



# **Vbrick Distributed Media Engine**

vbrick dme v3.25.1

Admin Guide



---

## Copyright

© 2021 Vbrick Systems, Inc. All rights reserved.

Vbrick Systems, Inc.  
607 Herndon Parkway, Suite 300  
Herndon, VA 20170 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 Mystro, 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

## DME Admin Guide

Welcome .....	vii
Chapter and Topic Organization.....	vii

### 1. Introduction

DME Overview .....	1
DME Features and Benefits .....	2
DME Supported Protocols .....	2
DME Server Models .....	3
DME Software-Only Version .....	4
Software Development Kit .....	4
DME Compatibility with Vbrick Products .....	4
Glossary .....	4

### 2. Installation

DME Installation Overview.....	7
--------------------------------	---

### 3. Getting Started

How the DME Functions .....	9
Plan for your DME Deployment.....	9
DME Components.....	10
Streaming Servers .....	10
VOD Servers.....	11
FTP Server .....	11
Caching (HTTP) Server.....	11
Storage Extension Capabilities .....	11
Streaming Overview.....	11
Served VOD Streams .....	12
Pushed Streams .....	13
Pulled Streams .....	14
Transmuxed Streams.....	14
Transrated Streams .....	14
VAdmin.....	15
Login to the DME.....	15
Log Out of the DME .....	16
End User License Agreement (EULA) .....	16
Register the DME.....	16
The Apply, Revert, and Default Buttons .....	17
Reset the System .....	18
Online Help.....	19
DME Status (Snapshot).....	19

DME Status (Historical) . . . . .	21
Configuration Menu . . . . .	24
DME Status Bar . . . . .	25
VBDirectory . . . . .	29
Configure the DME with Secure Shell (SSH) or a Console . . . . .	30

## 4. System Configuration

Network . . . . .	41
Fully Qualified Domain Name (FQDN) . . . . .	41
IPv4 Network Interface 1 . . . . .	42
NAT . . . . .	44
Domain Name Server . . . . .	44
Network Time Synchronization . . . . .	45
Proxy . . . . .	46
Ports . . . . .	48
Security . . . . .	50
New Password Requirements . . . . .	52
SNMP . . . . .	52
General . . . . .	54
System Maintenance . . . . .	55
Login . . . . .	55
System Time . . . . .	56
System Reset . . . . .	56
Streaming . . . . .	57
Differentiated Services Values . . . . .	60
Caching . . . . .	61
Standalone DME or Legacy (DME with VEMS) Caching Configuration . . . . .	62
HLS CDN Reflection . . . . .	66
Mesh with Rev Caching Configuration . . . . .	67
Manage Configuration . . . . .	72
SSL Certificates . . . . .	73
SAN/iSCSI Setup . . . . .	76
Activate Feature . . . . .	77
Rev Interface . . . . .	79

## 5. Rev Integration Functions

DME Video EdgeIngest to Rev . . . . .	81
Required File Types for Bulk Video Upload . . . . .	81
Start a Bulk Video Upload to Rev . . . . .	83
Monitor a Bulk Video Upload to Rev . . . . .	83

## 6. SAP Configuration

Announcement Types . . . . .	85
Management SAP . . . . .	85
Announce SAP . . . . .	85
Announcements . . . . .	85

---

SAPs for Unannounced Streams . . . . .	87
<b>7. Input Stream Configuration</b>	
RTMP/RTSP Pull . . . . .	89
RTP Playlists . . . . .	90
Create or Edit an RTP Playlist . . . . .	91
Transport Stream In. . . . .	93
MPG2TS Streams . . . . .	93
<b>8. Output Stream Configuration</b>	
RTMP Push . . . . .	95
Flash Multicast. . . . .	96
Assigning a Multicast Address . . . . .	98
Vbrick Multicast. . . . .	99
RTSP Push. . . . .	101
Transport Stream Out . . . . .	102
HLS Streaming. . . . .	103
Playlist Conventions . . . . .	106
HDS Streaming . . . . .	106
Playlist Conventions . . . . .	109
RTP Relay Overview . . . . .	109
Create or Edit an RTP Relay. . . . .	110
Stream on Demand . . . . .	112
Advanced StreamOnDemand Configurations. . . . .	113
Stream Conversion. . . . .	114
Rev Initiated Multicast and Reflection. . . . .	116
Automatic Multicast for Rev VC Live Webcast and Custom Devices . . . . .	116
HLS Stream Preparation for Automatic Multicast and Reflection Using Rev Custom De-	
vices. . . . .	117
<b>9. User Configuration</b>	
Username and Password . . . . .	119
Readonly Username and Password . . . . .	120
Stream Input Authentication . . . . .	120
<b>10. Rev Devices</b>	
Set Top Box Connector. . . . .	123
Discovered Set Top Boxes . . . . .	123
<b>11. Logging</b>	
Enable Error and Access History Logging . . . . .	125
<b>12. Monitor and Logs</b>	
MPS Connections . . . . .	127
RTP Connections. . . . .	131

---

Relay Status .....	131
Recording Status .....	132
Access History .....	134
Upgrade Log .....	134
Error Log .....	135
User Login Log .....	136
Upload Log .....	136
<b>13. Maintenance</b>	
System Maintenance .....	139
Disk Status .....	140
Provision a New Disk .....	141
<b>14. Diagnostics</b>	
Trace Capture .....	145
Ping Test .....	146
Traceroute Test .....	147
Caching Diagnostics .....	147
<b>15. Detailed Use Cases</b>	
MultiCast Relay Use Case Overview .....	149
Configure a Multicast Relay with a Unicast Source .....	149
H.264 Encoder Setup .....	149
DME Setup .....	150
Configure a Multicast Relay with an Auto-Unicast Source .....	151
H.264 Encoder Setup .....	151
DME Setup .....	151
<b>16. Other Tasks</b>	
Install Security Updates .....	153
Manage Disk Space .....	153
Backup and Restore .....	153

---

# DME Admin Guide

## Welcome

This document explains how to configure and use Vbrick's Distributed Media Engine (DME). The DME is a versatile, highly-configurable media distribution engine that moves streaming media to and from a wide variety sources and endpoints.

For example, it can take a unicast RTP stream and multicast it to thousands of local IP users, or it can transmux and serve the same RTP stream to RTMP users on the Internet.

The information in this document is available Online on the Vbrick website. For all the latest technical documentation for Vbrick products, go to [www.vbrick.com/documentation](http://www.vbrick.com/documentation)

**Note:** This Admin guide is not written for casual users. It assumes readers will have a working knowledge of network addressing, communication protocols, and configuration concepts, as well as hands-on experience working with streaming video products.

## Chapter and Topic Organization

Topics may be reference material or how-to materials for specific use cases.

For best results, please familiarize yourself with the way the information is organized and follow the steps listed in .

<a href="#"><u>Introduction</u></a>	A system overview and detailed explanation of the different DME models available. Also contains a glossary of terms.
<a href="#"><u>Installation</u></a>	How to set up and test the server hardware. It also explains how to configure the DME as a VOD server in VEMS.
<a href="#"><u>Getting Started</u></a>	How the DME works including an overview of the major system components. The VBAdmin management program is also covered.
<a href="#"><u>System Configuration</u></a>	Reference chapter; provides a detailed description of all the parameters on the System Configuration page in VBAdmin.
<a href="#"><u>Rev Integration Functions</u></a>	Detailed use cases with step-by-step instructions that explain how to use the various integration functions between the DME and the Rev media management system.
<a href="#"><u>SAP Configuration</u></a>	How to configure SAP announcements for different kinds of streams.
<a href="#"><u>Input Stream Configuration</u></a>	How to configure DME input streams including RTMP Pull, TS In, and RTP Playlists.
<a href="#"><u>Output Stream Configuration</u></a>	How to configure DME output streams including RTMP Push, TS Out, HLS, and RTP Relays.
<a href="#"><u>User Configuration</u></a>	How to configure the DME user name and password and the announce settings that let you push streams into the DME.

---

<u>Rev Devices</u>	View Rev/DME Set Top Box Connector Configurations and Logs.
<u>Logging</u>	How to enable and configure the Access History and the Error Log.
<u>Monitor and Logs</u>	How to view the various status and log pages to monitor important DME resources and tasks such as connected users and CPU Load.
<u>Maintenance</u>	How to reset or shutdown the system.
<u>Diagnostics</u>	How to capture trace files for Vbrick Support Services when troubleshooting issues.
<u>Detailed Use Cases</u>	The detailed steps required (on the encoder and on the DME) to configure input and output for common use cases.
<u>Other Tasks</u>	Other common tasks such as how to upgrade the server when new software is available from Vbrick.



## Introduction

### DME Overview

The Vbrick H.264 Distributed Media Engine (DME) simplifies delivery of high definition video and other rich media content across multi-site enterprises and campus environments. If properly configured, you can simultaneously input multiple streams (of different types) into the DME and output them as the same stream types or as different stream types.

For example, you can input RTP and TS (transport streams) into the DME and output those same streams as RTMP or HLS (for Apple iOS devices). The DME also provides video content caching, storage, and serving to ensure that stored content is delivered from a DME as close to the end user as possible.

The DME may be deployed at a central location, to support transmuxing, or at remote locations to support distribution. It is a single integrated platform providing media redistribution, media transformation and video-on-demand content storage.

The DME accepts multiple H.264 media streams from multiple central sites and redistributes that content to diverse endpoints including PCs/MACs, mobile phones and televisions/monitors. This one integrated platform optimizes WAN bandwidth use, simplifies endpoint support and offers local storage of centrally managed content.



The DME is offered on a choice of three robust hardware platforms, all leveraging Vbrick's experience with high performance, low touch appliances. It is also offered as a software product to be installed on the customers own hardware (including VMWare).

It requires only a web browser interface for management, and the H.264 DME seamlessly integrates as a distributed element within the Vbrick enterprise IP video platform. This includes working in concert with a central Vbrick Enterprise Management System (VEMS) to intelligently store and serve content from a local DME.

Deploying the H.264 Distributed Media Engine assures users of access to high definition quality video on both fixed and mobile endpoints, even if they are located across campus or across the world.

---

## ***DME Features and Benefits***

- Bandwidth Conservation – Redistribute high quality, live or on-demand, media via RTP multicast; enables more end users to share a single media stream. Leveraging multicast eliminates the need to incrementally scale network bandwidth to support more viewers.
- Media Transformation – Stream high quality H.264 content once and leverage the DME at distributed locations to deliver multiple formats (RTP, RTMP, and/or HTTP progressive download) to reach multiple types of endpoints.
- Mobile Device Support – Enables delivery of live H.264 content to mobile devices.
- Transrating provides for delivery of content to mobile devices of different types on networks of varying quality.
- Intelligent Central Management – Content is created once and then intelligently managed by the Vbrick Enterprise Media System (VEMS) regardless of the location. Stored content is appropriately distributed to local DMEs so users have faster access to frequently viewed content without the need to contend with constrained WAN or Internet links.
- Robust Appliance Design – Requiring only a web browser for management, the DME eliminates the need to separately manage patches and security updates on commercial server operating systems.
- Secure – Designed to meet the security requirements of demanding government information assurance policies.
- Firewall Friendly – Supports video on demand content via HTTP download; eliminating barriers imposed by network security policies.
- Enhanced User Experience – Increases user adoption and impact by assuring outstanding picture quality and response from video applications. The DME easily accommodates increased user demand without degrading performance or the user experience.

## ***DME Supported Protocols***

The table below describes the supported protocols of the DME.

Protocol	Description
Incoming	<ul style="list-style-type: none"><li>• RTSP Announce</li><li>• RTP Over UDP (with RTCP) Unicast and Multicast</li><li>• RTP over TCP (with RTCP) Unicast Only</li><li>• RTP over UDP (SDP file delivered via FTP)</li><li>• FTP for VOD file transfer</li><li>• RTMP via RTMP Push over TCP</li><li>• Transport Stream (MPEG2TS delivery of H.264 audio and video content)</li></ul>

Protocol	Description
Outgoing	<ul style="list-style-type: none"> <li>• RTP via RTSP (stream)</li> <li>• UDP, TCP Interleaved, and HTTP Tunneled</li> <li>• RTP via RTSP (relay - Push)</li> <li>• UDP, TCP Interleaved using Announce</li> <li>• RTMP (stream and relay)</li> <li>• RTMP</li> <li>• HTTP (progressive download)</li> <li>• TS (transport stream)</li> <li>• HLS (Apple HTTP iPad/iPhone live streaming)</li> <li>• HDS</li> <li>• HTTP Caching Server</li> </ul>
Management	<ul style="list-style-type: none"> <li>• HTTP/HTTPS for management</li> <li>• IGMPv3</li> </ul>

## DME Server Models

Vbrick currently supports a variety of shelf and rack-mount models. See the latest *DME Release Notes* for a detailed description of DME models and specifications. There are no absolute rules for sizing a multipurpose device like the DME but there are some basic guidelines that can help you select the right model.

The smaller Model 7530 does not offer redundant power supplies or redundant VOD storage so if these attributes are important, you should consider the larger models. The Model 7530 is shelf-mount only while the larger models are rack mount 1U and 2U servers. Users seeking significant VOD content playback should consider one of the two larger models.

The RAID arrays built into the Models 7550 and 7570 (seen below) are much more powerful and better suited for frequent requests than for concurrent VOD playback. The single drive on the Model 7530 is well suited for small to medium offices that have occasional VOD demands.



All of the models have excellent throughput performance and are designed to manage occasional traffic bursts exceed recommended performance characteristics. The throughput recommendations are based on a combination of input and output. For example, a Model 7530 (with 250 Mbps throughput) can support four 1 Mbps streams in, and reflect out 96 1 Mbps unicast streams of RTP or RTMP (any combination that equals 250 Mbps).

Also keep in mind that one multicast stream out counts as a single stream from a bandwidth perspective, regardless of how many users are watching. Please refer to the latest *DME Release notes* for complete hardware specifications.

---

## DME Software-Only Version

The DME is available as a hardware/software combination in which case Vbrick will deliver the DME server hardware with the DME software already installed. You can also purchase the DME in a VMware virtualized version in which case you must install the DME software on your own server platform.

For more about this option, and server hardware recommendations, see the “Software-Only Version” topic in the latest *DME Release Notes*.

## Software Development Kit

The DME Software Development Kit (SDK) is available for customers who want to build custom applications to control the DME. It assumes the reader is an experienced software developer with a working knowledge of Web Services. All code examples are written in C#.

The SDK includes an .xml document with DME name/value pairs, a sample application, and the *DME SDK Reference Guide* which explains how to use the APIs. For more information contact your certified Vbrick reseller or Vbrick [Support Services](#).

## DME Compatibility with Vbrick Products

The table below specifies DME compatibility with other Vbrick products:

Vbrick Product	Compatible With Version †
VEMS Mystro® Portal Server	6.0.1
VEMS Portal Server	5.4
H.264 Encoding Appliance	3.0 (RTP)
H.264 Encoding Appliance	3.1 (RTP, RTMP)
H.264 Decoding Appliance	3.0
Rich Media Desktop (RMD)	1.1
Rich Media Studio	1.3 (1.6 recommended)
Rev	7.0

† Use version shown or higher.

## Glossary

These terms are used throughout this document and DME’s Online help.

Auto Unicast	A transmitter mode that allows an encoder to "automatically" establish and maintain a connection with a streaming server like Quicktime or Darwin. The stream is pushed to a configured publishing point external clients can connect to retrieve the stream.
CDN	Content delivery networks are distributed server systems of deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.
DASH	Dynamic Adaptive Streaming over HTTP. DASH is a multimedia streaming technology where a multimedia file is partitioned into one or more segments and delivered to a client using HTTP.

DME	Distributed Media Engine is an integrated platform that provides media redistribution, media transformation and video-on-demand content storage.
Caching Server	Content is cached at remote locations so subsequent requesting clients can access it locally.
Flash	Multimedia platform used to add video and interactivity to web pages. Flash uses RTMP and is a proprietary Adobe technology. Note: Flash is a legacy platform and no longer in use by Rev.
FTP Server	The DME uses File Transfer Protocol to populate the DME with files for progressive download.
HDS	HTTP Dynamic Streaming is Adobe's HTTP streaming protocol. Like other HTTP adaptive streaming protocols, it breaks the stream into small HTTP-based files so the client can select from different streams containing the same material encoded at different data rates. This allows the streaming session to adapt to available data rates.
HLS	HTTP Live Streaming is Apple's HTTP streaming protocol for QuickTime and iPhone. Like other HTTP adaptive streaming protocols, it breaks the stream into small HTTP-based files so that the client can select from different streams containing the same material encoded at different data rates. This allows the streaming session to adapt to available data rates.
HTTP Server	The DME has an internal web server that serves VOD files via progressive download.
ICP	Internet Cache Protocol coordinates multiple web caches. It finds the most appropriate location to retrieve a requested object when multiple caches are in use at a single site. The goal is to minimize the number of remote requests to the originating server.
Multicast	A highly-efficient streaming mechanism wherein one stream is sent to multiple clients without impacting available bandwidth. Multicast is a one-to-many connection between client and server. Used only in local IP networks (not the Internet); requires support from a switch. See <a href="#">Unicast</a> .
Progressive Download	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. The files are downloaded—not streamed.
Pull	The mechanism whereby a video stream is requested, and <i>pulled</i> , from an RTP server (e.g. QuickTime or Darwin), an RTMP server (e.g. Wowza or FMS), or another Vbrick DME.
Push	The mechanism whereby an RTP or RTMP stream is continuously <i>pushed</i> to a configured destination.
RTMP	Real Time Messaging Protocol is a proprietary protocol developed by Adobe for streaming audio and video over the Internet. The DME has an internal RTMP server.
RTMPS	RTMP over a secure SSL connection.

RTP	Real Time Transport Protocol is the Internet-standard protocol for the transport of realtime audio and video over the web. The DME has an internal RTP server. Darwin, QuickTime, and Vbrick VOD-W streaming servers are RTP servers.
RTSP	Real Time Streaming Protocol is a network control protocol used to control streaming media servers. RTSP defines the control sequences in streaming playback and uses TCP to maintain an end-to-end streaming connection.
SDP	Session Description Protocol. A standard which provides information about the timing and format of a live RTP stream and provides information on how to tune into the stream. It can be provided as part of a session creation in a protocol such as RTSP or as a text file with a .sdp extension.
SIP	Session Initiation Protocol is a signaling protocol widely used for controlling video conferencing communication sessions.
StreamPlayer	Vbrick PC application used to view live and on-demand streams. StreamPlayer can discover program names on a network by listening for session announcements (SAPs) from Vbrick devices.
Transmux	The process whereby a digital bit stream is converted from one file format or streaming protocol to another—without changing the compression method. An example of transmuxing is when a unicast stream is converted to multicast or when an RTP stream is converted to RTMP.
Transport Stream (TS)	MPEG transport stream (MPEG2TS) is a standard format for transmission and storage of audio and video. Transport Stream specifies a container format encapsulating packetized elementary streams, with error correction and stream synchronization features for maintaining transmission integrity when the signal is degraded.
Transrate	Change the speed/compression characteristics of a stream without changing the compression algorithm to accommodate different devices (e.g. laptop, mobile phone) on networks of varying qualities of service
Unicast	A bandwidth-intensive streaming mechanism wherein a separate and complete video stream is sent to each requesting client. Unicast is a one-to-one connection between the client and the server. See <a href="#">Multicast</a> .
VAdmin	An integrated management interface that lets you manage the DME configuration from an external web browser.
VBDirectory	A proprietary Vbrick application used to auto-discover Vbrick devices (including DMEs) on a local IP network. It is available on the Vbrick <a href="#">Downloads</a> page for new customers and is automatically installed when you perform an upgrade.
VBDME Download	A proprietary Vbrick application used to perform a software upgrade on DME appliances.
VC Gateway	Vbrick's Video Conference Gateway uses standards-based SIP and H.264 technology to become a participant in a video conference and stream the content to multiple endpoints including PCs, Macs, iPads, iPhones, etc.
VOD	Video-on-demand files are stored streams that can be played from the DME's FTP server via progressive download.

# Installation

## DME Installation Overview

There are two different ways that the server may be purchased from Vbrick – either as software (a virtual machine supplied as OVA or Hyper-V), or as physical hardware with the software. Partners may sell hardware with/without VMware to host the Vbrick virtual machine. Please identify which of the deployments you have for each of your DMEs.

Installation instructions are standardized to each DME version in Vbrick Release Notes and contain all the information necessary to deploy that version's DME as either a VM or as an update to an existing version.

Please refer to the [DME Installation](#) section of the DME Release Notes for the specific version of DME you are installing for further details.





# Getting Started

## How the DME Functions

The Vbrick DME is a multi-faceted platform that performs a variety of serving, reflecting, and transmuxing, and transrating activities and is comprised of the major components shown in the [DME Components](#) topic.

In a typical application, a DME receives a unicast stream over the WAN link (often over TCP) to effectively traverse the LAN and pass through firewalls. The DME then streams via unicast and/or multicast to a variety of different clients in the streaming protocol of choice for each client.

To conserve bandwidth, reflectors can be linked across the WAN to relay video streams from one remote site to multiple downstream DME reflectors. The net effect is that a single unicast stream across the WAN can reach tens of thousands of viewers. To improve reliability, reflectors can either pull or push streams across the WAN using TCP. If a network outage occurs, the DMEs will automatically reconnect and resume streaming without any user intervention.

To reach different classes of clients (e.g. PCs, STBs, and mobile devices), a single stream of H.264-encoded multi-bitrate (MBR) video can work in concert with reflectors to distribute streams in the most efficient manner. Reflectors can also *transmux* video streams, converting from one type of transport stream on the input to another type of transport on the output. In transmuxing, a digital bit stream is converted from one file format or streaming protocol to another—without changing the compression method.

An example of transmuxing is when a unicast stream is converted to multicast or when an RTP stream is converted to RTMP. H.264 offers a variety of transport protocols to ensure the reliable delivery of video over a variety of networks.

For live broadcasts, the Real-Time Transport Protocol (RTP) is efficient, while the Real-time Streaming Protocol (RTSP) offers the player controls (fast forward, rewind) needed for VOD playback. Newer transport protocols like RTMP and HTTP are optimized for Internet clients and mobile devices.

[DME Components](#)

## Plan for your DME Deployment

The DME provides a powerful way to redistribute media by allowing you to reach multiple/remote locations and multiple users with minimal use of streaming bandwidth. Streams can be converted from unicast to multicast or delivered as HLS streams from an RTMP/RTSP/RTP source. Since the DME accepts multiple types of input streams and provides multiple ways to output streams, it may not be entirely clear which use cases apply to you and what is the simplest way to deploy your solution using the DME. The best way to determine how to use the DME effectively is to understand three basic factors:

- How you will be delivering media to the DME. This is typically determined by how your media is currently being created, for example as RTP, RTMP, etc.
- How your clients will be viewing content from the DME.
- Which firewalls, virtual networks, proxies, encryption systems, etc. are in place that will need to be traversed and/or reconfigured.

Once you have a better understanding of these issues you are ready to start considering what type of input streams you will have (RTP or RTMP) and how will they be distributed. For example they can be pushed to the DME, pulled from the DME, or by unannounced unicast from the source or an announced auto-unicast to the DME. You will also know how your clients will be viewing the content, for example as RTP, RTMP, or both, using a standalone player, an embedded web page, or through Vbrick's VEMS Portal Server. You will also know whether or not the content needs to be relayed to another remote DME or to a CDN for Internet Distribution. Finally, knowing how many users you have and the bandwidth consumed by each will help to clarify how many DMEs and which models you will need to distribute the streams. By gathering this information in advance, and reading this manual carefully, you can help to ensure a successful deployment of the DME in your own unique environment.

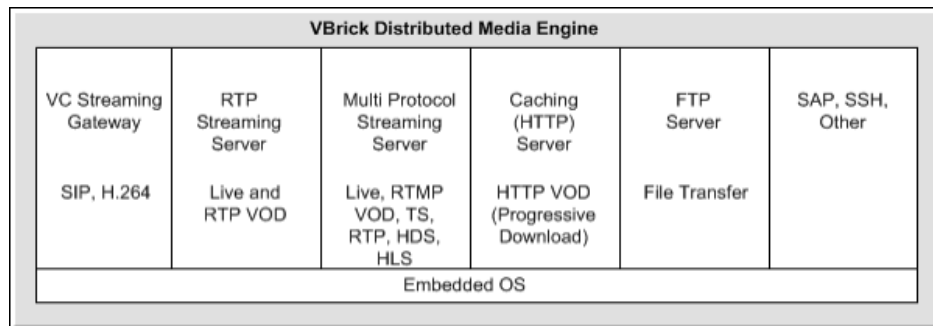
Firewalls can also play an important role in determining which use cases are appropriate. When no firewalls apply, a push or an auto unicast solution can be easily deployed. However if the DME is behind a firewall, you probably cannot reach it with a push without having to reconfigure the firewall. Similarly, you can probably pull a stream from a source into the DME. However if the source is also behind a firewall, more network planning, such as placing the DME in a "DMZ" (which the source can push to and the destination can pull from) may be a better solution. If virtual IP addresses are used, you will need to know more about the configuration of the network; and if deploying Vbrick multicast or RTP streams that will travel over UDP, your firewall may need to be configured to allow UDP data in and out.

## DME Components

### *Streaming Servers*

As shown in the figure below, the DME has an RTP server, a Multi Protocol server, and an HTTP server for progressive download.

The streaming servers and the VOD servers are built on a robust embedded operating system.



### How the DME Functions

## VOD Servers

The DME engine includes an RTP VOD server, a Multi Protocol VOD server, and an HTTP Progressive Download server. All stored VOD files are added to the DME via FTP.

The VOD servers support all of the file types shown in the table below.

VOD Server	Supported File Types
RTP	mp4, mov, m4a, m4v
Multi Protocol	flv, f4v, mp4, mov, m4a, m4v (H.264)
HTTP	all available files including M3u8 (HLS) and f4m(HDS)

## FTP Server

The DME has a fully functional Web server that uses File Transfer Protocol (FTP) to populate the DME with files for progressive download. You can FTP to the **FTP** folder on the DME or to a sub-folder.

When adding VOD files via FTP, you must wait for the ingestion to complete before the stream will play in VEMS. You can view the ingestion progress on the **Status** page in the VEMS client. If the ingestion is not complete, the title will display but the stream will not play.

## Caching (HTTP) Server

The DME has an internal Web server that serves VOD files via progressive download. It also serves video content via the various HTTP adaptive streaming protocols. The HTTP content is cached at remote locations so that subsequent requesting clients can acquire the content that is cached on a local server.

### Caching

## Storage Extension Capabilities

The DME supports Storage Area Network (SAN)/iSCSI storage extension options if needed. New disks may be added to the VMWare virtual environment as well to extend the current content area available. At present, these are the only supported extension options available.

### SAN/iSCSI Setup

### Provision a New Disk

## Streaming Overview

DME input and/or output streams can be configured to play on desktops (with a variety of players), set top boxes, and mobile devices at different locations and in a variety of different physical configurations. Vbrick recommends using a generalized streaming playback software (VLC is a good example at [www.videolan.org](http://www.videolan.org)). In order to test the stream, it must be accessible from the DME (in terms of network reachability, origin stream availability for streaming into DME, and stream availability for streaming out of DME). This approach is not feasible when the DMEs are in Stream Authorization mode. URLs for the streams are available on the DME under the MPS Connections page.

---

The DME supports unicast and/or multicast for both input and output.

Unicast streams typically have one source and one destination; most network traffic between clients and servers is unicast.

Multicast packets have a single source and multiple destinations. Instead of sending out individual unicast packets to each client, a single stream of multicast packets can be viewed by multiple clients. This can save substantial network bandwidth when multiple clients are accessing the same stream.

### ***Served VOD Streams***

The DME has an RTP server, an RTMP server, and an HTTP Progressive Download server for stored VOD files (including Windows Media files). In server mode, a served stream does not become active on the network until requested by a client. The client may be a software player like StreamPlayer or QuickTime running on a PC, a Macintosh, a mobile device, or a set top box like the Vbrick Multi Format set top box.

The user requests a stream from the DME by directing the client to issue an RTSP/RTMP/HTTP request via a URL to the DME. The client and the DME then exchange a sequence of RTSP/RTMP messages to direct the DME to send the program to the client.

The DME server examines the file to determine Transport Type, Video Rate, Audio Rate, and other parameters. It then plays the stream using optimal settings adjusted for bandwidth, frame rate, etc.

**Note:** New content files that are transferred via FTP will not be available immediately for VOD RTMP streaming until the associated seek and meta files are generated. Meta and seek files are typically generated within a few minutes of being transferred.

**Table 1.** Supported Stored Stream Types/Players

			Players										
			WM Player	iPhone, iPad	Android	QuickTime (MAC)	QuickTime (PC)	Flash Player	StreamPlayer, Vbrick MAC Player	Silverlight/Smooth Streaming Player	MF-STB	Amino STB	
<b>Stream Types</b>	Windows Media (wmv, wma, asf)	Progressive Download	Yes	No	No	No	No	No	No	Yes	Yes	No	No
	Flv, f4v	Progressive Download	No	No	No	No	No	Yes	No	No	No	No	No
	m4v (assumes AAC audio)	Progressive Download	No	Yes	No	Yes	Yes	Yes	No	No	No	No	No
	MPG, TS (H.264, Mpeg2)	Progressive Download	No	No	No	No	No	No	No	No	No	No	No
	MP4, mov (H.264)	Progressive Download	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
	MP4, mov(MPEG4P2)	Progressive Download	No	No	No	Yes	Yes	No	No	No	No	No	No
	Flv, f4v	RTMP, RTMPT	No	No	No	No	No	No	Yes	No	No	No	
	m4v (assumes AAC audio)	RTMP, RTMPT	No	No	No	No	No	No	Yes	No	No	No	No
	MP4 (H.264)	RTMP, RTMPT	No	No	No	No	No	No	Yes	No	No	No	No
	MP4, mov (H.264)	RTSP	No	No	Yes*	Yes*	Yes*	No	Yes*	No	Yes*	No	No
	MP4, MOV (Mpeg4P2)	RTSP	No	No	No	Yes*	Yes*	No	Yes*	No	Yes*	No	No
	MPG, TS (H.264, Mpeg2)	RTSP	No	No	No	No	No	No	No	No	No	No	No
	HLS file (m3u8 manifest)	DASH	No	Yes	Yes (4.0)	Yes	No	No	No	No	No	No	No
	HDS file (f4m manifest)	DASH	No	No	No	No	No	No	Yes	No	No	No	No
	Smooth Streaming files (ism manifest)	DASH	No	No	No	No	No	No	No	No	Yes	No	No

\* Only if the MP4 files are hinted

## **Pushed Streams**

The DME also pushes live streams to a configured destination. The destination may be a single endpoint in the case of a unicast, or multiple endpoints in the case of multicast. The transmitter does not directly depend on a client to initiate the streaming but is always transmitting (in the case of multicast) and transmits if the client is reachable and listening (in the case of unicast). The streams are transmitted across the network via RTP, RTMP, or Transport Stream. Note that RTMP is a unicast-only protocol.

## Pulled Streams

The Multi-protocol Streaming Server can pull live streams from an RTSP/RTP server or an RTMP server. It can pull from various outside sources, for example from another DME, or from a Wowza, FMS, QuickTime, or Darwin streaming server. These streams can then be served or pushed via various protocols.

## Transmuxed Streams

Transmuxing is the process whereby a digital bit stream is converted from one file format or streaming protocol to another—without changing the compression method (as opposed to *transcoding* which actually changes the compression method). The DME transmuxes streams; it does not transcode streams. An example of transmuxing is when a unicast stream is converted to multicast or when an RTP stream is converted to RTMP. The following table shows the live input streams that are supported in the left column and the live output streams that are supported in the top row.

**Table 1.** Live Transmux Capabilities

		DME Output Streams										
		RTMP Unicast Pull	RTMP Auto-Unicast	RTP Unicast Push	RTP Auto-Unicast	RTP Unicast RTSP Pull	RTP Multicast	TS Unicast Push	TS Unicast RTSP Pull	TS Multicast	Apple HLS	VC SIP
<b>DME Input Streams</b>	RTMP Unicast Pull	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	RTMP Auto-Unicast	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	RTP Unicast Push	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	RTP Auto-Unicast	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	RTP Unicast RTSP Pull	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	RTP Multicast	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	TS Unicast Push	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	TS Unicast RTSP Pull (3.1.1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	TS Multicast	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	Apple HLS	No	No	No	No	No	No	No	No	No	Yes (Cache)	No
Adobe HDS	No	No	No	No	No	No	No	No	No	Yes (Cache)	No	
VC SIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	

## Transrated Streams

Transrating is the process where a digital bit stream is converted from one bit rate to another—without changing the compression. An example of transrating is when a high bit rate stream is converted into multiple lower bit rate streams for delivery to mobile devices. Note that the

DME does not change the resolution of the source stream, although the receiving device will generally display the stream at its preferred resolution.

**Note:** When working with streams with closed captions, do not change the framerate. You can still change the resolution and bitrate, but changing the framerate will have adverse effects on CC data. In these cases, please keep framerate set to **Current Rate**.

### Stream Conversion

## VBAAdmin

The Vbrick DME server has an integrated management interface (VBAAdmin) that lets you manage the DME configuration from an external Web browser. This allows network managers to remotely configure and monitor the appliances from virtually any location that has Web access.

The most convenient way to access the VBAAdmin interface ([DME Status \(Snapshot\)](#)) is via the [VBDirectory](#) utility. After installing VBDirectory you will see the initial screen shown for [VBDirectory](#). Locate a specific DME and simply double-click on the **Name** to launch the VBAAdmin [Login to the DME](#) screen.

To optimize the functionality of this tool, set the **Host Name** of the DME (on the **System Configuration > Network** page) to a meaningful text string during initial configuration.

Alternatively, if you know the DME's IP address, you can access it directly from a browser. As shown in the table below, you can launch VBAAdmin in Internet Explorer or Firefox (other browsers are not supported by Vbrick). Connect to VBAAdmin by pointing to the IP Address and Port Number (for example: <http://192.168.5.5:8181>) of the DME and log in with valid credentials. **Note that the DME's management interface is not on Port 80.** By default the admin port for the DME is **8181**. This allows Port 80 to be reserved for HTTP downloads.

Browser	Version
Microsoft Internet Explorer	8.0 or higher
Mozilla Firefox	3.6 or higher

[DME Status \(Snapshot\)](#)

[VBDirectory](#)

[Login to the DME](#)

### ***Login to the DME***

The DME ships with DHCP enabled and you can use [VBDirectory](#) to auto discover the IP addresses of all DMEs in your network. The VBDirectory application (which you can install on a local PC) is provided free of charge. It is available on the Vbrick [Downloads](#) page for new customers and is automatically installed when you perform an upgrade.

Once you know the DME's IP address, you can login by entering the server's IP address or host name and the management port (**8181**) in the address bar of your browser.

When the login page is displayed, enter a valid **User Name** and **Password** (default = **admin** for both) to launch the VBAAdmin management interface.

---

A typical login URL would have the following format:

**http://172.22.2.50:8181**



**Note:** Administrators should be aware that the *DME's management interface is not on Port 80* as is typical for most web-based admin tools. By default the admin port for the DME is 8181. This allows Port 80 to be reserved for HTTP downloads.

[VAdmin](#)

[VBDirectory](#)

[DME Status \(Snapshot\)](#)

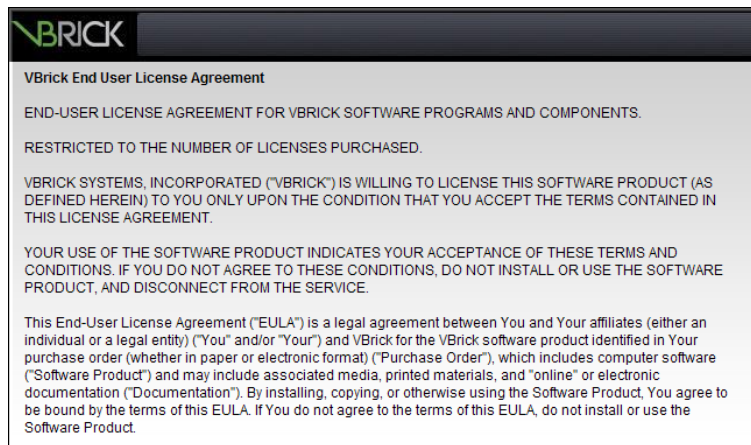
## **Log Out of the DME**

To log out of the application, click **Log Out** in the navigation panel on the left. As a security measure, if no keyboard activity is detected for 20 minutes, VAdmin will automatically timeout and display the Login page.

It is highly recommended that you use the **Username and Password** page in VAdmin to change the user name and password after logging in for the first time. The user name and password cannot exceed 20 characters.

## **End User License Agreement (EULA)**

The first time you launch the DME you will need to page down and click on **Accept EULA**. This means that you accept the end user license agreement for the Vbrick software. The application will not run if you decline to accept the EULA.



## **Register the DME**

**Note:** If you have purchased a hardware DME, it will come pre-registered from the factory and you do not have to complete the registration steps described in this section. These steps below are for software-only DMEs only.



The registration splash page is automatically displayed after accepting the EULA. You will need to register your DME with Vbrick before you can run the application.

The following items will be required to register a DME:

1. The MAC address of the DME machine
2. The serial number(s) for future support
3. A license file.

The MAC address is pre-filled on the registration page (see above); the serial number(s) are available using the “License Activation” letter you received with your order. And a license file is obtained through Vbrick Support Services.

▼ To obtain a license file and register your DME:

1. Contact Vbrick Support to obtain the license files needed for the type of DME and features purchased.
2. Click on the green hyperlink for information on how to contact support.
3. When prompted, browse to a folder where you will save the .lic license file (once received from support).
4. Open the .lic file in Notepad and copy the entire contents. Then go back to the **DME Registration Page** and paste the contents into the license text box.
5. Enter the Serial Number(s) from the sticker in the serial number text box on the “License Activation” letter you received with your order.
6. Click **Finish Registration** to complete your registration.
7. A similar process is followed to license and activate new features on a previously existing and license DME.

Activate Feature

## *The Apply, Revert, and Default Buttons*

Depending on screen resolution, it may be necessary to scroll down the page to see additional information and fields. The **Apply**, **Revert** and **Default** buttons however, are always shown at the bottom of the page when appropriate.

You may also see **Refresh**, **Reset Counters**, and other buttons depending on what page you are on.

Apply	Applies the changes made on the screen to the appliance. Each configuration page has an <b>Apply</b> button. You must click <b>Apply</b> before you exit the page; otherwise your changes will be lost.
Revert	Aborts all changes made on the screen and returns to the values that were present prior to any changes. The <b>Revert</b> button restores the values that were present prior to the last "apply."
Default	Returns to the default settings for all parameters on the page. You must still click <b>Apply</b> for these default settings to take effect.

## System Reset

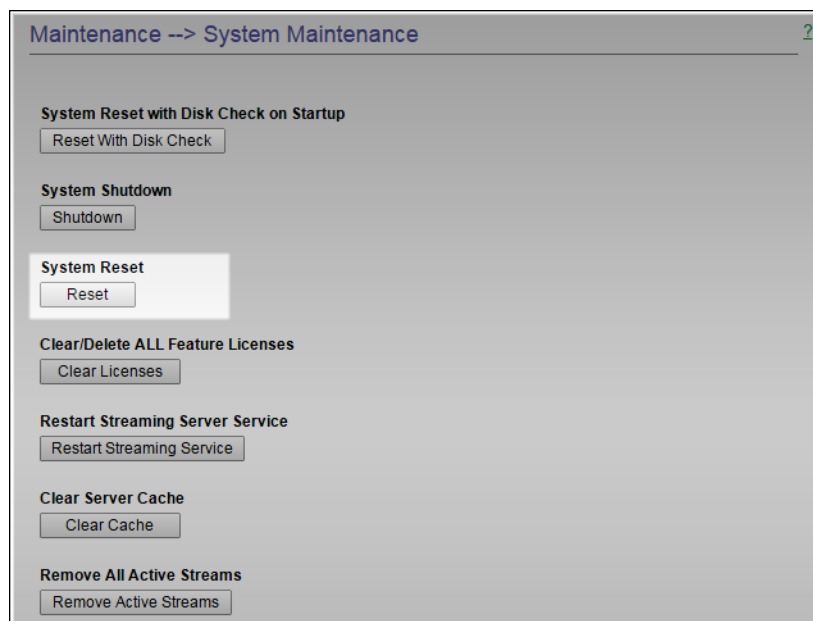
### *Reset the System*

A system reset resets (i.e. reboots) the appliance. It does not change, save, or reset any configuration parameters.

▼ To reset the DME:

1. Navigate to Maintenance > System Maintenance.
2. Click the **Reset** button under the **System Reset** label.

**Note:** Some changes to the configuration will initiate an automatic reset. When this happens, wait approximately 60 seconds, then refresh the page and log back in with your user name and password.

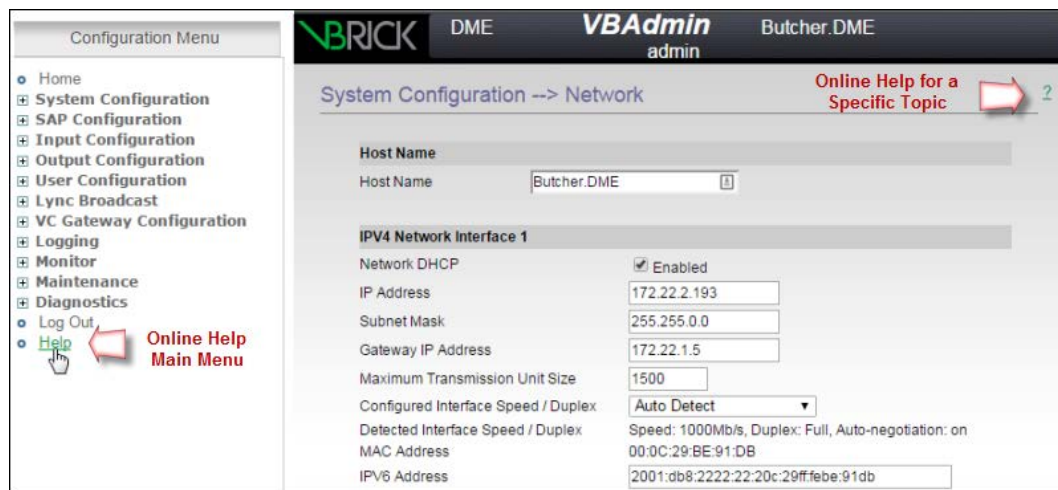


## System Reset

## Online Help

A link to the Online help system is available from the Configuration Menu on the left side of the VBAAdmin page. This help system has a powerful full-text search engine that can quickly find the information you need. You may wish to take a few minutes to familiarize yourself with the help system. It can save time when trying to find information about DME parameters or options.

When using VBAAdmin, click on the question mark hyperlink in the upper-right corner of each page to get context-sensitive help for that page. *Be aware that you must have an Internet connection to see the Online help.*



## DME Status (Snapshot)

The DME **Status Snapshot** page has the **Configuration Menu** on the left and a read-only **Status Bar** displaying the health of the system on the bottom. The Status Snapshot is the first page that you see upon logging in to the DME and displays relevant system information about your DME.

Each section of your Status Snapshot page is explained below.

**Note:** Be aware that the VBAAdmin pages (including the snapshot page) are not automatically refreshed. To update any page with the latest information, re-click the link for that page in the **Configuration Menu** in the left pane.

Status (Snapshot) 2

For additional system status, please refer to the Status Bar at the bottom of the screen.

**CPU Configuration**

CPU(s): 32 total ICPU [2 Sockets, 8 Cores, 2 Threads/Core]

**Disk Status**

Disk Usage System: Used: 2046 MB (1%), Available: 437578 MB (99%)

Disk Usage Content: Used: 93146 MB (2%), Available: 4671531 MB (98%)

Disk Health:

- 0 SMART Health Status: OK
- 1 SMART Health Status: OK
- 2 SMART Health Status: OK
- 3 SMART Health Status: OK
- 4 SMART Health Status: OK
- 5 SMART Health Status: OK
- 6 SMART Health Status: OK
- 7 SMART Health Status: OK

iSCSI Usage: iSCSI Disabled

**Memory & Swap Status**

	Used		Free		Total
RAM:	12.5 GB	20%	50 GB	79.9%	62.5 GB
SWAP:	0 KB	0%	47.9 GB	100%	47.9 GB
<b>Total:</b>	<b>12.5 GB</b>	<b>11.3%</b>	<b>98 GB</b>	<b>88.6%</b>	<b>110.5 GB</b>

**Software Licenses**

DME HIGH Expires: 2029-04-30  
Transrate Expires: 2029-04-30

Settings compared to installed **DME HIGH** license

	Required	Actual
CPU:	16	32
Physical Memory:	32 GB	62.5 GB
SWAP Memory:		47.9 GB

Licensed Settings	Maximum	Current
MPS Connections:	2200	2200
MPS Bandwidth:	3072 MB	3072 MB

Field	Description
CPU Configuration	<p>This section reports the CPU configuration of the machine or VM. It will identify the following:</p> <ul style="list-style-type: none"> <li>Total number of Logical CPUs (lCPUs). This number is repeated in the Software Licenses section with the required number of CPUs.</li> <li>The CPU configuration is also provided, defining the number of sockets, cores and threads. (Note: 2 threads/core implies Hyper Threading).</li> </ul> <p><b>See:</b> <a href="#">Vbrick DME Checkup Guide</a></p>
Disk Status	<p>The disk status reports both usage and health (as reported by SMART). These is over the two logical disks for Content (where your downloaded videos, created HLS, and disk caching storage is kept) and System (where your OS is kept.) Please monitor the size and health of your Content disk.</p> <ul style="list-style-type: none"> <li>Disk Usage System: Total megabytes used and available for DME system resources.</li> <li>Disk Usage Content: Total megabytes used and available for DME content.</li> <li>Disk Health: Reports any disk issues found during the nightly SMART reports and returns a PASSED condition if none are found. This includes any error condition or pre-failure of the DME disk.</li> <li>iSCSI Usage: Total megabytes used and available on iSCSI device (if enabled).</li> </ul>
Memory & Swap Status	<p>RAM and Swap memory usage statistics (used, free, and total). These are the values reported to the DME (using the linux free command).</p> <p>Note: Memory MIB values retrieved by SNMP are different. Please refer to the System Configuration &gt; SNMP help page.</p>

Field	Description
Software Versions and Licenses	<p>The DME is a collection of multiple services running on a server. This section identifies the current version numbers, as well as your system licenses. Please use these version numbers when contacting Vbrick Support. Please monitor the license expiry dates and act as necessary.</p> <ul style="list-style-type: none"> <li>• Application Code Revision: DME software code revision currently installed.</li> <li>• MPS Server Version: RTMP server software code revision.</li> <li>• OS Registration Number: OS registration number.</li> <li>• System Licenses: Types of licenses installed and expiration dates.</li> </ul>

### Configuration Menu

#### DME Status Bar

#### DME Status (Historical)

#### VBAdmin

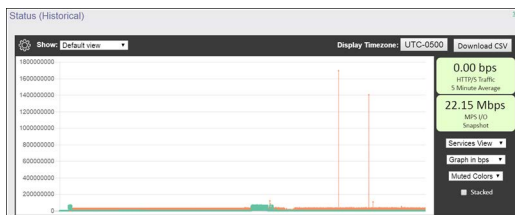
#### VBDirectory



#### Login to the DME



## **DME Status (Historical)**

The DME **Status Snapshot (Historical)** page provides a historical view of various health measures of your DME in an easy to review chart format. These measures and charts are meant to show trends for quick viewing. Stronger reporting should happen through SNMP or Rev. The data presented in these charts are held for a 2 week window and older measures are deleted in a nightly process (at about 4am local DME time.) Therefore, the graphs will only contain up to 2 weeks of data.

**Top Bar Controls:** There are several controls displayed within the top bar, spanning the charts. These are not chart specific.

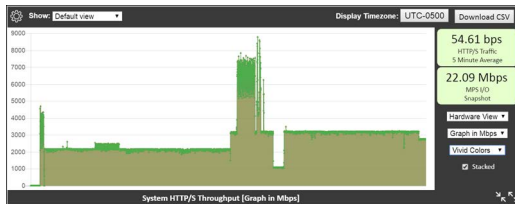


Control	Description
	Clicking the <b>Gear</b> icon toggles the display of the bottom axis for each graph as well as the legend (which are both off by default.) Once displayed, clicking on the Data set names within the Legend will toggle its display within the graph.
	The <b>Show</b> drop-down allows you to pick the number of days to display. This displays today or up to the last N days. In this way, smaller more pinpointed views can be generated.

Control	Description
	<p>The <b>Display Timezone</b> button displays the current timezone in UTC. It will be of the format UTC+#### or UTC-####, where #### is the displacement in hours off UTC. Clicking this button toggles between the DME's native timezone and UTC+0000. Only the dates on the graph will change if displayed. Toggling the timezone is handy when comparing graphs from multiple DMEs in different timezones, as all can be normalized to UTC+0000 and provide direct time comparisons. This relieves the need for the addition and subtraction previously necessary.</p>
	<p>The <b>Download CSV</b> button is for advanced users who wish to chart or investigate information offline. This downloads a file (named DMEStats- &lt;&lt;DATE&gt;&gt;to&lt;&lt;DATE&gt;.csv) of all the measurements within a comma-separated-values format – easily imported into common spreadsheet programs. This may take a moment for the DME to generate and download, so please be patient. Each of the columns is labeled and represents a 5 minute average measurement. Note: cpu_time is not an average, but a snapshot measurement. Definitions of the included data can be found in "<i>Squid: The Definitive Guide</i>" at <a href="https://www.amazon.com/Squid-Definitive-Guide-Duane-Wessels/dp/0596001622">https://www.amazon.com/Squid-Definitive-Guide-Duane-Wessels/dp/0596001622</a> or via PDF off the Internet. Again, remember that the data is only kept for two weeks, so please download accordingly.</p>

### Notes on Each Graph:

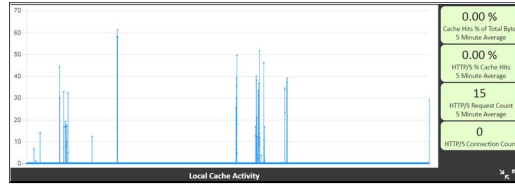
**System HTTP/S Throughput.** This graph shows all the HTTP or HTTPS (e.g., HLS) traffic that is going through the caching engine. These numbers are 5 minute averages and samples. Snapshots of additional current measures are provided on the right hand side.



There are three controls related to this graph:

- **Services View / Hardware View.** This will switch the view of the graph to display either the streaming services bandwidth, or to view bandwidth by NIC (network interface card). Selecting the Hardware View will automatically stack the results and hide the Total (which is the sum of all the NICs).
- **Graph in UNIT\_MEASURE.** This allows you to select the unit measure for the graph. It is always displayed in bps (bits per second), but you can display it in Mbps, Gbps, etc. Changing the units will also change the chart title at the bottom of the chart to help avoid confusion.
- **Colors.** A selection of different colors for the chart.

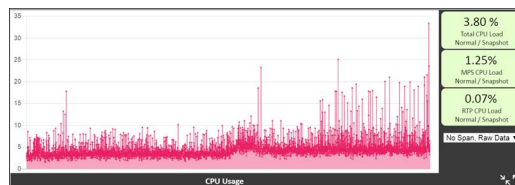
**Local Cache Activity.** This multi dataset graph provides insight into how much your local DME cache is being used (either from local or remote requests). These numbers are 5 minute averages and samples. Snapshots of additional current measures are provided on the right hand side.



Toggle the axis and legend to see the datasets included in this chart, they are:

- **Dataset: Cache Hits % of Total Bytes.** This is the percentage of bytes delivered that come from the cache. Logically, the higher the better for this measure as performance from the cache is quicker and more efficient. In some cases you may see negative results – this represents requests made but not fully delivered by the cache (this is expected in some use cases).
- **Dataset: HTTP/S Request Count.** This is a raw count from our cache engine on the number of requests to the DME.
- **Dataset: HTTP/S % Cache Hits.** This is the percentage of request counts that are delivered by the cache. This differs from the measure above because this is a count of requests, not total bytes delivered by the requests. Again, the higher the better – this translates directly as how your cache is being used.

**CPU Usage.** This is a running representation of your (aggregated) CPU usage. In most cases, your CPU usage will bounce within a range (these are snapshots, not averages), but the trend should be evident. This view can also illustrate the impact of high CPU DME actives (e.g., transrating via Stream Conversion feature). Snapshots of additional current measures are provided on the right hand side.



There is one additional control related to this graph:

- **Windowed Average.** The dropdown within the CPU chart will allow for viewing the raw data (select "No Span, Raw Data") or a windowed average ("Average Span N=?"). A windowed average is calculated as the average of all the numbers (based on N) around a data point. For example, using N=5 window or span, calculating the 12 element in the dataset would be:

$$\text{Data}[12] = (\text{Data}[10] + \text{Data}[11] + \text{Data}[12] + \text{Data}[13] + \text{Data}[14])/5$$

And so on. Using these views will disable the raw view for clarity. These views are useful if you have increased variability in the CPU measures. The CPU measures, as a reminder, are pinpoint measurements and may fluctuate quite a bit depending on your DME use.

**Note:** The CPU Usage graph, in particular, can contain a great deal of data. As such, it may take a moment to load and subsequently process any view or chart changes. This may also be affected by the compute power of your PC and connectivity. This is to be expected for large datasets. For detailed analyses, please take advantage of the data download capability.

**Note:** Be aware that Historical status page is not automatically refreshed, nor are the changes to views retained. To update this page with the latest information, re-click the link for that page in the **Configuration Menu** in the left pane.

All graphs have the common controls explained below.

Control	Description
Decrease Height of Graph	This will decrease the height of the graph. This does not refresh the data on the page, only the display parameters.
Increase Height of Graph	For cases where you wish to drill into the data or have higher resolution, this will increase the height of the graph. This can be clicked numerous times. This does not refresh the data on the page, only the display parameters.

[Configuration Menu](#)

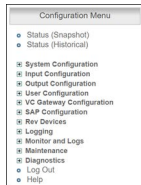
[DME Status Bar](#)

[VBAdmin](#)

[VBDirectory](#)

[Login to the DME](#)

## Configuration Menu



The DME **Configuration Menu** on the left side of the VBAdmin page provides access to all configurable DME parameters. Use the (plus and minus) tree controls to expand or collapse the menu. Click on any item in the menu to display the corresponding configuration page. Note that the DME is a reflector will always send what is received. For this reason, there are no video or audio configuration fields on the DME pages nor do the destination pages let you select different video and audio rates.

<a href="#">DME Status (Snapshot)</a>	Displays a snapshot of important status indicators including software version and the current number of client connections.
<a href="#">DME Status (Historical)</a>	Provides a historical view of various health measures of your DME in an easy to review chart format. These measures and charts are meant to show trends for quick viewing. Stronger reporting should happen through SNMP or Rev.



<a href="#">System Configuration</a>	Provides access to configurable system parameters such as Network, Streaming and Caching. You may also activate new licenses or DME features through this menu option.
<a href="#">Input Stream Configuration</a>	Lets you configure input stream types.
<a href="#">Output Stream Configuration</a>	Lets you configure output stream types.
<a href="#">User Configuration</a>	Lets you configure the DME user name and password and the announce settings that let you push streams into the DME.
<a href="#">SAP Configuration</a>	Allows configuration of announcements of DME capabilities and streams.
<a href="#">Rev Devices</a>	Allows configuration of Vbrick's Multi-Format Set Top Boxes for use with Rev (via multicast SAP messages captured by local DMEs and forwarded to Rev).
<a href="#">Logging</a>	Lets you enable and configure the <a href="#">Access History</a> and the <a href="#">Error Log</a> .
<a href="#">Monitor and Logs</a>	The <a href="#">Monitor and Logs</a> pages show status information for users and relays as well as the Access History and the Error Log.
<a href="#">Maintenance</a>	Provides access to system maintenance options including Shutdown and Reset.
<a href="#">Diagnostics</a>	Explains how to run diagnostics when troubleshooting issues.
<a href="#">Log Out of the DME</a>	Logs out the current user and displays the <a href="#">Login to the DME</a> page. VAdmin automatically times out and displays the Login page after 20 minutes with no activity.
<a href="#">Online Help</a>	Displays the Online help system. You can also click the question mark (?) icon on any page to go directly to the help for that specific page. You will need an Internet connection to display the Online help topics.

## DME Status Bar

The DME **Status Bar** on the bottom of the VAdmin page provides near-real time updates and reporting on DME functions. The values on the bar update every two minutes or you may use the **Refresh** link to update them manually as needed. The different sections and what they mean are described below.



Section	Description
---------	-------------

DME/Server Status	<p>The first section identifies the following:</p> <ul style="list-style-type: none"> <li>• DME Version. Hover to see uptime.</li> <li>• Overall DME Status (Normal, Warning, and Alert) text</li> <li>• Server status message. The “Server is Running” message indicates that the MultiProtocol Server (MPS) is running and will change to “Server is Idle” if the MPS is not running (e.g., if the Disable Server button is toggled.) The field’s background color will change indicating its health status. The server status (Normal, Warning, and Alert) is tied to Content Disk, CPU, Throughput and Memory status – any elevation of these statuses will be reflected in this status.</li> <li>• This field also provides the following information: <ul style="list-style-type: none"> <li>• Status of Stream Authorization feature (either Disabled or Enabled).</li> <li>• Any pending License Expiry dates (within 45 days of expiry).</li> </ul> </li> </ul>
MPS Streams	<p>This area displays the number of streams going through your Multiprotocol server, your stream capacity, and associated CPU usage. This covers your RTMP, RTMFPS, HLS, and HDS streams.</p>
RTP Streams	<p>This area displays the number of streams going through your RTP server, your stream capacity, and associated CPU usage.</p>
CPU Usage	<p>This is a snapshot of the aggregated <b>CPU Use</b>. The field’s background color will change indicating its health status. The available statuses are: Normal (0%-70% CPU usage), Warning (71%-80%), and Alert (&gt; 80%). As a snapshot, this is a transient measure that may self-correct. These thresholds are applied on snapshots and represent hard cut-offs between the status – please consider your use cases, the status, and the actual measure within the status to help determine if action is necessary.</p> <p>Additionally, to the aggregate number, is a breakout of CPU usage by the primary streaming services.</p> <p><b>Guidance:</b> A DME, depending on load may bounce into and out of a Warning or Alert stages during the normal course of use. If your DME is constantly running in Warning, you should consider and monitor the CPU usage. Please also investigate CPU intensive configurations (such as Stream Conversion / transrating). If this leads to adding additional CPU resources (e.g., within a VM), then please review the <a href="#">DME Checkup PDF</a> in <a href="#">DME Supplementary Documentation</a> for additional information.</p> <p>If your DME bounces into an out of Alert, but does not remain in that state for more than 1 or 2 refreshes of the Status Bar, action may not be necessary but as a cautionary measure you may wish to monitor the DME load and playback experiences. If your DME is consistently reporting in Alert status, then please evaluate your configuration and load. Particularly, watch the MPS monitor page for stream packet loss which may indicate that the DME is running too hot. The Critical alert is a range, so the higher it goes the more drastic intervention Linux will take to keep the system running.</p>

Memory + Swap Usage	<p>This is a snapshot of the <b>Memory Use</b> in your system. Memory is measured as your physical plus swap. Hovering your mouse over the measures will provide detailed measures.</p> <p>The field's background color will change indicating its health status. The available statuses are: Normal (0%-50% memory usage), Warning (51%-85%), and Alert (&gt; 85%). As a snapshot, this is a transient measure that may self-correct. These thresholds are applied on snapshots and represent hard cut-offs between the status – please consider your use cases, the status, and the actual measure within the status to help determine if action is necessary.</p> <p><b>Guidance:</b> A DME, depending on load, shares its memory with all other system services. When we examine the memory, we combine the system RAM and SWAP because it is really a high measure of this combination that may indicate issues. In most cases, the SWAP will have little use, but there are some use cases that may drive it up. Because the memory measure includes SWAP it may drive higher into Warning or Alert based on the frequency that the system returns SWAP memory from running or terminating apps. In most cases, spikes of memory use that drive Warning or Alert reflect singleton events within the system, and may be transitory. Meaning, if your DME bounces into an out of Warning or Alert, but does not remain in that state for more than 1 refresh of the Status Bar, action may not be necessary but as a cautionary measure you may wish to monitor the use and playback experiences.</p>
---------------------	--

Content Disk Usage

This is a snapshot of the **Content Disk Usage**. DMEs can be thought of as having two logical partitions – an OS partition and the content partition. This snapshot measures the content partition and does not include the OS partition. The content partition, however, does include some system files. The field's background color will change indicating its health status. The available statuses are: Normal (0%-85% usage), Warning (85%-90%), and Alert (> 90% OR less than 32GB free). As a snapshot, this is a transient measure that may self-correct. These thresholds are applied on snapshots and represent hard cut-offs between the status – please consider your use cases, expansion of content plans (disk growth can be fast or slow depending on content ingestion into Rev), the status, and the actual measure within the status to help determine if action is necessary.

It should be noted that a DME that is reporting Warning or Alert will actively try, via our LRU (Least Recently Used algorithm) to free up space within the UploadedVideos directory. So, depending on settings, DMEs should not stay in this state.

**Guidance:** When evaluating the content disk size, please consider that this partition is shared by a number of DME activities. This partition will include not only (per configuration) new pre-positioned content, but also any content that gets pre-positioned during normal use. Recording are maintained in this space. And, the system swap file (which can be several GB depending on your DME License) is contained within the content space.

Also, it should be noted that your Caching system also utilizes the content store as well in accordance to the levels specified on the Streaming page. So, if you mark your DME as a DEDICATED caching server, much disk space will be used. In terms of guidance, it depends on your use case. If your DME is used in a highly caching environment, then running at higher disk use will automatically self correct. Also, even in a largely pre-positioned environment, the DME will self correct – it will delete pre-positioned content as it needs space. It will not, however, delete space that has been used by the caching engine (which can be cleared manually on the Maintenance page). If you are concerned about your disk availability, please review your Cache settings, pre-position settings on Rev, and potentially add additional space through the DME Admin interface.

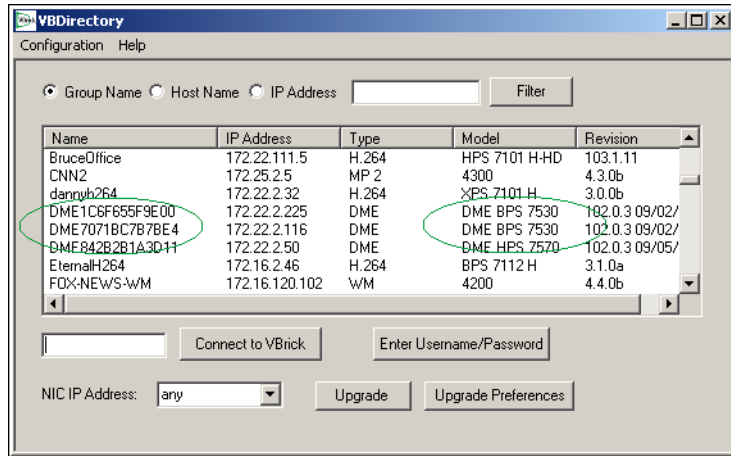
MPS IO	<p>Snapshot of current <b>MPS</b> (only) IO (throughput) and is measured in accordance to the allowable limit for the DME license. The field's background color will change indicating its health status. The available statuses are: Normal (0%-60% throughput usage), Warning (61%-90%), and Alert (&gt; 90%). As a snapshot, this is a transient measure that may self-correct. These thresholds are applied on snapshots and represent hard cut-offs between the status – please consider your use cases, number of current streams IN/OUT, the status, and the actual measure within the status to help determine if action is necessary.</p> <p>**</p> <p><b>Guidance:</b> A DME, depending on load may bounce into and out of a Warning status during the normal course of use. If your DME is constantly running in Warning, you should consider your distribution configuration against available licensed throughput. If your DME bounces into an out of Alert you may wish to actively monitor the use and playback experiences. If your DME is consistently reporting in Alert status, then please evaluate your configuration and load. Particularly, investigate the IN/OUT configuration of streams, number of attaching DMEs/players, and watch the MPS monitor page for stream packet loss which may indicate that the DME is running too hot.</p>
Cache IO	<p>Snapshot of current <b>HTTP/S caching (only) throughput</b>. Hovering your mouse over this field will provide detailed measures for in/out traffic and local cache use. These measures are averaged over 5 minutes.</p> <p><b>Note:</b> Unlike the other measures, this measure is not compared to thresholds and does not report a health status or color.</p>
DME/Server Status	<p>The last section contains a number of important items:</p> <ul style="list-style-type: none"> <li>• DME FQDN and IP – hover for uptime.</li> <li>• MPS running status (hover for MPS version)</li> <li>• RTP running status</li> <li>• Rev status (Status to denote if the DME is linked to Rev and if the Rev interface is running. If either of these is Red, it indicates a problem connecting with Rev. Please check your Rev Interface page.)</li> <li>• Refresh countdown (Countdown until the Status Bar values are refreshed automatically by the DME. Refresh link to refresh them manually. If the Status Bar does not automatically refresh, you may also refresh the whole page using your browser refresh.)</li> <li>• MPS Disable Server button which will toggle the status of the MPS server.</li> </ul>

## VBDirectory

VBDirectory is Vbrick management application that discovers and displays all Vbrick devices (including DMEs) connected to your network. It displays the **Name** (as DME and MAC Address), **IP Address**, and **Model** (see the table below) for each DME on your network.

VBDirectory is an easy way to connect to the management pages for the DME or other Vbrick devices. The VBDirectory application is available on the Vbrick [Downloads](#) page for new customers and is automatically installed when you perform an upgrade.

*Be aware that you will need VBDirectory v5.3 or higher to discover the DMEs on your network.*



Type	Model	Recommended Concurrent Users
DME	BPS 7530	50–100
DME	XPS 7550	1000 or less
DME	HPS 7550	1000 or more

[VBAAdmin](#)

[Login to the DME](#)

[DME Status \(Snapshot\)](#)

## Configure the DME with Secure Shell (SSH) or a Console

The DME ships with a configuration and monitoring tool called the SSH Admin Interface. The tool is available via a Secure Shell (SSH) v2 connection (or on the Console if you have direct access.) This tool is useful to perform basic configuration and monitoring. Specifically, it is useful to initially configure your network connections after an install.

To access the tool, please log in using SSH. This requires a client application like PuTTY, mRemoteNG (Windows) or a similar Telnet/SSH client. Use the DME administrator login name and password for access. SSH is enabled by default on the DME, and can be modified on the **System Configuration > Security** page.

**Caution:** As a reminder, the DME ships with `admin|admin` as the username and password. Be sure to change this on the DME User Configuration > Username and Password screen. This should be done BEFORE allowing internal/external access to the DME.

Once you have logged into the SSH Admin Interface, the tool will first perform a quick review of the CPU and Memory configuration. In most cases, the review takes less than 1 second and you will not see anything. However, if the DME does not have sufficient CPU (by count) or Memory resources (by percentage, anything below 80% will be reported), then the interface will provide an upfront message. The message will also identify possible false-positive cases for early versions of hardware DMEs. Messaging will appear similar to the image(s) below:

```

----- CPU UNDER-PROVISIONED (need 12 additional CPUs) -----

We have detected that your system is currently underprovisioned for CPUs. This can impact your
ability to provide streaming, transrating, and recording capabilities.

Note: There are legacy 7550 DMEs provisioned with less than 8 CPUs. These are old configurations that we
no longer ship. Please be advised that these configurations may be flagged here.

In underprovisioned DMEs, Vbrick cannot guarantee system or streaming performance.
This is particularly a concern in high use scenarios.

Consult our online help at www.vbrick.com for additional details on minimum
configurations. Or, if you have further questions, please contact Vbrick Customer Service.

Thank you

Code: CPU
-----

Press enter to continue ... █

```

```

----- Memory UNDER-PROVISIONED by more than 20% -----

We have detected that your system is currently underprovisioned for Memory. This can impact your
ability to provide streaming, transrating, and recording capabilities.

Note: There are legacy 7550 DMEs provisioned with less than 16 GB. These are old configurations that we
no longer ship. Please be advised that these configurations may be flagged here.

In underprovisioned DMEs, Vbrick cannot guarantee system or streaming performance.
This is particularly a concern in high use scenarios.

Consult our online help at www.vbrick.com for additional details on minimum
configurations. Or, if you have further questions, please contact Vbrick Customer Service.

Thank you

Code: MEMORY
-----

Press enter to continue ... █

```

If you receive one of these warnings, you will also see a notification at the top of the primary menu screen. These warnings may indicate an under provisioned DME and require attention. Please Refer to the **DME Release Notes** (for your version of DME) for CPU/Memory/Disk requirements, or the **DME CheckUp FAQ** (at: [DME Supplementary Documentation > Best Practices and FAQ Guides](#)) for additional details.

If your DME is provisioned correctly, you will not see anything.

Next, the tool will perform and display a quick log analysis. The analysis provides a cursory search of targeted system log files. This is not meant to be a complete analysis, but one that could quickly identify and highlight issues that may need addressing. Example output of this is displayed below:



```

This performs a quick once over of select logs. This is not a complete analysis, nor is it intended
to be. This only provides top-level directions to investigate. A deeper investigation may be necessary.

Quick system check for halt/core files. This check only reports findings for the last 7 days.
*** Looking halt files for: System, Avenger Interface, RTMP Server.
*** Found 1 AvengerInterface HALT logs. Investigate these.
*** Done.

Quick Rev Communication Interface log analysis (only on current .log file, not the compressed ones.)
*** File found /var/www/html/log/avenger/avengerinterface.log, 8482529 B, Last modified 2019-01-30 14:34:43.546554296 --0600 bytes
*** Overall Health Conditions: 652 Normal, 0 Caution, 3 Alert statuses found.
*** Found 4 CURL errors and retries.
*** Done.

Quick Mesh log analysis (only on current .log file, not the compressed ones.)
*** LOG: /var/www/html/log/avenger/mesh.log
*** Looking for: Missing file size warnings, CURL failures, xtmp warnings, restarts, and failed fetches.
*** Done.

Quick Access log analysis (only on current .log file, not the compressed ones.)
*** LOG: /var/www/html/log/squidlog/access.log
*** Looking for: 500/502/504 Errors, Timeouts, Swapfills, Denied, Aborted, or Long requests.
*** Found 1 500 errors. Investigate these.
*** Found 20 504 errors. Investigate these.
*** Done.

Quick Cache log analysis (only on current .log file, not the compressed ones.)
*** LOG: /var/www/html/log/squidlog/cache.log
*** Looking for: Warnings, Errors, Fatal, Unreachable Network, failed TCP, Forwarding Loop, Dead reports
*** Found 5 lines with ERROR. Investigate these.
*** Found 53 lines with failed TCP connections. Investigate these.
*** Done.

Press enter to continue ... █

```

In this example, you will notice analysis of several different logs. This analysis should be quick, however, if the log is large (and the Rev Communication Interface log can be very large) then it may take several moments. Each section, when complete, displays a **Done**.

Issues that require immediate attention or possibly investigation will be noted. If no issues, for the specific log search, are not found then there will be no message. This is an exceptions based report.

If the DME is operating correctly, then the reports may identify historical issues that may no longer be concerning. On the other hand, if your DME is not operating correctly, then this page may help you and Vbrick Support to quickly target and identify investigation areas.

This log analysis is also provided as a Menu option. So, if you need to review the results you can re-run the analysis. After the analysis is complete, pressing enter (or waiting 120 seconds) will bring up the main menu for the SSH Admin Interface.

When running the tool, always review the system characteristics displayed within a banner at the top of the page. It will look similar to this image:

```

Vbrick DME: 10.10.7.204 / pokey.
3.21.0 rhel7 01/29/2019 02:22 PM Build(95)
7530 Small Hardware, CPUs: 4 of 4 [1 S,2 C,2 Th], Memory: 3.61 of 4 GB (90%)

*****
*** The DME is NOT upgrading. You may safely reboot or shutdown. ***
*****

```

The banner includes system characters that should be spot-checked at each usage:

- IP Address
- Name (should be an FQDN)
- DME Version
- DME type (7530, 7550, 7570) and if it is VM or Hardware
- Number of CPUs with DME type requirements with configuration (Sockets, Cores, and Threads). Total CPU = Sockets \* Cores \* {1 | 2 for threads}
- Memory with DME type requirement
- Current Date, Time, Time Zone and Year
- System load averages in parentheses for past 1, 5, and 15 minutes. (Please review Linux documentation for meaning and uses of load average.)
- Uptime of Server



- Users that are currently logged into the system (SSH or Console, not VAdmin GUI). Users are prompted with Select task by number to enter in a number from the menu above it. 99 will exit the tool and terminate the SSH session.

The top banner also indicates if the DME is currently upgrading or not. It is *very* important not to reboot or apply changes if the system is currently running an upgrade – this can cause instability within the server. The banner will clearly indicate if the system is NOT being updated as well. Also keep in mind, that a DME that is currently upgrading will reboot as part of that process and drop the SSH session.

Below the banner, a primary menu list of Administration Tasks are provided by number. Each task is executed by typing in its corresponding number. For example, at the **Select Task by Number** prompt you would enter “1” to **Configure Network Settings**. The current menu structure is missing some numbers by design. This is because there are historical numbers that were kept, while Vbrick improved the grouping of functions in later versions of the Admin Interface tool.

Several tasks require a Reboot of the DME for the settings to be applied. Those are clearly identified and there will be a confirmation prompt before the Reboot. Remember, rebooting the DME will cause interruptions in streaming, recording, and all DME functions.

There are live tasks, such as watching the Rev Interface log, that will continue until terminated by the user or by closing the SSH session. All live tasks, or repeating measure displays, can be terminated by a Control-C. This will return you to the primary menu.

Depending on the version, the complete page with banner will look similar to:

```

chernabog. .vbrick.com ( . ) 3.22.0 rhel7 09/11/2019 06:25 PM Build( . )
7530 Small H/W, CPUs: 4 of 4 [1 S,2 C,2 Th], Mem: 3.61 of 4 GB (90%)
Fri Oct 4 12:01:40 EDT 2019 ( 0.32, 0.75, 0.86) up 2 weeks, 1 day, 17 hours, 45 minutes
[75] Users: override pts/0, (1 total)
-----
DME Administration Tasks Menu

[1]: Configure Network Settings                [8]: Reboot Device
  [1.1]: Set Hostname (only)                  [8.1]: Shutdown Device
  [1.2]: Clear DNS (temporarily)              [8.2]: Recent Shutdown History

[4]: Reset To Default Settings                [10]: Sysuser Login Failures
  [4.1]: Reset To Factory Default Settings    [10.1]: Reset Sysuser Login
  [4.2]: Remove License                       [10.2]: Review SSH Admin Logins

[5]: Realtime System Usage Snapshots          [11]: Reset Passwords (pwreset)
  [5.1]: CPU Realtime Usage                   [14]: Display Kernel messages
  [5.2]: Memory Realtime Usage               [14.1]: Kernel messages Err & above
  [5.3]: Disk Realtime Usage

[6]: Review Network Settings                 [18]: Generate Log Collection for Vbrick
  [6.1]: Advanced Network Health             [18.1]: Clean Up Logs/Memory Dump
  [6.2]: TCP Network Health                  [18.2]: Quick Log Analysis
  [6.3]: UDP Network Health
  [6.4]: Ping Test
  [6.5]: Traceroute Test
  [6.6]: Speed Test

[7]: System Services (Status & Restart)
  [7.1]: Streaming Services
  [7.2]: HTTPd/Caching Services              [99]: Exit
-----
>> Select task by number [1-21,99]: 

```

Commands are entered at the bottom banner of the page next to **Select task by number**.

```

-----
>> Select task by number [1-21,99]: 

```

As a reminder, do not perform any task that requires a reboot during:

- Upgrade is ongoing (identified at the top of the menu).
- DME is servicing WebCast, Recording, or heavy streaming load.

Each Administration Task menu option is described in the following table.

Group	Administration Task	Description
Network Tasks	Configure Network Settings	<p>Used to quickly configure your network settings. This includes the ability to configure for DHCP or static address and designate an IP address, Subnet Mask, and Gateway. Changing the Hostname will assign a self-signed Cert which will need to be updated within the DME VAdmin UI.</p> <p>This is the same ability that is included on the <b>System Configuration &gt; Network</b> screen on the DME. This allows you to set the FQDN, IP/Subnet/Gateway/DNS addresses, and a Search Domain for your DME before you begin using your appliance.</p> <p>Changing parameters in this task may require a system reboot. Please do not reboot during any upgrade activity (identified at the top of the screen).</p>
	Set Hostname (only)	<p>The DME Hostname identifies the appliance to various network applications including. By default, this value is DME&lt;MAC ADDRESS&gt;. This task will allow customization of the Hostname.</p> <p>Best Practice and Strong Recommendation is to use a FQDN (fully qualified domain name) provided by your IT department with associated DNS entries. Vbrick DME accepts wildcard certs, e.g., *.mydomain.com for FQDNs like dmeEurope.mydomain.com or dmeAsia.mydomain.com. Vbrick DME does not utilize SAN Certs with multiple names.</p> <p>As a reminder, changing this value will force the DME to create a new self-signed certificate. Please review <b>SSL Certificates</b> management section in Help for more details. This is the same ability that is included on <b>System Configuration &gt; Network</b> page.</p> <p>Changing parameters in this task may require a system reboot. Please do not reboot during any upgrade activity (identified at the top of the screen).</p>
	Clear DNS (temporarily)	<p>If the DNS entries are not reachable, the device may respond sluggishly. Clearing the DNS entries may alleviate the situation. This will temporarily remove the Primary and Secondary DNS settings. These session will return once the system is rebooted.</p> <p>This will also remove any Search Domain settings – <i>which will not return and must be re-entered within VAdmin.</i></p>

Group	Administration Task	Description
Reset Tasks	Reset to Default Settings	<p>This task resets most settings (except for network settings and passwords) to their default settings. The same task may be executed from the <b>System Configuration &gt; Manage Configuration</b> form in the DME.</p> <p>This task requires a system reboot. Please do not reboot during any upgrade activity (identified at the top of the screen).</p>
	Reset to Factory Default Settings	<p>This task resets ALL settings (including network and passwords) to factory defaults. Use with caution. The same task maybe be executed from the <b>System Configuration &gt; Manage Configuration</b> form in the DME.</p> <p>This task requires a system reboot. Please do not reboot during any upgrade activity (identified at the top of the screen).</p>
	Remove License	<p>This task will remove Vbrick DME licenses. This will require you to acquire and reapply a new license (or any license you may have saved) to the DME for proper operation.</p> <p>This task requires a system reboot. Please do not reboot during any upgrade activity (identified at the top of the screen).</p>

Group	Administration Task	Description
Realtime Usage Tasks	Realtime System Usage Snapshots	This task, using the Linux application <b>sar</b> , will provide usage snapshots for CPU, Memory, Paging System, SWAP, and DISK. These results are only snapshots and do not provide trending. Please review online Linux documentation for <b>sar</b> command for details on particulars of reported data.
	CPU Realtime Usage	This task, using the Linux application <b>sar</b> , provides a 20 reports at 3 second intervals (1 minute total) of CPU use within the DME. This is meant to be a more detailed view than the snapshots, but only report for the minute selected. Hitting <b>Control-C</b> will terminate the live report and return you to the main menu. Please review online Linux documentation for <b>sar</b> command for details on particulars of reported data.
	Memory Realtime Usage	This task, using the Linux application <b>sar</b> , provides a 20 reports at 3 second intervals (1 minute total) of memory use within the DME. This is meant to be a more detailed view than the snapshots, but only report for the minute selected. Hitting <b>Control-C</b> will terminate the live report and return you to the main menu. Please review online Linux documentation for <b>sar</b> command for details on particulars of reported data.
	Disk Realtime Usage	This task displays the disk partitions and usage for attached disks, the last SMART report (if the DME is hardware), and using the Linux application <b>sar</b> , provides a 20 reports at 3 second intervals (1 minute total) of disk use within the DME. This is meant to be a more detailed view than the snapshots, but only report for the minute selected. Hitting <b>Control-C</b> will terminate the live report and return you to the main menu. Please review online Linux documentation for <b>sar</b> command for details on particulars of reported data.

Group	Administration Task	Description
Network Monitoring Tasks	Review Network Settings	<p>This task will show various Linux commands and result details of your network settings.</p> <p>Please review online Linux documentation for the associated/ displayed command for details on particulars of reported data.</p> <p>Each report will display the DME Hostname and command to the screen and wait for you to <b>Press Enter to continue</b>.</p>
	Advanced Network Health	<p>This task will show various Linux commands and result details of your network settings. Utilizing <b>ifstat</b>, this task will show snapshots and a repeating display of RX/TX Pkts statistics across interfaces. This task also provides the measures using netstat.</p> <p>Please review online Linux documentation for the associated/ displayed command for details on particulars of reported data.</p> <p>Each report will display the DME Hostname and command to the screen and wait for you to <b>Press Enter to continue</b>.</p>
	TCP Network Health	<p>This task will show various Linux commands and result details of your network settings. Specifically, <b>netstat</b> is used to review active TCP connections with their state, and metrics per protocol.</p> <p>Please review online Linux documentation for the associated/ displayed command for details on particulars of reported data.</p> <p>Each report will display the DME Hostname and command to the screen and wait for you to <b>Press Enter to continue</b>.</p>
	UDP Network Health	<p>This task will show various Linux commands and result details of your network settings. Specifically, <b>netstat</b> is used to review active UDP connections with their state, and metrics per protocol.</p> <p>Please review online Linux documentation for the associated/ displayed command for details on particulars of reported data.</p> <p>Each report will display the DME Hostname and command to the screen and wait for you to <b>Press Enter to continue</b>.</p>
	Ping Test	<p>This task will allow entry of a Hostname or IP address to perform a ping test. Five tests will be performed and displayed.</p> <p>This is a useful feature to test your connection to Internet or locally based servers. Also, this is highly useful to validate your ability to reach your Rev instance (default address for test).</p>
	Traceroute Test	<p>Like the ping test, this task will allow entry of a Hostname or IP address to perform a traceroute. Each line will be displayed with a max of 30 hops.</p> <p>This is a useful feature to test and view the path to reach your Rev instance (default address for test) or other online Hostnames.</p>
	Speed Test	<p>This item will run an Internet speed test utilizing speedtest.net. In order to run this test, the DME will need Internet access. It will reach out and pull down a list of available servers, and connect to a close server to retrieve a sample dataset. Nothing will be stored on your DME.</p> <p>This is only a snapshot representing conditions during the test.</p>

Group	Administration Task	Description
Running Services Tasks	System Services (Status & Restart)	<p>This task will display system information and status and memory use of several System Services. If appropriate, user will be prompted to restart the service.</p> <p>Do not restart services during an upgrade, or while there is heavy server use. Restarting services may have an impact on streaming delivered from the DME.</p>
	Streaming Services	<p>This task will display system information and status and memory use of several DME (streaming, ingest) Services. If appropriate, user will be prompted to restart the service.</p> <p>Do not restart services during an upgrade, or while there is heavy server use. Restarting services may have an impact on streaming delivered from the DME.</p>
	HTTP/Caching Services	<p>This task will display a quick log review, system information and status and memory use of system services related to the DME . Caching Engine and Web page Serving. If appropriate, user will be prompted to restart the service. Do not restart services during an upgrade, or while there is heavy server use. Restarting services may have an impact on streaming delivered from the DME.</p>
Rebooting Tasks	Reboot Device	<p>This task will Reboots the device allowing the user to specify an option disk check on reboot.</p> <p>If the DME is shut down improperly, the disk may need to be checked to verify and recover any bad sectors. Use this option to do so. Depending on the size of your disks, this may take a great deal of time.</p> <p>Do not reboot during an upgrade, or while there is heavy server use. Rebooting will have an impact on streaming delivered from the DME.</p>
	Shutdown Device	<p>A graceful shutdown and power off that will require human intervention to power the device back on.</p> <p>Do not shutdown during an upgrade, or while there is heavy server use. Rebooting will have an impact on streaming delivered from the DME.</p>
	Recent Shutdown History	<p>This task will display a recent history of shutdown activities, as well as any sleep entries (there should not be any of these).</p>
Reset Tasks	Sysuser Login Failures	<p>Displays information related to the current login failures for the Sysuser. The current lockout is set to 3. If you are locked out, please wait 15 minutes before attempting logging again.</p>
	Reset Sysuser Login	<p>This will reset the login password to original settings and reset any log in failure that may have occurred for the Sysuser.</p>

Group	Administration Task	Description
Password Functions	Reset Passwords	This will reset the Admin password to default. It will also reset the http and https ports used by vbadm. This feature will terminate your SSH session.  Note: The default Admin password is not secure. Do not perform this action if the DME is reachable by the external Internet. Once this feature is performed, please immediately visit the VAdmin UI and change the Admin credentials.
	Display Kernel messages	This task displays the contents of the system console (kernel ring buffer). Use this test only with support from Vbrick Customer Support.
Kernel Messages Tasks	Kernel messages Err & above	This task displays the contents of the system console (kernel ring buffer) for messages at the ERR or above level. Use this test only with support from Vbrick Customer Support.
	Generate Log Collection for Vbrick	This task item will create an encrypted file, stored in the ftp root under the zippedlogs directory. This file should only be created if/when Vbrick Customer Support requests it. It will only be able to be de-rypted at Vbrick. Depending on the size of your DME logs, this may take up to an hour to create.
Logging Tasks	Clean Up Logs/Memory Dump	This task will step through a series of system and DME specific logs and prompt for removal.
	Quick Log Analysis	The analysis provided with this task is a cursory search of targeted system log files. This is not meant to be a complete analysis, but one that could quickly identify and highlight issues that may need addressing.
	Live/Check Upgrade Status	This task will display two logs: dmeupgrade.log (also available from the VAdmin page) and rpmupgrade.log.  If the system is currently performing an upgrade, then the rpmupgrade.log will be displayed live. Meaning, the log should scroll with new results and you must hit Ctrl-C to exit viewing it. This is useful to follow along with an upgrade if necessary. If the system is not performing an upgrade, then the system will just display the log normally. As a reminder, the system will reboot twice during an upgrade.
Live Log Review Tasks	Live/Review Rev Interface Logs	This task will allow direct viewing of the Rev Interface logs. This should only be executed in conjunction with Vbrick Customer Service.
VMware Specific (optional)	VMware Tools	If your DME is deployed as a VM on a VMware ESXi Host, then this task option will be displayed. It is not available and will not be displayed for Vbrick/Cisco Hardware, or Microsoft Hyper-V DMEs.  This task will return a number of VMware specific metrics including contention and memory use. Please see VMware documentation for specific details on each measure.
	Exit	This will exit the tool.

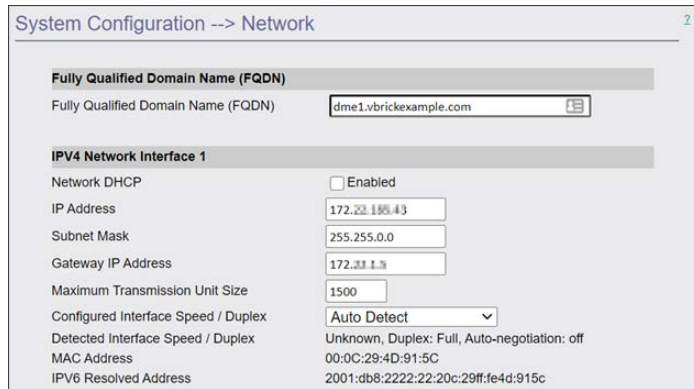




## System Configuration

### Network

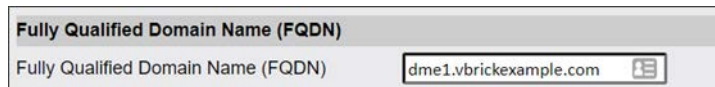
- ▼ To access the Network fields:
  1. Navigate to **System Configuration > Network**.



Fully Qualified Domain Name (FQDN)	
Fully Qualified Domain Name (FQDN)	dme1.vbrickexample.com
IPv4 Network Interface 1	
Network DHCP	<input type="checkbox"/> Enabled
IP Address	172.22.185.43
Subnet Mask	255.255.0.0
Gateway IP Address	172.22.1.1
Maximum Transmission Unit Size	1500
Configured Interface Speed / Duplex	Auto Detect
Detected Interface Speed / Duplex	Unknown, Duplex: Full, Auto-negotiation: off
MAC Address	00:0C:29:4D:91:5C
IPv6 Resolved Address	2001:db8:2222:22:20c:29ff:fe4d:915c

### Fully Qualified Domain Name (FQDN)

- ▼ To access the Fully Qualified Domain Name (FQDN) field:
  1. Navigate to **System Configuration > Network > Fully Qualified Domain Name (FQDN)** section.



Fully Qualified Domain Name (FQDN)	
Fully Qualified Domain Name (FQDN)	dme1.vbrickexample.com

Use this field to configure your **Fully Qualified Domain Name** (e.g., yourdmehostname.yourcompanydomainn.com).

**Caution:** Please make sure to enter your FQDN in all lowercase letters.

This name will be shown in the banner graphic at the top right of all the DME Admin UI configuration pages.

Currently, the FQDN defaults to DME<MAC ADDRESS>. While you can continue to use this, it is recommended that you change it. Please contact your network administrator to make sure that this FQDN is registered within your DNS servers for easy access. Also remember that this FQDN will identify the appliance to various network applications -- including DHCS and the **VBDirectory** application.

**Note:** Be aware that the FQDN field is tied to your current SSL Certificate. Changing this value will revert the DME back to a self-signed certificate. Please review the application of Certificates to align this name with the contents of the certificate.

## SSL Certificates

### IPv4 Network Interface 1

If your system has more NICs, then the DME will identify them. You will see a similar interface to what is depicted below.

▼ To access the IPV4 Network Interface field(s):

1. Navigate to **System Configuration > Network > IPV4 Network Interface** section.

IPV4 Network Interface 1	
Network DHCP	<input type="checkbox"/> Enabled
IP Address	172.17.1.5
Subnet Mask	255.255.0.0
Gateway IP Address	172.17.1.1
Maximum Transmission Unit Size	1500
Configured Interface Speed / Duplex	Auto Detect
Detected Interface Speed / Duplex	Unknown, Duplex: Full, Auto-negotiation: off
MAC Address	00:0C:29:4D:91:5C
IPV6 Resolved Address	2001:db8:2222:22:20c:29ff:fe4d:915c

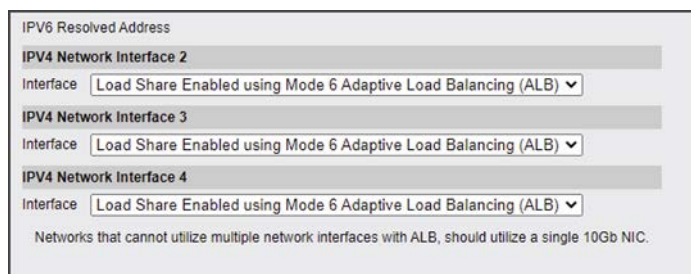
The DME supports up to four network interface (NIC) cards you can use to increase the bandwidth and throughput available to the DME. A DME with one NIC card has an overall bandwidth limitation of 1GB for all output streams. A DME with the load shared over four NIC cards provides 4GB of bandwidth. Note that when load sharing is enabled, the primary NIC card (IPV4 Network Interface 1) cannot use DHCP. **With multiple NIC cards and load sharing enabled all NICs will use the same IP address as the primary.**

Field	Description
Network DHCP	<p>Default = Enabled. Dynamic Host Configuration Protocol. If DHCP is enabled, the appliance gets its IP Address, Subnet Mask, and Gateway from the DHCP server. If the DHCP server supplies the DNS server address, these parameters will replace the user-entered DNS settings.</p> <p>The DME is setup by default to acquire an IP address via DHCP. If the DHCP server is not available at boot time, the DME DHCP IP address acquisition will fail and the appliance will retry to re-acquire the address every 10 minutes. During the 10 minute retry period, the appliance uses a default IP address of <b>172.17.1.5</b> with a subnet mask of <b>255.255.0.0</b>. If you need to change the DME to use a static IP address instead of getting one from DHCP, connect the DME to the network, connect a laptop to the network, set the laptop to be on the same subnet, and give the laptop a fixed IP address of <b>172.17.1.6</b> with subnet of <b>255.255.0.0</b>. You can then go into the DME management interface (default: <b>http://172.17.1.5:8181</b>) to login and give the appliance a static IP address.</p>
IP Address	This is either a static or a DHCP-enabled IPv4 address. Do not enter an IPv6 address.

Field	Description
Subnet Mask	Subnet mask for the DME address.
Gateway IP Address	Gateway IP Address for communicating across distinct network segments.
Maximum Transmission Unit Size	Range 500–1500 (default = 1500). The MTU is used for all network traffic from the DME and defines the largest network packet size that will be transmitted. A higher MTU brings higher bandwidth efficiency and Vbrick recommends using the default. However you may wish to reduce MTU size to meet the requirements of some networks with VPN or other security tunnels that cannot tolerate 1500 byte packets.
Configured Interface Speed / Duplex	Default = Auto Detect. Use Auto Detect or manually set the bit rate and duplex setting for network devices that do not support auto negotiation. With Auto Detect the DME will automatically adjust its duplex setting and speed to match the switch or hub to which it is attached.
Detected Interface Speed / Duplex	Read only. Displays the current connection speed and duplex setting.
MAC Address	The Media Access Control address is a unique identifier assigned to the DME for network communications.
IPv6 Resolved Address	This is an automatically set IPv6 address (if configured within the network). Note: While IPv6 address is displayed, it can only be used to manage the DME appliance – meaning, it can be used to access the DME VAdmin GUI. IPv6 address cannot be used for streaming (receiving or sending).

## IPv4 Network Interface 2–4

IPv4 Network Interface 2-4	The DME will auto detect the number of network interfaces (physical or virtual) installed. If more than one is installed, you can use the additional interfaces to increase bandwidth and throughput through load sharing.
----------------------------	--



DMEs utilize **Adaptive Load Balancing (ALB)** to spread network traffic across multiple network interfaces. ALB, or Mode 6, does not require any external switch settings.

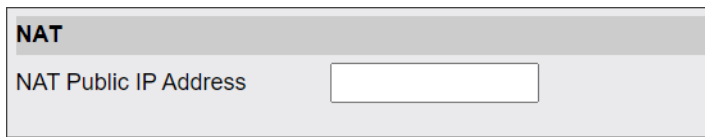
- **Disabled** – Default. This will disable the network interface and will not be used for network access. You can disable the interface if, for example, you have bandwidth constraints imposed by your network or service provider.
- **Load Share Enabled** – If Enabled, the network interface will be used to help load balance the resources used by output streams.

**Note:** Networks that cannot utilize ALB should use a single 10Gb NIC. Further, Vbrick recommends that customers that can leverage 10Gb network interfaces, use those. No bonding is necessary.

## NAT

▼ To access the NAT Public IP Address field:

1. Navigate to **System Configuration > Network > NAT** section.



The screenshot shows a configuration panel for NAT. At the top, there is a header labeled "NAT". Below the header, there is a label "NAT Public IP Address" followed by an empty text input field.

Network address translation is the method by which private IP address are held and referenced in a network translation table. It is common practice to hide an entire IP address space, usually consisting of private IP addresses, behind a single IP address.

To avoid ambiguity in the handling of packets, a one-to-many NAT alters higher level information such as TCP/UDP ports in outgoing communications and maintains a translation table so that return packets can be handled correctly. The DME allows stream access through a direct IP address, a Natted IP address, or both.

Field	Description
NAT Public IP Address	The public IP address in a network translation table.

## Domain Name Server

▼ To access the Domain Name Server fields:

1. Navigate to **System Configuration > Network > Domain Name Server** section.

Domain Name Server	
Primary Server IP Address	<input type="text" value="172.16.0.21"/>
Secondary Server IP Address	<input type="text" value="172.16.0.22"/>
Search Domain	<input type="text" value="local"/>

Field	Description
Primary Server IP Address	<p>This is the primary server used for DNS lookups. This service will resolve a Fully Qualified Domain Name (FQDN) into numerical IP addresses.</p> <p>If the user interface pages are loading slowly, make sure this is a valid IP address. If you are not using a DNS server, leave this field blank. Please consult your Network Administrator if you have questions.</p> <p><i>Note: An invalid IP address will adversely impact the operation of the user interface.</i></p> <p>Note: DNS server addresses are automatically supplied if you have Network DHCP enabled. Any changes to these addresses will be overwritten at boot up if DHCP is enabled.</p>
Secondary Server IP Address	<p>This is the secondary server used for DNS. It serves the same purpose as the primary server, but will be used if the primary server is unable to resolve the FQDN to an IP address.</p>
Search Domain	<p>These domains will be searched by your computer when performing IP lookups for less than fully qualified or non-canonical host names.</p> <p>For example, if your Search Domain is “mycompany.com” and you perform a ping on “testComputerA”, then “testComputerA.mycompany.com” will resolve (if possible) and be pinged. Ping is used here just an example – any application that needs name resolution will use this field for domain search restriction.</p> <p>Note: The Search Domain field is automatically supplied if you have Network DHCP enabled. Any changes to these addresses will be overwritten at boot up if DHCP is enabled.</p>

## Network Time Synchronization

▼ To access the Network Time Synchronization fields:

1. Navigate to **System Configuration > Network > Network Time Synchronization** section.

Network Time Synchronization	
Network Time Protocol	<input type="checkbox"/> Enabled
Primary Server IP Address	<input type="text" value="time.nist.gov"/>
Secondary Server IP Address	<input type="text" value="pool.ntp.org"/>
NTP Status	Disabled
NTP Time Offset	
NTP Source	

These fields are used to synchronize network time using the host name or IP address of a known server to provide a synchronized time for all appliances in the network.

**Note:** *Network Administrators please note.* DHCP Option 4 (TIME) and Option 42 (NTP) are requested from the DHCP server to obtain SNTP server addresses. One or both of these options must be enabled in the DHCP server for these addresses to be returned to the DME. If both are returned, the DME will use the NTP server address. If the DHCP server configuration is unknown, it is recommended that the address(es) be manually entered since the DHCP server-supplied address will always override a manually-entered address.


Field	Description
Network Time Protocol	Check to enable network time synchronization. Default = Disabled.
Primary Server IP Address	Primary host name (DME Host Name or DNS Host Name) or IP address of valid SNTP server providing time synchronization. A blank field indicates the server address will be acquired via the DHCP server only if the <b>Network DHCP</b> field above is checked.
Secondary Server IP Address	Secondary host name (DME Host Name or DNS Host Name) or IP address of valid SNTP server providing time synchronization. A blank field indicates the server address will be acquired via the DHCP server only if the <b>Network DHCP</b> field above is checked.

## Proxy

If your network utilizes HTTP(s) proxies, use this screen to specify them.

▼ To access the Proxy fields:

1. Navigate to **System Configuration > Network > Proxy** section.

Proxy	
Proxy	<input type="checkbox"/> Enabled
HTTP Proxy URL	<input type="text"/>
HTTPS Proxy URL	<input type="text"/>
Proxy Exceptions	<input type="text"/>
Username	<input type="text"/>
<input type="checkbox"/> Password	<input type="password"/> 

Field	Description
Proxy	Check to enable a proxy server. Disabled by default.
HTTP Proxy URL	<p>HTTP URL of a valid HTTP proxy server. An IP address or Fully Qualified Domain Name (FQDN) can be used. This should be in one of the following example formats:</p> <p>http://10.10.1.201:3128</p> <p>http://httpproxyname.mycompany.com:3128</p> <p>Where 10.10.1.201 is an IP address, the FQDN is an HTTP proxy server address, and 3128 is the proxy port.</p> <p>Consult your Network Administrator for your own unique network specifics.</p> <p>Note: If FQDN is used, please use all lowercase letters.</p>
HTTPS Proxy URL	<p>HTTP URL of a valid HTTPS proxy server. An IP address or Fully Qualified Domain Name (FQDN) can be used. This should be in one of the following example formats:</p> <p>http://10.10.1.201:3128</p> <p>http://httpsproxyname.mycompany.com:3128</p> <p>Where 10.10.1.201 is an IP address, and the FQDN is an HTTPS proxy server address, and 3128 is the proxy port.</p> <p>Consult your Network Administrator for your own unique network specifics.</p> <p>Note: If FQDN is used, please use all lowercase letters.</p>
Proxy Exceptions	<p>Use Exceptions when you want to bypass proxies for specific destinations. To create an Exception(s), include IP addresses or Domain Names of Exceptions, separated by commas. This should be in the following example format:</p> <p>10.10.0.1, 10.10.0.23.</p> <p>DME accepts wild cards in the format “.testing.com” (not “*.testing.com”). Separated by commas</p>
Username	Username for the proxy
Password	Password for the proxy

## Ports

▼ To access the Ports fields:

1. Navigate to **System Configuration > Ports**.

System Configuration --> Ports 2

RTSP Server Port	<input type="text" value="554"/>
MPS Server Port	<input type="text" value="1935"/>
MPS RTMPS Server Port	<input type="text" value="4443"/>
Multi-Protocol Server RTSP port	<input type="text" value="5544"/>
VAdmin Server Port	<input type="text" value="8181"/>
Secure VAdmin Server Port	<input type="text" value="8383"/>
HTTP Server Port	<input type="text" value="80"/>
HTTPS Server Port	<input type="text" value="443"/>
HTTP Streaming Tunneling Port	<input type="text" value="8080"/>
HTTP Caching ICP Port (starting port of 8 consecutive ports)	<input type="text" value="3130"/>
FTP Data Port	<input type="text" value="20"/>
FTP Command Port	<input type="text" value="21"/>
SFTP Port	<input type="text" value="8022"/>

Field	Description
RTSP Server Port	Default = 554. RTSP port for VOD streams from RTP server. Cannot be changed. Used to receive an RTP Auto Unicast stream as input and to serve RTSP RTP clients for output
MPS Server Port	Default = 1935. MPS Server Port for RTMP streams from MPS server. Allows MPS streams as input. For example a Vbrick H.264 encoder can be an MPS input stream. Note: This was formerly labeled the RTMP Server Port.
MPS RTMPS Server Port	Default = 4443. MPS Server Port for RTMPS streams (secure RTMP) to be pushed into DME/MPS server.
Multi-Protocol Server RTSP port	Default = 5544. The port number used by the Multi-Protocol Server to listen for announcements.
VAdmin Server Port	Default = 8181. Specifies the listener port for HTTP management connections as follows: <b>http://IPaddress:port</b> where <b>IPaddress</b> = DME IP address or hostname, and port. The port number can be moved to another port if required as long as it does not conflict with another existing port in the system.
Secure VAdmin Server Port	Default = 8383. Specifies the listener port for management and HTTPS connections. Used for HTTPS connections when enabled on the <a href="#">Security</a> configuration page. Can be moved to another port number if required.



Field	Description
HTTP Server Port	Default = 80. Sets the port used for progressive download (HTTP), HLS streams, and Caching. This port can be 80 or a safe port in the range 1025–65535. An error message will indicate an invalid port.
HTTPS Server Port	Default=443 Secure HTTP port
HTTP Streaming Tunneling Port	Default = 8080. Sets the port for HTTP tunneling via RTSP. The default is 8080 but if you are streaming HTTP directly from a DME via the Internet, it is a common practice to change this to 80 and to set any other service using port 80 to a different port. <i>If you change this value you will need to make a comparable change on the player and on the DME configuration (i.e. HTTP Tunnel Port) in VEMS.</i>
HTTP Caching ICP Port (starting port of 8 consecutive ports)	This defines the starting port of a range of 8 consecutive UDP ports used for ICP. This value sets the ports used to discover multiple web caches on the local (source) DME and on remote DMEs. The default UDP port is 3130, and it is <i>highly recommended</i> that this value is not changed. Changing this port will impact DME shared caching (MESH). If you must change this range of ports, then it must be changed (to the same value) on ALL DMEs within your deployment.
FTP Data Port	Default = 20. Defined for FTP data port; works for FTPS as well.
FTP Command Port	Default = 21. Defined for FTP command port; works for FTPS as well. The FTP client that connects to the DME must use ACTIVE mode to utilize this port.
SFTP Port	This is the port that SFTP will utilize.

**Note:** For correct operation of the DME Mesh and shared caches, do not change the HTTP and HTTPS default ports. Additionally, changing the HTTP Caching ICP Port must be changed on ALL DMEs and is therefore not recommended.

## Security

▼ To access the Security fields:

1. Navigate to **System Configuration > Security**.

Field	Description
External VBAAdmin	VBAAdmin cannot be completely disabled: Select HTTP or HTTPS. Default = HTTP. <ul style="list-style-type: none"> <li>• HTTP – VBAAdmin is enabled via HTTP.</li> <li>• HTTPS Only – VBAAdmin is encrypted and secured using HTTPS.</li> </ul>
VBAAdmin Browser Timeout (minutes)	This defines the browser timeout in minutes.
SSH Shell	Default = Enabled. SSH Secure Shell access may be used by Vbrick Support Services. Do not use except as directed.
External FTP Server	Default = Disabled. Disabled will prevent FTP sessions to the DME appliance. Note that this feature must be enabled to upgrade the appliance firmware.

Field	Description
External FTP Server Mode	<p>The FTP server can run in one of two modes: Standard FTP (which is the default), FTPS TLS Forced.</p> <p>The FTPS TLS Forced is secure and utilizes TLS 1.1 or TLS 1.2. This mode is only Explicit FTPS.</p> <p>When changing the DME between Standard and FTPS TLS Forced, the DME will default the data channel to port 20, and the command channel to port 21. If you wish a different port, please modify it on the Ports page AFTER selecting the appropriate FTP mode.</p> <p><b>Note:</b> The DME does not support the alternative SFTP.</p> <p>Any changes to this setting will not reboot the server but will restart the FTP service—ending any active FTP transfers in progress.</p>
SNMP Server	Select to enable the SNMP server. Required to enable SNMP traps and alarms.
SNMP Server Mode	Specify what version of SNMP to enable.
RTMP Receiver and Server	<p>If Enabled, the RTMP Server/Multi Protocol Server will receive and serve streams to viewers/players.</p> <p>Default = Enabled.</p>
RTSP Receiver and Server	<p>If Enabled, the legacy RTSP Server will receive and serve streams to viewers/players.</p> <p>Default = Enabled.</p>
RTMP Server Authentication	<p>Default = Enabled. If enabled, then RTMP streams pushed to the DME must be authenticated using credentials on the <b>Stream Input Authentication</b> screen. If disabled, then any RTMP stream can be pushed to the DME without authentication being required.</p> <p>Note: As always, it is recommended that you modify the default passwords.</p>
Serve HTTP/HLS Videos	This setting controls how HTTP content, e.g. HLS, will be delivered. The default setting is to allow either HTTP or HTTPS delivery. It should be noted that VEMS will utilize HTTP, On Premises Rev (depending on configuration) may use either HTTP or HTTPS, and Cloud Rev requires HTTPS for the player. Changing from this default is not recommended.
TLS Support	Use this dropdown to select the level of TLS support you want the DME to use.
Cache Manager Utility	Default = Disabled. For debugging only.
Kernal Dump Service	Default = Enabled. This allows the creation of a core file in the case of service abnormal termination. This should be enabled if you are experiencing difficulties with your DME or if Vbrick Support requests it.

---

## New Password Requirements

The following settings allow Administrators to control the strength of entered passwords. These only cover passwords defined within the DME and not external passwords. These are applied when a new password is entered.

Field	Description
Force Numeric	This forces new passwords to include numeric characters. Default = Enabled.
Force Special Characters	This forces new passwords to include special characters. Character sets for each password are defined within the help for each affected DME page. Default = Enabled.
Force Upper and Lower Case	This forces new passwords to include both upper and lowercase characters. Default = Enabled.
Minimum Length	This defines the minimum length of a new password. Default = 7.
Password Expire	This controls if the password expires. Default = Enabled.
Expiration Period (Days, 5-365)	If passwords are set to expire, this field defines the number of days till expiry. Default = 35
Prohibit Reused Passwords	This controls if the DME will enforce NEW, non-used passwords. Note: Previous passwords are not stored on the DME. The DME stores strongly encrypted, one-way HASH of previous passwords for comparison. Default = Enabled.
Passwords to Remember	If the DME is prohibiting reused passwords, this controls the depth (number to "remember") passwords. Default = 10. Values = 1-10.

## SNMP

Vbrick supports SNMP v2 and SNMP v3 traps. SNMP traps are a subset of the SNMP management component of the appliance. Use of any element of the SNMP management system requires use of an SNMP browser or SNMP manager application (not supplied).

Traps are SNMP base messages used by SNMP elements to report changes in status or alarm conditions to remote SNMP management entities. Traps are generally used to alert network administrators of potential equipment problems or other noteworthy events. The trap event will be sent every time the monitored event occurs and then not again unless the condition goes away and returns or if SNMP is restarted or reconfigured on the DME.

Currently defined traps are sent with the root Vbrick OID of 1.3.6.1.4.1.4289 with text indicating which trap it is.

Vbrick supports read-only access to the following standard MIBs (DMEs currently support MIB-I, but not MIB-II/MIB-2 standards):

- HOST-RESOURCES-MIB (.1.3.6.1.2.1.25.)
- UCD-SNMP-MIB (.1.3.6.1.4.1.2021.)
- IP-MIB (.1.3.6.1.2.1.4.)
- IF-MIB (.1.3.6.1.2.1.2.)

Note: The VAdmin UI utilizes the Linux free command to determine memory usage (free and swap). This is a different calculation of memory than is reported by the UCD-SNMP-MIB (which does not include slab allocation in cache). For more accurate free physical memory, you may wish to consider tracking the sum (memAvailReal.0 + memBuffer.0 + memCached.0) – also still lower than what is reported by free. This also affects HOST-RESOURCES-MIB. Please be aware of this and review if you are using SNMP to track memory via either of these MIBs.

▼ To access the SNMP fields:

1. Navigate to **System Configuration > SNMP**.

Field	Value
SNMP Server Running	True
Read Community	public
SNMPv3 Username	snmpkmayo
SNMPv3 Authentication Password	
SNMPv3 Authentication Protocol	MD5
SNMPv3 Privacy Password	
SNMPv3 Privacy Protocol	DES
SNMPv3 Security Level	Authentication Only
Trap Mode	Traps Disabled
Trap Destination	
Disk Space Threshold (1-99%)	75
CPU Threshold (1-99%)	75

Field	Description
SNMP Server Running	Default = False. Enabled on the Security page. Must be enabled to allow SNMP reads and traps.
Read Community	The community string used for SNMP v2 and v1 read access. May include any combination of alphanumeric characters and only the underscore special character.
SNMPv3 Username	Default = "SNMPadmin". May include any combination of alphanumeric characters and only the underscore special character.
SNMPv3 Authentication Password	Enter password. Must be at least 8 characters. May include any combination of alphanumeric characters but only the following special characters: ~ ! # \$ ^ * + & [ ] { }   < > _ <b>Note:</b> For security, you are not able to see the currently set password. The viewing icon only toggles the display for entered passwords. If you forget your password(s), you will need to reset your password(s).

Field	Description
SNMPv3 Authentication Protocol	Select protocol: MD5 or SHA. Select the authentication protocol that matches the set up in the SNMP management tool you are using. If both are present in the management tool, SHA is regarded as the more secure choice.
SNMPv3 Privacy Password	Required. Must be at least 8 characters. May include any combination of alphanumeric characters but only the following special characters: ~ ! # \$ ^ * + & [ ] { }   < > _ <b>Note:</b> For security, you are not able to see the currently set password. The viewing icon only toggles the display for entered passwords. If you forget your password(s), you will need to reset your password(s).
SNMPv3 Privacy Protocol	Select protocol: DES or AES. AES is more secure and should be selected here unless your management tool does not support this protocol.
SNMPv3 Security Level	<ul style="list-style-type: none"> <li>• Authentication Only (Default)</li> <li>• None (No Authentication or Privacy)</li> <li>• Authentication and Privacy</li> </ul>
Trap Mode	Default = Traps Disabled. Used to enable v2 or v3 SNMP Traps.
Trap Destination	The IP Address of a SNMP management station where traps are sent. The SNMP management application should be active on this station in order to receive any traps.
Disk Space Threshold	A percentage between 1 and 99 of available allotted disk space. The trap is triggered when the amount of disk used for content (Home page > Disk Usage Content field) reaches or exceeds this percentage.
CPU Threshold	A percentage between 1 and 99 of allotted CPU processing power. The trap is triggered if the “Total CPU Load” (Home page > Total CPU Load field) reaches or exceeds this percentage.

## General

▼ To access the General fields:

1. Navigate to **System Configuration > General**.

The screenshot shows the 'System Configuration --> General' window. It is divided into three main sections: System Maintenance, Login, and System Time. The System Maintenance section includes fields for System Description, System Model Number, System Serial Number, System Licenses, System Name, System Location, and System Contact. The Login section includes System Login Message and System Login Banner. The System Time section includes Date/Time, Time Zone, and Daylight Saving Time. At the bottom, there are buttons for Apply, Revert, and Default, and a System Reset section with a Reset button.

## System Maintenance

▼ To access the System Maintenance fields:

1. Navigate to **System Configuration > General > System Maintenance**.

This screenshot shows a close-up of the System Maintenance section. It lists the following fields and their values: System Description (VBrick Systems Inc, Distributed Media Engine (DME)), System Model Number (7500-0252-0300), System Serial Number (Software Only, 1111111111, 2222222222, 3333333333), System Licenses (DME HIGH, VC Gateway, Transrate, VB Mix), System Name (DME System Name), System Location (DME System Location), and System Contact (DME System Contact).

The **Name**, **Location**, and **Contact** fields are used to identify the appliance. They *are not* changed when you click **Default**. (They *are* changed when you reset to the defaults on the Manage Configuration page.)

Field	Description
System Description	Read-only. Company name and product name.
System Model Number	7530, 7550, or 7570.
System Serial Number	Unique serial number assigned to unit. See label on DME.
System Licenses	Displays whatever licenses are currently installed.
System Name	User-defined. System name, for example Biology Dept.
System Location	User-defined. System location, for example West Campus.
System Contact	User-defined. Contact person, for example Jane Doe.

## Login

▼ To access the Login fields:

1. Navigate to **System Configuration > General > Login**.

Field	Description
System Login Message	This customized message (max = 8k chars) will be displayed on the <a href="#">Login to the DME</a> page.
System Login Banner(200x45px)	If default is unchecked a custom Logo can be uploaded.

## System Time

▼ To access the System Time fields:

1. Navigate to **System Configuration > General > System Time**.

Field	Description
Date Time	Sets system date and time in <b>mm/dd/yyyy hh:mm</b> format. The appliance will reset when you click <b>Set Time</b> .
Time Zone	Select from list: (GMT-12) Eniwetok – (GMT +12) Auckland.
Daylight Saving Time	U.S. only. Check this box and the appliance will automatically adjust for Daylight Savings Time. This is particularly useful when monitoring the System Logs.

## System Reset

▼ To access the Reset button:

Navigate to **System Configuration > General > System Reset**.

Button	Description
Reset	Resets (i.e. reboots) the appliance. A reset does not change, save, or reset any configuration parameters.

[The Apply, Revert, and Default Buttons](#)

[Reset the System](#)



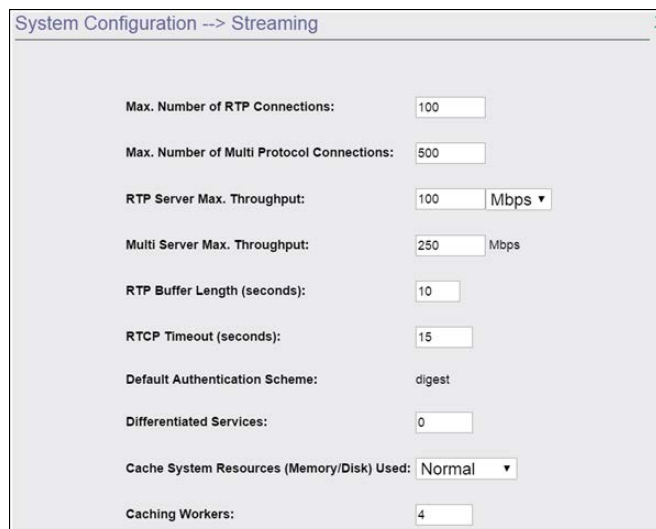
## Streaming

▼ To access the Streaming fields:

1. Navigate to **System Configuration > Streaming**.

This page is used to set various configuration constraints. Be aware that it is possible to overload the DME. That is, you can configure the maximum number of RTP connections (and the maximum throughput) in such a way that performance will be seriously degraded.

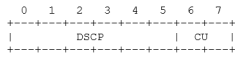
If this happens, **all** clients will be affected and some connections may actually be rejected. Guidelines for choosing the number of connections depend on the model number (shown on the System Configuration > [General](#) page) of your DME. For best results, use the recommendations shown below.



Field	Value
Max. Number of RTP Connections:	100
Max. Number of Multi Protocol Connections:	500
RTP Server Max. Throughput:	100 Mbps
Multi Server Max. Throughput:	250 Mbps
RTP Buffer Length (seconds):	10
RTCP Timeout (seconds):	15
Default Authentication Scheme:	digest
Differentiated Services:	0
Cache System Resources (Memory/Disk) Used:	Normal
Caching Workers:	4

Field	Description
Max. Number of RTP Connections	<p>Range: 0–1000. Select this value based on number of expected connections. When selecting the number of connections, the total expected bandwidth of the streams should not exceed recommendations. The recommendations shown here for each model are for total throughput (input and output) in megabits per second:</p> <ul style="list-style-type: none"> <li>• <b>DME Model BPS 7530</b> - Do not exceed 100 Mbps. <ul style="list-style-type: none"> <li>- Hardware Part # 8000-0222-0x00</li> <li>- Software Part # 7500-0250-0x00</li> </ul> </li> <li>• <b>DME Model XPS 7550</b> - Do not exceed 500 Mbps. <ul style="list-style-type: none"> <li>- Hardware Part # 8000-0223-0x00</li> <li>- Software Part # 7500-0251-0x00</li> </ul> </li> <li>• <b>DME Model HPS 7570</b> - Do not exceed 3000 Mbps. <ul style="list-style-type: none"> <li>- Hardware Part # 8000-0224-0x00</li> <li>- Software Part # 750-0252-0x00</li> </ul> </li> </ul> <p><b>Defaults (7530/7550/7570): 100/100/100</b></p>

Field	Description
Max. Number of Multi Protocol Connections	<p>The maximum number of allowed connections. This will vary by DME model.</p> <ul style="list-style-type: none"> <li>• <b>DME Model 7530</b> - May not exceed 100.</li> <li>• <b>DME Model 7550</b> - May not exceed 1000.</li> <li>• <b>DME Model 7570</b> - May not exceed 2200.</li> </ul> <p><b>Defaults (7530/7550/7570): 100/1000/2200</b></p>
RTP Server Max. Throughput	<p>Set maximum allowed throughput in mbit/sec or kbits/sec. See recommendations above.</p> <p><b>Defaults (7530/7550/7570): 100/100/100</b></p>
Multi Server Max. Throughput	<p>Maximum amount of bandwidth used by streaming clients within the Multi Protocol Server. This includes RTP/RTSP/RTMP/RTMFP/Vbrick Multicast. This number is capped by the appropriate DME license, but can be set lower to limit the actual max bandwidth used.</p> <p><b>Defaults (7530/7550/7570): 100Mb/500Mb/3072Mb</b></p>
RTP Buffer Length (seconds)	<p>The maximum time a packet will sit in a streaming buffer before being delivered to the client. This is adjusted for poor quality networks between client and server. Lower numbers may reduce playback latency. The higher number allows it to behave better with poor network connections.</p> <p><b>Defaults (7530/7550/7570): 10/10/10</b></p>
RTCP Timeout (seconds)	<p>The maximum time the DME will wait for a RTP server will wait before timing out the connection. Setting a value of 0 means never timeout. This is useful if the source is not sending any RTCP reports. Also, when using Pause in a RTP player, this number is what the server will wait as a maximum before terminating the paused connections. Setting it to 360 will allow a maximum pause of 5 minutes. It also means it will wait up to 5 minutes to drop connections that do not terminate gracefully, including live content, where the stream is interrupted.</p> <p><b>Defaults (7530/7550/7570): 15/15/15.</b></p>
Default Authentication Scheme	<ul style="list-style-type: none"> <li>• Basic – the DME server sends authentication credentials over the network in Base64 encoded text.</li> <li>• Digest – the DME server sends encrypted authentication using MD5 credentials over the network.</li> </ul> <p><b>Defaults (7530/7550/7570): digest/digest/digest</b></p>

Field	Description
Differentiated Services	<p>Differentiated Services (DiffServ) is a course-grained mechanism and setting used to help manage a network's quality-of-service (QoS). The setting is injected into the IP header to allow network prioritization for the data packet for UDP and TCP. The setting is an encoded 1 byte value, and is entered as decimal.</p> <p>Please consult the tables below for actual decimal settings in red (these are the correct translation to include to two low-order bits.) You should also consult your network administrator before using this feature.</p> <p>DiffServ takes up the first 6 bites of the 1-byte value you enter. The DS field structure is presented below:</p> <div style="text-align: center;">  <pre> 0 1 2 3 4 5 6 7 +-----+-----+   DSCP   CU   +-----+-----+ </pre> <p>DSCP: differentiated services codepoint CU: currently unused</p> </div> <p>Therefore, any value you intend to use will fill the first 6 bits, with the 7th and 8th unused. The two tables below this one outline the correct entries for a number of common DiffServ settings.</p> <p><b>Note:</b> Additional information can be found in <b>RFC2474</b> <a href="https://www.ietf.org/rfc/rfc2474.txt">https://www.ietf.org/rfc/rfc2474.txt</a>, and <b>RFC2475</b> <a href="https://tools.ietf.org/html/rfc2475">https://tools.ietf.org/html/rfc2475</a>.</p> <p><b>Note:</b> Use of Explicit Congestion Notification (ECN) (in the 7th and 8th bit) is not covered here. Please see <b>RFC3168</b> <a href="https://tools.ietf.org/html/rfc3168">https://tools.ietf.org/html/rfc3168</a>. This value is in decimal.</p> <p><b>Note:</b> All output stream types from MPS use this setting except HLS and HDS served locally from the DME. Starting with DME v3.22, this setting also effects HLS pushed to Akamai.</p> <p><b>IMPORTANT:</b> This value, when changed, will automatically restart the streaming server impacting existing streams. This assures that all future configured streams will adopt the setting. However, current streams that are running will not use the setting unless each individual stream is manually stopped and started. In other words, this setting is not automatically propagated through all existing outgoing lines and their headers regardless of the server restart.</p> <p>Therefore, when resetting this value, all outgoing lines must be disabled and then re-enabled for this value to be used within each of the streams' headers. It is not sufficient to disable or reboot the server.</p> <p><b>Defaults (7530/7550/7570): 0/0/0</b></p>

Field	Description
Cache System Settings Used	<p>Be aware that this setting has a direct impact on memory and disk usage. If not configured properly, system memory will not be available for other functions. Do not change the default (Normal) unless you will be using the DME for a different function as explained below.</p> <ul style="list-style-type: none"> <li>• Low – the DME will not be used for caching.</li> <li>• Normal – the DME will be used primarily as a reflector and secondarily as a caching engine.</li> <li>• High – the DME will be primarily used as a caching engine and secondarily as a reflector.</li> <li>• Dedicated – the DME will be used exclusively for caching.</li> </ul> <p>See <a href="#">Caching</a> for additional details.</p> <p><b>Defaults (7530/7550/7570): Normal/Normal/Normal</b></p>
Caching Workers	<p>Allows the number of Caching Workers to be adjusted. If you are primarily doing DME to DME caching, then set this number high. If you are primarily doing Akamai pulls into the DME, set this number to 1. <b>Note:</b> The number of maximum available workers is the number of DME cores but it is capped at 8.</p> <p><b>Defaults (7530/7550/7570): 4/4/8</b></p>

## Differentiated Services Values

The following tables provide the 8-bit encoded values to be used within the DME. Please select the correct value from the **VAdmin DiffServe Value** column from the appropriate table. Do not effect changes to DiffServ without engaging your Network Administration Group to avoid conflicts and align with their policies and procedures.

### Class Selector Values

DSCP	Binary	VAdmin DiffServ Value	Typical Application	Examples
CS0 (Default)	000000 00	0		
CS1	001000 00	32	Scavenger	YouTube, Gaming, P2P
CS2	010000 00	64	OAM	SNMP, SSH, Syslog
CS3	011000 00	96	Signaling	SCCP, SIP, H.323
CS4	100000 00	128	Realtime	TelePresence
CS5	101000 00	160	Broadcast video	Cisco IPVS
CS6	110000 00	192	Network control	EIGRP, OSPF, HSRP, IKE
CS7	111000 00	224		

List of the commonly used DSCP values described in [RFC 2475](#). Please consult your Network Administrator before modifying any DiffServ values.

Commonly Used DSCP Values

Binary	VBAAdmin DiffServ Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101110 00	184	Expedited forwarding (EF)	N/A	101 Critical
000000 00	0	Best effort	N/A	000 Routine
001010 00	40	AF11	Low	001 Priority
001 100 00	48	AF12	Medium	001 Priority
001110 00	120	AF13	High	001 Priority
010010 00	72	AF21	Low	010 Immediate
010100 00	80	AF22	Medium	010 Immediate
010110 00	88	AF23	High	010 Immediate
011010 00	104	AF31	Low	011 Flash
011100 00	112	AF32	Medium	011 Flash
011110 00	120	AF33	High	011 Flash
100010 00	136	AF41	Low	100 Flash Override
100100 00	144	AF42	Medium	100 Flash Override
100110 00	152	AF43	High	100 Flash Override

Configuration of this feature is within Rev. See: [Enable and Configure a DME for Automatic Multicast and Reflection.](#)

## Caching

The goal of caching within the DME and a DME network is to allow a viewer to locate and playback content hosted by any (with reachability) DMEs. Set up will depend on the deployment used:

- Standalone DMEs or Legacy (VEMS)
- DMEs with Rev

The caching system on the DME, which is independent from the content directories, is stored either in Memory or on Disk. These caches are maintained, and content is aged out by the caching system.

Depending upon your specific needs for this particular DME, you may wish to increase or decrease the caching capabilities. Specifically, you can control how much memory and disk the caching system can utilize. These settings control only HTTP based protocol caching (which includes progressive mp4, HLS and HDS delivery). Each of these settings will also have an impact on the amount of available storage for VOD content. Further, extensive use of the CPU will have a trade-off effect with other CPU intensive features (like transrating). As such, High or Dedicated settings should only be used on DMEs that will be used as

---

reflectors or purely caching. DMEs that are used as prepositioned content servers should be set with Normal to Low caching settings.

This setting is unique to each of your DMEs within your deployment. As an example, it may be, based on your deployment architecture, that a few edge DMEs will be set as High Caching to facilitate remote reflection, while larger content DMEs may be set for Normal or Low. Please consider this setting during your deployment architecture design.

The table below defines the memory and disk allotments (what is available to be used as a percentage of system resources) by usage level (Dedicated, High, Normal, or Low – as selected and defined by the Cache System Resources (Memory/Disk) Used: setting within the DME.) These allotments are consistently applied across all DME versions, e.g., Large DMEs set to High will use the same percentage of memory (30%) as a Small DME set to High. These percentages are based off the memory within the system, so any over- or under-provisioning within VMs will be reflected in the allotment. The table also defines a minimum setting (or floor) for each of the values.

These allotments are based on a 75%/25% rule of use that prioritizes in-memory cache use over on-disk cache use. In other words, the DME reserves up to 75% of allowable memory (based on the chart below) for in memory objects, while the remaining 25% is used for indexes of on-disk caching. By limiting our disk cache index use to 25%, we have also reduced the addressable on-disk cache. This rule has had an reduction impact on the size of disk cache, as compared to older DME versions, but still represent a sizable use of storage depending on usage level.

These settings can be configured on the **System Configuration** > [Streaming](#) page in the **Cache System Resources Used** drop-down.

		Dedicated	High	Normal	Low
<b>Memory</b>	Allowable Use	50%	30%	12.5%	6.25%
	Minimum Setting	512 MB	256 MB	200 MB	100 MB
<b>Disk</b>	Allowable Use	14.5%	8.6%	3.5%	1.7%
	Minimum Setting	8192 MB	4096 MB	2046 MB	1024 MB

**Tip:** Your system Cache (both memory and disk) can be cleared by the **Clear Cache** button on **Maintenance** > **System Maintenance** page.

Please see the [System Maintenance](#) topic for details.

[Standalone DME or Legacy \(DME with VEMS\) Caching Configuration](#)

[Mesh with Rev Caching Configuration](#)

[Manage Configuration](#)

## ***Standalone DME or Legacy (DME with VEMS) Caching Configuration***

Creating a caching solution within a Legacy (VEMS) or Standalone DME deployment is discussed in this topic.

Although, a major focus of the feature is to allow access to HLS or HDS content created in another DME, the mechanism is generally the same for all HTTP accessed content. This is accomplished by creating a configuration of parents and alternate sources (i.e. siblings) on each DME. Then a client is directed to a DME located in the same zone by providing the URL of the local DME. It is not uncommon to have different sources for different types of HTTP content. Given that the most common and efficient way to configure the caching network is to configure parent relationships, the configuration allows different parent configuration for each major type of HTTP content.

The goal of configuring the caches on each DME in a network is to allow a client in any subnet (i.e. a "zone" in the VEMS context) to access content hosted by an HTTP server elsewhere in the network. Although, a major focus of the feature is to allow access to HLS or HDS content created in another DME, the mechanism is generally the same for all HTTP accessed content. This is accomplished by creating a configuration of parents and alternate sources (i.e. siblings) on each DME. Then a client is directed to a DME located in the same zone by providing the URL of the local DME. It is not uncommon to have different sources for different types of HTTP content. Given that the most common and efficient way to configure the caching network is to configure parent relationships, the configuration allows different parent configuration for each major type of HTTP content.

As shown on the **System Configuration > Caching** page, each DME configuration consists of parents for each of a number of types of HTTP content, one **Default Parent**, and multiple **Alternate Sources**. Each of these IP addresses must be unique.

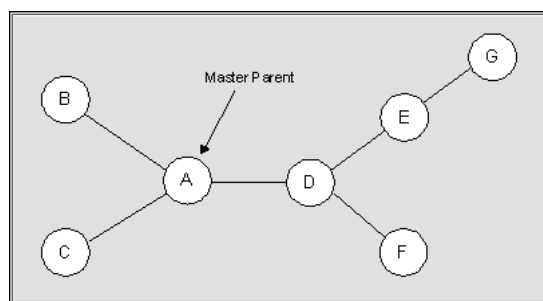
When the DME receives a request for HTTP content it will first determine if the content is cached locally. It will then try to find the content by completing the following steps:

1. Determines if the content is produced locally.
2. Checks with the **Alternate Sources** that have been defined.
3. Attempts to obtain the content from a **Content Specific Parent**.

**Content Specific Parents** are checked before the **Default Parent**. Each parent may follow the same process trying to locate the content. Once the content is found, it is delivered to the requesting client through the discovery path. Each DME in the path will also cache the content to allow provide more efficient delivery to other requestors.

For many simple caching matrices, configuring the **Default Parent** is all that is required. Note that HLS/HDS/Smooth Streaming/DASH playlists are never cached since in the case of a live events, the playlists are constantly updated.

The image below shows a sample network diagram of multiple DMEs with one DME in each zone. In general, the goal is (1) to allow any DME to be a source of appropriate HTTP content, and (2) to allow clients in any subnet to access appropriate HTTP created in any other DME.



Multiple DME Configuration (Sample Network Diagram)

▼ To access the Caching fields:

1. Navigate to **System Configuration > Caching**.

When configuring a DME, the first step is to designate one **Content Specific Parent** for each content type. Also identify a **Default Parent** for the DME for content not explicitly handled by one of the other parents.

In the following example for simplicity, only a **Default Parent** for each DME is defined- no **Content Specific Parents**. When **Content Specific Parents** are present, separate caching matrices exist for each content type.

In order to minimize the amount of required information, the master parent (DME A) should be at the "center" of the caching mesh, although you can actually designate any DME as the master. Each DME should designate as its parent the DME most efficiently on the path to the master parent. The master parent should designate all other DMEs that may be generating content as **Alternate Sources** (i.e. siblings).

It is recommended (but not required) that any DMEs which can not be efficiently accessed on the master parent path, be entered as **Alternate Sources**.

The table below shows the recommended configuration for the image displayed above.

**Table 1.** Recommended Sample Configuration

DME	Default Parent	Alternate Source
G	E	None
F	D	G
D	A	E, F, G
A	None	B, C, D, E, F, G

In another example, suppose a client co-located with DME E in the image above wants to access an HLS stream initiated on DME G. Since this configuration defines DME A as the Master Parent, the ultimate path for content delivery would be as follows (with asterisks showing where caching occurs):

DME G\* > DME E > DME D > DME A\* > DME D\* > DME E\*

Note that if DME G was designated as an alternate source for DME E, the path would simply be: DME G\* > DME E\*. Although this example designates a DME as master parent (as often happens if the content to be cached is HLS or HDS where content is not sourced from a DME, e.g. Smooth Streaming), the master parent will likely be an HTTP server.

In the Vbrick ecosystem, a Vbrick H.264 encoder can generate a Smooth Stream to a Microsoft IIS server that can then deliver it to multiple Silverlight clients or to DME caching engines. Since IIS servers do not utilize the same caching protocols as the DME, an IIS server cannot be used as an alternate source.



Field	Description
Display	Select number of sources (20, 50, or 200) and the number of available entries in the Alternate Sources table will be adjusted to match.
Mystro Server Default Parent	A DME has one <i>Default</i> parent. When the DME receives a request for content, this is the final place it looks after failing to discover the content locally, at an alternate source, or being directed to a content specific parent. The syntax is: <b>&lt;ip_address&gt;:port</b> Note: The specified port number overrides the displayed port number. See <a href="#">Ports</a> for more information.
Force HTTPS:	Secure SSL communication can be enforced between a DME and any of its parents (selected individually). A DME can also communicate securely with alternate sources (siblings) on an all or nothing basis.
Content Specific Parent	Certain types of content that can be cached and streamed may not be created directly by a DME. This can be because a DME cannot transcode into that type (Smooth Streaming or DASH), or simply because the administrator decided not to do that with a specific device. In this case, an administrator can name an "alternate parent" for a specific type of content. The DME will look to the alternate parent when a specific type of content is requested, is not in cache, and cannot be located on an alternate source. In all cases the syntax is: <b>&lt;ip_address&gt;:port</b> Note: The specified port number overrides the displayed port number. See <a href="#">Ports</a> for more information
Apple HLS	HTTP Adaptive Streaming used for display of live or stored streams on iPhone/iPad.
Smooth Streaming	Microsoft-specific HTTP adaptive streaming typically used by the Microsoft Silverlight player or Windows mobile video display.

Field	Description
Adobe HDS	HTTP Dynamic Streaming used by players for HTTP adaptive display of video.
MPEG DASH	An emerging video distribution standard for display of video via HTTP adaptive streaming. Players are not yet widely available.
WM Session Files	WM Session Files (asx or nsc) are often used to display WM video and are required for display of Windows Media multicast. They are generated by a Vbrick Appliance (not DME)
MPEG Multicast Session Files	MPEG multicast Session Files (.sdp) are required for display of RTP multicast video. They are generated by Vbrick VB6000, VB7000, and VB9000 appliances.
Alternate Sources (siblings)	If the DME does not already contain the requested content it will look sequentially through the alternate sources before it checks the parents. The syntax is: <b>&lt;ip_address&gt;:port</b> Note: The specified port numbers override the displayed port numbers. See <a href="#">Ports</a> for more information.

## HLS CDN Reflection

Beginning with DME v.3.12, the DME is able to retrieve, cache and distribute (to viewers) HLS streams from external sources. This allows customers to utilize their DMEs for caching and distribution of HLS streams from CDNs. This feature currently only supports retrieval, caching, and distribution of Akamai HLS streams. Further, this feature is only for VEMS customers, as Rev utilizes these settings for distribution of live Conference.

As an example, in this scenario, the DME receives an HLS request (m3u8/manifest or video chunk) from a viewer/player. The DME identifies the stream as an Akamai stream. The DME will pull the requested content from Akamai, cache it, and deliver the content to the player. Other subsequent requests are pulled from the local DME cache, Mesh, directly from Akamai (in this order) and delivered to those players. Manifest files are only minimally locally cached (< 2 seconds), while video chunks are kept longer. This feature allows customers to better leverage their Akamai investment jointly with their on premise DME investment

The configuration of this feature requires knowledge of the Akamai publishing **hostnames**, and the ability to identify a unique string, **identificationString**, within the URL. While a simple string will work, the **identificationString** will also take a Regular Expression.

For example, your Akamai playback URL may be:

Example Akamai HLS Playback **URL**: **http://myCompany.akamaihd.net/i/streamName@streamID/master.m3u8**

The URL provided to the DME (from a player) would be:

Example DME HLS Playback URL: **http://dmeIP/i/streamName@streamID/master.m3u8**

Note the parallelism/similarity highlighted in the two URLs – this is necessary for the feature to work. In this example, the **hostname** would be myCompany.akamaihd.net. The **identificationString** (regular expression) must be supplied which will uniquely identify (to the DME) incoming HLS playback URLs. In this example, the **identificationString** we use is **viv -**

- which will uniquely identify the ‘/i/’ within the playback URL. Any URL with that string will be processed as an Akamai HLS playback URL.

These settings (**hostname** and **identificationString**) are specified on the **Cache** page within the DME vbadm GUI. Entering them requires the following format:

**hostname**::{80 if http, 0 otherwise}::{443 if https, 0 otherwise}::**identificationString**

Special attention should be paid to make sure that the notation matches this format, including the double colon separators, without spaces.

For example, the following will treat any HLS (http or https) URL that contains ‘/i/’ to be serviced by myCompany.akamaihd.net publishing point.

**myCompany.akamaihd.net::80::443::\i\**

Once entered, you can hover over the field to review the ports and **identificationString**.

Special note about **identificationString**: The **identificationString** must uniquely match the playback URL associated with one and only one Akamai **hostname**. If more than one Akamai **hostname** is configured, the **identificationString** must be sufficiently unique to differentiate between playback URLs. For example, the following entries:

**myCompany-1.akamaihd.net::80::443::\i\**

**myCompany-2.akamaihd.net::80::443::\i\2**

Both of these entries match the following presented URL:

**http://dmeIP/i/2/streamName@streamID/master.m3u8**

The system would use the **myCompany-1.akamaihd.net** publishing point as opposed to the **myCompany-2.akamaihd.net** version. This illustrates and stresses the need for unique **identificationString** across all entries.

**Note:** This feature is available for general use, but Rev (or hybrid) customers will begin to see Rev overwriting these stream specifications in early 2017. VEMs customers can continue to use this feature.

If your Akamai hosts do not support port 443 (SSL), then you should not enable the “Use HTTPs to Browser”.

### Mesh with Rev Caching Configuration

## **Mesh with Rev Caching Configuration**

### **DME Mesh Architecture**

If you are using Rev with your DME(s), you will automatically utilize a shared cache that takes advantage of the DME mesh architecture. The goal of this architecture is for all your DMEs to communicate and reduce out-of-network bandwidth costs as a result. This, in turn, will reduce bandwidth for both DME to Rev-cloud communications and within your network topology from DME to DME. The DME mesh architecture also focuses on delivering content as close to the edge as possible. Once the content is within the DME mesh architecture, DMEs communicate between themselves to distribute the content effectively.

In terms of reducing network bandwidth, Vbrick’s first approach is to support reducing the number of DMEs to which Rev will pre-positioned content. This reduces out-of-band network bandwidth, as well as storage requirements for the DME. Once content is ready, Rev

---

instructs all pre-positioned DMEs to retrieve it. When the DMEs receive the download command, they first inspect their local storage to see if they already have the content and, if so, they are done.

For DMEs that do not have the content, a specific, randomly assigned, rotating DME (from the set of pre-positioned DMEs) will immediately begin downloading the content while the other DMEs wait a random amount of time (no more than 5 minutes). This allows the first DME to be seeded with the content, and subsequent download requests will utilize the DME mesh architecture if possible. (Larger content may require more time than is allotted and thus be requested directly from Rev until it is seeded in the mesh.) After the wait, each of the other DMEs will begin by first inspecting the mesh for the content, or download it from Rev as necessary.

**Note:** Pre-positioning is determined by customers. DMEs are defined as pre-positioned by system administrators within the Rev interface. Please see [Rev Online Help](#) for details.

In terms of improving playback, the DME mesh also focuses on state-of-the-art edge caching and multi-protocol first-time. Once the content is in the DME mesh, Vbrick leverages several technologies so it can be distributed and retrieved seamlessly by Vbrick players.

To illustrate the mesh architecture, several common use cases are presented below. Consider the example of 3 DMEs, DME-1 (prepositioned), DME-2, and DME-3 all reachable. DME-1 is the only prepositioned DME, so any new content uploaded to Rev will automatically be downloaded to DME-1. DME-1 currently has the following stored videos: video1.mp4, video2.m3u8 (HLS).

- **Case 1: HTTP.** A player requests to play video2.m3u8 from DME-2. DME-2 first checks locally for the HLS, but cannot find it. DME-2 then checks with the mesh. The mesh reports DME-1 has the HLS file and delivers it to DME-2. DME-2 caches the HLS file and then delivers it to the player. Playback begins for the user from DME-2. DME-2 will (first-time) cache all the .ts files that make up the HLS stream. Any additional (new) player requests for the HLS stream to DME-2 will pull from its cache.

This is the general solution when dealing with HTTP based content. If it is not local, then the Mesh is inspected. If it is found in the mesh, it is cached on the second DME. If it is not in the Mesh, then the player will fall back to Rev delivery.

- **Case 2: RTMP.** A player requests to play video1.mp4 using RTMP from DME-2. DME-2 first checks locally for the video1.mp4 file, but cannot find it. DME-2 then queries the mesh. The mesh reports DME-1 has the file. We cannot use the shared cache for delivery across RTMP to the player, so we redirect the player to DME-1. Playback begins for the user from DME-1.

DME-2, in parallel, has identified missing requested content that is present in the mesh, but not locally present. DME-2 will then initiate a mesh-copy of the content to get a local copy of video1.mp4. Once local, this copy can be provided directly for any subsequent RTMP requests. This is the general solution when dealing with requests across RTMP.

- **Case 3. Ultimate Fallback.** A player requests a video from DME-2 that is not present or in any reachable DMEs. At this point, if it is not on the DME-2 and it is not within the mesh architecture, the request will fail and the player will fall back and play from Rev. Playback begins for the user from Rev.

DME-2, in parallel, has identified missing requested content that is not present in the mesh, and not locally present. DME-2 will then notify Rev of the cache-miss content. Rev will receive the notification and then immediately re-position the content to all pre-positioned DMEs and the DME that reported the miss.

These case studies illustrate the basic use cases of retrieving data and how the mesh identifies, locates, and distributes content. This provides for a much more efficient delivery and distribution of content, but it also fills up our DMEs.

Starting with DME version 3.7, Vbrick introduced an automated process for removing older prepositioned content. This is done to keep enough storage space ready for additional downloads. The system monitors disk storage and when it reaches a predefined threshold, content is then evaluated on the DME and deleted based on a modified LRU (least recently used) algorithm. The thresholds are defined on the [DME Status Bar](#) help page.

The LRU algorithm identifies and orders content (ONLY from the UploadedVideos directory) by when it was last watched. The rationale reflects the standard caching theory that important content is watched more often than less important content. Any content not recently watched represents potential storage savings. The DME then removes sufficient content (to meet the threshold). The DME will only remove content from the UploadedVideos folder (which is content prepositioned by Rev), as such, there may be cases where the DME cannot recover space because of other services using the disk – e.g., multiple or long running HLS creation that is in Appending mode.

## DME Rules for Mesh Architecture

All DMEs will be automatically included within the mesh and utilized for content location and distribution. As such, reachability (ability to connect) between the DMEs is a critical issue for the mesh architecture. The mesh architecture has limited usefulness if DMEs cannot reach each other.

When moving into the DME mesh, the following guidelines should be considered:

- Do not add DMEs to Rev during peak use times. Adding a DME will cause a mesh update across all DMEs. This will cause playback disruptions as the mesh resets.
- Do not add DMEs to Rev during any live event. This will cause playback disruptions as the mesh resets. Adding a DME will cause a mesh update across all DMEs. This will cause playback disruptions as the mesh resets.
- Every meshed DME must have reachability to at least one other DME. DMEs rely on other DMEs to get and share content. If they cannot communicate, then they cannot share content. Visit the **System Configuration > Caching** page to see peered DMEs and their reachability status.
- Every meshed DME must have reachability to at least one other prepositioned DME. As mentioned above, DMEs need DMEs to share content. However, there should be reachability to at least 1 prepositioned DME for all DMEs. By doing this, any prepositioned content will be available to the non-prepositioned DME.
- Every stream and video file must have a unique name across the DMEs and within the mesh. This is a critical component of the mesh. Within the mesh, streams and pieces of streams (e.g., HLS .ts files) are flowing between DMEs that are serving them to players. When a duplicate name is entered into the system from separate DMEs this causes the mesh to deliver incorrect packets of streams to players. If you are transmuxing, transrating or creating new streams on DMEs please verify that the names are unique.
- Best Practices:

- When in doubt, set the DME to preposition.
- Double preposition (to a location) if availability is key.
- Create a naming scheme for your DME streams and video files (Rev enforces uniqueness of video file names).
- Plan for the appropriate use of your DMEs. Are they simply reflectors? VOD storage? Stream manipulation and transmuxing? Configuration depends on your topology and use.
- Most importantly, evaluate your network topology to best utilize the mesh. Vbrick Customer Service and Professional Services are a good resource for questions and solutions.

As noted, see the “Preposition DME Content” topic in Rev Online help for details on how to preposition content in Rev.

- ▼ To review or troubleshoot the status of your DME within the Mesh, do the following:
  1. First, evaluate if the DME is connected to Rev appropriately.
    - Navigate to **System Configuration > Rev Interface** and make sure the Rev Interface has been enabled and is running. See: [Rev Interface](#) for details if you need instructions.
    - As a short cut, in the bottom of each page to the far right should be two True or False indicators, one on top of the other. The top indicator is True if the Rev Interface is Enabled, and the bottom indicator is True if the Rev Interface Service is running. Both should be True for correct communication to Rev. If either is false, reset the Rev Interface by going to the **System Configuration > Rev Interface** page verify your settings and uncheck the **Rev Enabled** checkbox, click **Apply**, re-enable it, and click **Apply** again.
  2. Next, inspect the DME settings and connections to peer DMEs within the Mesh.
    - Navigate to the **System Configuration > Streaming** page and verify the **Cache System Resources** (Memory/Disk) setting. This is an overall setting that controls the amount of caching resources the system will use. Please see the [Caching](#) topic for more details.
    - Navigate to **System Configuration > Caching**. On this page, you can see how the DME is configured, HLS Remote Hosts, and all the peer DMEs within the Mesh. Inspect each peer DME to identify connectivity (via the Reachable column) and when the last connection was made.
    - The HTTP Port and ICP Port should be listed at the top of the page. Best practice is to use default port numbers for proper mesh usage.
    - Within the HLS Remote Hosts section you may see 1 or more hostnames – these are set by Rev if your account is enabled and using the Video Conference Recording and Streaming functionality. Otherwise, these will be blank. Do not edit these fields.
    - Review how this DME is configured, it will be identified as setup/or not for VOD playback and prepositioning. If the setting is (or should be) different, visit Rev to centrally reset it.
    - Within the Alternative Sources section you should see the list of your peer DMEs (to this current DME). This DME should be able to reach at least one prepositioned DME, OR this DME should be prepositioned. If you cannot see all of the peers, please use the Display dropdown list at the top of the page to increase the display size.

- There is also a Lock icon that can be hovered over to display status on certificate installation. This represents if a DME is locked down to https serving or not.
3. Lastly, if you feel that the DME's connection to the Mesh is faulty or needs re-configuration, do the following:
- Click the **Auto-Configure from Rev** button to perform a Mesh Update from Rev. This will request from Rev all mesh information (list of peer DMEs) and process each as necessary. If the DME detects any change between the current settings and the new list downloaded from Rev, then the DME will locally resets its caching system. This may have an impact on existing streams and viewers.

Because each DME can be configured differently within your deployment, this should be repeated on each DME you wish to inspect.

**Tip(s):**

- If you do not want to utilize the distributed caching mechanism, DME Mesh, then set all DMEs to preposition content on Rev.
- DMEs can be set as prepositioned on Rev. You cannot set it within the DME.
- From your DME, if there are no other reachable prepositioned DMEs (identified within the table) then this DME cannot utilize the Mesh and is stranded. Consider making this DME prepositioned.
- If you are an existing customer, when you upgrade to Rev v7.6 and DME v3.6 (or beyond), your DMEs will be automatically defaulted as prepositioned.

System Configuration --> Caching 2

---

Display 20 Sources ▾ HTTP Port: 80  
ICP Port: 3130

**HLS Remote Hosts**

01 <input type="text"/>	02 <input type="text"/>
03 <input type="text"/>	04 <input type="text"/>
05 <input type="text"/>	06 <input type="text"/>
07 <input type="text"/>	08 <input type="text"/>
09 <input type="text"/>	10 <input type="text"/>

This DME is setup for VOD Playback, but will NOT preposition content from Rev. These settings can be changed on Rev.

---

**Alternative Sources** Auto-Configure from Rev

Address	Prepositioned (1 total)	Reachable (2 total)	Last Attempted Contact
001 qadme05.lab.vbrick.com	✗ NO	✓ YES	3/16/2017 09:22:01
002 10.150.1.148	✗ NO	✓ YES	3/16/2017 09:22:01
003 10.150.1.20	✓ YES	✓ YES	3/16/2017 09:17:01
004 qadme04.lab.vbrick.com	✗ NO	✓ YES	3/16/2017 09:22:01
005 <input type="text"/>			
006 <input type="text"/>			

Standalone DME or Legacy (DME with VEMS) Caching Configuration



## Manage Configuration

▼ To access the Manage Configuration buttons:

1. Navigate to **System Configuration > Manage Configuration**.

Use the **Manage Configuration** page to set the DME defaults or reset the DME to the factory defaults. It also lets you save the DME configuration to an xml file or restore the configuration from a previously saved xml file.

**Caution:** Be aware that when you change the user name and password for the server (See: [Username and Password](#)) you are changing the FTP user name and password as well. However, when restoring previously saved settings, the FTP username and password will not be the same as the system user name and password.

For best results you will need to login again and change the user name and password to match the FTP username and password. (To keep the same username and password, change the username and password to something different, and then change it back again to the current username and password.).

Field/Button	Description
Set Defaults	Reset most settings except for Network Settings, and passwords to the factory defaults.
Set Factory Defaults	Reset all settings including Network Settings and passwords to the factory defaults.
Save Configuration	This will allow you to save all configuration settings that can be restored at a later time. This action will (1) copy and save settings (EXCEPT NETWORK or CERTIFICATE setting) in a system location (i.e. a "snapshot point") and (2) prompt you to download and save a physical file that can be restored at a later time. This does not save NETWORK or CERTIFICATE settings in these configurations so that configurations can be shared between different DMEs.



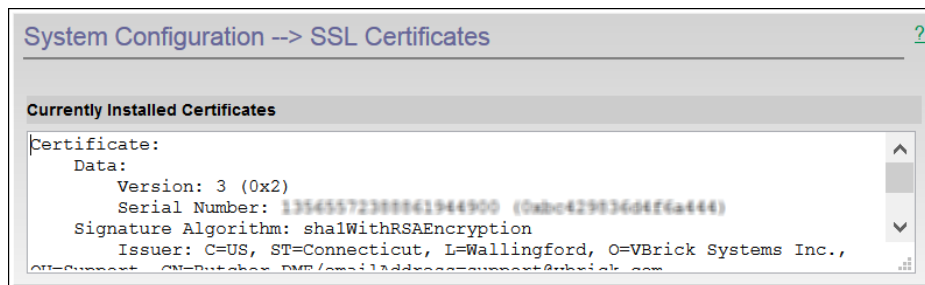
Field/Button	Description
Restore Configuration	<ul style="list-style-type: none"> <li>Restore from a file – This allows you to restore a previously saved configuration settings file. This operation will not restore the FTP user name and password. After a "restore configuration" you will need to manually change this (if desired) using the Username and Password page. Further, all NETWORK and CERTIFICATE settings will remain as previously set before the restore – please review and adjust accordingly. After any restore, it is good practice to review and possibly change your Username and Passwords, configuration settings, and streams.</li> <li>Restore from a snapshot point – Restores from the snapshot point created with a “Save Configuration.” Note: This option only works if there is a previously saved snapshot created with a “Save Configuration.” Also, similarly to Restoring from a file, all NETWORK and CERTIFICATE settings will remain as previously set before the restore – please review and adjust accordingly. After any restore, it is good practice to review and possibly change your Username and Passwords, configuration settings, and streams.</li> </ul>

## SSL Certificates

▼ To access the SSL Certificates fields:

1. Navigate to **System Configuration > SSL Certificate**.

When using SSL, a server certificate is required for secure communications. DME Supports two types of SSL security certificates: **Self-Signed** and **Authority Generated** (e.g. Verisign). Organizational security requirements determine which to use. Both are supported by the DME. Notice that the **Currently Installed Certificates** are displayed at the top of the form.



In the case of self-signed certificates, select the **Generate and Install a Self-Signed CERT** button and the certificate is simply generated and installed by the DME.

**Create a Certificate Request**

This section will help you create a CSR (Certificate Signing Request). A CSR is a block of encoded data generated by your web server that contains all the necessary information about your domain and organization. It will be encrypted by a Private Key that will be automatically created. Please review your internal security procedures and necessary field contents before beginning this process.

Country:

State (or Province):

City:

Company or (Organization):

Department:

Fully Qualified Domain Name:

Contact Email Address:

OR

If an organization elects to use a certificate from an authority, a PEM formatted certificate from the authority is necessary. The process for getting the certificate is:

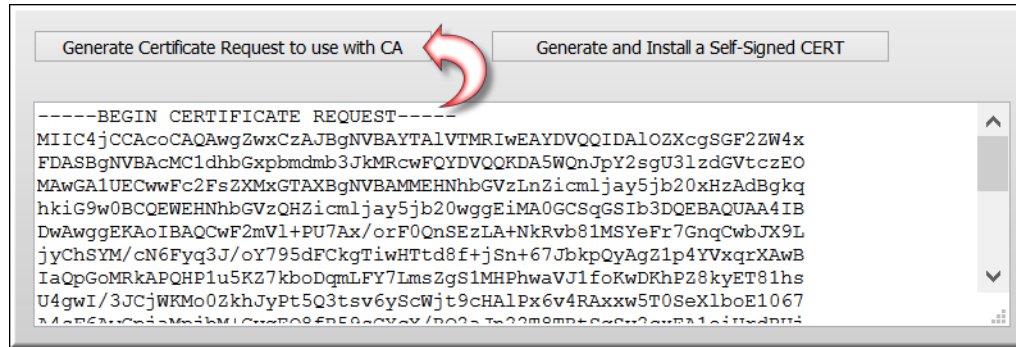
1. Generate a server certificate request by completing the fields in the table below.

Field	Description
Country	Information only. Country of certificate holder.
State (Province)	Information only. State of certificate holder.
City	Information only. City of certificate holder.
Company or Organization	Information only. Company of certificate holder.
Department	Information only. Department of certificate holder.
Fully Qualified Domain Name	The complete name of the domain, also referred to as a FQDN (fully qualified domain name) as registered on any Internet DNS. This name must be unique within the domain, and possibly accessible by the CA for verification. <i>All lowercase letters must be used.</i>
Contact email address	Information only. Email address of certificate holder.

**Caution:** Please make sure to enter your FQDN in all lowercase letters without leading or trailing spaces.

The DME does not support certificates with multiple FQDNs populating the **Subject Alternative Name (SAN)** field. If customers want to apply the same certificate to multiple DMEs, Vbrick recommends using a wildcard certificate. When applying/creating a host specific certificate, the SAN field should match the "cn=" field FQDN to meet browser security requirements. If you use the DME to create the CSR, then the field is a common name copied automatically into the SAN field by the DME.

2. Then click the **Generate Certificate Request to use with CA** button. The **Server Certificate Request** field will display an encoded CSR such as seen in the image below. During this process Vbrick stores a private key on the DME that will be used later.



3. With the encoded CSR, engage a Certificate Authority (that is trusted by all browsers within your organization – it is recommended that you use a well known CA).
4. Purchase the certificate specifically for the correct domain name for the DME (make sure the DME has that name, and organization DNS entries). Wildcard or star Certificates are also common – those certificates can be use on multiple servers in your organization. There are special naming conventions, please see the requirements of your CA.
5. Receive the certificate from the Certificate Authority and request PEM formatting.
6. If the CSR was generated on this DME, then the private key is on this machine as well and you can continue to step 7. However, if this is a Certificate whose CSR was generated on another machine, you will need to procure a private key. This approach is common when dealing with wildcard/star certificates. In order for the DME to correctly apply the Certificate, please make sure that the private key is also in the PEM. Select the **PEM Includes Key** checkbox if applicable. When selected, you will also need to complete an additional FQDN field to name your DME.
7. Install the certificate by pasting the PEM and all contents in the **Install New Certificate** field (at the bottom of the page) and then clicking the **Verify and Install New Certificate** button.
8. Finally, verify that your certificate was installed in the **Currently Installed Certificates** window (at the top of the page). An invalid certificate will not be installed. Also, the DME will reboot itself when the certificate is installed correctly.

Certificates provided by a certificate authority (CA) may include multiple components: a private certificate, one or more intermediate certificates, a root certificate, and a private key. The order of these items (for processing by the DME) must be:

- private key
- private cert
- intermediate cert(s)
- root cert

---

If you edit the PEM file to correct order, please do not change any content.

**Note(s):**

- Be aware that if the **Host Name** field of the DME is changed (**System Configuration > Network > Host Name**), the SSL certificate will revert back to a self-signed certificate. If the certificate is invalid and the DME interface is unable to be reached, the Admin console may be used.
- If you have installed your certificate and inadvertently overwrite it (through a factory reset, host name change, etc.), contact Vbrick Support Services for assistance in getting your old certificate back.
- Once you have finished working on installing a new CERT, please FTP into the DME and remove (delete or take offline) the folder containing your backup cert within the FTP log folder.
- Security Certificates should be created with 2048bit keys. Other lengths are currently not supported.

Fully Qualified Domain Name (FQDN)

## SAN/iSCSI Setup

In some configurations it may be desirable to extend the storage space of your DME. This can be done in the following ways: (1) add a new virtual disk to a VM, (2) add a new physical disk to a medium or large DME (small DMEs do not have the capability of adding additional space), or (3) add a network storage device. For options 1 and 2, please see [Disk Status](#).

This topic supports connecting a networked iSCSI device to the DME. Adding this device is different than adding additional virtual or physical disks – which extends the content storage location.

Adding an iSCSI actually mounts the an iSCSI device to a virtual folder name (directory location within the DME FTP root). Access to that directory is available through FTP and customers can store content there. Rev, however, only stores content within the UploadedVideos directory within the FTP root. Therefore, if you want to extend the storage space for Rev, you must mount to the UploadedVideos directory (Virtual Folder Name). This has the effect of making the original UploadedVideos directory (and any content) inaccessible while the iSCSI is mounted on UploadedVideos. Of course, the goal would be to mount a much larger iSCSI device that would provide all the necessary VOD storage.

Unlike the addition of new disks or virtual disks to VMs, iSCSI devices can be mounted and unmounted accordingly. Removing them will remove all the associated VOD content.

In older versions of the DME, it was possible to provision iSCSI devices (once connected via this page) on the **Disk Status** page. This is not recommended because it requires the iSCSI device to always be present for the DME. Current recommendations is to create a singleton iSCSI device with sufficient storage and mount that as UploadedVideos.

▼ To access the SAN/iSCSI Setup fields to review and provision your connections:

1. Navigate to **System Configuration > SAN/iSCSI Setup**.

Field	Description
Device	Enables the DME for SAN use. Disabling will remove the SAN device and restart the DME. Enabling the device will discover the device and provision the disk using the folder name specified below.
Username/Password	SAN access rights may require use of a user name and password. Please enable the password checkbox if a password exists.
Device IP Address	Where the SAN is found on the network.
Virtual Folder Name	The name given to the SAN disk as a mapped folder. "iSCSI" is recommended and becomes the folder name in the default FTP path. Be sure the name you choose is not already in use.
Format Destination	<ul style="list-style-type: none"> <li>Do Not Format – Default.</li> <li>Force Format – When used in conjunction with enabling the device, this option will delete all content on the disk. If the disk was previously provisioned, you may <u>not</u> want to format the disk again.</li> </ul>
Discovered Device	Read-only. If the SAN is found the device identification will be provided automatically.
Status	Read-only. Displays the disk size, or "unknown" if no SAN is discovered.

## Activate Feature

The DME is a licensed product from Vbrick. A license file, available from Vbrick Support, will provide access to Vbrick DME functionality – both the DME in general, as well as features. The **System Configuration > Activate Feature** page provides the ability to apply, maintain and update licenses on the DME.

- If you purchased a hardware DME from Vbrick, it will come with the license already installed.
- If you purchased a software Virtual Machine version of the DME, you will need to download the ova and install it and contact Vbrick Support for the License.
- If you purchase a feature in the future, you will need to get your Currently Installed License (from the System Configuration > Activate Feature page) and contact Vbrick Support to augment the license.

▼ To activate a new license or feature on the DME:

1. Navigate to **System Configuration > Activate Feature**.

Some optional DME features, for example Stream Conversion, must be “activated” before the functionality is available on the Configuration Menu.

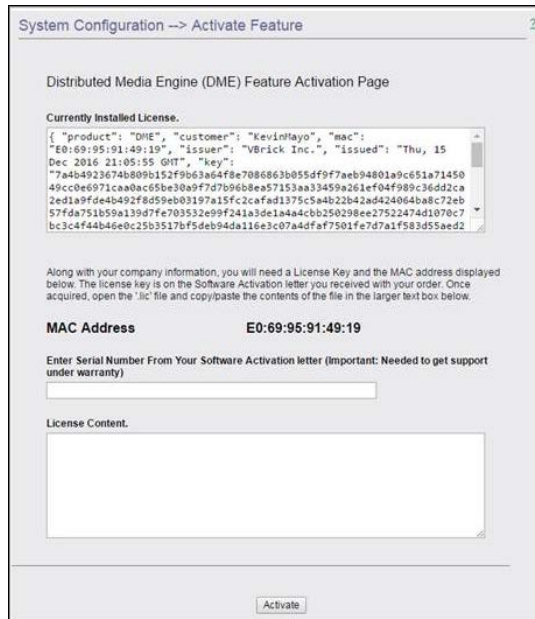
You will need:

- The MAC address of the DME machine.
- The serial number for future support.
- A license file from Vbrick Support that includes the feature.

The MAC Address of the DME machine is shown on the Activate Feature page (seen below); the Serial Number and License File are available using the “License Activation” letter you received with your order.

After you get the license file (as explained below) you will copy and paste the entire contents of the file into the License Content text box.

Once activated, the system license will be shown on the **System Configuration > General** page.



- ▼ To obtain a license file and activate a feature:
  1. Navigate to **System Configuration > Activate Feature** page.
  2. Contact Vbrick Support to obtain the license file needed for your DME and features purchased. You may need to provide the license text from the Currently Installed License text box for verification and modification.
  3. Vbrick Support will supply the new license text (either as a .lic file, or as text within an email).
  4. Open the file in Notepad and copy the entire contents and paste it into the **License Content** text box.
  5. Enter the serial number from the sticker in the **Serial Number** text box.
  6. Click **Activate** to close the application and display the login page.
  7. Login and repeat these steps for each additional licensed feature.

Register the DME

## Rev Interface

▼ To configure the DME to interface with Rev:

1. Navigate to **System Configuration > Rev Interface**.

To stream and store content from Vbrick Rev, you must first configure your DME to integrate with Rev. You must complete the fields below and click **Apply** before you will be able to add this DME as a device in Vbrick Rev.

Field	Description
Rev Interface Running	Indicates whether or not the DME service that communicates with Rev is running or not. This service is responsible for communicating with Rev and must be running for communication between the DME and Rev to occur (videos can still be accessed on the DME by Rev). If the service is not running and set to false, toggle and save the <b>Rev Enabled</b> checkbox to restart the service. If you experience further trouble with the service restarting, contact Vbrick Support Services.
Rev Enabled	Select to enable integration with Rev with your DME. This allows your DME to be linked with Rev.
Rev Server URL	The URL of your Rev server.
API Key	An API key that is created through the Vbrick Rev interface. This key must match the key that is created for the device in Rev's Device module for the DME. <b>Please note that the API key may not contain the special characters ``]%'&amp;+'&lt;</b>

Field	Description
Default User	<p>Used to define the Uploader metadata attribute when using Rev's POST uploads/videos API to upload VOD files to Rev. This is normally used when the "no metadata" field is specified in the corresponding JSON file or anytime the Uploader field is not present in the JSON file. It is good practice to specify an Uploader to your video file so it is recommended that the JSON file contain this field or that you use the DME Default User field to specify the Uploader. If no value is specified in this field, the DME will supply a default value of "DME".</p> <p><i>Important: Whatever value is specified in this field, a valid Rev user account must match that value. For example, if the default value of "DME" is used, a Rev user name of DME must also be present.</i></p> <p>See: <b>Required File Types for Bulk Video Upload</b> topic for details.</p>
Default Folder to Store Media	If your DME is designated as a VOD storage device in Vbrick Rev, the folder content will be stored in for later access and playback.
MAC Address	The MAC Address of your DME device. Vbrick Rev will ask for this address when you add your DME as a device in Rev's Device module.
Retry Rev Uploads	Click to manually restart a bulk VOD ingestion process to Rev if it fails for any reason. See: <b>Start a Bulk Video Upload to Rev</b> topic.

Once you have successfully configured the DME to interface with Rev, you may perform the integration features that have been implemented for Rev. For more details on those functions, view the **Rev Integration Functions** help topic.

[Rev Integration Functions](#)



# Rev Integration Functions

## DME Video EdgeIngest to Rev

**Tip:** Before any Rev integration functions may be performed, you must configure your DME to interface with Rev correctly.

See: [Rev Interface](#).

EdgeIngest easily allows admins to bulk ingest content up into the Vbrick Rev system. To do this, the admin generates a metadata file for each media file to upload (JSON formatted as described below) and then places the files into a specific directory within the DME. The DME takes over from there and copies the contents up to Rev.

This is a simple and handy method for uploading Video on Demand (VOD) content. This feature is limited to Vbrick Rev.

**Note:** Admins should be aware of local bandwidth constraints and impacts when uploading multiple large media (with metadata) files. Admins can limit network use and saturation by uploading the media and metadata files in small batches during low use periods.

- ▼ The following steps outline the use of EdgeIngest to upload videos from any DME to Rev:
  1. Prepare the required media and metadata (JSON) files for ingestion
  2. FTP the files to the EdgeIngest directory (in the base FTP directory)
  3. Monitor and troubleshoot the ingestion as needed

### Required File Types for Bulk Video Upload

Two files are needed for each video EdgeIngest upload; the video file itself in .mp4 format and a corresponding metadata file in JSON format with the exact same name. These are the two files Rev's API will use to upload the video to Rev's interface; all other file types will be ignored. For example, for a video named VirginiaVideo, two files will be supplied: VirginiaVideo.mp4 and VirginiaVideo.json.

The following data fields may be included in the JSON metadata file.

- Title
- Description
- Uploader
- Categories
- Tags
- EnableComments
- EnableRatings

- EnableDownloads
- IsActive
- VideoAccessControl
- AccessControlEntities

**Note:** Files will only be uploaded if a corresponding JSON file is present and valid. Also, please *do not* upload more than 6000 files at any one time. For large numbers of files, it is best to stagger placing the files into the EdgeIngest folder so the DME can process them in turn.

An example of a JSON metadata file:

```
{
  "title": "Title for the video file",
  "description": "Description for the video",
  "enableComments": "false",
  "enableRatings": "false",
  "enableDownloads": "true",
  "uploader": "adminuser",
  "isActive": "true",
  "tags": ["video", "upload", "mp4"],
  "categories": ["Category1", "Category2"],
  "CategoryIds": ["<id1>", "<id2>"],
  "videoAccessControl" : "Public" ,
  "accessControlEntities" : [
    {"name": "user1", "type": "User", "canEdit": "false"},
    {"name": "group1", "type": "Group", "canEdit": "false"},
    {"name": "team1", "type": "Team", "canEdit": "false"}
  ]
}
```

Keep in mind that all fields are optional. This means that you may upload a file to Rev with no metadata. However, you will still need to supply a JSON file for the video ingestion to start.

To accomplish this, a “no metadata” keyword field has been created to alert the DME that no metadata will be sent to Rev. In this case, only the **Uploader** field that is identified on the DME Rev Interface page will be provided to Rev. If this field is not provided in the DME either, the DME will default the field to “DME”.

▼ To send no metadata to Rev:

```
{ "noMetadata" : "any string or integer" }
```

**Notes on JSON file formatting:** The JSON format will not accept certain characters such as a Tab or Carriage Return. Processing will fail on JSON files that include these special characters. However, these characters may still be included if they are encoded.

To include these characters within your JSON file, please use the following table to encode the strings. For example, if you want a string “**Hello ^t World**” where ^t is a Tab character, it would be encoded as “**Hello \t World**”. Embedded single quotes are not supported.

\b **Backspace** (ascii code 08)

\f **Form feed** (ascii code 0C)

\n **New line**

\r **Carriage return**

\t **Tab**

\ " **Double quote**

\\ **Backslash character**

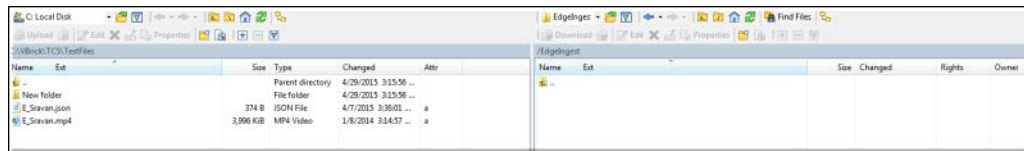
**Tip:** Please refer to the [Rev REST documentation](#) for a complete list of metadata that Rev can accept with the Upload Video API.

## Start a Bulk Video Upload to Rev

The DME monitors the EdgeIngest directory for new .mp4 and JSON files. When new files are copied to this directory, the DME will start the ingestion process to Rev.

- /var/www/html/EdgeIngest

Using an FTP client, copy the video and FTP files into the directories referenced above.



## Bulk Video Upload to Rev File Properties

The copied video files and their corresponding JSON (metadata) files are sent to Rev through Rev's POST uploads/videos API found on the Vbrick documentation site.

Keep in mind that if the .mp4 file or JSON file is missing any metadata fields, the DME will not supply any default fields. The exception to this is the **Uploader** field which may be provided through the DME's Rev Interface page and is defaulted to "DME". You must have a Rev user account with the same name as the **Uploader** field in the DME if you decide to use this function instead of supplying it through the JSON file.

Rev will also supply any default values through the API itself if you do not provide the metadata fields. To understand how these fields are handled through Rev in this case, view the Rev REST API Online help.

Once the files have been uploaded to Rev, they will be removed from the DME directory. The result of the ingestion will be logged. You may view this log at **Monitor > Upload Log**.

**Note:** If the upload fails for any reason, often due to network issues, you may manually start the upload process again by using the **Upload** button under the **Rev Interface** page.

## Monitor a Bulk Video Upload to Rev

The **Upload Log** is used to provide status on files that Rev uploads from the DME. The date, time, file name, and status of each ingestion is provided.

See: [Monitor and Logs > Upload Log](#) for details.

Keep in mind that the DME will continue the upload process controlled by the following variables (Note: These are system variables that may not be modified at this time):

- **Max\_Rev\_Uploads:** The number of simultaneous upload attempts that may occur. Default = 50.
- **Max\_Reload\_Retry:** The number of times to retry an upload. Default = 10.

- 
- Delay\_Reload\_Retry: The number of seconds to delay before the next retry. Default = 300.

Rev Interface

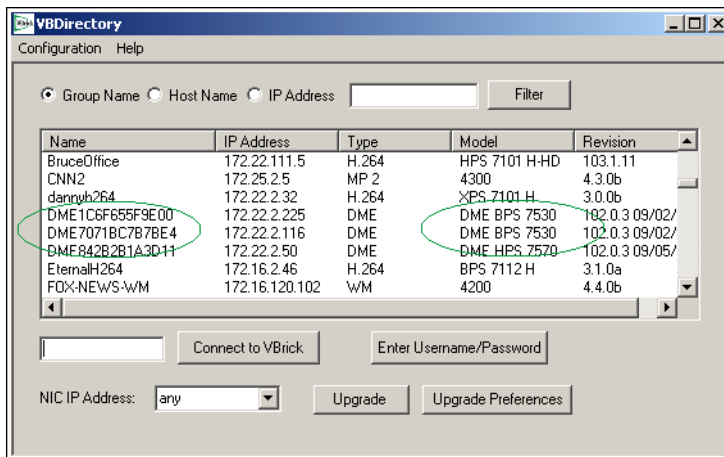
# SAP Configuration

## Announcement Types

### Management SAP

Management SAPs provide the ability for a DME to announce its existence to interested programs/devices on a network. The major clients for these announcements are:

- VBDirectory - A free application from Vbrick. VBDirectory provides an easy way to access a DME from any PC for configuration or upgrade. It lets you see the status and code revision levels of all networked Vbrick devices.
- VEMS Mystro - Vbrick's portal product uses the announcements to recognize the existence of DMEs and to make DME configuration easier and less error-prone.



### Announce SAP

Announce SAPs are used by a DME to announce the existence of live streams. The major clients for these announcements are:

- StreamPlayer – This application provides an easy way for a PC to view video transmitted by DMEs. It can be useful as a test device for VEMS Mystro users, or as a standalone player for much of the content distributed by the DME.
- VEMS Mystro – Vbrick's portal product uses the announcements to recognize the existence of video streams from DMEs. Streams appear on the Mystro interface without manually configuring URLs of the sourced video.

## Announcements

- ▼ To access the Announcements fields:
  1. Navigate to **SAP Configuration > Announcements**.

**Management SAP**

---

Transmit Enable  Enabled

Group Name

Unit Number

Retransmit Time

Time To Live

Differentiated Services

IP Address

Port

Management SAP Fields	Description
Transmit Enable	Check to enable transmit for management SAPs. Default = <b>Enabled</b> .
Group Name	Optional. This parameter is included in the Management SAPs used by VBDirectory. It is used for organizing Vbrick devices into groups to simplify use of VBDirectory.
Unit Number	Optional. The appliance unit number (range 0–2147483647) is used to identify each DME in a group.
Retransmit Time	Defines the Management SAP retransmit time.
Time To Live	For Unicast, the number of hops (between routers) for which an IP packet is valid in the network. For multicast the distribution scope of the SAP.
Differentiated Services	<b>Differentiated Services Code Point (DSCP)</b> field in the header of IP packets for packet classification purposes. DSCP replaces the three bit <b>Type of Service</b> byte of the IP header. See <b>Differentiated Services</b> on the <a href="#">Streaming</a> topic.
IP Address	Defines the Destination IP Address for Management SAPs.
Port	Defines the Destination Port for Management SAPs.

**Announce SAP**

---

Announce Enable  Enabled

Send SAP for Internal IP  Enabled

Send SAP for NAT'ed IP  Enabled

IP Address

Port

Transmit Interval

Time To Live

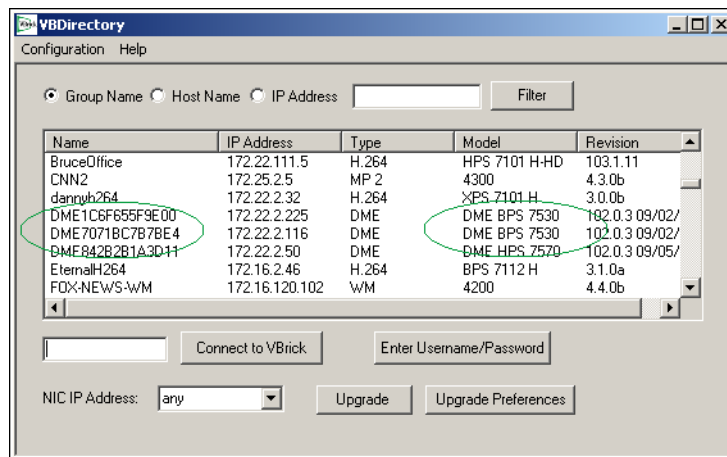
Differentiated Services

Author

Copyright

Announce SAP Fields	Description
Announce Enable	Enables configuration of the announcement.

Announce SAP Fields	Description
Send SAP for Internal IP	Destination IP address of the Multicast Announcement for Stream Announcements. Most commonly for multicast, but can be unicast for direct transmission to, for example, a VEMS Mystro server.
Send SAP for NAT'ed IP	Send a SAP for the natted IP address configured on the System Configuration > <a href="#">Network</a> page.
IP Address	Actual IP address of the SAP announcement.
Port	Announcement Destination Port.
Transmit Interval	How often the Announcement is transmitted in seconds.
Time to Live	For unicast, the number of hops (between routers) for which an IP packet is valid in the network. For multicast, the distribution scope of the SAP.
Differentiated Services	Value that instructs (capable) routers on how to handle a packet. These are generally quality of service items. This is typically set to all zeros. See <b>Differentiated Services</b> on the <a href="#">Streaming</a> topic.
Author	Optional author information
Copyright	Optional copyright information



## SAPs for Unannounced Streams

▼ To access the SAPs for Unannounced Streams fields:

1. Navigate to **SAP Configuration > SAPs for Unannounced Streams**.

Use this page to enable SAPs for streams which have been configured for input to the DME using Unannounced Unicast/Multicast (In-8). This is not a common configuration and it is recommended that an alternate input method be utilized if possible.

SAP Configuration --> SAPs for Unannounced Streams 2

Index	Enable	Publishing Point	Status
1	Disabled ▼		Disabled
2	Disabled ▼		Disabled
3	Disabled ▼		Disabled
4	Disabled ▼		Disabled
5	Disabled ▼		Disabled
6	Disabled ▼		Disabled
7	Disabled ▼		Disabled
8	Disabled ▼		Disabled
9	Disabled ▼		Disabled
10	Disabled ▼		Disabled
11	Disabled ▼		Disabled
12	Disabled ▼		Disabled
13	Disabled ▼		Disabled
14	Disabled ▼		Disabled
15	Disabled ▼		Disabled
16	Disabled ▼		Disabled
17	Disabled ▼		Disabled
18	Disabled ▼		Disabled
19	Disabled ▼		Disabled
20	Disabled ▼		Disabled

Field	Description
Enable	Enables the SAP of the stream
Publishing Point	The publishing point of the stream. The format of this publishing point is <streamname>.sdp and is the file name which has be manually placed on the DME.
Status	Current status of the connection and the SAP transmission for this stream.



# Input Stream Configuration

## RTMP/RTSP Pull

▼ To access the RTMP/RTSP Pull fields:

1. Navigate to **Input Configuration > RTMP/RTSP Pull**.

Use this page to configure streams that will be pulled into the RTMP Multi-protocol server on the DME. Both RTMP and RTSP streams are configured on this page.

As shown below the number of supported streams depends on the DME hardware you purchased. See table below for the number of configurable input streams.

Index	Stream Name	Type	Source IP Addr/Name	Application	Publishing Point	User Name	Password	Use RTCP	Enable	Status
1	scarPresenter	RTSP	scar.vb.loc		vbStream1S1			<input checked="" type="checkbox"/>	Enabled	Disconnected
2	JohnsStream	RTSP	172.22.113.3		vbStream1S1			<input checked="" type="checkbox"/>	Disabled	Disabled
3	hookPresenter	RTSP	hook.vb.loc		vbStream1S1			<input checked="" type="checkbox"/>	Enabled	Receiving
4	CCStream	RTMP	10.200.0.36	live	captiontest			<input checked="" type="checkbox"/>	Disabled	Disabled
5	pokeyRTP	RTSP	chernabog.lab.v		scarPresenter			<input checked="" type="checkbox"/>	Disabled	Disabled
6	aStream	RTSP	scar.vb.loc		vbStream1S1			<input checked="" type="checkbox"/>	Disabled	Disabled
7	RTSPPullfromUr	RTSP	10.10.7.211		vbStream1S1			<input checked="" type="checkbox"/>	Disabled	Disabled
8	BogusScarHLS	RTSP	scar.vb.loc		vbStream1s1			<input checked="" type="checkbox"/>	Disabled	Disabled
9	Weather	RTSP	10.10.3.140		vbstream1s1			<input checked="" type="checkbox"/>	Disabled	Disabled
10	RTMPPull	RTMP	127.0.0.1	live	JohnsStream			<input checked="" type="checkbox"/>	Disabled	Disabled
11	BogusHLS	RTSP	hook.vb.loc		vbStream1s1			<input checked="" type="checkbox"/>	Disabled	Disabled
12	BogusHLS2	RTSP	hook.vb.loc		vbStream1s1			<input checked="" type="checkbox"/>	Enabled	Receiving
13	MirrorThis	RTSP	hook.vb.loc		vbStream1s1			<input checked="" type="checkbox"/>	Enabled	Receiving
14	BogusHLS	RTSP	chernabog.lab.v		khanHLSPull			<input checked="" type="checkbox"/>	Disabled	Disabled
15	PullStream15	RTMP						<input checked="" type="checkbox"/>	Disabled	Disabled
16	PullStream16	RTMP						<input checked="" type="checkbox"/>	Disabled	Disabled
17	PullStream17	RTMP						<input checked="" type="checkbox"/>	Disabled	Disabled

Field	Description
Stream Name	Name used within the DME to connect input and output streams. It is possible to effectively retain the input stream name by making stream name and Publishing Point names the same or changing the stream name to the name used within the DME. In some cases, the publishing point names may be cryptic as is typically true if coming from a CDN
Type	<ul style="list-style-type: none"> <li>• RTSP – pull the RTSP stream into the DME.</li> <li>• RTMP – pull the RTMP stream into the DME.</li> </ul>
Source IP/ Address:Port	Enter the IP address of the source server. Enter a port number only if you are not using the default RTMP port (1935) or the default RTSP port (554). If pulling RTSP from the RTP Streaming server, enter <b>127.0.0.1</b> .

Field	Description
Application	Only required if you are pulling RTMP. This string is defined by the source. For example, on a Vbrick encoder, this string corresponds to the <b>RTMP Application</b> value on the Program Configuration > Transmitters page. Valid strings are limited to: <b>live</b> , <b>vod</b> , <b>vbrick</b> , and <b>vbApp</b> .
Publishing Point	This is Publishing Point Name on the source server. If the source is a Vbrick encoder, use the <b>Resource Name</b> on the Program Configuration > Servers page on the encoder.
User Name	Required if client-side authentication is required by the source server.
Password	Required if client-side authentication is required on the source server.
Use RTCP	Default = <b>Enabled</b> . RTCP server reports assist maintaining audio/video synchronization for some players. Uncheck if your server does not generate RTCP reports or if you wish to ignore RTCP reports from the source.
Enable	Use this dropdown to enable or disable the stream. All streams are disabled by default.
Status	Read only: Disabled   Connected   Receiving.

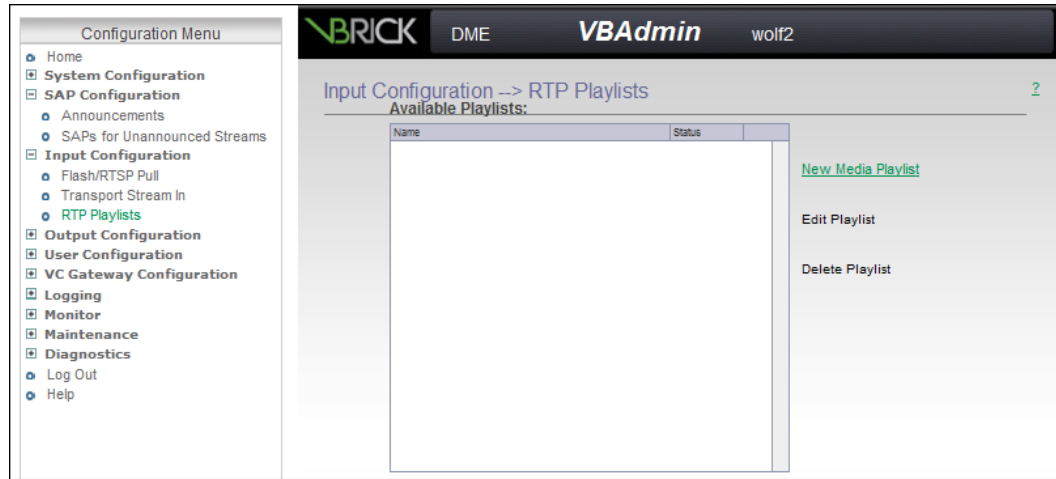
DME Model	Number of Configurable Input and Output Streams
7530	25
7550	35
7570	60

## RTP Playlists

RTP Playlists make it possible to send stored .mp4 (Part 10) VOD files as live streams. They can consist of a single file or multiple files and can be reordered and concatenated into a single playlist. They can also be weighted and played in differing modes; for example, they can be looped or played sequentially.

You can then use a playlist to create a multicast relay using the .sdp file, i.e. the **Mount Point**.

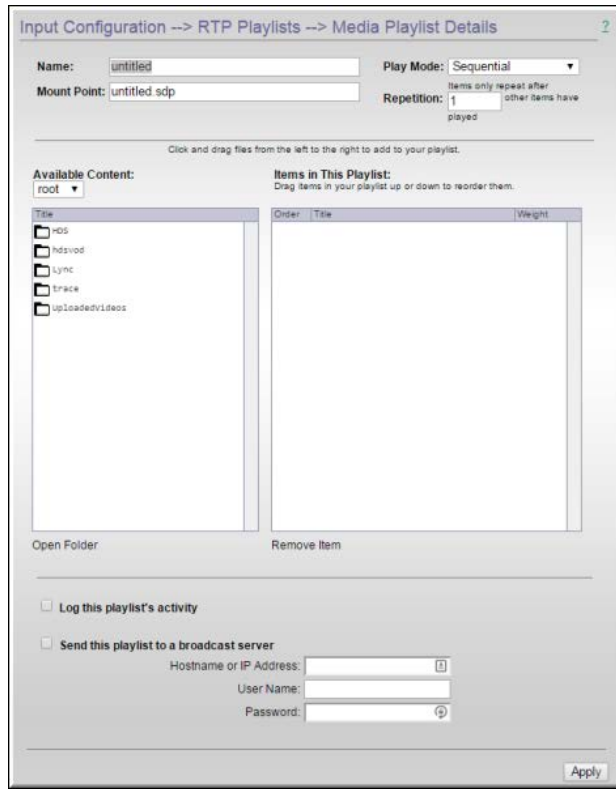
To launch a playlist, you can use it in an RTSP URL by specifying the .sdp file name or you can use it to create an RTP Relay.




Field/Icon	Description
Available Playlists	The playlist is playing. 
	The playlist is stopped. 
New Media Playlist	Create a new Media Playlist.
Edit Playlist	Edit the selected Playlist.
Delete Playlist	Delete the selected Playlist.

### *Create or Edit an RTP Playlist*

- ▼ To create or edit an RTP Playlist:
1. Navigate to **Input Configuration > RTP Playlists**.
  2. Click **New Media Playlist** to create a playlist or the playlist name and then **Edit Playlist** to modify an existing playlist.



Field/Icon	Description
Name	Unique name for the playlist.
Mount Point	The .sdp file name associated with the playlist in <b>ftproot</b> .
Play Mode	Determines the order in which individual streams are played. <ul style="list-style-type: none"> <li>Sequential – the streams are played once sequentially. Drag the streams up or down to set the order in which they are played.</li> <li>Sequential Looped – the streams are played sequentially in an endless loop.</li> <li>Weighted Random – the streams are played randomly according to the weighted value. Use the arrow icons to set the weight from 1–10.</li> </ul>
Repetition	Items only repeat after <b>nnn</b> other items have played.
Available Content	Use the dropdown to go up one folder at a time. Click and drag files from the left to the right to add to your playlist.
Items in This Playlist	Order – click and drag file up or down to modify order. Title – click to select. Weight – use arrow controls to assign weight (1 – 10).
Open Folder	 This control is active when you select a folder (icon shown here) in the Available Content list. Open a folder, then drag in a file and click <b>Apply</b> .
Remove Item	This control is active when you select an item in the playlist.

Field/Icon	Description
Log this playlist's activity	Log this playlist's activity in the <a href="#">Access History</a> log.
Send this playlist to a broadcast server	<ul style="list-style-type: none"> <li>• Hostname or IP Address – enter server host name or IP address of broadcast server.</li> <li>• User Name – enter valid administrator name on broadcast server.</li> <li>• Password – enter valid administrator password on broadcast server.</li> </ul>

## Transport Stream In

▼ To access the Transport Stream In fields:

1. Navigate to **Input Configuration > Transport Stream In**.

Use this page to configure streams pushed via unicast or multicast to the Multi-Protocol server using transport stream. The number of streams supported depends on the model of the DME.

Index	Stream Name	Multicast Source/Localhost	Port	Enable	Status
1	TSPullStream1			Disabled	Disabled
2	TSPullStream2			Disabled	Disabled
3	TSPullStream3			Disabled	Disabled
4	TSPullStream4			Disabled	Disabled
5	TSPullStream5			Disabled	Disabled
6	TSPullStream6			Disabled	Disabled
7	TSPullStream7			Disabled	Disabled
8	TSPullStream8			Disabled	Disabled
9	TSPullStream9			Disabled	Disabled
10	TSPullStream10			Disabled	Disabled
11	TSPullStream11			Disabled	Disabled
12	TSPullStream12			Disabled	Disabled
13	TSPullStream13			Disabled	Disabled
14	TSPullStream14			Disabled	Disabled
15	TSPullStream15			Disabled	Disabled
16	TSPullStream16			Disabled	Disabled
17	TSPullStream17			Disabled	Disabled
18	TSPullStream18			Disabled	Disabled
19	TSPullStream19			Disabled	Disabled
20	TSPullStream20			Disabled	Disabled
21	TSPullStream21			Disabled	Disabled
22	TSPullStream22			Disabled	Disabled
23	TSPullStream23			Disabled	Disabled
24	TSPullStream24			Disabled	Disabled
25	TSPullStream25			Disabled	Disabled

### MPG2TS Streams

The DME can accept a live unicast or multicast MPEG2TS (with an MP2 or MP4 H264 payload) and deliver it from the DME as unicast or multicast. (A live MPEG2TS is typically pushed from a a VB6000/7000/9000 Vbrick MPEG-2/H.264 encoder or another DME.)

For H264 content wrapped in an MPEG2TS, the stream can also be transmuxed and delivered as RTMP, HLS, RTP, or HDS.

*For MYPEG-2 content, there is no transmuxing.* In order to identify an incoming Transport Stream with MPEG-2 content (so that it can be “passed through” without further parsing), the incoming stream name must be preceded with “**mp2:**”.

For example, when configuring a **Transport Stream In** (with MPEG-2 content) the **Stream Name** must be: **mp2:streamname**.

Similarly, you must use the same **Stream Name** (preceded with **mp2:**) when configuring the stream for **Transport Stream Out**. Using this stream as input for HLS or other conversions will not work. Passthrough Transport Streams preserve KLV data when being delivered through the DME.

Field	Description
Stream Name	Name used within the DME to connect input and output streams. Use the default stream name ( <b>TSPullStream1</b> , <b>TSPullStream2</b> , etc.) or override as desired. See above, <u>MPG2TS Streams</u> (with MP2 content) must be prepended with <b>mp2:</b>
Multicast Source / Localhost	Source of multicast stream/local host. If the stream is a unicast to the DME, enter the DME's IP address. For source specific multicast addresses, enter it as "multicastipaddress:sourceipaddress.". Example: 232.1.1.1:172.22.2.166
Port	Port on which the stream is unicast or multicast. If there are multiple unicast input streams, be sure that each input stream has a unique port number.
Enable	Use to enable an input stream.
Status	Read only: Disabled   Connected   Receiving.

# Output Stream Configuration

## RTMP Push

▼ To access the RTMP Push fields:

1. Navigate to **Output Configuration > RTMP Push**.

Use this page to configure streams that will be pushed to a destination device using RTMP. Possible destinations for RTMP push include a CDN (content delivery network) like AWS, Akamai, or EdgeCast.

This is the preferred protocol for sending streams to another DME. As shown below the number of supported streams depends on the DME hardware you purchased. Note that some fields marked with a trailing (o): these (o)ptional fields may be required at the destination device, for example by a Wowza or other CDN server. See table below for the number of configurable output streams.

Index	Stream Name	Target Name	Destination IP Address:Port	Application	Emulate(o)	swf URL(o)	page URL(o)	User Name	Password	Protocol	Enable	Status
1	JohnsStream	PokeyPushingLo	pokey	live				broadcast	*****	rtmp	Enabled	Waiting for stream
2	RTSPPullfromLiv	PokeyPushingLiv	10.10.6.177:193	live				broadcast	*****	rtmp	Enabled	NotFound
3	JohnsStream	JohnsStreamFro	10.10.7.224:193	live				broadcast	*****	rtmp	Disabled	Disabled
4	hookPresenter	639883293166	live-api-4.facebc	rtmp						rtmp	Disabled	Disabled
5	pusadOBS	OBS2HLS	10.10.7.235:193	live				broadcast	*****	rtmp	Disabled	Disabled
6	MirrorThis	test_02_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Enabled	Connection failed
7	scarPresenter	ScarPresenterPh	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Enabled	Connection failed
8	BogushLS2	rtmpsPush	chernabog.lab.v	live				broadcast	*****	rtmps	Enabled	Streaming
9	BogushLS2	eLUBPin0NivW	bf5569e-rtmp.v	live				broadcast	*****	rtmp	Disabled	Disabled
10	BogushLS2	kevinRTMPush	qa-dme-04.lab.v	live				broadcast	*****	rtmps	Enabled	Streaming
11	BogushLS2	8ILZmqtcVDD	eo30031-rtmp.v	live				broadcast	*****	rtmps	Disabled	Disabled
12	MirrorThis	test_08_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
13	MirrorThis	test_09_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
14	MirrorThis	test_11_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
15	MirrorThis	test_12_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
16	MirrorThis	test_13_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
17	MirrorThis	test_14_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled
18	MirrorThis	test_15_from_c	koda.lab.vbrick.k	live				broadcast	*****	rtmp	Disabled	Disabled

Field	Description
Stream Name	Name identified on the Multi Protocol input for this stream.
Target Name	Stream name on the destination. When pushing to another DME it is generally easiest to reuse the Stream Name as the Target Name.
Destination IP/Address:Port	The IP address and port number of the destination server.

Field	Description
Application	<p>The application is defined by the destination. For example, when sending to another DME, the string should be <b>live</b>, <b>vbApp</b>, <b>vbrick</b>, or <b>vod</b>. When sending to a CDN, the string will need to be extracted from the publishing URL the CDN gives to you.</p> <p>An example publish to URL from a CDN such as Edgecast is:  <b>rtmp://fso.dca.A3CD.edgecastcdn.net/20A3CD/HLSTest/vBrick?xZ7q0oCEoQ6hvp5</b></p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Target Name = <b>vBrick?xZ7q0oCEoQ6hvp5</b></li> <li>• Destination = <b>fso.dca.A3CD.edgecastcdn.net</b></li> <li>• Application = <b>20A3CD/HLSTest</b></li> </ul>
Emulate (o)	Optional May be required for some destination devices.
swf URL (o)	Optional May be required for some destination devices.
Page URL (o)	Optional May be required for some destination devices.
User Name	Required if client-side authentication is required by the destination server
Password	Required if client-side authentication is required on the destination server
Enable	Use dropdown to enable or disable the stream. All streams are disabled by default.
Status	Read only: Disabled   Streaming   Waiting for Stream (Input source <stream_name> not yet available.)

DME Model	Number of Configurable Output Streams
7530	25
7550	35
7570	60

## Flash Multicast

**Important!** Vbrick has removed the ability to deliver Flash playback URLs from Cloud Rev. In other words, Rev no longer directs players to Flash. Be advised, DME v3.26 will remove Flash Multicast entirely as a result.

▼ To access the Flash Multicast fields:

1. Navigate to **Output Configuration > Flash Multicast**.

This page will allow you to convert a stream to Adobe's Flash Multicast. This protocol can be played by existing, fielded Flash players removing the need to distribute players for multicast playback. Vbrick continues to see the necessity and need for multicast within the enterprise environment and provides Flash Multicast as an alternative for this support.



The most common use case here is for organizations to unicast a stream from a central location to one or more remote DMEs, where that DME then multicasts to local viewers.

**Note:** When you first begin to use and deploy Flash Multicast, please initially click the **Rename** button on all indexes to assure uniqueness of URLs. This only needs to happen once.

Output Configuration --> Flash Multicast 2

Multicast TTL

Index	Stream Name	Multicast/Destination IP Addr/Name	Port	Enable	Status
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Disabled	Disabled
	<input type="button" value="Rename"/>	URL: http://172.22.2.193/FMout/58bb5fb4-35e0-4dde-a151-8072a9f7b4fe.f4m			
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Disabled	Disabled
	<input type="button" value="Rename"/>	URL: http://172.22.2.193/FMout/cff950fd-ec88-408a-bcf-73d2ba2a32c8.f4m			
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Disabled	Disabled
	<input type="button" value="Rename"/>	URL: http://172.22.2.193/FMout/df80fb6-8719-494d-bf89-5f43d5ac97fa.f4m			
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Disabled	Disabled
	<input type="button" value="Rename"/>	URL: http://172.22.2.193/FMout/74682c80-10cd-405e-80bb-621a2a910ae9.f4m			
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	Disabled	Disabled
	<input type="button" value="Rename"/>	URL: http://172.22.2.193/FMout/f42ef900-9f08-4025-ae59-239785205465.f4m			

Field	Description
Multicast TTL	Multicast streams are passed from router to router until a request is serviced. This approach propagates the stream across organization WANs. The Multicast TTL is a counter used to better control the number of "hops" or passes between routers. Each router, unless configured differently, decrements the multicast TTL (in the header) as it is passed along. Once the TTL is zero, the packet is dropped. DME's recommended default value is 63 – adjust as necessary to your needs and network configuration.
Stream Name	Name of internal stream (to this DME) selected to be converted to multicast.
Multicast Destination IP/ Address:Name	The multicast destination IP address. This is an IP address in the multicast address space of 224.0.0.0 - 239.255.255.255. Note: Please coordinate with local IT department and honor reserved addresses.
Port	The port of the destination multicast. DME defaults to 4444. There is no need to change this unless recommended by your IT department.
Enable	Use dropdown to enable or disable the stream. All streams are disabled by default.
Status	Read only: Disabled   Streaming   Waiting for Stream (Input source <stream_name> not yet available.)

Field	Description
Rename Button	Rename the manifest URL. Each Flash Multicast stream has a unique URL. This can be integrated with Rev or other players. These streams may be left up for extended periods of time. Clicking this button will irrevocably change that URL when security is a concern.

Some Customers have reported video artifacts on larger than 1M streams using RTMFP (Flash Multicast) on Windows 7 with Chrome. These issues are ONLY seen in Chrome on Windows 7. The artifacts arise from the stream overrunning the default (8K) OS system default buffer sizes on the viewers PCs. Larger streams exhibit more video artifacts by overrunning the buffer faster.

Investigations around expanding the default Windows 7 buffer size have shown that the following settings will help alleviate the issue. However, this setting must be applied on a per-machine basis and requires editing the Windows registry. If you are not familiar with registry edits, please consult your IT department.

Create or modify the registry DWORD parameter as follows:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\AFD\Parameters\DefaultReceiveWindow**

**Set to decimal 196724**

This setting will change the default receive window size for all application running on the PC. Some applications will override this setting [within their code]. You may wish, depending on your environment and the sizes of your multicast streams, to select a different size other than the one illustrated above. For example, the default setting is 8K (8192) and the above example is 192K – you may wish to test 16K, 64K, or some other value. Higher values come at the expense of increased system resource usage.

These settings are ONLY for Windows 7 (any version) for Chrome viewers of Flash Multicast. If this is not your target player environment, please do not attempt the changes.

Also, always be sure to test this in your environment before deploying.

## Assigning a Multicast Address

Many factors must be considered when designing a multicast address infrastructure since Ethernet switch implementations can significantly vary between vendors. Furthermore, multicast addressing techniques rely on an Ethernet to IP Address mapping rule, which does not guarantee a unique physical address. In fact, it is possible to create multicast addresses that differ from an IP perspective, but overlap when presented to the Ethernet network. Addresses created in this situation can cause significant network and operational problems.

Specifically, multiple IP Addresses are mapped into the same physical layer address. For example, all IP multicast addresses with the same or differing first octet, and the second octet differing by exactly 128, map to the same physical address (226.5.5.4, 227.5.5.4, and 228.133.5.4 all map to the same physical address).

Another factor to keep in mind when assigning multicast addresses is that 224.x.x.x is a range containing reserved addresses, particularly in the range 224.0.0.x. For example, 224.0.0.1 is the 'all hosts' multicast address and 224.0.0.2 is the 'all routers' reserved address. Other 224.0.0.X numbers are reserved for RIP, OSPF, DVMRP, etc. Here are some recommended rules for multicast IP Address assignment:

1. Do not use 224 in the first octet since many of these are reserved. (Vbrick encoders enforce this rule.)
2. Use a digit between (225–239) for the first octet and standardize on it for each network.
3. In the second octet, either use numbers from 1–127, or 129–255, do not mix ranges on a given network.

## Vbrick Multicast

Vbrick Multicast is a Rev + DME feature that provides plugin-less multicast to Vbrick's Rev player. Browsers are adopting ever increasing security protocols and sand-boxing of running code – these are all good improvements for the security of our environments. Browsers cannot natively receive UDP packets that multicast would utilize. Therefore, Vbrick has developed a PC and Mac multicast agent that can be silently installed by corporate IT departments. Please refer to Vbrick Rev and Vbrick Multicast [documentation](#) (under Rev Documentation section) to get the agent and deploy it. Computers with this agent will, in accordance to settings on Rev, receive Vbrick Multicast.

All configuration of Vbrick Multicast is performed in Rev. You may still enable and disable on the DME, but please centralize all control within Rev.

This is a different form of multicast that should not be confused with Flash Multicast which is no longer supported.

▼ To access the Vbrick Multicast fields:

1. Navigate to **Output Configuration > Vbrick Multicast**.

Use this page to view Vbrick Multicast streams that have been created in Rev and that have been pushed to the DME from Rev. Most values that are viewed here are pulled from Rev.

Output Configuration --> vbrick Multicast

Vbrick Multicast TTL:

Index	Stream Specifications
1 +	<p>Details for this line item. Click plus or document icon to hide.</p> <p>Input Stream:</p> <p><input type="checkbox"/> Enabled DISABLED</p> <p>Multicast IP Address/Name:</p> <p>Multicast Port: 4096</p> <p>Packet Size: 4096</p>
2 +	<p><input type="checkbox"/> Enabled :: DISABLED :: Click plus or document icon for more details on this line item.</p> <p>Multicast IP Address/Name:</p>
3 +	<p>Details for this line item. Click plus or document icon to hide.</p> <p>Input Stream: recordingStream</p> <p><input type="checkbox"/> Enabled DISABLED</p> <p>Multicast IP Address/Name: 239.22.195.158</p> <p>Multicast Port: 4444</p> <p>Packet Size: 8192</p>
4 +	<p>Details for this line item. Click plus or document icon to hide.</p> <p>Input Stream: vhtest1</p> <p><input checked="" type="checkbox"/> Enabled WAITING FOR STREAM</p> <p>Multicast IP Address/Name: 230.12.34.54</p> <p>Multicast Port: 4567</p> <p>Packet Size: 4096</p>

Field	Description
Vbrick Multicast TTL	Multicast streams are passed from router to router until a request is serviced. This approach propagates the stream across organization WANs. The Multicast TTL is a counter used to better control the number of "hops" or passes between routers. Each router, unless configured differently, decrements the multicast TTL (in the header) as it is passed along. Once the TTL is zero, the packet is dropped. DME's recommended default value is 63 – adjust as necessary to your needs and network configuration.
Enabled	Select to enable or disable a stream. Default is disabled.
Input Stream	This is the name of the stream (available on the DME) specified within the Rev interface to utilize Vbrick Multicast.
Multicast IP Address/Name	This is the destination IP of the multicast address as specified within the Rev interface. This is an IP address in the multicast address space of 224.0.0.0 - 239.255.255.255. Note: Please coordinate with local IT department and honor reserved addresses.
Multicast Port	This is the UDP destination PORT of the multicast as specified within the Rev interface. This value does not need to be unique and in most cases the default port number 4444 will be fine for all multicast streams on your network. In rare cases your IT department may require use of a specific port.
Packet Size	This is the packet size as specified within the Rev interface.

## RTSP Push

▼ To access the RTSP Push fields:

1. Navigate to **Output Configuration > RTSP Push**.

Use this page to configure streams that will be pushed to a destination device using Auto Unicast RTP. Possible destinations include servers such as Darwin, Wowza, another DME or a CDN. The number of configurable streams is dependent on the model of the DME.

Index	Stream Name	Target Name	Destination IP Addr:Name:Port	User Name	Password	Enable	Status
1	PullStream1	test.sdp	127.0.0.1	broadcast	*****	Enabled	Not Found
2	PullStream4					Disabled	Disabled
3						Disabled	Disabled
4						Disabled	Disabled
5						Disabled	Disabled
6						Disabled	Disabled
7						Disabled	Disabled
8						Disabled	Disabled
9						Disabled	Disabled
10						Disabled	Disabled
11						Disabled	Disabled
12						Disabled	Disabled
13						Disabled	Disabled
14						Disabled	Disabled
15						Disabled	Disabled
16						Disabled	Disabled
17						Disabled	Disabled
18						Disabled	Disabled
19						Disabled	Disabled
20						Disabled	Disabled
21						Disabled	Disabled
22						Disabled	Disabled
23						Disabled	Disabled
24						Disabled	Disabled
25						Disabled	Disabled

Field	Description
Stream Name	Name identified on the Multi Protocol input for this stream.
Target Name	Sets the stream name on the destination. The Target Name has the format <TargetStreamName>.sdp. When pushing to another DME it is generally most straightforward to reuse the Stream Name as the Target Name.
Destination IP/Address:Port	Enter the destination IP address. Override the Port if not using the default (554).
User Name	Required if client-side authentication is required by the destination server.
Password	Required if client-side authentication is required by the destination server.
Enable	Default - Disabled - Enables the push.
Status	Read only: Disabled   Streaming   Waiting for Stream (Input source <stream_name> not yet available.)

## Transport Stream Out

- ▼ To access the Transport Stream Out fields:

Navigate to **Output Configuration > Transport Stream Out**.

Output Configuration --> Transport Stream Out

Multicast TTL:

Index	Stream Name	Multicast/Destination IP Addr/Name	Port	Announce Name(o)	Enable	Status
1	PullStream2	239.45.75.75	4466	AndyTest5	Enabled	NotFound
2	PullStream1	239.45.75.175	4468	AndyTest6	Enabled	NotFound
3	PullStream3	239.25.75.175	4470		Enabled	NotFound
4					Disabled	Disabled
5					Disabled	Disabled
6					Disabled	Disabled
7					Disabled	Disabled
8					Disabled	Disabled
9					Disabled	Disabled
10					Disabled	Disabled
11					Disabled	Disabled
12					Disabled	Disabled
13					Disabled	Disabled
14					Disabled	Disabled
15					Disabled	Disabled
16					Disabled	Disabled
17					Disabled	Disabled
18					Disabled	Disabled
19					Disabled	Disabled
20					Disabled	Disabled
21					Disabled	Disabled
22					Disabled	Disabled
23					Disabled	Disabled
24					Disabled	Disabled
25					Disabled	Disabled

Apply Revert Default

Field	Description
Multicast TTL	Multicast streams are passed from router to router until a request is serviced. This approach propagates the stream across organization WANs. The Multicast TTL is a counter used to better control the number of "hops" or passes between routers. Each router, unless configured differently, decrements the multicast TTL (in the header) as it is passed along. Once the TTL is zero, the packet is dropped. DME's recommended default value is 63 – adjust as necessary to your needs and network configuration.
Stream Name	The input stream name you will be sending out as a transport stream. Note: For MPEG-2 content, the Stream Name must be preceded with "mp2:" See <a href="#">MPG2TS Streams</a> for more information.
Multicast/ Destination IP/ Address	If multicast output, the multicast address of the output stream, If unicast, the destination IP address.
Port	The port number you will be sending the stream to.
Announce Name	(optional) If multicast, the program name to be included in the SAP for this stream. If not filled in, Stream Name is used.
Enable	Enable or disable the output transport stream.

Field	Description
Status	Disabled   Waiting for Stream   Streaming

## HLS Streaming

Use this page to specify HLS streams. Each **Index** will create one HLS master stream with one or more sub-streams contained within. Adding multiple **Input Streams** will create an MBR (Multi bitrate HLS) – which, when played, will tune to the correct stream based on current network conditions of the player.

▼ To access the HLS Streaming fields:

1. Navigate to **Output Configuration > HLS Streaming**.

Field	Description
Unique Playlist Name	<p>The Unique Playlist Name (UPN) is used in the definition of the HLS storage structure and URL. The UPN <i>must</i> be unique and not match any other stream name or playlist name – across <i>all</i> DMEs. Please restrict names to unique (across account) text without spaces using only lowercase “a-z”, “0-9”, “-” or “_”. Utilizing the same UPN on different DMEs will corrupt sharing across the DME mesh.</p> <p>The UPN is used to group 1 to 4 streams (renditions) into a single HLS specification referenced by a single URL. In this way, multiple bitrates (MBR) can be provided and the Vbrick Rev HTML5 HLS Player will adapt (ABR) and pull the correct bitrate rendition for best viewing experience with respect to local networking conditions. This is a very common approach to distributing video content across very different network situations.</p> <p><b>Note:</b> Changing this value will disassociate automatic Akamai distribution (if configured for this stream on Rev).</p>
Announce Name	<p>(optional) The program name to be included in the SAP for this stream. Please restrict names to text without spaces using only “A-Z”, “a-z”, “0-9”, “-” or “_”. If not filled in, Stream Name is used. This is used with VEMS, but not used in Rev.</p>

Field	Description
Input Streams	<p>Use this area to define 1 to 4 input streams. Selecting more than one stream will combine them into a MBR HLS under the UPN.</p> <p>Each Active stream is selectable and be displayed in the stream dropdown. The stream bitrate is also displayed. Use the bitrate as a guide and select the highest bitrate rendition first (i.e, within index 1). The HLS player will play the first stream first (before any bandwidth testing or negotiation between renditions.) While an HLS may have only 1 stream, typically they have more than one in order to take advantage of ABR playback.</p> <p>Each stream has an associated bitrate field, which defaults to “Auto”. This value is used within the HLS playlist as the reported bitrate of the stream. In most cases, the default option of Auto is recommended. However, entering a value (with Kbps units) into that field will override the measured bitrate and included that within the HLS playlist.</p> <p>When active, each sub-stream is created (as HLS) and displayed in the <b>Monitor and Logs &gt; MPS Connections</b> page. There will also be the master playlist which is used as the HLS MBR stream.</p> <p><b>Note:</b> When HLS streams are configured in Rev (on the <b>DME Management</b> page, <b>Create URLs</b> tab) they are named (UPN) as <b>rev_&lt;StreamName defined on Rev&gt;</b>. Do not change this name, and also, do not change the first (index 1) stream within the <b>Input Streams</b>. Changing the UPN or value for the first (index 1) input stream will disassociate automatic CDN (Akamai) distribution (if configured for this stream on Rev.) Values in the 2nd through 4th can be changed/add and will be pushed with any specified Akamai distribution. As a reminder, live Akamai distribution is tied to Vbrick Webcasts.</p>
HLS Type	<p>The number of video segments in a playlist is defined by the Playlist Length. This field determines how the DME will handle the generated segments:</p> <ul style="list-style-type: none"> <li>• Rolling – the playlist will have a fixed length regardless of the number of HLS segments generated. Segments will be added or deleted to maintain a fixed playlist length.</li> <li>• Appending – the Playlist Length is ignored and the DME creates a continuously growing playlist. The maximum playlist duration is seven days.</li> </ul> <p>Note 1: Multiple appending playlists may use a large amount of disk space unnecessarily. Use this option only if you will need to return to the beginning of the playlist.</p> <p>Note 2: The entire playlist will be deleted if you "disable" HLS generation (on the "HLS Streaming" page). When the stream is active, the playlists and associated segments can be extracted via FTP.</p>



Field	Description
Playlist Length	The number of segments to include in a playlist. Default = 10. This value is used to enable scroll back in the client player. You can scroll back up to the number of segments specified here. Be aware that this function uses disk space for segments that may never be viewed.
Seconds per Segment	<p>The number of seconds for which a media segment is created. Range 1–600. Default = 8. By increasing this number you will increase the initial time it takes to play the HLS stream. Since a separate HTTP access is required for each segment, Performance is optimized by keeping this number larger. Since a separate HTTP access is required for each segment, performance is improved by keeping this number larger. For best results, this number should always be a multiple of the IDR Frame Interval on the encoder. For example, if the IDR Frame Interval is 4, this value should be 8, 12, 16 and so forth.</p> <p>Latency Tuning for HLS/HDS</p> <p>Latency is a common concern when delivering live content across HLS or HDS. Latency can be tuned up or down and will impact server load.</p> <p>The Minimum Segment Length (MSL) field, as defined above, has a big impact on latency. The system needs 3 segments to build a playlist (even if the playlist length is greater than 3). Once that playlist is created, players can retrieve it and begin playing. Therefore, with the current default of an 8 second segment length, it takes 24 seconds before a playlist is created. This introduces 24 seconds of latency. Lowering the MSL reduces latency by reducing the time to generate the playlist; however, it creates a larger resource need on the server. Smaller segments mean an increased number of HTTP requests from players for more segments and playlists. It is also important to reiterate, as noted above, if you reduce your MSL to make sure that it is a multiple of the IDR Frame Interval from the encoder.</p>
Automatic Detection	Automatic Detection will evaluate the stream and provide optimized Segment Size. For example, if you set your encode to have 2 seconds between keyframes (note: this is the recommended setting), then by selecting this option the DME will automatically create optimized HLS segments and reduce the HLS introduced latency.
Enable	Enable or disable the stream. Note that if HLS is streaming and is then disabled, it may take several minutes for HLS to mark that input stream as disconnected / not found.
Status	Disabled   Waiting   Active
URL	This will display the URL for the master playlist. Use this URL for testing and/or distributing to viewers.

Field	Description
CDN Distribution	<p>This field provides information on CDN distribution. In most cases, you will be directed back to Rev for the CDN configuration within the DME Management page.</p> <p>Note: Do not edit the name and or first sub-stream for a stream created on Rev. The stream will need to be recreated on Rev to reestablish Akamai distribution.</p> <p>Additional sub-streams (numbered 2-4) can be added to each index to provide MBR. Once the stream is set up in Rev and communicated to DME, Administrators can come to this page, locate the appropriate HLS stream and add addition input streams to create an MBR.</p>

### Playlist Conventions

When generating HLS streams it is important to understand the conventions used for creating playlists so they can be played via an HTTP URL.

To Play:	iOS Viewing URL
Individual streams that are part of a master playlist:	<code>http://&lt;dme_ip_address&gt;/&lt;master_playlist_name&gt;/&lt;stream_name&gt;/playlist.m3u8</code>
Individual streams that are <u>not</u> part of a master playlist:	<code>http://&lt;dme_ip_address&gt;/HLS/&lt;stream_name&gt;/playlist.m3u8</code>
All streams in a master playlist:	<code>http://&lt;dme_ip_address&gt;/&lt;master_playlist_name&gt;/playlist.m3u8</code>

## HDS Streaming

▼ To access the HDS Streaming fields:

1. Navigate to **Output Configuration > HDS Streaming**.

HDS (Adobe MPEG-4 based HTTP adaptive file streaming protocol) is an HTTP-based media streaming protocol implemented by Adobe. It works by breaking the overall stream into a sequence of small HTTP-based downloads, each download loading one short chunk of a video stream. As the stream is played, the client can select from a number of different alternate streams containing the same material encoded at a variety of data rates, allowing the streaming session to adapt to the available data rate. At the start of the streaming session, it downloads an extended f4m playlist containing the metadata for the various substreams which are available. Since its requests use only standard HTTP transactions, HDS is capable of traversing any firewall or proxy server that allows standard HTTP traffic, unlike UDP-based protocols such as RTP.

Output Configuration --> HDS Streaming 2

Index	Stream Name	Master Playlist Name	Announce Name(o)	Bandwidth Override	Type	Playlist Length	Minimum Segment Length	Enable	Status
1	PullStream3	vcHDS			Rolling	10	8	Enabled	NotFound
2					Rolling	10	8	Disabled	Disabled
3					Rolling	10	8	Disabled	Disabled
4					Rolling	10	8	Disabled	Disabled
5					Rolling	10	8	Disabled	Disabled
6					Rolling	10	8	Disabled	Disabled
7					Rolling	10	8	Disabled	Disabled
8					Rolling	10	8	Disabled	Disabled
9					Rolling	10	8	Disabled	Disabled
10					Rolling	10	8	Disabled	Disabled
11					Rolling	10	8	Disabled	Disabled
12					Rolling	10	8	Disabled	Disabled
13					Rolling	10	8	Disabled	Disabled
14					Rolling	10	8	Disabled	Disabled
15					Rolling	10	8	Disabled	Disabled
16					Rolling	10	8	Disabled	Disabled
17					Rolling	10	8	Disabled	Disabled
18					Rolling	10	8	Disabled	Disabled
19					Rolling	10	8	Disabled	Disabled
20					Rolling	10	8	Disabled	Disabled
21					Rolling	10	8	Disabled	Disabled
22					Rolling	10	8	Disabled	Disabled
23					Rolling	10	8	Disabled	Disabled
24					Rolling	10	8	Disabled	Disabled
25					Rolling	10	8	Disabled	Disabled

Apply Revert Default

Field	Description
Stream Name	Input stream used to generate HLS content.
Master Playlist Name	<p>If the stream will be part of a group of alternate streams identified by a master playlist, enter the master playlist name. A group may consist of multiple streams with different bit rates and the HDS player will switch between available streams to provide the best viewing experience.</p> <p>When using this page to create a group, <i>you must put the highest bit rate stream first</i> (at the top of the list). This is the first stream the client will try to play. You will typically have more than one HLS stream referencing the same Master Playlist Name. If this stream is not part of a master playlist, leave this field blank.</p>
Announcement Name	(optional) The program name to be included in the SAP for this stream. If not filled in, Stream Name is used.
Bandwidth Override	Master Playlists for multiple bit rate streams require the bandwidth of each individual stream to be included in the Master Playlist. For example, if the stream is sourced from a Vbrick H.264 encoder, the DME will detect the bandwidth associated with each multiple bit rate stream. For non-Vbrick encoders, enter the bandwidth value (in Kbps) associated with the stream. In general, use this field only if the encoder does not supply a bandwidth value. <i>Be aware that if used, this value will override the encoder-supplied value.</i>

Field	Description
Type	<p>The number of video segments in a playlist is defined by the Playlist Length. This field determines how the DME will handle the generated segments:</p> <ul style="list-style-type: none"> <li>• Rolling – the playlist will have a fixed length regardless of the number of HDS segments generated. Segments will be added or deleted to maintain a fixed playlist length.</li> <li>• Appending – the Playlist Length is ignored and the DME creates a continuously growing playlist. The maximum playlist duration is seven days.</li> </ul> <p><u>Note 1:</u> Multiple appending playlists may use a large amount of disk space unnecessarily. Use this option only if you will need to return to the beginning of the playlist.</p> <p><u>Note 2:</u> The entire playlist will be deleted if you "disable" HDS generation (on the <a href="#">HDS Streaming</a> page). When the stream is active, the playlists and associated segments can be extracted via FTP.</p>
Playlist Length	<p>The number of segments to include in a playlist. Default = 10. This value is used to enable scroll back in the client player. You can scroll back up to the number of segments specified here. <i>Be aware that this function uses disk space for segments that may never be viewed.</i></p>
Minimum Segment Length	<p>The number of seconds for which a media segment is created. Range 1–60. Default = 8. By increasing this number you will also increase the initial time it takes to play the HLS stream. For best results, this number should always be a multiple of the IDR Frame Interval on the encoder. For example, if the IDR Frame Interval is 4, this value should be 8, 12, 16 and so forth.</p> <p>Latency Tuning for HLS/HDS</p> <p>Latency is a common concern when delivering live content across HLS or HDS. Latency can be tuned up or down and will impact server load.</p> <p>The Minimum Segment Length (MSL) field, as defined above, has a big impact on latency. The system needs 3 segments to build a playlist (even if the playlist length is greater than 3). Once that playlist is created, players can retrieve it and begin playing. Therefore, with the current default of an 8 second segment length, it takes 24 seconds before a playlist is created. This introduces 24 seconds of latency. Lowering the MSL reduces latency by reducing the time to generate the playlist; however, it creates a larger resource need on the server. Smaller segments mean an increased number of HTTP requests from players for more segments and playlists. It is also important to reiterate, as noted above, if you reduce your MSL to make sure that it is a multiple of the IDR Frame Interval from the encoder.</p>
Enable	Enable or disable the stream.
Status	Disabled   Waiting   Active.

## Playlist Conventions

When generating HLS streams it is important to understand the conventions used for creating playlists so they can be played via an HTTP URL.

To Play:	iOS Viewing URL
Individual streams that are <u>not</u> part of a master playlist:	<code>http://&lt;dme_ip_address&gt;/HDS/&lt;stream_name&gt;/playlist.f4m</code>
All streams in a master playlist:	<code>http://&lt;dme_ip_address&gt;/HDS/&lt;master_playlist_name&gt;/playlist.f4m</code>

## RTP Relay Overview

▼ To access the RTP Relay functionality:

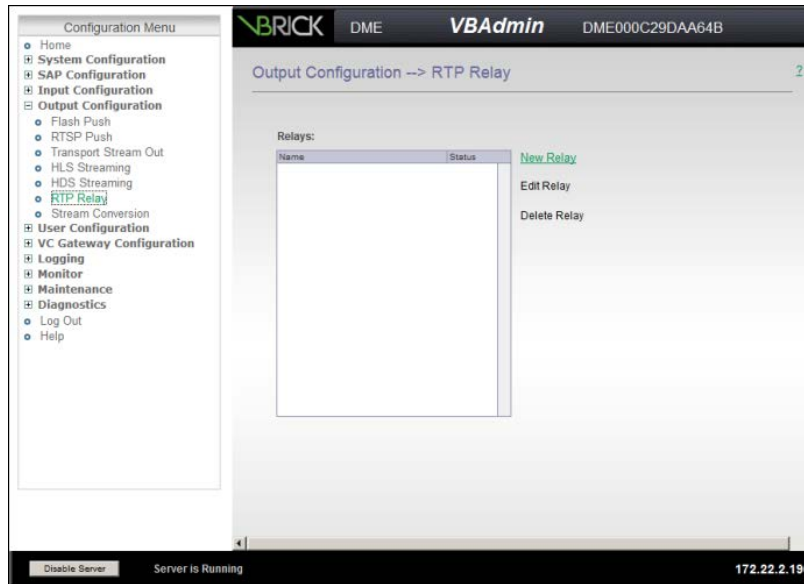
1. Navigate to **Output Configuration > RTP Relay**.

Use this page to configure or edit relays. A streaming RTP relay forwards an RTP stream from a source to either a multicast or multiple unicast destinations. One of the primary functions of a relay is to minimize the usage of network bandwidth across limited bandwidth WAN links by receiving an single incoming stream and outputting either a multicast stream or serving multiple unicast streams.

**Note:** Each relay must have a unique source. A single source may have multiple destinations.

Relays can also be used to distribute the load across multiple servers. The incoming stream can be provided to multiple destination servers and then redistributed to clients. Possible destination servers, include QuickTime, Darwin, or another DME. There are a number of methods for receiving an incoming stream. The most common is to receive an incoming stream into the Multi Protocol Server and then push the stream to the RTP Server (Out-10). It is also possible to receive a Push directly into the RTP server (In-3) or to receive an unannounced unicast or multicast. In this scenario you will need to manually place the multicast/unicast .sdp file from the source on the destination server.

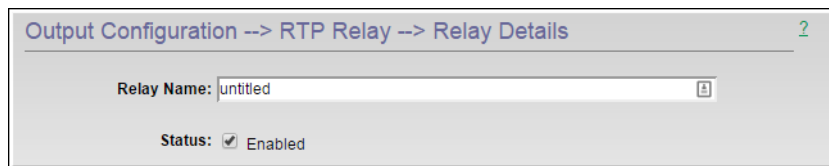
**Note:** If a stream which is present on the RTP server is to be used as source for any output from the Multi Protocol server, an RTSP/RTP Pull must be configured on the Multi Protocol server.



Field/Hyperlink	Description
Relays	Shows all defined relays.
New Relay	Creates a new relay.
Edit Relay	Edit the selected relay.
Delete Relay	Delete the selected relay.

### Create or Edit an RTP Relay

- ▼ To create or edit an RTP Relay:
  1. Navigate to **Output Configuration > RTP Relay**.
  2. Click **New Relay** to create a new relay or the relay name and then **Edit Relay** to modify an existing relay. Complete the fields described below as required.



Field	Description
Relay Name	Enter a unique relay name.
Status	Check to enable. Remember to click <b>Apply</b> before you exit the page.

### Source Settings

These settings describe the source of the stream to be relayed. It can be sourced internally from the DME (127.0.0.1) or it can be fetched from elsewhere. You can also wait for it to be announced. The dominant use case is to source the stream internally from the DME.

**Source Settings**

Source Hostname or IP Address:

Mount Point:

Request incoming stream

User Name:

Password:

Wait for announced stream(s)

Field	Description
Source Hostname or IP Address	Hostname or IP address of the source server. Commonly this is 127.0.0.1. This is set to an external address only if a stream is being requested from an external server via RTSP/RTP. Normally RTSP/RTP requests originate at the Multi Protocol Server (In-6). Each relay must use a unique source. Each unique source may then have multiple destinations.
Mount Point	SDP file name.
Request incoming stream	For all normal use cases, this option is selected. Check to request a stream from another DME or server.
User Name	(optional) Name used for authentication on source server. Used only in the uncommon case of a stream requested from an external server via RTSP/RTP.
Password	(optional) Name used for authentication on source server. Used only in the uncommon case of a stream requested from an external server via RTSP/RTP.
Wait for announced stream(s)	Check to wait for an announced stream from the specified hostname or IP address. This is an uncommon case.

## Destination Settings

**Destination Settings (1 of 1)**

Hostname or IP Address:

Announced UDP

Mount Point:

User Name:

Password:

Unannounced UDP

Base Port:

Output SDP file:

TTL:

[Remove Destination](#)

---

[Add Destination](#)

Field	Description
Hostname or IP Address	Hostname or IP address of the destination server. Each unique source created may have multiple destinations.
Announced UDP	Use when relaying a stream to another DME or server via auto unicast. <ul style="list-style-type: none"> <li>• User Name – Name used for push authentication to destination server.</li> <li>• Password – Password used for push authentication to destination server.</li> </ul>
Unannounced UDP	Use when pushing the stream to another DME or server and publishing the associated .sdp file. Although this option can be used for either multicast to clients and servers or unicast to a specific server, the dominant case is multicast. <ul style="list-style-type: none"> <li>• Base Port – The base port will be incremented by 2 for each RTP stream. In most common cases, there are two RTP streams (audio and video) so 4 ports are required for the relay. The ports must be unique on the destination device for unicast or on the multicast IP.</li> <li>• Output SDP file – Auto-generates an .sdp file using the <b>Output SDP file</b> name and including the destination information.</li> <li>• Multicast TTL – For unicast, the number of hops (between routers) for which an IP packet is valid in the network. For multicast defines the distribution scope of the stream. Range = 1–255.</li> </ul>
Add   Remove Destination	A relay can send the stream to multiple destinations. Use this button to add or remove a configured destination.

## Stream on Demand

The DME’s **Stream on Demand** feature enables you to set up VOD or Live video streams only when requested. This saves organizational bandwidth by not requiring networks to backhaul video streams in the event they “may” be needed and only streams video sources when they are actually requested.

This feature utilizes files, with the extension .vod, to contain the actual URI of the video source.

That source can be either a live stream or a VOD file.

The **Stream on Demand** interface within the DME will allow the creation and management of .vod files. It is important that the file names are unique across all DMEs, and the UI will enforce unique file names by assigning GUIDs (globally unique IDs) when the file is created and will also require an additional action to Rescan the folder within the UI. All of these files are stored on the DME within the ftp root within the StreamOnDemand folder. Users can add content via FTP, but should be aware of the restrictions on the file names (they must be unique across DMEs).

▼ To access the Stream on Demand files:

1. Navigate to **Output Configuration > Stream on Demand**.



Output Configuration --> Stream on Demand

Stream on Demand files have ".vod" extensions. This page supports creating and editing ".vod" files.  
Navigation key: is a VOD File, and is a Streaming VOD File

Rescan **Please select your Stream on Demand (VOD) file:**

- StreamOnDemand/
  - StreamOnDemand/EU/
  - StreamOnDemand/NorthAmerica/

**We will autogenerate your filename. Please select a containing (parent) directory and enter the file contents.**

Containing Directory: StreamOnDemand/NorthAmerica/

New Filename: 004c071c-e324-4ff4-93e1-d6272baea492.vod

URL: rtmp://172.22.2.193:1935/vod/004c071c-e324-4ff4-93e1-d6272baea492.vod

uri=rtmp://172.22.2.193/vod/mp4:UploadedVideos/test.mp4

e.g., uri=rtmp://10.10.1.1/live/vbStream  
uri=rtmp://10.10.1.1/vod/mp4:UploadedVideos/exampleFile.mp4

Button	Description
Add Folder	Adds a new folder to your StreamOnDemand directory within your DME. Selecting this button will display the add folder interface at the bottom of the form where you can define the name and location of the directory. Adding a new folder will automatically restart the streaming server.
Add File	Adds a new .vod file. Selecting this button displays the add file interface at the bottom of the form (seen in the example image). The UI will automatically create a file name but will allow you to select the containing directory. Enter the URI of the stream in the text field and hit <b>Save</b> .
Refresh	When you add or remove folders or files, you will need to refresh the directory listing. Click this button to refresh the Stream on Demand interface
Rescan	Different from refresh; If you add or remove directories via FTP within the StreamOnDemand folder, you need to Rescan. You only need to rescan once after your changes.
Edit File	Clicking on a .vod file name will allow you to edit the file. You can change the URI only or delete the file.
Edit Folder	Clicking on a folder name will allow you to delete the folder. Refresh to see the deletion.

### Advanced StreamOnDemand Configurations

Additionally, this feature can be utilized to access geographically remote streams while minimizing bandwidth. In this case, DMEs can cascade the .vod file requests from DME to DME. Doing this will automatically create a stream from one DME through a sequence of hopped DMEs to the source while minimizing bandwidth.

---

As an example, consider an implementation that might include DME-1 with a .vod file that points to a .vod file on DME-2. DME-2, in turn, within the .vod file could point to a stream on DME-3. In this manner, a request to DME-1 will auto generate all the necessary linkages to connect to the stream provided by DME-3 (connecting through DME-2). This is useful because only one stream returns to DME-1, and anyone attaching to view the stream on DME-2 does not create another stream from DME-3. So, in all cases of viewing from DME-2 there would be only 1 stream from DME-3. Likewise, in viewing from DME-1 only creates one stream to DME-2 and one stream from DME-2 to DME-3. All the streams are viewable on each of the DMEs while minimizing the bandwidth.

Finally, all the streams are automatically dropped when all viewers disconnect.

## Stream Conversion

▼ To access the Stream Conversion fields:

1. Navigate to **Output Configuration > Stream Conversion**.

The **Stream Conversion** page provides a generalized transrating capability which allows modification of live streams in a number of ways. Here, you can transrate a stream to a lower bitrate, a different resolution, etc. The conversion process does not modify the resolution of the incoming stream, but creates a new stream that can be used/viewed.

To help illustrate the use of this feature, here are a couple of use cases:

1. Locally creating an adaptive bitrate stream. Consider a remote DME that has limited bandwidth. It may be necessary to push/pull a single higher bitrate stream to that DME, and then transrate it to a number of reduced bitrate/resolution streams. Then, within the HLS Streaming page, they can be combined into a single stream for adaptive playback reflecting the unique needs of the remote viewers.
2. Create a Mobile sized Resolution and Bitrate stream. The DME can, if needed, take a stream and using this feature reduce the bitrate and resolution to be better provisioned to smaller form-factor mobile players.

**Important Usage Note.** This feature provides multiple levels of customization for stream size, resolution, and bitrate. However, software-based transrating features often require a great deal of CPU support depending on the complexity of the transrating. For example, with Vbrick's internal benchmarks and using multiple, representative streams with the "HDTV 1080 – High Motion" predefined profile, it was found that, depending on your DME model, the CPU was impacted differently (e.g., on a DME 7530 there was 80-100% CPU utilization, while the 7550 saw 45-70% peaking to 90, and the 7570 a 6-9% utilization). This profile requires a great deal of processing. Looking at the opposite end, using the "Small Form Factor" profile, a 10-30%, 6-10% and negligible utilization for DMEs 7530, 7550, and 7570 respectively, are observed. Please keep in mind that these impacts are additive based on the number of transrates the DME is performing. These examples are provided to illustrate the differences in CPU impacts and the necessity for end-user qualification and testing.

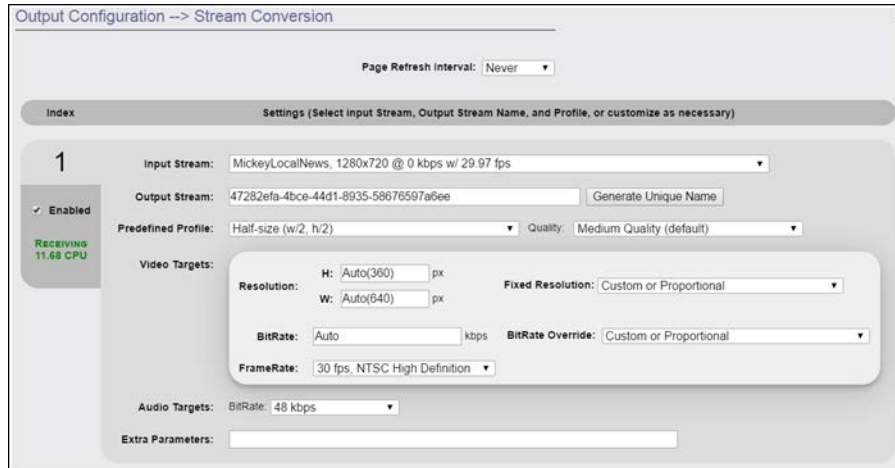
Therefore, when using this feature please use a representative stream(s) (i.e, resolution, bitrate, framerate, motion) to (1) test the quality of the transrated output, (2) monitor the CPU usage because high usage will have an impact on the DME performance, and lastly (3) perform multiple conversions to create a representative computational load mirroring how you will use the DME in production.

To use this feature, first select an input stream. An output stream will be automatically named, but if you rename it – the name must be unique, and best to be unique across all of

your DMEs. Then select a **Predefined Profile**. At this point you can enable it, or you can further define characteristics within the **Video Target** area. When complete, you can enable it.

- **Best Practice.** If possible, based on available bandwidth, it is better to use purpose built devices (e.g., our family of 9000 encoders) to create the multiple bitrate necessary for adaptive playback. Then, use the DME to combine and serve the streams.
- **Best Practice.** The act of transrating will always reduced the amount of "data" or quality of the stream. While it is possible to upscale videos, that cannot ever add "data" but can interpolate between existing data. If possible, start a transrate with a data stream larger (resolution/bitrate) than the resulting stream.
- **Best Practice.** Test. Test. Test. Always pretest your source and any associated transrated streams. Different sources can impart different characteristics within the stream which may influence (good or bad) the transrate. If you have tested enough, test one more time

**Note:** DMEs 7550 and 7570 come standard with the **Stream Conversion** feature. If you are on a DME 7530 and have licensed and activated the Stream Conversion separately, it is critical that you monitor the CPU usage of this feature. For more information see [Activate Feature](#).



Field	Description
Enabled	Select to enable or disable the conversion. Disabled by default.
Input Stream	Name of the Vbrick pre-configured source streams you may select from the dropdown list. Each stream, along with a Vbrick Predefined Profile, will contain the recommended Video Target settings. You may overwrite these settings if desired.
Output Stream	The stream name for the converted output stream. This name must be unique across all DMEs in your ecosystem. The default GUID name is automatically assigned but you may overwrite. If you overwrite this field, it is advised that you use the <b>Generate Unique Name</b> button to ensure you retain a unique name for the output stream.

Field	Description
Predefined Profile	<p>Name of the Vbrick pre-configured proportional profiles you may select from the dropdown list based on the Input Stream you have selected. Each profile, along with an Input Stream selected above, will define the recommended Video Target settings including bit rate, resolution, and frame rate.</p> <p>In the image above for example, the Input Stream is defined at 1280x720 resolution while the profile specifies a half-size. As a result, the final resolution in Video Target settings is defined as 640x360.</p> <p>You may also select common stream and common television profiles. You may overwrite these settings if desired.</p> <p>Note: You should not change the Framerate if you have closed captioning.</p>
Quality	<p>Medium = default. Set to Extreme, High, Medium, or Low. Higher and Extreme quality settings have higher bit rates and will require more processing.</p>
Video Targets	<p>Sets the video, audio, and resolution parameters for the output stream based on the Input Stream and Predefined Profile you select.</p>
Extra Parm	<p>The DME currently uses the ffmpeg library for doing stream conversions. Use this field to enter specific parameters to ffmpeg for your streams.</p> <p>For a library of possible conversion options please visit <a href="https://ffmpeg.org/ffmpeg.html">https://ffmpeg.org/ffmpeg.html</a>. This is an advanced feature, so use additional options with care. They will override the selected template in the Conversion Type. As such, not all possible combinations are tested or supported by Vbrick. Also, if not used properly they can adversely affect DME performance as this is a CPU intensive feature.</p>

**Note:** When working with streams with closed captions, do not change the framerate. You can still change the resolution and bitrate, but changing the framerate will have adverse effects on CC data. In these cases, please keep framerate set to **Current Rate**.

## Rev Initiated Multicast and Reflection

### Automatic Multicast for Rev VC Live Webcast and Custom Devices

With DME v.3.23 and Rev 7.34, configured correctly, Video Conferencing streams can be automatically pulled into a DME, reflected as unicast HLS, and converted to Vbrick multicast.

To utilize this feature, you must first set up the Rev Video Conference Recording and Streaming feature and be provisioned with Akamai publishing points/hostnames. **Note:** This is a back-end activity by the Vbrick Operations team.

Configuration of this feature is within Rev. **See:** [Enable and Configure a DME for Automatic Multicast and Reflection](#).

## HLS Stream Preparation for Automatic Multicast and Reflection Using Rev Custom Devices

Utilizing Automatic Multicast and Reflection has some implications for HLS stream configuration. HLS streams are basically structured playlists of segments that the player pulls and plays. For this, the DME needs to pull the HLS stream like a browser as well. However, there are some settings, configurations, and characteristics of HLS streams that are not supported by this feature. Vbrick endeavors to support as many different HLS stream implementations as possible, but there are some restrictions.

For example, the DME limits the size of the HLS URL. This includes, but is not limited to, the size of all playlists, sub-playlists, and TS or video chunks within the HLS stream. The URL length limit is 256, and it is there to keep Vbrick's caching engine optimum for all streams within the DME, not just the Automatic Multicast and Reflection Custom Device Streams.

In addition to the URL length, the URL may not include redirections. All HLS URLs must use direct paths, and *not* relative paths. Vbrick URLs all use direct paths.

There are some HLS tags that this feature does not support. Meaning, if your HLS within the Custom Device has the following tags, it cannot be used by this feature. These include:

- EXT-X-KEY

Additionally, the size of the segments (particularly large segments) may adversely impact and introduce some “bursty” behavior within the stream. While in many cases this behavior will not drive playback behavior, Vbrick recommendation is HLS streams that are ingested for this feature to have segments lengths of 4 to 6 seconds. Common use cases are outlined below.

### DME Generated HLS Streams Use Case

When using another DME to create the HLS stream, please view the stream settings and conform to the following recommended settings:

- HLS Type: Rolling
- Playlist Length: 3
- Seconds per Segment:
  - [Recommended] Auto
  - Set to 4 or 6 seconds (a multiple of 2, for the source IDR Setting)

### Akamai Stream Packaging (RTMP input, HLS Output) Use Case

Akamai provides a service, called Stream Packaging, that will take in a RTMP stream and output an HLS stream. This is a common approach for streams that originate outside of an organizations firewall – e.g., pushing a stream from a remote encoder up to Akamai, and having Vbrick distribute the HLS internally.

These HLS streams from Akamai (using the RTMP in and HLS output service called Stream Packaging) use a default 10 second segment length.

For example:

[http://engineering-lh.akamaihd.net/i/StreamName\\_1@232323/master.m3u8](http://engineering-lh.akamaihd.net/i/StreamName_1@232323/master.m3u8)

In this purely fictional example, the stream name is StreamName\_1 and 232323 is the stream ID. This stream will utilize a 10 second segment length. However, this stream can be changed to 4 or 6 second segment lengths by appending a set-segment-duration parameter on the URL:

- [Recommended Setting] For 6 seconds segment size append: ?set-segment-duration=quality

Example: `http://engineering-lh.akamaihd.net/i/StreamName_1@232323/master.m3u8?set-segment-duration=quality`

- For 4 seconds segment size append: ?set-segment-duration=responsive

Example: `http://engineering-lh.akamaihd.net/i/StreamName_1@232323/master.m3u8?set-segment-duration=responsive`

## Encoder Settings

In both examples above, the optimal encoder IDR setting to support the HLS generation is 2 seconds. This is also a strong Vbrick recommendation. By using 2 second IDRs, downstream playback (both in start up, and during playback) is optimized. This setting fits as a multiple of the 4 or 6 second recommendation for segment size.

Please set your source encoder IDR accordingly.

## Vbrick 9000 Encoder Example

As an example, here is how to set the Vbrick 9000 Encoder to use the correct IDR setting for the pushing a RTMP stream to Akamai Stream Packaging. As mentioned above, it is recommended that the encoder's IDR Frame Interval is 2 seconds. Note the change within the "IDR Frame Interval (sec)" field.

The screenshot shows the VAdmin 9000 Series encoder configuration interface. The main heading is "Encoder Configuration --> Video Encode". Below this, there is a "Video Rate Settings" section with a table of configurations for different rates. The table has columns for Enabled, Resolution, Bit Rate, Frame Rate, IDR, Rate Control, Profile, and Entropy. Rate 3 is selected and expanded to show detailed settings.

Enabled	Resolution	Bit Rate	Frame Rate	IDR	Rate Control	Profile	Entropy
<input checked="" type="checkbox"/>	1280x720	1,000,000	60	4	5: Best Quality	High	CABAC
<input checked="" type="checkbox"/>	656x368	750,000	30	4	5: Best Quality	High	CABAC
<input checked="" type="checkbox"/>	960x544	750,000	30	2	5: Best Quality	High	CABAC
<input checked="" type="checkbox"/>	656x368	750,000	30	4	5: Best Quality	High	CABAC
<input checked="" type="checkbox"/>	656x368	750,000	30	4	5: Best Quality	High	CABAC

Expanded settings for Rate 3:

- Rate 3 Enable:  Enabled
- Template: Custom Settings
- Resolution: 960x544
- Target Bit Rate (bit/sec): 750000
- Target Frame Rate (frames/sec): 30
- IDR Frame Interval (sec): 2
- Rate Control Setting: 5: Best Quality
- Profile: High
- Entropy Coding: CABAC

## Streaming

# User Configuration

## Username and Password

▼ To access the Username and Password fields:

1. Navigate to **User Configuration > Username and Password > Administration User Management** section.

Use this page section to change the user name and password (default for both = **admin**) for the DME server (and the FTP server). There is only one user name and password on the system and this access is not the same as ReadOnly access. If you change the user name and password, be sure to record the new name and password. If you lose the user name or password you will be unable to login to the server.

**Caution:** Be aware that when you change the user name and password for the server you are changing the FTP user name and password as well.

Field	Description
Current User Name	Enter current user name.
Current Password	Enter current password.
New User Name	Enter new administrator user name.
New Password	Enter new administrator password.
Re-enter New Password	Re-enter new password and be sure to click <b>Change Password</b> .

### Readonly Username and Password

---

## Readonly Username and Password

▼ To access the Readonly Password field:

1. Navigate to **User Configuration > Username and Password > Readonly User Management** section.

Use this page section to change the **Readonly** user account password if desired. The Readonly account user name and password (default for both = **readonly**) is used specifically for read only access to the DME server.

When logged in as a Readonly user, the user may *only* browse the DME interface. No modifications may be made.

**Caution:** Be aware that you must know the current Administrator User Name and Password to change the Readonly password. Further, while you may change the password for the Readonly account, the User Name will always be the default, “readonly”, and may not be changed.

Readonly User Management

Current Administrator:

Current Administrator Password:

Readonly User New Password:

Re-enter New Password:

Field	Description
Current Administrator	Enter current Administrator user name.
Current Administrator Password	Enter current Administrator password.
Readonly User New Password	Enter new Readonly password.
Re-enter New Password	Re-enter new password and be sure to click <b>Change Readonly Password</b> .

[Username and Password](#)

## Stream Input Authentication

▼ To access the Stream Input Authentication fields:

1. Navigate to **User Configuration > Stream Input Authentication**.

Use this page to configure a “broadcast” password that will allow you to publish streams to this server. This password is needed when sending a stream via auto unicast to a DME using either In-2 or In-3 or when sending an RTMP stream from a live encoder to the DME In-1.



Only one login user name and password are used for all inputs into the system. The login name cannot be the same name as the administrator name.

**User Configuration --> Stream Input Authentication** 2

Current Stream Input Authentication User Name: broadcast

New User Name:

New Password:

Re-enter New Password:

Cancel Change Password

Field	Description
Current Stream Input Authentication User Name	This read only field displays your current Stream Authentication username. The defaults (broadcast   broadcast for user name and password) are set at install time. Before enabling <b>Stream Input Authentication</b> for the scenarios listed above, please reset these values.
New User Name	Enter new announce user name.
New Password	Enter new announce password. This password may take the following special characters: !#\$%&()*+,-./;<=>?@[^_{}~'"
Re-enter New Password	Re-enter new password and be sure to click <b>Change Password</b> .



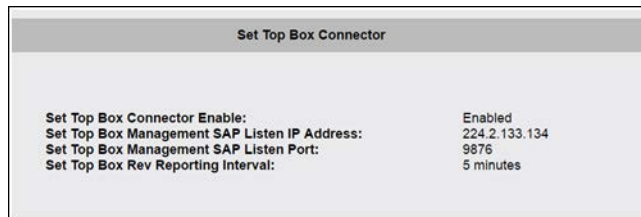
## Rev Devices

### Set Top Box Connector

Vbrick's Multi-Format Set Top Box (MF-STB) is supported starting with Rev version 7.16 and DME version 3.16. With this support, each MF-STB can be identified (via multicast SAP messages captured by local DMEs and forwarded to Rev), monitored for status, and set to view specific content from the Rev interface (See the “Set Top Boxes” topic in Rev Online Help for details) Please review your DME settings in Rev to select which DMEs will listen and report on MF-STBs.

Rev works in conjunction with on-premise DMEs to communicate to and from each MF-STB. This section, which is purely informational, displays the connector information (on the **Rev Devices > Configuration Page**) and the currently identified MF-STB that are visible to this DME (on the **Rev Devices > Devices** page).

The **Rev Devices > Configuration** page displays the following information:



Set Top Box Connector	
Set Top Box Connector Enable:	Enabled
Set Top Box Management SAP Listen IP Address:	224.2.133.134
Set Top Box Management SAP Listen Port:	9876
Set Top Box Rev Reporting Interval:	5 minutes

### Discovered Set Top Boxes

The **Rev Devices > Devices** shows information about each identified/found MF-STB.

The table contains information about each MF-STB. Clicking on the header for any of the table columns will sort the view and entering text within the filter box will filter against all content within the table by row.

Discovered Set Top Boxes (STBs)					
<a href="#">Show/Hide Last Set Top Box Rev Report</a>			<a href="#">Go to Rev Communications Log</a>		
<input type="button" value="Refresh STB List"/>		<input type="text" value="Filter STB List"/>			
IP-Address	Host-Name	Model	S/W-Version	Last-Report	Status
10.10.6.107	MACe0915398b63e	STB-HWM	2.2.5	2017-06-20@09:56:36	Ok
10.10.6.106	MACe0915398b55e	STB-HWM	2.2.5	2017-06-20@09:56:35	Ok
10.10.6.111	MACe0915398b4c8	STB-HWM	2.2.5	2017-06-20@09:56:36	Ok
10.10.6.109	MACe09153993bb6	STB-HWM	2.2.5	2017-06-20@09:56:35	Ok
10.10.6.112	MACe0915398b430	STB-HWM	2.2.5	2017-06-20@09:56:36	Ok
10.10.6.99	MACe091536e2cfb	STB-HWM	2.2.5	2017-06-20@09:56:39	Ok
10.10.6.74	MACe0915309d9b7	STB-HWM	2.0.1	2017-06-20@09:56:39	Ok

Field/Link	Description
Show/Hide Last Set Top Box Report	Toggle that will display/hide the most recent STB report.
Go To Rev Communications Log	Displays a list of the most recent Rev interface communications logs. You may also manually generate new logs from this form.
Refresh STB List	Manually refresh the list of discovered STBs.
Filter STB List	Filters the list of found STBs.
IP-Address	IP address of the STB.
Host-Name	Host name of the STB as identified with the MF-STB SAP message.
Model	Software version of the STB. Please use this to identify MF-STBs that need updating.
S/W-Version	Software version of the STB
Last-Report	The date and time a report was obtained from the STB. This is a periodic update, so this value will change.
Status	The status of the STB. Possible states are: <ul style="list-style-type: none"> <li>• Ok: The STB was accessed successfully by the DME</li> <li>• Invalid Credentials: The DME could not log-in to the STB</li> <li>• WebServiceDisabled: Remote access to the STB is disabled</li> <li>• Error: The operation failed for an unknown reason</li> </ul>

**Note:** Clicking **Show/Hide Last Set Top Box Rev Report** will show the formatted information that the DME sends to Rev. This is to be used in conjunction with Vbrick Customer Support if necessary as requested.

Clicking **Go to Rev Communications Log** links to the page where the DME to Rev interface logs may be viewed. The full logs are also available within the DME Logs directory. This is also to be used in conjunction with Vbrick Customer Support if necessary as requested.

## Logging

### Enable Error and Access History Logging

The **Error Log** on the Monitor > Error Log page displays DME status messages as well as errors.

**Access History** on the Monitor > Access History page shows files that have been accessed since the last reset.

The **Logging** page specifies logging rotation and overwrite rules.

▼ To specify logging rotation and overwrite rules:

1. Navigate to **Logging > Logging**.



Field	Description
Roll Logging	Check to enable the Error Log and/or the Access History rotation per the <b>Roll log</b> defined settings. If this box is not selected, logging is still enabled but it will continue to accumulate into individual log files rather than being rotated per the roll log settings defined below. Logged entries are shown the respective <b>Monitor</b> pages. The error log displays DME status messages as well as errors. The access log shows files that have been accessed since the last DME reset.
Roll log	Overwrite the logs every <b>nnn</b> KB or every <b>nnn</b> files (whichever comes first).
Remote Logging	The DME can provide remote logging of system services. Use this checkbox to enable and disable the service.
Remote Server Address	Please provide the remote server IP/FQDN address here.
Remote Server Port	Please provide the remote server port here; 514 is default.



## Monitor and Logs

### MPS Connections

The DME has several different servers that cooperate to distribute various forms of video content. This page reports on the MultiProtocol Server (MPS) streaming types. This includes all RTP/RTSP, RTMP/RTMFP, Vbrick Multicast (VBM), and Stream Conversion streams. In other words, most all streams that are pushed or pulled to/from the DME are reported within this page.

**Note:** HLS, HDS are not served to viewers via the MPS. They are http based protocols, so they are served via the DME's caching system. You will see HLS/HDS stream within the MPS Monitor Page if they are generated within the DME. However, you will not see all the viewer connections to the live HLS/HDS, nor connects for VOD HLS/HDS/Progressive Download.

The primary use cases for the **Monitor and Logs > MPS Connections** page revolve around the use of the MPS table, and they are:

1. **Verifying the existence of a stream.** This is probably the most used feature of this page. The DME can be configured to pull various streams from remote locations, push various streams to remote locations, and accept streams from various sources. This page provides an entry in the table identifying each of the existing streams within the DME. If the stream is not listed, then the stream is currently not in the DME.
2. **Get playback URLs and test streams from the DME.** For each stream identified within the MPS table, a number of “URLs to Copy” are provided. Hovering over these will display the URL. These are designed so that a right-mouse click will allow you to “Save like as...” and copy the link to your clipboard. This is highly useful so that you can paste that URL into the player of your choice and verify the playback of the stream. We recommend that you paste these links into Rev (on the **Upload > Add URLs** menu item) and view them with the Rev layer as your viewers would do. You can also paste these URLs into VLC or other players.
  - **HLS Streams.** These URLs can be added and played directly from Rev – our recommended approach. The Safari browser has native HLS playback support, while others do not (and will only download the m3u8 playlist).
  - **RTMP/RTMFP.** While browsers are moving away from this technology, there are still use cases that require it. Note: Using RTMP to push streams from DME to DME is still common because of latency issues—this should not be confused with the RTMP playback within the browser which is diminishing. Copying the URL into browsers that support these protocols will playback accordingly.
  - **RTSP/RTP.** Like RTMP, RSTP/RTP is a protocol more often used for distributing video through a network. Playback of these protocols requires specialized players – and we recommend using VLC for testing.

3. **Check stream quality.** While not a complete picture of quality, the “Packets/Segments Sent” and “Packets/Segments Lost” provide a picture of the streams health. If you see a large number of “Packets/Segments Lost”, then you should investigate the stream (either push or pull) and connectivity between the devices.
4. **Check longevity of stream.** The MPS table provides a “Time Connected” measure. This will tell you how long a stream has been active within the DME. If the stream should be long-lived (e.g., always on) then compare this time with the DME uptime in the lower left-hand corner and investigate if there is a discrepancy.
5. **Check the sub playlists within an MBR (multiple bit rate) HLS stream.** The DME can in take several streams (containing the same content but at different bit rates) and create an MBR playlist. It is often desirable to test each of the individual streams for the various bitrate levels. The MPS table provides an entry for each of the sub-playlists, as well as the master playlist. The naming convention is: StreamName/\* (for Master playlist), and StreamName/SubstreamName1 accompanied by StreamName/SubstreamName# for each of the sub playlists. Each of which, including the master, are individually playable using the playback URLs.
6. **Review Stream Conversion stream quality.** Using Stream Conversion to create different stream versions (with different characteristics that drive bitrate, such as resolution, bitrate cap, or framerate) is a common use case for the DME. Each of these different streams is identified within the MPS table and the URLs can be copied out for playback testing. Streams converted to different bitrates/resolutions should always be tested for acceptance. Also note, that while Stream Conversion is a useful capability of the DME, Vbrick recommends creating the different bitrates at the creation time. (Meaning use encoders to create the various bitrates – having purpose built hardware is better assurance for quality.)

These don’t represent all of the possible use cases for this page, but do illustrate this page’s usefulness. Vbrick recommends that all Administrators become familiar with this page and its capabilities.

To access the MPS Connections fields:

1. Navigate to **Monitor > MPS Connections.**

As described above, this page provides details on all streams within the MultiProtocol Server (MPS) in the DME. Click on the column header to sort the entries up or down.

Controls above the table include:

Field	Description
Page Refresh Interval	From the dropdown, select the desired page refresh interval. This will actively refresh the page based on the time selected. <b>Note:</b> Do not select a small refresh if you have a large number of connections/rows within the table – refreshes are time/CPU intensive. For very large number of connections, this feature is disabled.
Table Filter Field	Entering text here will filter the table below. It will match any text within each row, so in some cases where information is hidden the row will still display. Uses of this filter are: <ul style="list-style-type: none"> <li>• Enter IP address to find viewer or stream</li> <li>• Enter Stream Name to find all uses of the stream</li> </ul>



Field	Description
Only Streams with Loss or Errors	This will toggle the view to display Only Streams with Loss or Errors. Clicking on this toggle will remove any existing filter on the table. Uses of this toggle are: <ul style="list-style-type: none"> <li>• Quick identification of Streams with errors</li> </ul>
Reset	This will remove all filters and toggles.
Reload	This will re-query the DME for more up-to-date information.

**Note:** If you have a large (>20) number of connections, it is recommended that you *not* automatically refresh the page. Instead, use the **Reload Button** (rather than a **Page Refresh Interval**) to reduce the load on the DME.

MPS (Multi-Protocol Server) Connections 2

Page Refresh Interval: Never   Only Streams with Loss/Errors Reset Reload

**13 Connected MPS Streams (of 100)** Tue, 13 Apr 2021 10:33:59

Stream OR Event	Action	Configuration	URL(s)	Statistics	Time
147565be-3d6e-4f4e-a5ec-51f6a2471623	Stream Conversion	Configured on DME	ORIGIN	Received Packets 52,378,040	18:21:07
	Generated MPS Streams	Automatic	RTSP RTSP-TS RTMP		
	HLS Generation	Configured on DME	HLS	Sent Packets 52,368,236	18:20:55
45e716b0-9df6-46a6-b9b8-55cc8a834214	Stream Conversion	Configured on DME	ORIGIN	Received Packets 35,946,200	18:21:07
	Generated MPS Streams	Automatic	RTSP RTSP-TS RTMP		
encoderStream	Receiving RTSP	Configured at source	ORIGIN	Received Lost Packets 4,681,069 3	18:21:09
	Generated MPS Streams	Automatic	RTSP (1) → RTSP-TS RTMP		
	Pushing RTMPs	Configured on DME	RTMPS Unicast	Sent Packets 4,677,912	18:20:25

Field	Description
Stream OR Event	This is the <b>Stream Name</b> , and is associated with each sub-row (to the right).
Action / Configuration	This field contains the following: <ul style="list-style-type: none"> <li>• The <b>Stream Type</b>, e.g., <b>Receiving RTSP</b> which means a source is pushing an RTSP stream into this DME (with the stream name identified in the Connect To column).</li> <li>• Configuration information which identifies where the configuration for the particular stream is occurring. E.g., <b>Configured at source</b> would imply that the source of the stream is controlling the configuration. This field will identify if it is configured locally, remote, or on Rev.</li> <li>• If a stream is being generated, say <b>HLS Generation</b>, it will be identified here as well.</li> </ul> <p><b>See:</b> <a href="#">Possible Stream Types</a> and <a href="#">Possible Stream Type Configurations</a></p>

Field	Description
URL(s)	Each data element, which indicates a URL, can be viewed if you hover. Hovers contain information specific to each type of URL. Each URL can be copied using right-click and browser equivalents of “Copy Link Address”.  Lastly, if the element contains a “(#)” that indicates a listing of viewers (IP addresses) is available. Clicking on that will expand the table in the Statistics column listing out the viewers.
Statistics	Each row may have different statistics based on the stream type. These are included within the column.  Lost packets will only be listed if they exist, otherwise blank.
Time	This is the time the stream has been connected. In some cases, the system will display reconnects and reconnect periods.
Status	The last column will display exception status.

## Possible Stream Types

**Receiving <PROTOCOL>** Where <PROTOCOL>= { RTSP | RTMP | RTMPS }

This is a stream that is being actively pushed to the DME by another source (encoder, DME, 3rd party source). Once received, this is a stream that can be manipulated within the DME.

**Pulling <PROTOCOL>** Where <PROTOCOL> = { RTSP | RTSP-TS | RTMP | RTMPS | RTMP Stream on Demand | HLS Passthrough | HLS }

These are streams being pulled from another source and are configured on Rev or within the DME. Once received, this is a stream that can be manipulated within the DME.

**Pushing <PROTOCOL>** Where <PROTOCOL> = { RTSP | RTSP-TS | RTMP | RTMPS | RTMPS for Enrichment | Vbrick Multicast | to CDN | to CDN Inactive }

These are streams being pushed to another source and are configured on Rev or within the DME.

### Stream Conversion

These are streams that are being translated in terms of resolution and/or bitrates. The settings can be found on the Stream Conversion DME page.

**HLS <FUNCTION>** Where <FUNCTION> = { Generation \ | Sub Playlist [Generation] \ | Reflection }

These represent HLS streams either being created or pulled (for distribution).

## Possible Stream Type Configurations

**Configured on DME.** This stream was configured on the DME.

**Configured on Rev.** This stream was configured on Rev.

**Configured on DME for Rev.** This stream was configured on the DME, but used by Rev.

**Configured on Rev for DME.** This stream was configured on the Rev, but communicated and set up on the DME automatically.

**Automatic via Client.** This stream was automatically instantiated via a Client/browser call.

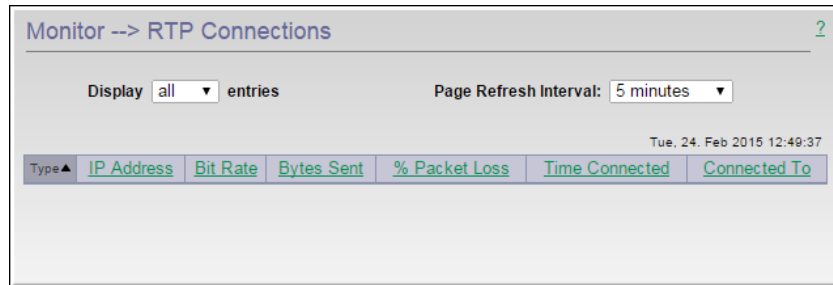
**Rev Initiated.** This stream was initiated by Rev, but being serviced by DME.


## RTP Connections

▼ To access the RTP Connections fields:

1. Navigate to **Monitor > RTP Connections**.

This page shows all RTP users currently connected to the DME. Click on the column header to sort the entries up or down.



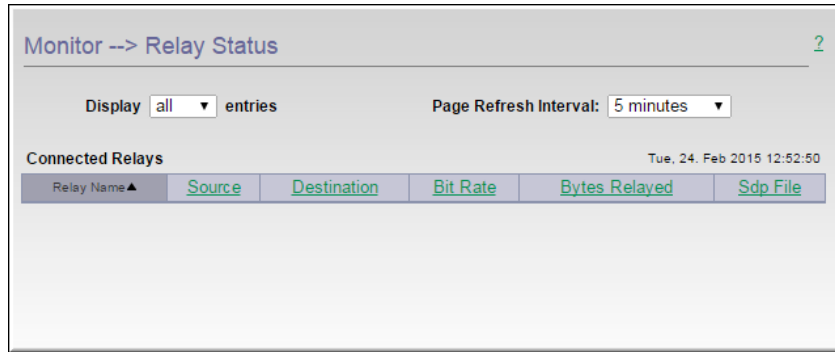
Field	Description
Display entries	From the dropdown, select the number of entries you wish to display on the page.
Page Refresh Interval	Select the desired page refresh interval from the dropdown.
Connected Users	<p>The DME displays the following information for each connected user. Click on the header field to sort ascending or descending.</p> <ul style="list-style-type: none"> <li>• Type – a video icon indicates a stream is present. </li> <li>• IP Address – user IP address.</li> <li>• Bit Rate – stream bit rate in Kbps.</li> <li>• Bytes Sent – total bytes sent.</li> <li>• % Packet Loss – percentage packet loss.</li> <li>• Time Connected – total time connected.</li> <li>• Connected To – target IP address.</li> </ul>

## Relay Status

▼ To access the Relay Status fields:

1. Navigate to **Monitor > Relay Status**.

This page shows the status of all defined relays. Click on the column header to sort the entries up or down



Field	Description
Display entries	From the dropdown, select the number of entries you wish to display.
Page Refresh Interval	From the dropdown, select the page refresh interval.
Connected Relays	<p>The DME displays the following information for each connected relay. Click on the header field to sort ascending or descending.</p> <ul style="list-style-type: none"> <li>• Relay Name – relay name.</li> <li>• Source – source IP address.</li> <li>• Destination – destination IP address.</li> <li>• Bit Rate – stream bit rate in Kbps.</li> <li>• Bytes Relayed – total bytes relayed.</li> </ul>

## Recording Status

▼ To access the Recording Status fields:

1. Navigate to **Monitor > Recording Status**.

This page provides real-time status on any ongoing recordings on this DME. DMEs must be set in Rev first to serve as a recording device for live streams. Refer to [Media Settings > Recording](#) (in Rev Help) for Recording for help setting DMEs that will record.

For DMEs that are set to record, the **Monitor and Logs > Recording Status** page will provide real time updates for ongoing recordings. While there are many reasons to visit this page, the primary use cases are:

1. **Verify the Existence of an Ongoing Recording.** This is, arguably, the most important use of this page. Visiting this page will identify all the current recordings. If the stream is not listed, then it is not being currently recorded.
2. **Verify Status of the Ongoing Recording.** Secondly, this page can identify recording durations and size. Visit the page, make note of the size, and then (after a few moments) refresh the page. The size should be increasing. If the size is not increasing, check the Status and the stream.
3. **Get a Copy of Source URL.** This page also allows Administrators to get a copy of the source URL. If the stream is in difficulty, Administrators can use the source URL with external players to test the stream.

Controls above the table include the following:

Field	Description
Page Refresh Interval	This drop-down will control how often the page will refresh. Refreshing will get up to date information on each of the recordings. It is From the drop-down, select the page refresh interval.
Table Filter Field	This field, defaulted to “Enter text to filter table” allows users to filter the Active Recordings table below. This feature is useful for quickly finding streams in a large table. This value is not retained over a page refresh.
Reload	This button will reload the <b>Monitor and Logs &gt; Recording Status</b> page.

**Note:** If you have a large (>5) number of recordings, it is recommended not recommended that you automatically refresh the page. It is recommended that you use the Reload Button instead of a low Page Refresh Interval to reduce load on DME.

The **Active Recordings** table will list all ongoing recordings (in accordance to any filter entered). Each of the column are sortable – just click the column name to sort or reverse sort the column. The columns in the table include:

Field	Description
Source URL	This is the source URL for the stream that is being pulled into (or already present) the DME for recording.
Duration	This is the current duration of the recording. For live ongoing recordings, this should increase accordingly., this should increase accordingly.
File Size	This is the current size (in bytes) of the recording. For live ongoing recordings, this should increase accordingly.
Status	This is the status of the recording. This will include Recording, Recording Complete, and any error states.

Additionally, as shown in the table below, the hover state for each stream will provide more data. This includes:

- WebCast ID (which ties the recording back to a Rev WebCast),
- the Start time of the recording,
- the maximum recording time (this is the maximum allowable time for the recording, and recording will stop by default after the max time), and
- the output file name (useful to tie recording back to a Rev WebCast).

41 Active Recordings (of 50)					Fri, 4 Oct 2019 11:29:50
	Stream Name	Source URL	Duration	File Size	Status
1	400k	rtsp://172.25.127.173:5544/400k	00:01:46	5,808,128	Recording Complete
2	400k	rtsp://172.25.127.173:5544/400k		062	Recording
3	400k	rtsp://172.25.127.173:5544/400k		352	Recording
4	400k	rtsp://172.25.127.173:5544/400k		746	Recording
5	400k	rtsp://172.25.127.173:5544/400k	00:43:12	134,683,040	Recording
6	400k	rtsp://172.25.127.173:5544/400k	00:41:34	129,613,770	Recording

WebCast ID: 27c80ec2-c58e-4a04-acc6-3d7777744e55  
 Start time: 2019-10-03 @ 17:47:18  
 Max recording time: 01:58:59  
 Output: 434057b6-2670-45ca-a489-2ffe89e8e122

## Access History

▼ To access Access History information:

1. Navigate to **Monitor > Access History**.

This page shows the file names that have been requested by all users since the last DME reset.

It is enabled and rolls over (i.e. overwrites the information) as configured on the [Logging](#) page.

Monitor --> Access History ?

---

**Files Requested Since Last Reset**

File Requested	Requests

Field	Description
Files Requested	File names requested since the last DME reset.
Requests	Number of times the individual file was requested.

## Upgrade Log

▼ To access the DME Upgrade Log:

1. Navigate to **Monitor > Upgrade Log**.

This log shows a history of all DME upgrade activity. Any .rpm upgrades will be reported on this page as successful, incorrectly signed, or failed.

These results are explained in more detail below. For an explanation of how to upgrade your DME, see the [Install Security Updates](#) topic.

```

Monitor --> Upgrade Log
Mon Jan 6 09:16:05 EST 2014
installing cumulative update package: /upgrade/vbrick-dme-3-1-7-1.rpm
cumulative update package status: success
Fri Feb 28 05:35:37 EST 2014
installing cumulative update package: /upgrade/vbrick-dme-3-2-0-3.rpm
cumulative update package status: success
Wed Mar 5 06:37:11 EST 2014
installing cumulative update package: /upgrade/vbrick-dme-3-2-0-5.rpm
cumulative update package status: success
Thu May 8 07:30:59 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-2-4-1.rpm
cumulative update package status: success
Tue Jun 3 21:34:10 EDT 2014
package: /upgrade/vbrick-dme-103.3.0.14-1.x86_64.rpm status: install success
Tue Jun 3 22:10:22 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-103-3-0-14.rpm
cumulative update package status: success
Thu Jun 26 07:01:33 EDT 2014
Thu Jun 26 07:01:52 EDT 2014
Wed Jul 9 08:14:57 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-3-0-33.rpm
cumulative update package status: failure
Wed Jul 9 09:23:31 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-3-0-33.rpm
cumulative update package status: success
Tue Jul 29 04:44:20 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-3-0-47.rpm
cumulative update package status: success
Wed Oct 1 23:42:59 EDT 2014
Wed Oct 1 23:43:26 EDT 2014
Wed Oct 1 23:51:28 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-4-1-5.rpm
cumulative update package status: failure
Wed Oct 1 23:58:57 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-4-1-5.rpm
cumulative update package status: failure
Thu Oct 2 05:21:01 EDT 2014
installing cumulative update package: /upgrade/vbrick-dme-3-4-1-5.rpm
cumulative update package status: success
Thu Jan 15 13:46:45 EST 2015
installing cumulative update package: /upgrade/vbrick-dme-3-4-5-19.rpm
cumulative update package status: success

```

Field	Description
Success	The .rpm was signed by Vbrick and successfully installed.
Not Signed	The .rpm you tried to install does not have the correctly signed Vbrick key.
Fail	Either the .rpm upgrade has already been installed or is not valid for this DME.

## Error Log

▼ To access the DME Error Log:

1. Navigate to **Monitor > Error Log**.

The Error Log displays status messages as well as errors. It is enabled and rolls over (i.e. overwrites the file) as configured on the [Logging](#) page.

To reset the Error Log manually, scroll to the bottom of the page (if necessary) and click **Reset Error Log**. If problems occur, you can copy and paste the error text from this page and send to Vbrick Support Services via email. You may also be asked to fetch other log files available in DME root via FTP.

```

Monitor --> Error Log
#Log File Created On: 01/13/2015 05:44:27
# Streaming SHUTDOWN 2015-01-13 05:44:27
# Streaming STARTUP 2015-01-13 05:44:32
2015-01-13 05:44:33: INFO: Module Loaded...DMEDMERTSPPostProcessorModule [dynamic]
2015-01-13 05:44:33: INFO: Module Loaded...DMEHomeDirectoryModule [dynamic]
2015-01-13 05:44:33: INFO: Module Loaded...DMERefMovieModule [dynamic]
2015-01-13 05:44:33: INFO: Module Loaded...DMEFileModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEReflectorModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMERelayModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEAccessLogModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEFlowControlModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEPosixFileSysModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEAdminModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEMP3StreamingModule [static]
2015-01-13 05:44:33: INFO: Module Loaded...DMEAccessModule [static]
# Streaming SHUTDOWN 2015-01-15 06:07:55

```

## User Login Log

▼ To access the User Login Log fields:

1. Navigate to **Monitor > User Login Log**.

The User Login Log keeps a record of all log ins to the DME. It will store up to 700 KB of information before it begins removing old records which equates to approximately 11,000 user records/logins. The **IP Address**, **Username**, date/time, and **Status** is tracked of each log in. This page will alert you to an unauthorized access (or an attempt) to your DME.

Monitor --> User Login Log

Log Starting from 02/Oct/2014 05:32:27

IPAddress	Username	Time	Status
10.20.4.56	admin	02/Oct/2014 05:32:27	Login Success
10.10.0.188	admin	02/Oct/2014 05:38:49	Login Success
10.20.4.55	admin	02/Oct/2014 05:46:25	Login Success
10.10.0.212	admin	06/Oct/2014 03:43:39	Login Success
10.10.0.212	admin	06/Oct/2014 04:43:40	Login Success
10.10.0.212	admin	06/Oct/2014 05:17:51	Login Success
10.10.6.191	admin	23/Oct/2014 08:15:35	Login Success
10.10.6.191	admin	23/Oct/2014 08:23:24	Login Success

## Upload Log

▼ To access the Upload Log fields:

1. Navigate to **Monitor > Upload Log**.

The Upload Log is used to provide status on files that Rev ingests from the DME. The date, time, file name, and status of each ingestion is provided.



```

Monitor -> Upload Log 2
04/06/15 15:16:41, VBADMIN, Retry Rev Uploads
04/06/15 15:18:13, VBADMIN, Retry Rev Uploads
04/06/15 15:22:56, VBADMIN, Retry Rev Uploads
04/06/15 15:24:20, VBADMIN, Retry Rev Uploads
04/07/15 11:58:23, .tcs_ingest/O142834685800-38732844fl.mp4, Detected new or changed file
04/07/15 11:58:23, .tcs_ingest/O142834685800-38732844fl.mp4, Starting Rev upload
04/07/15 11:58:23, .tcs_ingest/O142834745800-74167646fl.mp4, Detected new or changed file
04/07/15 11:58:23, .tcs_ingest/O142834745800-74167646fl.mp4, Starting Rev upload
04/07/15 11:58:24, .tcs_ingest/O142834685800-38732844fl.mp4, Uploading to http://qa-u1204-
ha-34a.lab.vb.loc/api/uploads/videos/
04/07/15 11:58:24, .tcs_ingest/O142834745800-74167646fl.mp4, Uploading to http://qa-u1204-
ha-34a.lab.vb.loc/api/uploads/videos/
04/07/15 11:58:27, .tcs_ingest/O142834685800-38732844fl.mp4, Ingested Successfully.
04/07/15 11:58:28, .tcs_ingest/O142834745800-74167646fl.mp4, Ingested Successfully.
04/07/15 11:58:34, .tcs_ingest/O142834685800-38732844fl.mp4, Detected new or changed file
04/07/15 11:58:34, .tcs_ingest/O142834685800-38732844fl.json, Detected new or changed file

```

The log includes the following status updates:

- Ingested successfully (no errors)
- Metadata file invalid, JSON syntax
- Failed to upload to Rev after X retries
- Rev is not configured
- No network connection to Rev
- JSON contains invalid metadata (from Rev)
- Invalid video file (from Rev)

The log file may also be reset by clicking the **Reset Upload Log** button at the bottom of the screen.

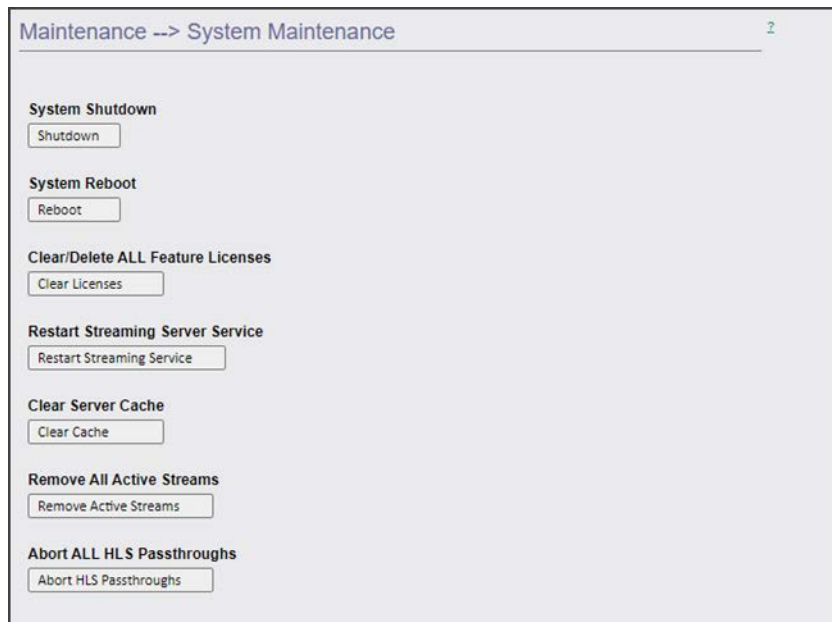
---

## Maintenance

### System Maintenance

- ▼ To access the System Maintenance function:
  1. Navigate to **Maintenance > System Maintenance**.

**Note:** After a power failure the DME may go into read-only mode and FTB will be disabled. As a best practice, always run **Reset with Check Disk** after a power failure.



Function	Description
Shutdown	This button will perform a graceful shutdown of the DME. It will not restart after this action. To restart a hardware DME, toggle the physical power switch. To restart a VM, reboot from the VM host.
Reset	This resets (i.e. reboots) the appliance. A reset does not change, save, or reset any configuration parameters. <b>Note:</b> RTP UDP Auto Unicast connections from a Vbrick encoder are not restored after a System Reset. To restore the connection, disable and then enable the RTP transmitter on the encoder.

Function	Description
Clear Licenses	<p>This clears all licenses within the DME. This is useful for removing DEMO licenses, which are only good for 31 days. Use this button to clear a demo license and activate a feature before your demo license has expired. After clearing any licenses, please go to Activate Feature to activate a new license.</p> <p>If you have active licenses, be aware that Clearing the Licenses has the following effects:</p> <ul style="list-style-type: none"> <li>• Removes all active stream conversions and defaults stream conversion config</li> <li>• Turns off and deletes swap</li> <li>• Reboots</li> </ul>
Restart Streaming Service	<p>The DME is made up of several services. There are two different streaming engines within the DME. This button controls the RTSP server (that by default uses port 554). Clicking this button will reset the RTSP server.</p> <p>The second streaming service, also referred to as the Multiprotocol Server, controls RTSP/RTMP/RTMFP/RTSP/HLS streams (that by default use 1935, 5544, and 80 depending on protocol). If you wish to reset this server, then please use the "Disable Server""Enable Server" toggle button at the far left of the bottom status bar with DME VBAAdmin (Web UI).</p>
Clear Cache	<p>Use this button to clear the cache on the DMEs. This clears all DME Cached content (both memory and disk cache for any http traffic) – it will not remove any pre-positioned content that is stored on the disk. After clearing, our caching engine will start fetching, first-time caching and serving new web pages rather than serving cached pages. Once the cache has the content, it will be served from the cache.</p>
Remove Active Streams	<p>This button removes all actively configured input and output streams. Should be used in conjunctions with Vbrick Support only. After use, all active streams will need to be disabled and then re-enabled to start again.</p>
Abort ALL HLS Passthroughs	<p>This button terminates all existing HLS Passthrough streams. This will not re-notify Rev of a stream termination, but in some cases the streams will begin pulling again. Please do not use this feature during any ongoing events as they will be impacted.</p>

## Disk Status

▼ To access the Disk Status information:

1. Navigate to **Maintenance > Disk Status**.

In some configurations it may be desirable to extend the storage space of your DME. This can be done in the following ways: (1) add a new virtual disk to a VM, (2) add a new physical disk to a medium or large DME (small DMEs do not have the capability of adding additional space), or (3) add a network storage device (See: [SAN/iSCSI Setup](#)).

If you have added a new virtual or physical disk, then the **Disk Status** page will allow your DME to access the disk. Disks that are added to the DME in this manner are merged into a single, common storage location. Therefore, once added, these disks cannot be removed (if physical) or deleted (if virtual) – and the DME will be rendered inoperable if a disk is removed. Please plan accordingly.

This page shows the size and status of **Existing Disks** (i.e. those disks that were present originally or were added using the “provisioning” process) and of **New Disks Found** which have not yet been provisioned.

Maintenance --> Disk Status		
Page Refresh Interval: 30 seconds		
<b>Existing Disks</b>		
Disk Name	Size	Status
Harddisk1	20 GB	Built-in Disk
<b>New Disks Found</b>		
Disk Name	Size	
None		

Field	Description
Page Refresh Interval	<ul style="list-style-type: none"> <li>Never – Never refresh page.</li> <li>30 seconds – Refresh page every 30 seconds.</li> </ul>
Existing Disks	<ul style="list-style-type: none"> <li>Disk Name – Disk name.</li> <li>Size – Configured size in KB.</li> <li>Status – Displays either "Built-in Disk" or "Provisioning" if a provisioning is in progress.</li> </ul>
New Disks Found	<ul style="list-style-type: none"> <li>Disk Name – Disk name.</li> <li>Size – Configured size in KB.</li> </ul>
Provision	Shown only when a new disk has been found. Click the named button to start the provisioning process for that disk. Note that this step is irreversible. See <a href="#">Provision a New Disk</a> for more information.

**Tip:** When extending space with Virtual Disks, Vbrick recommends creating additional virtual disks and provisioning them using the **Maintenance > Disk Status** page. While VM hosts allow the expansion of already provisioned virtual disks, they do not automatically expand the OS disk partitions contained within. Meaning, the DME does not detect that expansion of the partition on the virtual disk so the added space will not be detected. Alternatively, iSCSI disks can also be added to VMs – please see [SAN/iSCSI Setup](#).

## Provision a New Disk

To provision new disks, first turn off you DME (either physically or shutdown a VM). Add the disk accordingly. After restarting your DME you should see the new disk in the **New Disks Found** table with a button to "**Provision**". Provisioning is the act of formatting (for xfs file system) and adding the new disk storage to the DME common data storage location. In other

words, this extends the existing files system over the new disk and the new disk may not be removed once provisioned.

It is also important to note that for VM installs Vbrick only supports the expansion of the disk space by creating additional virtual disks and provisioning them using the **Maintenance > Disk Status** page. While VM hosts may allow the expansion of virtual disks, they do not automatically expand the disk partitions within the VM OS. Meaning, the DME does not detect that expansion of the partition on the virtual disk. The solution in this case is to add an additional new virtual disk.

SAN/iSCSI use is a different model. Please refer to the help page [SAN/iSCSI Setup](#).

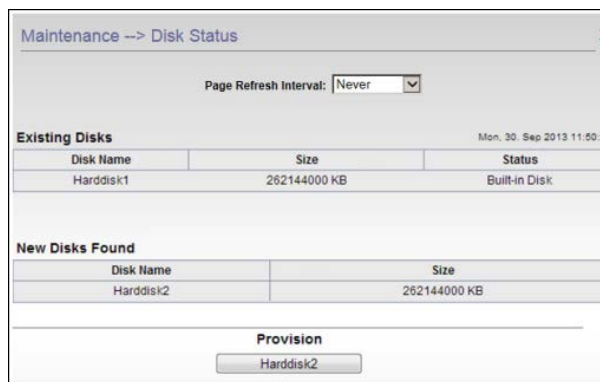
**Note:**

- Be aware that disk provisioning is irreversible. Once you have added a new virtualized disk, it cannot be removed.
- Always create a VMWare "snapshot" before you begin so that you can revert to you original configuration if anything goes wrong.
- Provisioning a disk is not the same as adding an iSCSI disk to the DME. If you are adding an iSCSI disk see the topic on [SAN/iSCSI Setup](#).

▼ To add a new disk in a virtual environment:

1. Navigate to **Maintenance > System Maintenance**.
2. Use the **Shutdown** button and shut down your DME. Verify with the virtual host to make sure the device is shutdown.
3. As a best practice, create a snapshot of the virtual machine using the virtual host tools or some other method. This will allow you to revert if anything goes wrong.
4. Add a disk to this virtual machine using the virtual host tools or any other method you use to manage your virtual machines.
5. When done, restart the DME virtual machine.
6. After the restart, navigate to **Maintenance > Disk Status**.

As noted, a new disk will be shown in the **New Disks Found** area (shown below) and a named button will let you provision the new disk. If you added more than one disk, the button will provision only one disk at a time and you will need to repeat the provisioning process for each additional disk.



7. Press the **Provision Disk** button to begin provisioning the new disk as an extension to the existing disk. A pop-up message will indicate approximately how long this will take. (The provisioning time is usually minimal but may take several hours depending on the type of

disk being added.) **Be aware that this will stop all streaming services from the DME until provisioning is complete and the device reboots.**

Maintenance --> Disk Status 2

Page Refresh Interval:

**Existing Disks** Mon, 30 Sep 2013 13:03:45

Disk Name	Size	Status
Harddisk1	262144000 KB	Built-in Disk
Harddisk2	262144000 KB	Provisioning

**New Disks Found**

Disk Name	Size

Disk Provisioning Started at: Mon Sep 30 11:50:54 2013  
Approximate duration for completion: 1 Hours

8. When provisioning is complete, the DME will reboot, the streaming services will restart, and the **Maintenance** > Disk Status page will show the new disk as active and available for use.
9. Navigate to the DME Status (Snapshot) link at the top of the **Configuration Menu** and the **Disk Status** section will show exactly how much space is in use and available for use.





# Diagnostics

## Trace Capture

▼ To access the Trace Capture diagnostic functions:

1. Navigate to **Diagnostics > Diagnostics**.

The Trace Capture utility creates a TCP dump of network traffic that can be used by Vbrick Support Services when troubleshooting issues. It captures packets based on the criteria you select and can subsequently be viewed in Wireshark or a similar application. As explained below, you run the utility, retrieve the capture file, and send to it Vbrick.

Field	Description
Page Refresh Interval	Choose how often to refresh the information on the page.
Interface to capture from	<ul style="list-style-type: none"> <li>• eth0 – this is the same as bond0 if load sharing is enabled on the IPv4 network interface.</li> <li>• bond0 – captures a trace across all network interfaces that are enabled.</li> <li>• any – captures a trace for both external and internal interfaces (bond0 and lo).</li> <li>• lo – captures a trace of the local host interface (127.0.0.1) only.</li> </ul>
Capture file size	Specify the size (default = 50 MB) of the capture file. The capture will terminate when file size reaches this value.
Status	Displays <b>Capturing</b> while a trace capture is in progress or blank when finished or idle.
Start   Stop Capture	Start or stop the capture process.

▼ To create a trace capture:

1. Select an interface from the dropdown.

2. Specify a size for the capture file. You can use the default or the value suggested by Vbrick Support Services.
3. Click **Start Capture** and confirm.
4. Run the capture until complete or click **Stop Capture** at any point.
5. FTP to the device and navigate to the **trace** folder.
6. The trace file will be in DME root with a name similar to this: **/trace/eth0.pcap**
7. Copy the file and send to Vbrick [Support Services](#).

## Ping Test

▼ To access the Ping Test diagnostic functions:

1. Navigate to **Diagnostics > Ping Test**.

The ping test diagnostic utility enables you to enter a domain name or IP (IPv4) to ping another device from the DME to make sure it may be reached.

Field	Description
Destination	Domain name or IP (IPv4 or IPv6) to ping.
Number of Packets	Default = 4. Number of packets that will be sent during the ping test. Packet number must be a positive integer between 1 and 25.
Packet Size	Default = 56. The size of packet that will be sent during the ping test. Packet size must be a positive integer between 32 and 1400.
Transmit Interval (sec.)	Default = 1. The delay between each packet in the ping test. Transmit interval must be a positive integer between 1 and 10.
Transmit Timeout (sec.)	Default = 5. The wait duration for each packet response in the ping test. Transmit timeout must be a positive integer between 1 and 10.

Ping Test Result:

Result	Description
Response Counter	Number of packets that the host responded with under the ping test.

Result	Description
Timeout Counter	Number of packets that were not responded with by the host under the ping test.
Resolved IP Address	IP address of the host under the ping test.
Ping Result	Will return “Host is alive” or “No response from host”.

## Traceroute Test

▼ To access the Traceroute Test diagnostic functions:

1. Navigate to **Diagnostics > Traceroute Test**.

The traceroute diagnostic utility enables you to enter a domain name or IP (IPv4 or IPv6) to print the route packets from the DME to a specific host.

**Diagnostics --> Traceroute Test**

**Traceroute Test Result**

Resolved IP Address 10.200.0.67

traceroute to vbrick.com (10.200.0.67), 30 hops max, 60 byte packets

1 172.22.1.5 (172.22.1.5) 0.370 ms 0.401 ms 0.421 ms

2 10.250.0.9 (10.250.0.9) 2.143 ms 2.144 ms 2.130 ms

Traceroute Result

3 172.27.151.233 (172.27.151.233) 6.619 ms 6.550 ms 6.464 ms

4 172.27.151.238 (172.27.151.238) 21.289 ms 21.221 ms 21.201 ms

5 172.27.151.238 (172.27.151.238) 21.203 ms 21.166 ms 21.171 ms

6 10.200.0.67 (10.200.0.67) 22.012 ms \* \*

**Traceroute Test Configuration**

IPv4 IP or Hostname

Start Save Revert Default

Field	Description
Destination	Domain name or IP (IPv4) to traceroute test.

Traceroute Test Result:

Result	Description
Resolved IP Address	IP address of the host under the traceroute test.
Traceroute Result	Lists the IP of each gateway along with cumulative time each packet takes to reach the host under the test.

## Caching Diagnostics

▼ To access the Caching Diagnostic functions:

1. Navigate to **Diagnostics > Caching Diagnostics**.

The Caching Diagnostics page is provided to allow access to underlying caching features and functionality. These features should *only* be changed or modified in conjunction with Vbrick Support or Development. Changing these features without Vbrick support may adversely impact your DME's performance.

**Caution:** The advanced features described on this topic should not be modified without explicit directions from Vbrick Support or Development.

Diagnostics --> Caching Diagnostics 2

---

**Caching Debug Settings**

Do not change these settings unless instructed by Vbrick

Caching Debug Configuration

Caching Core Size Limit

Caching Auto Recovery  Enabled

Override Caching Directives  Enabled

**Rev Interface Debug Settings**

Do not change these settings unless instructed by Vbrick

Validate Complex Rev JSON messages  Enabled

**Table 1** Caching Debug Settings

Field	Description
Caching Debug Configuration	This is an advanced field that should only be modified in conjunction with Vbrick Support or Development. Please consult with Vbrick before modifying this field.
Caching Core Size Limit	This controls the size of system core files.
Caching Auto Recovery	This checkbox controls a process that will automatically recover the caching system under specific conditions. The default and recommended value is Enabled / Checked.
Override Caching Directives	This checkbox controls the ability of the caching engine to determine which override directives, provided by browser requests, can be overridden for increased performance and stability within the DME. The default and recommended value is Enabled / Checked.

**Table 2** Rev Interface Debug Settings

Field	Description
Validate Complex Rev JSON messages	Do not modify this setting unless directed to by Vbrick Support.

# Detailed Use Cases

## MultiCast Relay Use Case Overview

The use cases included in this online help describe all of the steps you will need to perform (in order) to create a Multicast RTP Relay.

The first topic explains how to configure for a unicast source; the second topic explains how to configure for an auto unicast source.

These use cases provide a complete example of the types of things you will need to do to use the DME effectively. The Vbrick DME contains a fully featured RTP server which lets you create an Multicast RTP Relay stream. The relay can be streamed from a unicast source or from an auto unicast source on a Vbrick (7000/9000 Series) H.264 encoder. Both of these scenarios are explained in each topic.

For more information about encoder settings and parameters, see the [Vbrick H.264 Encoder Admin Guide](#).

[Configure a Multicast Relay with a Unicast Source](#)

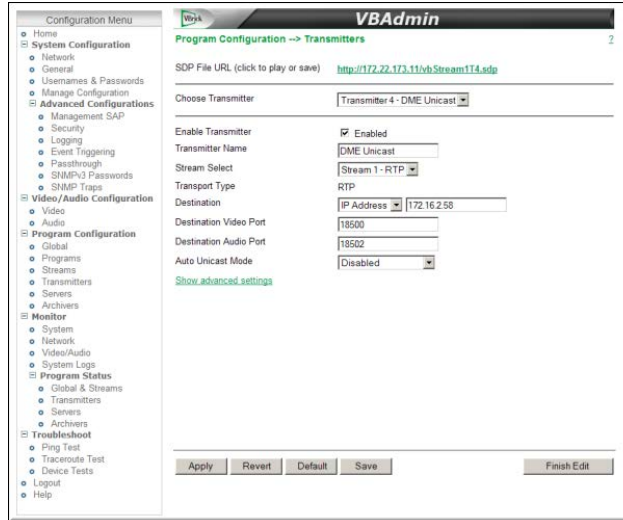
[Configure a Multicast Relay with an Auto-Unicast Source](#)

## Configure a Multicast Relay with a Unicast Source

This topic explains how to use the DME to relay an H.264 unicast stream from a Vbrick H.264 encoder as a multicast stream. Clients will then be able to join the multicast via HTTP to the DME. *This example shows how a relay can be streamed from a unicast source on a Vbrick H.264 encoder.*

### H.264 Encoder Setup

1. Configure a 7000/9000 Series H.264 encoder with a valid RTP stream then configure a transmitter to unicast to the DME (using higher video/audio port values).
2. Navigate to **Program Configuration > Transmitters** and configure the transmitter with the values displayed below:



## DME Setup

1. Create a new RTP Relay. See: [Create or Edit an RTP Relay](#).



2. Configure the RTP Relay as follows:
  - a. Enter a **Relay Name**.
  - b. Set the **Status** to Enabled.
  - c. Enter the IP Address as **127.0.0.1** and enter the original .sdp file name.
  - d. Select **Request incoming stream**.
  - e. Enter the Multicast IP Address from the .sdp file.
  - f. Enter the **Output SDP file** name.
  - g. Enter the Video Port value and Multicast TTL.

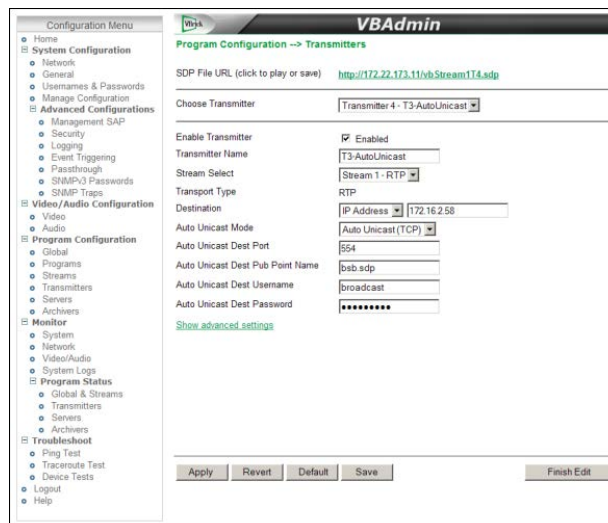
The user will view the video using QuickTime and entering the HTTP url to the SDP file located on the DME. In the example above the original sdp file is **taco-uni.sdp** and the output sdp is **taco-uni1.sdp**. So the URL will be **http://172.22.2.50/taco-uni1.sdp**.

## Configure a Multicast Relay with an Auto-Unicast Source

The Vbrick Distributed Media Engine contains a fully featured RTP server, giving the administrator the ability to provide an RTP Relay Multicast stream. When configured, clients will then be able to join the multicast via HTTP to the DME. *This example shows how a relay can be streamed from an auto unicast source on a Vbrick H.264 encoder.*

### H.264 Encoder Setup

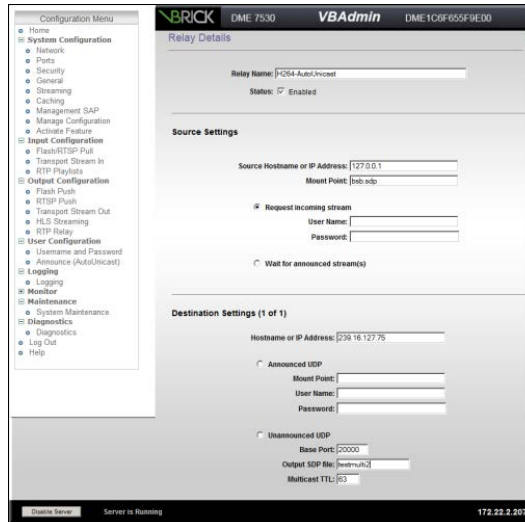
1. Configure the encoder with a valid Auto Unicast (TCP) stream and then navigate to **Program Configuration > Transmitters** and configure a transmitter to unicast to the DME.



2. Configure the transmitter with the following settings:
  - a. Set the **Auto Unicast Dest Port** to the RTSP port of the DME.
  - b. Configure the **Auto Unicast Dest Pub Point Name** to the desired sdp file name. This .sdp file will be automatically placed in the root folder. (Note: The file name must be appended with .sdp or the auto unicast will fail.)
  - c. Enable the transmitter and verify it is sending to the DME.

### DME Setup

1. Create a new RTP Relay. See: [Create or Edit an RTP Relay](#).



2. Play the Multicast Relay using QuickTime with a URL in the following format. **http://<dme\_ip\_Address>/<testmulti2.sdp>**

If desired, a URL can be added to the Vbrick's external **Announce Settings** on the Program Configuration > Transmitters page.



## Other Tasks

### Install Security Updates

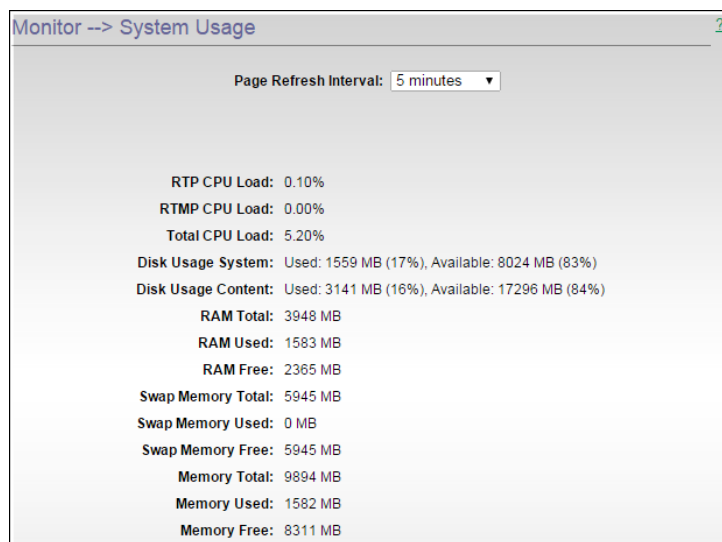
Signed Vbrick security updates may be periodically available. Do not neglect to install these updates. However, to avoid impacting performance, install updates only when the system is idle.

Do not update the DME with any software except as directed by Vbrick.

### Manage Disk Space

Your system has differing amounts of content storage available depending on the model you purchased. For example, the Model 7570 has (6) 300 GB of RAID 5 storage.

For best results and to avoid impacting performance, it is important to regularly monitor your CPU load and disk usage on the Monitor > [MPS Connections](#) page.



### Backup and Restore

As a best practice you should periodically save your configuration settings in case they need to be restored at a later time.

The [Manage Configuration](#) topic explains how to save and restore a DME configuration and how to reset the DME to the Vbrick factory defaults.

