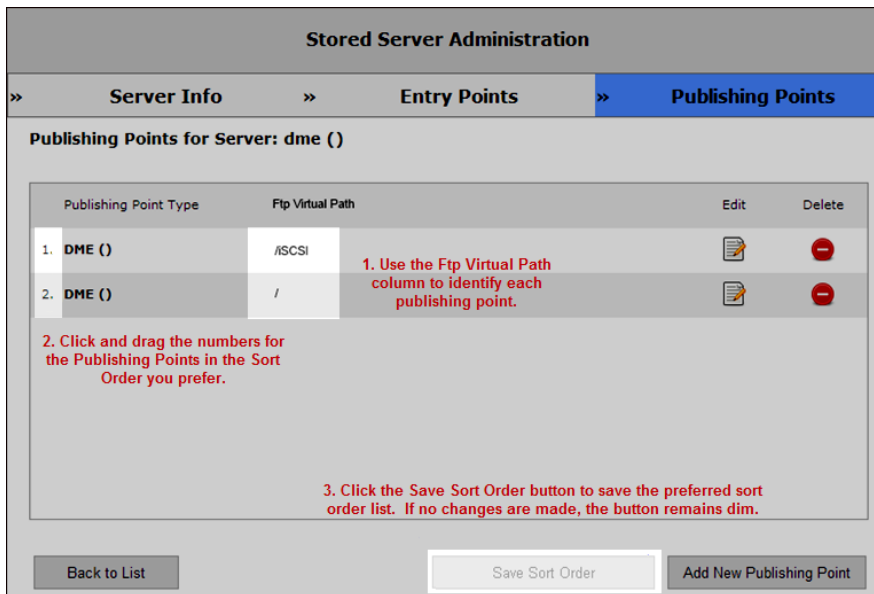
Hostname List	This is the primary IP address or Host Name of the VOD server for LAN users. The Server Name or IP address entered into the VEMS Portal Server must be accessible to Portal Server users.
Add New Entry Point	The only time you will have multiple entry points is if you have multiple NICs installed. A new Hostname or IP Address will be entered.

Publishing Points

The **Publishing Points** page shows options that are available all server types. Click on the **Edit** icon to display this page. As shown in the images on the following pages, the required parameters are different for each server type. The remaining fields will still be displayed but are not used.

Admins are able to arrange the order of the stored server **Publishing Points** if desired by dragging and dropping on the number of the Publishing Point Type of the preferred order from the **Stored Server Administration** page and then clicking the **Save Sort Order** button (this button will remain dim if no changes are made). The file ingestion process will always pick the first publishing point defined. Further, only the first Publishing Point of the same type will be ingested to.

For example, a stored server that has 2 WMSTD Publishing Points and 1 FileServerHttp Publishing Point will only have the first WMSTD Publishing Point and the FileServerHttp Publishing point used. Admins may define which stored server publishing point is selected first for ingestion using this sorting process.



VOD-W

The VOD-W supports H.264 and MPEG-4 streams on VOD-W 5.x (32-bit) or VOD-W 6.x (64-bit) server machines. The required parameters are circled on the following screenshot.

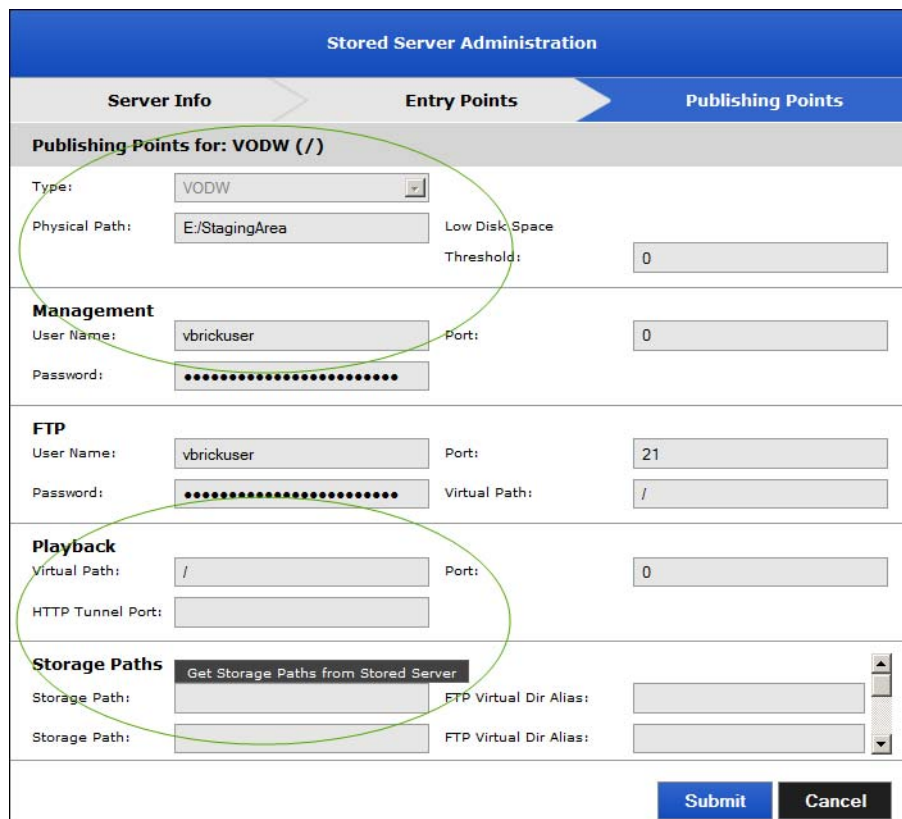


Figure 6. VOD-W (Required Fields)

Publishing Points	Type	Select server type from dropdown. See Table 8 on page 8 for a description of all supported servers.
	Physical Path	Maps the Publishing Directory to the physical location on the VOD server. On the VOD-W this is always <code>E:/StagingArea</code> .
	Low Disk Space Threshold	Reserved for future use.
Management	User Name	Management user name to access the VOD-D server. Default = <code>vbrickuser</code> .
	Password	Management password. Default = <code>vbrickuser</code> .
	Port	Management port. Default = 80.
Playback	Virtual Path	The virtual directory that points to the video for playback.
	HTTP Tunnel Port	VOD-W servers can stream to clients via the HTTP protocol. By default this uses port 8000. 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 <i>must</i> correspond with the port setting on the server. See System Settings > Global Settings > Always Use TCP Protocol for Playback.
	Port	0
Storage Paths	Storage Path	Get this information from the VOD-W server. See 1. Get the Configured Storage Paths From VOD-W on page 116.
	FTP Virtual Dir Alias	Get this information from the VOD-W server. See 2. Add a Virtual Directory for Each Storage Path on page 116.

VOD-WM

The VOD-WM server (Standard and Enterprise) supports .wmv files. The "standard" model supports unicast streams; the "enterprise" model supports unicast and multicast. 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 on the **Stored Video** page.

Figure 7. VOD-WM (Required Fields)

Publishing Points	Type	Select server type from dropdown. See Table 8 on page 8 for a description of all supported servers.
	Physical Path	Maps the Publishing Directory to the physical location on the VOD server.
	Low Disk Space Threshold	Reserved for future use.

Management	WM Enterprise only. *These Management parameters are used when scheduling a Rebroadcast Content on the client application.	
	User Name	Management user name to access the VOD-WM server in the format: <domain_name>\<user_name>. This user must have 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 in the format: <machine_name>\<user_name>. 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.
	Password	Management password. Default = <i>vbrickuser</i> .
	Port	Management port. Default = 80.
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 VOD-D, VOD-WM, and FTP servers is <i>vbrickuser</i> . The default user name for VOD-W servers is <i>anonymous</i> . 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.
	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 <i>vbrickuser</i> . If the FTP Password is changed on the server, it must be changed here as well. Use any combination of alphanumeric and special characters.
	Port	Port that FTP server is running on. Default = 21.
	Virtual Path	Maps the publishing directory to the physical location on the VOD server. The FTP Virtual Path field/column on the Stored Server Administration page is also used to identify Publishing Points (so that they may be sorted for ingestion if desired).

Playback	Virtual Path	The virtual directory that points to the video for playback.
	HTTP Tunnel 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 <i>must</i> correspond with the port setting on the server.
	Port	Port used for playback. Default = 554. If you will be playing back to PC clients, use the default. If you will be playing back to PC clients and Multi-Format Set Top Boxes, use Port 80.

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 [Creating a VOD-WM FTP Server](#) on page 102.
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.
 - 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.

- ▼ 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:

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 Stored Server Administration page.

VOD-D

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 103.) For more about downloading, installing, and configuring a Darwin server, go to <http://developer.apple.com/opensource/server/streaming/index.html>

The screenshot shows the 'Stored Server Administration' interface. At the top, there are three tabs: 'Server Info', 'Entry Points', and 'Publishing Points'. The 'Publishing Points' tab is active, showing 'Publishing Points for: VODD (/)'. The form contains several sections:

- Publishing Points for: VODD (/)**: Includes a 'Type' dropdown menu set to 'VODD', a 'Physical Path' field, and a 'Low Disk Space Threshold' field set to '0'.
- Management**: Includes 'User Name' (vbrickuser), 'Port' (0), and a 'Password' field with masked characters.
- FTP**: Includes 'User Name' (vbrickuser), 'Port' (21), 'Password' (masked), and 'Virtual Path' (/).
- Playback**: Includes 'Virtual Path' (/), 'Port' (0), and 'HTTP Tunnel Port' (0).

At the bottom right, there are 'Submit' and 'Cancel' buttons. A green circle highlights the 'Type' dropdown and the 'Physical Path' field in the first section, and another green circle highlights the 'User Name', 'Password', 'Virtual Path', and 'HTTP Tunnel Port' fields in the 'FTP' and 'Playback' sections.

Figure 8. VOD-D (Required Fields)

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.

- ▼ 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 Publishing Points page.

VOD-FMS

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, multi-user 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 [VOD-Wowza](#) on page 104.

The screenshot shows the 'Stored Server Administration' interface with three tabs: 'Server Info', 'Entry Points', and 'Publishing Points'. The 'Publishing Points' tab is active, showing configuration for 'Publishing Points for: VODFMS (-/VOD)'. The form is divided into several sections:

- Publishing Points for: VODFMS (-/VOD)**: Contains a 'Type' dropdown menu set to 'VODFMS', a 'Physical Path' text box, and a 'Low Disk Space Threshold' text box set to '0'.
- Management**: Contains 'User Name' (vbrickuser), 'Password' (masked with dots), and 'Port' (0).
- FTP**: Contains 'User Name' (vbrickuser), 'Password' (masked with dots), 'Port' (21), and 'Virtual Path' (/FMS).
- Playback**: Contains 'Virtual Path' (/VOD) and 'Port' (1935).

At the bottom right, there are 'Submit' and 'Cancel' buttons. A green circle highlights the 'Type' dropdown and the 'Physical Path' field in the Publishing Points section.

Figure 9. VOD-FMS (Required Fields)

VOD-Wowza

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 105 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. See [Stored Entered URLs](#) on page 46.
- Live VOD streams – can be added by configuring a live stream URL (see [Live Entered URLs](#) on page 43) 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.

The screenshot shows the 'Stored Server Administration' interface with the 'Publishing Points' tab selected. The configuration is for a publishing point named 'VODWOWZA (/VOD) ()'. The 'Type' is set to 'VODWOWZA'. The 'Physical Path' is empty, and the 'Low Disk Space Threshold' is set to 0. Under 'Management', the 'User Name' is 'vbrickuser' and the 'Port' is 0. The 'Password' field is masked with dots. Under 'FTP', the 'User Name' is 'vbrickuser', the 'Port' is 21, and the 'Virtual Path' is '/'. Under 'Playback', the 'Virtual Path' is '/VOD' and the 'Port' is 1935. There are 'Submit' and 'Cancel' buttons at the bottom right.

Figure 10. VOD-Wowza (Required Fields)

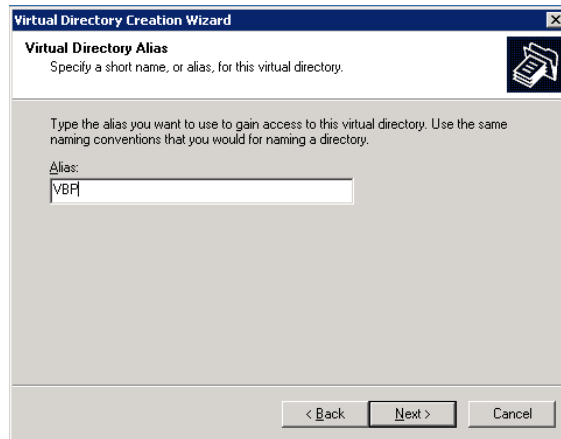
Playback	Virtual Path	The application name (default = vod) on the Wowza server where content will be accessed and managed by the VEMS Portal Server. The content path is C:\Program Files\Wowza Media Systems\Wowza Media Server 2\applications\vod
	Port	Default = 1935 for all protocols. The same port will be used for all Wowza "applications" added to VEMS.

Creating a Wowza FTP Server

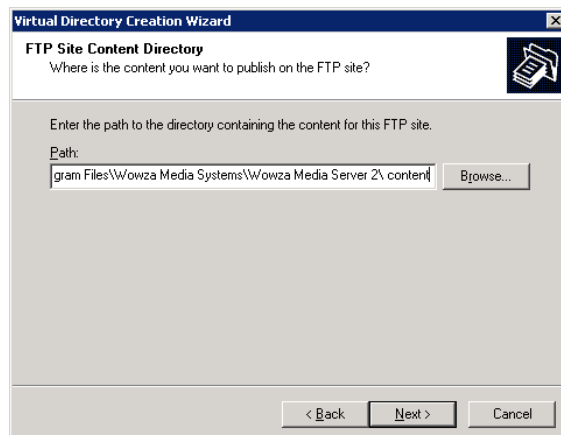
To get started go to the [Wowza](#) website, download the Wowza Media Server application and sign up and obtain a development license. Before you run the Wowza installer you will also need to install the [Java](#) JRE and JDK on the server machine if not already present. When creating a Wowza server 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. 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 2008.

- ▼ To set up an FTP server:
 1. Enable the FTP Service (if not already enabled):
 - a. Go to **Start > Control Panel > Administrative Tools > Server Manager**.
 - b. Expand **Roles**.

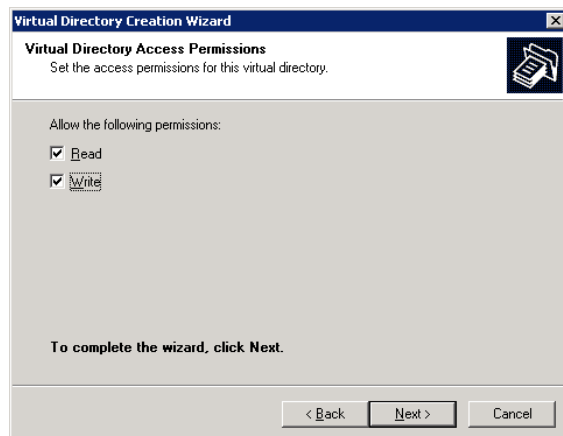
- c. If **Web Server (IIS)** is present you are done.
 - d. If **Web Server (IIS)** is not present click **Add Roles > Server Roles**.
 - e. Check the **Web Server (IIS)** box and click **Install**.
 - f. Then complete the wizard and exit.
2. Optional. Configure FTP Server Security. This optional step disables anonymous connections so that only authenticated users can access the server.
 - a. Go to **Start > Administrative Tools > IIS 6.3 Manager**.
 - 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**.

File Server-HTTP

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 [VBricks \(Encoders\)](#) on page 120 for more about progressive download.)

The screenshot shows the 'Stored Server Administration' interface with the 'Publishing Points' tab selected. The configuration is for a 'File Server-HTTP' publishing point. The 'Type' is set to 'FileServerHTTP'. The 'Physical Path' is empty, and the 'Low Disk Space Threshold' is set to 0. Under the 'Management' section, the 'User Name' is 'd:\inetpub\ftproot' and the 'Port' is 0. The 'Password' field is empty. Under the 'FTP' section, the 'User Name' is 'administrator', the 'Port' is 21, and the 'Virtual Path' is '/'. The 'Password' field is masked with dots. Under the 'Playback' section, the 'Virtual Path' is '/PAD' and the 'Port' is 80. The 'Support HDS' checkbox is checked. 'Submit' and 'Cancel' buttons are at the bottom right.

Figure 11. File Server-HTTP (Required Fields)

Adding MIME Types

By default, Windows Server 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 work around this issue, you will need to add the MIME types for these extensions to IIS on the Windows Server 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**.

The screenshot shows the 'Add MIME Type' dialog box. It has two input fields: 'File name extension:' and 'MIME type:'. Below the fields are 'OK' and 'Cancel' buttons.

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 2003 only)

Extension	MIME Type
.m4a	audio/mp4
.ts	video/MP2T
.m3u8	application/x-mpegURL

FTP	User Name	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.
	Password	The valid password of the user specified above.
	Virtual Path	Path to a user-created virtual FTP directory. See File Server-HTTP on page 107 for more information. The FTP Virtual Path field/column on the Stored Server Administration page is also used to identify Publishing Points (so that they may be sorted for ingestion if desired).
Playback	Virtual Path	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.
	Port	<ul style="list-style-type: none"> • 80 – default port for HTTP playback. • 443 – default port for HTTPS playback. To use Secure Playback, the file server must be configured for SSL. • Support HDS – Use to indicate if the stored server can serve HDS files.

Using HTTP Playback

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.

Using FTP Playback

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 be 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.

File Server-FTP

Use a File Server-FTP to store and play (via progressive download). The files are saved to `ftp:\root`.

Note When configuring an FTP file server, be aware that the user credentials connecting to the server must have read/write permissions at the FTP level and operating system level in order to properly read/write content on the FTP publishing point.

The screenshot displays the 'Stored Server Administration' interface. At the top, there are three tabs: 'Server Info', 'Entry Points', and 'Publishing Points'. The 'Publishing Points' tab is selected, showing a section titled 'Publishing Points for: File Server FTP ()'. Below this, there are several input fields: 'Type' (set to 'FileServerFTP'), 'Physical Path', and 'Low Disk Space Threshold'. A green circle highlights the 'Type' dropdown and the 'Physical Path' field. Below these are sections for 'Management' (with 'User Name' and 'Password' fields) and 'FTP' (with 'User Name', 'Password', and 'Virtual Path' fields). At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 12. File Server-FTP (Required Fields)

Publishing FTP Server

A Publishing FTP Server stores content in repository only. It does not serve (i.e. play) streams. It is typically used to store webcasts and user-initiated recordings.

The screenshot shows the 'Stored Server Administration' interface. At the top, there are three tabs: 'Server Info', 'Entry Points', and 'Publishing Points'. The 'Publishing Points' tab is active, showing a section titled 'Publishing Points for: Publishing FTP Server ()'. This section contains several input fields: 'Type' (a dropdown menu set to 'Publishing FTP Server'), 'Physical Path', and 'Low Disk Space Threshold'. Below this is a 'Management' section with 'User Name' and 'Password' fields. Underneath is an 'FTP' section with 'User Name', 'Password', 'Port', and 'Virtual Path' fields. At the bottom right, there are 'Submit' and 'Cancel' buttons. Two green circles highlight the 'Type' dropdown and the 'FTP' section fields.

Figure 13. Publishing FTP Server (Required Fields)

DME

VBrick's Distributed Media Engine can be used as a VOD server supporting automatic discovery and playback of H.264/MP4, Windows Media, and Flash content. Live content is supported by manually entering the appropriate URLs in the VEMS Mystro system. The DME supports the playback methods listed below with content that now includes HLS and HDS. For more information, please refer to the *DME Admin Guide* at www.vbrick.com/documentation.

Note When configuring a DME, the default parameters are automatically filled in for all fields—except FTP User Name and Password. This means that, if nothing has been changed on the DME, you can simply enter the default VBrick username and password (`admin` and `admin`) in those fields, and then save, and you are done.

- Flash Content – Played back by the Flash Player using RTMP.
- Windows Media – Played back with the Windows Media Player using progressive download (HTTP).
- H.264 Content – Played back with the VBrick player or the Flash player using RTSP or RTMP. (To set playback method, go to Global Settings > Content Configuration.)

Stored Server Administration	
» Server Info	» Entry Points
» Publishing Points	
Publishing Points for: DME ()	
Type:	DME <input type="button" value="v"/>
Caching This DME will cache HTTP HLS/HDS Live Streams: <input type="checkbox"/>	
Management	
User Name:	admin Port: 0
Password:
FTP	
User Name:	admin Port: 21
Password: Virtual Path: /iSCSI
Playback	
HTTP Tunnel Port:	8080
Use RTMPS?:	<input type="checkbox"/>
Progressive Download Playback	
Virtual Path:	/iSCSI <input type="button" value="X"/> Port: 80
Flash Playback	
Virtual Path:	/vod Port: 1935
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Caching	If checked, this DME server will cache HTTP HLS/HDS live streams.	
Caching Source IP's	This DME server will only cache HTTP HLS/HDS live streams from the specified DME source IP addresses. The addresses specified here are configured as "Alternate Sources" on the DME's System Configuration > Caching page. If the DME does not already contain the requested content it will look sequentially through the alternate sources.	
Management	User Name	Used by DME SDK to check the DME version when scheduling a stored broadcast.
	Password	Used by DME SDK to check the ME version when scheduling a stored broadcast.

FTP	User Name	This is the FTP user name that the Portal Server uses when discovering content or publishing content to the server. The default user name for DME servers is <code>admin</code> . 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.
	Password	The FTP password the Portal Server uses when publishing content to the server. The default FTP password for DME servers is <code>admin</code> . If the FTP Password is changed on the server, it must be changed here as well. Use any combination of alphanumeric and special characters.
	Port	Port that FTP server is running on. Default = 21.
	Virtual Path	Maps the publishing directory to the physical location on the VOD server. The FTP Virtual Path field/column on the Stored Server Administration page is also used to identify Publishing Points (so that they may be sorted for ingestion if desired). Note that if using iSCSI storage with a DME, it <i>must</i> start with /iSCSI in this field. Conversely, non-iSCSI storage may <i>not</i> start with /iSCSI. Further, not all DME versions support iSCSI fully. You must be using v.3.1.7e or greater.
Playback	HTTP Tunnel Port	VOD-W, VOD-WM, VOD-D, and DME 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 <i>must</i> correspond with the Ports setting (i.e. HTTP Streaming Tunneling Port) configured on the DME.
Progressive Download Playback	Virtual Path	The virtual directory for playback of progressive download content on the DME. <i>Note, if using an iSCSI Publishing Point, this field should mirror the FTP Virtual Path field.</i>
	Port	The port for the progressive download server on the DME.
Flash Playback	Virtual Path	The virtual directory for playback of Flash content on the DME.
	Port	The port for the Flash server on the DME.

Cloud

Content stored on a "cloud" server is basically available to anyone with an Internet connection and a VBOSS (VBrick Online Streaming Service) account. VBOSS lets anyone deliver professional-quality stored video (live streams not supported) to viewers via the public Internet. It includes a VBrick encoder, a streaming bandwidth package, file storage, personalized pages, and a remote management system. Once you have configured a Cloud server, VEMS will auto-discover any stored content associated with your VBOSS account and make this content available to authenticated VEMS users.

Note Before you can configure and use a "Cloud" server you must have a VBOSS account and VBOSS account credentials. Contact [Support Services](#) to purchase this service or obtain more information.

- ▼ To create a Cloud server:
1. Create a VBOSS account at www.VBrick.com/
 2. In VEMS create a "category" where the videos in your account will be stored.
 - a. Open the VEMS admin interface and go to Content Management > [Category Management](#).
 - b. Click **Add New Category** and create a category for your VBOSS content at the root level.
 3. Configure a Cloud server.
 - a. Complete the Server Info page and skip the Entry Points page.
 - b. On the Publishing Points page, click **Add New Publishing Point** and select **Cloud** from the **Type** dropdown.
 - c. Enter the **Account Credentials** (see screenshot below) you received from VBOSS Support, select the **Root Category** you created above, and click **Submit** when done.
 4. Go to the System Settings > [Task Scheduler](#) page and run the **Verify Online Servers** task to verify your VBOSS credentials for the Cloud server. When the status changes from RunRequest to Ready your VBOSS credentials have been verified.
 5. On the Task Scheduler page, run **Refresh Stored Content** to populate the Root Category on the Portal Server with content discovered from your VBOSS account. This may take up to 15 minutes depending on the amount of discovered content (subsequent refreshes will discover only new content and will not take as long). By default, VEMS refreshes stored server content every two hours. You can "edit" the **Refresh Stored Content** task to run the discovery more or less often.

The screenshot shows the 'Stored Server Administration' interface. At the top, there are three tabs: 'Server Info', 'Entry Points', and 'Publishing Points', with 'Publishing Points' being the active tab. Below the tabs, there is a section titled 'Publishing Points for:'. Under this section, there is a 'Type:' dropdown menu currently set to 'Cloud'. Below that is the 'Account Credentials' section, which includes two input fields: 'Identity Key:' and 'Shared Secret:'. The 'Root Category (discovered content will be assigned to this category)' section has a checked checkbox and a selection of 'My VBOSS Content'. At the bottom right of the form, there are two buttons: 'Submit' and 'Cancel'.

Type	Select the server type Cloud from the dropdown.
Identity Key	Contact VBOSS Support for this information.
Shared Secret	Contact VBOSS Support for this information.
Root Category	Select one new or existing category (i.e. "folder") that will be used for all content associated with your VBOSS account. To create a category, see Category Management on page 39.

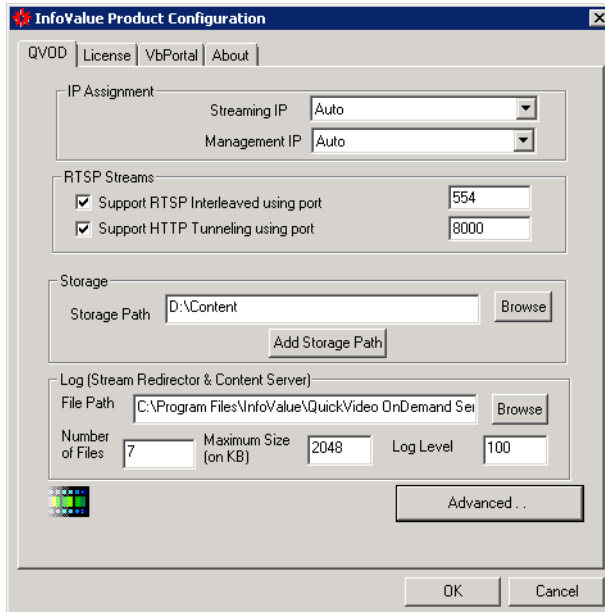
- ▼ To verify discovered VBOSS content on a Cloud server:
 1. Login to Portal Server user interface and go to **All Videos**.
 2. In the navigation tree on the left click on the "root" category you specified above for VBOSS content.
 3. Select any video in the category to playback content from the Cloud server. The video will stream in the player best suited for the content type and your viewing platform (e.g. a desktop, an Android or iOS smartphone, etc.).

Configuring a Cloud Server to Synchronize VOD-W Content

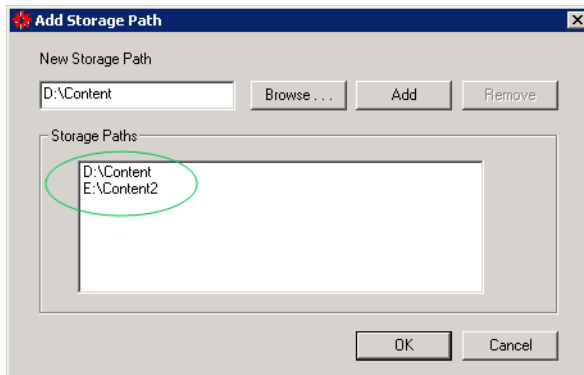
If you will be using the **Request Sync with Cloud** feature to upload content from a VOD-W server to a Cloud server, some additional configuration steps are required on the VEMS Mystro server and on the VOD-W server. This topic assumes the VOD-W has already been configured in VEMS and explains how to setup the required virtual directories on the FTP site. When a sync is requested from a local VOD-W server to the cloud, the video from the VOD-W server must be FTPed to the cloud. The storage paths and virtual directories must be defined for the VOD-W server in VEMS Mystro using the publishing point (VODW) and the virtual directories physically configured on the VOD-W server. The physical paths on the virtual directories must be the same as the **Storage Paths** configured on the VOD-W server.

1. Get the Configured Storage Paths From VOD-W

1. On the VOD-W server machine, go to **Start > Control Panel > InfoValue QuickVideo** and click on the **Add Storage Path** button.



2. When the Add Storage Path page is displayed, make a note of the Storage Paths shown in the box.

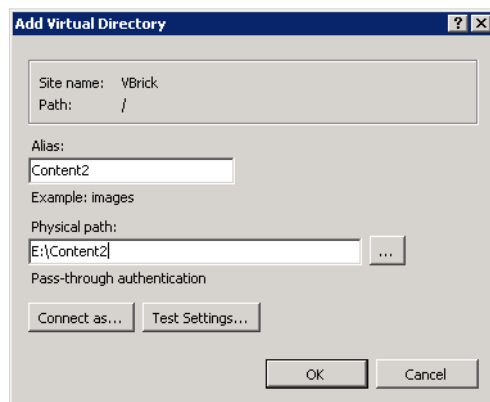


2. Add a Virtual Directory for Each Storage Path

Note The following procedure explains how to add virtual directories on a 64-bit machine configured with Windows Server 2008 R2 Standard software. If you are using a different version of the server software, the screens will be slightly different but the procedure is basically the same.

1. On the VOD-W server machine, perform the following steps for each storage path noted above.
2. See note above. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
3. Expand the tree and expand **Sites**.
4. Right-click on **VBrick** and select **Add Virtual Directory**.

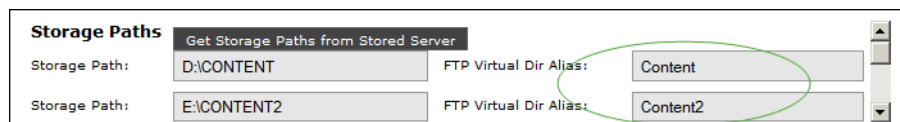
5. Click **Next** on the wizard. When the Virtual Directory Alias page is displayed:
 - a. In the **Alias** field, enter the Storage Path name noted above.
 - b. In the **Physical path** field, enter (or browse) to the Storage Path. (The FTP account (i.e. vbrickuser) must have read permission to this physical path. If you change the VOD-W FTP user name in VEMS, you will need to verify that your new user has read access to the Storage Paths.)



6. Click **OK** when done.
7. Repeat these steps for each defined Storage Path.

3. Configure the Storage Paths in VEMS

1. Launch the Portal Server admin interface and go to **Devices > Stored Servers**.
2. Edit the **VOD-W** server you wish to configure and click on the **Publishing Points** page.
3. Edit the Publishing Point and enter the Virtual Directory Alias you defined above in the **FTP Virtual Directory Alias** field.



4. This completes the Cloud server synchronization procedure. VEMS end users will now be able to seamlessly upload content from a VOD-W server to a Cloud server using the **Request Sync with Cloud** functionality on the metadata **Instances** tab on the user interface.

Learn360

Learn 360 is an educational content provider that provides K-12 multimedia educational resources. VEMS Mystro integrates with Learn360 content by importing Learn360 video content available in the cloud for playback from VEMS. Learn360 provides stored content only—no live content. Since Learn360 files and playback is via the Internet, an Internet connection is required. Learn360 and VEMS integration is playback only. VEMS does not ingest or publish to Learn360.

▼ To configure a Learn360 server:

1. Complete the Server Info page and skip the Entry Points page (the entry point will be auto-populated with Learn360.net).
2. On the Publishing Points page, click **Add New Publishing Point** and select **Learn360** from the **Type** dropdown.

- Enter the **Account Credentials** (see screenshot below) you received from your Learn360 account representative and click **Submit**.

Stored Server Administration

» **Server Info**
» **Entry Points**
» **Publishing Points**

Publishing Points for: Learn360 ()

Type:

Account Credentials

Client Key:

Type	Select server type Learn360 from the dropdown.
Account Credentials	In order to use a Learn360 server to discover and playback Learn360 content, you will need: (1) a license purchased from VBrick, and (2) a Client Key obtained from Learn360. Before running a discovery, the system will validate the Account Credentials and the discovery will fail with an invalid Client Key . Contact your Learn360 account representative for this information.

- On the Task Scheduler page, run **Refresh Stored Content** to populate the Stored Video pages with Learn360 content. This may take up to 15 minutes depending on the amount of discovered content. By default, VEMS refreshes stored server content every two hours. You can "edit" the **Refresh Stored Content** task to run the discovery more or less often. After a successful discovery, the system will import up to 5000 Learn360 videos that are automatically assigned to categories. A description and keywords may also be generated.

Learn360 Playback



Learn360 content is always displayed with a special "watermarked" thumbnail like the one shown here. Learn360 content can be "Featured," "Favorited," "Required," or "Recommended" just like any other content and will be displayed on the appropriate **Home** or **My Videos** pages. Learn360 content cannot be added to playlists nor can you generate clips from Learn360 content. The player used to playback content is delivered over the Internet from Learn360. For this reason the controls and appearance are slightly different and VEMS has no control over the player or the controls. All Learn360 content plays back as Flash on PC and Mac devices only, in any browser. Learn360 content does not play on set top boxes or iOS devices.

Note Internet Explorer users must enable third-party cookies in order to playback Learn360 content. To enable third-party cookies in Internet Explorer go to Tools > Internet Options > Privacy > Advanced > Accept Third-party Cookies.

Discovery Education

Discovery Education is an educational content provider that provides K-12 multimedia educational resources. VEMS Mystro integrates with Discovery Education content by

importing the video content available in the cloud for playback from VEMS. Discovery Education provides stored content only—no live content. Discovery Education files require an Internet connection for playback. Discovery Education and VEMS integration is playback only. VEMS does not ingest or publish to Discovery Education.

Note Before configuring a Discovery Education server, you should enable your **Discovery Education Base URL** where you may house your own server if desired. You may obtain this information from VBrick Support Services or from your Discovery Education Account Representative. If you do not enable this URL, the default Base URL will be used. View the [Global Settings](#) section of the [System Settings](#) topic for more information.

▼ To configure a Discovery Education server:

1. Complete the Server Info page and skip the Entry Points page (the entry point will be auto-populated with DiscoveryEducation.net).
2. On the Publishing Points page, click **Add New Publishing Point** and select **Discovery Education** from the **Type** dropdown.
3. Enter the **Metadata Import Path** that points to the content metadata and click **Submit**.

The screenshot shows the 'Stored Server Administration' interface. At the top, there are three tabs: 'Server Info', 'Entry Points', and 'Publishing Points', with 'Publishing Points' being the active tab. Below the tabs, the section is titled 'Publishing Points for: DiscoveryEducation ()'. There are two main fields: 'Type' with a dropdown menu set to 'DiscoveryEducation', and 'Metadata Import Path' with a text input field containing 'C:\Program Files (x86)\VBrick\Madu'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Type	Select server type DiscoveryEducation from the dropdown.
Metadata Import Path	Path that points to the Discovery Education content metadata.

4. On the Task Scheduler page, run **Refresh Stored Content** to populate the Stored Video pages with Discovery Education content. The first time this process is run, depending on the amount of discovered content, times may vary for content to finish populating. By default, VEMS refreshes stored server content every two hours. You can "edit" the **Refresh Stored Content** task to run the discovery more or less often.

Discovery Education Playback













Discovery Education content is always displayed with a special "watermarked" thumbnail. Discovery Education content can be "Featured," "Favorited," "Required," or "Recommended" just like any other content and will be displayed on the appropriate **Home** or **My Videos** pages. Discovery Education content cannot be added to playlists nor can you generate clips from Discovery Education content. The player used to playback content is delivered over the Internet from Discovery Education. For this reason the controls and appearance are slightly different and VEMS has no control over the player or the controls. All

Discovery Education content plays back as Flash on PC and Mac devices only, in any browser. Discovery Education content does not play on set top boxes or iOS devices.

Note Internet Explorer users must enable third-party cookies in order to playback Discovery Education content. To enable third-party cookies in Internet Explorer go to Tools > Internet Options > Privacy > Advanced > Accept Third-party Cookies.

VBricks (Encoders)

VBrick configuration is only required if you are using the **Scheduling** feature. All VBrick appliances must be configured in the Portal Server before they can be managed and used for scheduled events (and displayed on the dashboard). Once configured, all VBricks in the system are shown on the following window. SAP (Session Announcement Protocol) announcements are sent to the Portal Server by network-connected VBrick encoders and you can use the **Auto Discover VBricks** feature to find all VBrick encoders that are present on the network but have not been configured for use.

VBrick Device Administration				
VBrick Administration				
Select a VBrick:				
HostName	IP Address	Part Number	Edit	Delete
1. A1-TonyH264	172.22.2.120 SD H.264 encoder in 1RU box	9202-420X-0XXX		
2. Alpha-CD3-WM	172.22.182.202 WM Encoder	919X-42XX-0XXX		
3. Andy-Jarhead2	172.22.2.66 HD H.264 encoder in tall box	9200-421X-0XXX		
4. AndyM-9000	172.17.2.211 HD H.264 9000 Series Encoder, dual channel	931X-1200-0XXX		
5. AndyM-H264-VBSTAR	172.17.2.42 HD H.264 encoder in 1RU box, VBStar	9202-421X-YXXX		
6. ATB-H264	172.22.226.17 HD H.264 encoder in 1RU box	9202-421X-0XXX		

Manually Add VBrick	Manually add an existing VBrick to the system. Use this option if the SAP announcements on the VBrick have been turned off.
Auto Discover VBricks	Auto discover any VBricks present on your network.

Manually Add VBrick

To manually add a VBrick, complete the fields on this page and click **Save**.

VBrick Device Administration	
VBrick Information	
HostName:	IP Address:
<input type="text"/>	<input type="text"/>
Model	
VBrick Model:	<input type="text"/>
Software Revision:	MIB Ver: Part Number:
<input type="text"/>	<input type="text"/>
Management	
User Name:	VAdmin Port:
<input type="text"/>	<input type="text"/>
Password:	<input type="checkbox"/> Allow VAdmin Access in Scheduling?
<input type="text"/>	
<input type="button" value="Back to List"/>	<input type="button" value="Validate Connection"/> <input type="button" value="Auto-Discovery Check"/> <input type="button" value="Save"/> <input type="button" value="Clear"/>

Host Name	Required. Host name of VBrick appliance.
IP Address	Required. IP address of VBrick appliance.
VBrick Model	Select from dropdown box.
Software Revision	Optional. Use View VAdmin for VBrick link to open appropriate management application.
View VAdmin for VBrick	Launches the VBrick management application interface for the devices.
Part Number	Read-only.
Onboard Storage?	Read-only.
User Name	Management user name to access the VBrick. Default = <code>vbrickuser</code> .
Password	Management password. Default = <code>vbrickuser</code> .
Port	Management port. Default = 80.
Allow VAdmin Access in Scheduling?	Check to enable access to the VAdmin management application from the Scheduler module on the client interface.
Validate Connection	Verifies that the login credentials for the VBrick are valid.
Auto-Discover Check	When manually adding a VBrick, use this button to verify the appliance is actually available on the network. For example, if you enter a host name (or IP address), and click Auto-Discovery Check , the IP address (or host name) and other fields will be auto-populated with the correct data if the device is on the network. If not, an error will be displayed.

Auto-Discover VBricks

To auto-discover VBrick, click the auto-discovery button, and select the VBrick(s) you wish to add using the check boxes. This will populate the VBrick Device Administration page with the selected appliances. The next step is to "edit" the VBrick and define the **Slots** and **Viewing URLs**.

VBrick Device Administration

VBrick Administration – Auto Discovery

Select the VBricks to add:

HostName	IP Address	Part Number	Software Revision	Select
1. ScottsWM9	172.22.5.50 WM Dual Encoder, VBStar	919X-43XX-YXXX	104.4.7	<input type="checkbox"/>
2. VEMS-9000	172.22.2.156 HD H.264 9000 Series Encoder, quad channel	931X-1212-0XXX	2.0.0c	<input type="checkbox"/>
3. WenliWM-Self	172.22.2.21 WM Encoder	919X-42XX-0XXX	4.5.0a	<input type="checkbox"/>

Define Slots/Channels

Slot (and Channel) information is used by the Scheduler module. VBrick appliances come with a variety of capabilities and encoding options. As a result, the device characteristics will vary depending on the model you purchase. In some models the encoded streams are associated with physical "slots" on the device; in other models these physical slots will have multiple "channels." In general 6000 Series models have slots; 7000/9000 series models have channels. To define slots or channels, "edit" the VBrick, click on the **Slots** or **Channels** tab, and then "edit" the selected item. The configurable parameters on the slots or channels pages are the same on both pages.

Device	Encoding Format	Contains
9000 Series	H.264 (SD/HD)	multiple slots and channels.
7000 Series	H.264	one channel and no slots.
6000 Series	MPEG-2, MPEG-4, WM	one or two slots and no channels

Slot Configuration (6000 Series)

VBrick 6000 Series appliances may have two "slots" that can be scheduled separately. For example you can have an encoder in one slot and a decoder in the second slot, or you can have an encoder in both slots.

VBrick Device Administration	
VBricks	Slots
Slot for: BLDG-Front-Sales	
Slot Information	
Slot Number:	1
Type:	Encoder
Encoding Type:	WM
Slot Name:	<input type="text" value="BLDG-Front-Sales Slot 1"/>
Storage Location:	<input type="text" value="None"/>
Email Template (Used for Webcasts)	
<input type="text"/>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Slot Number	Read-only.
Slot Type	Read-only.
Encoding Type	Read-only.
Slot Name	Give the slot a user-friendly name that will be used by the Scheduler. Schedules are created at the slot or channel level.
Storage Location	Defines the storage location used by the Scheduler for archiving: None, Internal, or External.
Email Template	This field adds the specified text to an auto-generated e-mail for webcast recipients.

Channel Configuration (7000/9000 Series)

7000/9000 Series devices typically have multiple slots and channels. For example on a 9000 Series VBrick you can have slot 1/channel 1, slot 1/channel 2, and slot 2/channel 1, slot 2/channel 2. Each channel can be scheduled separately and each channel must be configured separately.

VBrick Device Administration	
>> VBricks	Channels >>
Channel for: AndyM-9000	
Channel Information	
Slot Number:	1
Channel Number:	1
Type:	Encoder
Encoding Type:	H264
Channel Name:	<input type="text" value="AndyM-9000 Slot 1 Channel 1"/>
Storage Location:	<input type="text" value="None"/>
Email Template (Used for Webcasts)	
<input type="text"/>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Define Viewing URLs

A viewing URL is used to define the source of a stream. It is not an IP address but rather a fully-qualified URL used when pushing a stream from an encoder to a reflector for scalability. The Viewing URL is published as part of the SAP announcement originating from a VBrick appliance.

VBrick Device Administration		
>>	VBricks	Channels >>
Viewing URLs for: AndyM-9000		
Channel Name:	<input type="text"/>	
URL:	<input type="text"/>	
Source IP:	<input type="text"/>	
Bit Rate:	<input type="text" value="0"/>	
Encoding Type:	<input type="text"/>	
<input type="checkbox"/> Is Multicast URL		
		Submit Cancel

Slot Name	Select a previously defined slot on the source device.
URL	<p>Enter the Viewing URL of the stream (sourced from a presentation device). Typical examples of a viewing URL 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:</p> <ul style="list-style-type: none"> Windows Media – <code>http://www.WM_Server_IP_Address/Publishing_Point</code> H.264 – <code>vbricksys:\\<multicast_url>&port=<port_number>&<source_ip_address></code> <p>Note: If you are using Zones, you may need to add a Source IP address. See Add New Live URL on page 45.</p>
Source IP	Used for Zones logic. If the stream is being reflected, enter the IP address of the reflector.
Bit Rate	Select a bit rate if available.
Encoding Type	Select the encoding type of the source stream, for example an H264 or SilverlightRMS stream coming from an RMS device.
Is Multicast URL	Check box if the source stream is defined as multicast.

Script Devices

A "script device" is a VBrick encoder, a set top box, a camera, a DVD player, etc. that you will subsequently control using a script. Script devices work with scripts and can be used to control devices that are attached to a VBrick encoder via the serial port. In order to use a script, the device (an encoder, set top box, 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 184) 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 pattern.

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 about this option.

▼ To add a Script Device configuration:

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

The screenshot displays the 'Script Devices Administration' interface. At the top, there is a header 'Script Devices Administration' and a sub-header 'Script Devices'. Below the sub-header, there is a text input field labeled 'Select a script device:' and a button labeled 'Script Devices'. The main content area contains a table with the following data:

Device Name	Address	Port	Edit	Delete
1. Yada Yada	172.22.2.2	23434		
2. Sony DVD	172.2.2.2.2.	9999		

2. Click **Script Devices**.

Script Devices Administration

Script Device Information

Device Name:

Address:

Port:

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, click on the **Edit** button.

Device Name	Any user-defined name.
Address	Hard-coded device IP address. This is usually the address of the VBrick encoder or the address of the VBrick encoder 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

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 player directly connected to a VBrick encoder.) Once configured, a special icon on the **All Videos** page indicates you can control the stream using a "virtual" remote control panel as shown in Figure 14 below. VBrick currently supports DVDs from multiple manufacturers as well as the VBrick VBIR infrared remote controller that can be customized for use with a wide variety of "non-supported" devices. See [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 player is rack-mounted in an inaccessible metal enclosure, you *must* use the Portal Server interface or a VBIR.

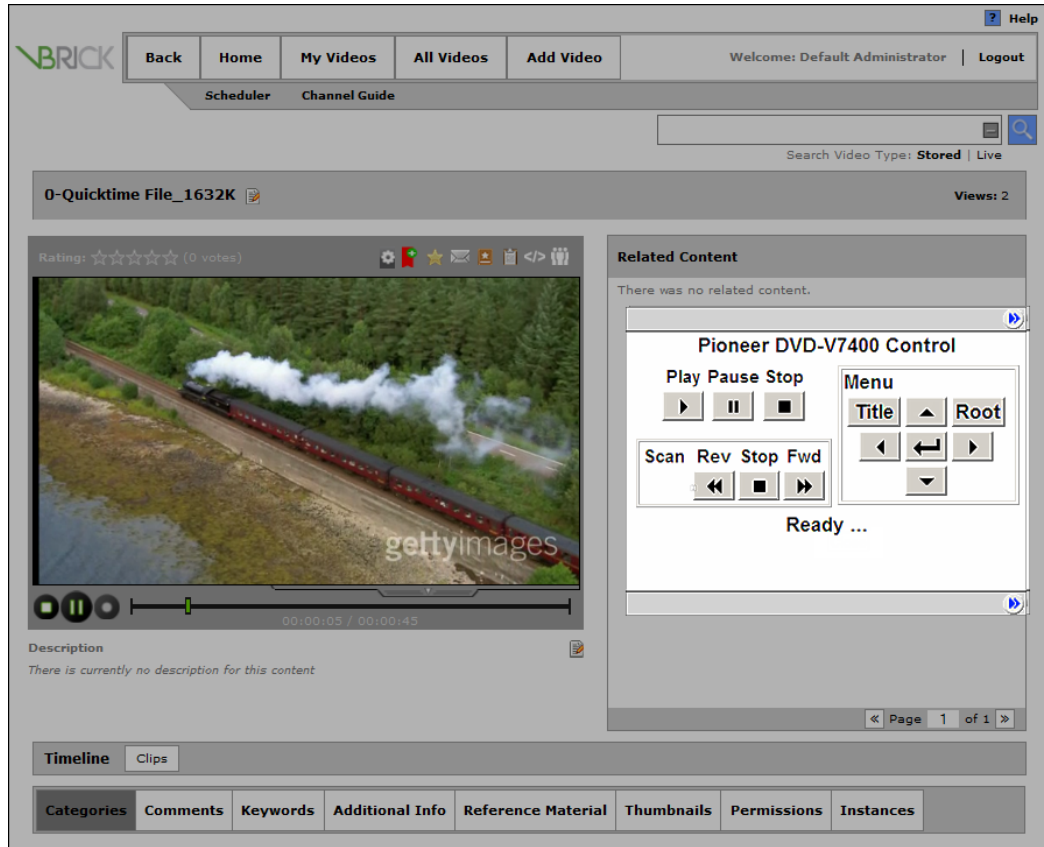


Figure 14. "Virtual" Remote Control Panel on All Videos Page

As shown in Figure 15 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 shown in Figure 16 on page 133).

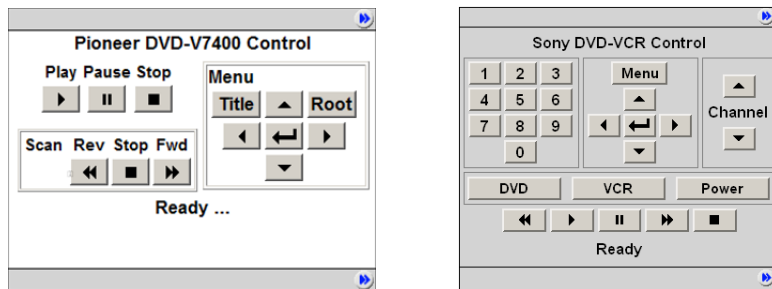



Figure 15. Control Panel for Direct-Connect Devices (left) and VBIR Devices (right)

Note The AmiNET130 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 AmiNET130 set top box.

Add Control Devices

 Use the following pages to define or modify control devices. As noted, these devices will be displayed on the **All Videos** 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 access to the encoder and other permissions. See the "Scheduler" topic 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 **Devices > Control Devices** and select **Add Control Devices**.

Control Devices Administration

Control Devices Administration

Select Control Device :

Name	Device	Source	Live Video Stream Url
1. Andy Control Dev	Panasonic AG-2560c	ControlDev- DualWM Slot 1	 

2. Complete the fields on the next screen as explained below and click **Submit**.

Select Device

Control Devices Administration

Control Device Information

Name :

Device :

Source :

Pioneer DVD-V7400

Panasonic AG-2560c

Panasonic AG-5710

JVC SR-S365U

Panasonic AG-2580 - Spitfire 2

Panasonic AG-2580 - Spitfire 3

JVC SR-V101US - Spitfire 2

JVC SR-V101US - Spitfire 3

Panasonic DVD-RV32 - Spitfire 2

Sony DVP-NSxxP - Spitfire 2

Sony DVP-NSxxP - Spitfire 3

Sony SLV-D380P - Spitfire 3

JVC HR-XVC11B - Spitfire 3

Name	Enter a unique, descriptive name that will be displayed on the virtual remote. For example in Figure 14, "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 (see User Defined VBIRs 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 a live channel from a VBrick encoder.

Select Source

Control Devices Administration

Control Device Information

Name :

Device :

Source :

- ATB-WM-VBStar Slot 1
- BillsVB9000 Slot 1 Channel 1
- BillsVB9000 Slot 1 Channel 2
- BillsVB9000 Slot 2 Channel 1
- BillsVB9000 Slot 2 Channel 2
- BLDG-Front-Sales Slot 1
- BLDG-REAR-MIDDLE Slot 1
- Bobb0007df01073d Channel 1
- Brian-Support-7000 Channel 1
- CD-ZITI-113 Channel 1
- CNBCMrktgDemoPtrl Channel 1
- CNBC-WM Slot 1
- ControlDev-DualWM Slot 2
- EternalDual1 Slot 1 Channel 1
- EternalDual1 Slot 1 Channel 2**
- EternalH264 Channel 1
- JamesR-107a1 Slot 1 Channel 1
- JamesR-107a1 Slot 1 Channel 2
- JoeM-Rhino Slot 1 Channel 1
- JoeM-Rhino Slot 1 Channel 2

User Defined VBIRs

The VBrick VBIR is an external (SpitFire) hardware device from [Innotech Systems](#) that uses the passthrough port on a VBrick encoder to send control commands *via an infrared link* to third-party devices like DVD players that have an IR sensor. **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.** Figure 17 on page 134 provides a high-level view of how these devices are connected. 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 (2 or 3) you have. When done, the new device is added to the **User Defined VBIRs** list as well as to the **Source Device** dropdown list. The following links will provide a list of VCR/ DVD device codes for SpitFire II and III models. Be aware that the device codes in these documents 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.

[SpitFire II DeviceCodes.pdf](#)

[SpitFire III DeviceCodes.pdf](#)

User Defined VBIRs Administration

User Defined VBIRs Administration

Select VBIR :

Name			
1.	Panasonic AG-2580 Spitfire 2		
2.	Panasonic AG-2580 Spitfire 3		
3.	JVC SR-V101US Spitfire 2		
4.	JVC SR-V101US Spitfire 3		
5.	Panasonic DVD-RV32 Spitfire 2		
6.	Sony DVP-NSxxP Spitfire 2		
7.	Sony DVP-NSxxP Spitfire 3		
8.	Sony SLV-D380P Spitfire 3		
9.	JVC HR-XVC11B Spitfire 3		
10.	Test Spitfire 2		

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 [Updating the VBIR Command Set](#) on page 135 for details.

User Defined VBIRs Administration

VBIR Information

Name : Code :

Spitfire 2
 Spitfire 3

AUX1 : <input style="width: 80px;" type="text"/>	FNC1 : <input style="width: 80px;" type="text"/>	CMD1 : <input style="width: 80px;" type="text"/>
AUX2 : <input style="width: 80px;" type="text"/>	FNC2 : <input style="width: 80px;" type="text"/>	CMD2 : <input style="width: 80px;" type="text"/>
AUX3 : <input style="width: 80px;" type="text"/>	FNC3 : <input style="width: 80px;" type="text"/>	CMD3 : <input style="width: 80px;" type="text"/>

Modifying the Control Panel

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 16 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 16.

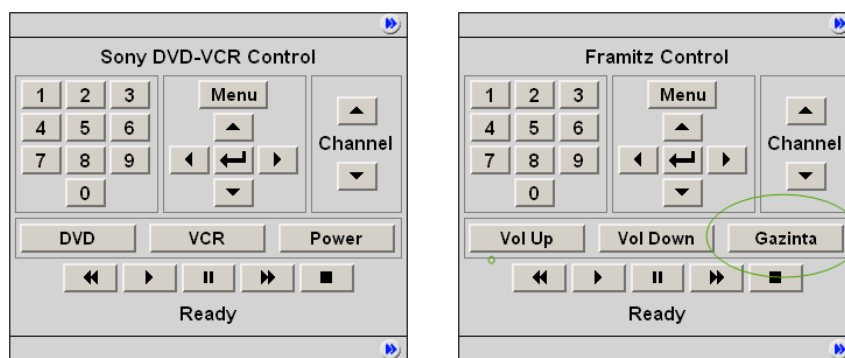


Figure 16. Modifying the SpitFire III Control Panel

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" (see above right) 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 encoder. The buttons will map properly and correctly perform the defined functions.

Connecting 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 24) 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 17) 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.

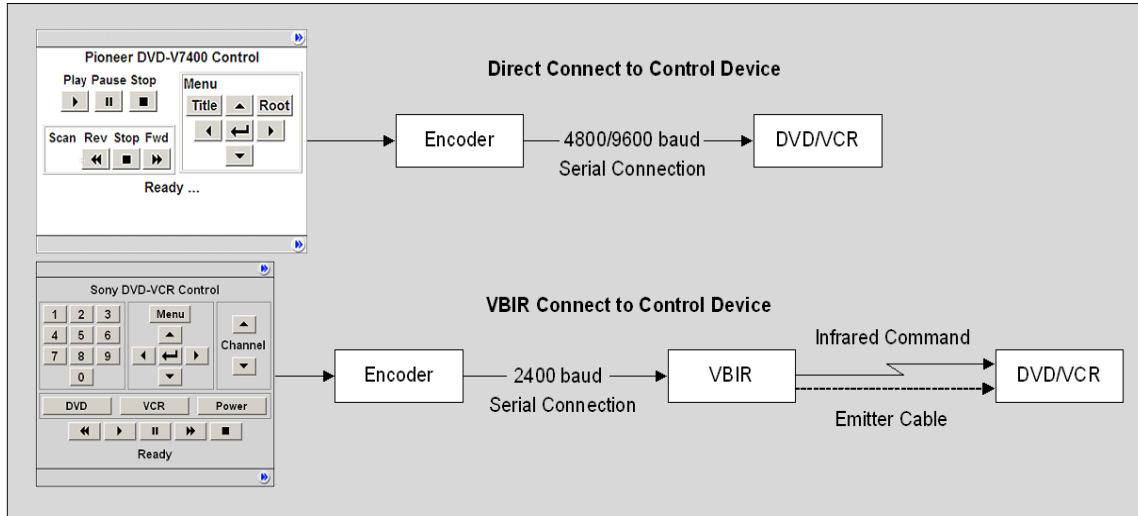


Figure 17. Connecting Control Devices

Table 24. Device Connectors

Device	Connector
VCR	DB-9 †
DVD	DB-15 †
Encoder (MPEG-2/4/WM/H.264)	RJ-45

† Typical device connector.

Configuring Control Devices

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

Table 25. Baud Rate and Passthrough State

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

The screenshot shows the VBAAdmin configuration interface for a 9000 Series device (MAC0007df00d9d3). The breadcrumb path is System Configuration -> Advanced Configurations -> Passthrough. The left sidebar contains a Configuration Menu with options like Home, Dashboard, System Configuration, Advanced Configurations, Encoder Configuration, Monitor, and Troubleshoot. The main configuration area for Passthrough includes the following settings:

Choose Passthrough Port	COM2
Passthrough State	Responder
Port	4439
Baud Rate	9600
Stop Bits	1
Parity	None
Com Interface Type	RS232
RTS Control	Automatic
DTR Control	Automatic
Operational State	Disabled

At the bottom of the configuration area, there are buttons for Apply, Revert, Default, Save, and Finish Edit.

Updating 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 (see 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 available slots 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 [Learning IR Commands](#).

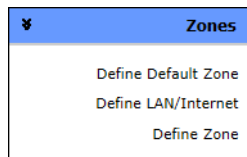
Downloading External Libraries

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 [Downloading External Libraries to the VBIR](#).



Zones

In large multi-site environments, it's always a good idea to locate video sources like servers as close as possible to the client to minimize traffic on the network backbone. The Zones feature helps to minimize traffic congestion by directing clients to a specific server (or a group of servers) within a specified address range. Each Zone associates incoming client IP addresses with one or more server addresses. By using Zones, you can create different named zones with different sets of client and server IP addresses for optimum load-balancing and scalability. In a branch office, for example, you can put the branch VOD server and clients in the same Zone so that all VOD traffic stays local to that office. (Zones also work in conjunction with DMEs to distribute content to edge servers.) You can also use Zones for load-balancing and redundancy by putting two or more VOD servers in the same zone and letting VEMS automatically load-balance the traffic. The VEMS server also periodically polls all VOD servers in the network and will automatically redirect traffic to a failover server if it detects a server failure.



Define Default Zone	138
Define LAN/Internet.....	139
Define Zone	139

Overview

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 [Define LAN/Internet](#) page. This is normal Portal Server behavior. In a Professional or Enterprise configuration, the number of zones available for configuration depends on the licensing model (see Table 26) at your site. You will only be able to configure the number of zones for which you are licensed.

The Zones page directs Portal Server clients (or a range of clients) to *specific* servers (or a range of servers) within the address range(s) specified. It associates each incoming network address with one or more server addresses. When 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)**.

Note IPv6 can adversely impact zone filtering. For Zones to work properly, if your network supports IPv6, it must be disabled on the VEMS server machine. If IPv6 is enabled on the VEMS server machine, it must be disabled on individual client machines. For more information, see the "IPv6 Support" topic in the *Portal Server Release Notes*.

Table 26. Zones Licensing Models

Licensing Model	Zones Available
Standard †	2
Professional	10
Enterprise	100

† A Standard Zones license provides limited flexibility in that you can only define a LAN zone and an Internet zone. In order to leverage the real power of Zones logic, you will need either a Professional or Enterprise license.

Define Default Zone

This page is used to redirect clients to the default zone when the client does not match a defined zone or when there is a server failure. The Portal Server polls all networked VOD servers and if the poll indicates a server failure, the specified Portal Server clients are automatically redirected to the failover server(s).

Define Default Zone

Default Zone Administration

Server/Encoder Addresses

Clients in the Default Zone can access devices located at/within these addresses/address ranges.

Failover Zone

If the default address fails, fallback to addresses defined in this Zone.

Allow Multicast from Failover Zone?

Server/Encoder Addresses	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.
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).
All Multicast from Failover Zone?	Determines whether or not multicasting from the Failover Zone to clients is allowed if multicast content is available.

Note If the Default Zone setting is changed, the administrator must either define a zone that contains all the Application Server IP addresses or add all the servers to the default zone. If this is not done, inter-server communication will fail (e.g. Clear Cache schedule task will fail).

Define LAN/Internet

Use this page to define the range(s) of IP addresses that define the LAN or the Internet domain for the first two zones available at your site. *Both 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. 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. The choices on the page are self explanatory and the first option is the default.

Define LAN/Internet

Define LAN/Internet Address Ranges

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 of the range(s) are in the Internet domain

Specify INTERNET Address Range(s); assume users/servers/VBricks outside of the range(s) are in the LAN domain

Address Ranges (separate each range with a comma):

Define Zone

Use this page to define the zones in your system. When zones are configured, a client selecting a video is algorithmically directed to a load-balanced (Internet or LAN) server. The first two zones are configured on the [Define LAN/Internet](#) page, and the remaining zones are configured here. 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 have a Source IP defined on the Live Entered URLs page if the stream source is not defined in the URL.

Define Zone

Zone Definition

Zone Name:

Zone Type:

Client Addresses:

Server Addresses:

Zone Supports Multicast?:

Failover Zone:

Multicast From Failover Zone?:

Zone Name	User-defined string that identifies the zone.
Zone Type	<ul style="list-style-type: none"> • LAN – Addresses are in the LAN zone. • Internet – Addresses are in the Internet 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 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.
Zone Supports Multicast?	Check to allow multicast from Failover Zone. Default = disabled.
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.

Configuring Zones

Configuration Using Global Assignments

LAN and Internet Zones are defined on the [Define LAN/Internet](#) 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 and 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 always a 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

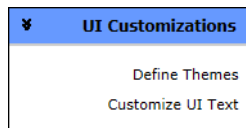
When an encoder IP is defined in a Zone, all enabled SAPs from this encoder are available to the Zone's clients with the exception of the encoder's External SAP. If the External SAP is configured, the URL IP entered in the External SAP will determine what Zone the SAP is directed to. The IP of the External 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 Presentation's video stream. When a manual Live Video Stream URL is used, 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.

Note Use the option **X-Forwarded-For HTTP header to determine the client IP address** in [Global Settings](#).

UI Customizations

VEMS Mystro lets you use themes to customize various text and graphic elements of the user interface so that it matches the look-and-feel of your company or organization. You can also customize any of the text labels on the user interface pages so that the displayed text strings are better suited to your own users or environment.



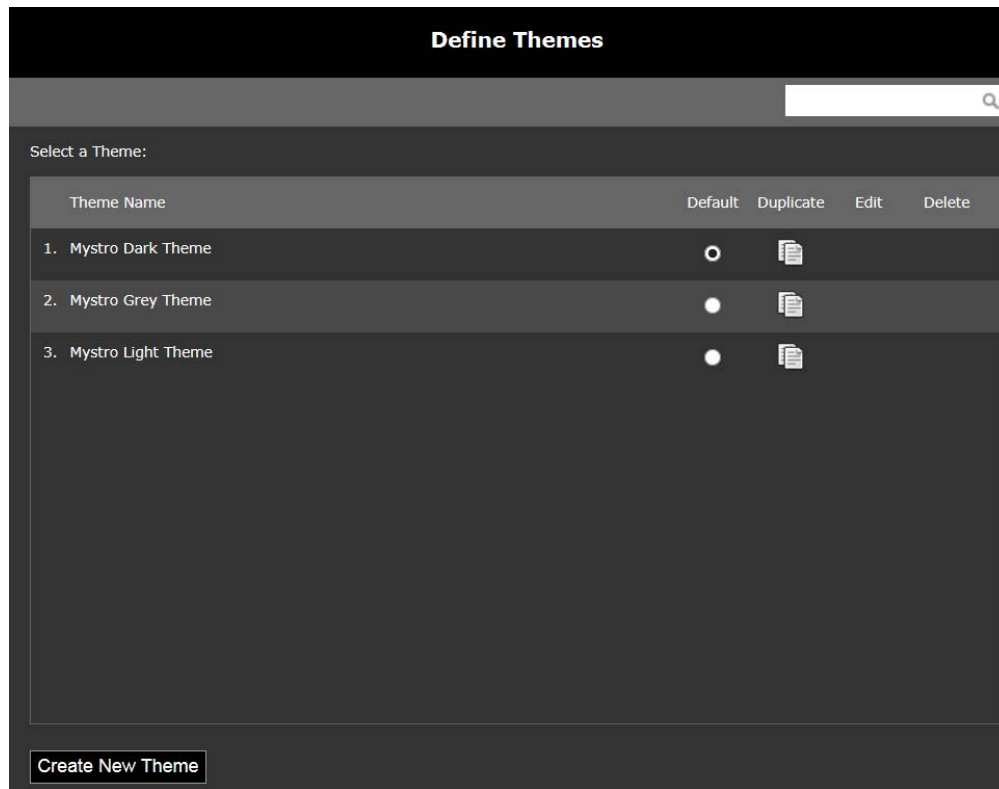
Define Themes	143
Customize UI Text	147
Modifying Existing CSS and JS Files	149

Define Themes

This page shows all "themes" that currently exist in the system. A theme is a complete set of properties that defines the look-and-feel of the user interface and the admin interface. These properties include the base font type, base font size, background color, background image, page element and hover colors, logo image, and the default thumbnail for new videos that do not yet have a thumbnail. A theme consists of a palette of six base colors that are used throughout the application along with other specialized colors and images. A single VEMS Mystro installation can have any number of themes defined and available.

VEMS Mystro is initially configured with three default themes: **Light**, **Dark** and **Grey**. These themes can be set as the active theme (using the **Default** radio button) but cannot be updated or deleted. To create your own theme you will need to duplicate and then modify an existing theme which can then be set as the default theme for the application as well as the embedded player. **Note that the theme you select for the user interface will apply to the admin interface and vice versa.** Each user can then select a preferred theme which is saved in a cookie and will persist across sessions. On the user interface you select a theme using the control at the bottom of every page (see Notes below—this control can be hidden); on the admin interface the theme selection control is on the [Dashboard](#).

-
- Notes**
- The UI Customizations you can perform on these pages are designed for users with no special web design skills. You can basically change the colors, fonts, and logos to customize the look-and-feel of the application. To perform more complex tasks like changing where the various widgets are displayed or hiding buttons, see the Portal Server *Customization Guide*. This guide is written for web designers who are familiar with cascading style sheets (CSS), Javascript, Photoshop, Illustrator, and other tools.
 - The **Theme Override** setting on the System Settings > [Global Settings](#) page determines whether or not users will be allowed to change themes. If disabled everyone will be required to use the same theme.
-



Note The default themes (**Light**, **Dark** and **Grey**) cannot be modified; however they can be duplicated and will become a second instance of the original themes with your added changes. For example, you can change the default logo and thumbnail and retain the rest of the default dark theme. You can also rename the "new" default theme, make it the default, and then delete the old one.

Create New Theme

To create a new theme you start by cloning (i.e. duplicating) an existing theme, giving it a name and description, and then choosing fonts, colors, and other effects. Then use the **Preview Theme** button to get an idea of how your changes will look. When you are happy with the changes click **Submit** and the new theme will be added to the list of available themes on the admin and user interfaces. To see what the theme will actually look like in a production environment you will need to go to the admin or user interface and use the **Change Theme** control to select the new theme.

Note

- For best results use a Font Size of 11 px or less when creating themes. Larger font sizes may not display properly in some parts of the user interface, for example in the Scheduler.
- When entering a hex color where the pair of digits repeats (e.g. 223344), you get the abbreviated color code (e.g. 234) in the field. This is not a bug and does not affect functionality.

Define Themes

Add/Edit Theme

Theme Name:

Description:

Logo Image: Success!
The viewable area for the logo is 100x100 pixels. Your logo will be centered, but not adjusted to fit.

Font Family:

Font Size:

Loading Image:

Thumbnail Image: Success!
Thumbnail images will look best if they are a 13:9 size ratio.

Application Background:

Color:

Or

Images:

Tiled Centered

Colors:

Color 1: Bold text

Color 2: Banner backgrounds

Color 3: Widget backgrounds

Alternate: Alternating row color
Value will be generated based on Color 3. It will look best if it is similar to Color 3

Color 4: Widget borders

Color 5: Standard text

Color 6: Highlight color, link and button hover

Text & Border Effects:

Style 1: Normal: Hover:

Style 2: Normal: Hover:

Style 3: Normal: Hover:

Background Effects:

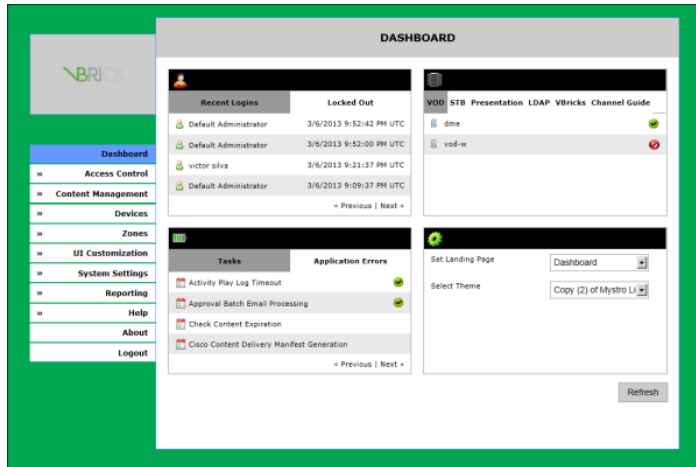
Style 1: Normal: Hover:

Style 2: Normal: Hover:

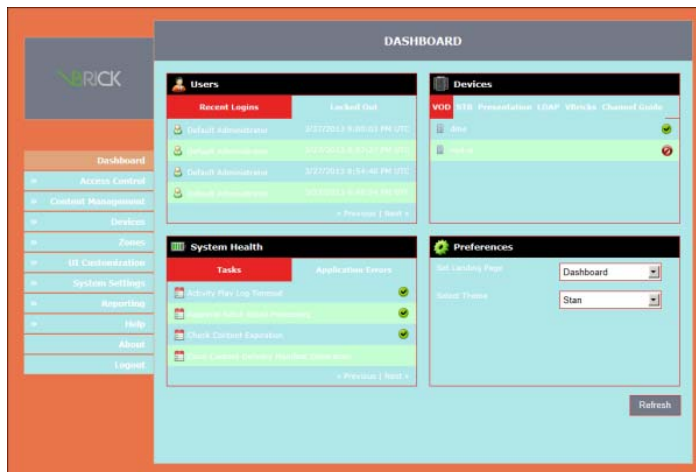
Style 3: Normal: Hover:

Theme Name	This name will display in the list of available themes on the user and admin pages.
Description	Enter a brief, user-friendly description.
Logo Image	Select a logo (or leave blank for no logo). The viewable area for the logo varies depends upon the interface used: <ul style="list-style-type: none"> • PC-based browsers - 100x100 pixels • iPad and Android devices - 30x130 pixels • iPhones - 30x320 • If all devices are being used, the default VBrick logo size is recommended - 95x22.
Font Family	Select one of the following web-safe fonts: Arial, Helvetica, Tahoma, Times Roman, or Verdana . Web-safe colors are also recommended. Non web-safe colors can adversely impact the design of your pages.

Font Size	The text may not display properly in some widgets (e.g. the Scheduler) if the font size is too large. For best results use a font size of 11 or less.
Loading Image	Black or white.
Thumbnail Image	The default thumbnail that will be used for streams on the user interface. Thumbnail images look best with 16:9 aspect ratio.
Application Background	The background can be a color or an image (tiled or centered). This example shows the application page with a green background.

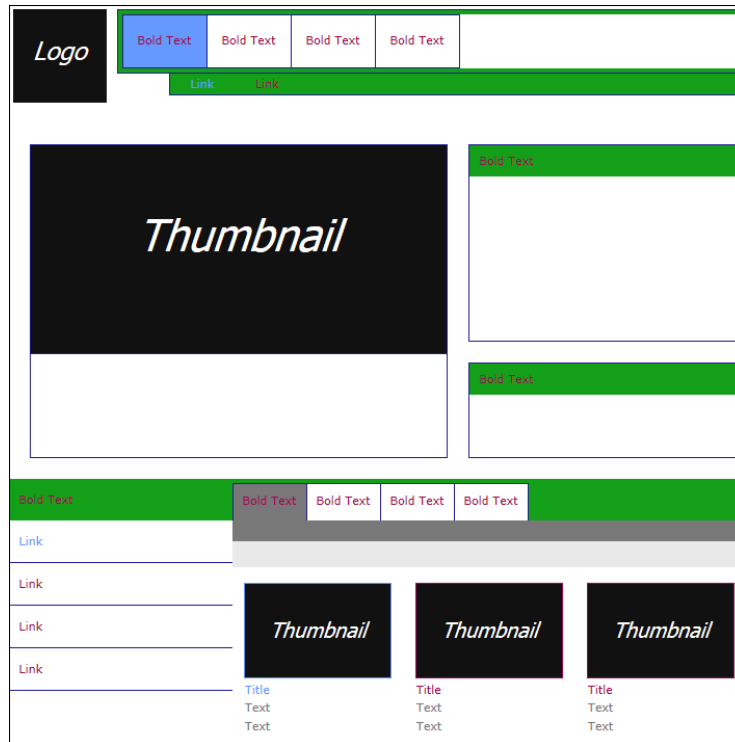


Colors	Use the controls in this pane to define from 1–6 colors named Color 1, Color 2, etc. These are assigned to various page elements (e.g. widget borders) and are also the available colors when you define Text & Border Effects and Background Effects below. This example shows many of the various elements that can be assigned a named color.
--------	--



Text & Border Effects	For best results experiment with different color combinations. The available colors for each Style (e.g. Color 1, Color 2, etc.) are defined in the Colors pane above. Use the Preview Theme button (see below) to get an idea of how the interface will look. Save the theme and actually apply it to the interface to see how it will look in a production environment.
Background Effects	These settings define the background color for text boxes and the hover colors for mouseovers. For best results experiment with different color combinations.

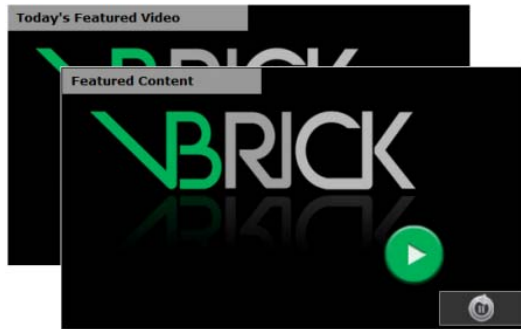
Preview Theme



Customize UI Text

Many features and functions in the user application use "widgets" to perform specific tasks and functions. The Customize UI Text feature lets you change the text label associated with each item in the widget. For example, the `FeatureContentWidget` on the home page has a text label that says **Featured Content** (see below). You can change this label to read **Today's Featured Content** using the Customize UI Text feature. Note that VEMS Mystro currently supports text labels in English, French, and Spanish only.

-
- Notes**
- **This feature only applies to the text labels on the user interface.** The admin interface uses fixed labels for each of the languages in the system.
 - This feature does not set or change the preferred language. You select the preferred language on the [Global Settings](#) page or on the individual user interface pages.
 - All screen text is cached. Users will not see your changes until you run the Clear Cache task in System Settings > Task [Task Scheduler](#). You should also clear the cache in your browser when making changes.
-



Pick the widget containing the text you'd like to change:

Select the name of the on-screen text you'd like to change:

Select the appropriate language:

Edit the text:

Pick the widget to change	Select a widget from the alphabetized list of all widgets.
Select the on-screen text to change	Select the on-screen text to change. The dropdown shows all on-screen text labels associated with the widget you selected above.
Select the language	VEMS Mystro currently supports English, French, or Spanish.
Lookup Current Text	Click to find the current string for the selected on-screen text.
Edit the text	Modify the text as desired. When done run the Clear Cache task in the Task Scheduler and also clear the cache in your browser.

Modifying Existing CSS and JS Files

Cascading Style Sheets (CSS) and JavaScript (JS) files are now minified in VEMS. These CSS and JS files are served to the browser named as `{CSS_FILE_NAME}.min.css` or `{JS_FILE_NAME}.min.js`.

The server contains both the minified and non-minified (original) files. For example, both `admin.min.css` and `admin.css` are included in the server.

If you are customizing or modifying these out of the box CSS and JS files then make the changes to the non-minified version (`admin.css` or `date.js`) and copy them as the minified file names (`admin.min.css`).



System Settings

Global Settings are used to define global options that apply to the entire system. These include the SMTP server name used for e-mail, the login policies designed to deter intruders, and the maximum duration for recorded files. The Task Scheduler lets you run important system tasks, such as purging deleted content, at the interval you specify. You can only run existing tasks; you cannot create new tasks. The Password Complexity feature lets you define, edit, and test the complexity of the passwords used to login to the system. This is an important security feature that, combined with Login Policies, can help to meet stringent security requirements.

System Settings	Global Settings	151
Global Settings	Password Complexity	165
Password Complexity	Player Preference	167
Player Preference	SAP Configuration	169
SAP Configuration	Task Scheduler	170
Task Scheduler	Cisco Content Delivery.	172
Cisco Content Delivery	Transcoding Presets	174
Transcoding Presets	Transcoding Profiles.	180
Transcoding Profiles	Scripts	184
Scripts		

Global Settings

Global Settings that apply to the entire system are listed and explained below. (Note: Due to image size, not all are displayed in the image below)

Note To specify that Internet content will always be played back using the HTTP Tunneling port you must check **Always Use TCP Protocol for Playback** under Content Configuration. This option is disabled by default.

Global Settings	
Content Configuration	
Disassociate unavailable, deleted, or inaccessible content after (Days):	<input type="text" value="30"/>
Always Use TCP Protocol for Playback?:	<input type="checkbox"/>
Default Max. Concurrent Viewers:	<input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
Enable VOD Content Download (Permission Level):	<input type="checkbox"/>
Allow VOD Content Download by Default:	<input type="checkbox"/>
Flash Player Aspect Ratio:	<input type="text" value="Letterbox"/>
Display UserName on Comments Section:	<input type="checkbox"/>
NPAPI Plugins Whitelisted:	<input checked="" type="checkbox"/>
Content Metadata Restriction	
Categories:	<input type="checkbox"/>
Comments:	<input type="checkbox"/>
Keywords:	<input type="checkbox"/>
Reference Material:	<input type="checkbox"/>
Email Configuration	
SMTP Server Name:	<input type="text"/>
SMTP Server User Name:	<input type="text"/> *
SMTP Server Password:	<input type="text"/> *
Enable SSL:	<input type="checkbox"/>
Use Gmail SMTP:	<input type="checkbox"/>
Login Policies	
Login Max Allowed Retries:	<input type="text" value="3"/> *
Login Max Allowed Retry Period (Seconds):	<input type="text" value="120"/> *
Account Lockout Duration (Minutes):	<input type="text" value="30"/>
Login Max Retries Before Freeze:	<input type="text" value="10"/> *

Content Configuration	Disassociate unavailable, deleted, or inaccessible content after (Days):	<p>Number of days to keep:</p> <ul style="list-style-type: none"> • Stored content marked for deletion. • Expired content. • Abandoned or deprecated live instances. • Stored instances that are unavailable (e.g. when a stored server is offline). <p>Note: When <i>all</i> instances of the content are unavailable the title will cease to display in the user content list.</p>
	Always Use TCP Protocol for Playback	If true, stored playback will attempt to use an HTTP protocol using the configured tunnelling port on the publishing point.
	Default Max. Concurrent Viewers	<p>Applied to new live and stored content to limit the number of simultaneous viewers. Default = Unlimited. (You can override this value on an individual content basis using the Permissions tab in Content Metadata.) Does not apply to scheduled broadcasts, presentations, playlists, and clips but is enforced for the individual items making up the playlist or clip. It applies to new content added by one of the following methods:</p> <ul style="list-style-type: none"> • auto-discovered via live SAPs. • discovered by Refresh Stored Content task. • submitted via Add Video. • added via Live/Stored Entered URLs. • that was push-button recorded. • recorded from scheduled events. • recorded and published from live presentations.
	Enable VOD Content Download (Permission Level)	Check to enable VOD content download (from DME servers only) from the "Permissions" tab on the Mystro user interface. Applies to all content types except HLS and HDS.
	Allow VOD Content Download by Default	Check box above <u>and</u> this box to enable VOD content download (from DME servers only) by default for all content. A "download" icon will display in the "community tools" panel above the player window.
	Flash Player Aspect Ratio	<p>Select the aspect ratio of the Flash Player:</p> <ul style="list-style-type: none"> • None • Letterbox • Stretch • Zoom
	Display Username on Comments Section	Check to display Usernames when comments are made on videos.
	NPAPI Plugins Whitelisted	<p>Enabled by default. Google has announced that NPAPI plug-in support (https://sites.google.com/a/chromium.org/dev/developers/npapi-deprecation) will be deprecated. As of January, NPAPI plug-ins must be whitelisted by a company in order to be used. This setting allows you to indicate whether the NPAPI plug-in has been whitelisted for your company. If it has not been whitelisted, VEMS</p>

Content Metadata Restriction	Categories	If checked, users will be required to enter the specified metadata when using Add Video or pushbutton recording.
	Comments	
	Keywords	
	Reference Material	
Email Configuration	SMTP Server Name	Required field. SMTP mail server name used for webcast invitations and content expiration messages. (For an example go to Microsoft Exchange > Tools > E-mail Accounts > E-mail > Microsoft Exchange Server > servername.) 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.
	SMTP Server User Name	
	SMTP Server Password	
	Enable SSL	Enable SSL on the SMTP mail server.
	Port for TLS/STARTTLS	Displayed is SSL enabled.
	Use Gmail SMTP	Use a Gmail SMTP server. Requires a Port for TLS/STARTTLS.
Login Policies	Login Max Allowed Retries	Total number of incorrect logins allowed.
	Login Max Allowed Retry Period	How quickly must LoginMaxAllowed retries occur before we take action.
	Account Lockout Duration	How long to freeze the account if the user exceeds the max incorrect logins within the retry period.
	Login Max Retries Before Freeze	Max number of login attempts before freeze.
Rating Feature	Disable ratings	If checked, the rating by number of stars feature will be hidden on the stored video pages.
Comments Feature	Disable comments	If checked, the comments tab will be hidden on the stored video pages for all video. You may also disable comments for specific videos only on the Permissions tab of each video.

Recording Configuration	Maximum 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.
	Maximum File Ingestions	Specify the maximum number of concurrent ingestion operations that are allowed to a VOD server.
	Delete File After Ingestion	Used push button recording. Specifies whether or not to delete the recorded file from the NVR after ingestion. Enabled by default.
	FTP Staging Area	Specify the staging area folder name for non-infovalue vod servers.
	Purge Completed Requests Interval	The system will purge successful request (record/ftp/ingest) status after the specified number of minutes.
Scheduling Configuration	Minimum Multicast IP Address	Minimum multicast address range used for VOD multicast.
	Maximum Multicast IP Address	Maximum multicast address range used for VOD multicast.
	Last Used Multicast IP Address	Last used multicast address used from allowed range for VOD multicast.
	Minimum Multicast Port:	Minimum multicast port range used for VOD multicast.
	Maximum Multicast Port	Maximum multicast port range used for VOD multicast.
	Last Used Multicast Port	Last used multicast port used from allowed range for VOD multicast.
Server Hostnames	Local Static Hostname	Hostname to be used for external links within the LAN. This is used, among other things, for Sharing and Embed. Use hostname only—not the complete URL.
	Internet Static Hostname	Hostname to be used for external links external to the LAN. This is used, among other things, for Sharing and Embed. Use hostname only—not the complete URL.
Task Service Configuration	Task Service Refresh Interval	Task service will check for updates to task table every n seconds.
User Home Page Configuration	Auto-Generate Related Content	If true, Content without explicitly defined Related Content will instead display all content that shares at least one Category with it. Otherwise, only explicitly defined Related Content will be shown.
	Cycle Featured Content Gallery	If true, the Featured Content will auto-cycle.

Theme Override	Allow Users to Change Themes?	If not checked, the theme selection control on the user interface will not be displayed and everyone will be required to use the same theme.
User Session Configuration	State Timeout	How long to wait before expiring a session
	User Profile Timeout	How long before we destroy the cached user profile that is stored in session state (user profile stores things like the user's permissions, zones, etc.)
VBrick Device Configuration	VBrick Device User Name	Default login user name (default = operator) used for VBrick device when a new VBrick device added to system and the login user name and password were blank.
	VBrick Device Password	Default login password (default = operator) used for VBrick device when a new VBrick device added to system and the login user name and password were blank.
	Search by LDAP Group Cache	Import all LDAP groups into local database and let administrator select those to manage. This option controls how the system discovers LDAP groups for an administrator to manage.
	Include Direct LDAP Groups Only (default)	Enable/disable indirect LDAP group support. In Active Directory, "direct" LDAP groups are those in which a user has been explicitly included; "indirect" LDAP groups are those in which they are included only because of the nested group hierarchy. This option controls how the system behaves during a user login. Customers with large and complex LDAP trees may wish to disable indirect group support for faster sign-on.
Data Purging Configuration	Purge Login History Interval	How often the login records are deleted.
	Purge Content Play History Interval	How often content play records are deleted. This parameter determines how often the items on the "My Recently Viewed" page are cleared.
	Purge Change Log Interval	How often the Change Log is deleted. This log contains records of every update to the database.
	Purge Exception Log Interval	How often the exception log is deleted. This log contains a record of all system errors.
	Purge Content Expiration Log Interval	How often content expiration log records are deleted.

Content Expiration Configuration	Enable Auto Expiration	Check box to enable.
	Content Expires After	If Auto Expiration is enabled, any new content added to the system (via push-button recording, auto-ingest, or Add Video) will auto expire after the specified number of days.
	Expiration Warning Recipient	Valid (semi-colon delimited) e-mail address(es) for the users responsible for managing content expiration. See above: requires a defined SMTP mail server.
	Expiration Warning Period Length	The number of days, before the content expiration date, during which a warning will be displayed.
	Expired Content Purge Delay	The number of days, after the content expiration date, when content will be deleted.

YouTube Configuration	Disable YouTube Integration	This option will enable or disable YouTube Video functionality on the Add Video > Stored Video page. If disabled, no YouTube options will be displayed. Default = enabled.
	YouTube Client ID	A YouTube OAuth 2.0 client ID is entered here so that VEMS is authorized to upload video to YouTube. Documentation for creating an OAuth 2.0 client ID is found on the Google Help site at: Setting up OAuth 2.0 . VEMS specific settings for creating this ID are documented at: Create an OAuth 2.0 Client ID .
	YouTube Public Key	A YouTube public API key is created so that VEMS is authorized to search for video on YouTube that may then be added to VEMS. Documentation for creating a public API key is found on the Google Help site at: API Keys - Public API access . VEMS specific settings when adding this key are documented at: Create a Public API Key .
	YouTube Client Secret	The YouTube Client Secret is generated when the YouTube OAuth 2.0 Client ID is created. See Create an OAuth 2.0 Client ID for specifics. To see a sample ID and Secret, view: VEMS YouTube Configuration .
	YouTube Redirect URI	During creation of the YouTube OAuth 2.0 Client ID, redirect URIs should be entered in the format of //VEMS application domain/oauth2callback. See Create an OAuth 2.0 Client ID for specifics. Keep in mind that Google requires Redirect URIs to end with a public top-level domain (such as .com or .org). If your VEMS domain is private and you do not wish to make VEMS generally available, you should configure a dynamic DNS to redirect to your local IP address and provide the DNS as the redirect URI instead.

Language and Regional Formats	Preferred Language	Controls the language used for labels in both the admin and client interfaces. The selected language overrides the browser language setting. <ul style="list-style-type: none"> no preference – use browser setting. EN US – English U.S. (default). FR CA – French Canada. ES – Spanish.
	Preferred Short Date Format	Select from dropdown.
	Preferred Long Date Format	Select from dropdown.
	Preferred Short Time Format	Select from dropdown.
	Preferred Long Time Format	Select from dropdown.
Content Approval Workflow	Enable Content Approval Workflow	Enable Disable Content Approval Workflow.
	Disable Flag as Inappropriate	Shown when Content Approval Workflow is enabled. When checked, the "Flag as Inappropriate" functionality is disabled and icon will not display on the user interface.
	Approval Email Notifications	<ul style="list-style-type: none"> Off – Default. No Email notification. Individual – Notifies approvers every time a video requiring approval is submitted. Digest – Notifies approvers each time the Approval Batch Email Processing task runs in the Task Scheduler (default = once per day).
	Email "From" Address	The "From" address that will appear in the Email Notifications sent to content approvers. You may want to change this to your own domain name. Default = DONOTREPLY@VBrick.com
	Send a test email	Sends a test email to the specified address. Assumes a valid SMTP mail server is configured. See ""Email Configuration" above.
Digital Signage	Digital Signage Server URL	Enter a valid URL pointing to a Digital Signage Content Manager Server. This will add a Digital Signage link to the navigation bar which you can use to launch the application.
Ingestion Options	Enable Transmux on H.264 Content	Enables ingestion options and adds "hinting" for MP4 and MOV files. Default = Enabled. For H.264 video and AAC audio files, the following transmuxes are enabled: <ul style="list-style-type: none"> MP4 > H264TS, H264TS > MP4 MOV > MP4, MOV > H264TS
	Ingest H.264 Transport Stream and MP4 Files	Ingest <u>both</u> H.264 Transport Stream and MP4 files. Default = On.
	Ingest H.264 Transport Stream Files Only	Ingest <u>only</u> H.264 Transport Stream files.
	Ingest H.264 MP4 Files Only	Ingest <u>only</u> MP4 files.

Transcode	Show Transcoding Profile to User	If checked, the list of available transcode profiles will be displayed for authenticated users on the Add Video page and the Schedule Record page of the user interface. Default = not checked.
LMS	Enable Integration	If checked, Blackboard is integrated with VEMS so that content from VEMS may be sent to specific courses in Blackboard and viewed. View the VEMS Blackboard Integration topic for more details.
	LMS User Name	The user account in Blackboard that is responsible for authenticating incoming video content from VEMS.
	LMS Password	The password for the LMS User Name.
	LMS URL	The URL that will be used to send data to the Blackboard Building Block.
	LMS Custom Field Name - Course ID	Name for the field where users will enter the Blackboard Course ID that they want VEMS content sent to. This is most often titled simply "LMS Course ID".
	LMS Custom Field Name - Send to LMS	Name for the field where users decide to flag if the content should be sent to the LMS Course ID with either a yes or no option. This is most often titled simply "Send to LMS".
	LMS Shared Secret	Unique key used for peer-to-peer authentication; should be the same value as entered for the Web Services Shared Secret during Blackboard Administrative Setup.
MFTSB Upgrade Server Page Configuration	Set Upgrade Server Page URL on MFSTB	Enable the upgrade server page URL for Multi-Format set top boxes. See the <i>Multi-Format STB Quick Start Guide</i> for an explanation of how to use these settings.
	Upgrade Server Page URL	The URL of the upgrade server on the VEMS Mystro server. Default = http://myMFSTBUpgradeServer/STB/MFSTB_Upgrade/UPG/upgrade/upgrade.html
Zones	Use X-Forwarded-For HTTP header to determine client IP address	This is the standard way to identify the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer.

External Identity Token (SharePoint) Configuration	Allow External Identity Token	If true, when a user is accessing VEMS Mystro via an embedded widget in a SharePoint page, an identity token will be created and passed to the VEMS Mystro widget. This eliminates the need for a double login when SSO is enabled on an LDAP server in some multi-domain network configurations.
	External Identity Token Shared Secret	Click button to generate the secret. This secret is needed to validate the authenticity of the identity token generated by the SharePoint web part.
	External Identity Token Expiration	Sets the length of time the identity token is valid. Default = 5 minutes. The server times for SharePoint and VEMS Mystro must be in-sync. If the time the identity token was created by the SharePoint widget is more than the configured "expiration" time, the token will be rejected. Note that the token can be used only once in VEMS Mystro regardless of this setting.
Discovery Education	Discovery Education Base URL	By default, http://app.discoveryeducation.com . You may specify your own URL. Obtain this information from VBrick Support Services or from your Discovery Education Account Representative. If you do not enable this URL, the default Base URL will be used. For more information on configuring the Discovery Education integration, view the Discovery Education section in the Devices topic.
Automatic Component Upgrade	Disable automatic upgrade of components for Chrome/Firefox	When this checkbox is enabled, the VBrick Player will <i>not</i> be automatically upgraded for the Chrome and Firefox browsers when a new player is available. By default, this checkbox is disabled which means that automatic upgrades will occur for Chrome/Firefox, similar to IE.

YouTube Content Delivery Configuration

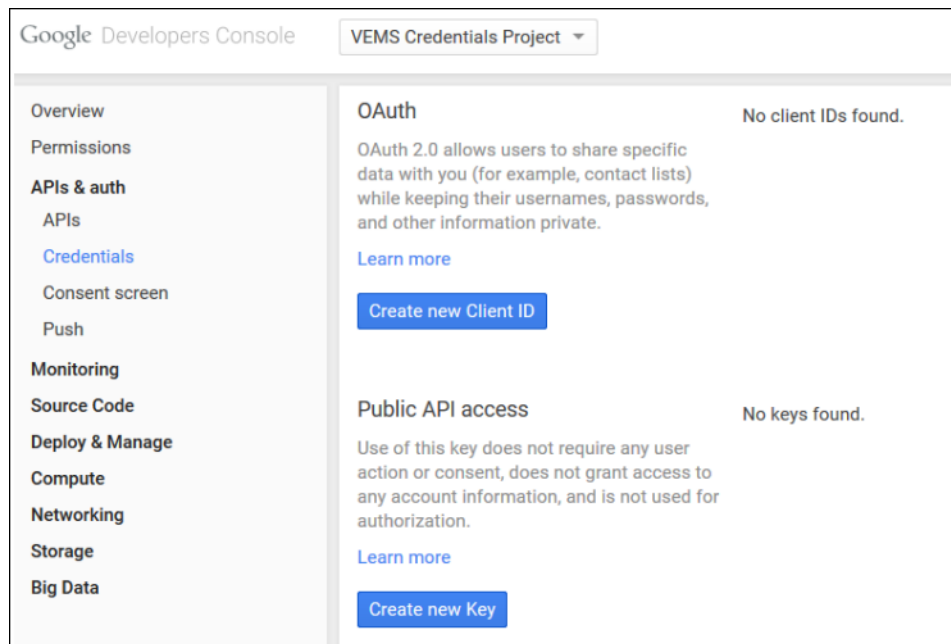
To enable your VEMS application to search for and upload content to YouTube, you must configure Google's YouTube API v3 to work correctly with VEMS.

Note The Google YouTube API v3 has changed as of VEMS v6.3.14. You must reconfigure your VEMS application to be able to search and upload videos to YouTube once you have upgraded to v6.3.14 or VEMS will no longer work with YouTube.

There are three steps to configuring YouTube to work with VEMS:

1. Authorize a Google account for the [Google Developers Center](#) to create and work with the Google API. It is suggested that a VEMS admin Google account be used.
2. Create a new OAuth 2.0 Client ID and Public API key in the Google Developers Console (see image below).

- Enter the OAuth 2.0 Client ID values and Public API key and secret created in the VEMS YouTube Configuration section in System Settings as described above.



Create an OAuth 2.0 Client ID

The OAuth 2.0 client ID is created so that VEMS is authorized to upload video to YouTube. Documentation for creating an OAuth 2.0 client ID is found on the Google Help site at: [Setting up OAuth 2.0](#).

VEMS specific settings are shown in the image below.

- Application Type:** Web application
- Authorized JavaScript origins:** VEMS application domain

- **Authorized redirect URIs:** VEMS application domain/oauth2callback

Note Google requires Redirect URIs to end with a public top-level domain (such as .com or .org). If your VEMS domain is private and you do not wish to make VEMS generally available, you should configure a dynamic DNS to redirect to your local IP address and provide the DNS as the redirect URI instead.

Create a Public API Key

The public API key is created so that VEMS is authorized to search for video on YouTube. Documentation for creating a public API key is found on the Google Help site at: [API Keys - Public API access](#).

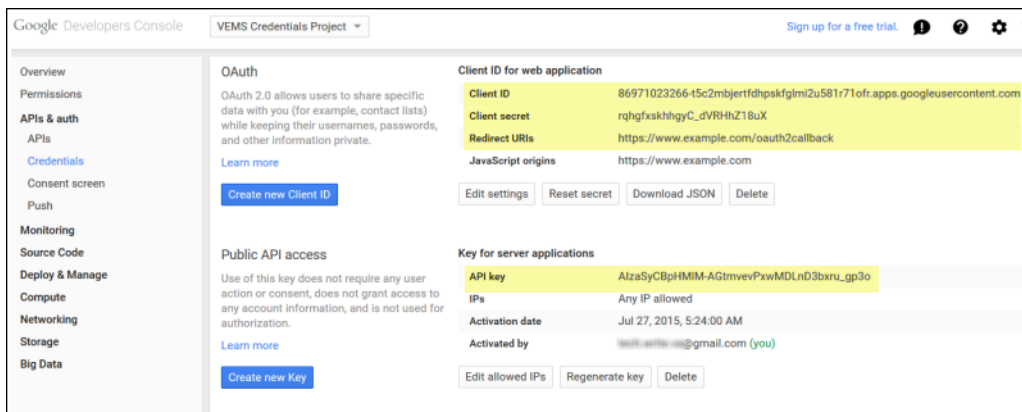
VEMS specific settings are shown in the image below.

The screenshot shows a dialog box titled "Create a server key and configure allowed IPs". It contains the following text: "This key should be kept secret on your server." followed by "Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request's userIp parameter, (if specified). If the userIp parameter is missing, your machine's IP address will be used instead. [Learn more](#)". Below this is a section "Accept requests from these server IP addresses (Optional)" with a subtext "One IP address or subnet per line. Example: 192.168.0.1, 172.16.0.0/12, 2001:db8::1 or 2001:db8::/64" and a note "Or if you leave this blank, requests will be accepted from any address. Be sure to add IP addresses before using this key in production." There is a large empty text input field. At the bottom are "Create" and "Cancel" buttons.

- **Type of Key:** Server (not shown in image above, select Server when prompted)
- **IP addresses:** Left blank. This will allow any IP address to search.

VEMS YouTube Configuration

Once you have your OAuth 2.0 Client ID and Public API key generated, you are ready to configure VEMS. Your Google Developers Console should look similar to the image below. The values you will need to transfer to VEMS are highlighted.



- ▼ To configure VEMS for YouTube:
1. Navigate to Admin > **System Settings** > **Global Settings** > **YouTube Configuration**
 2. From the Google Developers Console, enter the following values in the VEMS fields seen below:
 - a. OAuth 2.0 Client ID (Google field) > YouTube Client ID (VEMS field)
 - b. Public API Access Key (Google field) > YouTube Public Key (VEMS field)
 - c. OAuth 2.0 Client Secret (Google field) > YouTube Client Secret (VEMS field)
 - d. OAuth 2.0 Redirect URIs (Google field) > YouTube Redirect URI (VEMS field)

YouTube Configuration	
Disable YouTube Integration:	<input type="checkbox"/>
YouTube Client ID:	<input type="text" value="OAuth 2.0 Client ID"/>
YouTube Public Key:	<input type="text" value="Public API Key"/>
YouTube Client Secret:	<input type="text" value="OAuth 2.0 Client Secret"/>
YouTube Redirect URI:	<input type="text" value="VEMSAplicationdomain/oauth2callbac"/>

Your VEMS application is now ready to search for and upload video content to YouTube. Users will be prompted for their Google account credentials the first time they attempt to search or upload content.

Password Complexity

This page is used to set the password complexity rule for all user and admin passwords. It has five predefined complexity models. You can use the predefined models or you can create your own. The password complexity model supports regular expressions.

Password Complexity Administration

The current active "Password Complexity Rule" for this site is:

1 Character minimum

Description	Pattern	Use	Test	Edit	Delete
1. 1 Character minimum	(?=.{1,})	<input checked="" type="radio"/>			
2. 8 Character minimum	(?=.{8,})	<input type="radio"/>			
3. 12 Character minimum	(?=.{12,})	<input type="radio"/>			
4. 15 character minimum	(?=.{15,})	<input type="radio"/>			
5. 20 character minimum	(?=.{20,})	<input type="radio"/>			
6. 6 to 25 Characters letter and number	(?!^[0-9]*\$)(?!^[a-zA-Z!@#%&*()_+=<>?]*\$)^(?!^[a-zA-Z!@#%&*()_+=<>?0-9]{6,25}\$)	<input type="radio"/>			
7. 6 character minimum with upper and lower case letters	^(?=.*[a-z])(?=.*[A-Z])(?=.{6,})	<input type="radio"/>			
8. 6 characters minimum with 3 of 4 of the following: Upper, Lower, Digit, Special	^(((?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])) ((?=.*[a-z])(?=.*[A-Z])(?=.*[!@#\$%^&*()_+=<>?])) ((?=.*[a-z])(?=.*[0-9])(?=.*[!@#\$%^&*()_+=<>?])) ((?=.*[A-Z])(?=.*[0-9])(?=.*[!@#\$%^&*()_+=<>?]))){6,25}\$	<input type="radio"/>			

Edit Password

Add/Edit Password Complexity Rule

Description:

Pattern:

Test Password

Password Complexity Tester

Policy:
1 Character minimum

Pattern:
(?=.{1,})

Type a password in the box below and click the Test Pattern button to test this rule:

Player Preference

H.264 and MP4 content will play on a variety of players. The Player Preference feature lets an administrator define which players are used to play back H264/MP4 and Flash content (on either PC or Mac). There is one tab for PC preferences and one tab for Mac preferences. In general, the **VBrick** player will play anything except Flash or QuickTime files. The **Flash** player plays only Flash files; the **QuickTime** player plays only QuickTime files. Each VEMS client desktop will be prompted to download any required components the first time the client launches a stream. (For Flash or QuickTime files, the end user will need to download player components from [Adobe](#) or [Apple](#) respectively.) Thereafter, when a user launches a stream, VEMS will automatically load the correct player in the Preview window (Figure 18).

-
- Notes**
- Note that Windows Media and MPEG-2 content are not affected by Player Preferences.
 - The file types available actually depend on what type of server is hosting the stream (see the "Supported File Types" topic in the *Portal Server Release Notes* for details).
 - For a more detailed discussion of how player preferences work see [Player Preference and Instance Selection](#) on page 243.
 - For YouTube videos to be visible and playable within VEMS Mystro, QuickTime must be set to **Prefer** or **Allow**.
-

Player Preference

Player Preference

H.264/MP4 for PC	H.264/MP4 for MAC
Use the table below to define player preference when displaying H.264 or MP4 content on PC devices	
Player Type	Prefer Allow Deny
Flash	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
VBrick	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
QuickTime	<input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>

- ▼ To set player preferences for H.264/MP4 content:
1. Select the one preferred player (Flash, VBrick, or QuickTime). For each supported player you can choose one of three options (**Prefer**, **Allow**, or **Deny**). One player must be selected as **Prefer** for both PC and Mac (you need not set any others to **Allow**).
 2. For the remaining players select **Allow** or **Deny**.
 - When there is only a **Prefer** player (and no players marked for **Allow**), the system will only use that preferred player to playback H.264/MP4 content.
 - If there are other players set to **Allow** the system will first try to use the **Prefer** player for a given piece of content, but will fall back to the **Allow** player if the content cannot be played by the preferred choice.

Example The QuickTime player is set as **Prefer** and VBrick player set as **Allow**. User selects H264TS content. QuickTime cannot play back H264TS content, therefore the system will deliver the VBrick player to the user.
 3. If there are no **Prefer** or **Allow** players set for a given content type, VEMS will filter out the content so it is not shown on the user interface (and users will not be prompted to download players that have not been authorized).

Example The QuickTime player is set as **Prefer** and no other players are set as **Allow**. H264TS content will be filtered out of the interface since it cannot be played by QuickTime.

Example The Flash player is set as **Deny**. Flash content will be filtered out of the interface since it cannot be played by other players.

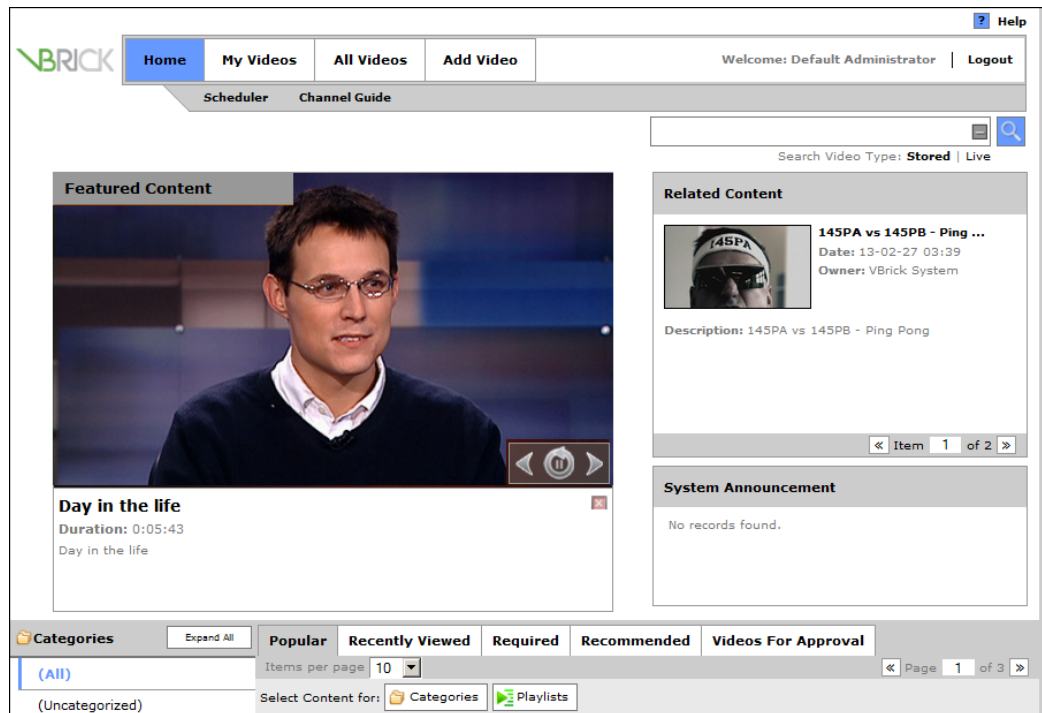


Figure 18. Preview Window

SAP Configuration

SAP (Session Announcement Protocol) announcements are typically emitted by VBrick devices (e.g. encoders, set top boxes, and DME servers). These announcements identify the VBrick devices to various network applications including DHCP, StreamPlayer, and VBDirectory, as well as VEMS. This page is used to identify the addresses (and ports) on which the VBSapSrv component running on the VEMS Mistro server receives announcements. The VBrick devices must be configured with the same announcement address and port number.

Note Any changes made to SAP announcements will not take effect until the VBSAPSRV Service is restarted. When done you will need to restart this service or reboot the server.

SAP Configuration

Management Announce

IP Address Port Edit

RTSP Announce

IP Address Port Edit





















Multicast Announce

IP Address Port Edit

Management Announce	<ul style="list-style-type: none"> • IP Address – changes the Management address on which (SAP) Announcements are received. By default the addresses and ports for all VBrick devices are equivalent to the VEMS defaults on this page. For proper functionality the device addresses and ports must match the settings in VEMS. • Port – VEMS port used to listen for management announcements.
RTSP Announce	Same as above for RTSP announcements.
Multicast Announce	Same as above for Multicast announcements.

Task Scheduler

The Task Scheduler lets you schedule and run various tasks that need to be performed on a regular basis. These tasks include purging deleted content, refreshing the LDAP groups, and others. You can schedule and run existing tasks only. You cannot use the Task Scheduler to create new tasks. Use the **Edit** button to modify a task; use the **Run** button to launch a task.

Task Scheduler						
Current Tasks:						
Name	Status	Last Run	Result	Next Run	Edit	Run
1. Activity Play Log Timeout	Ready	2/27/2013 11:24 AM	Success	2/27/2013 1:24 PM		
2. Approval Batch Email Processing	Ready	2/27/2013 11:24 AM	Success	2/28/2013 11:24 AM		
3. Check Content Expiration	Ready	2/27/2013 5:00 AM	Success	2/28/2013 5:00 AM		
4. Cisco Content Delivery Manifest Generation	Disabled					
5. Clear Cache	Ready	2/26/2013 3:15 PM	Success	3/3/2013 5:00 AM		
6. Purge Deleted Content	Ready	2/27/2013 11:24 AM	Success	2/28/2013 11:24 AM		
7. Purge Logs	Ready	2/27/2013 11:24 AM	Success	2/28/2013 11:24 AM		
8. Refresh Channel Guide	Ready	2/27/2013 5:05 AM	Success	3/6/2013 5:05 AM		
9. Refresh LDAP Groups	Disabled					
10. Refresh LDAP User Groups	Ready	2/27/2013 11:24 AM	Success	2/28/2013 11:24 AM		

1	Activity Play Log Timeout	Closes play records that do not have a stop time.
2	Approval Batch Email Processing	Determines how often approvers will receive a batch "digest" of videos requiring approval.
3	Check Content Expiration	When stored content exceeds its expiration date, it becomes "expired" and only appears in video lists of users with admin access to the content. This task will (1) send email to configured recipients warning of imminent expirations and (2) delete content past its purge date (purge date = expiration date + purge delay). See Content Expiration Configuration for more information.
4	Cisco Content Delivery Manifest Generation	This task will generate a manifest file according to the settings on the Cisco Content Delivery page. Default = disabled.
5	Clear Cache	The system caches license information, language strings, and other data. Run this task if you add VOD servers, change licenses, upload a new language file, or make other significant changes to the configuration. The Refresh Cache button on the About page does the same thing.
6	Purge Deleted Content	Purge content that has already been deleted.
7	Purge Logs	Purges User Login and Content Play logs.
8	Refresh Channel Guide	Determines how often the Channel Guide is refreshed with new content data.
9	Refresh LDAP Groups	Re-import all LDAP groups.

10	Refresh LDAP User Groups	Re-import all LDAP user groups.
11	Refresh Live Content	Auto-discover all live content.
12	Refresh Stored Content	Auto-discover all stored content.
13	Start Auto-Ingest	Start autoingesting files.
14	State Cleanup	Deletes all user session information.
15	Verify Faulting Servers	Verify servers that have reported user exceptions.
16	Verify Offline Servers	Verify servers that are offline. You may want to poll these servers at a more frequent interval than online servers.
17	Verify Online Servers	Verify servers that are online. You may want to poll these servers at a less frequent interval than offline servers.

Edit Task

Use this page to edit the **Interval** and/or the **Scheduled** run time and recurrence of the task. As a best practice, VBrick recommends keeping the factory defaults.

Task Information

Edit Features: Activity Play Log Timeout

Interval:

Every: Minutes

Scheduled:

Run at:

Every: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Enabled

Cisco Content Delivery

ECDS (Enterprise Content Delivery System) and ACNS (Application and Content Networking System) are [Cisco](#) technologies that provide demand-pull caching and prepositioning of content for accelerated delivery of web applications, objects, files, and streaming media. (ACNS is a legacy version of this technology.) By caching on-demand content, or prepositioning frequently accessed content, ECDS/ACNS minimizes the need for the same digital media content to traverse WAN links from the data center to branch offices. When using this feature, the manifest file on the Portal Server will be used by ECDS/

ACNS to ensure that the content on the ECDS/ACNS server matches the content on the Portal Server. When the Portal Server is configured to integrate with an ECDS/ACNS network, content playback is redirected to stream from the ECDS/ACNS network—not from the Portal Server.

Cisco Content Delivery - Manifest Generation Configuration

Cisco Content Delivery System Type:

Full Path of Manifest File (on MASTER Server):

Address Range(s) of VOD Servers to Include in Manifest (separate multiple ranges with a comma):

Encoding Types to Include in Manifest:

H.264
 MP4
 FLASH
 MOV
 Windows Media

Categories to Include in Manifest:

Include All Categories

(Uncategorized)
 1
 AutoIngestedVideos
 FMS
 HDS
 HLS
 Recordings
 UploadedVideos
 UrlRecordings
 WebcastVideos

Cisco Content Delivery System Type	<ul style="list-style-type: none"> • ECDS – Default. Includes H.264, MP4, Flash, Mov, and Windows Media. • ACNS – Includes H.264, MP4, and Windows Media.
Full Path of Manifest File	Full path to manifest.xml file on the <u>master</u> Mystro server. Default = C:\Program Files (x86)\VBrick\Maduro\CiscoManifest.xml
Address Range(s) of VOD Servers:	Optional. One or more IP address ranges. If an entry is made in this field, only content from VOD servers/DMEs whose address lies within one of the ranges is included in the manifest. If blank, all VODs/DMEs are included.

Encoding Types	Specifies the encoding types to include in manifest. Any combination of these checkboxes can be chosen. By default all the checkboxes are selected.
Categories	Only content in the checked categories (or All Categories) is included in manifest. Default = All Categories.

Transcoding Presets

The VEMS Mystro transcoder is a licensed Portal Server feature that *transcodes* a stored file from one video encoding format to another. It transcodes a variety of different input formats to the output formats shown in Table 27. For example, when adding a stored MPEG-2 video, the file can be automatically transcoded to WM, H.264, HLS, or HDS. The transcoding "presets" are used to configure the Bit Rate, Frame Rate, Aspect Ratio etc. of the transcoded output. Transcoding can be configured to occur with some or all of the following user actions. A list of transcoding profiles from which to select can be configured to automatically display on the **Add Video** and **Scheduled Record** pages.

- Add Video
- Auto Ingest
- Record
- Scheduled Record
- Webcast Record
- Existing Content

Table 27. Supported Input/Output Formats

Input Formats †	WMV, MOV, AVI, MPEG-2, TS, MP4/H.264
Output Formats	WM, H.264, HLS, HDS



† Other formats are supported but have not been fully tested.

Table 28. Supported Video and Audio Codecs

Video Codec	Audio Codec
H.264	AAC MP4
H.264	AAC TS
H.264	LATM TS
H.264	AAC MOV
MPEG4P2	AAC MP4
MPEG4P2	AAC MOV
H.264	PCM MOV
VC-1	WMA ASF
MPEG-2	AC3 TS
DV	PCM AVI
IntelIYUV	PCM AVI
Microsoft Video1	PCM AVI

Video Codec	Audio Codec
Uncompressed Video	PCM AVI
VP6	MP1L3 Flash 8 (FLV)
H.264	MPEG1L2 TS
H.264	AC3 TS
MPEG4p2	PCM MOV
MPEG-2	MPEG1L2 TS
MPEG-2 ATSC	AC3 TS
MPEG-2 ATSC	MP1L2 TS
V9	WMA WMV
VC1	WMA WMV

There is a separate license for transcoding feature if you are using a version of VEMS prior to v6.3.8. If the license is not available, the transcoding options will not be displayed on the user interface. There is one transcoding license for the entire VEMS Mystro system that defines the maximum number of concurrent transcodings allowed. The license file must be installed on all VEMS Mystro servers in the system. For example, a five concurrent transcoding license will let you install up to five VBrick transcoders. (The total number of concurrent transcodings is limited to five.) The maximum number of simultaneous transcodings is shown on the Devices > [Application Servers](#) page. This number is read-only and derived from the installed license. If you have updated to VEMS v6.3.8 or beyond, this is not applicable and a separate transcoding license is not required. As a result, the number of licenses displayed in the images below, would not be displayed.

Application Server Administration				
Server Administration				
The maximum number of simultaneous recordings allowed by license: 10				
The maximum number of simultaneous transcodings allowed by license: 3				
Server List	Type	Max. Recordings	Edit	Delete
1. Homer (TestApp Server Description)	Master	2		

The Server Info page shows the maximum number of concurrent transcodings (and the load balance priority) configured for each server. You may choose to install only one transcoder on a powerful machine and set it to run five concurrent transcodings; or you may choose to install a transcoder on five different machines and let each one execute one transcoding operation at a time.

Application Server Administration

» Server Info
» Entry Points

Server Information

Type: Server Name:

Description:

FTP

User Name: Virtual Path:

Password: Local Path:

Record

Max. Recordings: Max. Bandwidth (kbps):

Recording Path:

AutoIngest

AutoIngest Path: Waiting List Size:

Active List Size:

Transcode

Max. Transcodings: Transcoder Priority: High

Max. Transcodings	Defines the max. number of concurrent transcodings allowed on this particular application server. The default is zero which disables transcoding on this server. If the maximum number of transcodings defined by the license file has been reached, an error message will be displayed if you try to increase the Max. Transcodings number. As noted, this is only applicable if you are using a version of VEMS prior to v6.3.8. See: Transcoder Licensing .
Transcoder Priority	Use the slider to defines the priority of the selected Application Server. If the priority is low, the server is less likely to be selected in the transcoder load balancing logic.

Best Practices

Transcoding is used with **Add Video**, **Auto Ingest**, **Record**, and other VEMS Mystro features to transcode stored content into different formats. One common use of the transcode feature is to automatically create HLS and/or HDS versions of stored content so it can be played on Apple and/or Adobe players respectively. Another common use with **Add Video** and **Auto Ingest** is to automatically convert files created using other tools into a format that VEMS Mystro can store and play. There is one transcoding instance included and installed with each VEMS Mystro and NVR server/software you purchased. Use the guidelines below to get the best performance from your transcoder instance(s) without impacting the performance of other VEMS functions.

Note VEMS Admin settings let you distribute your transcoding instances among your VEMS servers, however be aware that each transcoding instance can use as much processing power as is left over beyond the higher priority real-time functions of VEMS. Because of this you cannot generally improve performance by allocating multiple transcoder instances to the same VEMS server. For installations that require maximum transcoding performance VBrick recommends that you configure a dedicated NVR server for transcoding as explained below. See [Application Servers](#) on page 69 for more information.

The transcoding feature can be enabled on all VEMS Mystro servers including a Master server, a Redundant server, or an NVR. **As a best practice however, since transcoding is CPU-intensive, VBrick recommends you do not enable it on the Master server.** The transcoder is most CPU-intensive when configured to create HLS and/or HDS, so only enable those transcoder output formats when you know they are necessary for your installation and your users. For optimum transcoding performance, with minimal effect on other VEMS functions, you can dedicate an NVR server to perform only transcoding functions as explained below:

1. Add one or more NVR-10 or NVR-40 server(s) to the system.
2. Disable recording on the new server: set **Max. Recordings** to 0.
3. Enable transcoding on the new server: set **Max. Transcodings** to 1.
4. Disable transcoding on all other Mystro servers: set **Max. Transcodings** to 0.

Configuring Transcoding Presets

The transcoding presets are shown below and explained in the following table. The list can be filtered by **Type** and you can mouseover each preset to see a brief description. The list also includes the special "No Transcoding" preset which cannot be duplicated or deleted. The **Active** icon is only shown for those presets that are currently enabled (on the Edit page) For best results when editing the presets, use the **Duplicate** button in order to preserve the original profile.

Transcoding Preset Administration						
Transcoding Preset List						Q
Preset List	Filter By Output Type: All	Type	Active	Duplicate	Edit	Delete
1. H.264-Baseline - Mobile 288p 1.5M CBR		H.264	✓			
2. H.264-Baseline - Mobile 288p 750K VBR2		H.264	✓			
3. H.264-High - HD 720p 2M VBR2		H.264	✓			
4. H.264-High - SD 360p 1.5M CBR		H.264	✓			
5. H.264-High - SD 360p 1.5M VBR1		H.264	✓			
6. H.264-Main - HD 720p 2M CBR		H.264	✓			
7. H.264-Main - HD 720p 2M VBR2		H.264	✓			
8. HDS 720P		HDS	✓			
9. HLS 720P		HLS	✓			
10. No Transcoding			✓			
11. VC-1 Advanced - HD 720p 3M VBR		WM	✓			
12. VC-1 Advanced - SD 360p 1.5M CBR		WM	✓			

Table 29. Transcoder Presets

	Preset	Type	Video Codec	Optimized for:
1	H.264-Baseline - Mobile 288p 1.5M CBR	H.246	H.264 Baseline	Mobile-compatible
2	H.264-Baseline - Mobile 288p 750K VBR2	H.246	H.264 Baseline	Mobile-compatible low bitrate
3	H.264-High - HD 720p 2M VBR2	H.246	H.264 High	Streaming
4	H.264-High - SD 360p 1.5M CBR	H.246	H.264 High	Storage and LAN streaming
5	H.264-High - SD 360p 1.5M VBR1	H.246	H.264 High	Streaming
6	H.264-Main - HD 720p 2M CBR	H.246	H.264 Main	Storage and LAN streaming
7	H.264-Main - HD 720p 2M VBR2	H.264	H.264 Main	Storage and LAN streaming
8	HDS 720P †	HDS	H.264 Baseline	Low bitrate streams < 450K
			H.264 - Main	High bitrate streams > 450K
9	HLS 720P ††	HLS	H.264 Baseline	Low bitrate streams < 450K
			H.264 - Main	High bitrate streams > 450K
10	No Transcoding			
11	VC-1 Advanced - HD 720p 3M VBR	WM	VC-1 Advanced	Streaming
12	VC-1 Advanced - SD 360p 1.5M CBR	WM	VC-1 Advanced	Streaming
13	VC-1 Main - 480p 1.5M VBR	WM	VC-1 Advanced	Streaming
14	VC-1 Main - HD 720p 6M CBR	WM	VC-1 Main	Storage and backwards compatibility
15	VC-1 Simple - 136p 350K CBR	WM	VC-1 Simple	Backwards compatibility

- † HTTP Live Streaming (for Apple iOS devices).
- †† HTTP Dynamic Streaming (for Adobe applications).

When using this page, click the **Edit** button to modify the preset templates; for best results use the **Duplicate** button to create your own preset and preserve the original. Click the **Save** button (in the "stream" panel) to save the video frame size and bitrate information only. Click the **Submit** button to save all changes including the video frame size and bitrate. Also be aware that some fields on the page may be displayed/hidden and some field labels may be changed depending on the selected preset.

Transcoding Preset Administration

Transcoding Preset Information

Preset Name: Enabled:

Description:














Video codec: Mixed. H.264 - Baseline for low bitrate (less than 450K) streams, H.264 - Main for high bitrate streams; Encoding mode: CBR - 1 pass.

Output Encoding Type: HDS

Prevent Upscale:

Buffer Window (s): Frame Rate (fps):

Key Frame Interval (s): Video Aspect Ratio:

	Frame Width	Frame Height	Video Bitrate (Kbps)	Save	Delete
1.	<input type="text" value="1280"/>	<input type="text" value="720"/>	<input type="text" value="2962"/>		
2.	<input type="text" value="856"/>	<input type="text" value="480"/>	<input type="text" value="1800"/>		
3.	<input type="text" value="640"/>	<input type="text" value="360"/>	<input type="text" value="1200"/>		
4.	<input type="text" value="640"/>	<input type="text" value="360"/>	<input type="text" value="688"/>		
5.	<input type="text" value="512"/>	<input type="text" value="288"/>	<input type="text" value="420"/>		
6.	<input type="text" value="476"/>	<input type="text" value="268"/>	<input type="text" value="230"/>		
	<input type="text"/>	<input type="text"/>	<input type="text"/>		

Audio Codec: AAC-LC
 Audio Bitrate (kpbs): Audio Sample Rate (kHz):

Preset Name	User friendly name for the preset.
Enabled	Check to enable disable.
Description	Meaningful description of the preset.
Output Encoding Type	Read-only: WM, H.264, HLS, HDS.

Prevent Upscale	If checked the transcoder will try not to upscale the video in terms of frame size and bitrate. When checked, the target frame size will not exceed the original frame size; the target bitrate will not exceed twice the original bitrate. Default = checked. For HDS/HLS, the target output streams are based on the source file bitrate and frame size. For example, if you select the HDS 720P preset, and the source file is only 360P, there will be only four output streams (360P @ 1200Kbps, 360P @ 688Kbps, 288P @ 420Kbps and 268P @ 230Kbps. The other two streams defined in the preset will not be created.
Buffer Window	Specifies the number of seconds the file should buffer before playback.
Key Frame Interval	Specifies the number of seconds between key frames.
Frame Rate	Specifies the frame rate of the video. For HLS low bit rate streams, Apple recommends a target frame rate of 15 fps for legacy devices (for example the iPhone 3G). For all other HLS/HDS streams, if the Frame Rate is Source (default), the target frame rate will be the same as the source frame rate if the source frame rate is not larger than 30. If the source frame rate is larger than 30, the target frame rate will be set to 29.97. If you selects a frame rate other than Source, Mystro will use the selected frame rate.
Video Aspect Ratio	Specifies the aspect ratio of the output frame or choose Source to match the aspect ratio and pixel aspect ratio of the source file.
Frame Width	Specifies the width of the video. Enter zero (0) to use the source frame width.
Frame Height	Specifies the height of the video. Enter zero (0) to use the source frame height.
Video Bitrate	Specifies the bitrate of the video.
Audio Codec	Read-only: selected audio codec.
Audio Bitrate	Specifies the bitrate of the audio.
Audio Sample Rate	Specifies the sample rate of the audio.

Transcoding Profiles

The default transcoding profiles are shown below. Transcoding profiles contain one or more presets. The transcoder will create one stream for each preset contained in the profile. The profile **None** can be enabled, disabled, or edited to change the name but it cannot be deleted. The **Active** icon is shown when the profile is enabled on the edit page. You can drag and drop to change the order and click on the profile name to see what presets are included in the profile.

Note You can use drag-and-drop to reorder the Transcoding Profile List. This is important because the first profile in the list will be the default profile on the **Add Video** and **Scheduled Record** pages (if the Profile List is configured in Global Settings to be displayed to users on those pages).

Transcoding Profile Administration

Transcoding Profile List 🔍

Profile List	Active	Edit	Delete
1. None (Do not transcode)	✔	📄	
2. H.264 (Transcode to H.264)	✔	📄	✖
3. VC-1 (Transcode to VC-1)	✔	📄	✖
4. H.264 and VC-1 (Transcode to both H.264 and VC-1)	✔	📄	✖
5. HDS (Transcode to HDS)	✔	📄	✖
6. HLS (Transcode to HLS)	✔	📄	✖

Add New Profile
Define Default Profile
Save Sort Order

	Profile	Description	Presets Included
1	None	Do not transcode.	None
2	H.264	Transcode to H.264.	H.264-High - SD 360p 1.5M VBR1
3	VC-1	Transcode to VC-1.	VC-1 Advanced - SD 360p 1.5M CBR
4	H.264 and VC-1	Transcode to both H.264 and VC-1.	<ul style="list-style-type: none"> H.264-High - SD 360p 1.5M VBR1 VC-1 Advanced - SD 360p 1.5M CBR
5	HDS	Transcode to HDS.	HDS 720P
6	HLS	Transcode to HLS.	HLS 720P

Note The **Show Transcoding Profile List to User** option on the System Settings > [Global Settings](#) page will determine whether or not the profile list is displayed on the Add Video page and the Scheduled Record page.

Configuring HLS/HDS VOD Servers

HLS VOD Server

All web servers can serve HLS files created by VEMS Mystro. Mystro will ingest HLS to all configured [File Server-HTTP](#) publishing points. The Mystro administrator will be responsible for configuring the File Server-HTTP web server for the following MIME types:

Extension	Mime Type
.ts	video/MP2T
.m3u8	application/x-mpegURL

HDS VOD Server

Not all web servers can serve HDS. HDS requires Apache 2.2 and a special module from [Adobe](#). In addition, VEMS Mystro will only ingest HDS to a [File Server-HTTP](#) publishing point that has the **Support HDS** box checked.

Note DME v3.1.0 or above supports HDS. The DME version will be auto- detected when a DME is added to the VEMS Mystro system. If the DME version is 3.1.0 or above, it will ingest HDS files.

Add New Profile

Use the following page to add a new profile to the **Transcoding Profile List**. Note that the system will return errors if there are multiple presets with the same output type. To create a new profile, simply move the desired preset(s) from **Available Transcoding Presets** to **Selected Transcoding Presets** and click **Submit**. The new profile (if enabled) will be added to the list of available profiles.

The screenshot shows the 'Transcoding Profile Administration' web interface. At the top, there is a header 'Transcoding Profile Administration'. Below it is a section titled 'Transcoding Profile Information'. This section contains a 'Profile Name' text input field, a 'Description' text area, and an 'Enabled' checkbox which is checked. Below this is a 'Filter Search' section with a dropdown menu set to 'All' and a search input field. The main area is divided into two columns: 'Available Transcoding Presets' and 'Selected Transcoding Presets'. The 'Available Transcoding Presets' list includes: H.264-Baseline - Mobile 288p 1.5M CBR, H.264-Baseline - Mobile 288p 750K VBR2, H.264-High - HD 720p 2M VBR2, H.264-High - SD 360p 1.5M CBR, H.264-High - SD 360p 1.5M VBR1, H.264-Main - HD 720p 2M CBR, H.264-Main - HD 720p 2M VBR2, HDS 720P, HLS 720P, No Transcoding, VC-1 Advanced - HD 720p 3M VBR, and VC-1 Advanced - SD 360p 1.5M CBR. The 'Selected Transcoding Presets' list is currently empty. Between the two lists are 'Add' and 'Remove' buttons. At the bottom of the interface are 'Back to List' and 'Submit' buttons.

Define Default Profile

Use this page to define the default transcoding profile for each VEMS Mystro operation e.g. Add Video, Scheduled Record, etc. By default, the transcoding profile **None** is initially selected for all operations meaning no transcoding will occur.

Note If transmux is enabled on the System Settings > [Global Settings](#) page and the input file and transcode output files are both H.264/AAC MP4, only the transcoded file will be transmuxed to H.264/AAC TS.

Transcoding Profile Administration		
Transcoding Profile Defaults		
Operation	Transcoding profile	Ingest Original
1. Add Video	None	<input checked="" type="checkbox"/>
2. Auto-ingest	None	<input checked="" type="checkbox"/>
3. Record	None	<input checked="" type="checkbox"/>
4. Scheduled Record	None	<input checked="" type="checkbox"/>
5. Webcast Record	None	<input checked="" type="checkbox"/>
6. Existing Content	None	<input type="checkbox"/>

Back to List Submit

Transcoding Existing Content

You can transcode existing content in batch mode using the AutoIngest folder on the Devices > Application Servers > Server Info page (see [Auto Content Ingestion](#) on page 237 for more about this) or by transcoding individual files as explained below. As described on the previous pages, the basic steps are as follows:

- ▼ To transcode existing content:
 1. On the Devices > Application Server page, set the **Max Transcodings** parameter to 1.
 2. On the System Settings > Transcoding Presets page, pick a transcoding preset that works for you.
 3. On the Transcoding Profiles page, create a Transcoding Profile that uses the selected Preset.
 4. On the Transcoding Profile page click **Define Default Profile**.
 5. On the Transcoding Profile Defaults page, use the dropdown to select the Transcoding profile to use for **Existing Content**.

VOD-W Only If the file(s) you want to transcode are on a VOD-W server, you will need to create an FTP virtual directory that maps to the Storage Paths defined on the Publishing Points page for the VOD-W. For details follow all of the steps in [Configuring a Cloud Server to Synchronize VOD-W Content](#) on page 115.

6. Then use the following steps for each video file you want to transcode:
 - a. In the VEMS user interface, launch the video from the **Stored Video** page.
 - b. Wait until the stream begins to play and click the stop button.
 - c. Click on the **Instances** tab and click on the **Transcode** icon.
 - d. The file will be transcoded without further messages. To verify that a new (transcoded) instance has been added, repeat Steps a, b, and c and verify that a new instance has been added.

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 encoder you select (MPEG-2, H264, etc. You can script commands to change any of the parameters available in the MIB database for the selected device.

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.

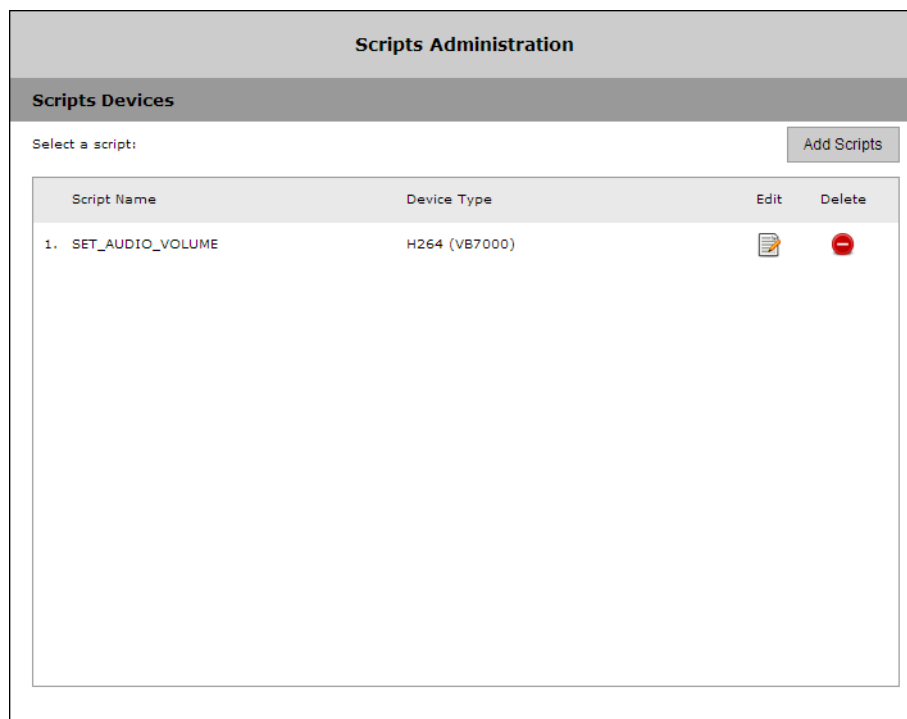
You can control devices that require binary input by pasting binary input into the **Script Content** text box. Binary scripts let you provide a sequence of commands for devices that require binary input. This type of script will pass binary input through the serial passthrough port on a VBrick encoder 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.

Add 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**.

Scripts Administration

Script Information

Script Name:

Device Type:

Select Device:

Available Devices:

- A1-TonyH264
- AndyM-H264-VBSTAR
- ATB-H264
- Bob0007df01073d
- Brian-Support-7000
- CNBCMrtgDemoPtrl
- EternalH264
- Live-H264-DS-DEMO
- MAC0007df00c03c
- MAC0007df01073c
- Marketing-CBS

Add

Remove

Entered Devices:

- CD-ZITI-113
- JohnS-7000

Script Content

Parameter Name: Parameter Value:

Parameter Name	Parameter Value
<input type="text" value="vbrickEncoderAudioCommonAutomaticVolumeControl"/>	<input type="text" value="parm1"/>

3. In **Script Configuration**, enter a **Script Name** and select a **Device Type** (MPEG2/MPEG4/WM, H264 (VB7000), H264 (VB9000), 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 [Finding VBrick Parameters and Values](#) 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 on the **Scheduler**. Then create a schedule by selecting a date, time, and (optionally) a recurrence pattern. Then select the script you want to run on the schedule you just defined. See the "Scheduler" topic in the *VEMS Mystro User Guide* for more information.

Examples

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 the "Serial Port Passthrough" topic in the *9000 Series Appliance Getting Started 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 [Support Services](#).

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

Scripts are typically used to set options or parameters at runtime for an encoder. In order to create scripts, you need to determine the correct parameters and values to use. In general the best way to find the value(s) associated with a parameter is to view the encoder's Management Information Base (MIB) using a standard MIB browser or a text editor. The MIBs are typically available on the VBrick Support [Downloads](#) site for the encoder. For more about this refer to the encoder documentation or contact VBrick Support Services.

Reporting

VEMS Mystro reporting has realtime features that include the admin [Dashboard](#), [Global Recording Status](#), and diagnostic reporting such as [Export to Excel](#) which provides content, group, and user-related reports. You can use the reporting data in Microsoft Excel or it can be imported into Crystal Reports or other applications. You can create any number of reports by merging the data from several report outputs. Mystro reporting also lets you view the **Global Recording Status** which is a snapshot of all current "record" activity.

	Export to Excel	187
	Global Recording Status.	191
	Content Approval Status	192

Note System Diagnostics that report the response times from the VEMS Server, the database server, and the LDAP server are located on the [About](#) page.

Export to Excel

The Reporting feature lets you export selected system data to an Excel spreadsheet. For example you can export user **Login Activity** that shows who logged in to the system and at what time, or you can export **Play Activity** that shows exactly which videos were played and for how long. Some reports, like **Content Inventory** or **User List Report**, are simply downloaded from the VEMS Mystro database to a comma-separated file you can open in Excel.

Reporting

Export To Excel

Select a report:

Content Related Reports:
Play Activity
Plays Tried Over Maximum
Content Inventory
Content Statistics
Content Expiration
Recommended Content
Required Content
Content Approval
Content Rejected
VOD Content

Group Related Reports:
Group Membership
Group Category Permissions

User Related Reports:
Login Activity
User List Report
User Category Permissions
User Content Permissions

System Configuration Reports:
Configuration Reports

System Exceptions:
Exceptions Log

Other reports, like **Play Activity**, require a start date and an end date. (For best results click in the field and use the calendar control.)

Reporting

Export To Excel

Select a report:

Start Date: (M/d/yyyy)

End Date: (M/d/yyyy)

Still others, like **Recommended Content** and **Required Content**, need you to select the users who recommended or required the content, and the users for whom the content is recommended or required.

Reporting

Export To Excel

Select a report: Recommended Content

Recommended By:

-- Any --
Admin
ContentAdministrator
ContentPublisher
ContentViewer
Guest
nick
Scheduler
SystemAdministrator
UserAdministrator
VBrickAdministrator

Page: Of 2 >>

Recommended For:

-- Any --
Admin
ContentAdministrator
ContentPublisher
ContentViewer
Guest
nick
Scheduler
SystemAdministrator
UserAdministrator
VBrickAdministrator

Page: Of 2 >>

Download
Clear

▼ To create a report:

1. Select a report from among the following report types on the dropdown list.

Content Related	<ul style="list-style-type: none"> • Play Activity (Note: to improve performance this report can be disabled when scheduling a webcast.) • Plays Tried Over Maximum • Content Inventory • Content Statistics • Content Expiration • Recommended Content • Required Content • Content Approval (and current status) • Content Rejected • VOD Content
Group Related	<ul style="list-style-type: none"> • Group Membership • Group Category Permissions
User Related	<ul style="list-style-type: none"> • Login Activity • User List Report • User Category Permissions • User Content Permissions
System Configuration	<ul style="list-style-type: none"> • Configuration Reports
System Exceptions	<ul style="list-style-type: none"> • Exception Log

2. If necessary enter a **Start Date** and **End Date** either manually or using the calendar. Dates and Times are entered as Universal Time Coordinated (UTC). They are **not** entered as the local date and time of the server.
3. If necessary, enter the **Recommended/Required By** and **Recommended/Required For** users.

Reporting

Export To Excel

Select a report: Play Activity

Start Date: 2/26/2013 (M/d/yyyy)

End Date: << Feb 2013 >>

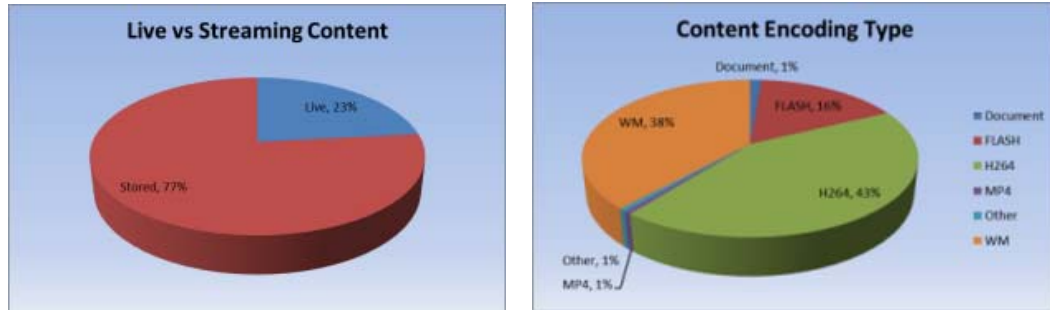
							1	2
3	4	5	6	7	8	9		
10	11	12	13	14	15	16		
17	18	19	20	21	22	23		
24	25	26	27	28				

Download
Clear

4. Click **Download** and choose to **Open** (in Excel) or **Save** the report file.

	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Play Durat	User Nam	User IP	Content E	Live/Store	Content P	Content T	Content B	Content P	Applicati	ClientOS	MulticastI	MulticastI
2	0:01:44	Admin	172.22.2.8	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows XP		
3	0:00:13	Admin	172.22.2.8	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows XP		
4	0:00:00	Admin	172.22.2.8	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows XP		
5	0:00:00	Admin	172.22.2.8	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows XP		
6	0:00:00	Admin	172.22.2.8	H264	Stored	HTTP	1_21_h264	0	http://172	MaduroW	Windows XP		
7	0:00:32	Admin	172.22.2.8	H264	Stored	HTTP	1_11_11_C	0	http://172	MaduroW	Windows XP		
8	0:00:19	Admin	172.22.2.8	H264	Stored	HTTP	1_11_11_C	0	http://172	MaduroW	Windows XP		
9	0:00:00	Admin	172.22.2.8	WM	Stored	HTTP	13 apr title	0	http://172	MaduroW	Windows XP		
10	0:00:00	Admin	172.22.2.8	H264	Stored	VBRTSP	1_42 live w	0	vbrtsp://1	MaduroW	Windows XP		
11	0:00:00	Admin	172.22.2.8	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
12	0:00:00	Admin	172.22.2.8	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
13	0:00:36	Admin	172.22.184	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows 7		
14	0:00:41	Admin	172.22.184	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows 7		
15	0:00:37	Admin	172.22.184	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows 7		
16	0:00:36	Admin	172.22.184	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows 7		
17	0:00:31	Admin	172.22.184	WM	Stored	RTSP	1_CD_WM	0	rtsp://172	MaduroW	Windows 7		
18	0:01:00	Admin	172.22.184	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows 7		
19	0:00:27	Admin	172.22.2.5	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
20	0:01:01	Admin	172.22.2.5	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
21	0:00:00	Admin	172.22.2.5	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
22	0:00:00	Admin	172.22.2.5	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		
23	0:00:38	Admin	172.22.2.8	WM	Stored	RTSP	1_CNN_W	0	rtsp://172	MaduroW	Windows XP		

The administrator can provide these reports which can easily be converted into visual reports such as shown below.



Global Recording Status

This page provides a current snapshot of all "recording" activity, including recordings, conversions, FTPs, and ingestions that are currently in progress on configured VOD servers and NVRs. It lets an administrator view, cancel, or purge all active or individual procedures that were initiated by any VEMS user. You can expand the tree next to each item to see all of the recording procedures (e.g. Conversion or FTP) associated with that item. Use the sort button next to each header to sort by **User**, **Title**, **File Name**, etc. When all of the procedures are done, the item is no longer "active" and is removed from the page. **This page does not show the status of any content that was uploaded using the Add Video feature.**

Global Recording Status




Search by Server IP Address

1 Number of Active Recordings |
 0 Number of Additions |
 0 Number of Auto Ingestions |
 0 Number of Downloads
0 Number of Active Conversions |
 0 Number of Active FTPs |
 0 Number of Active Ingestions

Refresh every minutes

Recordings		Add Videos		Downloads		Auto Ingestions	
Sort by	User A-Z	10	Items per page	Go to page	1	of 1 pages	
	User	Title	File Name	Server	Status %	Cancel	Purge
1.	+	nick	NM7000TSt_13_02_27_19_14_08	d:\inetpub\ftproot\VBrick\Record\NM7000TSt_13_02_27_19_14_08.mpg	Homer	Record completed.	<input checked="" type="button"/> <input type="button"/>
2.	+	vs	Recording of Victor WM	d:\inetpub\ftproot\VBrick\Record\Victor WM_13_02_26_19_52_53.wmv	Homer	Failed to capture Window Media stream	<input checked="" type="button"/> <input type="button"/>
3.	+	vs	Recording of Victor WM	d:\inetpub\ftproot\VBrick\Record\Victor WM_13_02_26_20_07_40.wmv	Homer	Failed to capture Window Media stream	<input checked="" type="button"/> <input type="button"/>
4.	+	vs	Victors_H264_TS_13_02_27_19_06_15	d:\inetpub\ftproot\VBrick\Record\Victors_H264_TS_13_02_27_19_06_15.mpg	Homer	23%	<input checked="" type="button"/> <input type="button"/>

Search by	Search for a recording status by title or by the user name who initiated the recording.
Active Recordings	Displays the number of active recordings currently in progress.

Additions	Displays the number of "add videos" currently in progress.	
Auto Ingestions	Displays the number of auto ingestions currently in progress.	
Downloads	Displays the number of downloads currently in progress.	
Active Conversions	Displays the number of active conversions (transmuxes and transcodings) currently in progress. See System Settings > Ingestion Options for more about this.	
Active FTPs	Displays the number of active FTPs currently in progress.	
Active Ingestions	Displays the number of active ingestions currently in progress.	
Refresh every n minutes	Set the refresh interval for this page to 2, 5, or 10 minutes, or click Refresh Now .	
Cancel All	Cancels all active recording procedures (i.e. recordings, conversions, FTPs, and ingestions) that are currently in progress. Use the individual Cancel buttons to cancel individual procedures.	
Purge All	Purges (i.e. deletes) all procedures from this page that have been previously cancelled. Use the individual Purge buttons to purge individual procedures.	
Cancel		Cancel the selected operation.
Purge		Purge (i.e. delete) the selected operation.
Retry		Retry the selected (failed/conversion/ftp) operation. When a root operation and its descendant operations are canceled, failed, or have succeeded, and one of the conversion or ftp operations has either failed or been canceled, the Retry button is displayed at the root level. Click Retry to restart the failed/ canceled conversion/ftp operation.

Content Approval Status

If [Content Workflow](#) functionality is enabled this page provides a current snapshot of all content approval activity. These reports show the number of items that have been approved, rejected, deleted, or are waiting for approval. Select the type of live on-screen report you wish. Use the calendar to select the **Start Date** and **End Date**.

Content Approval Status

Select Type: Requires Approval
 Approved
 Rejected
 Deleted

Start Date: (M/d/yyyy)

End Date: (M/d/yyyy)

« Mar 2012 »

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Content Approval Status

Content Title	Owner	State	Workflow Name	Workflow Step Name	Approver User Name
education-340Kbps	Admin	Approved	Default Content Approval Workflow	-	andy
education-2Mbps	Admin	Approved	Default Content Approval Workflow	-	andy
MP4 Audio Only	andy	Approved	Default Content Approval Workflow	-	andy
Things We Said Today/I'll Be Back (acoustic Beatle...	andy	Approved	Default Content Approval Workflow	-	andy

SharePoint 2013 Integration

Overview	195
Embedding a VEMS Interface.....	196
Configuring an "Add Video" Widget.....	198

Overview

If you are using Microsoft SharePoint to manage content, you can easily integrate SharePoint with VEMS components. As explained below, you can embed a VEMS interface that will let you play live and stored video content directly from SharePoint. You can also add a VEMS “widget” that you can use to add video to SharePoint. If you purchased a “software only” version of VEMS and are installing the software on your own machine, the VEMS Mystro SharePoint functionality is provided on a separate “SharePoint” CD. You must install VEMS Mystro from the VBrick Support [Downloads](#) site before you install the VEMS Mystro SharePoint functionality from the SharePoint CD. See the readme file on the SharePoint installation CD for installation and upgrade instructions.

-
- Notes**
- The SharePoint CD also includes installation files for SharePoint Enterprise Search. SharePoint Enterprise Search is a feature that integrates video content into SharePoint search results. **SharePoint Enterprise Search must be installed in conjunction with VBrick Professional Services.** For more information contact your certified VBrick reseller or VBrick [Support Services](#).
 - This topic explains how to embed a VEMS interface in SharePoint 2013. If you are using SharePoint 2010, please see the VEMS 6.3.3 documentation located at www.vbrick.com/documentation
-

Finally, both the SharePoint 2010 and SharePoint 2013 integration documents are also located at www.vbrick.com/documentation.

Embedding a VEMS Interface

The VEMS SharePoint interface provides an interface for live and stored content which can be embedded into a SharePoint Page Viewer Web Part. This interface can be modified to better conform to the style of the SharePoint façade in use.

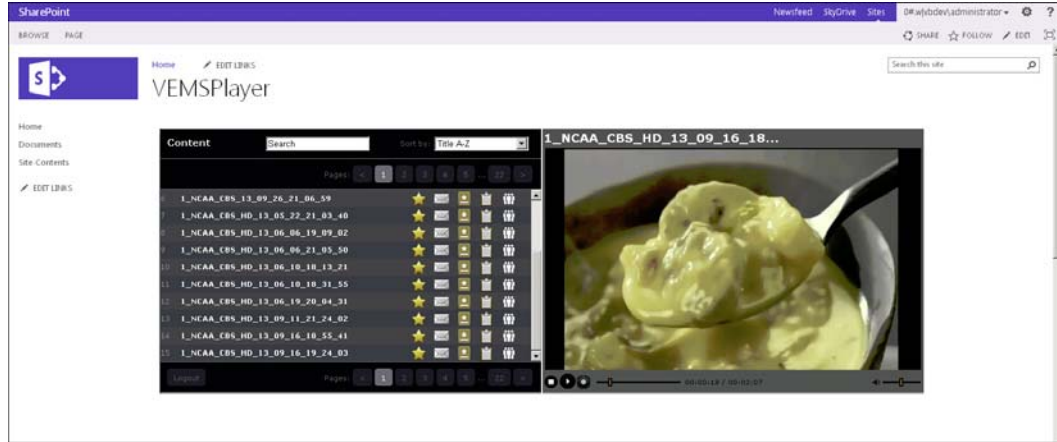
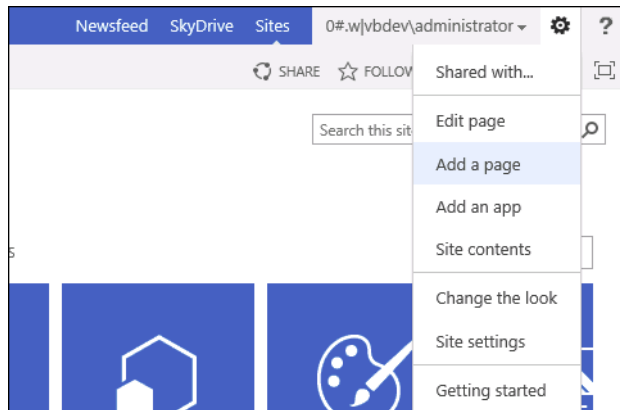


Figure 19. VEMS Content List Page in SharePoint

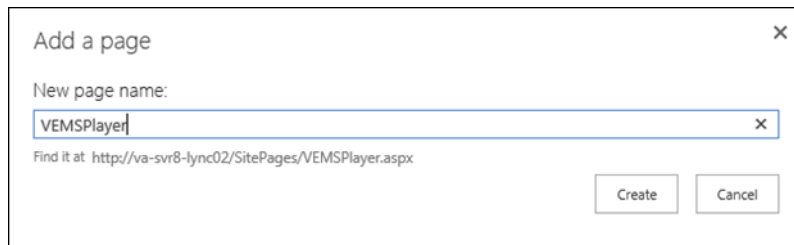
Creating a Page in SharePoint 2010

▼ To create a new page:

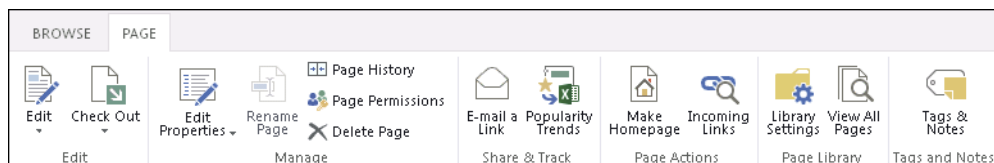
1. Log into SharePoint as user with ability to create a new "Site Page".
2. Click the gear icon at the top right of the screen and click **Add a page**.



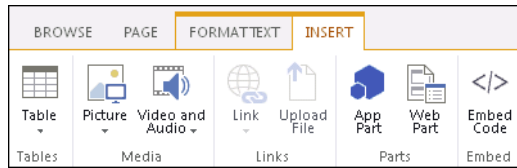
3. Give the page a name when prompted and click **Create**.



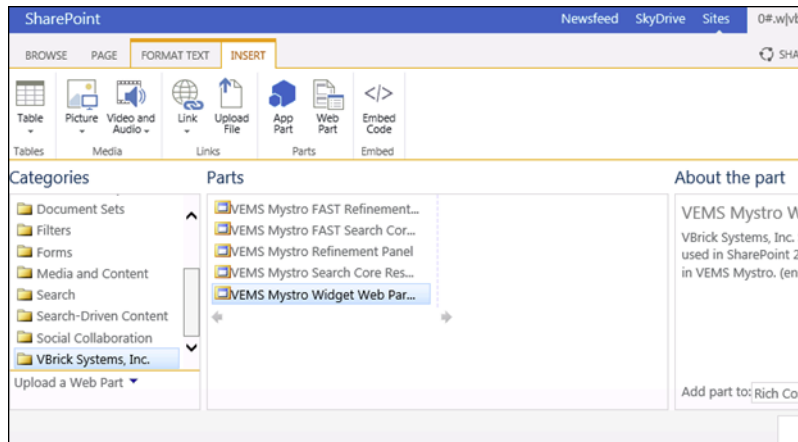
4. When the new page appears, click "Page" in the top bar to view Page tools, then click on the **Edit** icon.



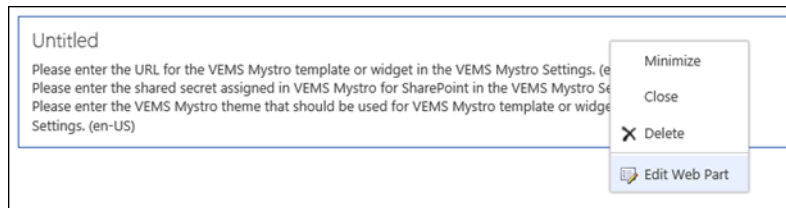
- In the new menu that appears, move to the Insert tab of the Page tools and click WebPart.



- Insert the VBrick player web-part using by selecting “VBrick Systems, Inc.” under Categories
- Select “VEMS Mystro Widget Web Part” and clicking “Add”



- Click on the VBrick web-part then click on the drop down arrow at the top right of the web-part container and select Edit Web Part.



- In the “Page Viewer” settings, set the Link to `http://<VEMS 6.0 FQDN>/vemsweb/EmbedContentList.html`
- In the Appearance, set the height to 450 pixels and the width to 1405 pixels.
- Click "OK".
- The Default Mystro SharePoint Interface should appear in the new page (Figure 19).

Client Side Settings

In order for the client to function properly in Internet Explorer, the VEMS Server needs to be added as a trusted site to IE. If the VEMS server is not added as a trusted site the interface will still function but the user will be forced to log into the VEMS SharePoint interface on every visit to a SharePoint page with the VEMS SharePoint interface embedded.

Setting Page Properties

The VEMS SharePoint interface provides a mechanism to display a content list from Mystro in a SharePoint interface. This content list provides numerous adjustable properties you can use to modify the look and feel of the list to match the look and feel of SharePoint. In order to modify the look and feel of the VEMS SharePoint Interface, you must modify the embed file on the VEMS server. VEMS comes with an embed file pre-made which may be modified, this file is called “EmbedContentList.html” and it is located in the “vems/vemsweb” virtual directory. Alternatively, you may copy this file and make a new embed file and modify this copy. This is the preferred way to modify the look and feel.

▼ To change the look and feel of the VEMS SharePoint Interface:

1. Copy `EmbedContentList.html` to a new file, for this example you can name it “NewEmbedSample.html”.
2. Make sure the copy is in the same folder as “EmbedContentList.html” (virtual directory ‘vems/vemsweb’).
3. Open “NewEmbedSample.html” in a text editor such as Wordpad. You should see the code below:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title></title>
</head>
```



```

<body>
<span id="list"><iframe type='text/html' src='/VEMSWeb/Widgets/
EmbedContentListWidget.html' width='575' height='400' frameborder='0'
scrolling='no' dataOverrides="{
  playerless: 'false',
  searchField: '70',
  searchValue: '',
  widgetHeight: '400',
  widgetWidth: '575',
  maxItems: '15',
  videoType: 'stored',
  displayIcons: 'true',
  category: '',
  widgetFontFamily: 'Verdana',
  widgetFontSize: '11px',
  widgetFontColor: '#727272',
  titleText: 'Content',
  titleFontSize: '15px',
  titleFontFamily: 'Verdana',
  titleFontColor: '#ffffff',
  listItemFontSize: '11px',
  listItemFontFamily: 'Verdana',
  listItemFontColor: '#ffffff',
  backgroundColorBody: '#1a1c1e',
  backgroundColorEven: '#3A3E42',
  backgroundColorOdd: '#424649',
  loginBackgroundColor: '#1a1c1e'}"></iframe></span>

<span id="player"></span>
</body>
</html>

```

4. Adjust the parameters to your liking. Be careful about "" marks and "," marks as any improper syntax may break the page.
5. Note: when adjusting the “widgetHeight” and “widgetWidth” properties, be sure to modify the “height” and “width” properties of the “iframe” tag to match. Unusual heights and widths may result in an unusable widget as it may be too small, too thin or too short.
6. In step 9 of the “Install Procedure” section, replace <http://vems-ip/vemsweb/EmbedContentList.html> with <http://vems-ip/vemsweb/NewEmbedSample.html>.

Table 30. Parameter Definitions

Parameter	Description	Example
playerless	Determines if the player window is shown to the right of the content list, or opens a new window or tab to play content. Values: 'true' 'false'	playerless: 'false'
searchField	Tells the searchValue setting what search targets are available to search by. Values: '70' - All Fields '71' - Title '72' - Description '248' - Keyword	searchField: '70'

Parameter	Description	Example
searchValue	searchValue can be anything that you wish to search for. Searches fields set in the searchField value. Default 70. When a serachValue is entered here, the search box is unavailable on the client interface.	searchValue: 'test'
widgetHeight	The height of the content list in pixels. For best results use a value of 200 px or more.	widgetHeight: '400'
widgetWidth	The width of the content list in pixels. Note that page will not display properly if set to less than 550 px.	widgetWidth: '575'
maxItems	Determines the number of items on the screen before paging occurs.	maxItems: '15'
videoType	Display live or stored content. Values: 'live' 'stored'	videoType: 'live'
displayIcons	Every user has ability icons associated with their profile such as Favorites, Recommended, etc. This hides or shows those icons. Values: 'true' 'false'	displayIcons: 'false'
category	Filter content based on a category	category: 'history'
widgetFontFamily	Sets the font family for general widget text items. Be advised that if you choose a font unsupported by your browser you will see the default browser font displayed.	widgetFontFamily: 'Verdana'
widgetFontSize	Sets the font size for general widget text items	widgetFontSize: '20px'
widgetFontColor	Sets the font color for general widget text items	widgetFontColor: '#ff0000' widgetFontColor: 'red'
titleText	Sets the title text which displays at the top left of the widget.	titleText: 'Stored Content'
titleFontSize	Sets the font size of the title text	titleFontSize: '14px'
titleFontFamily	Sets the font family of the title text. Note: If you choose a font not supported by your browser, the default browser font will be used.	titleFontFamily: 'Arial'
titleFontColor	Sets the font color of the title text	titleFontColor: 'white'
listItemFontSize	Sets the font size of the items in the list	listItemFontSize: '15px'
listItemFontFamily	Sets the font family of the items in the list. Note: If you choose a font not supported by your browser, the default browser font will be used.	listItemFontFamily: 'Times New Roman'
listItemFontColor	Sets the font color of the items in the list	listItemFontColor: 'blue'

Parameter	Description	Example
<code>backgroundColorBody</code>	Sets the background color of the widget.	<code>backgroundColorBody: 'blue'</code> <code>backgroundColorBody: '#ff0000'</code>
<code>backgroundColorEven</code>	Sets the background color of even lines in the list	<code>backgroundColorEven: 'red'</code> <code>backgroundColorEven: '#ff0000'</code>
<code>backgroundColorOdd</code>	Sets the background color of odd lines in the list	<code>backgroundColorodd: 'white'</code> <code>backgroundColorEven: '#ffffff'</code>
<code>loginBackgroundColor</code>	Sets the background color of the login interface	<code>loginBackgroundColor: 'green'</code> <code>loginBackgroundColor: '#000000'</code>

Configuring an "Add Video" Widget

This topic explains how to install the Add Video Embedded Widget (Figure 20). This widget lets you use the VEMS "Add Video" functionality from SharePoint. In order to use the Add Video embedded widget, the SharePoint embedding module for VEMS must be installed. This functionality is available on the SharePoint Product CD. After installing the SharePoint module from the Product CD, follow the directions below for configuration. For an explanation of the "Add Video" functionality in VEMS, see the *Portal Server User Guide*.

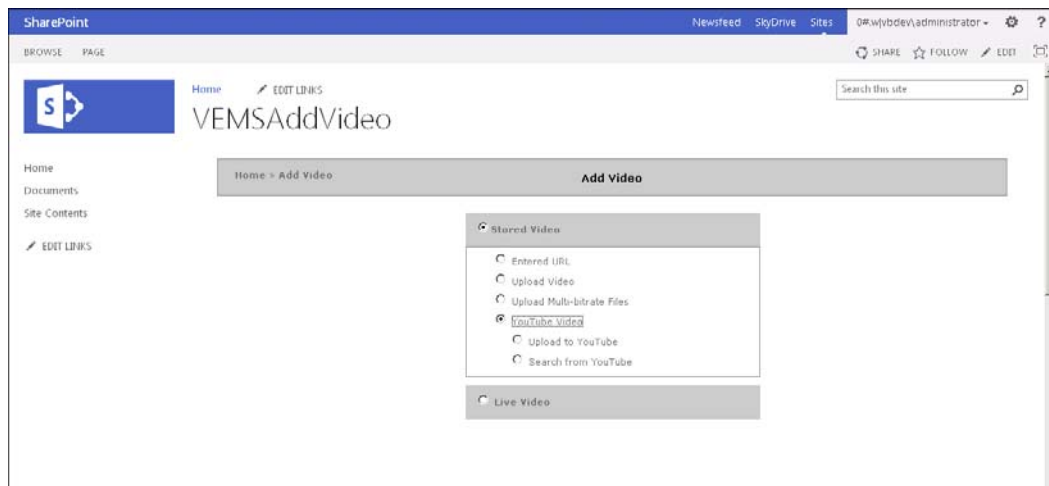


Figure 20. VEMS Add Video Page in SharePoint

VEMS Configuration

Default Configuration

Once installed, a default embedding configuration will be available. The default configuration consists of the following files:

Template file	ProgramFiles\VBrick\Maduro\VEMSWeb\Embedded\Templates\EmbeddedAddVideoTemplate.xml
Style files	Program Files\VBrick\Maduro\VEMSWeb\Styles\embedded\ (all files)

Modifying the Configuration

The `EmbeddedAddVideoTemplate.xml` file is the main configuration file. By adjusting this file we configure the behavior of the Embedded Add Video Widget. However, it is suggested that this file not be directly modified. Instead, create a duplicate of this file and modify the duplicate. This file manages what data overrides are passed into the embedded widget. Data overrides in the template file control the behavior of the widget. Available data overrides for the Embedded Add Video Widget are:

Required Data Overrides

<code>isEmbedded: true</code>	This value places the widget into embedded mode. It is set to true by default and must be true if used in any embedded environment. Do not use quotes around this value.
<code>embeddedTheme: 'embedded'</code>	This value represents the name of the style folder found in “Program Files\VBrick\Maduro\VEMSWeb\Styles\”. By default the value is “embedded” and will point to the default style folder of the same name. Should the admin create a new style folder and modify the look and feel they would point to that new folder name here. The folder MUST be located in “Program Files\VBrick\Maduro\VEMSWeb\Styles\”.

Optional Data Overrides

<code>embeddedCategory: 'category'</code>	This data override is not displayed by default and thus not initially active. If this value is specified, the end user will not be presented with a choice of what categories to apply to their added video. Instead, the category applied to new content will be the value specified in this field. The specified category must be an available VEMS category. In order to specify a subcategory, a "/" must be used. For example, the subcategory of "algebra" under "math" would be entered as "math/algebra." Only a single category entry is allowed but it can have multiple subcategories.
---	---

Modifying the Style/Theme

In order to change the look and feel of the embedded widget to match the embedding environment the style / theme must be modified. This is done by creating a custom theme. The easiest way is to duplicate the folder:

```
Program Files\VBrick\Maduro\VEMSWeb\Styles\embedded
```

And give it a new name. Let's assume that we've created a new folder called:

```
Program Files\VBrick\Maduro\VEMSWeb\Styles\newtheme
```

Enter the “newtheme” folder and modify the css files as needed to fit the embedding environment. Once complete, adjust the data override value for `embeddedTheme` to match

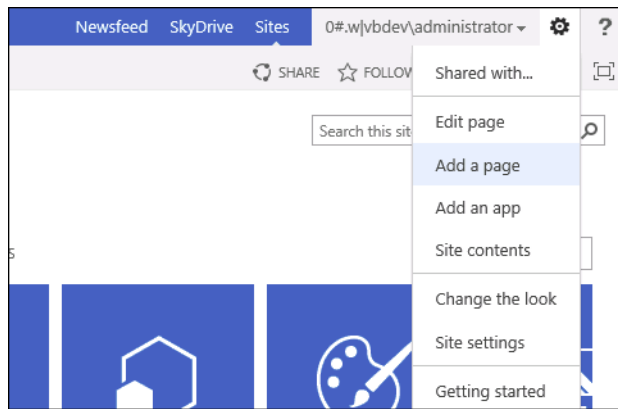
“newtheme”. Now your embedded widget will adopt the look and feel of the theme files in the “newtheme” folder. All custom theme folders must reside in:

Program Files\VBrick\Maduro\VEMSWeb\Styles

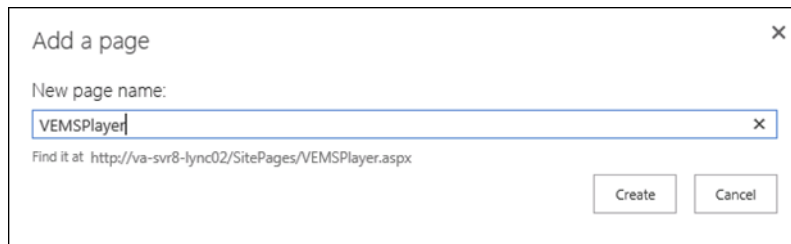
SharePoint Configuration

Now that our template file is created and our theme is set we must configure SharePoint to see the widget. This is done by using the “Page Viewer Web Part” in SharePoint 2010. There are many ways to add a web part to a SharePoint page. One of them is described below.

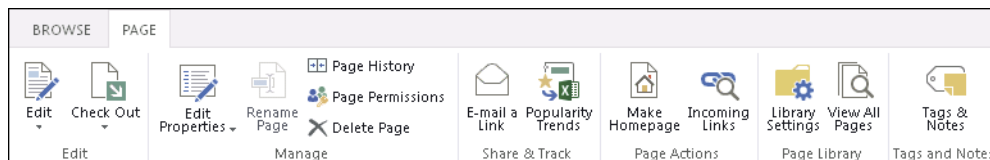
1. Log into SharePoint as user with ability to create a new "Site Page".
2. Click the gear icon at the top right of the screen and click **Add a page**.



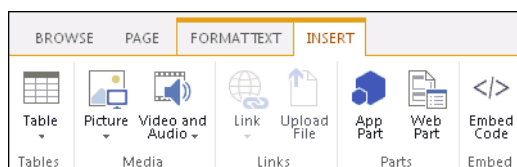
3. Give the page a name when prompted and click **Create**.



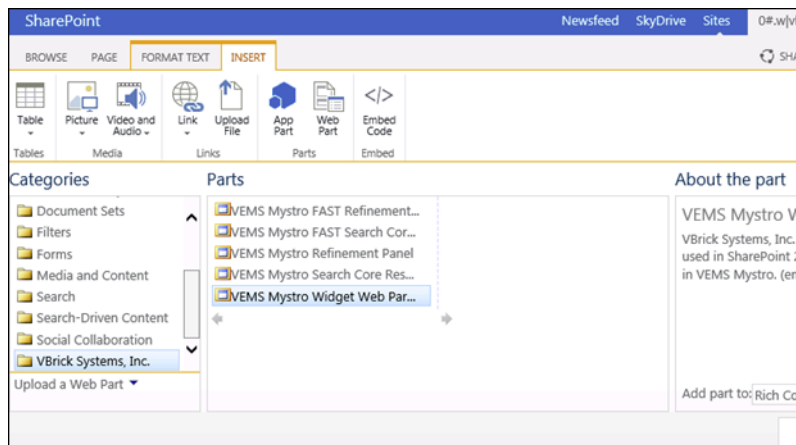
4. When the new page appears, click "Page" in the top bar to view Page tools, then click on the Edit icon.



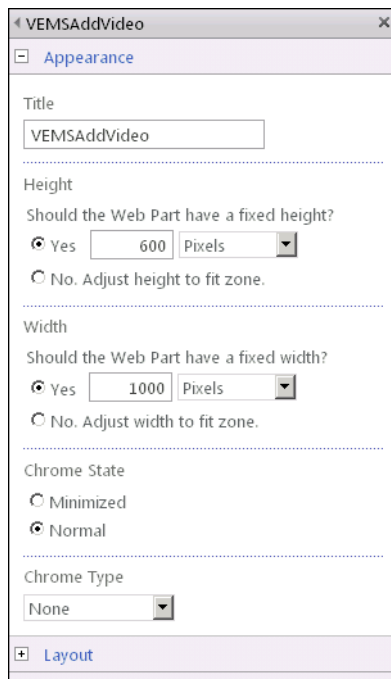
5. In the new menu that appears, move to the Insert tab of the Page tools and click WebPart.



6. Insert the VBrick player web-part using by selecting “VBrick Systems, Inc.” under Categories
7. Select “VEMS Mystro Widget Web Part” and clicking “Add”



8. Click on the VBrick web-part then click on the drop down arrow at the top right of the web-part container and select Edit Web Part.
9. In the “Page Viewer” settings, set the Link to <http://<VEMS 6.0 FQDN>/vemsweb/EmbeddedHost.html?VBTemplate=Embedded/>
 Note: If you are using a custom template be sure to replace “EmbeddedAddVideoTemplate.xml” with the name of your file as described in the section “Modifying Configuration”.
10. In the Appearance, set the height to 600 pixels and the width to 1000 pixels.



11. Click "OK".
12. The Embedded Add Video widget should now appear in your page. If you have security enabled you may see a log in prompt. Otherwise, the VEMS Add Video page will be displayed.

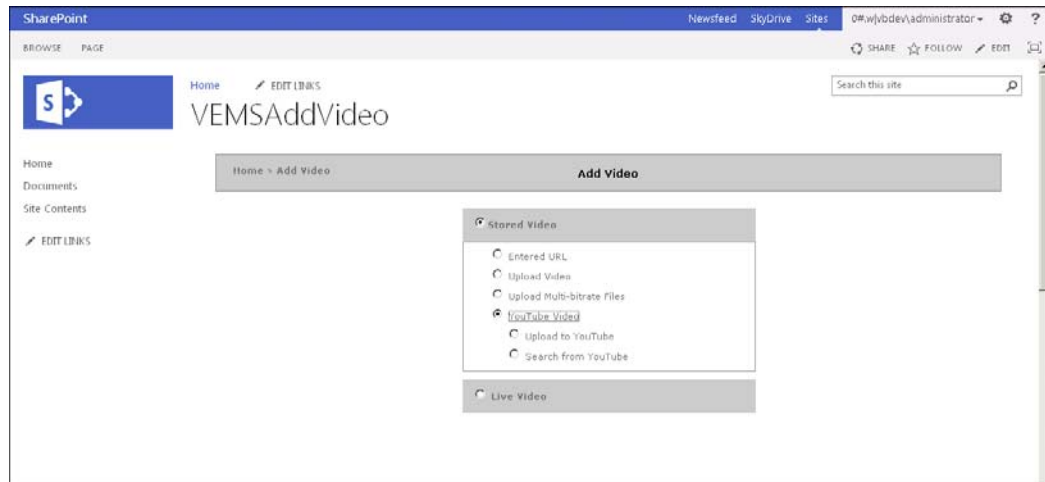


Figure 21. VEMS Add Video Page

Note Single Sign On (Windows Integrated Authentication) login is not compatible with JSONP. When using a widget in embedded mode in an SSO environment, it will make the login call using regular JSON. This may result in a cross-domain scripting error. To eliminate this error and still use the embedded widget, the VEMS server must be set as a Trusted Site on the client PC's Internet Explorer Trusted Sites setting.



VEMS Blackboard Integration

Overview	207
Blackboard Administrative Setup.....	207
VEMS Mystro LMS Configuration and Settings	209

Overview

The VEMS Mystro Blackboard integration module can be used to send stored and/or live video content information to Blackboard. For example, your users may choose to add a video in VEMS Mystro and then send that video’s URL to a specific course in Blackboard. This chapter describes the processes for configuring both the VEMS Mystro and Blackboard settings needed for this integration. For more information on how to use VEMS Mystro so that the desired content information is sent to Blackboard once you have configured your integration, view the VEMS Mystro *Portal Server v6.3.15 User Guide > Using Blackboard with VEMS*.

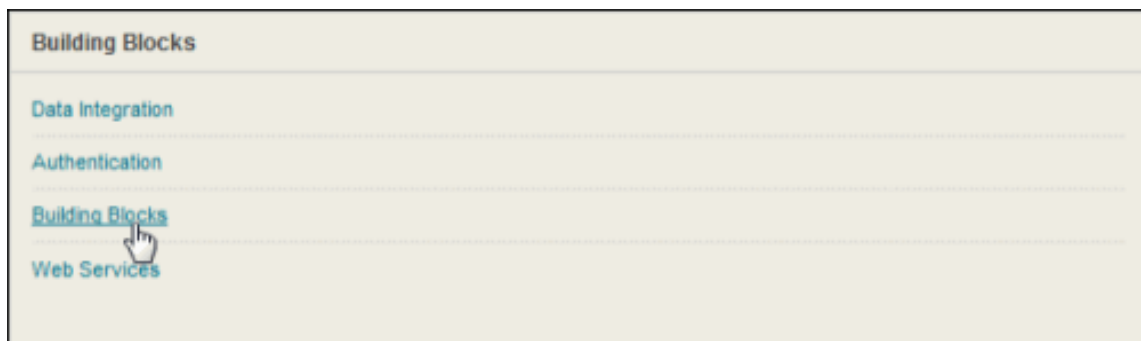
Notes This integration is specific to the Blackboard Learn platform release 9.1 or later.

Blackboard Administrative Setup

Before you may begin sending VEMS Mystro content to Blackboard, you must first install the VBrick Building Block on Blackboard.

▼ To install the VBrick Building Block, complete the following steps:

1. Log-in to Blackboard as a user with administrative privileges.
2. Click on **System Admin**.
3. Click on **Building Blocks > Building Blocks**.



4. Click on **Installed Tools**.

Building Blocks

Featured Building Blocks

Manage and install Featured Building Blocks

Installed Tools

Configure or Delete Building Blocks that were included with the system.

Proxy Tools

Manage and register Proxy Tools and define their Global Properties.

LTI Tool Providers

Manage and register LTI Tool Providers.

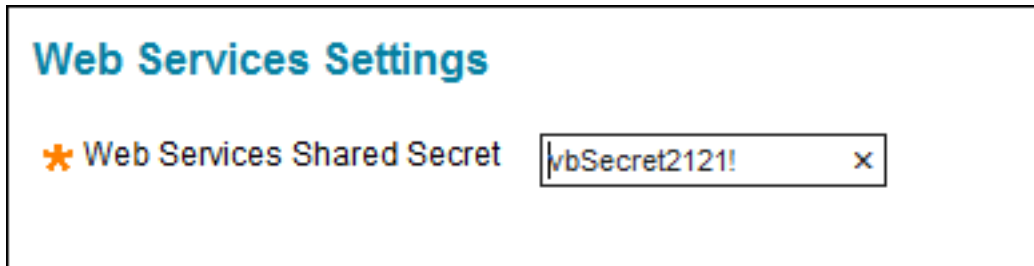
5. Click on **Upload Building Blocks**.
6. Click **Browse**.
7. Navigate to previously downloaded **VBrick Building Block** (vbrick-bb.war).

Notes The vbrick-bb.war file may be downloaded from the VBrick [Downloads](#) page.

8. Click **Submit**.
9. Locate the VBrick Plugin in the list of Building Blocks that now appear.
10. Open the drop-down menu and click on **Set Available**.

Software Updates	Blackboard Inc.	2.5.0	Available	! New Update Available
Stream Views	Blackboard Inc.	9.1.110082	Available	? No Info Available
<input type="checkbox"/> Text	Blackboard Inc.	9.1.110082	Available	✔ Up to Date
<input type="checkbox"/> Time	Time	9.1.110082	Available	? No Info Available
<input checked="" type="checkbox"/> VBrick Plugin	VBrick Systems Inc.	1.0.0	Inactive	? No Info Available

11. On the Make Building Block Available page, click **Approve**.
12. Open the drop-down menu and click **Settings**.
13. Enter a value for the **Web Services Shared Secret** field under Web Services Settings, seen below. *Remember this value.* This is a unique key that you will use again in the LMS Shared Secret field during VEMS Mystro LMS Configuration and Settings setup in the next section for peer-to-peer authentication.



Web Services Settings

* Web Services Shared Secret

14. Click **Submit**. You must now perform the required setup tasks in VEMS Mystro before you may begin using your Blackboard integration. These are explained in the following section.

VEMS Mystro LMS Configuration and Settings

Before content in VEMS Mystro can be integrated with Blackboard, the LMS integration must be enabled and configured in VEMS.

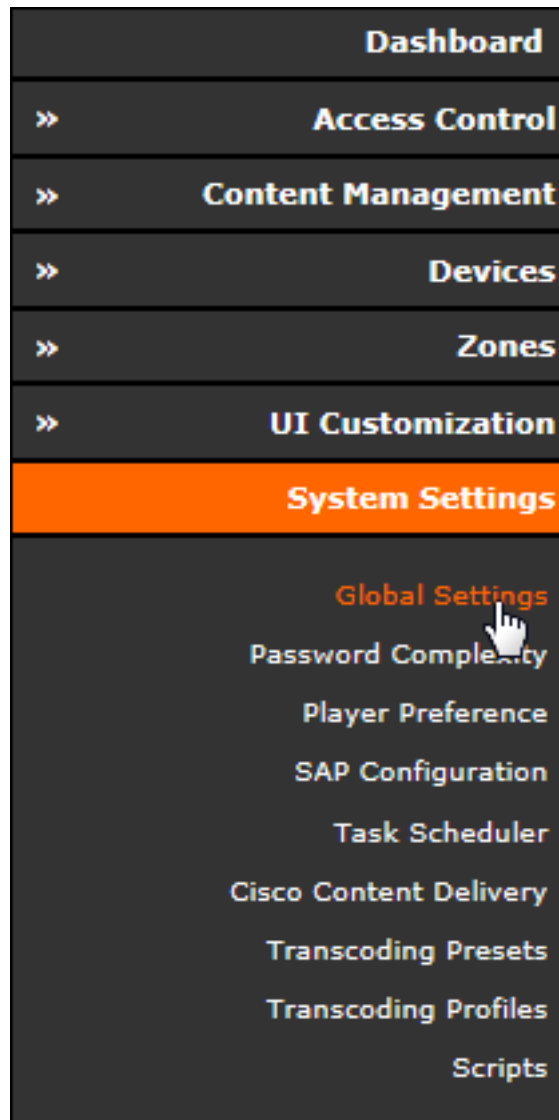
There are two steps to configuring your LMS integration in VEMS:

- Define your global settings.
- Configure your custom field settings.

Both are discussed in more detail below.

Define VEMS Mystro Global Settings

- ▼ To define the VEMS Mystro global settings, complete the following steps:
 1. Open a Web browser and enter the URL to your VEMS server.
 2. Log-in to the Administrative interface.
 3. Click on **System Settings > Global Settings** and scroll down to the LMS Section.



- ▼ Define the LMS settings as follows:
1. **Enable Integration** - Select this checkbox.
 2. **LMS User Name** - This user name should be the user in Blackboard that will be responsible for authenticating the incoming video content from VEMS Mystro.
 3. **LMS Password** - Enter the password for the LMS User Name account.
 4. **LMS URL** - Specify the URL that will be used to send the data to the Blackboard Building Block. Example: `http://10.10.7.56/webapps/vb-vbrick-bb-BBLEARN/service/content`
 5. **LMS Custom Field Name - Course ID** - Define the desired name of the field where your users will enter the Blackboard Course ID that they want content sent to. You will create and configure this field in the next section. This field should be a descriptive name that leaves no doubt as to what your users will be entering in the field. For example, you might title this field, "LMS Course ID", to indicate to your users that they will enter the course ID in this field so that VEMS content may be integrated if desired. As noted, once this field is defined, it must be added and configured. This is explained in the next section.

6. **LMS Custom Field Name - Send to LMS** - Define the desired name of the field where your users can specify if the content they are tagging and/or adding should or should not be integrated with the Blackboard course ID specified. You will create and configure this field in the next section. For example, you might title this field, "Send to LMS". As noted, once this field is defined, it must be added and configured. This is explained in the next section.
7. **LMS Shared Secret** - Enter the same value here that you entered in the **Web Services Shared Secret** field during Blackboard Administrative Setup. This is a unique key that is used for peer-to-peer authentication.

The screenshot shows the LMS configuration interface with the following fields and values:

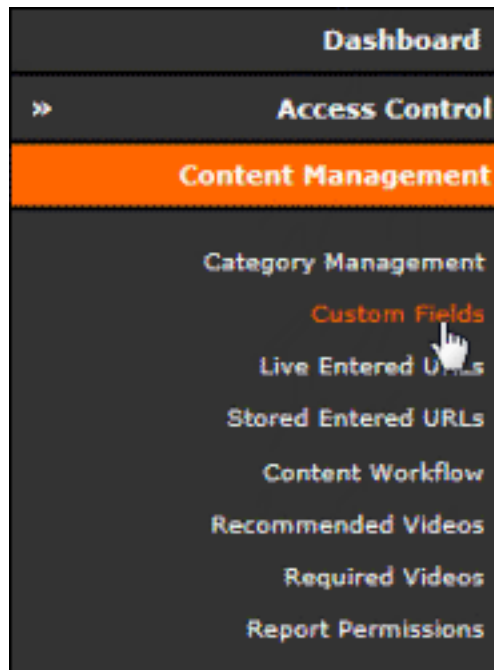
Field Name	Value
Enable Integration	<input checked="" type="checkbox"/>
LMS User Name:	TButcher
LMS Password:	••••••••••
LMS URL:	http://10.10.7.56/webapps/vb-vbrick-bb-E
LMS Custom Field name - Course ID:	LMS Course ID
LMS Custom Field name - Send to LMS:	Send to LMS
LMS Shared Secret:	vbSecret2121!

8. Once **LMS** settings are defined, the final step in **Global Settings** is to define the local hostname. In the **Server Hostnames** section, set the **Local Static Hostname** field. This field *must* be set to the VEMS server hostname or IP address (do not use http://).

Configure VEMS Mystro Custom Fields

Once you have defined your fields in Global Settings, you must then add and configure them in custom fields. Recall that you defined two fields; one for LMS Course ID, a text field, and one for Send to LMS, an option field that will allow the user to choose yes or no (and synchronize the course to the LMS as a result).

- ▼ To add and configure a custom field, complete the following steps:
 1. Open a Web browser and enter the URL to your VEMS Mystro server.
 2. Log-in to the Administrative interface.
 3. Click on **Content Management > Custom Fields**. The Custom Field Administration form appears.



4. Add a new field for the **LMS Custom Field Name - Course ID** defined in the previous section:
 - Click the **Add New Custom Field** button.
 - **Select Field Type** - Select **Text**.
 - **Field Name** - Enter the value you defined in Global Settings. In our example, we use LMS Course ID.
 - Click the **Submit** button to add the field.

Note: The **Submit** button will change to **Update Name** if you are modifying the name of the field as opposed to adding a new field.

5. Next, add a new field for the **LMS Custom Field Name - Send to LMS** field that was defined in the previous section to indicate if the content should be sent to Blackboard:
 - Click the **Add New Custom Field** button.
 - **Select Field Type** - Select **Option**.
 - **Field Name** - Enter the value you defined in Global Settings. In our example, we use Send to LMS.
 - Click the **Add Options** button.
 - Enter "YES" and click **Submit**.

- Enter "NO" and click **Submit**.
- Click the **Finish** button to add your new option field.

Add/Edit Fields:

Select Field Type:

Field Name:

Option Value	Edit	Delete
1. YES		
2. NO		
3. <input type="text"/>	<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>

Note: You may click the **Edit** and **Delete** buttons next to either option to edit or delete an option.

Your users are now ready to begin synchronizing both live and stored content to Blackboard courses. View the *VEMS Mystro Portal Server v6.3.15 User Guide* for more information.

VEMS Lync Integration

Overview	215
Add the DME Lync as a Presentation Device	216
Schedule a Lync Meeting Event Type	218

Overview

Microsoft Lync meetings are now able to be broadcast to more than 250 users when integrated with your DME and VEMS. The DME integrates Lync servers and clients while VEMS schedules Lync meetings and displays presentation pages to attendees through Scheduler. VEMS is also able to leverage existing VEMS zone logic features for all your Lync meetings.

You must purchase a Lync Broadcast system license for your DME before you will be able to integrate Lync with your DME and VEMS. Further, your DME must be set up to integrate with Lync and a “DME Lync User” created as well.

See: DME Admin Guide > Lync Broadcast for more information on how to do this.

Three features are included as part of the Lync Broadcast integration with VEMS and a DME. They are:

1. Lync conference set-up with up to five Lync participants and one DME Lync User.
2. Lync conference chat enabled in a separate window when viewing a Lync conference.
3. A VBrick provided plug-in for Lync which enables desktop sharing to be streamed to the DME so that VEMS can then display the stream as part of the Lync conference.

If the Lync Broadcast integration has been enabled and a Lync conference has been set up, the DME Lync User may be invited to the conference and stream the active speaker’s stream to thousands of users viewing the DME stream. Further, the Lync conference may be recorded through Lync/Microsoft and migrated into VEMS for later viewing if desired as well.

The steps to begin a Lync Streaming Broadcast Meeting are:

1. Set Up your DME for a Lync Integration. (DME Admin Guide > Lync Broadcast). This will include setting up a Lync user for your DME and running a VBrick provided utility used to identify the DMEs host name and SIP address via Active Directory. This is important to distinguish between multiple DMEs on a network.
2. Add the DME Lync as a Presentation Device in VEMS once it is set up.
3. Schedule a Lync Meeting Event Type in VEMS Scheduler after adding your DME Lync presentation device.
4. Start a Video Conference in Lync with a DME User once you start your Lync Meeting event.

Notes This integration is specific to Microsoft Lync 2013 or later.

Add the DME Lync as a Presentation Device

You must add the DME you have configured for a Lync integration as a presentation device in VEMS.

▼ To add a DME Lync as a Presentation Device:

1. Navigate to Admin > **Devices** > **Presentation Devices** > **Add Presentation Device** > **Presentation Device Model** > **DMELync**.

Hostname	Hostname of the DME used for Lync integration
IP Address	IP Address of the DME used for Lync integration
Software Revisions	Not used at this time.

2. Any DME to be used with Lync must be of type **DMELync** because VEMS presently does not allow the same DME to be added as a second presentation device. The DMELync designation alleviates this issue.
3. Further, when DMELync is selected as the presentation device model type, the **Streams** tab will create a stream titled **Lync Meeting** (seen below). This stream is not editable nor are any other streams able to be created for this presentation device.

Stream Name	Stream	Type	
1. Lync Meeting	1	DMELync	Stream for DMELync type device cannot be edited/deleted

4. You may configure all daisy chained DMEs on the Viewing URLs tab. This will apply zone logic for these streams when attendees view the meeting through VEMS.

Stream Name	A Stream Name should be configured for the Lync Meeting as well. It will appear automatically in the Stream Name dropdown.
URL	The URL should include the following format. Note that “lync://” must be present before the DME host name or IP address: <code>lync://<DME_HOSTNAME_OR_IPADDRESS></code>
Source IP	The DME IP address
Bit Rate	Not used for Lync Meetings
Encoding Type	H264 or Flash
Is Multicast URL	Not used for Lync Meetings

5. A **Chat** tab is created for DMELync presentation devices that is used to configure the DME Chat server.

Chat DME Hostname/IP Address	The Chat DME Hostname/IP Address field should include the IP Address of the DME Lync DME and the port of the DME Lync in [IPAddress]:[Port] format. You may obtain the port of the DME Lync from the Lync Chat Port field in the DME. DME Admin Guide > Lync Broadcast for DME set up steps. The default port number is 6789.
------------------------------------	---

Once your DME Lync presentation device has been added, you may schedule a Lync Meeting in the VEMS Scheduler.

Schedule a Lync Meeting Event Type

Once Microsoft Lync has been integrated with VEMS, a Lync Meeting may be scheduled in VEMS Scheduler so that it may be broadcast to your users who attend the meeting.

▼ To schedule a Lync Meeting in Scheduler:

1. Navigate to User > **Home** > **Scheduler**.
2. Schedule a new event.

Event Type	Lync Meeting
Event Name	What you will title your Lync Broadcast meeting
Description	Description of the Lync Broadcast meeting.
Time Zone	Time zone the event will take place in.
Start / End Date(s)	The start/end date(s) and time of the event. If you enter a start and end date for the event, it will require a host or moderator to start it. Click the Now button to enter the current time and day. You may use the Duration fields to modify these dates as well. These fields are not present if the Is Permanent checkbox is selected.
Is Permanent	This checkbox should be selected if the meeting is always on. A host/moderator is not needed to start the meeting as is the cast for a live Webcast.
Anonymous	Disables authentication for users who log in via an auto-generated email link. Often used for large Webcast events to speed up the log in process.

Disable view count	Improves performance by disabling the Logged In Viewers counter on the Live Webcast Presenter page. Often used for large Webcast events.
Disable Play content Activity	Improves performance by disabling the Play Activity report. Often used for large Webcast events.

- In the **Devices** section, all presentation devices of model designation "DME Lync" will be displayed. Click the **Select This Device** button next to a specific device to use it for your meeting. You will be alerted if any device conflicts occur such as scheduling conflict.

Device	
Lync Meeting <input type="button" value="Select This Device"/>	Host Name: Lync-Broadcast-DME IP Address: 172.22.2.193 Stream: 1 Encoding Type: H264
Lync Meeting <input type="button" value="Select This Device"/>	Host Name: 10.10.0.133 IP Address: 10.10.0.133 Stream: 1 Encoding Type: H264

- Once your Lync Meeting is created, it will appear in the Event Calendar and you will be able to see the URL when it is accessed on the Calendar page. Before you begin the meeting, however, you should [Start a Video Conference in Lync with a DME User](#).

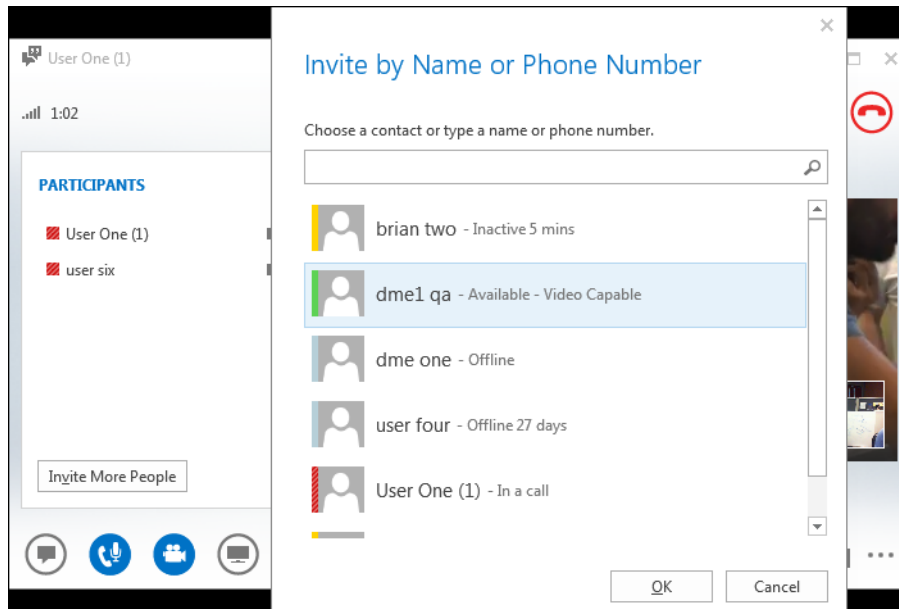
Scheduled Event	
Event Name:	Weekly Project Managers Meeting - Lync Broadcast Event
Event Type:	Lync Meeting
Start:	Thursday, August 14, 2014 2:30:00 pm
End:	Thursday, August 14, 2014 5:30:00 pm
Duration:	Hours: 3 Minutes: 0 Seconds: 0
Recurring:	No
Occurrence Number:	N/A
Owner:	Default Administrator
Anonymous View Link:	http://172.22.2.152/VEMSWeb/VEMSHost.html?VBTemplate=Templates/LyncMeetingAnonymousTemplate.xml&contentID=553
Description:	Weekly PjM meeting is now Lync broadcast enabled to easily distribute weekly goals to entire company on an ongoing basis.
<input type="button" value="Create New Event"/> <input type="button" value="View Event"/> <input type="button" value="Reschedule Event"/> <input type="button" value="End Event"/> <input type="button" value="Cancel"/>	

Start a Video Conference in Lync with a DME User

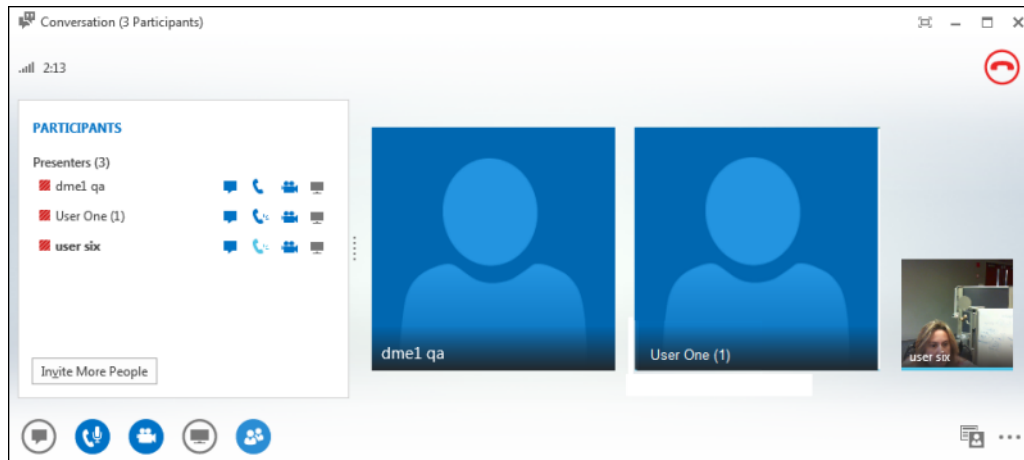
To stream your Lync video meeting to your VEMS event, you must start a Lync video conference and invite your DME Lync User first.

Note View [Microsoft Lync](#) documentation if you are not sure how to set up and use Lync video conferencing.

- ▼ To start a video conference and invite a DME user:
- 1. Start a video conference in Microsoft Lync and invite the DME user you created in Active Directory into the call.



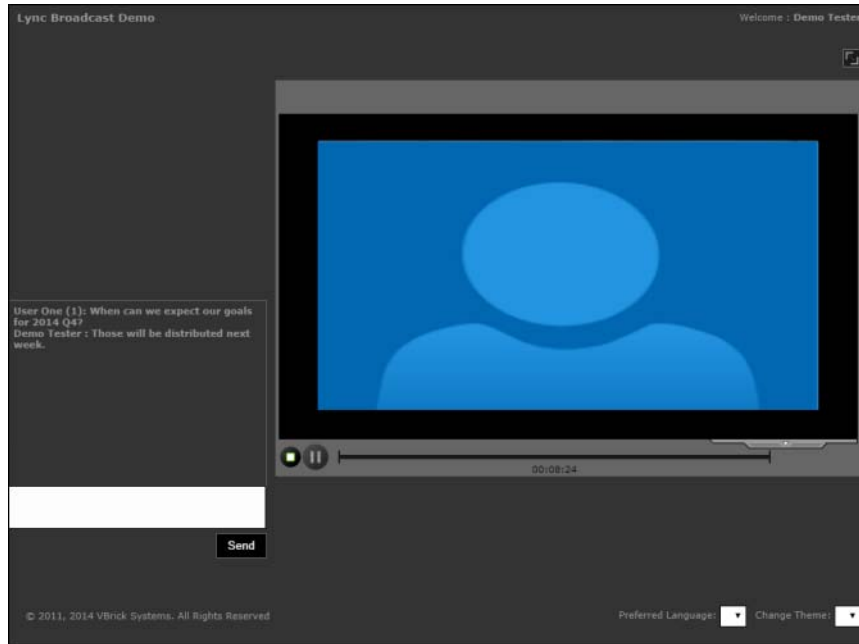
- 2. The DME user will be shown as a participant in Conversation list.



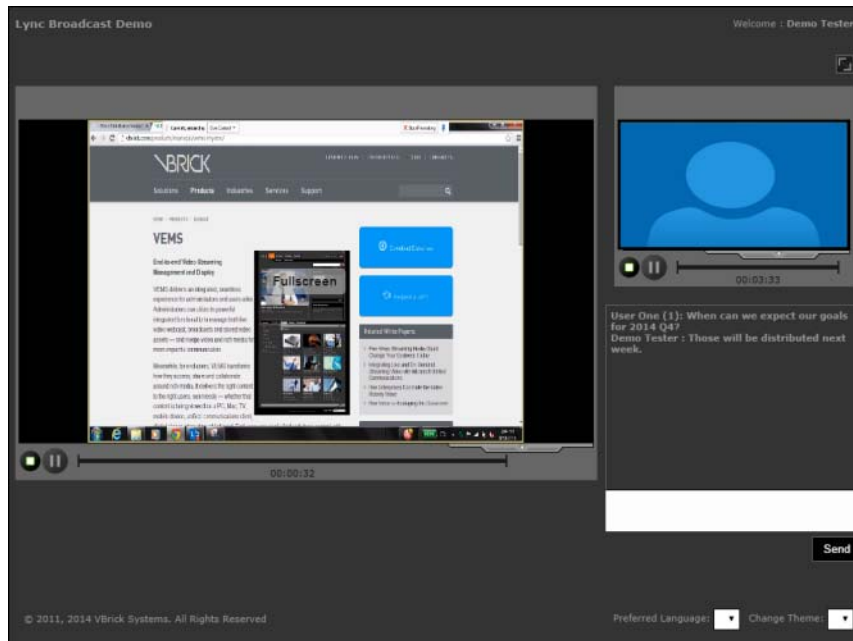
- 3. Click the desktop sharing button in Lync and share the desktop. You will see a "transmitting" icon in the system tray to indicate you are broadcasting your screen. The VBrick plug-in icons are:

	VBrick Lync screenshare plug-in is active.
	VBrick Lync screenshare plug-in is active and transmitting.
	VBrick Lync screenshare plug-in is not transmitting and an error has occurred. For example, it may be as simple as Lync not running or you may need to check the Windows Event Viewer > Application logs for VBrick exceptions.

4. Now that the Lync video conference with the DME user has been initiated, the Lync Event in VEMS that has been set up may be started and broadcast. See the previous topic: [Schedule a Lync Meeting Event Type](#).
5. VEMS users should expect to see Webcast events as they normally would. Lync Meetings with no presentation uploaded will have video appear next to a chat window in large format similar to the image below.



6. Lync Meetings that contain presentations will be viewed with the presentation appearing larger than the Presenter window, similar to the view seen below.



7. Note that the Presenter view displays the active speaker which is based on the person talking loudest.

-
8. You may also utilize chat features in Lync and they will appear in the VEMS Lync Event and vice versa.
 9. Once the conference has ended, you may upload your Lync recorded video into VEMS for later VOD viewing.

Configuring for SSL

Overview	223
Configuring SSL.....	224
Disabling SSL for the Poodle Vulnerability	232
Configuring Secure FTP	232

Overview

Secure Sockets Layer (SSL) provides endpoint authentication and communications privacy over the Internet using cryptography. Whenever there is a concern regarding confidentiality 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 all pages in the Portal Server Admin and client applications. **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 will be encrypted as follows:

- VEMS Admin Console – All pages in the management interface pages will be encrypted to protect management information and other sensitive data.
- VEMS User Portal – All Portal Server client pages will be encrypted along with the login page.
- 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. See [Using LDAP with SSL](#) on page 81 for related information.
- VOD-W Server – Communication between the Portal Server and a VOD-W server *only* can be encrypted by enabling SSL on the VOD-W server. See "Secure Communication" in the *VOD-W Server Release Notes*.

Note When configuring for SSL, you must request and obtain a valid X.509 certificate, *in advance*, before you can install it on the Portal Server. You will also need to configure IIS in Windows Server 2008 *before* you run the script that enables HTTPS.

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 in IIS.
 5. Enable HTTPS.

SSL Prerequisites

- In order to use the Portal Server in secure (HTTPS) mode, you must have a signed and valid SSL certificate purchased from a trusted Certificate Authority (e.g. Verisign or another vendor) or at least a self-signed certificate. If the certificate is not signed, or if it is expired or otherwise invalid, video playback issues will occur.
- Be aware that SSL encryption requires significant resources and can substantially impact performance. Use SSL only when absolutely necessary in environments that require all pages to be encrypted.

Configuring SSL

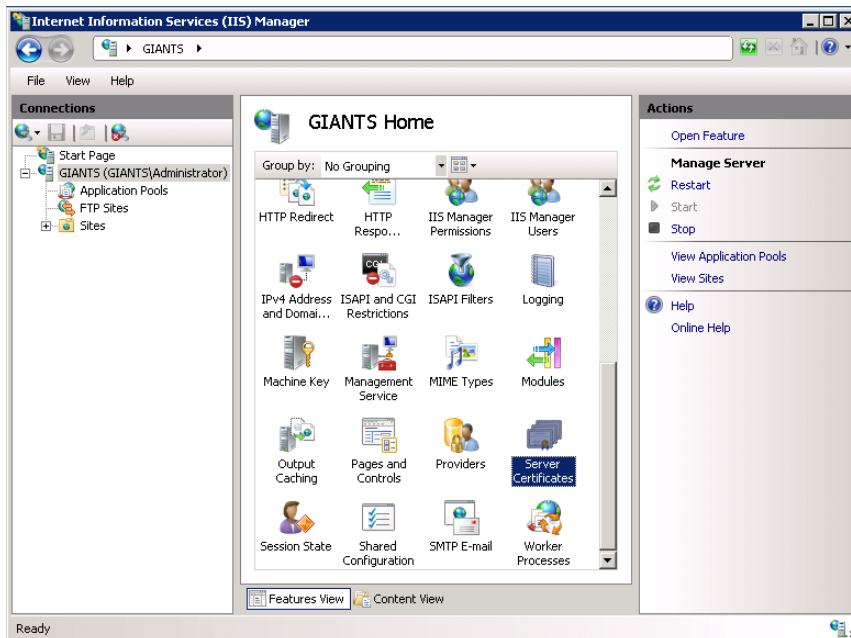
The following procedure explains how to configure SSL on Windows Server 2008.

1. Generate a Certificate Request

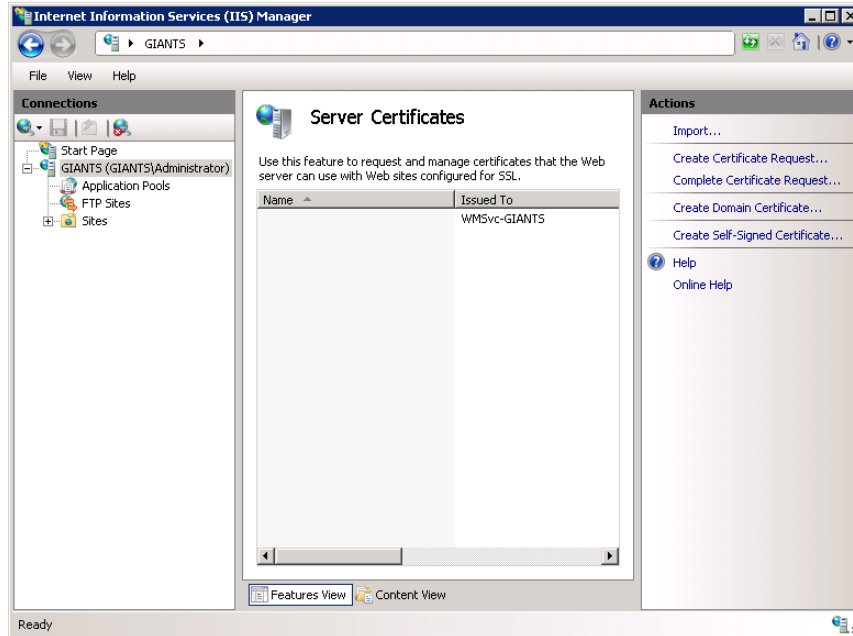
If your company does not have a X.509 certificate, or does not have one for the Portal Server, a new certificate request must first be created.

▼ 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 extremely important because it must exactly match the domain name you will be using to connect to the server regardless of whether it is a wildcard certificate or for a specific subdomain.)
6. Enter the appropriate information in the **Country/Region**, **State/Province**, and **City/locality** fields, and then select **Next**.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

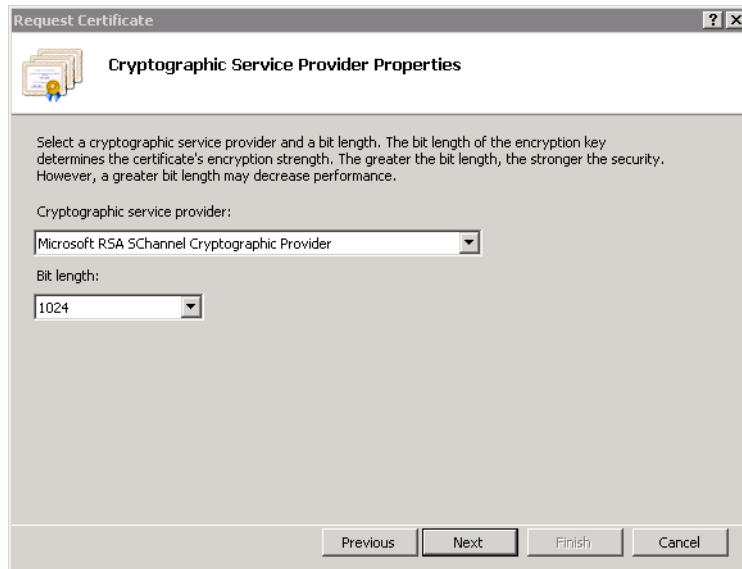
City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

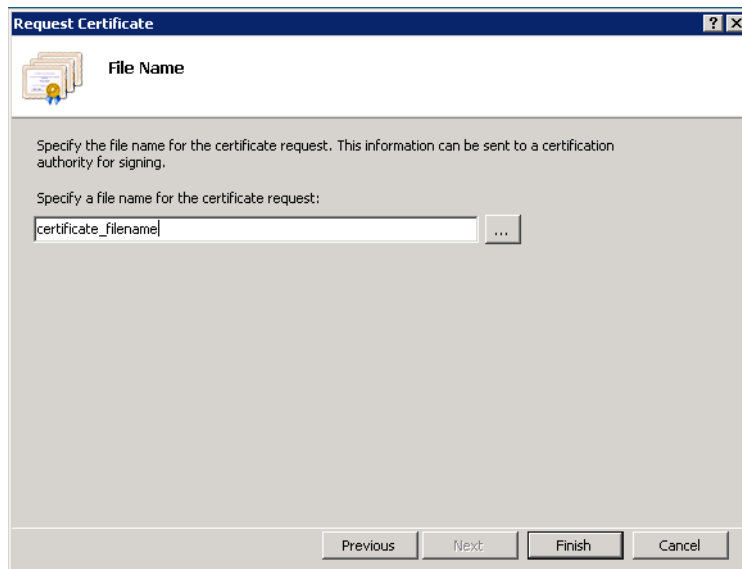
7. Select a **Cryptographic Service Provider** and **Bit Length** and click **Next**.



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.

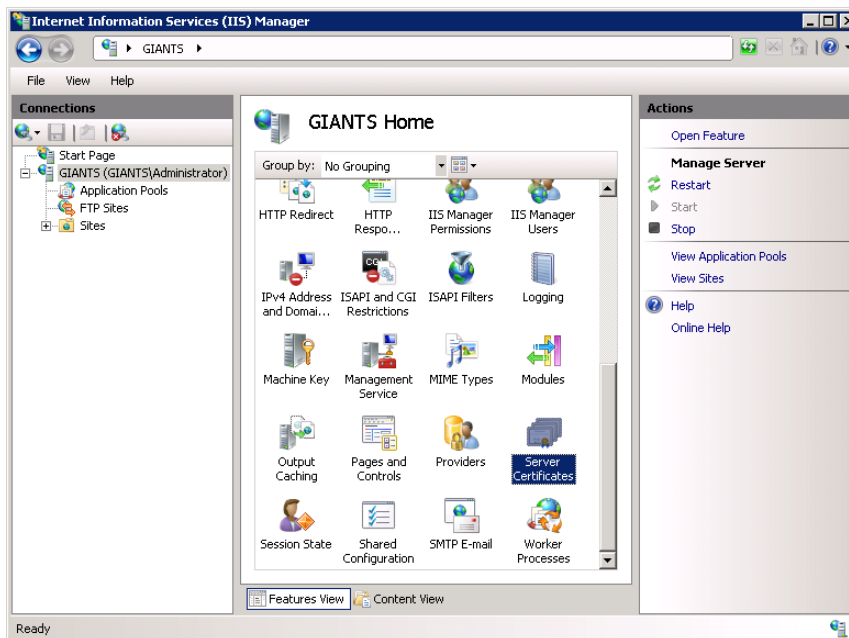
2. Submit a Certificate Request

If a CA-signed Certificate from a trusted Certificate Authority (such as [VeriSign](#) or [Thawte](#)) 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.

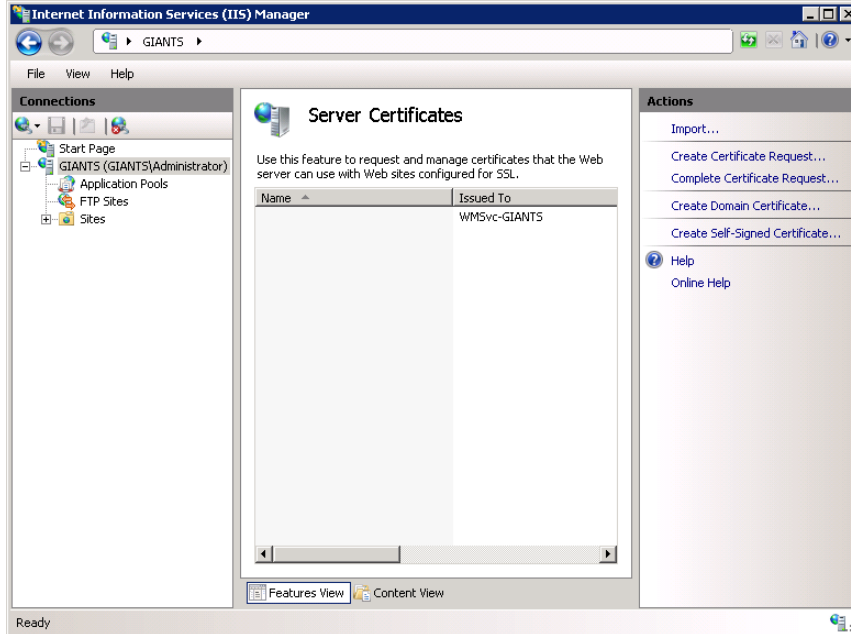
Note To use SSL, the certificate installed must be CA-signed, not self-signed. This is regardless of whether a certificate representing this server already exists or you are purchasing one now.

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**.



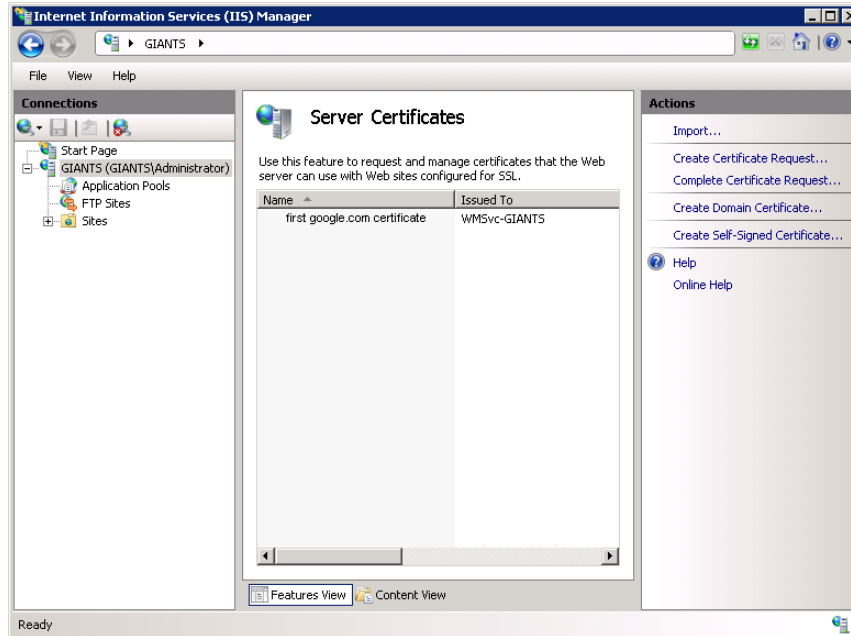
3. In the Actions column on the right, click on **Complete Certificate Request ...**



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.



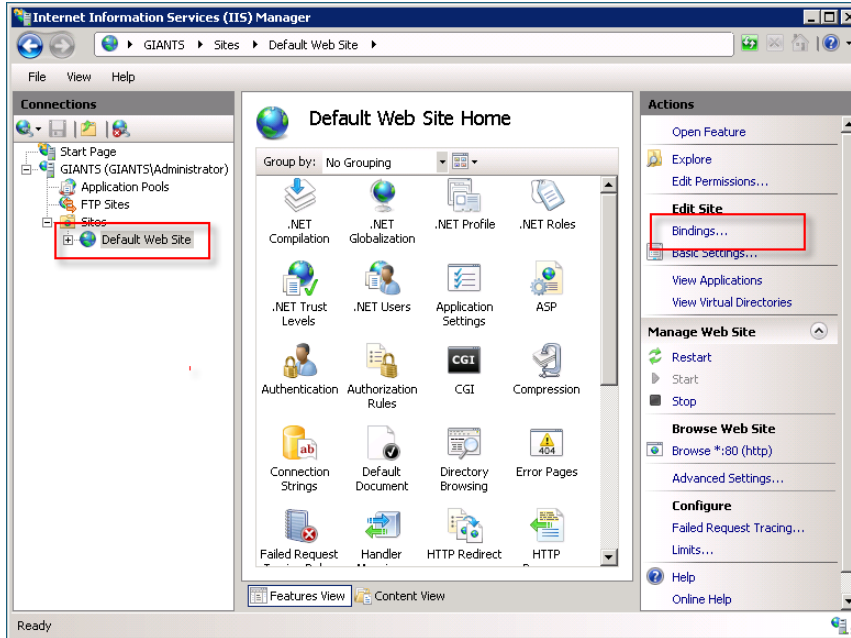
6. Examine the certificate overview, click **Next**, and then click **Finish**. A certificate is now installed on the VEMS Portal Server.

4. Configure Portal Server Resources for SSL in IIS

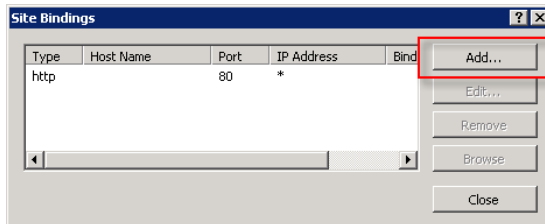
After installing the certificate on the Portal Server, the Portal Server can now be configured for SSL. When properly configured, all pages in the Portal Server Admin and Portal Server client applications are secured with SSL. Users will see the padlock icon at the bottom of the screen on all pages. **Be aware that SSL encryption requires significant resources and can substantially impact performance.** Use SSL only when absolutely necessary in environments that require all pages to be encrypted.

▼ To configure the Portal Server for SSL:

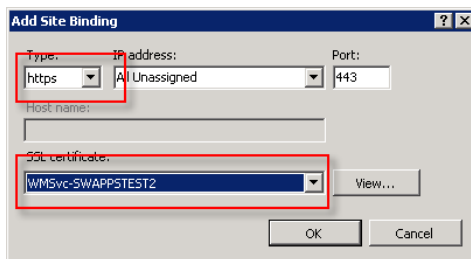
1. Login to the Windows Server that is hosting the VEMS Portal Server application with a valid local Windows administrator account or domain account with local administrative permissions.
2. Launch the Internet Information Services Manager. Go to Start > Control Panel > Administrative Tools > Internet 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:



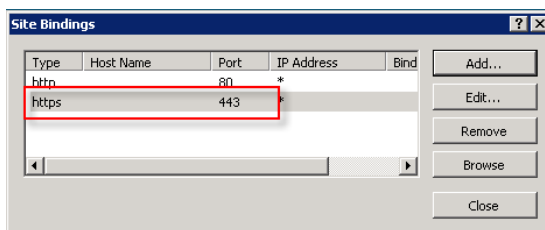
6. Click on **Bindings** in the right column and then click the **Add** button.



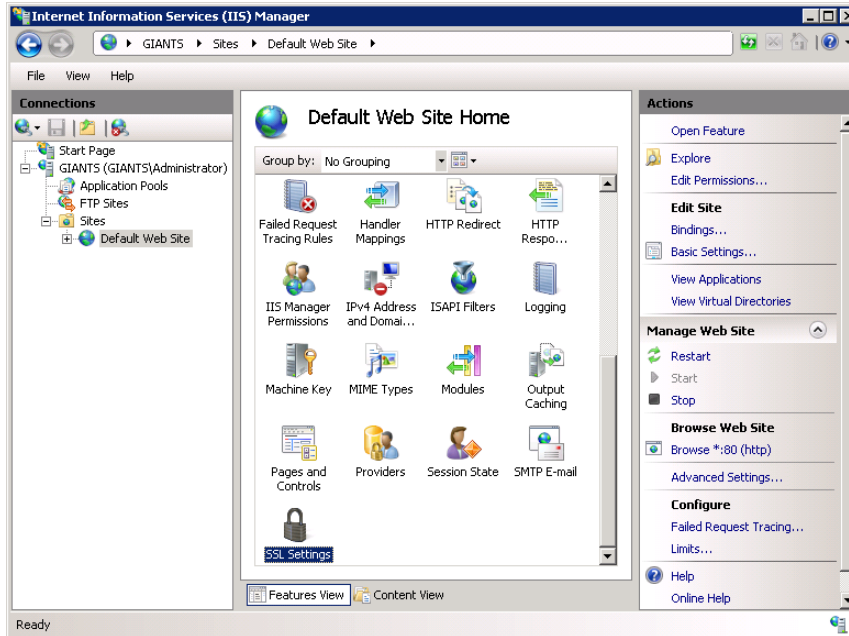
7. Change the **Type** to **https**. Then select the SSL certificate you just installed and click **OK**.



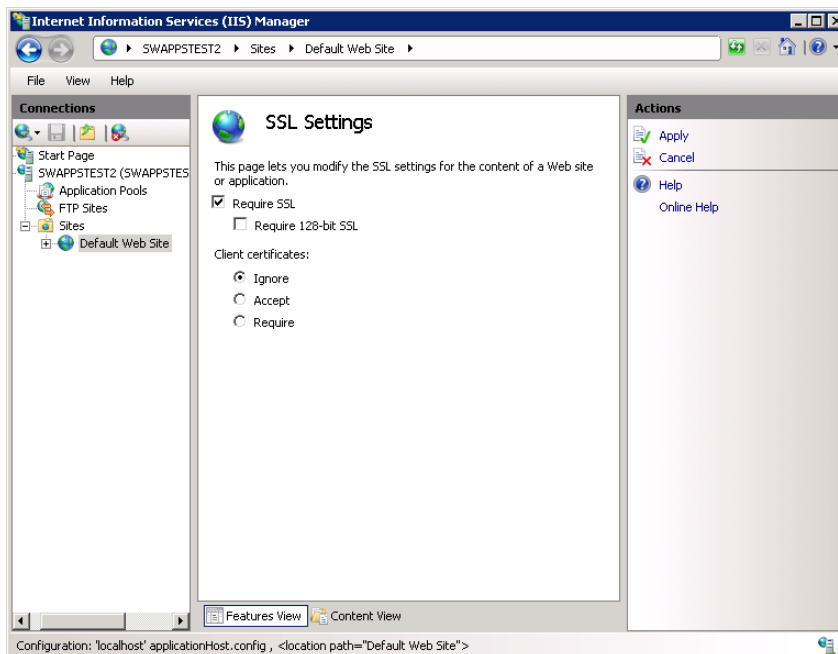
8. You will now see the binding for Port 443 listed. Click **Close**.



9. Double-click the **SSL Settings** button.



10. Select **Require SSL** and click **Apply**.
11. Go to **Default Website > VEMSWEB > VODMulticastFiles**, click on **SSL Settings**, and uncheck **Require SSL**.



12. Restart the Windows Server 2008 machine.

5. Enable HTTPS

13. Enable HTTPS. To enable (or disable) HTTPS, you will also need to (1) run the [MaduroSSLSettings.exe](#) script and (2) enable SSL in IIS. See [Enable/Disable Single Sign-On and HTTPS/FTPS on page 80](#) and [Enable/Disable HTTPS in IIS on page 80](#) for complete details.

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.

Disabling SSL for the Poodle Vulnerability

The Poodle vulnerability (CVE-2014-3566 and CVE-2014-8730) will affect VEMS as it impacts any communication using SSL 3.0 when using “Https”.

To mitigate this vulnerability, it is recommended that SSL 2.0 and SSL 3.0 are disabled on the Web server where VEMS is installed (Note this may impact clients using lower versions of SSL when communicating with the server).

- ▼ To disable SSL 2.0 and SSL 3.0, edit the registry on Windows server as follows (this works for Windows server 2003 to 2012):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server] "Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server] "Enabled"=dword:00000000
```

- ▼ For additional security, disable weak ciphers by editing the registry as follows:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56] "Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL] "Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128] "Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128] "Enabled"=dword:00000000
```

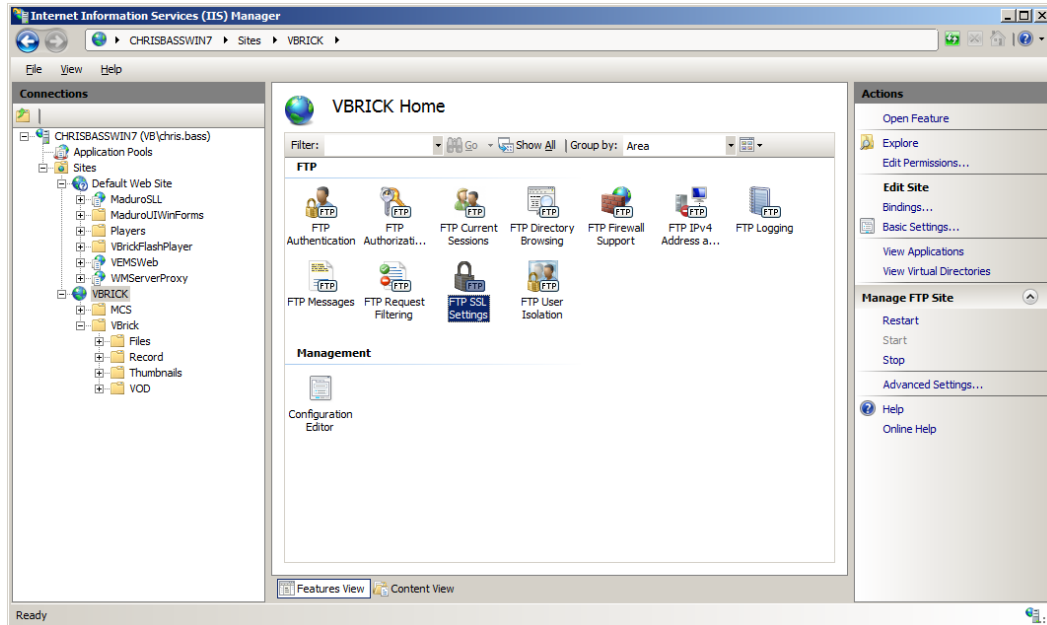
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128] "Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128] "Enabled"=dword:00000000
```

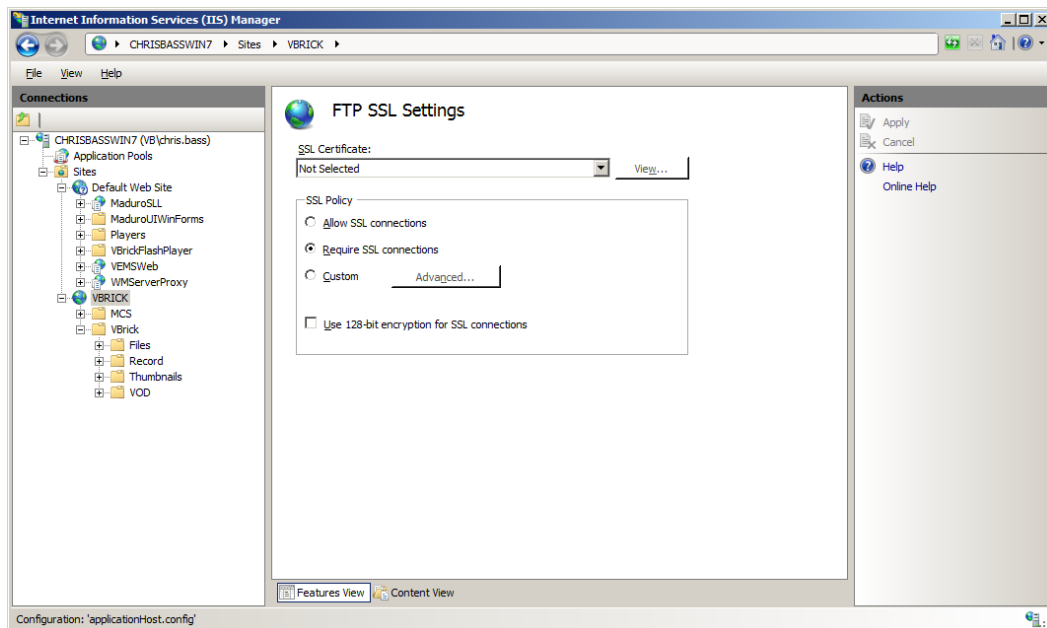
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128] "Enabled"=dword:00000000
```

Configuring Secure FTP

- ▼ To configure for Secure FTP:
 1. Open IIS. Go to Start Administrative Tools > Internet Information Services (IIS) Manager.
 2. Select the `VBRICK` FTP server.
 3. Select **FTP SSL** Settings on the right.



4. Select **Require SSL connections**.
5. Select your **SSL Certificate** from the dropdown.



6. When done click **Apply** on the right.



Network Video Recording

NVR Overview 235
 Using an NVR 236

NVR Overview

The Network Video Recorder (NVR) provides a mechanism to perform multiple simultaneous recordings of live streams coming from VBrick encoders. The NVR provides the ability to record live streams from the network and store these recorded video files on a specified location. It records H.264, Windows Media, MPEG-2, and MPEG-4 streams. NVR resources can be scheduled via the VEMS Scheduler module and you can add multiple NVRs depending on your requirements. An NVR can also be used with VBrick's Video Conferencing Gateway to record and deliver video conference audio and video to other elements in the VBrick ecosystem. For more about this see the *Distributed Media Engine (DME) Admin Guide*.

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 scale to 10 or 40 seat licenses to offload recording tasks and improve overall performance. Additional NVR licenses are cumulative within the system e.g. 10 + 10 = 20 NVR slots. As explained below, the NVRs are delivered in several different configurations.

Table 31. NVR Models

NVR Type	Description
NVR 10	Software only. Supports 10 simultaneous recordings. Runs on the VEMS Mystro server or on a server which may include a VEMS Transcoder.
NVR 10	Software and hardware. Supports 10 simultaneous recordings. Runs on a high performance server which may include a VEMS Transcoder.
NVR 40	Software only. Supports 40 simultaneous recordings. Runs on the VEMS Mystro server or on a dedicated server.
NVR 40	Software and hardware. Supports 40 simultaneous recordings. Runs on a dedicated high-performance server which may include a VEMS Transcoder.

The NVR is tightly integrated with the Portal Server and the Scheduler and provides these standard features.

- Multiple simultaneous recordings – Enables 10 or 40 simultaneous streams per license on master server or standalone server. These licenses are cumulative and can be divided among several servers in a multi-server environment.
- Format independence – Records H.264, Windows Media, MPEG-2 and MPEG-4 formatted video streams

-
- On-network recording – Leverage your IP network with a software-only NVR offering or deploy in conjunction with hardware recorders such as VBrick encoders or the Distributed Media Engine (DME).
 - Application flexibility – Designed to be easily integrated into the VEMS Mystro scalable architecture. NVRs also can be deployed as standalone recording units enabling applications such as continuous news archiving.

Using an NVR

When a recording is initiated using the "record" button on the **Live Video** page of the Portal Server, the record file is be automatically ingested to available VOD servers, based on the stream type and user permissions. After ingestion, the record file can be automatically deleted from record server based on the configuration settings.

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.

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 recordings are supported; when using MPEG-2 at 15Mbps, 15 simultaneous recordings are supported.

Auto Content Ingestion

Topics in this section

Auto Content Ingestion 237
Auto Content Ingestion via XML 239

Auto Content Ingestion

You can use the AutoIngest feature to FTP or copy your video content to a predefined folder on the Portal Server for easy ingestion to the VOD server(s). The folder is monitored and the content is automatically ingested (autoingested) at a periodic interval. The VEMS Portal Server periodically (every 15 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 the StreamPlayer application. The content to be ingested is placed in any named folder as configured on the Devices > Application Servers page. Content placed in the named folder (Figure 23) will be ingested into the `AutoIngestedVideos` folder on the VOD server. Note that if you will be using FTP, the content folder must be under `ftproot`: e.g. `D:\inetpub\ftproot\VBrick\AutoIngest`. To disable AutoIngest entirely, simply leave the **AutoIngest Path** blank.

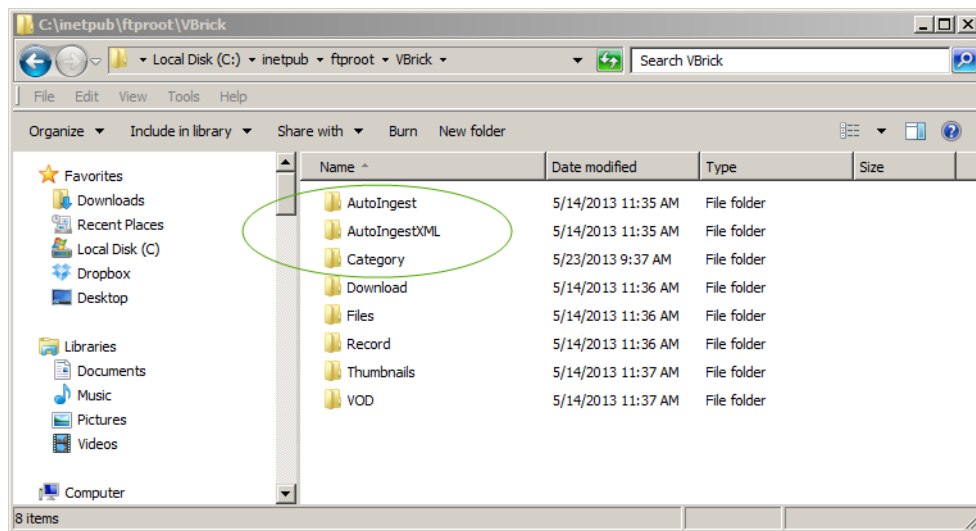


Figure 22. Windows Explorer Auto Ingest Folders

Application Server Administration	
Server Info	Entry Points
Server Information	
Type: <input type="text" value="Master"/>	Server Name: <input type="text" value="Homer"/>
Description: <input type="text" value="TestApp Server Description"/>	
FTP	
User Name: <input type="text" value="vbrickuser"/>	Virtual Path: <input type="text" value="/VBrick"/>
Password: <input type="password" value="....."/>	Local Path: <input type="text" value="d:\inetpub\ftproot\VBrick"/>
Record	
Max. Recordings: <input type="text" value="2"/>	Max. Bandwidth (kbps): <input type="text" value="225000"/>
Recording Path: <input type="text" value="d:\inetpub\ftproot\VBrick\Record"/>	
AutoIngest	
AutoIngest Path: <input type="text" value="D:\inetpub\ftproot\VBrick\AutoIngest"/>	Waiting List Size: <input type="text" value="10"/>
	Active List Size: <input type="text" value="2"/>
Transcode	
Max. Transcodings: <input type="text" value="0"/>	Transcoder Priority: Low <input type="range" value="50"/> High
<input type="button" value="Back to List"/> <input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 23. VEMS Mystro AutoIngest Path

Auto Content Ingestion by Category

This feature is similar to standard Auto Content Ingestion except that you can auto ingest content into a specific "categories" in VEMS Mystro, rather than into the root folder. The first step is to manually create the categories you wish to use in the `inetpub\ftpproot\VBrick\` folder (see Figure 22). For example, if you create the following folder structure, when you drop content into the `myCategoryA` folder, it will be ingested and assigned to `myCategoryA` in VEMS (the categories will be auto created in VEMS). When you drop content into `myCategoryB`, it will be ingested and assigned to `myCategoryB`, etc.

```
AutoIngest\Category
AutoIngest\Category\myCategoryA
AutoIngest\Category\myCategoryB
...
```

Note If Advanced Content Distribution has been enabled, a category for AutoIngested videos will automatically be created.

Auto Content Ingestion via XML

This feature lets you autoingest video files by placing an .xml file in the `AutoIngestXML` folder (see Figure 22) 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. The Portal Server monitors this folder for .xml command files and autoingests any files at five-minute intervals. The video file name, target categories, and metadata for each video is contained in the .xml file. The Portal Server autoingest folder is under FTP root on the Portal Server at `/VBrick/AutoIngestXML`. Videos placed in this folder will be autoingested at the configured interval. 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.

Note The source video file and the .xml file must both be FTPed to the `AutoIngestXML` folder. You must FTP the video file first or the ingestion will fail. If the video name matches the content name placed in `AutoIngestXML` folder the metadata of the same will be updated and video will be autoingested. If there are multiple videos in `AutoIngestXML` folder, all of the videos will be ingested but the metadata will only be updated for those videos that have information present in the metadata.xml file. Also be aware that all servers in use (both master and redundant) during the AutoIngest process must have the same file and path structure or the task will result in a failure.

Using the XML Template

Use the sample code below to create an .xml file that includes one entry for each video file you want to ingest. Use Notepad, TextPad, or a similar tool and then FTP this file to the `AutoIngestXML` folder on the Portal Server. (Note that 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 entry for one video file. Table 32 explains a description for each tag.

```
<?xml version="1.0" encoding="utf-8"?>
  <AutoIngestedVideos>
    <Video Name="Video11.mp4" >
      <Owner>Guest</Owner>
      <Titles>Video11</Titles>
      <Descriptions>This is xml ingested video</Descriptions>
      <Duration>60</Duration>
      <CategoriesAssigned>
        <CategoryName>SampleCategory1</CategoryName>
        <CategoryName>Chris</CategoryName>
      </CategoriesAssigned>
      <Keywords>
        <Keyword>keyword1</Keyword>
        <Keyword>keyword2</Keyword>
      </Keywords>
      <Comments>
        <Comment Name="Guest">Comment1</Comment>
        <Comment Name="ContentViewer">Comment2</Comment>
      </Comments>
      <FileLink>
        <Link Name="Microsoft">www.microsoft.com</Link>
```

```

    <Link Name="Google">www.google.com</Link>
  </FileLink>
  <CustomFields>
    <Field Name="Custom">Check</Field>
    <Field Name="Color">Green</Field>
  </CustomFields>
  <Restrictions>
    <Restrict Name="Viewers">13</Restrict>
    <Restrict Name="Date">5/9/2013</Restrict>
  </Restrictions>
</Video>
</AutoIngestedVideos>

```

Table 32. AutoIngestXML Tags

Tag	Description
Video	Required. Video name and extension (see supported file types in Table 33). Contains the source video file name to be ingested. This file must reside in the <code>AutoIngestXML</code> directory (<i>it must be FTPed first</i>) on the Portal Server. This file will ultimately be copied to one or more VOD servers. The format is simply the filename for example: <code>ingest001.wmv</code>
Owner	Required. Enter owner name or "Guest".
Titles	Required. Cannot be blank.
Descriptions	Optional. Description of the video. Used for search.
Duration	Video length in minutes.
CategoriesAssigned	The categories to which this video will be assigned. These categories must be configured in advance.
Keywords	Optional. Keywords associated with this video. Used for search.
Comments	Optional. Add user comments as desired. Note that name used is the Username of the user who posted the comment.
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 Edit a Category on page 40 for more. Each custom field must contain: <ul style="list-style-type: none"> 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.
Restrictions	<ul style="list-style-type: none"> Viewers – Optional. Maximum number of concurrent viewers allowed. -1 = unlimited. If unspecified, -1 (unlimited) is assumed. Date – Optional. Content expiration date, e.g. 20130430-1130. Format: <code>yyyymmdd-hhmm</code> Used for copyright protection.

Table 33. Supported File Types

File Type	File Extension
MPEG-2	.mpg
MPEG-4	.mp4
H.264/MP4	.mp4
H.264/TS	.mpg
WM	.wmv, .wma, .mp3, .asf
FLV	.flv
SWF	.swf
F4V	.f4v
MOV	.mov
M4V	.m4v
M4A	.m4a



Using Mystro with a DME

Topics in this section

Understanding Instances	243
Player Preference and Instance Selection.	243

Understanding Instances

VEMS Mystro and the Distributed Media Engine (DME) are integrated components in VBrick's comprehensive streaming ecosystem. The DME can be a standalone media distribution engine, a VOD server for VEMS Mystro, and A Video Conferencing (VC) Gateway. This topic assumes you have a VEMS Mystro installation and a DME configured as a VOD server. When you record a file in VEMS Mystro and send it to a DME, or when you add a file to VEMS Mystro using **Add Video**, VEMS Mystro will create up to three stored instances of that file on the DME, reflecting Mystro's ability to playback the content by three different techniques:

- HTTP Progressive Download
- RTSP (Darwin)
- Flash

VEMS Mystro creates three instances so you can test all of the playback mechanisms using the **Instances** tab available in the content metadata for the content. These three instances assume that the file can be played back in three ways like an .mp4 file containing H.264/AAC. If you were to upload a WM file (for example) it could only be played back from a DME using Progressive Download; so only one instance would be created. If you were to upload an .mp4 file containing MPEG4-P2 content, it would be available only for RTSP (consequently one instance). For a detailed explanation of Mystro playback mechanisms, see the "Supported File Types" topic in the *VEMS Mystro Release Notes*.

Be aware that these instances are further filtered by (1) the **Player Preference** settings in Mystro and (2) the machine/user displaying the instances. For example if the **Flash** is player is set to **Deny**, then the Flash instance will not be displayed. Similarly, if your machine can only access a Progressive Download server (e.g. because of Zones logic) and not a DME server, the RTSP instance will not be displayed. All of these scenarios are described in detail in the paragraphs that follow. For more about managing instances, see the "Instances" topic in the *VEMS Mystro User Guide*.

Player Preference and Instance Selection

This topic explains how the Mystro Player Preference settings work and how they influence what content instances get played, or not played. (See [Player Preference](#) on page 167 for an explanation of how to actually set preferences.) The first concept you will need to understand is that the **Player Preference** mechanisms does not "fall back" to a different player once a specific player is chosen by the server. Mystro chooses the "best" player, the "best" instance

of the content to playback, and the "best" playback mechanism (i.e. the URL or pattern used by the client to play the content). It does not try a different player/instance if the file it has selected is bad or corrupted or if the client does not have the proper plugin installed—instead it will prompt the client to install the plugin.

In order to play H264/AAC (MP4) content, we have three possible PC/Mac players (QuickTime, Flash and VB Player) and three different ways that content can be played back from a DME (HTTP, RTSP/VBRTSP, and RTMP). Generally speaking, a piece of H264/AAC (MP4) content can be played back from the DME using any of the following three players.

Player	Protocol
QuickTime	HTTP (iOS), RTSP
VB Player	VBRTSP, HTTP (de prioritized)
Flash	RTMP

Player Preference Example

This example assumes a PC client that clicks on a stored video in Mystro and that happens to be a piece of H264/AAC (MP4) content present on the DME only. The initial "possible" instance pool has three instances (with three possible ways to play them back: HTTP, RTSP/VBRTSP, RTMP). Mystro first checks what players are set to **Prefer** or **Allow** (on the System Settings > Player Preference page) and filters out any instances that are not compatible with the **Prefer** or **Allow** players. For example if the **Flash** player is set to **Deny**, the **VB Player** set to **Prefer**, and the **QuickTime** Player set to **Allow**, there are no RTMP-capable players available and the system will remove all RTMP-playable instances from the initial "possible" instance pool. This means that there are now only two "possible" instances that can be selected for playback: RTSP/VBRTSP and HTTP. This example also assumes there are no Zones defined and this is a single DME.

At this point if you were to navigate to the **Instances** tab on the client user interface, you would see two possible instances (representing RTSP/VBRTSP and HTTP) since both of these could *conceivably* be played based on the client profile and the preferred players. However before the stream is played back the instance selection engine will perform some additional filtering.

Since we are a PC (non-iOS) client we are going to prioritize the RTSP/VBRTSP playable instance (eliminating the Progressive Download/HTTP instance). At this point there remains only a single playable instance (RTSP) and the system now checks the players which are available in order to decide the best way to play this remaining instance. Since the VB Player is set as the preferred player in this example, the system will choose a VBRTSP playback pattern to send to the client to play back this piece of content since that's the way the VB Player plays back RTSP. (If instead I had the **QuickTime** player set to **Prefer** and the **VB Player** set to **Allow**, the system would send back an RTSP playback pattern to the client since that's the way the QuickTime player plays back RTSP.)

Corrupted Files and Exceptions

Be aware that if for some reason this single playable RTSP instance is broken or corrupted, it will not be detected by VEMS Mystro and the system will not fallback and try a different instance or player. The system chooses an instance and player based on the pattern/rules above and assumes that if the VOD server is online that this instance is valid and playable. It

will not fallback and try a different player/instance if the playback fails once an instance is selected and sent to the client.

Similarly the system will not try a different player if (for example) the user does not have the **Prefer** player installed on their machine. Mystro assumes that if an instance can be found (using the pattern/rules above) that can be played in the preferred player then that is the player the client should use (in this case the system will prompt the user to download the appropriate plugin). The system only falls back to an **Allow** player if it can't find an instance to play that matches the requirements of the **Prefer** player.

As an example, assume the **QuickTime** player is set to **Prefer** and **VB Player** is set to **Allow** and the content has only H.264 TS instances. The system will first try to find an instance that is playable in the "preferred" **QuickTime** player but will fail to do so because it knows that QuickTime cannot playback H264 TS. Instead it will fallback to the **VB Player**. In another scenario for this example (when the content has only H264 TS instances), if **QuickTime** is set to **Prefer** and no other players are set to **Allow**, this content would be filtered out completely and not even shown on the available list.

Multiple Allow Players

In a scenario where an instance cannot be found to satisfy the **Prefer** player (e.g. there are no Flash instances for a piece of content and the customer has **Flash** as their preferred player) but the customer has multiple Allow players (i.e. both **VB Player** and **QuickTime**) and instances have been found that are appropriate for both **Allow** players, then (on a PC) VEMS Mystro always assigns the lowest priority to the **QuickTime** player.

Failover

If playback of a specific piece of content fails, the player reports that failure back to the server and the server will try to determine if the playback failed because the VOD server was down. If Mystro determines the VOD server was down, the server will be marked as "offline" and Mystro will subsequently try to playback that content from a different server if possible.

STB Users Utility

Topics in this section

STB Users Utility	247
-------------------------	-----

STB Users Utility

In a VEMS Mystro environment, each (**Multi-Format or AmiNET130**) STB must be associated with a VEMS user and each VEMS STB user must be unique. In large-scale deployments, creating these users is a time-consuming manual process. The **STB Users Utility** is a program that automates this process: it automatically creates users and assigns them to each STB. The workflow to accomplish this requires several steps using both the VEMS admin interface and the STB Users Utility. The required steps are listed below and explained in detail on the following pages.

1. Use the VEMS admin interface to create a group (or multiple groups), assign a role, and configure the desired folder permissions.
2. Add the STB devices to the VEMS system configuration using the VEMS admin interface.
3. Run the **STB Users Utility** to create and (optionally) assign users to a targeted STB list that was generated by the STB filter controls.

Installation

The STB Users Utility is installed on the VEMS server machine and runs on the VEMS server machine. The application is located in the following directory on the VEMS server machine. Click on the `setup.exe` or the `STBUsers` one-click application install file. Once installed, the program will create a shortcut on the Windows **Start** menu.

C:\Program Files (x86)\VBrick\Maduro\Utils\STBInstall (64-bit machines)

C:\Program Files\VBrick\Maduro\Utils\STBInstall (32-bit machines)

1. Create Groups

After installing the application, the first step is to create the groups which will eventually contain the users created by the **STB Users Utility**. On the VEMS admin interface, go to **Access Control > Groups** and create one or more groups. Do not assign users to these groups but do assign a **Content Viewers** role and permissions. The "permissions" refer to the folders which the group(s) can access. Different groups will typically be defined with different folder privileges. See [Access Control](#) on page 27 for details about creating groups and assigning permissions.

Groups Administration

Group Information

Group Name

Description

Group Users

All Users

Admin
ContentAdministrator
ContentPublisher
ContentViewer
Guest
nick
Scheduler
SystemAdministrator
UserAdministrator
VBrickAdministrator

Assigned Users

2. Add STBs to VEMS

The next step is to configure the new STBs (for which you need users) in VEMS Mystro.

1. On the VEMS admin interface, go to **Devices > STB**.
2. Click **Manually Add STB** or **Auto-Discover STB** to populate the STB list.
3. Select the new STBs you wish to configure in VEMS. See [STB](#) on page 86 for details about adding STBs.

STB Device Administration

STB Administration

Select a STB:

	HostName	IP Address	Part Number	Edit	Delete
1.	MAC000138ecda18	172.22.226.16 Multi Format STB	8000-0188-000X		
2.	MACe0915309d9b7	172.17.2.102 Multi Format STB	8000-0188-000X		
3.	MACe0915309d9b8	172.16.2.74 Multi Format STB	8000-0188-000X		
4.	MACe0915309d9bb	172.22.2.47 Multi Format STB	8000-0188-000X		

3. Run STB Users Utility

The last step is to run the **STB Users Utility**. The utility will create STB users and assign those users to the groups you configured in Step 1 and the STBs you configured in Step 2.

Login

1. Launch the **STB Users Utility** from the **Start** menu.
2. Click on the **Login** button to start a session.
3. Configure the input parameters for the utility as explained below.

Get STB List

Use this pane (and the filters) to get a list of STBs from those that are currently defined in VEMS. This populates the **STB List** in the utility.

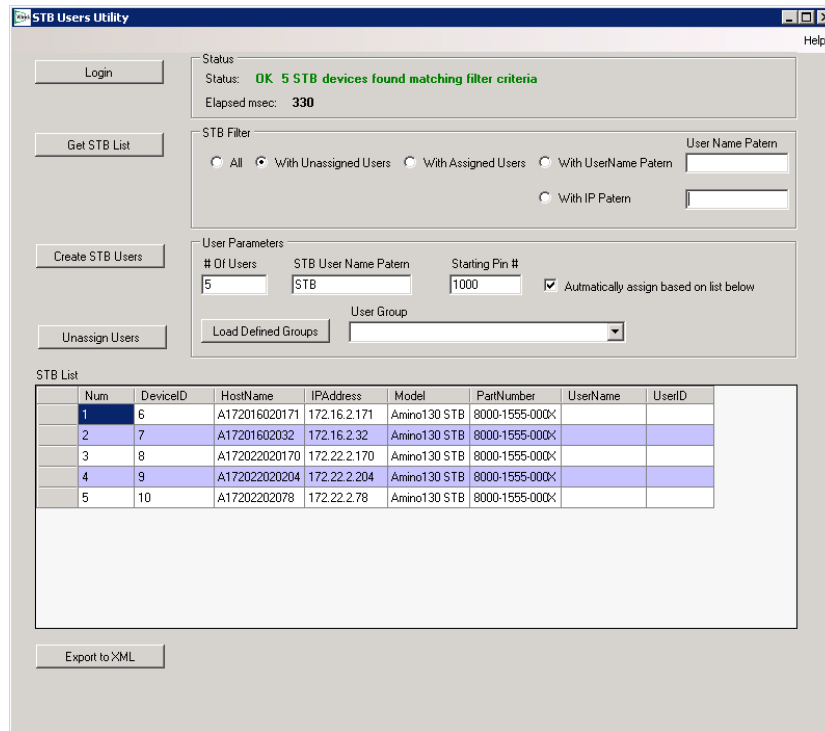
- All – all set top boxes in VEMS.
- With Unassigned Users – STBs with users not assigned.
- With Assigned Users – STBs with users already assigned.
- With UserName Pattern – STBs with users names that start with these characters.
- With IP Pattern – STBs with IP addresses that start with these digits.

Create STB Users	Use this pane to create a list of users and automatically assign them to the STBs listed below. <ul style="list-style-type: none"> • # of Users – number of users to create. This field is auto-populated when you click Get STB List. • STB User Name Pattern – beginning characters of the user name. • Starting PIN number – beginning digits of the PIN numbers. • Auto assign based on list – check this box to actually assign users to STBs. If unchecked, the users will be created but <u>not</u> assigned.
Load Defined Groups	Select the previously created group with which the STB users will be associated.
Unassign Users	Unassigns all users from the STBs in the displayed list. Note that it unassigns users; it does not remove them from VEMS.
Export to XML	Save the STB list and associated user names to an .xml file.

Get STB List

▼ To create STB users and assign them to groups:

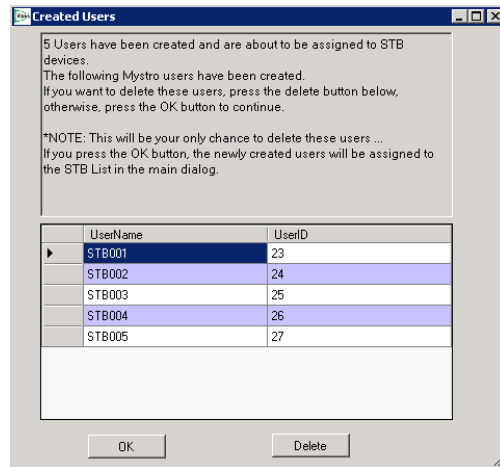
1. Select a radio button in the **STB Filter** pane and click **Get STB List**.



2. In the **User Parameters** pane, select the desired options.
3. Click **Load Defined Groups** and select the group to which the selected options will apply.

Create STB Users

1. When you are happy with the **User Parameters** and the **STB List**, click **Create STB Users** and confirm.



2. Verify the User Names in the list. If you need to make changes, click **Delete**. This will remove all users and you can start again.
3. If you are happy with the list, click **OK**. At this point there is no revert—the users will actually be assigned to the specified STBs (if the **Automatically assign based on list below** option is checked).
4. When done, the **STB List** will be automatically refreshed showing the STBs and assigned user names.

Command Line Interface

Topics in this section

Command Line Interface	253
CLI Structure	253
XML Structure	257

Command Line Interface

This topic explains how to use the Command Line Interface (CLI) to interact with the Portal Server SDK from third-party control systems.

Note When initiating a recording with a `StartTime` of `NOW`, the system overhead required to process the request may result in a recording with a `duration` that is less than the configured value.

SDK Message Structure

-
- Notes**
- Brackets "< >" are used to delineate each attribute. They are not literal, i.e. the actual messages will not include brackets.
 - `$0d` indicates a true carriage return (not the literal string “\$0d”).
 - A message in the following CLI format must be sent once, right after the client is connected to the server.
-

Configuring Mystro for CLI

Use the following steps to configure the Mystro server for CLI functionality.

- ▼ To configure the Mystro server for CLI:
 1. Go to: `C:\Program Files(x86)\VBrick\Maduro\Services\MaduroCLIService`
 2. Edit `MaduroCLIService.exe.config` with Notepad or other editor as follows:
 - a. Find `SDKProxyInterface` and set `value` to IP address of the Mystro server.
 - b. Find `SDKProxyPort` and set `value` to desired port. You can use the default (`10001`) or any non-used port (except `21` or `80`).
 3. When done restart the `MaduroCLIService` as follows:
 - a. Go to Start > Administrative Tools > Services.
 - b. Right-click on `MaduroCLIService` and select **Restart**.

CLI Structure

CLI\$0d

Login

In Arguments

Login:<username>,<userpassword>\$0d

Out Arguments

Login_OK:<sessionid>\$0d

or

Login_ERROR:<error01>,<error02>\$0d

Logout

In Arguments

Logout:<sessionid>\$0d

Out Arguments

Logout_OK:\$0d

or

Logout_ERROR:<error01>,<error02>\$0d

List Live

CanBeRecordedToVBrick (True/False) determines whether the content can be recorded to a VBrick device (i.e. a VBStar encoder with a hard drive) or not.

In Arguments

ListLive:<sessionid>\$0d

Out Arguments

ListContent:<Title>,<ContentID>,<CanBeRecordedToVBrick>\$0d
ListContent:<Title>,< ContentID>,<CanBeRecordedToVBrick>\$0d
...
ListContent:<Title>,< ContentID>,<CanBeRecordedToVBrick>\$0d
ListEnd:\$0d

Start Record (uses NVR)

Note Recorded files are saved in the "Recordings" category on the Portal Server.

In Arguments

StartRecord:<sessionid>,<contentID>,<ingesttitle>,<starttime>,<duration>,<custom>\$0d

ContentID	Unique ID of the Live content (returned by ListLive method).
------------------	--

IngestTitle	Should <u>not</u> include full path, i.e. test.mp4
--------------------	--

StartTime	Server time, such as "09/30/2010 03:00:00 pm" or "NOW" to start immediately.
------------------	--

Duration	Duration of recording in seconds.
-----------------	-----------------------------------

Custom	Sequence of name/value pairs, separated by a pipe symbol(“ ”) for custom MetaData names & values. For example, “color blue size 10” represents color=blue & size=10
---------------	---

Out Arguments

StartRecord_OK:<scheduleid>\$0d

or

StartRecord_ERROR:<error01>,<error02>\$0d

Start Encoder Record (uses VBStar)

Note Recorded files are saved in the "Recordings" category on the Portal Server.

In Arguments

StartEncoderRecord:<sessionid>,<contentID>,<ingesttitle>,<starttime>,<duration> \$0d

ContentID	Unique ID of the Live content (returned by <code>ListLive</code> method).
IngestTitle	Should <u>not</u> include full path, i.e. test.mp4.
StartTime	Server time, such as “09/30/2010 03:00:00 pm” or “NOW” to start immediately.
Duration	Duration of recording in seconds

Out Arguments

StartEncoderRecord_OK:<scheduleid>\$0d

or

StartEncoderRecord_ERROR:<error01>,<error02>\$0d

Stop Record (uses either NVR or VBStar)

In Arguments

StopRecord:<sessionid>,<scheduleid>\$0d

Out Arguments

StopRecord_OK:\$0d

or

StopRecord_ERROR:<error01>,<error02>\$0d

Get Channel Guide

Retrieve channel guide data.

In Arguments

ListChannelGuide:<sessionid>,<*startDateTime>\$0d *

* Denotes local time. Pass the string "now" to indicate current date/time

Out Arguments

```
ListChannelGuide_OK:$0d
ProgramData:<contentID>,<chanl#>,<chanName>,0,<progName>,<startDT>,<endDT>$0d
...
ProgramData:<contentID>,<chanl#>,<chanName>,N,<progName>,<startDT>,<endDT>$0d
ProgramData_End:$0d
OR
ListChannelGuide_ERROR:<error01>,<error02>$0d
```

Get List of STBs

Retrieve a list of all configured STBs.

In Arguments

```
ListSTB:<sessionid>,$0d
```

Out Arguments

```
ListSTB_OK:$0d
STB:<ID>,<Name>,<IPAddress><PartNumber>$0d
...
STB_End:$0d
OR
ListSTB_ERROR:<error01>,<error02>$0d
```

Tune STB

Tune the STB in the specified Schedule to the specified live stream. For this feature to work properly, the schedule must be pre-configured as follows:

- Event Type must be "Tune STB to Existing Stream".
- Both start and end date must be in the past.
- STB(s) must be specified for the schedule.

In Arguments

```
TuneSTB:<sessionid>,<scheduleID>,<liveContentID>$0d
```

Out Arguments

```
TuneSTB_OK:$0d
OR
TuneSTB_ERROR:<error01>,<error02>$0d
```

List STB Schedules

List all schedules configured as "Tune STB to Stream."

In Arguments

```
ListSTBSchedule:<sessionid>$0d
```

Out Arguments

```
ListSTBSchedule _OK:$0d
STBSchedule:<schedID>,<schedName>,<STBID>,<STBName>,<ContentID>$0d
...
STBSchedule_End:$0d
Or
ListSTBSchedule_ERROR:<error01>,<error02>$0d
```

STBID	If there is more than one STB configured, IDs will be delimited by a " ". For example, "2 3 4".
STBName	If there is more than one STB configured, names will be delimited by a " ". For example "A B C". Sequencing will be the same as for STBID.

XML Structure

XML\$0d

Login

In Arguments

```
<Request type="Login">
<UserName> </UserName>
<UserPassword> </UserPassword>
</Request>$0d
```

Out Arguments

```
<Response Command="login">
<Status>
<Error>OK</Error>
</Status>
<SessionId> </SessionId>
</Response>$0d
```

Or

```
<Response Command="login">
<Status>
<Error>error01</Error>
</Status>
</Response>
```

Logout

In Arguments

```
<Request type="Logout">
<SessionId> </SessionId>
</Request>$0d
```

Out Arguments

```
<Response Command="logout"><Status><Error>OK</Error></Status></Response>
```

or

```
<Response Command="logout"><Status><Error>error01</Error></Status></Response>
```

List Live

`CanBeRecordedToVBrick` (True/False) determines whether the content can be recorded to a VBrick device (i.e. a VBStar encoder with a hard drive) or not.

In Arguments

```
<Request type="ListLive">
  <SessionId> </SessionId>
</Request>$0d
```

Out Arguments

```
<Response Command="listlive">
  <Status>
  <Error>OK</Error>
</Status>
  <LiveContent>
  <Title> </Title>
  <ContentID></ContentID>
  <CanBeRecordedToVBrick></CanBeRecordedToVBrick>
</LiveContent>
  <LiveContent>
  <Title> </Title>
  <ContentID></ContentID>
  <CanBeRecordedToVBrick></CanBeRecordedToVBrick>
</LiveContent>
</Response>
```

Start Record (uses NVR)

Note Recorded files are saved in the "Recordings" category on the Portal Server.

In Arguments

```

<Request type="StartRecord">
<SessionId> </SessionId>
<ContentID> </ContentID>
<IngestTitle> </IngestTitle>
<StartTime> </StartTime>
<Duration> </Duration>
<CustomFields> </CustomFields>
</Request>$0d

```

ContentID	Unique ID of the Live content (returned by <code>ListLive</code> method).
IngestTitle	Should <u>not</u> include full path, i.e. test.mp4.
StartTime	Server time, such as "09/30/2010 03:00:00 pm" or "NOW" to start immediately.
Duration	Duration of recording in seconds.
Custom	Sequence of name/value pairs, separated by a pipe symbol(" ") for custom MetaData names & values. For example, "color blue size 10" represents color=blue & size=10

Out Arguments

```

<Response Command="startrecord">
<Status>
<Error>OK</Error>
</Status>
<ScheduleId></ScheduleId>
</Response>

```

Or

```

<Response Command="startrecord">
<Status>
<Error>error01</Error>
</Status>
</Response>

```

Start Encoder Record (uses VBStar)

Note Recorded files are saved in the "Recordings" category on the Portal Server.

In Arguments

```

<Request type="StartEncoderRecord">
<SessionId> </SessionId>
<ContentID> </ContentID>
<IngestTitle> </IngestTitle>
<StartTime> </StartTime>
<Duration> </Duration>
</Request>$0d

```

ContentID	Unique ID of the Live content (returned by <code>ListLive</code> method).
IngestTitle	Should <u>not</u> include full path, i.e. test.mp4.
StartTime	Server time, such as "09/30/2010 03:00:00 pm" or "NOW" to start immediately.
Duration	Duration of recording in seconds.

Out Arguments

```

<Response Command="startrecord">
<Status>
<Error>OK</Error>
</Status>
<ScheduleId></ScheduleId>
</Response>

```

Or

```

<Response Command="startrecord">
<Status>
<Error>error01</Error>
</Status>
</Response>

```

Stop Record (uses either NVR or VBStar)

In Arguments

```

<Request type="StopRecord">
<SessionId> </SessionId>
<ScheduleId> </ScheduleId>
</Request>$0d

```

Out Arguments

```

<Response Command="stoprecord">
  <Status>
    <Error>OK</Error>
  </Status>
</Response>

```

Or

```

<Response Command="stoprecord">
  <Status>
    <Error>error01</Error>
  </Status>
</Response>

```

Get Channel Guide

In Arguments

```

<Request Command="ListChannelGuide">
  <SessionId> </SessionId>
</Request>

```

Out Arguments

```

<Response Command=" ListChannelGuide ">
  <Status>
    <Error>OK</Error>
  </Status>
  <ProgramData>
    <ContentID> </ContentID>
    <ChannelNumber> </ChannelNumber>
    <ChannelName> </ChannelName>
    <Index> </Index>
    <ProgramName> </ProgramName>
    <StartDT> </StartDT>
    <EndDT> </EndDT>
  </ProgramData>
  ...
</Response>

```

Or

```

<Response Command="ListChannelGuide">
  <Status>
    <Error>error message</Error>
  </Status>
</Response>

```

Get List of STBS

In Arguments

```
<Request Command="ListSTB">
<SessionId> </SessionId>
</Request>
```

Out Arguments

```
<Response Command="ListSTB">
<Status>
<Error>OK</Error>
</Status>
<STB>
<DeviceID> </DeviceID>
<Hostname> </Hostname>
<IPAddress> </IPAddress>
<PartNumber> </PartNumber>
</STB>
...
</Response>
```

Or

```
<Response Command="ListSTB">
<Status>
<Error>error message</Error>
</Status>
</Response>
```

Tune STB

In Arguments

```
<Request Command="TuneSTB">
<SessionId> </SessionId>
<ScheduleID> </ ScheduleID >
<LiveContentID> </ LiveContentID >
</Request>
```

Out Arguments

```

<Response Command="TuneSTB">
<Status>
<Error>OK</Error>
</Status>
</Response>

```

Or

```

<Response Command="TuneSTB">
<Status>
<Error>error message</Error>
</Status>
</Response>

```

List STB Schedules

In Arguments

```

<Request Command="ListSTBSchedule">
<SessionId> </SessionId>
</Request>

```

Out Arguments

```

<Response Command=" ListSTBSchedule ">
<Status>
<Error>OK</Error>
</Status>
<STBSchedule>
<ScheduleID> </ScheduleID>
<ScheduleName> </ScheduleName>
<STBList> </STBList>
<STBName> </STBName>
<ContentID> </ContentID>
</STBSchedule>
...
</Response>

```

Or

```

<Response Command=" ListSTBSchedule">
<Status>
<Error>error message</Error>
</Status>
</Response>

```
