Imagine COMMUNICATIONS™

User Guide

Cloud DVR (cDVR)

Release 1.4

18-May-2015

Revision: A

Cloud DVR (cDVR) User Guide, Release 1.4
Document part number: 250-0339-01, Rev. A
Printed 5/15/2015

Publication Information

Copyright 2005-2015 Imagine Communications Corp. Proprietary and Confidential.
This material is protected by the copyright laws of the United States and other countries. No part of this document may be reproduced, distributed, or altered in any form, by any means, by any entity nor may it be used to make any derivative work (such as translation, transformation, or adaptation) except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Imagine Communications. All other uses are illegal.

Notice

This publication is designed to assist in the use of the product as it exists on the date of publication of this manual, and may not reflect the product at the current time or an unknown time in the future. This publication does not in any way warrant description accuracy or guarantee the use for the product to which it refers. Imagine Communications reserves the right, without notice to make such changes in equipment, design, specifications, components, or documentation as progress may warrant to improve the performance of the product.

Trademarks

Selenio™ and Telurio™ are trademarks of Imagine Communications. Microsoft® and Windows® are registered trademarks of Microsoft Corporation. All other trademarks and trade names are the property of their respective companies.

Patents

The products described herein are covered by one or more U.S. and foreign patents pending.
U.S. Patents: 6,996,129; 7,046,677; 7,818,355; 8,180,920. Other US and foreign patents pending.

Contact Information

Imagine Communications has office locations around the world. For domestic and international location and contact information see: http://www.imaginecommunications.com/contact-us/

Support Contact Information

For domestic and international support of Selenio VMG, Selenio BNP, Selenio SEP, Selenio MMC, Selenio TAT, Telurio Packager, Telurio Recording Manager, and Telurio AIM products, contact:

Support Contacts:	support@rgbnetworks.com http://www.rgbnetworks.com/support/rgb-customer-portal.php 1.877.RGB.NETW // (1.877.742.6389) - Inside North America +1.408.701.2800 - Outside North America

For domestic and international support of all other Imagine Communications' products not mentioned above, contact:

Support Contacts:	http://www.imaginecommunications.com/services/technical-support/

Document Change History

Cloud DVR (cDVR) User Guide document history

Part Number	Software Release	Release Date	Changes
250-0339-01 Rev A	1.4	05/18/2015	• Updated user guide with new Imagine Communications branding • New keyserver: Playready Leaf • Minor changes to JITP/RECORDER container fields • Minor changes to CHANNELS, SCHEDULES, EBR, and ASSETS status menus
250-0325-01 Rev A	1.3	01/26/2015	• Updated all screenshots and instructions for new API • Added private copy description & instructions • Added Appendix A: RESTful API
250-0310-01 Rev A	1.2	11/14/2014	• Minor GUI Changes • Added storage content management functionality description
250-0293-01 Rev A	1.1	9/19/2014	• Added GPFS storage mount • Minor GUI changes
DRAFT, Rev A	1.0.1	n/a	Production Release on 7/20/2014 (No UG)

Table of Contents

CHAPTER 1

Introduction

Imagine Communications' *Cloud Digital Video Recorder* (cDVR) solution is a multi-component, software based, cloud enabled system that provides end-to-end video recording delivery using the service provider's own data center or a hosted private cloud. Imagine Communications uniquely offers two different methods of operator or user-based scheduled recording—*Event-based* and *Continuous Record*—and seamlessly supports fast-forward, resume, and sliding window playback in both shared and private copy mode.

This release of cDVR is offered as a three-component, software-only solution, each of which runs on a Linux-based[1] operating system. You can deploy cDVR on your choice of server-based hardware or in a virtualized server environment.

This user guide describes functionality, configuration and usage of the *Recording Manager (*RM), the *cDVR* management component. Refer to the *Telurio™ Recording Manager Software Installation, Setup, and Upgrade Guide* for instructions on software installation.

In This Chapter

This chapter contains the following sections:

1. Refer to the *Release Notes* or the *Telurio™ Recording Manager Software Setup & Upgrade Guide* for compatible versions of CentOS.

Document Organization

This guide is organized as follows:

- Chapter 1, "Introduction," (this chapter) describes the contents and conventions used in the *Cloud DVR (cDVR) User Guide*.
- Chapter 2, "Solution Overview," provides a detailed description of cDVR and its features.
- Chapter 3, "cDVR Initial Setup," lists the procedure for initial configuration of the cDVR components.
- Chapter 4, "RM Redundancy Setup," provides instructions for setting up redundant *Recording Managers*.
- Chapter 5, "Recording Manager GUI Overview," provides an introduction and overview to the RM graphical user interface (GUI)
- Chapter 7, "Configuration," describes how to use the *Configuration* tab to set up recording parameters.
- Chapter 8, "System Configuration," covers all maintenance and system-related tasks such as software upgrades, database backups, diagnostics, and configuring SNMP and syslog servers.
- Chapter 9, "Reports & Troubleshooting," describes alarms and events related to cDVR in addition to general troubleshooting tips.
- Appendix A, "RESTful API," provides information on how to access the Telurio Recording Manager's online API help pages.

Document Audience

This guide is for system administrators and operators who are responsible for installation and maintenance of the Imagine Communications cDVR solution. You should be familiar with general video and networking practices and terminology, and should be familiar with basic installation of hardware.

Related Documentation

- *Telurio™ Recording Manager Software Setup & Upgrade Guide, Release 1.4*
- *cDVR Quick Start Guide, Release 1.4*
- *Telurio™ Recording Manager: List of Events, Release 1.4*

Document Conventions

Table 1 provides an easy way to recognize important information in this user guide.

Table 1. Document Conventions

When you see:	It means:
	**Notes** are indicated by the icon shown on the left, and point out information that may not be part of the text but provide tips and other helpful advice.
	**Cautions** are indicated by the icon on the left, and let you know that an action may have undesirable consequences if the instructions are not followed correctly. Cautions also indicate that failure to follow guidelines could cause damage to equipment or loss of data.
	**Warnings** are indicated by the icon on the left, and indicate that failure to take the necessary precautions or to follow guidelines could cause harm to equipment and personnel.
	**Navigation tip:** follow the path next to the pointer to navigate a specific GUI menu.
Clicking any blue link takes you to the referenced item.	

Graphics Used

In some cases, the screens shown in this manual may have been slightly modified after the manual was released, or may appear slightly different on different browsers.

All efforts have been made to ensure that the latest images are used. In all cases, the functionality described is current at the time of writing.

Acronyms Used

Table 2 provides is a list of acronyms commonly used in video processing and cDVR. Note that some of these acronyms may not be used in this user guide.

Table 2. Video processing industry acronyms

Acronym	Meaning
AAC	Advanced Audio Coding
ABR	Adaptive Bitrate
AC3	Audio Coding Version 3 (Dolby Digital 5.1, or DD)
ADM	Ad Management Service (function of AWE)
ADS	Ad Decision Service
AIM	Ad Insertion in Multi Screen (Imagine Communications term)
API	Application Programming Interface
AU	Access Unit
Avail	Available opportunity for ad placement
AWE	Ad Workflow Engine (Imagine Communications term)
B-Frame	Bidirectional compression picture frame
CDN	Content Delivery Network
cDVR	Cloud Digital Video Recorder
CIFS	Common Internet Files System (Microsoft based)
CNS	Content Name Server
CR	Continuous Record(ing)
CPI	Cost per Impression
CPM	Cost per Thousand-Impression
DAI	Digital Ad Insertion
DD	Dolby Digital (same as AC3)
DD+	Dolby Digital Plus (same as E-AC-3)
DASH	Dynamic Adaptive Streaming over HTTP
DMA	Designated Market Area
DMM	Dynamic Manifest Manipulation
DRM	Digital Rights Management
DTS	Decoding Time Stamp
DTS	Digital Theater Systems (Dolby)
DVR	Digital Video Recorder
E-AC-3	Enhanced Audio Coding 3 (Dolby Digital Plus 7.1, or DD+)
EBP	Encoder Boundary Point
EBR	Event-based Recording
EIDR	Entertainment Identifier Registry (CableLabs sponsored registry for TV & movie programming)
ENC	Encoder
ES	Elementary Stream

Table 2. Video processing industry acronyms

Acronym	Meaning
ESAM	Event Signaling and Messaging
FQDN	Fully Qualified Domain Name
GOP	Group of Pictures
GPFS	General Parallel File System
GUI	Graphical User Interface
HDS	HTTP Dynamic Streaming (Adobe)
HD	High Definition
HLS	HTTP Live Streaming (Apple)
HRD	Hypothetical Reference Decoder
HTTP	Hypertext Transfer Protocol
IAB	Interactive Advertising Bureau
IDR	Instantaneous Decoder Refresh
I-Frame	Intracoded compression picture frame
IIS	Internet Information Services (Microsoft based)
JIT	Just-in-time (Imagine Communications term)
JITP	Just-in-time Packaging (Imagine Communications term)
KMS	Key Management Server
MBR	Multi-Bit Rate
MSS	Microsoft Smooth Streaming (HTTP based)
NAS	Network Attached Storage
nDVR	Network Digital Video Recorder (another name for cDVR)
NFS	Network File System (Linux based)
nPVR	Network Personal Video Recorder (another name for cDVR)
NTP	Network Time Protocol
PCM	Pulse Code Modulation
PCR	Program Clock Reference
PES	Packetized Elementary Stream
P-Frame	Predicted compression picture frame
PID	Packet ID
PMT	Program Map Table
PO	Placement Opportunity (aka. ad-break, avail)
POIS	Placement Opportunity Information Service
PRRS	Playlist Rebuilder, Redirection Server (Now referred to as PS)
PS	Playlist Server (formerly referred to as PRRS)
PTS	Presentation Time Stamp
RM	Recording Manager
RPM	Revenue per-thousand impressions
RTMP	Real Time Messaging Protocol

Table 2. Video processing industry acronyms

Acronym	Meaning
SAP	Stream Access Point
SCTE-30	Society of Cable Telecommunications Engineers, Standard 30
SCTE-130	Society of Cable Telecommunications Engineers, Standard 130
SD	Standard Definition
SIS	Subscriber Information Service
TAC	Selenio Commander (Imagine Communications)
TAP	Telurio Packager (Imagine Communications)
TAT	Selenio Encoder/Transcoder (Imagine Communications)
TS	Transport Stream
UDP	User Datagram Protocol
URI	Universal Resource Identifier (contains URL & URN)
URL	Universal Resource Locator (always a URI)
URN	Universal Resource Name (not necessarily a URI)
UPID	Unique Program ID
UUID	Universally Unique Identifier (See RFC 4122)
VAST	Video Ad Serving Template
VES	Video Elementary Stream
VM	Virtual Machine
VMG	Video Multiprocessing Gateway (Imagine Communications)
VOD	Video on Demand
VSP	Video Service Provider
XML	Extensible Markup Language

CHAPTER 2

Solution Overview

A Cloud Digital Video Recording (cDVR) solution provides the ability for a subscriber to make recordings of many linear multiscreen channels and programs. Recordings can be initiated by an operator for Catch-up/Time-shift TV or initiated by a subscriber, where the end user selects when and what to record.

Imagine Communications' cDVR solution is a network based DVR solution that continuously records channels. Recorded content is managed in the service provider's network, thus helping operators optimize storage and CDN costs. Subscribers can then create recording assets by abstracting the continuously recorded content for delivery to their multi-screen devices.

This chapter provides an overview of Imagine Communications' cDVR features and functionality, as well as a brief description of other non-Imagine Communications components in an cDVR environment.

Note: *Several acronyms are used throughout this chapter. You may wish to refer to* Table 2, "Video processing industry acronyms," on page 13 *for their meanings.*

In This Chapter:

Adaptive Bitrate (ABR) Primer

To understand how cDVR works in a multi bit rate environment, a general description of ABR streaming is provided here.

ABR Technology

Adaptive streaming works via a video client's playback of a sequence of HTTP-requested short video file fragments, or "chunks." Adaptive HTTP streaming allows the client to request fragments of the same content—a video asset—encoded at different bit rates and resolutions (referred to as "profiles"). In this manner, as network bandwidth changes, the client can download the best possible quality fragment at any point in time.

Several player protocols have been developed for delivering and viewing adaptive streaming including: Apple HTTP Live Streaming (HLS), Microsoft Smooth Streaming (MSS), Adobe HTTP Dynamic Streaming (HDS), and MPEG's Dynamic Adaptive Streaming over HTTP (DASH).

HTTP-based streaming utilizes two types of files in order to accomplish dynamic streaming:

- **Manifest** files—contain metadata that describes the identity and location of all alternate multi-bitrate streams. Client players use manifest files (also referred to as "playlists") to determine information about the content including (but not limited to) available bitrates, codecs, video resolutions, markers, captions, and the location of segments. See Table 3 for a list of supported manifest formats.
- **Content** files—contain the actual video and audio that has been specially encoded in order for the client player to retrieve discrete file segments during playback. See Table 3 for a list of supported content formats.

Table 3. HTTP-based supported manifest & content

Player	Manifest Format	Content Format
HDS	F4M	FMP4
HLS	M3U8	TS
MSS	ISM	ISMC / ISMV
DASH-TS	MPD	TS
DASH-ISO	MPD	FMP4

Video Asset Delivery Methods

Media content can be delivered to customers in two ways: Live or On-demand.

- **Live** Delivery — This method ingests content in either a (stored) file or (live) stream format and delivers that content in real-time to the consumer. An example of live delivery could be either a sporting event (stream) or a network prime time TV show (file). In both cases, the ingest manner is different, but the client has no control of the program; it cannot be paused, stopped, or restarted at will (unless a digital recorder is used).
- **On Demand** Delivery — This method also ingests content in either a file or stream format, however, rather than delivering the content immediately in real-time, it is stored on a server (in file format) and made available for the consumer to watch at some point in the future (otherwise known as Video On Demand, or VOD). The client can start the program playback from the beginning at will, as well as stopping, pausing, or randomly seeking inside the program. An example of VOD content would be services like Netflix or Hulu.

cDVR Terminology

Below are some of the most commonly used cDVR-related expressions that industry professionals use.

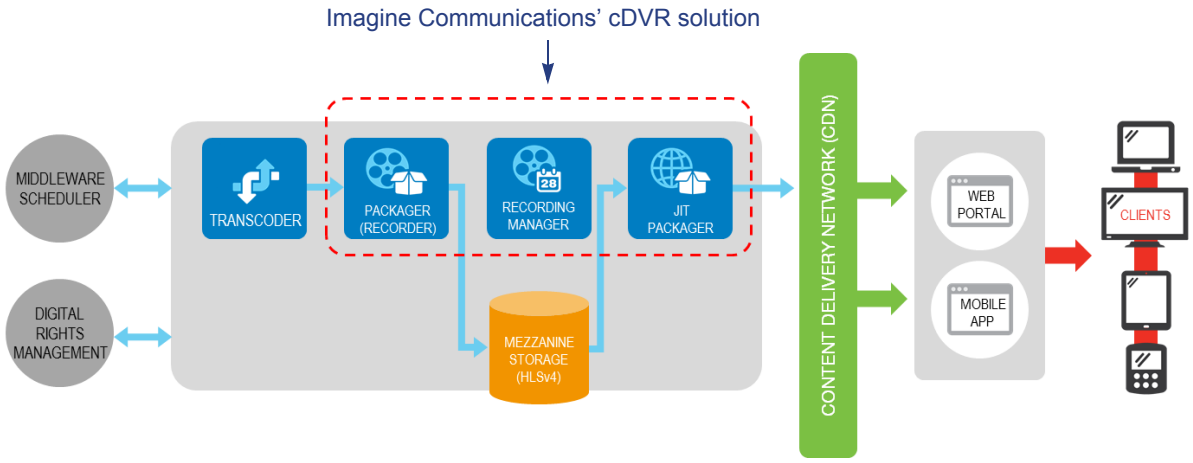
- **Cloud DVR**—the ability for a subscriber to create personal recordings that are saved in the network cloud rather than on the equipment at the subscriber's premises.
- **StartOver**—a subscriber can view a current program from the beginning that has already begun broadcasting, normally initiated from the Electronic Programming Guide (EPG).

- **TimeShift**—a subscriber can scroll back in time within the EPG to view a program that occurred some hours previous (usually limited to 6-8 hours back from the current time).
- **CatchUp**—a subscriber can watch content that has already aired, marked by the operator as "hot" content (usually limited to several programs per day, allowing the user to go back several weeks).
- **Event Based Recording**—start and end times are fixed; a single file asset is stored per event, which cannot be changed following the end of the recording.
- **Continuous Recording (CR)**—recording is abstracted (extracted from the original), which allows start and end times to be edited before, during, and after the recording. Abstracted recording allows for granularity, post-capture modification, and efficient use of storage.
- **Stitching**—when recording programs in CR mode, recordings are abstracted as a collection of video fragments and grouped together ("stitched") to create a single manifest file for requested content.
- **Unique Copy**—multiple recordings are stored and managed on a per subscriber basis, thus allowing each subscriber a private copy of a program.
- **Shared Copy**—a recording is stored and managed one time in order for the same copy to be available for any subscriber requesting it.

Solution Overview

This section provides an overview of all components that are used in a service provider's network when implementing cDVR functionality. The first part of this section describes Imagine Communications' cDVR components; the second part of this section describes additional components required for an end-to-end cDVR network.

Figure 1. cDVR network architecture



Imagine Communications' cDVR Solution Components

The Imagine Communications cDVR solution consists of three primary components:

1. Telurio™ Recording Manager — a GUI-based application that provides a RESTful set of APIs in order for middleware to schedule and playback recordings.
2. **Telurio™ Packager** as **Recorder** — a Packager licensed for recording MBR IDR aligned streams, which creates HLSv4 mezzanine format for delivery to a JITP-ready Packager.
3. **Telurio™ Packager** as **JITP (and Stitcher)**[1] — a Packager licensed for JITP and, in the case of continuous recording, manifest stitching. The JITP server creates ABR-ready chunks for either event-based or continuous recording. For CR, the Stitcher function then creates virtual assets by producing a variant manifest from the correct set of fragmented CR files.

Additional cDVR Components

The components in this section are not part of Imagine Communications' cDVR solution package, but are nonetheless recommended and/or required for an end-to-end cDVR system to function.

- *Middleware Scheduler*—third party application that sits between the EPG and RM. Uses RM API to manage user initiated schedules.
- *Digital Rights Management (DRM) server*—encrypts streams for secure delivery (not required for cDVR, but still recommended).
- *Video Transcoder*—ingests content, prepares audio and video assets for segmentation; this can be Imagine Communications' Selenio TAT, Selenio VMG, or a third party transcoder.
- *Mezzanine Storage*—Storage server for the HLS v4 mezzanine files generated by *Recorder;* this can be either NFS or GPFS format.
- *Content Delivery Network (CDN)*—an aggregation of storage and cache servers that contains content for video providers.
- *Clients*—end user devices that subscribe to and receive video content via set-top box, computer, or mobile devices.

cDVR Features

The following key component features are included as part of this solution:

Recorder

The Recorder provides live-to-file video capture of multi-bit rate (MBR) video. By recording the MBR video and audio of every channel to a mezzanine storage, subscribers have the ability to create personal recording of events in the future or even events that have already occurred in the past.

Since this content is saved as ABR in the network, the play out is available for any multi-screen device.

1. Stitcher is required for CR.

Recording Modes

Two recording modes are offered:

- **Continuous Recording** (CR) — any or all channels are recorded to mezzanine format. Subscribers' events can be abstracted from these recordings and stitched together based on the subscriber start and end times.
- **Event Based Recording** (EBR) — designed for systems in which storage space is constrained, EBR allows subscribers to define what is recorded based on subscriber start and end time.

Recording Function

The Recorder operates as an independent component, which provides the following benefits:

- The JITP output component can scale in a more practical manner;
- End client packaging can utilize more diverse use cases.

Telurio™ Recording Manager

The Telurio Recording Manager (RM) acts as the central management point for the cDVR solution; managing assets, storage, recordings and events.

As users select events to record from their EPG, these selections are routed through the operator's middleware device to the RM. With the RM's easy-to-integrate RESTful APIs, operators are not locked into a single middleware vendor.

Content Storage

By storing the recorded content once in a common format, an overall smaller footprint of storage space is realized. All video, audio and data are captured to ensure the richness of the entire stream is available for packaging to the end client. This single stored format is then packaged on-the-fly based on the client's device as requested.

Since the recorded content is in a common, non-proprietary format (HLSv4), use of the recorded content is not restricted. For those operators concerned with security of the recorded content, the mezzanine content can be encrypted.

Storage Types

Imagine Communications' cDVR solution offers several storage options to meet the various operator preferences:

- GPFS — General Parallel File System
- NFS — Network File System

Just In Time Packaging (JITP) Server

By converting recorded content on-the-fly, the JITP server provides multi-screen playback of the recorded content to whatever client format requested, including: HLS, MSS, HDS and DASH. This playback can be from assets recorded in the past or from live content that has been time-shifted (with an end in the future). Clients can invoke playback modes including pause, fast-forward, and rewind.

Scaling

The architecture of JITP allows the operator to scale to many thousands of simultaneous client requests.

DRM

The JITP server has been integrated with many types of DRM and can extend to other DRM vendors as needed. This capability allows operators to utilize their choice of encryption vendors and technologies.

Functionality Description

This section provides a functionality description of the key cDVR solution features; it is not an all-inclusive list.

Record-level Redundancy

In record-level redundancy, a Primary and Redundant Recorder are configured to provide active-muted redundant recording from the RM. Both Recorders are concurrently recording content received from the transcoder, but only one recording at a time is written to the storage server for JITP delivery. If a Recorder fails to write content to the storage server, then the redundant Recorder will pick up in its place and continue to write the content to the storage server.

Note: *A Recorder is a Packager that is licensed for recording. When you configure the Recorders tab in the RM, you are in effect configuring a specific type of package on a Packager.*

Recording Manager Node-level Redundancy

To allow for the highest level of redundancy which minimizes downtime, Imagine Communications' cDVR solution provides node-level, 1+1 active/standby redundancy for the RM in which an RM redundancy group contains a Primary (or Active) RM and a Standby RM. The redundancy group provides a failover capability from the active RM to the standby RM. Each time the configuration database for the active RM is updated, the standby RM synchronizes its configuration database with the active RM's configuration database.

Recording Manager Storage Management

One of the capabilities of the RM is the ability to manage storage. Operators define storage management parameters based on available disk space and the RM will control the recording and deletion of content accordingly. These parameters include:

- Days to continuously record live channels
- Time to keep unreferenced segments
- Time to keep assets

The Recorder functionality is integrated with key storage technologies as described in the section titled, "Storage Types" on page 20.

RM WebGUI

The RM WebGUI provides the user interface to the RM, Recorder, and JITP server by allowing configuration and monitoring of channels, monitoring managed nodes, and scheduling recording. The RM WebGUI is an integrated interface application that is automatically installed with the RM software image and accessed through the RM IP address. RM also performs cDVR management and configuration of the Recorder and JITP/Stitcher.

Unique and Shared Copy for Continuous Record

In a *shared copy* cDVR environment, a single copy of a recorded program is stored in the network and can be accessed by multiple subscribers. In a *unique copy* cDVR environment, one unique copy of a program is available only to the subscriber requesting it. If two subscribers wish to view the same program, a separate copy (i.e., two copies) must be available for each requesting subscriber. Unique copy allows service providers to deliver cloud-based DVR content to locations in which usage rights require private copies of programming per subscriber.

The RM has the ability to create either shared or unique copy recordings from recordings made continuously.

CHAPTER 3

cDVR Initial Setup

This chapter covers the basic steps required for initializing cDVR, which entails licensing and configuring the Telurio Packagers for their appropriate application (JITP and Recorder), and licensing the Telurio Recording Manager (RM).

In This Chapter:

Prerequisites

Prior to performing initial setup of cDVR, you must have installed the appropriate Packager[1] and RM software applications on your desired target servers. Refer to the *Telurio™ Packager Software Installation and Upgrade Guide* and the *Telurio™ Recording Manager Software Installation, Setup, and Upgrade Guide* for instructions.

Additionally, you must have the appropriate network communication to and from all Imagine Communications cDVR Solution components (RM, JITP, Recorder), as well as communication to and from all other related cDVR nodes, whether Imagine Communications or third party (Transcoder/VMG, Storage Mounts, or Object Store).

Overview

After you have installed the appropriate software onto your servers, you must configure each application with a valid license, and perform basic system configuration for the JITP server and Recorder.

Caution: *Each node in Imagine Communications' cDVR solution requires static IP (not DHCP) address configuration for correct operation. Refer to the Telurio™ Packager Software Installation & Upgrade Guide for instructions on configuring static IP addresses for Packager. Refer to the Telurio™ Recording Manager Software Setup & Upgrade Guide for instructions on configuring a static IP address for an RM.*

1. For JITP and Recorder server applications

Storage Server Configuration

Depending on which type of storage server you are using, additional port configuration may be necessary for the routing devices in your network. Follow the guidelines listed below for the applicable storage server.

NFS Port Configuration

When using NFS as a storage server, the cDVR solution requires that certain ports be available for communication. Table 4 below provides a list of protocols/components and their corresponding communication ports.

Table 4. Communication port usage for cDVR

Application	Communication Direction	Communication Target	Protocol	Port Number
XMLRPC API	Unidirectional	Recording Manager	XMLRPC	80 & 443
Recording Manager	Bidirectional	Recording Manager	UDP Multicast Safenet UDP	9036 12344-12346 5093
Recording Manager	Unidirectional	Recorder	XMLRPC	80 & 443
Recording Manager	Unidirectional	JITP Server (Packager)	XMLRPC	80 & 443
Recording Manager	Unidirectional	NAS-NFS	NFS	NFS
Recorder	Bidirectional	Recorder	UDP UDP Multicast	9047 9036 12344-12346
Recorder	Unidirectional	Recording Manager	XMLRPC	80 & 443
Recorder	Unidirectional	NAS-NFS	NFS	NFS
Origin	Unidirectional	JITP Server (Packager)	HTTP Content served from JITP	80
JITP Server (Packager)	Unidirectional	Recording Manager	XMLRPC Events	80 & 443
JITP Server (Packager)	Unidirectional	NAS-NFS	NFS	NFS

GPFS Storage

When configuring a GPFS storage mount, additional information as described below may be required when setting up a firewall.

Daemon Communication

Daemon communication occurs over port 1191 by default. In general, the default value is used in many GPFS production clusters.

Administrative Communication

GPFS administrative commands may use one or more TCP/IP ports to complete the command. For example, when using standard `ssh`, port 22 used. Additionally, other ephemeral ports (short-lived transport port) are opened for socket connections used to pass data to and from the GPFS daemons.

In some environments you may wish to limit the range of ports that the GPFS administration commands use. This is done by using this GPFS configuration command parameter: `tscCmdPortRange`.

When using the **tscCmdPortRange** command, ensure you configure enough ports to support all of the concurrent commands to or from a node, which will equate to about 20 or more ports.

Additional Information

Additional firewall configuration for GPFS may be found on the IBM developer wiki for GPFS.

Packager Configuration

Each instance of a JITP server and Recorder is, in actuality, a Packager application. Prior to performing any cDVR-related configuration from the RM, you must perform initial configuration and licensing on each Packager. Table 5 below provides a list of required system configuration that must be performed on each Packager, regardless of whether the Packager is used as a Recorder or JITP server.

Packager System Configuration — Required Menus

Table 5 provides a list of system parameters that will need to be configured or verified according to your network-specific parameters via the Packager's interface (GUI or API). Instructions for configuring each of these menus can be found in the *System Configuration* chapter of the *Telurio™ Packager User Guide* (Chapter 4).

Table 5. Required system configuration before configuring packaging

Parameter	GUI Menu / API Call	Requirement
Hostname[a]	sysconfig >> hostname	Optional, but recommended
License key	sysconfig >> license	Required
DNS	sysconfig >> network >> dns	Required
Network interface assignment[b]	sysconfig >> network >> interface >> assignment	Required
Packager IP address	sysconfig >> network >> ip	Required
Network routes	sysconfig >> network >> route	Required
NTP server(s)	sysconfig >> ntp	Optional, but recommended
POIS	sysconfig >> pois	Required if using ad insertion
Syslog server	sysconfig >> syslog	Optional, but recommended

Table 5. Required system configuration before configuring packaging

Parameter	GUI Menu / API Call	Requirement
Timezone	sysconfig >> timezone	Required if not using NTP server
JITP Output Format	configuration >> output >> format >> hls >> modify -> Change version to HLSv4[c]	Required for JITP Packagers only

a. When configuring a hostname for Packager, the hostname *must not* contain any uppercase letters.
b. Two parameters must be configured here: 1) The Management interface (set to eth0 or equivalent) and 2) The External interface (where the video or origin traffic is passed).
c. HLSv4 must be configured **after** the JITP server has been added to the RM database.

Packager Menus Configured by RM

The following GUI menus (or API calls) are configured by the RM and should ***not*** be configured directly from the Packager GUI or via an API call directly to the Packager server. Attempting to change the parameters in these menus without the RM can cause the cDVR network to malfunction.

Table 6. Packager menus that should not be changed in the Packager GUI

Packager Menu Tree / API Call NOT to be modified	Menu Action - OK to use	Menu Action - NOT OK to use
configuration >> audiomap (all)	show	add / modify / remove
configuration >> input (all)	show	add / modify / remove
configuration >> jitp (all)	show	add / modify / remove
configuration >> output >> directory (all)	show	add / modify / remove
configuration >> output >> format (all) — Recorder only[a]	show	modify
configuration >> output >> stream (all)	show	add / modify / remove
configuration >> package (all)	show	add / modify / remove
configuration >> session (all)	show	abort
configuration >> stitcher (all)	show	add / modify / remove
sysconfig >> config (all)	backup / backupfile	reset, restore
sysconfig >> database (all)	show	set
sysconfig >> defaults (all)	show	add / modify / remove
sysconfig >> ingestproxy	none	not used as part of cDVR; do not configure.
sysconfig >> keyserver (all)	show	add / modify / remove
sysconfig >> policy	show	set
sysconfig >> system	show	lock, restart, unlock

a. Modifying output formats is not allowed for Recorder; however, it is allowed for the JITP server

Installing the Packager License

Each instance of a JITP server and Recorder requires a separate, application-specific license. Each Packager appliance has a built-in License Server that manages licenses for packaging. If desired, Packager can use an external License Server; in this case, you must configure the Packager to point to

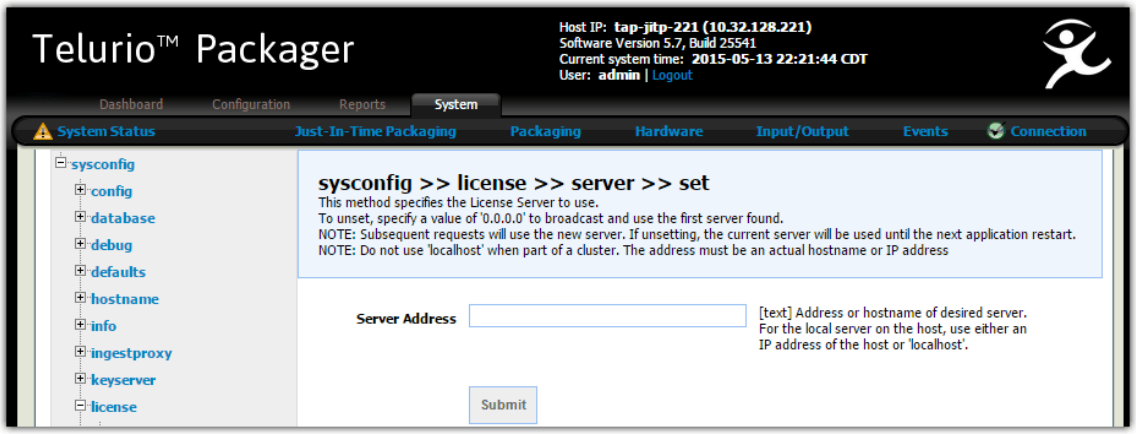
the IP address or host name (DNS name) for the external server where the Licensing Application is installed.

For a Packager appliance that leverages the localhost License Server, you must upload a new license key file to update licensing for the Packager.

Note: *Using the Packager as its own license server (localhost) is the most typical method of licensing.*

To install a Packager license, proceed as follows:

1. Log into the GUI by navigating to the Packager's IP address.
2. Enter the username and password for access (default is `admin/ripcode!`)
3. From the **System** tab, click through to **sysconfig >> license >> lockcode >> show**.
4. Copy the **Lockcode** field entry and contact Imagine Communications Customer Support for further instructions on receiving a license key.
5. After obtaining the license key from Imagine Communications, return to the Packager GUI.
6. From the **System** tab, click through to **sysconfig >> license >> server >> set**.
7. In the **Server Address** field, enter either the remote license server IP address or, if using the Packager as its own license server, enter the Packager's own IP address[2]



8. Click **Submit** to save changes.
9. From the **System** tab, click through to **sysconfig >> license >> update**.
10. In the **License File URL** field, enter one of the following, depending on what kind of license server you are using:
    - The full HTTP or TFTP URL to the remote license key file. For example:
      `http://remotehost/path/to/licenseFile.key`
      `tftp://remotehost/path/to/licenseFile.key`
      -or-
    - A path to a file located on the localhost using the following format: `file://<full path>`. For example:
      `file:///opt/path/licenseFile.key`
      -or-

2. Alternatively, you may enter "localhost" instead of the Packager's IP address; however, we recommend using the IP address instead.

- The actual license key strings as received from Imagine Communications (copying and pasting is recommended).

11. Click **Submit** to save changes and apply the new license.
12. Perform the steps in this section for every Packager within your cDVR system.

Note: *Each Packager requires its own license, regardless of redundancy or load balancing. For example, if you have two Recorders operating in 1+1 redundancy, two JITP-only servers, and 2 JITP-with-Stitcher servers, you will need a total of six (6) Packager licenses: 2 for Recorder, 2 for JITP only, and 2 for JITP+Stitcher.*

Viewing Packager Licensing

You can see which type of licensing the Packager has based on whether it has been licensed for Recorder, JITP, or JITP with Stitcher.

From the **System** tab, navigate to **sysconfig >> license >> show**, and click **Submit**.

Results will appear similar to the following:

Note: *In a typical network deployment, License Key Features will generally be for either JITP only or for Recorder only. The graphic below shows both JITP and Recorder licenses together for simplicity.*

License Key Features

Feature	Count/Limit	Type/Supported	Expiration Date	Remaining Trial Period	
ADOBE		enc Trial	Thu Jul 9 23:59:59 2015		
ADOBE FLASH ACCESS		enc Trial	Thu Jul 9 23:59:59 2015		
HLS		enc Trial	Thu Jul 9 23:59:59 2015		
JITP MAX SESSIONS	100	count Trial	Thu Jul 9 23:59:59 2015		← JITP only
LIVE STRM		enc Trial	Thu Jul 9 23:59:59 2015		
MAX OUTPUT STRM	200	count Trial	Thu Jul 9 23:59:59 2015		← Recorder only
MAX RECORD	100	count Trial	Thu Jul 9 23:59:59 2015		
MAX STITCH	100	count Trial	Thu Jul 9 23:59:59 2015		← JITP only
MPEGD		enc Trial	Thu Jul 9 23:59:59 2015		
Packager	1	Token Trial	Thu Jul 9 23:59:59 2015	Calendar: 345 days	
SS		enc Trial	Thu Jul 9 23:59:59 2015		
VOD		enc Trial	Thu Jul 9 23:59:59 2015		

Additional Packager Licensing Information

For additional details on installing, viewing, and testing Packager licensing, please refer to the *Telurio™ Packager User Guide, Release 5.7*.

Using Recorder for EBR vs. CR

If you are planning to use the same Recorder for both event-based recording (EBR) and continuous recording (CR), please note that the RM will set the output format to HLS version 4 so as to accommodate CR. If you wish to change the output format to something else for EBR, the following two rules should be followed when configuring a Recorder:

- Use separate Packagers for EBR and CR, -and-

- Do not change anything in the **configuration >> output >> format >> hls** menu of the Packagers.

Note: *For HLS output, a Packager, whether it is operating as a Recorder or a JITP server, can output either only HLSv2 or only HLSv4, but not both versions at the same time.*

RM Licensing

The *RM* has a built-in License Server that manages licenses for management. If desired, the *RM* can use an external License Server; in this case, you must configure the RM to point to the IP address or host name (DNS name) for the external server where the Licensing Application is installed.

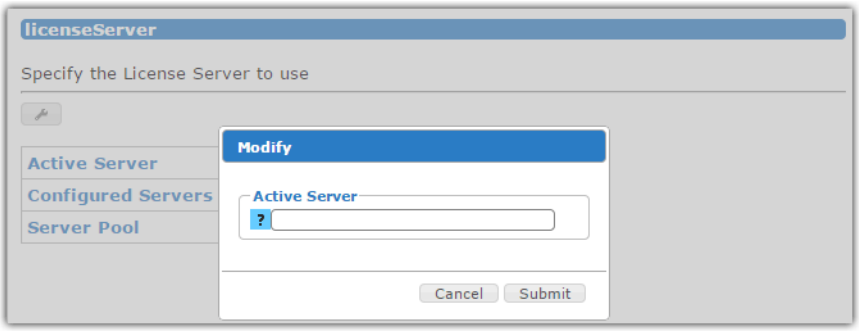
For an *RM* application that leverages the localhost License Server, you must upload a new license key file to update licensing for the *RM*.

Note: *Using the RM as its own license server (localhost) is the most typical method of licensing.*

Installing the RM License

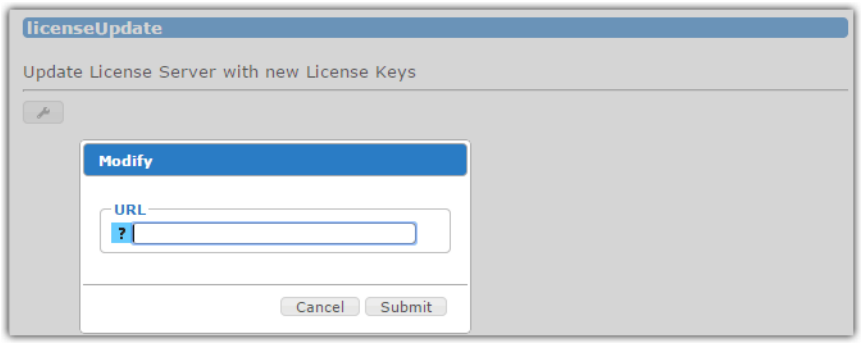
To install a RM license, proceed as follows:

1. Log into the GUI by navigating to the *RM's* IP address.
2. Enter the username and password for access (default is `admin/ripcode!`)
3. From the **System** tab, click the triangle symbol next to the **Licensing** container to expand the menu.
4. Click on **Lock Code**.
5. From the *license Lockcode* menu, copy the contents of the **Lock Code** field entry and contact Imagine Communications Customer Support for further instructions on receiving a license key.
6. After obtaining the license key from Imagine Communications, return to the expanded **Licensing** container in the RM GUI.
7. Click on **Server**.
8. Click the icon to bring up the *Modify* window..



9. In the **Active Server** field, enter either the remote license server IP address or, if using the RM as its own license server, enter the RM's own IP address[3].
10. Click **Submit** to save the new license server.
11. From the **Licensing** container, click on **Update**.

12. Click the icon to bring up the *Modify* window.



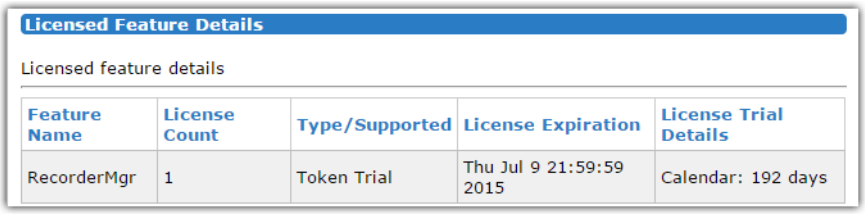
13. In the **URL** field, enter one of the following, depending on what kind of license server you are using:
    - The full HTTP or TFTP URL to the remote license key file. For example:
      `http://remotehost/path/to/licenseFile.key`
      `tftp://remotehost/path/to/licenseFile.key`
      -or-
    - A path to a file located on the localhost. For example:
      `/root/path/licenseFile.key`
      -or-
    - The actual license key strings as received from Imagine Communications (copying and pasting is recommended).
14. Click **Submit** to save changes and apply the new license.
15. If you are using RM 1+1 node-level redundancy, perform the steps in this section for both RMs that will be in the redundancy group.

Viewing RM Licensing

You can view RM licensing details as follows:

From the **System** tab, click the triangle symbol next to the **Licensing** container to expand the menu, then click **Details** to view the *Licensed Feature Details* contents.

Results will appear similar to the following:



3. Alternatively, you may enter “localhost” instead of the RM’s IP address; however, we recommend using the IP address instead.

What Next?

Now that you've performed initial configuration and licensing for your cDVR components, proceed to Chapter 5, "Recording Manager GUI Overview" to get familiar with the RM GUI.

CHAPTER 4

RM Redundancy Setup

This section describes how to set up two RMs to operate in node-level 1+1 active/standby redundancy. If you are not using RM redundancy in your deployment, you may skip this chapter and proceed to Chapter 5, *Recording Manager GUI Overview* on Page 39.

In This Chapter:

Prerequisites

In order to set up RM redundancy, you must have installed the RM software application on both devices meant to be redundant. (Refer to the RM Installation & Upgrade Guide for instructions.)

Networking Requirements

In order to configure RM node redundancy you must ensure the two target RMs can communicate multicast management traffic to each other.

Caution! RM *redundancy uses the multicast address of 225.0.0.38 for all redundancy communication. This multicast IP address should not be changed*[1] *on* RM. *As such if your WAN-based network routers are not configured to pass multicast traffic (the default) then you must manually configure all relevant interfaces on the router(s) to pass the 225.0.0.38 multicast address.*

Unicast over port 9036 is used for initial setup exchanges between RMs*, however, ongoing redundancy communication is performed through multicast over ports 12344-12346. For more information on communication protocols and their respective ports, refer to* "Storage Server Configuration" on page 24.

1. If your network configuration requires the use of a different multicast IP address, please contact Imagine Communications Customer Support for further instructions. See "Contacting Customer Support" on page 157.

Gateway Route Rules

In order for multicast messages to pass between the redundant RMs, the correct route tables must be configured. If you configured the redundant RMs with a static IP address (rather than the default DHCP configuration), you most likely configured a gateway IP address during the OS installation process. However, this did not automatically configure a default gateway. Rather, it was used to configure various internal network tables. In instances where multiple Ethernet interfaces[2] are available for a given RM, Imagine Communications recommends that you manually configure a default gateway in order to pass multicast traffic between redundant RMs.

Configuring a default route can be done in one of two ways: set a default route for both *Recording Managers* (recommended), or add a static route for both. Both methods are described below:

Option 1: Set Default Routes on both RMs (Recommended):

1. In both RMs' GUI, click the **System** tab and click through to **Network > IP > IP Address Configuration**.
2. Click the wrench ( ) icon next to the entry for the appropriate Ethernet interface.
3. In the **Mode** field, select **Default Gateway**.
4. A new field called **Gateway Address** will appear; enter the IP address of each respective device's default gateway IP address.

   Example: If RM-A's IP address is 10.10.10.15 with a 16-bit mask, its default gateway will most likely be 10.10.0.1. If RM-B's IP address is 192.168.30.150 with a 24-bit mask, it's gateway IP address will most likely be: 192.168.30.1.

5. Click **Submit**.
6. Restart the IP services for both RM's via the **System** tab **> Network > IP > IP Restart** menu.

Option 2: Configure a Static Route on both RMs:

Note: *This option should only be used to configure static routes, not the default gateway.*

1. In both RMs' GUI, click the **System** tab and click through to **Network > Routes** and click the plus ( ) icon to add a route.
2. Enter the destination *multicast* subnet address in the **Destination** field. (For example, this address could be 225.0.0.38)
3. Enter the subnet mask for the destination subnet in the **Mask** field. (For example, this address could be 255.255.255.255)
4. Enter the gateway IP address to use for the subnet in the **Gateway** field. Leave this field blank to use the default gateway.

Note: *For multicast addresses, the Gateway field must always be left blank.*

5. From the **Interface** drop-down box, select the appropriate target interface[3].
6. Click **Submit**.

2. If you have only one Ethernet interface on the system hosting the RM application, explicitly setting a default gateway is not required. With multiple interfaces, however, the OS setup process will automatically setup a default gateway on the first Ethernet interface it finds. As such, if the interface you wish to use is not the first one the OS finds, not having an explicit default gateway set up for the desired interface may prevent communication between RMs.

Special Notes on Routes

- Imagine Communications' multicast management traffic (used for redundancy management) is sent to the multicast group on 225.0.0.38.
- If the default gateway that you configured in *Option 1* was for an interface other than what is assigned as the management interface, then *Option 2* must also be used to configure an entry for 225.0.0.38 on the management interface.

Caution! *If more than one interface is configured and the management interface does not have a default gateway configured, without adding the 225.0.0.38 address to the management interface the redundancy multicast management traffic will use the interface containing the default gateway instead of the management interface, which will cause redundancy to fail.*

For more information on communication protocols and their respective ports, refer to "Storage Server Configuration" on page 24.

Redundancy Configuration Instructions

Perform the steps in this section ***from only the Primary RM***. You do not need to perform any steps from the Standby RM, except to verify settings.

Log In to Primary RM

1. Open a *Firefox* or *Chrome* web browser from a management computer that has access to the *Recording Manager*.
2. Navigate to the physical IP address of the RM that will start as the primary. This will be the group master as long as it's active.
3. Log in with the credentials: `admin/ripcode!`

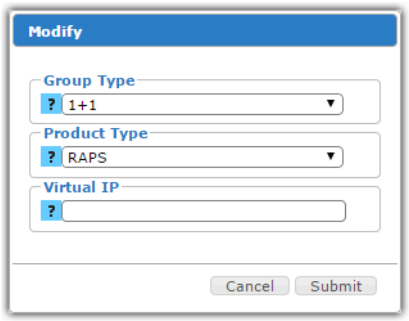
Configure Redundancy Group Details

4. Click the **System** tab.
5. Click the triangle [▶] symbol next to the **Redundancy** container to expand the menu, then click on **Group**.

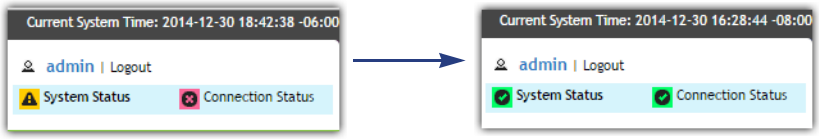
3. For multicast management traffic, RM expects to communicate over the currently configured management interface. Usually this defaults to *eth0*, however, the name of this interface depends upon the particular hardware in use.

6. Click the wrench [ ] icon to bring up the *Modify* window.

   The **Group Type** and **Product Type** menus are preselected for *1+1* and *RAPS* respectively as shown below. :



7. In the **Virtual IP** field, enter the virtual IP address that will be assigned to both the Primary and Standby RMs.
8. Click **Submit** to save and add the redundancy group.
9. Confirm the *Connection Status* icon in the top right corner of the GUI changes from red to green (response time should be less than a minute).

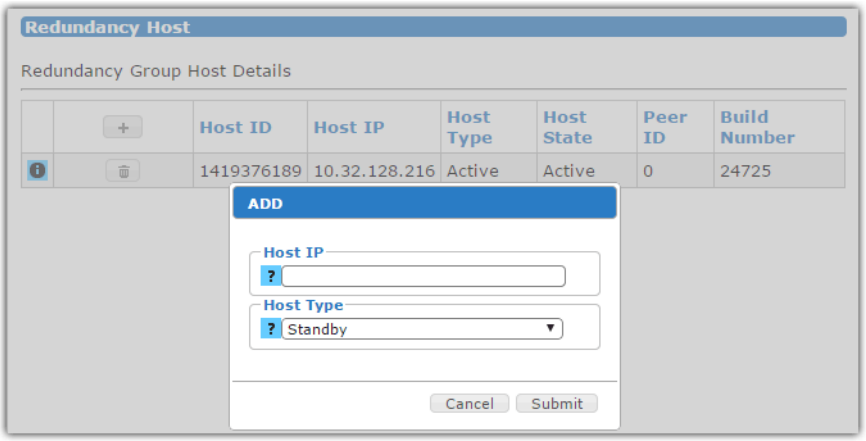


Note: *Once you have configured a redundancy group from the physical IP address of the master RM, all further configuration, including the section below, should be performed via the GUI of the VIP which you set in Step 7 above.*

Add Standby Host from Primary RM

10. Log in to the VIP address of the redundancy group.
11. From the **System** tab of the VIP RM, click the triangle [▶] symbol next to the **Redundancy** container to expand the menu, then click on **Hosts**.
12. From the *Redundancy Host* menu, click the plus (+) icon to add a host entry (the Primary host entry will already be present).

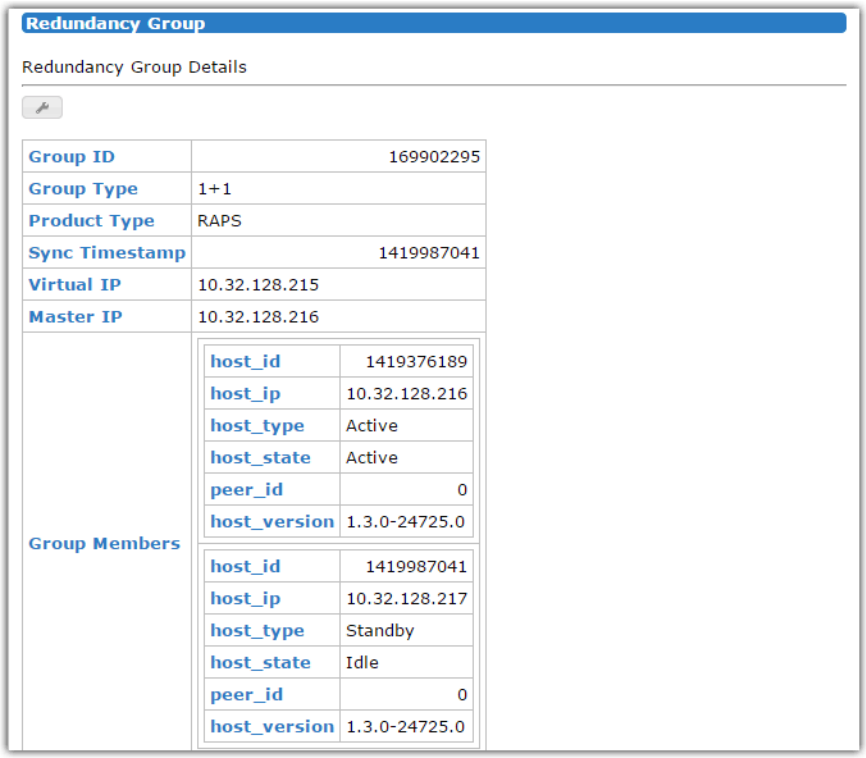
    The ADD menu will open.



13. In the **Host IP** field, enter the IP address of the Standby RM.
14. The **Host Type** drop-down menu should already be preselected to *Standby*.
15. Click **Submit** to save and add the Standby RM to the redundancy group.

Verify Redundancy

16. From the **System** tab, click the triangle [▶] symbol next to the **Redundancy** container to expand the menu, then click on **Group**.



17. Verify the **host_type** and **host_state** for the Primary RM show *Active/Active* as their entries.
18. Verify the **host_type** and **host_state** for the Standby RM show *Standby/Idle* as their entries.

Redundancy States (More Information)

For more information on the redundancy states and their meanings, refer to the section titled, "Redundancy Tree" on page 143.

Removing RM Redundancy

There are two levels of redundancy removal, depending on whether you wish to remove only the standby host, or redundancy altogether.

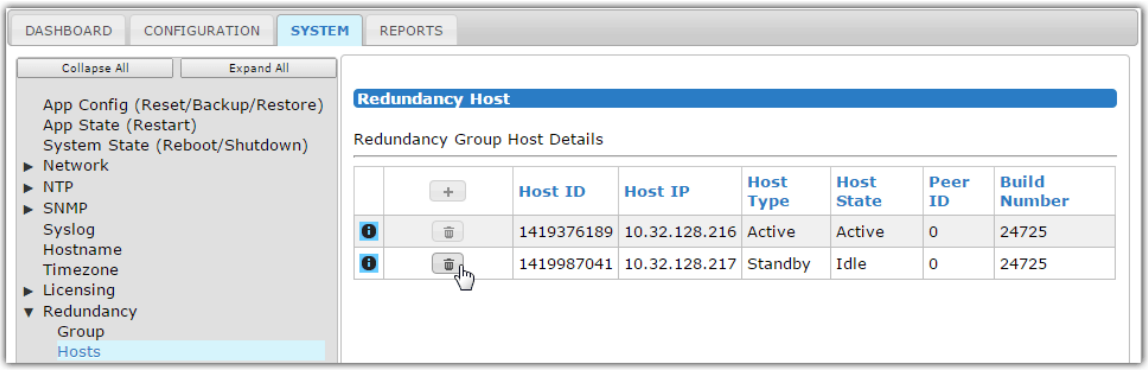
Note: *When performing any redundancy removal actions, whether removing a host from the group or the group itself, all actions are performed from the Active RM. No actions are required from the Standby RM.*

Remove Standby Host from Redundant Group

In certain upgrade, downgrade, or configuration situations, you may be required to remove the standby RM while keeping the redundancy group intact. For example, you may wish to make a standby RM a standalone RM or you wish to make a standby RM part of a different redundancy group.

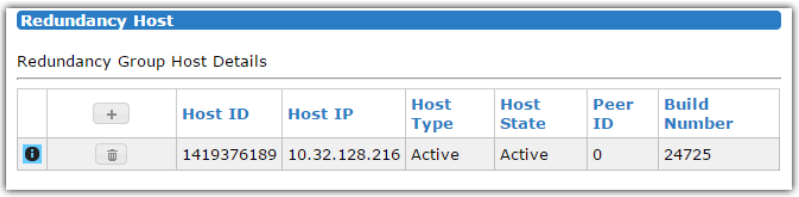
To remove only the standby RM, proceed as follows:

1. Log in to the ***Active*** *or* ***VIP*** RM.
2. From the **System** tab, click the triangle [▶] symbol next to the **Redundancy** container to expand the menu, then click on **Hosts.**
3. Locate the row entry in which the **Host Type** indicates **Standby** and click the trash (🗑) icon.



4. From the confirmation pop-up box, click **Delete** to confirm.

   The resulting **Redundancy Host** menu should now show only the Active RM as a host.



Note: *Once the Standby RM has been removed from the redundancy group, the Standby (now a standalone) will not be accessible until its services restart—about 30 seconds.*

Remove Redundancy Group

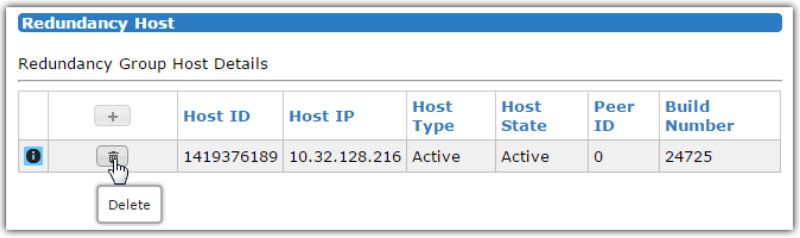
In certain upgrade, downgrade, or configuration situations, you may be required to completely tear down redundancy between two RMs. Tearing down redundancy means removing both the standby host and the redundancy group itself, thus leaving no trace of redundancy on either system.

To remove the redundancy group from the RM, proceed as follows:

1. Log in to the ***Active*** RM (**not** the VIP).
2. Remove the *Standby* host first as described in the previous section, "Remove Standby Host from Redundant Group" on page 37.

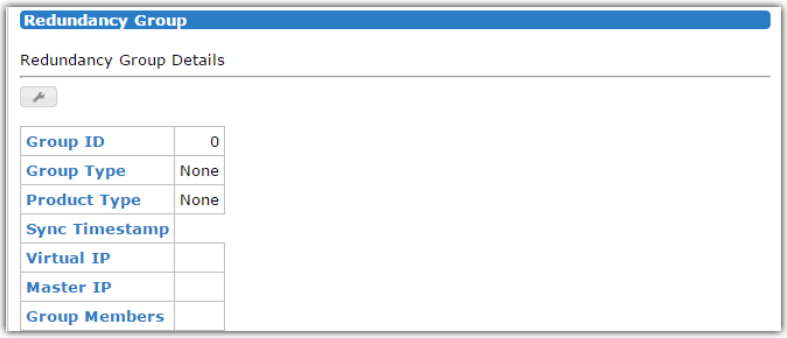
Caution: *You cannot remove an active redundancy host without first removing the standby host.*

3. From the **System** tab, click the triangle [▶] symbol next to the **Redundancy** container to expand the menu, then click on **Hosts.**
4. Select the row entry in which the **Host Type** indicates **Active** (which should be the only entry in the list) and click the trash ( ) icon.



5. From the confirmation pop-up box, click **Delete** to confirm.

   Navigating to the *SYSTEM* > *Redundancy* > *Group* menu should show empty fields from the **Redundancy Group** status menu.



What Next?

Now that you've performed redundancy configuration for your cDVR components, proceed to Chapter 5, "Recording Manager GUI Overview" to familiarize yourself with the RM GUI.

CHAPTER 5

Recording Manager GUI Overview

The Recording Manager (RM) GUI is the user interface for configuring and monitoring all RM components, including: node configuration, system configuration, channel management, event-based and continuous record, and alarm and event monitoring.

This chapter provides an overview for navigating the RM GUI interface.

In This Chapter:

Prerequisites

Before you can use the RM GUI you must have performed the procedures described in Chapter 3, "cDVR Initial Setup" and Chapter 4, "RM Redundancy Setup".

Launching RM

The RM GUI is installed with the RM server software and can be accessed by navigating to the RM's IP address from a standard *Firefox* or *Chrome* web browser.

Logging In to the RM GUI

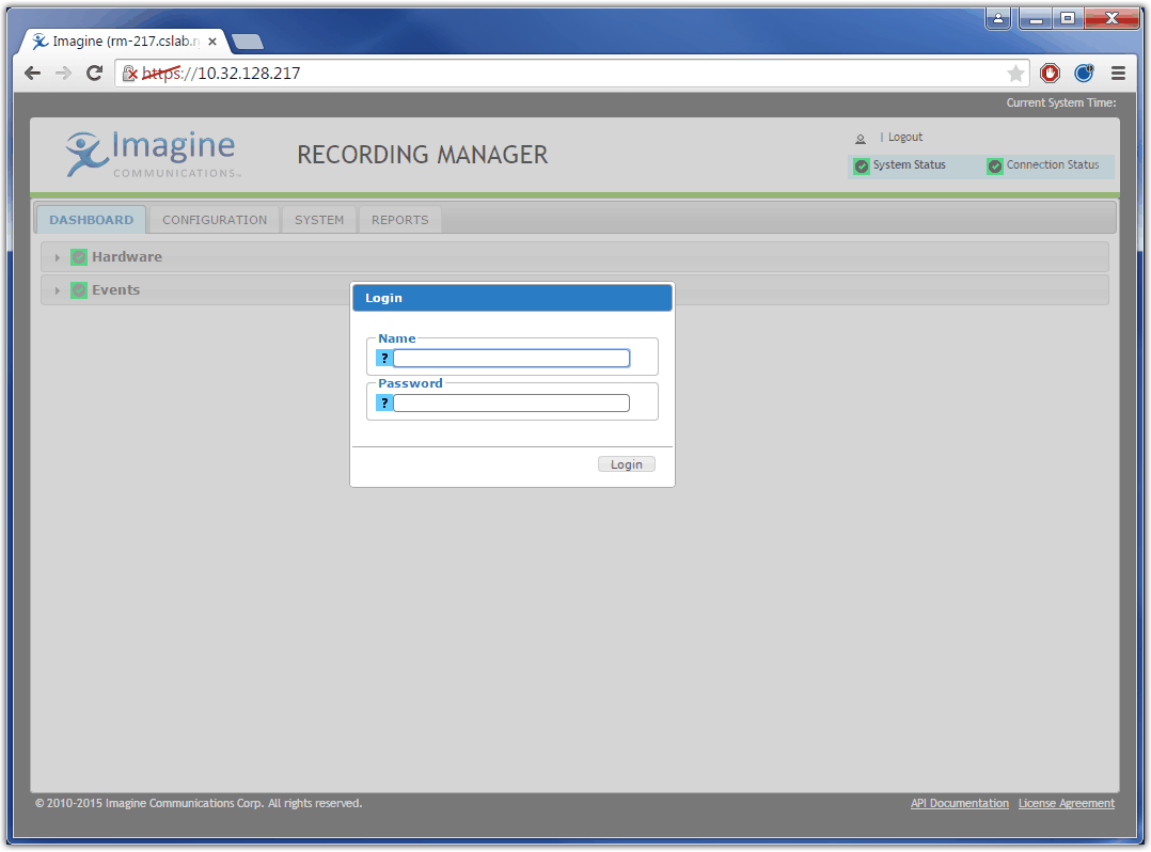
To log in to the GUI, you will need the IP address of the RM.

1. From a *Firefox* or *Chrome* browser, navigate to the RM's IP address.

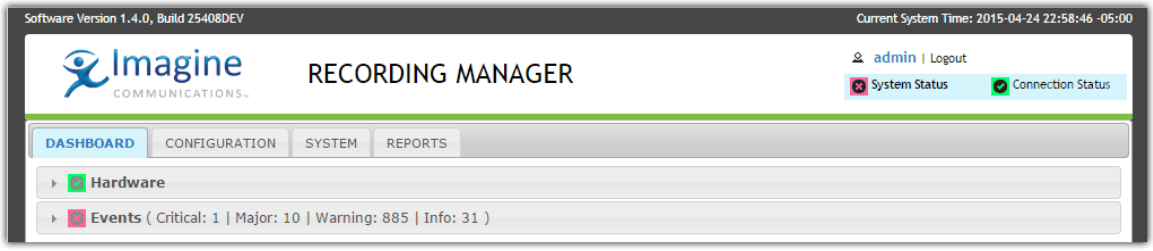
Note: *If you configured 1+1* RM *redundancy, log in using the VIP.*

2. Enter the default **Username** and **Password** as follows:

   Username: `admin`
   Password: `ripcode!`



Upon successful login, the RM GUI opens at the **Dashboard** tab:



Understanding RM Tools

Numerous tools are built into the RM interface to simplify configuration, management, and monitoring of the RM and Recorder components. This section describes the overall GUI, screen components, colorization, and icons. The following topics are covered:

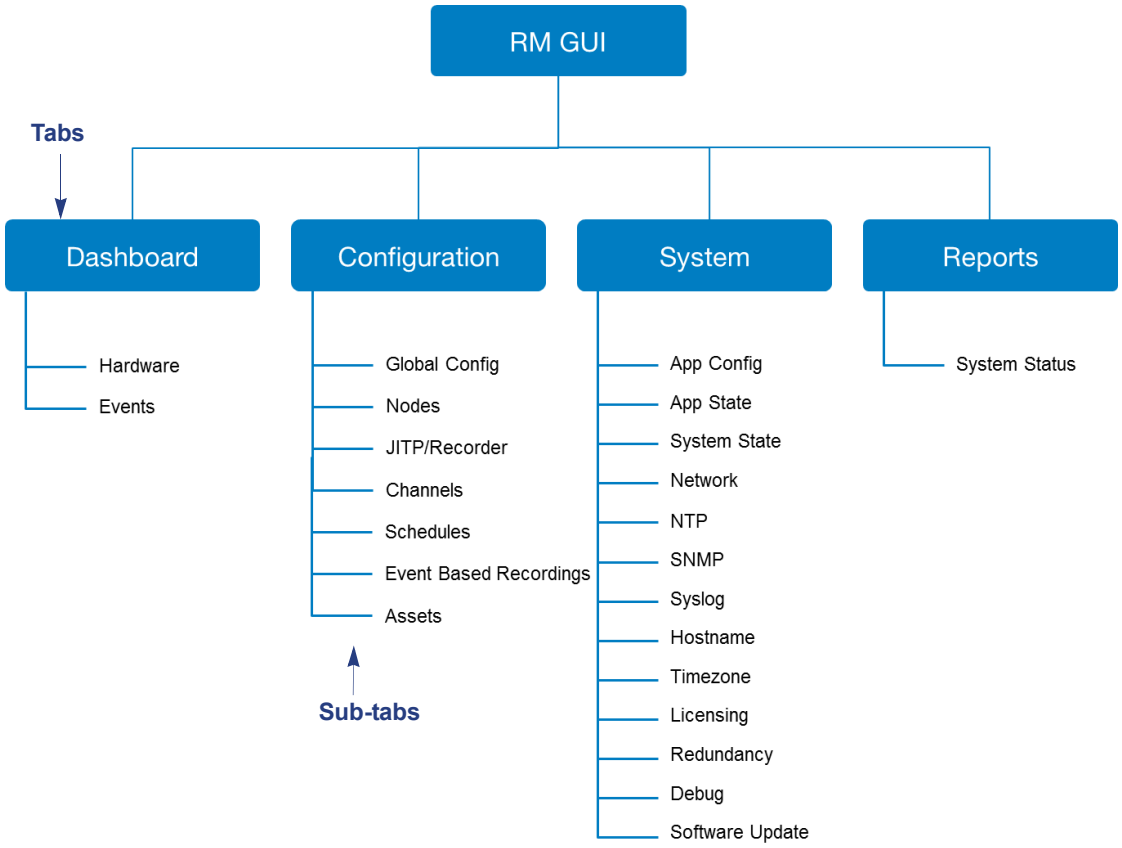
- RM GUI Hierarchy
- Navigating the RM GUI

RM GUI Hierarchy

The RM GUI is organized in a tab-to-container and tree-branch fashion, where the major configuration and monitoring functions are separated in tab-based menus that further drill down to nested or tree/branch containers.

Figure 2 below provides a quick snapshot of the overall RM menu hierarchy.

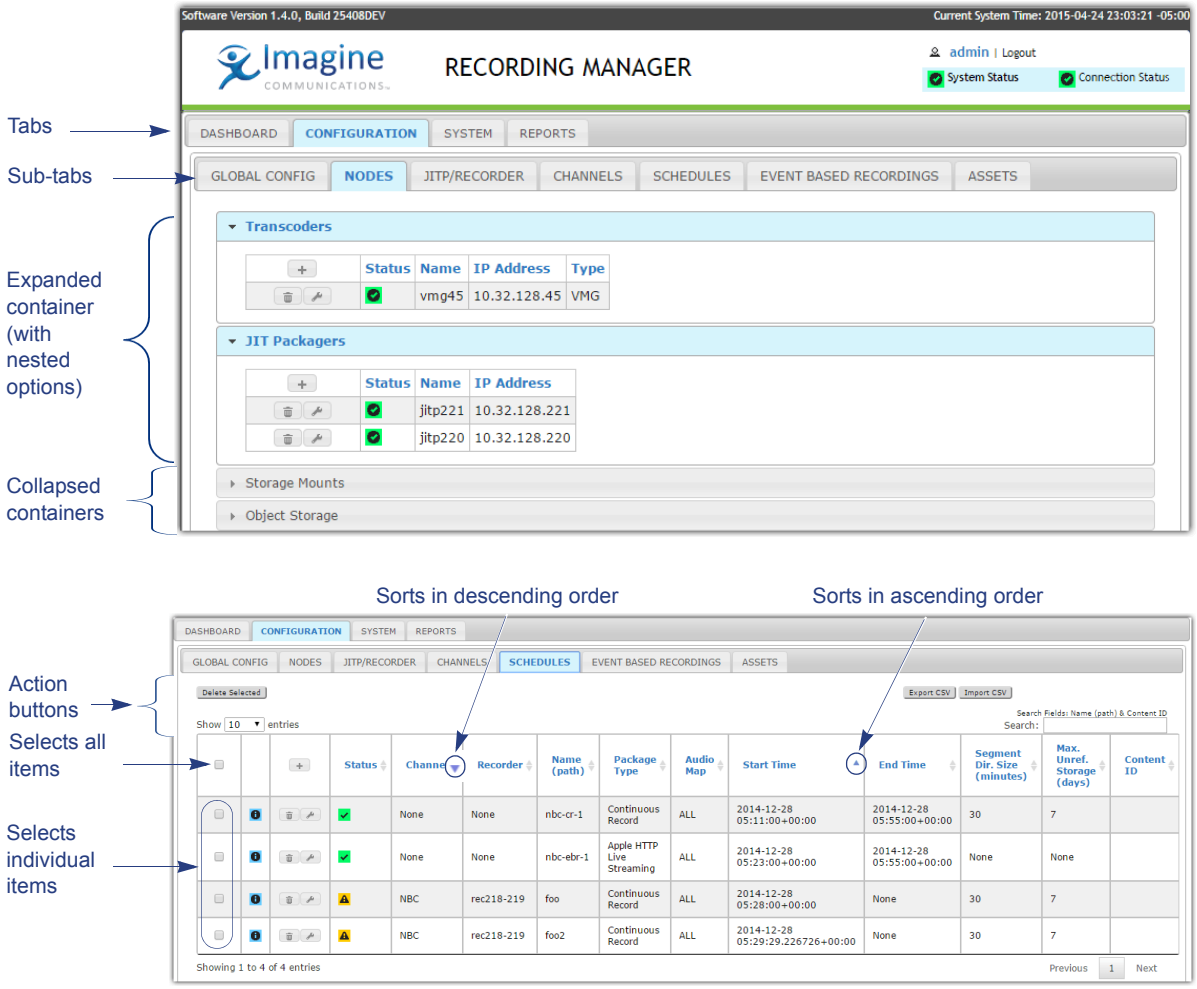
Figure 2. RM Hierarchy



Navigating the RM GUI

The RM GUI has several screen components to enable quick navigation and immediate system status. Figure 3 below provides an overview of the GUI's basic navigation tools.

Figure 3. GUI Navigation Tools



Icons and Buttons

The RM GUI makes use of several graphic and text based icons and buttons to easily convey status and actionable items. In general, an icon will display a status of some sort while a button or check-box provides the ability to make a change to the system.

Table 7 provides a description and general legend of each status icon and action button.

Table 7. Icon and Button Meanings

Symbol	Applies to:	Meaning
	General system NODES tab SCHEDULES tab ASSETS tab	**General system**—connectivity status to RM and hardware is good. **NODES**—status of node is good. Good connectivity, responsive to status checks. **SCHEDULES**—schedule is currently running. **ASSETS**—several states are conveyed with this icon: a) asset is currently in the process of being created; b) asset initialization success; c) a request for an immediate copy has successfully started; d) a scheduled copy has started successfully.
	General system NODES tab SCHEDULES tab ASSETS tab	**General system**—there are unacknowledged system errors of at least a Warning level, or there is a hardware-related warning. **NODES**—some sort of connectivity to a node may have failed or a redundancy failure has occurred. **SCHEDULES**—schedule has been set, but there is an error, or the schedule is attempting to run again. **ASSETS**—partial success in asset creation or another type of warning.
	General system NODES tab SCHEDULES tab ASSETS tab	**General system**—several states are conveyed with this icon: a) connectivity to RM has failed, b) hardware failure, or c) a critical alarm has occurred and has not been acknowledged. **NODES**—connectivity to node has failed. **SCHEDULES**—the schedule failed to run. **ASSETS**—asset failed to launch or failed to complete successfully.
	General system, all tabs	**General system & all tabs**—indicates more information is available for the status or configuration parameter of a particular item. Clicking on the icon will open a dialog box with more information.
	General system, all tabs	**General system & all tabs**—mousing over the question mark will open a tool tip for additional configuration help.
	SCHEDULES tab ASSETS tab	**SCHEDULES**—schedule has been completed. **ASSETS**—asset creation has been completed.
	ASSETS tab	ASSETS—when using PRIVATE copy, this icon indicates the private copy asset is complete, but there is a problem (either the copy failed or otherwise had issues).
	SCHEDULES tab ASSETS tab	**SCHEDULES**—schedule start is pending. **ASSETS**—asset creation is pending.
	SCHEDULES tab	**SCHEDULES**—schedule is marked for imminent deletion.
	SCHEDULES tab	**SCHEDULES**—schedule is either starting or stopping.

Table 7. Icon and Button Meanings

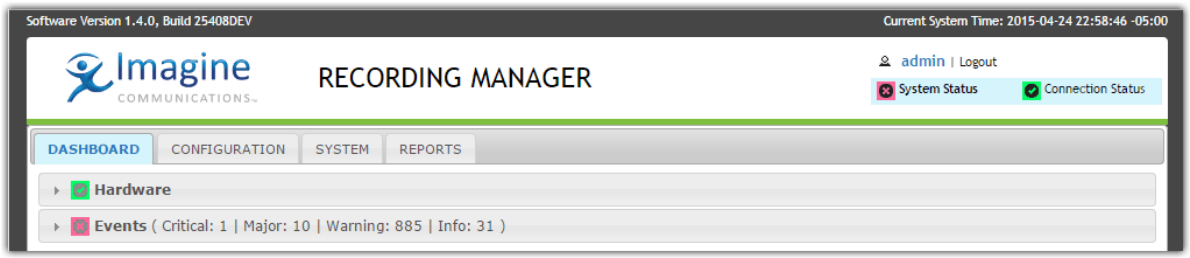
Symbol	Applies to:	Meaning
	DASHBOARD tab CONFIGURATION tab (sub tabs: GLOBAL, NODES, JITP/ RECORDER, & CHANNELS)	Clicking on the triangle or the container name will expand the menu out one level for additional configuration or information.
	SYSTEM tab REPORTS tab	Clicking directly on the triangle next to the menu tree will expand the menu out one level.
	All menus	Clicking this button opens a pop-up window to modify existing configuration.
	All menus	Clicking this button causes a command to be executed, such as a backup, a restart, or polling for information.
	All menus	Clicking this button adds a new row entry to the tree or branch category.
	All menus	Clicking this button deletes an existing row entry from the tree or branch category.

Tab Overview

There are four main tabs available in the RM GUI which allow you to configure and monitor the cDVR components: *Dashboard*, *Configuration*, *System*, and *Reports*. These tabs are briefly referenced here and are discussed in detail in the subsequent chapters of this user guide.

Dashboard

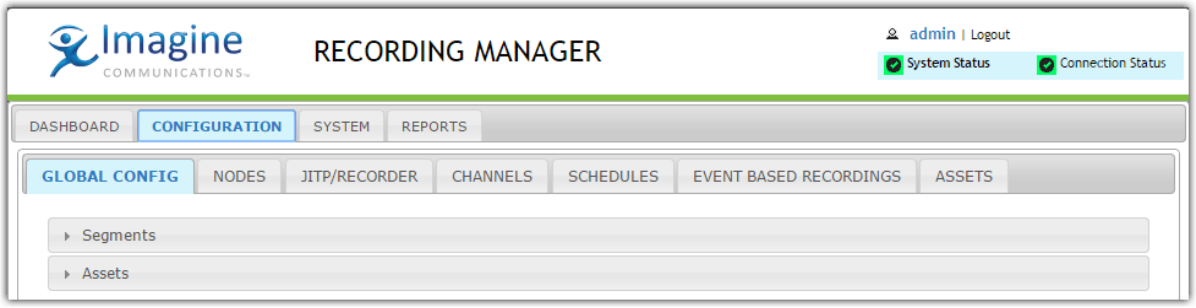
The **DASHBOARD** tab provides a snapshot view of the hardware status for the RM and cDVR-related events.



Configuration

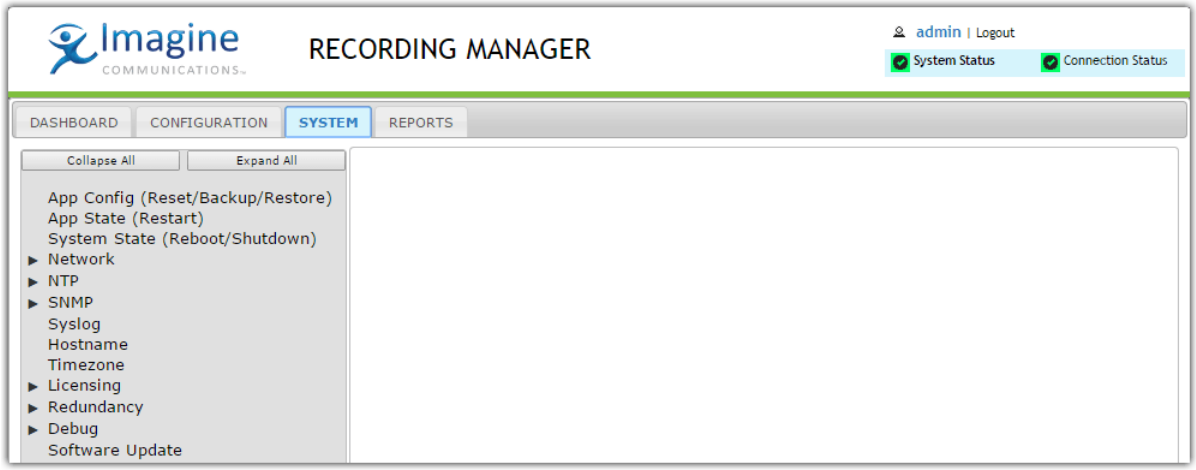
The **CONFIGURATION** tab is where you will do most of your cDVR provisioning, including global recording parameters, node setup, channel configuration, and recording scheduling. The tab includes

the following sub-tabs: *Main*, *Nodes*, *JITP/Recorder*, *Channels*, *Scheduler*, *Event Based Recordings*, and *Assets*.



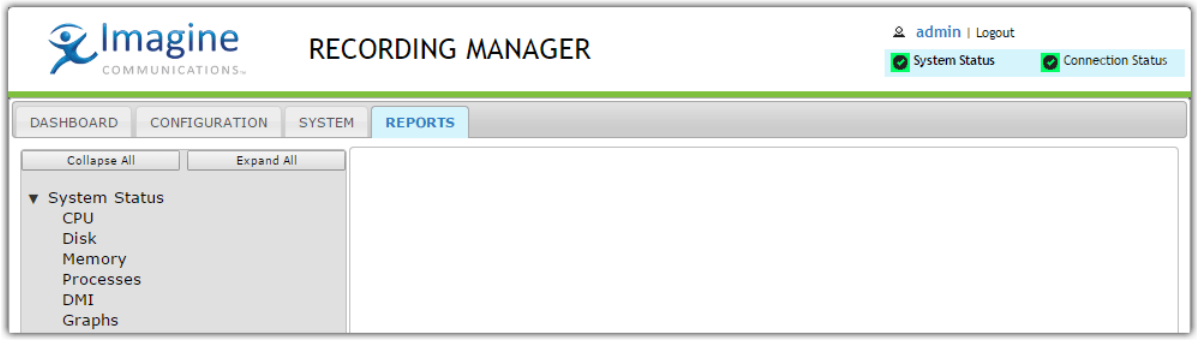
System

The **SYSTEM** tab provides functions related to maintaining and configuring RM system parameters. From here you can perform actions such as setting up network parameters, timezones, redundancy, and licensing; you can manage the RM database and services, and you can view and update software, in addition to other system-related setup.



Reports

The **REPORTS** tab displays capacity and statistical information about the RM, such as CPU, memory, and disk capacity, processes status, and additional information provided in graph format.



What Next?

The remaining chapters of this user guide provide detailed information about each RM tab and sub-tab, including explanations of each field or set up parameter.

For steps on how to set up an Imagine Communications cDVR system from beginning to end, refer to the *cDVR Quick Start Guide* for this release.

CHAPTER 6

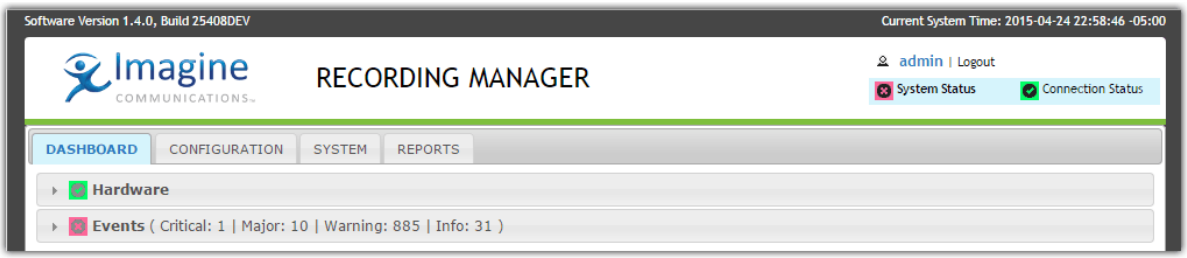
Dashboard

This chapter describes the **Dashboard** tab of the RM GUI, which can be accessed by logging in to the RM as described in the section titled, "Launching RM" on page 40.

In This Chapter:

Dashboard Overview

The ***RM* GUI Dashboard** tab presents information for Hardware and Events. Each container can be expanded or collapsed by clicking on the triangle next to the title of each section.



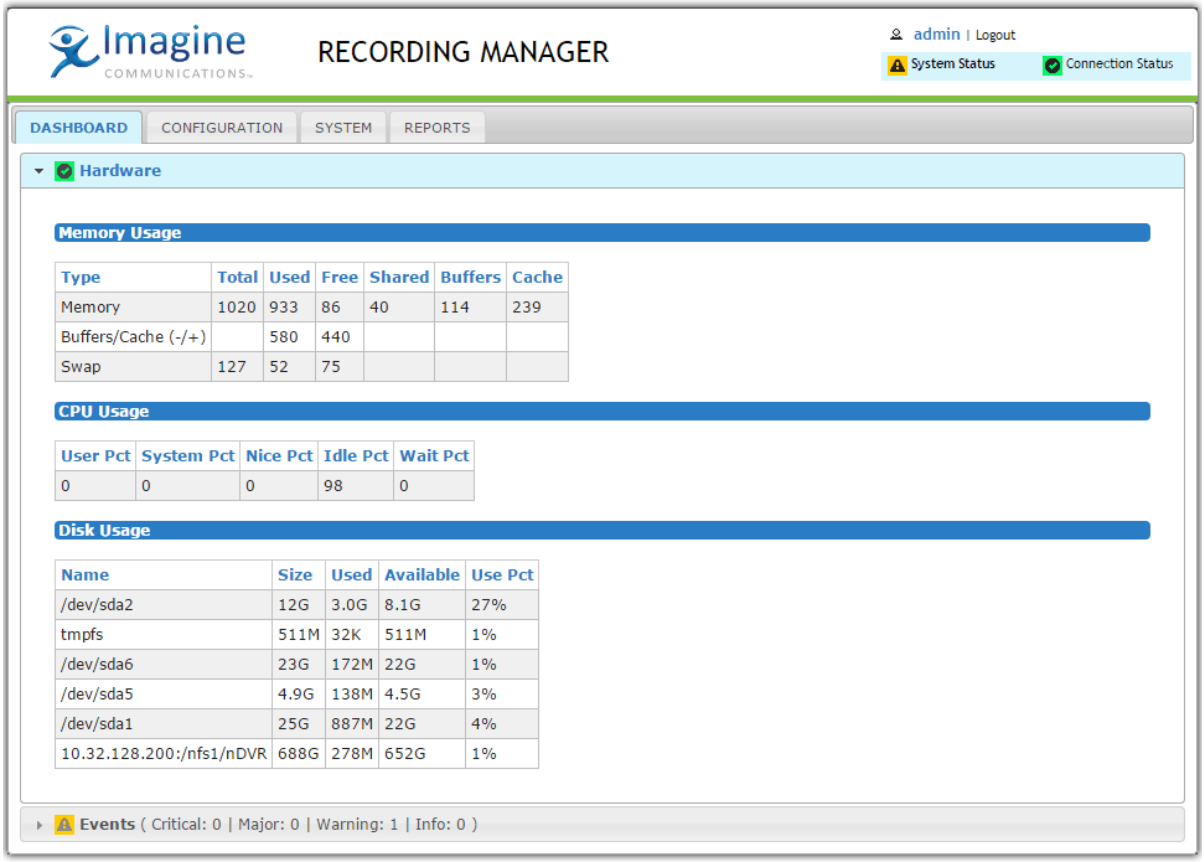
Icons

The icons displayed in the **Dashboard** indicate current system or line item status. Each item will display the highest error condition state for that category.

- — Indicates the current status is good; no errors are present on the *RM* or the specified task.
- — Indicates there is a major or warning condition present; some errors have occurred during recording operations.
- — Indicates the presence of a critical error condition.
- — Indicates more information is available for a particular event.

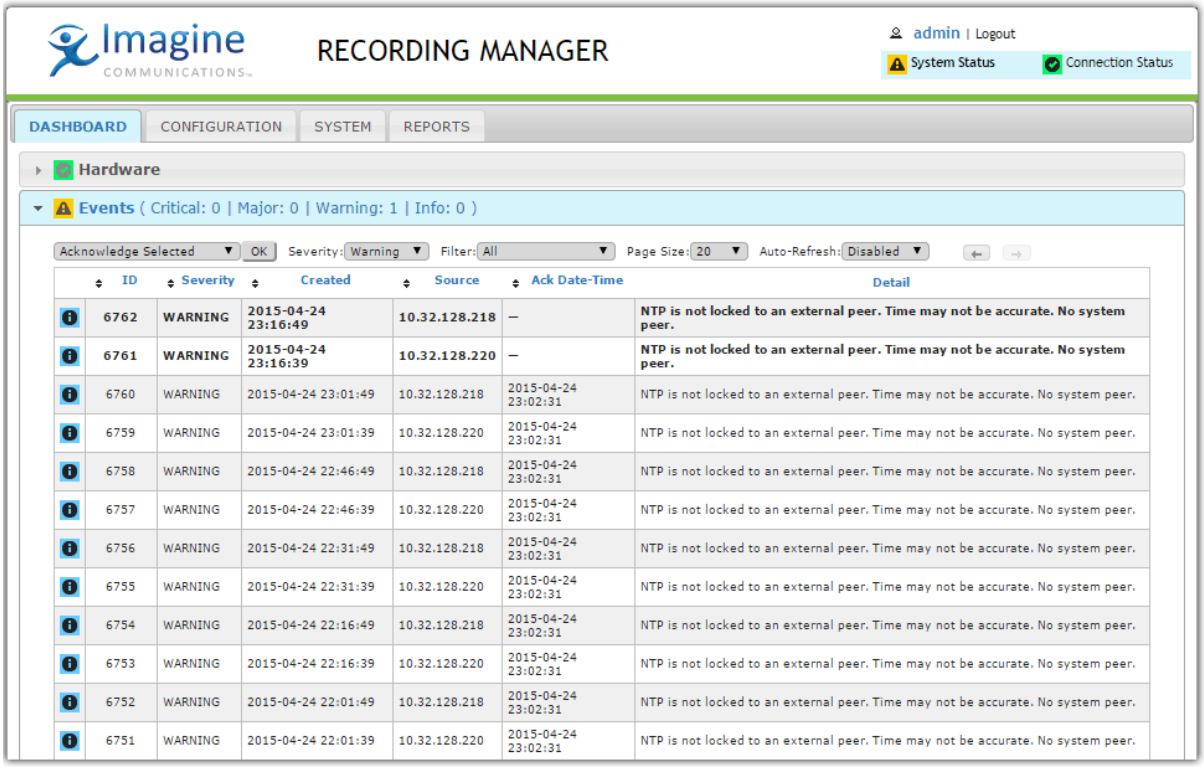
Hardware

This section displays information about the status of the RM hardware including Memory Usage, CPU Usage, and Disk Usage.



Events

This section displays current and historical events on the system for critical, major, warning, and informational severity levels. Many filtering options are available from the Events summary, including the ability to sort events based on category or acknowledged state.



Menu Description

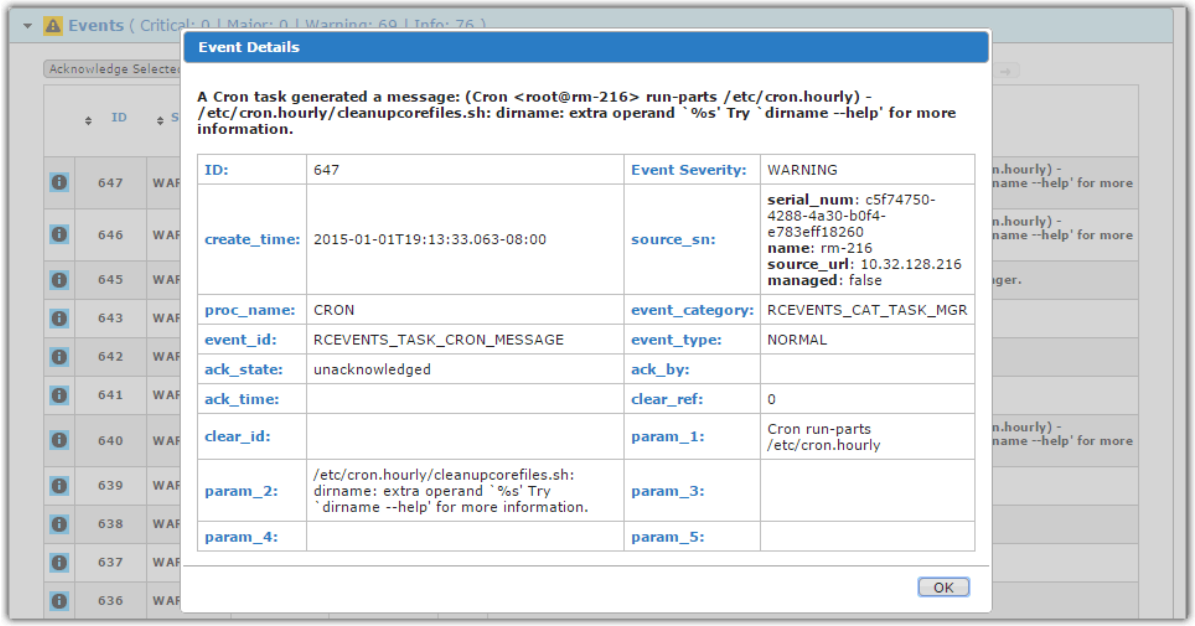
Table 8 describes the fields and columns available in the Events container:

Table 8. Events fields

Name	Type	Description
Acknowledgement	Action Button	Use the drop-down menu to select which type of acknowledgement to choose for one or more events. Choices are: *Acknowledge Selected* — acks highlighted events *Unacknowledge Selected* — unacks highlighted events *Acknowledge All* — acks all events
Severity	Menu Navigation	Use the drop-down menu to choose the minimum level of severity that will be displayed in the events list. Choices are: *Info* — displays all events, including Info events *Warning* — displays all events from Warning level and up, excluding Info events *Major* — displays all events from Major level and up, excluding Warning events *Critical* — displays all Critical level events, excluding all others.
Filter	Menu Navigation	Use the drop-down menu to filter displayed results. Choices are: All, Acknowledged, or Unacknowledged
Page Size	Menu Navigation	Use the drop-down menu to choose the number of results displayed per page. Choices are: 20, 50, or 100
Auto-Refresh	Menu Navigation	Use the drop-down menu to choose whether to enable or disable events from being automatically refreshed. Choices are: *Enable* or *Disable*
ID	Column Heading	Displays the line entry number of the event. Clicking on this column header will sort events by ascending or descending ID number
Severity	Column Heading	Displays the severity level of the event. Clicking on this column header will sort events by ascending or descending severity level.
Created	Column Heading	Displays the date and time the event occurred. Clicking on this column header will sort events by ascending or descending date and time.
Source	Column Heading	Displays the IP address or hostname of the node from which the event originated. The nodes whose events are reported are: *RM, JITP*, or *Recorder*. Clicking on this column header will sort events by ascending or descending IP address or hostname. *Note:* For JITP and Recorder, the event description will reference the JITP or Recorder as a Packager
Ack Date-Time	Column Heading	Displays the date and time that the event was acknowledged (if ack'd at all). Clicking on this column header will sort events by ascending or descending Ack date and time.
Detail	Column Heading	Provides a detailed description of the event

Viewing Detailed Information for an Event

You can view detailed information for a given event by clicking the icon next to a row entry. An *Event Details* window for a specific event will open similar to the one shown below.



Acknowledging and Unacknowledging Events

An active event condition may be cleared by *acknowledging* its status. When you *unacknowledge* an event, its active severity status is reinstated on the system.

To acknowledge or unacknowledge one or more events:

1. Select the desired events from the summary list.
   - To select a group of consecutive events, click on the first event in the group, hold down the SHIFT key on your keyboard, and click on the last event in the group.
   - To select a group of non-consecutive events, hold down the CTRL key on your keyboard while clicking on the desired events.
2. From the **Severity** field, choose the *minimum* severity level by which to filter the events.

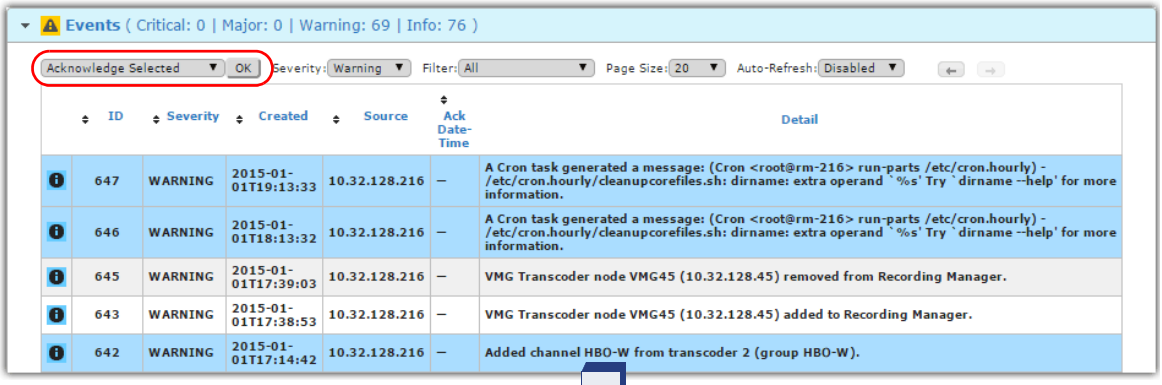
Note: *The severity filter will return events that match the minimum severity criteria. Choosing **Critical** will return events that are only critical severity. Choosing **Major** will return Major severity events and higher. Choosing **Warning** will return all Warning and higher events.*

3. From the **Filter** field, choose whether to sort events based on acknowledged state, or select *All* to display both acknowledged and unacknowledged events.
4. From the **Acknowledge** field, select whether to *Acknowledge Selected,* or *Unacknowledge Selected,* or *Acknowledge All* events.

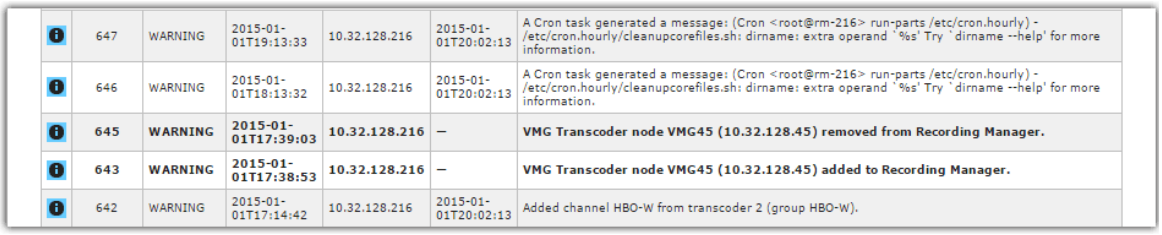
5. Click on **Ack/Unack** next to the drop down box.

   The selected event(s) are immediately *acked* or *unacked*.

Unacknowledged Events Shown



Acknowledged Events Shown



Note: *For a complete list of event messages, refer to the* Recording Manager List of System Events & Traps.

CHAPTER 7

Configuration

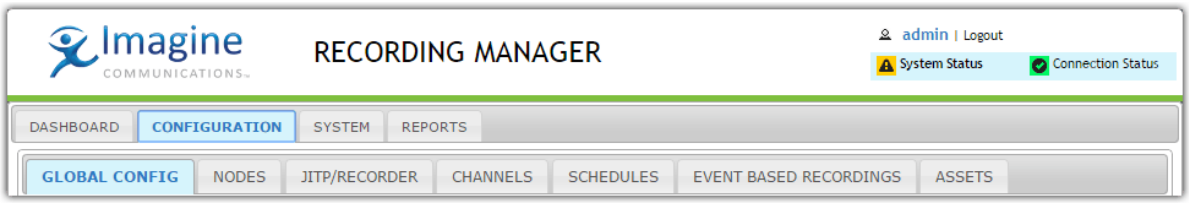
This chapter describes the **Configuration** tab of the RM GUI, which can be accessed by logging in to the RM as described in the section titled, "Launching RM" on page 40. All recording configuration and scheduling is performed in this tab. System related configurations for the RM are performed from the System Configuration tab (next chapter).

Note: *For end-to-end set up and configuration instructions, please refer to the "cDVR Quickstart Guide" for this release.*

In This Chapter:

Overview

The **CONFIGURATION** tab consists of several sub-tabs in which all recording-based parameters are provisioned for various cDVR components, such as transcoders (Imagine Communications-based or third party), Recorders, JITP servers, and storage devices. All scheduling and recording is performed from the **CONFIGURATION** tab. The sub-tabs are described in detail in subsequent sections, but are shown and briefly described below as an overview.



- **GLOBAL CONFIG** — contains global recording and content delivery parameters for system components

- **NODES** — allows you to add all node-related parameters, such as IP addresses and storage locations
- **JITP/RECORDER** — provides configuration for all packaging-related parameters, such as key servers, audio maps, JITP profiles, and source servers
- **CHANNELS** — allows you to add the transcoded programs that will be recorded
- **SCHEDULER** — provides detailed scheduling for both event-based and continuous recording.
- **EVENT BASED RECORDINGS** — displays a list of all event-based programs that have been or are currently being recorded
- **ASSETS** — provides the ability to create and display content assets from CR segments that have been or are currently being recorded.

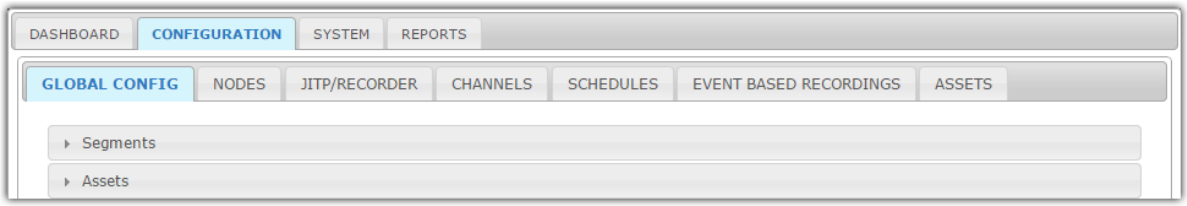
Sub-tab Organization

The sub-tabs are organized in a procedural left-to-right, top-to-bottom fashion. That is, the system should be configured starting with the left-most tab and ending with the right-most tab. Containers within each tab should be configured starting at the top and moving to the bottom.

Note that depending on your specific network deployment, not all tabs will require configuration or viewing. Specifically, the default settings in the *GLOBAL CONFIG* sub-tab may not need to be changed, and depending on whether you are using Event Based Recordings or Continuous Recordings, you may or may not need to view the *EVENT BASED RECORDINGS* or *ASSETS* sub-tabs.

Global Config Sub-tab

The **GLOBAL CONFIG** sub-tab is accessed by clicking through the **CONFIGURATION > GLOBAL CONFIG** menu path. In this menu, you can configure global parameters for segment directory and asset sizes and when to delete assets and segments.



The two containers in the Main sub-tab are:

- Segments Container
- Assets Container

Segments Container

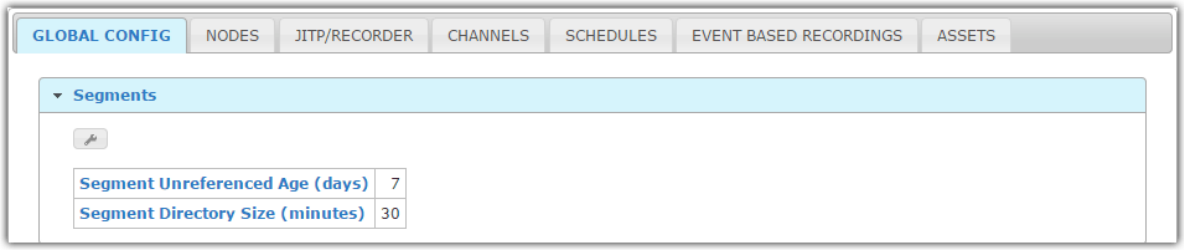
The **Segments** container allows you to customize duration and storage deletion parameters for segment directories.

A segment directory contains individual segment files (usually in .TS format). A segment file consists of multiple content fragments (pieces of video and audio). The **Segments** container pertains to settings for *segment directories only*, not individual segments and not fragments.

To open the segment parameters, navigate to:

CONFIGURATION → GLOBAL CONFIG → Segments → *[expand]*

Segments container - Default



If you wish to modify the parameters in this menu, click the wrench icon ( ) to open the *Modify* menu.

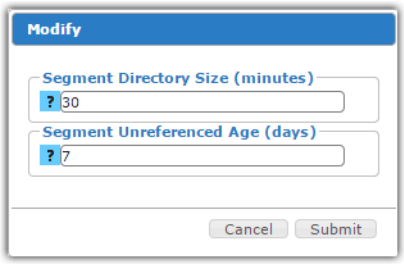


Table 9 describes the fields in the **Segments** nested container.

Table 9. GLOBAL CONFIG > Segments

Name	Description	Default
Segment Unreferenced Age (days)	Specifies the absolute number of days before a segment not associated with an asset is deleted. Once deleted, unreferenced segments are no longer available for asset creation. Value range: 1 - 40000	7
Segment Directory Size (minutes)	Specifies the maximum size (duration) in minutes of content in an asset's segment directory. A new segment directory is created when the duration is reached. Value range: 1 to 30	30

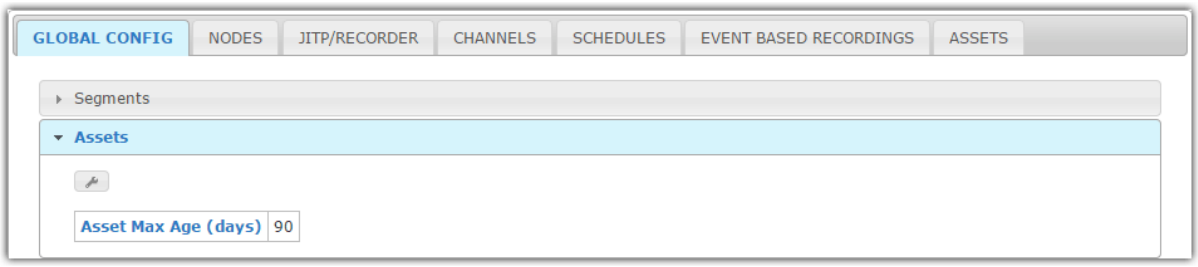
Assets Container

The **ASSETS** container allows you to set when CR assets are deleted from the storage server.

To open the assets parameter, navigate to:

CONFIGURATION → GLOBAL CONFIG → Assets → *[expand]*

Assets container - Default



If you wish to modify the parameters in this menu, click the wrench icon ( ) to open the *Modify* menu.

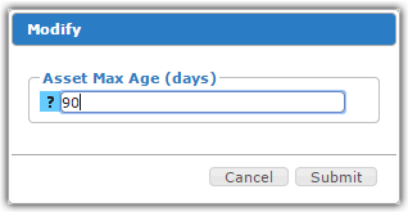


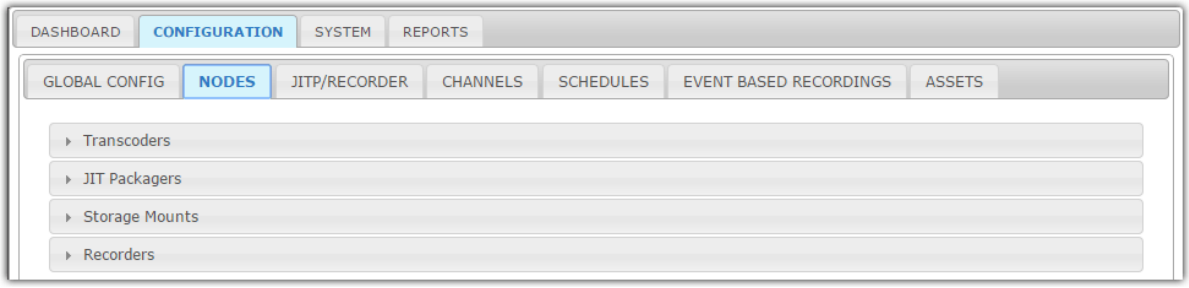
Table 10 describes the field in the **Assets** nested container.

Table 10. Main > Content Delivery fields

Name	Description	Default
Asset Max Age (days)	Specifies the absolute number of days before an asset (associated with segment directories) is deleted. Value range: 1 - 40000	90

Nodes Sub-tab

The **NODES** sub-tab is accessed by clicking through to **CONFIGURATION** > **NODES**. The NODES menu is where you will configure the bulk of your initial setup parameters including transcoders, JITP servers, storage mounts, and Recorders.



The following server components are described in this section:

- Transcoders Container
- JIT Packagers Container
- Storage Mounts Container
- Recorders Container

Each of these components is discussed in detail in "Solution Overview" on page 18. This section describes GUI configuration parameters for each container listed above.

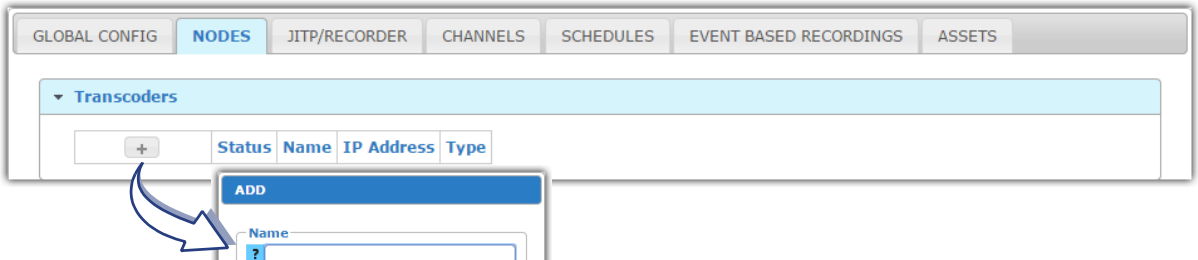
Transcoders Container

The **TRANSCODERS** container allows you to set up one or more transcoding devices that will be used for cDVR input. You can use an Imagine Communications transcoder, such as the Selenio™ VMG or Selenio™ TAT, or you can use a third party transcoder.

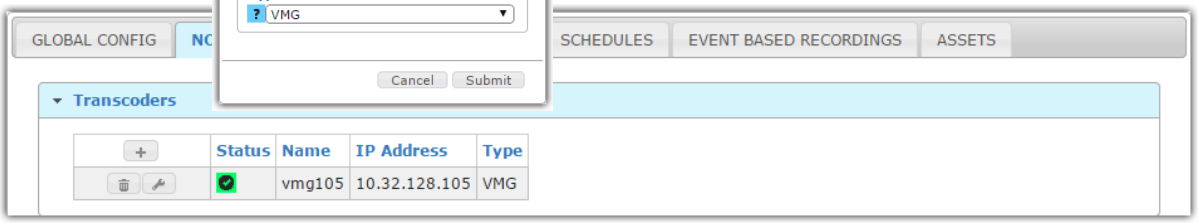
To view the **Transcoders** container, navigate to:

CONFIGURATION → NODES → Transcoders → *[expand]*

Default



Populated



Configuring a Transcoder

You can add(+), modify (🔧), or delete (🗑) a transcoder from this menu, using Table 11 below for guidelines.

Table 11. Transcoders Node fields

Name	Description	Default
Status	Indicates current RM connectivity status to the transcoder. One of two icons will be displayed here: *Green checkmark* — RM has good connectivity with the transcoder *Red "X"* — transcoder is in the RM's database, but there is no current connectivity.	n/a
Name	Specifies the name the RM will use when referencing the transcoder. When setting this parameter, use a unique name.	*Empty*
IP Address	Specifies the IP address of the transcoder.	*Empty*
Type	Specifies what type of transcoder is being used. Choices are: **VMG** — Imagine Communications' hardware-based transcoder **TransAct** — Imagine Communications' software-based transcoder **Other** — third party transcoder	*None selected*
+	Click this button to add a new entry.	n/a
🗑	Click this button next to an entry you wish to delete.	n/a
🔧	Click this button to modify parameters for an existing entry.	n/a

JIT Packagers Container

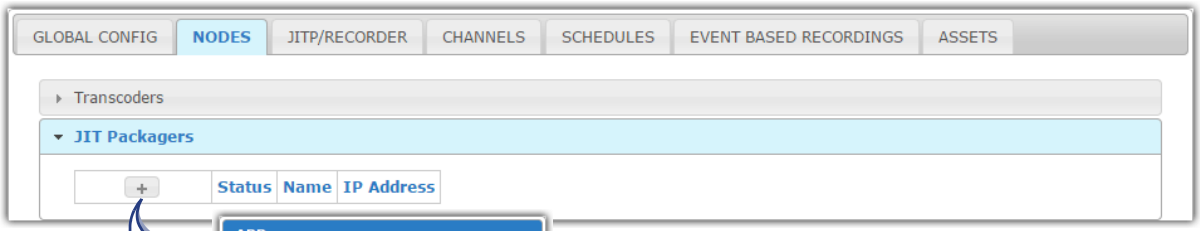
The **JIT Packagers** container allows you to set up one or more JITP servers that will be used to create ABR-ready chunks from the MBR IDR aligned streams generated by the Recorder. This device must be a Packager licensed for JITP (and optionally for Stitcher[1]).

Caution: *If you are using RM node-level redundancy for your system, you must first configure redundancy for the RM's before adding any JITP servers to this container. Refer to* Chapter 4, "RM Redundancy Setup" *for instructions.*

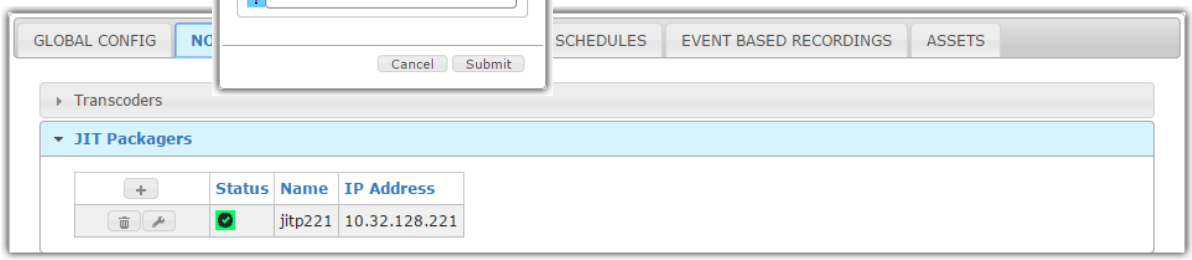
To view the **JIT Packagers** container, navigate to:

Configuration → Nodes → JIT Packagers → *[expand]*

Default



Populated



Configuring a JIT Packager

You can add(+), modify (🔧), or delete (🗑) a JIT Packager from this menu, using Table 12 below for guidelines.

1. Stitcher is required for CR.

Table 12 describes the fields in the **JIT Packagers** nested container.

Table 12. JIT Packagers Node fields

Name	Description	Default
Status	Indicates current RM connectivity status to the JIT Packager. One of two icons will be displayed here: *Green checkmark* — RM has good connectivity with the JITP *Red "X"* — JITP is in the RM's database, but there is no current connectivity.	n/a
Name	Specifies the name the RM will use when referencing the JITP. When setting this parameter, use a unique name.	*Empty*
IP Address	Specifies the IP address of the JITP.	*Empty*
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

Note: *When adding a new JITP to RM's database, the JITP's database will be reset so that RM can configure JITP from an empty database with default values. This process may take a few minutes.*

Storage Mounts Container

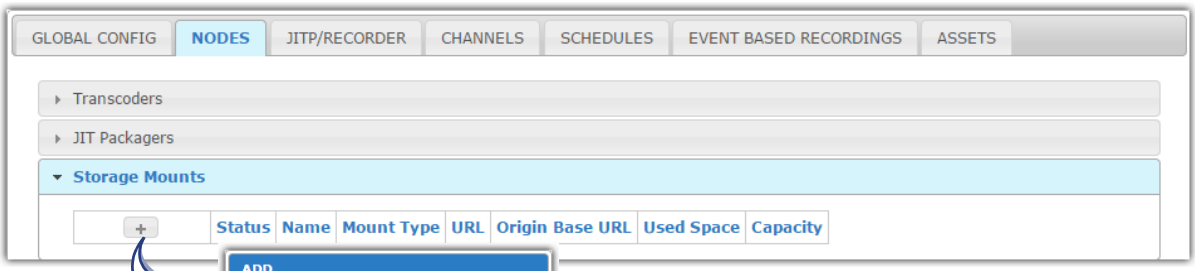
The **Storage Mounts** container provides the ability to specify a file server that will store the HLSv4 mezzanine content generated by Recorder for either EBR or CR. In the case of CR (and optionally EBR), the JITP server will pull content from the storage server in order to prepare and deliver ABR-ready chunks.

For EBR, the JITP server can ingest DASH-TS and HLS V4, or, when not using JITP for EBR, the content can be played back by any media player supported by a Packager.

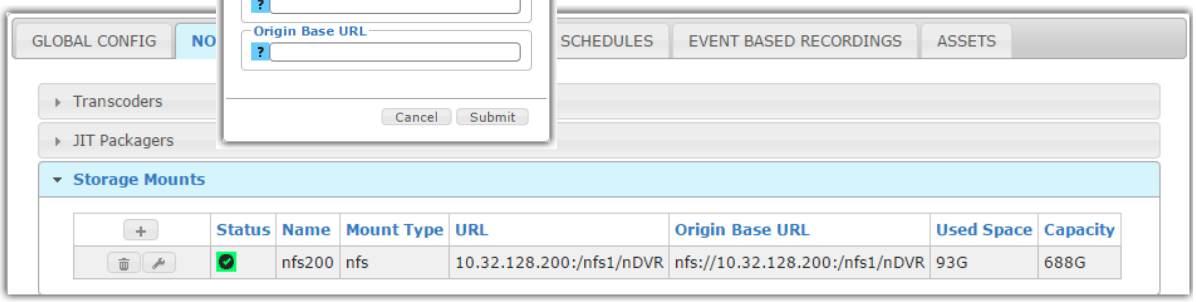
To view the **Storage Mounts** container, navigate to:

Configuration → Nodes → Storage Mounts → *[expand]*

Default



Populated (Direct)



Configuring a Storage Mount

You can add(+), modify (🔧), or delete (🗑) a storage mount from this menu, using Table 13 below for guidelines.

Table 13. Storage Mounts Node fields

Name	Description	Default
Status	Indicates current RM connectivity status to the storage mount. One of two icons will be displayed here: *Green checkmark* — RM has good connectivity with the storage mount *Red "X"* — storage mount is in the RM's database, but there is no current connectivity. *Red checkmark* — RM has connectivity to the device, but the device is disabled or otherwise degraded.	*Blue dots*
Name	Specifies the name the RM will use when referencing the storage server. When setting this parameter, use a unique name.	*Empty*
Mount Type	Specifies the type of storage server used. Choices are: **NFS** — Network File System (common client/server file storage system) **GPFS** — General Parallel File System (a clustered file system used for high performance storage) For more information on how to set up GPFS, refer to "GPFS Storage Details and Setup" on page 63.	*Empty*

Table 13. Storage Mounts Node fields

Name	Description	Default

URL	**For NFS access only.** Specifies the hostname or IP address and mount point path of the storage server where content will be stored. Proper format should be as follows:
	Two methods of configuration are available for NFS:
	Direct NFS access: In this case, the JITP server accesses the content directly via mount. Proper format should be as follows:
	[ip addr or hostname]:/[root directory]/[sub-directory]/[directory ..n]
	`nfs://myhost.domain.com:/ndvr/nfs-1/content`
	HTTP NFS access: In this case, the JITP uses HTTP to access the content. Proper format should be as follows:
	`http://`[ip addr or hostname]/[directory]/
	`http://10.32.128.200/ndvr/content`
	Note: for GPFS, this field is autopopulated with the mount path once a GPFS node is added.
		Empty

Origin Base URL	**For NFS access only.** Specifies the base URL that will be used for access to the storage mount.
	Two types of URLs available for NFS:
	Direct NFS access: This field is autopopulated for direct NFS access. Do not enter any data in this field. Proper format will be displayed as follows:
	nfs://[ip addr or hostname]:/[root directory]/[sub-directory]/[directory ..n]
	`myhost.domain.com:/ndvr/nfs-1/content`
	HTTP NFS access: If HTTP access to the storage mount is different from the entry in the URL field, a different URL may be added here. If the URL and Origin Base URL use the same URL, entry in this field is optional. Proper format to use for HTTP access is as follows:
	`http://`[ip addr or hostname]/[directory]/
	`http://10.32.128.200/ndvr/content`
		Empty

Used	Indicates the amount of space (in Gigabytes) in use on the NFS server. This number is auto-populated once the RM has established connectivity to the NFS.	*Blank (auto-populated)*
Capacity	Indicates the amount of space (in Gigabytes) available for use on the NFS server. This number is auto-populated once the RM has established connectivity to the NFS and is automatically refreshed at regular polling intervals.	*Blank (auto-populated)*
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

GPFS Storage Details and Setup

General Parallel File System (GPFS) is a scalable, high performance, clustered file system that can be used in addition to or in place of NFS. From the RM's perspective, a GPFS mount appears as a typical file system mount. If using GPFS as a storage mount, it must be set up on both the RM and the Recorder, both of which are considered clients. Various parameters must be set up before configuring

the **Storage Mounts** container to use GPFS on the RM and Recorder[2]. These requirements (for the RM) and their steps are described in this section.

Prerequisite Overview

Any GPFS deployment requires configuration of the GPFS cluster in order to communicate with client nodes. This involves setting up the client software, kernel module, and ssh private/public key pairs.

These steps are not done by default; they require manual configuration depending on the deployment. The RM and Recorder provide a set of base RPMs and updates. There are also a few RPMs that contain kernel modules, but you must verify these modules match the current kernel version on each client (RM and/or Recorder). If the kernel version of a Recorder or RM does not match one of the kernel RPMs provided, then a new version must be compiled for the target kernel version. In this case, refer to "Building the Kernel Driver" on page 69.

Prerequisite Steps

Below are the steps required for set up. Note that the hostnames have been identified as `gpfs-client` and `gpfs-server`. GPFS clients include the RM, Recorder and JITP.

Note: *If you are using a Direct Access GPFS mount for JITP, these steps must also be performed on the JITP server. Refer to the Telurio™ Packager User Guide, Release 5.7 for detailed setup instructions.*

2. See the *Telurio™ Packager User Guide, Release 5.7* for Recorder set up instructions

1. **Install RPMs** as shown in the code block below:

```
[root@gpfs-client ~]# yum -y install ksh
[root@gpfs-client ~]# yum install gcc-c++
[root@gpfs-client ~]# rpm -ivh /opt/gpfs/gpfs.*.rpm
Preparing...                ########################################### [100%]
   1:gpfs.base              ########################################### [ 25%]
   2:gpfs.gpl               ########################################### [ 50%]
   3:gpfs.msg.en_US         ########################################### [ 75%]
   4:gpfs.docs              ########################################### [100%]
[root@gpfs-client ~]# rpm -Uvh /opt/gpfs/updates/gpfs.*.rpm
Preparing...                ########################################### [100%]
   1:gpfs.base              ########################################### [ 25%]
   2:gpfs.gpl               ########################################### [ 50%]
   3:gpfs.msg.en_US         ########################################### [ 75%]
   4:gpfs.docs              ########################################### [100%]
[root@gpfs-client ~]# uname -a
Linux gpfs-cient.lab.ripcode.com 2.6.32-431.11.2.el6.x86_64 #1 SMP Tue Mar 25
19:59:55 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[root@gpfs-client ~]# ls -l /opt/gpfs/kernel/*
-rw-r--r-- 1 root root 1890738 Aug 12 20:45 /opt/gpfs/kernel/gpfs.gplbin-2.6.32-
431.11.2.el6.x86_64-3.5.0-19.x86_64.rpm
-rw-r--r-- 1 root root 1526284 Aug 12 20:45 /opt/gpfs/kernel/gpfs.gplbin-2.6.32-
431.5.1.el6.x86_64-3.5.0-19.x86_64.rpm
[root@gpfs-client ~]# rpm -ivh /opt/gpfs/kernel/gpfs.gplbin-2.6.32-
431.11.2.el6.x86_64-3.5.0-19.x86_64.rpm
Preparing...                ########################################### [100%]
   1:gpfs.gplbin-2.6.32-431.########################################### [100%]
[root@gpfs-client ~]# modprobe -l | grep mmfslinux
extra/mmfslinux.ko
```

2. **Setup ssh keys on all nodes.**

   Setting up the ssh keys on all nodes is a multi-step process that entails setting up ssh parameters for both the *server -> client* and the *client -> server* directions.

   a) **Server -> Client setup.**

   A server -> client setup is shown below, which entails the following three steps:

   - Set up the server to log into the client without requiring a prompt
   - Copy the server public key to the client's authorized_keys file

- Perform a simple ssh to the client to verify the login success
  An example is shown below:

```
kaluza|~$ ssh root@gpfs-server
root@gpfs-server's password:
Last login: Mon Aug 11 06:50:31 2014 from 10.10.100.43
[root@gpfs-server ~]# cat .ssh/id_rsa.pub | ssh root@gpfs-client "cat >> ~/
.ssh/authorized_keys"
The authenticity of host 'gpfs-client (10.10.83.54)' can't be established.
RSA key fingerprint is c9:22:9a:cc:a2:cd:b3:5a:33:11:1c:3e:43:c9:74:4a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'gpfs-client' (RSA) to the list of known hosts.
root@gpfs-client's password:
[root@gpfs-server ~]# ssh gpfs-client
Last login: Fri Apr 24 17:16:04 2015 from 10.10.70.192
[root@gpfs-client ~]# exit
logout
Connection to gpfs-client closed.
[root@gpfs-server ~]#
```

Note: *If each server in the cluster has a **unique public/private key pair**, repeat each step above from each server in the GPFS cluster to each client. When complete, every client should have an entry for each server in its authorized_keys file.*

Note: *If all servers in the cluster use **a single common public/private key pair** (the id_rsa and id_rsa.pub files are identical on each server), the steps above only need to be done from one server to each client. Each client only needs a single entry in its authorized_keys file and that key will be used for connections from any of the servers.*

b) Client -> Server setup.

This step adds the private key to the client node so that the client can execute GPFS commands against the server without requiring authentication. Two types of set ups are available: **Single Common Key** and **Unique Keys per Server**. If all servers in the GPFS cluster use the same common public/private key pair, follow the steps to set up a Single Common Key. If each server in the cluster has a unique public/private key pair, follow the steps to set up Unique Keys per Server.

- **Single Common Key** (assumes that Step 1, server -> client, has been completed successfully). Perform the commands shown below from one server to each client. When finished, each client should have a single id_rsa file in the .ssh directory:

```
kaluza|~$ ssh root@gpfs-server
root@gpfs-server's password:
Last login: Mon Aug 11 06:50:31 2014 from 10.10.100.43
[root@gpfs-server ~]# scp .ssh/id_rsa root@gpfs-client:/root/.ssh/
id_rsa                                        100%  406     0.4KB/s   00:00
```

- **Unique Keys per Server** (assumes that Step 1, server -> client, has been completed successfully). Perform the commands shown below from each server to each client. When finished, each client should have its own id_rsa.x file for each server and a config file in the .ssh directory::

```
kaluza|~$ ssh root@gpfs-server
root@gpfs-server's password:
Last login: Mon Aug 11 06:50:31 2014 from 10.10.100.43
[root@gpfs-server1 ~]# scp .ssh/id_rsa root@gpfs-client:/root/.ssh/
id_rsa.gpfs-server1
id_rsa                                        100%  406     0.4KB/s   00:00
```

  - Next, create a config file that links the specific id_rsa.x file to the appropriate server ssh request. Repeat this step for each client:

```
kaluza|~$ ssh root@gpfs-server
root@gpfs-server's password:
Last login: Mon Aug 11 06:50:31 2014 from 10.10.100.43
[root@gpfs-client ~]# vim .ssh/config
```

  - Finally, paste the following into the editor:

```
StrictHostKeyChecking no
GSSAPIAuthentication no
Host gpfs-server1
   User root
   IdentityFile ~/.ssh/id_rsa.gpfs-server1
Host gpfs-server2
   User root
   IdentityFile ~/.ssh/id_rsa.gpfs-server2
```

  - Repeat the Host entry for each server in the cluster, changing the host name and identity file as appropriate.

- **Test the Connection:** After the ssh keys have been set up, perform a simple ssh connection from each client to each server, and from each server to each client to ensure the "Are you

sure you want to continue connecting (yes/no)?" prompt is cleared and there is no prompt for a password.

3. **Add the client node from the server.** For example, login to gs1 and run the following:

```
[root@gpfs-server ~]# mmaddnode gpfs-client
Tue Aug 12 20:16:12 PDT 2014: mmaddnode: Processing node gpfs-client.lab.ripcode.com
The authenticity of host 'gpfs-client.lab.ripcode.com (10.10.83.54)' can't be estab-
lished.
RSA key fingerprint is c9:22:9a:cc:a2:cd:b3:5a:33:11:1c:3e:43:c9:74:4a.
Are you sure you want to continue connecting (yes/no)? yes
mmaddnode: Command successfully completed
mmaddnode: Warning: Not all nodes have proper GPFS license designations.
    Use the mmchlicense command to designate licenses as needed.
mmaddnode: Propagating the cluster configuration data to all
  affected nodes.  This is an asynchronous process.
[root@gpfs-server ~]# mmchlicense client --accept -N gpfs-client
The following nodes will be designated as possessing GPFS client licenses:
    gpfs-client.lab.ripcode.com
mmchlicense: Command successfully completed
mmchlicense: Propagating the cluster configuration data to all
  affected nodes.  This is an asynchronous process.
[root@gpfs-server ~]# mmstartup -N gpfs-client
Tue Aug 12 20:17:07 PDT 2014: mmstartup: Starting GPFS ...
[root@gpfs-server ~]# mmstatus -a
-bash: mmstatus: command not found
[root@gs1 ~]# /usr/lpp/mmfs/bin/mmgetstate -a
 Node number   Node name        GPFS state
------------------------------------------
       1       gpfs-client        active
       2       gpfs-client2       active
       3       gpfs-client3       active
       4       gpfs-client4       active
```

Changing the GPFS Mount Path for RM

By default, the GPFS mount is mounted at **`/mnt/RGBGPFS`**. If the GPFS mount path is different, you will have to change the location on the RM as follows:

- From the Linux CLI, modify the file `/etc/ripcode/ripcode.conf` as follows:
  - Change the value of "`GPFSMountDir`" from "`/mnt/RGBGPFS`" to the desired path.
- From the Linux CLI, modify the file `/etc/rgbconfig/conf.d/rm.json` as follows:
  - Add an entry titled, "gpfs_mount" with the value of your desired mount name. For example, if you wish to change the mount name to "visage," the entry in the `rm.json` file would look like this (note that the quotes around each word and the colon must have a single space before and after):

    `"gpfs_mount" : "visage"`

Once you have changed and save the ripcode.conf and rm.json files, restart the RM services by entering this command from the Linux CLI:

```
service ripcode restart
```

Limiting Memory Usage by GPFS kernel module

The `mmfsd` will use a fixed amount of memory on each node; by default this is 4GB. This memory usage is based on the tunable "`pagepool`." Running the GPFS command `mmlsconfig` will display the page pool size. Additionally, you can change the size of the page pool by running "`mmchconfig pagepool=1GB`" if, for example, you wish to set the page pool on all nodes to 1GB in size. After this change is made, clients will have to be shutdown (`mmshutdown`) and started back up (`mmstartup`) in order to execute the change. Also, you can limit what nodes on which to apply these page pool changes to by providing the `-N` flag and listing a series of target nodes.

Notes about using GPFS

- There is support for only one GPFS mount from a file system point of view. From the RM point-of-view, you can add multiple mounts, but they will all point to the same location (`/opt/RGBGPFS` by default).
- GPFS clients require manual configuration intervention before it can be used. This may be unavoidable and even required by your operations team if GPFS is part of your deployment.

Building the Kernel Driver

Building a client-side kernel driver is required if your kernel version is not 2.6.32-431.5.1 or 2.6.32-431.11.2. Building the kernel driver should be done from an RM or Recorder. Depending on the CentOS DVD version install, gcc-c++ may also need to be installed.

The commands below assume that all required libraries are already installed:

```
cd /usr/lpp/mmfs/src
make LINUX_DISTRIBUTION=REDHAT_AS_LINUX Autoconfig
make World
make InstallImages
make rpm
```

Recorders Container

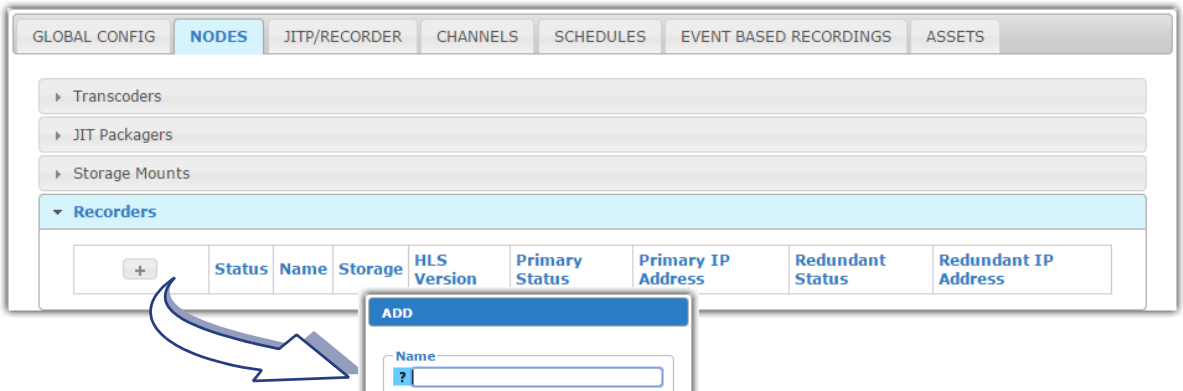
The **Recorders** container allows you to set up one or more Recorder devices that will be used to record MBR IDR streams (from the transcoder) and create the HLSv4 mezzanine format for storage and delivery to a JITP server.

Caution: *If you are using RM node-redundancy for your system, you must first configure redundancy for the RM's before adding any Recorders to this container. Refer to* Chapter 4, "RM Redundancy Setup" *for instructions.*

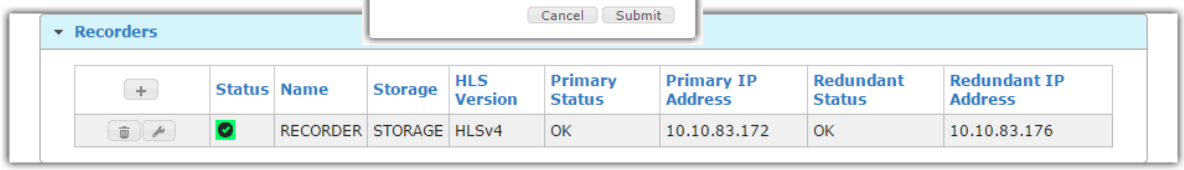
To view the **Recorders** container, navigate to:

CONFIGURATION → NODES → Recorders → *[expand]* **→** *[expand on **Recorder** row entry]*

Default



Populated (redundant shown)



Configuring a Recorder

You can add(+), modify (🔧), or delete (🗑) a storage mount from this menu, using Table 14 below for guidelines.

Table 14. Recorders Node fields

Name	Description	Default
Status (**For Recorder** container group)	Indicates current RM connectivity status to the Recorder. One of two icons will be displayed here: *Green checkmark* — RM has good connectivity with the Recorder *Red "X"* — Recorder is in the RM's database, but there is no current connectivity. *Red checkmark* — RM has connectivity to the device, but the device is disabled or otherwise degraded.	*n/a*
Name	Specifies the name the RM will use when referencing the Recorder(s). When setting this parameter, use a unique name.	*Empty*
Storage	Specifies which storage server to use for the Recorder group. Whatever was configured from the *Configuration > Nodes > Storage Mounts* container will be displayed here in a drop-down box.	*None Selected*
HLS Version	Specifies the HLS version that the Recorder will use for creating the storage mezzanine format. Choose from either *HLSv2* or *HLSv4*. *Note:* HLSv4 should be used for this version of software.	*None Selected*

Table 14. Recorders Node fields

Name	Description	Default
Primary Status	Indicates the operational status of the Primary Recorder. One of three status indications will be displayed: OK - Good connectivity, Recorder is operational SET FAILURE - No connectivity, Recorder is disabled DISABLED - There is connectivity, but Recorder is disabled for another reason.	*n/a*
Primary IP Address	Specifies the IP address of the Recorder.	*Empty*
Redundant Status	Indicates the operational status of the redundant Recorder (if it has been configured). One of three status indications will be displayed: OK - Good connectivity, Recorder is operational SET FAILURE - No connectivity, Recorder is disabled DISABLED - Recorder is disabled due to either no redundant node being configured or another type of redundancy failure.	*n/a*
Redundant IP Address	Specifies the IP address of the redundant Recorder. Recorder redundancy is enabled as soon as the redundant IP address is configured and connectivity is established. *Note:* To add another non-redundant Recorder, click the "+" icon in the table and add a new node.	*Empty*
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

Note: *When adding a new Recorder to RM's database, the Recorder's database will be reset so that RM can configure it from an empty database with default values. This process may take a few minutes.*

Record-level Redundancy

In record-level redundancy, a Primary and Redundant Recorder are configured to provide active-muted redundant recording from the RM. Both Recorders are concurrently recording content received from the transcoder, but only one recording at a time is written to the storage server for JITP delivery. If a Recorder fails to write content to the storage server, then the redundant Recorder will pick up in its place and continue to write the content to the storage server.

Note: *A Recorder is a Packager that is licensed for recording. When you configure the **Recorders** tab in the RM, you are in effect configuring a specific type of package on a Packager.*

In essence, record-level redundancy from the RM works in the same manner that package-level redundancy works on a Packager, with one exception: in record-level redundancy, the Recorders are not writing content to the storage server at the same time; rather, they are recording content at the same time, but only one Recorder writes the content to disk at a time.

Master/Slave Behavior

In record-level redundancy, reference timing control is based on a first-come first-serve basis. The redundant recording that starts first effectively becomes the 'master' record, on which the 'slave'

recording will base its PTS timing, segment number, encryption key, and various other points of reference. If the master fails, the slave begins writing its recording to disk in addition to becoming the new master on which the old master will base its reference timing if and when it recovers. The same behavior ensues for a slave recording that is manually stopped (rather than having stopped due to network error or outage).

Hardware and Networking Requirements

Since Recorder is an extension of a Packager, the hardware and networking requirements for record-level redundancy are the same as for package-level redundancy. Please refer to the section titled, "Package-level Redundancy" in Chapter 6 of the *Telurio™ Packager User Guide, Release 5.7* for information on hardware and networking requirements.

JITP/Recorder Sub-tab

The **JITP/RECORDER** sub-tab is accessed by clicking through to CONFIGURATION > JITP/RECORDER. From this menu you can configure global packaging / recording parameters for the JITP servers and Recorders in the RM's cluster.

This section provides an overview of each container in the **JITP/RECORDER** sub-tab and describes its GUI parameters.

- Key Server Container — Applies to both JITP and Recorder
- Audio Map Container — Applies to both JITP and Recorder
- Profile Container — JITP Only
- Source Server Container — JITP Only

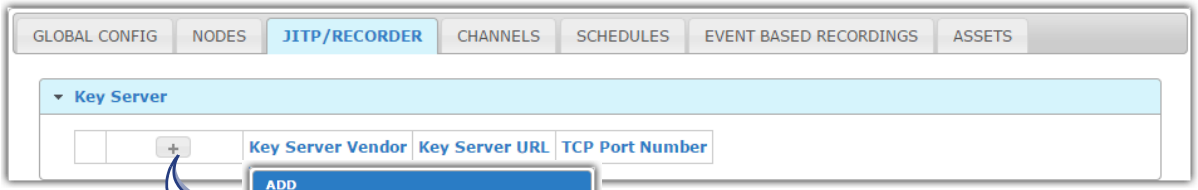
Key Server Container

The **Key Server** container allows you to set up one or more key servers to manage encryption keys between the JITP or Recorder and the client player. When a key server is configured in this menu, it will be applied to all JITP servers and Recorders within the RM cluster. Whether or not the key server is used for a particular package or recording depends on how an individual channel is configured (see "Channels sub-tab fields" on page 84 for more information on configuring key servers for channels).

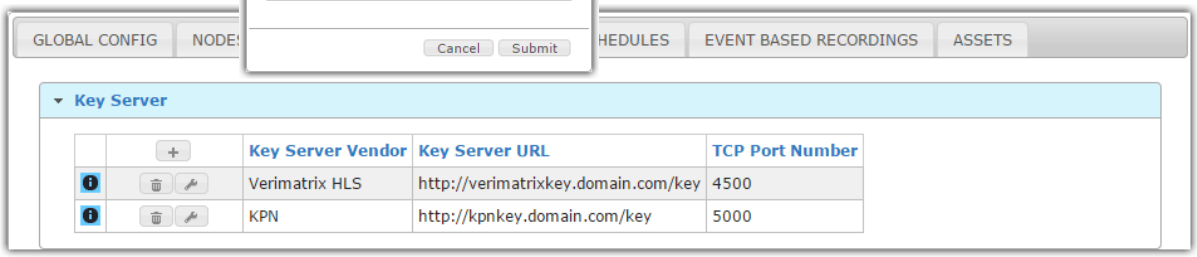
To view the **Key Server** container, navigate to:

CONFIGURATION → JITP/RECORDER → Key Server → *[expand]*

Default



Populated



Configuring a Key Server

You can add(+), modify (🔧), or delete (🗑) a key server from this menu, using Table 15 below for guidelines.

Table 15. Key Server Node fields

Name	Description	Default
Key Server Vendor	Specifies which key server vendor to add. Choices from the drop-down menu are: None, Verimatrix HLS, Nagra[a], Verimatrix PlayReady, Internal PlayReady, KPN, and PlayReady Leaf	Verimatrix HLS
Key Server URL	Specifies the URL where the key server is running. Proper format is: http://[domain]/[subdirectory]/... **Only applies to: Verimatrix HLS, Nagra, Verimatrix PlayReady, KPN, and PlayReady Leaf.**	*Empty*
Port	Specifies the port number under which the Key Server is running for the Key Server URL. Valid range is 0 - 65535. **Only applies to: Verimatrix HLS, Nagra, Verimatrix PlayReady, and KPN** *Note*: If leaving this value at 0, the default port of 80 will be used for HTTP and 443 will be used for HTTPS.	0
Client Key Request URL	Specifies the URL for the client to use when authenticating with the key server. Maximum of 1024 characters. **Only applies to: Internal PlayReady**	*Empty*

Table 15. Key Server Node fields

Name	Description	Default
Client Certificate	Specifies the HTTP or TFTP URL to download for the client certificate file. Maximum of 1024 characters. **Only applies to: PlayReady Leaf**	*Empty*
Client Key	Specifies the HTTP or TFTP URL to download for the client certificate file. This field only applies if the certificate is a PFX file (PKCS 12) or a .PEM file (certificate file). If a .PFX file is entered, leave the *Client Key* field blank as the key will be automatically extracted from the file. Maximum of 1024 characters. **Only applies to: PlayReady Leaf**	*Empty*
Client Key Password	Specifies the PlayReady Leaf client password. This field only applies if the *Client Certificate* field is a .PEM file (certificate file), in which case the *Client Key* must be manually entered here. Maximum of 1024 characters. **Only applies to: PlayReady Leaf**	*Empty*
PlayReady Key Seed	Specifies the PlayReady key seed to use when using an Internal PlayReady key server. Valid range is 30 - 512 characters. **Only applies to: Internal PlayReady**	*Empty*
User Name	Specifies the username for logging into the key server. **Only applies to: KPN**	*Empty*
Password	Specifies the password for logging into the key server. **Only applies to: KPN**	*Empty*
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

a. This option is only available for use with HLSv2, which is a beta-only feature for this release.

Audio Map Container

The **Audio Map** container implements Packager's late-binding audio feature, which allows for the inclusion of one or more alternative audio tracks to be published within a single recording. Audio map rules determine how (or if) content audio tracks are published by evaluating each input audio track against a set of user-defined rules. Having audio map rules allows for delivery protocols to adjust for variations in audio language and quality based on the client device's parameters and bandwidth capacity.

The **Audio Map** container is configured in two steps:

1. Create an audio map template
2. Add rules to the audio map template

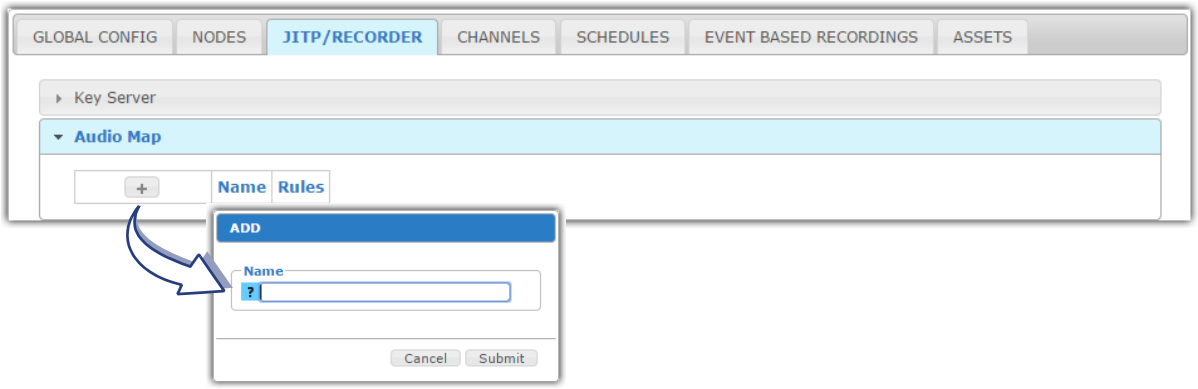
Audio Map Template Names

Before you can add an audio map rule, you must first create an audio map template name.

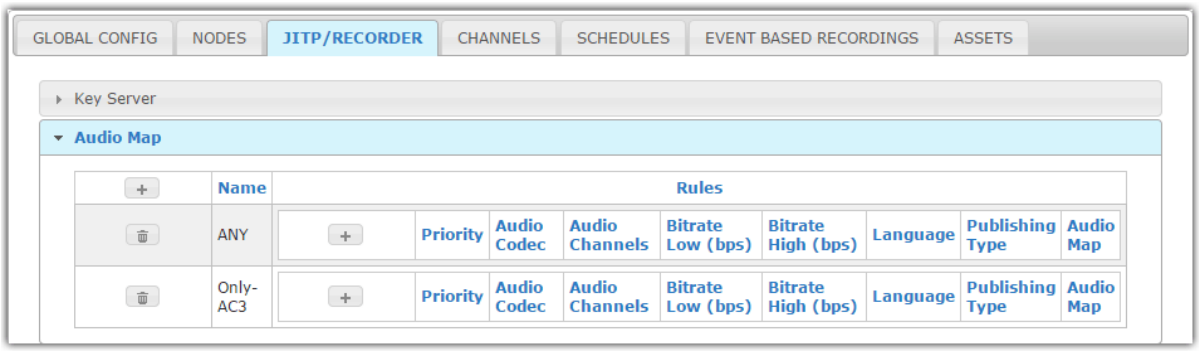
To view the **Audio Map** container for template names, navigate to:

CONFIGURATION → JITP/RECORDER → Audio Map → *[expand]*

Default (template name)



Populated (template name)



Configuring an Audio Map Template

You can add(+), modify (🔧), or delete (🗑) an audio map template from this menu, using Table 16 below for guidelines.

Table 16. Audio Map container fields - template name

Name	Description	Default
Name	Specifies the name of the audio map template. This field can be up to 23 alphanumeric characters long. *Note:* Once the **Name** has been saved to the RM database, it *cannot* be modified. If you wish to change the name, you must delete the entry and add a new one.	*Empty*
+	Click this button to add a new entry.	n/a
🗑	Click this button next to an entry you wish to delete.	n/a
🔧	Click this button to modify parameters for an existing entry. *Note*: If the specified audiomap is in use by an active recording, this field cannot be modified until the recording is complete or stopped.	n/a

Audio Map Rules

After creating an audio map template, up to 8 rules may be defined for each template. A rule consists of several configurable input audio conditions that, when met, will produce a specified output audio publishing option as described in Table 18 on page 78.

Audio map rules are applied on an exclusive basis, which means that once the rule conditions are met for the highest priority rule, no further rules are processed for the matching input audio track.

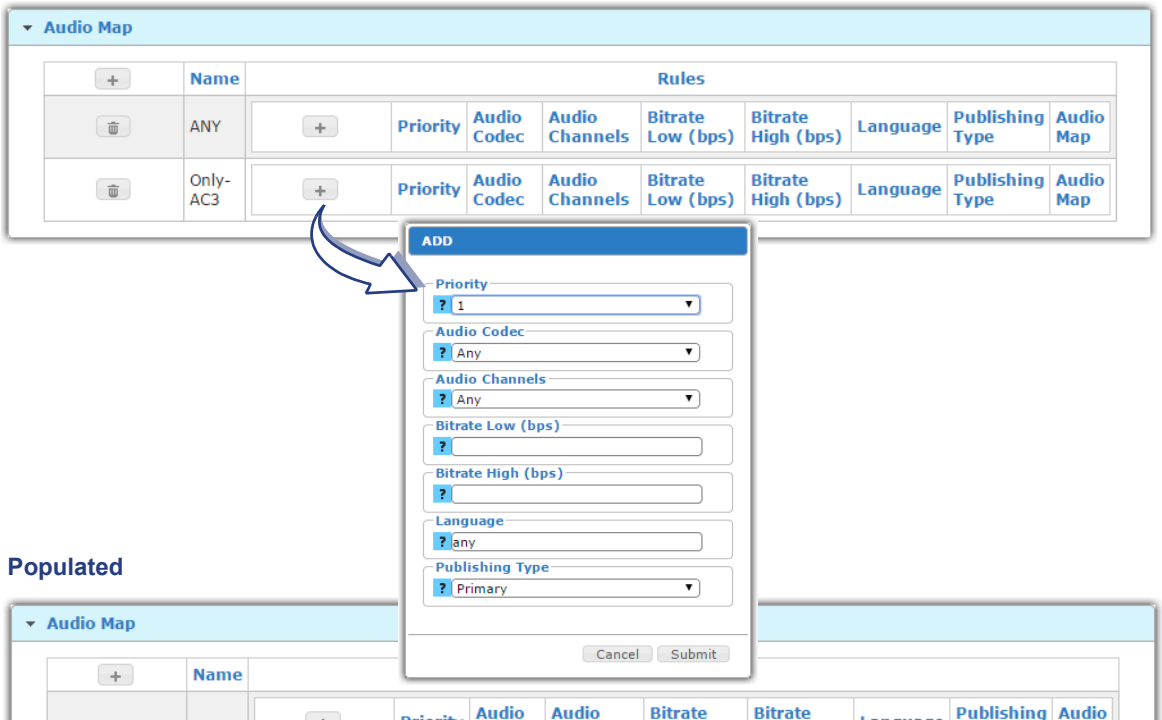
Note: *Since audio map rules are applied exclusively based on highest priority rule match, the rule priority should be set with the most specific audio characteristics as the highest, and each less specific characteristic (more generic) as subsequently lower priorities.*

Caution: *The Recorder and JITP servers do not support segmentation for multiple audio tracks where the language code, codec, and bitrate are identical. That is, each audio input track being fed to nodes of the same content must be unique, either in language, code, or bitrate. If such identical audio input tracks are fed to the Recorder and JITP, cDVR will not work correctly, which can result in "Out-of-Sync" messages and incorrect audio track publishing.*

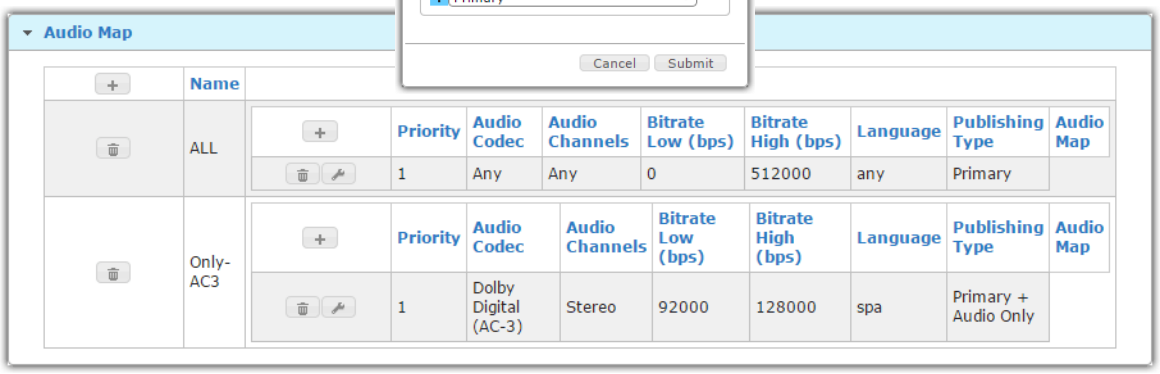
To view the **Audio Map** container for template names, navigate to:

Configuration → JITP/Recorder → Audio Map → *[expand] → [expand Audio Map name]*

Default



Populated



Configuring an Audio Map Rule

You can add( ), modify ( ), or delete ( ) an audio map rule from this menu, using Table 17 below for guidelines.

Table 17. Audio Map container fields - rule

Name	Description	Default
Priority	Sets the order in which rules are evaluated against the audio input tracks, 1 being the first (or highest priority) and 8 being the last (or lowest). Once a rule matches an audio track, no subsequent rules will be evaluated. *Note*: Priority should be configured from most specific audio characteristics (highest priority) to least specific audio characteristics (lower priority). *Note:* Once the **Rule** has been saved to the RM database, it *cannot* be modified. If you wish to change the parameters or priority level, you must delete the entry and add a new one.	1
Audio Codec	Specifies the input codec to which this rule will apply. Options from the drop-down menu are: • *Any* (rule will apply for any audio codec provided it matches all other conditions) • AAC-LC — Advanced Audio Coding Low-Complexity • AAC-HE — Advanced Audio Coding Low-Complexity + SBR • Dolby Digital (AC-3) • AAC-HEv2 — Advanced Audio Coding Low-Complexity + SBR + PS • Dolby Digital Plus (E-AC-3)	Any
Audio Channel	Select the number of input channels to which this rule will apply. Options are: • Any (rule will apply for any number of audio channels provided it matches all other conditions) • Mono • Stereo • 5.1 Surround	Any
Bitrate Low	Enter the lowest input audio bit rate for which the rule will apply. Acceptable value is any number between 0 and 640000 bps. *Note*: If you want the rule to apply to an input track of any bit rate range, enter 0 here and 640000 in the **Bitrate High** field.	*Empty*
Bitrate High	Enter the highest input audio bit rate for which the rule will apply. Acceptable value is any number between 8000 and 640000 bps. *Note*: If you want the rule to apply to an input track of any bit rate range, enter 640000 here and 0 in the **Bitrate Low** field.	*Empty*
Language	Enter the language of the audio track for which this rule will apply. • This field may contain only 3 characters and must comply to the ISO639-2 language code standard. • The code "*any*" is a valid entry option and will apply the rule to an audio track of any language.	any

Table 17. Audio Map container fields - rule

Name	Description	Default
Publishing Type	Select the type of audio output that will be published when all input conditions have been met. Choices are: **Primary**, **Primary+AudioOnly**, **AudioOnly**, **Do Not Publish**. See Table 18 on page 78 for a detailed description of these publishing types and how they may vary based on player.	Primary
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

Audio Output Publishing Options

Four types of output publishing options are available when a rule condition is matched. Based on the delivery protocol, each publishing option has a specific behavior. Table 18 describes each condition:

Table 18. Audio map behavior based on delivery protocol

Output Publishing Type	HLS Behavior	HDS Behavior	MSS Behavior
Primary	Matching audio will be published as the *default* audio with the video.	Matching audio will be published as the *default* audio with the video.	Matching audio will be *published*.
Primary + Audio Only	Matching audio will be published as the *default* audio with video **-and-** offered as an *audio-only* feed.	Same as Primary: matching audio will be published as the *default* audio with the video.	Same as primary: matching audio will be *published*.
Audio Only	Matching audio will be published by itself as an *audio-only* feed (no video)	*Ignores* this rule, and proceeds to next rule for a match. If no match is found, audio is considered *alternate*.	*Ignores* this rule and proceeds to next rule for a match.If no match is found, audio is *published*.
Do Not Publish	Matching audio will be *dropped* at the input and will not appear in any generated output.	Matching audio will be *dropped* at the input and will not appear in any generated output.	Matching audio will be *dropped* at the input and will not appear in any generated output.
No Rule Match	Input audio that does not match any rule will be published as a *non-default* feed.	Input audio that does not match any rule will be published as an *alternate* feed.	Input audio that does not match any rule will be *published*.

Profile Container — JITP Only

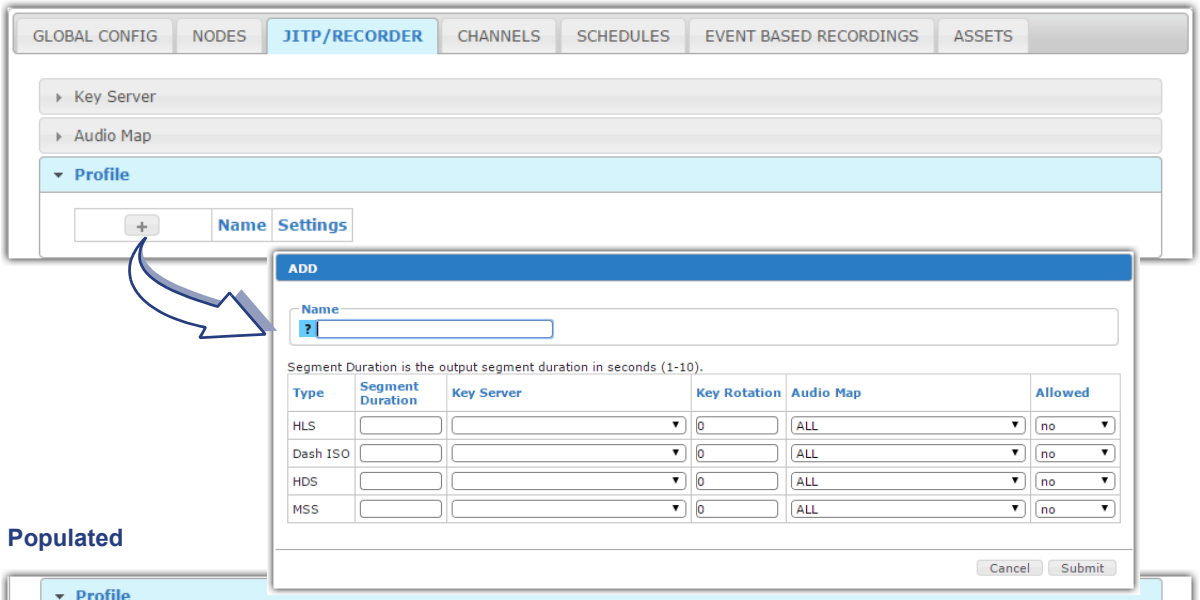
The **Profile** container applies only for JITP servers in the RM cluster, not to Recorders. The **Profile** container provides the ability to set variables for JITP profile tables that determine whether an output format is allowed for packaging and how that format is handled in terms of segment duration, audio map rules, and key servers.

Caution: *When modifying system values for JITP, the asset cache for all the JITP servers in the RM clusters will be will be flushed and ongoing playback may fail and need to be restarted. It is advisable to perform these actions only during a scheduled maintenance window.*

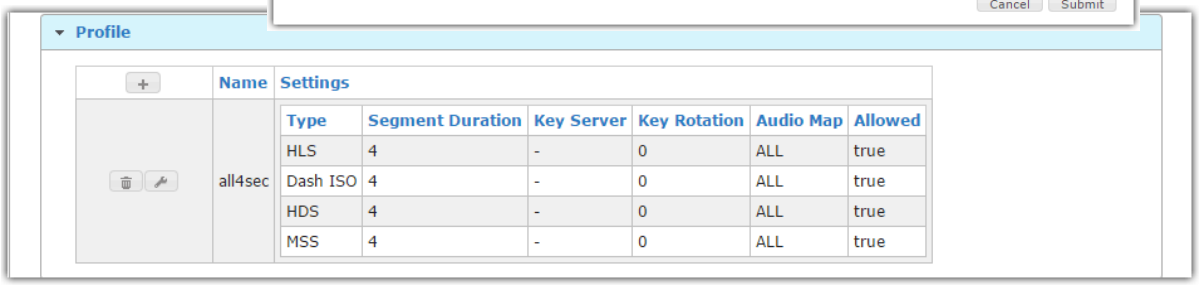
To view the **Profile** container, navigate to:

CONFIGURATION → JITP/RECORDER → Profile → *[expand]* **→** *[expand again]*

Default



Populated



Configuring a Profile

You can add( ), modify ( ), or delete ( ) a player profile from this menu, using Table 19 below for guidelines.

Table 19. Profile container fields - template name

Name	Description	Default
Name	Specifies the name of the profile. This field can be up to 23 alphanumeric characters long. *Note:* Once the **Name** has been saved to the RM database, it *cannot* be modified. If you wish to change the name, you must delete the entry and add a new one.	*Empty*
Type	Specifies the output package format for which the JITP settings will apply. Available types are: HLS, DASH ISO, HDS, and MSS	*n/a*
Segment Duration[a]	Specifies the recording length (in seconds) of each segment for the specified player. For HLS, if this field is set to 0, no additional segmentation will be performed for this package type and the HLS stream will be passed through as is.	*Empty*
Key Server	Specifies which, if any, encryption key server to use. Drop-down box populates with key servers configured in the **Key Server** container.	*Unselected*
Key Rotation *(minutes)*	Specifies the duration of time (in minutes) that a particular encryption key will be used. After the time period expires, a new encryption key will be required. Enter 0 or leave blank for no rotation.	0
Audio Map	Specifies which audio map template and associated rules to use for the player. Drop-down box populates with audio maps configured in the **Audio Map** container.	*Unselected*
Allowed	Specifies whether the package format will be allowed for JIT packaging. Choices are **yes** or **no**.	false
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

a. The first frame for each fragment is an IDR frame or RAI flag.Therefore, the fragment duration specified with periodic modes is not an absolute, but a minimum target. The final duration will be based on how far the IDR or RAI frames are from the fragment duration. For example: an IDR periodic fragment duration of 3 seconds with IDRs inbound at a 2 second interval will produce 4-second fragments.

Source Server Container — JITP Only

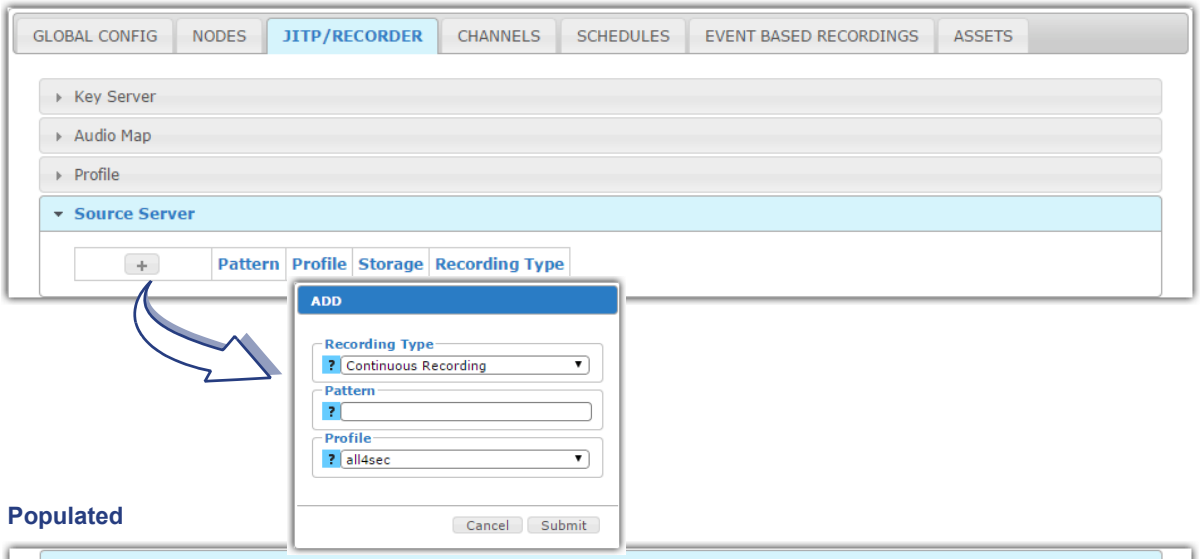
The **Source Server** container applies only for JITP servers in the RM cluster, not to Recorders. The **Source Server** defines where inbound content is stored for JITP.

Caution: *When modifying system values for JITP, the asset cache for all the JITP servers in the RM clusters will be flushed and ongoing playback may fail and need to be restarted. It is advisable to perform these actions only during a scheduled maintenance window.*

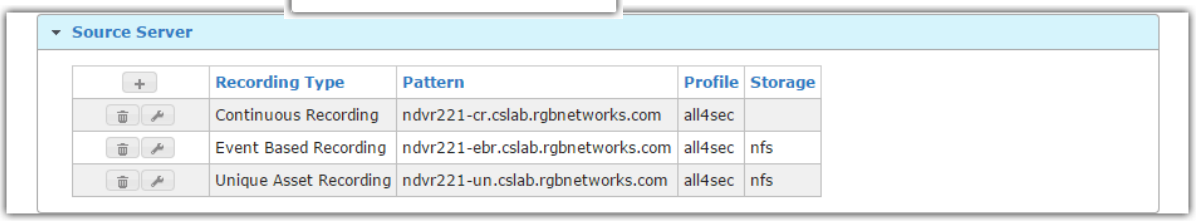
To view the **Source Server** container, navigate to:

CONFIGURATION → JITP/RECORDER → Source Server → *[expand]*

Default



Populated



Configuring a Source Server

You can add(+), modify (🔧), or delete (🗑) a source server from this menu, using Table 20 below for guidelines..

Table 20. Source Server container fields - template name

Name	Description	Default
Recording Type	Specifies which type of recording for which the Source Server settings will apply. Choices from the drop-down menu are: *Continuous Recording*, *Event Based Recording*, or *Unique Asset Recording*	Continuous Recording
Pattern	Specifies the identifier for the source server that contains the inbound content for Just-in-Time packaging. It is used to map to a valid hostname, or a directory ID for a file system mount. • Can be up to 255 characters (`a-z`, `0-9`, `-` [dash] and `.` [dot]) • Pattern cannot *begin* or *end* with a dash *Note*: This entry cannot be the management IP address or host name.	*Empty*
Profile	Specifies the output package profile for which the JITP settings will apply. The drop-down list is populated from the **Profile** container.	*Unselected*

Table 20. Source Server container fields - template name

Name	Description	Default
Storage	Specifies the storage server for which the Source Server settings will apply. The drop-down list is populated with the storage devices configured in the **CONFIGURATION > NODES > Storage Mounts** container. *Note*: This option is only displayed when *Event Based Recording* or *Unique Asset Recording* is set as the *Recording Type*.	*Preselected with first Storage Mount entry*
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

Channels Sub-tab

The **CHANNELS** sub-tab allows you to create or delete channels from transcoded output that the RM will use to schedule recordings; it also provides a snapshot view of all configured channels.

Channels Sub-tab Tour

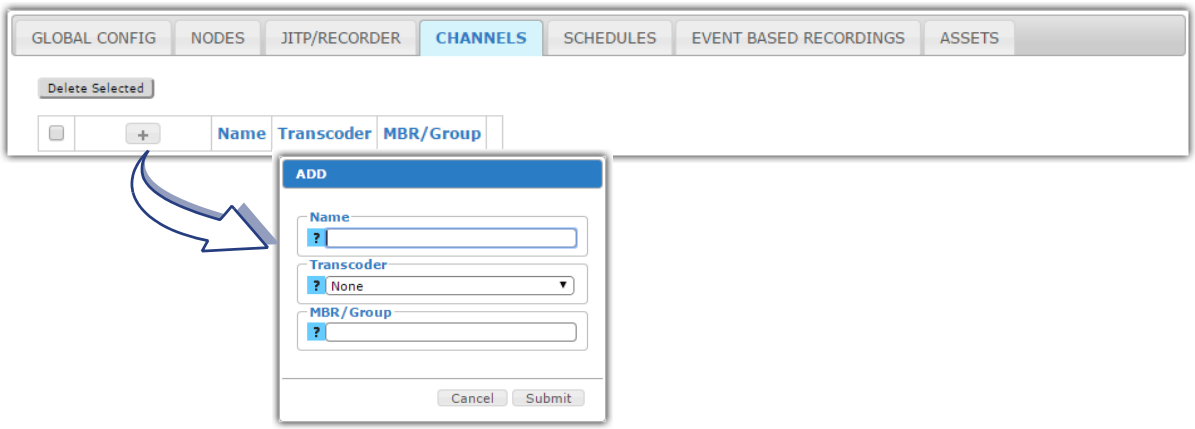
To view the **CHANNELS** sub-tab, navigate as follows:

CONFIGURATION > **CHANNELS**.

Default View

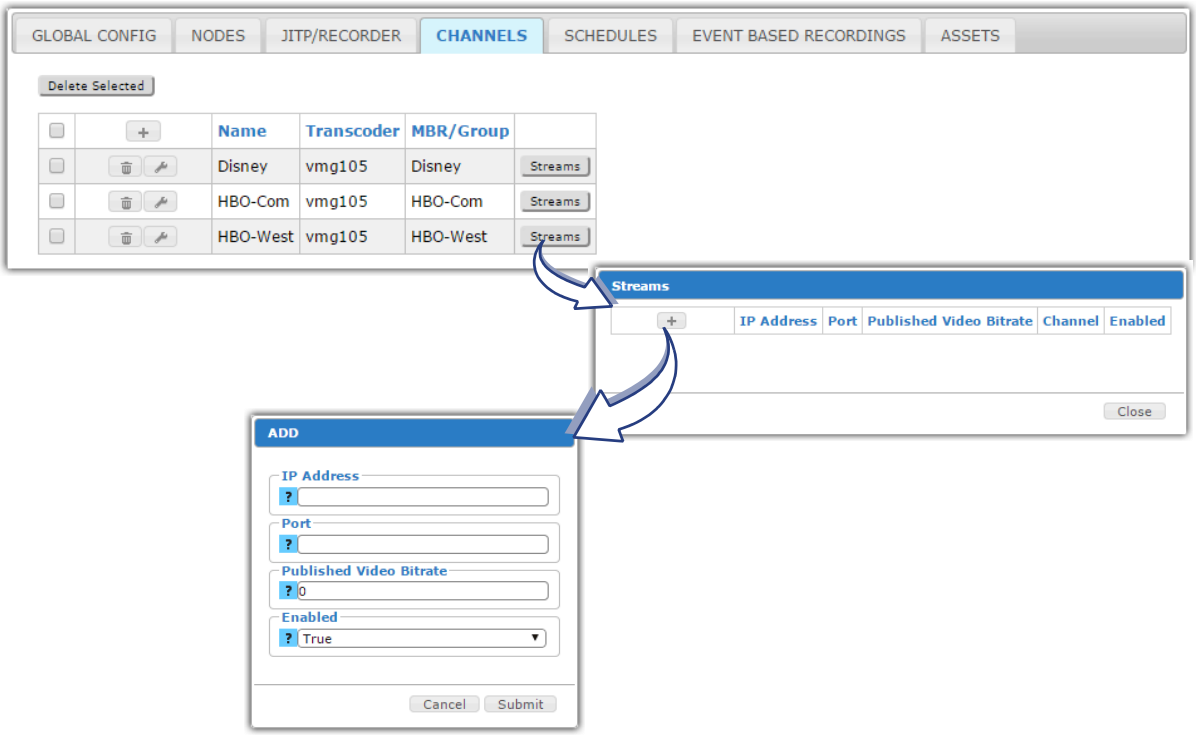
When you first view this menu, no channels will be configured and the window will appear as follows:

Channels tab - no channels configured



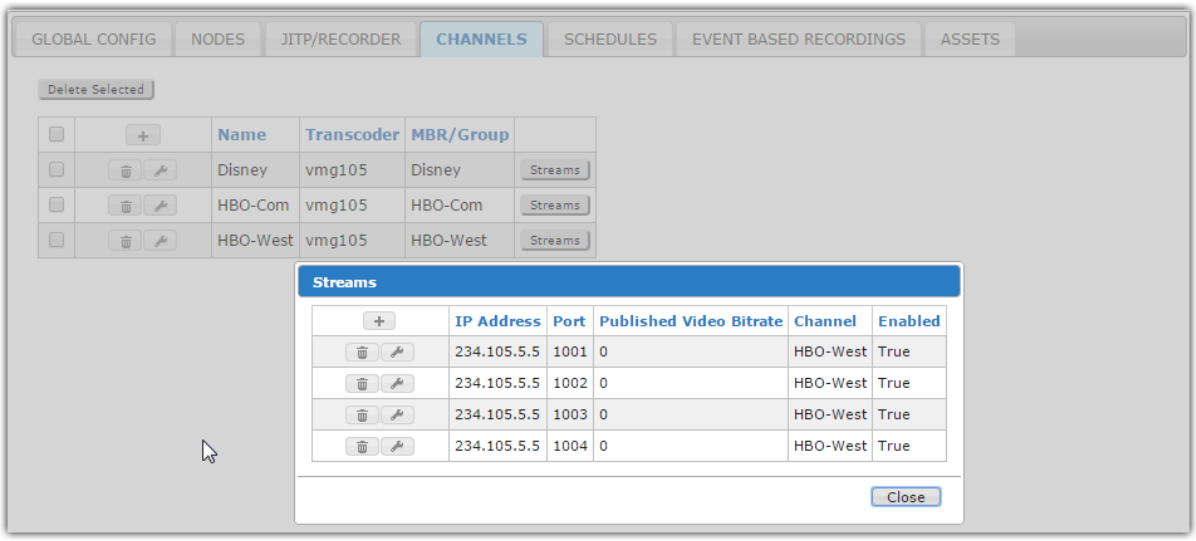
Configured View - Collapsed

A configured **Channels** sub-tab will appear similar to the following:



Configured View - With Streams

Clicking on the Streams button will open a pop-up window that allows entry of individual streams for a particular channel, similar to what is shown below.



Configuring Channels and Streams

You can add( ), modify ( ), or delete ( ) a channel and its streams from this menu, using Table 21 below for guidelines.

Table 21. Channels sub-tab fields

Name / Type	Description	Default
Channel container fields		
Name	Specifies the name of the channel. This field can be up to 23 alphanumeric characters long. *Note:* Once the **Name** has been saved to the RM database, it *cannot* be modified. If you wish to change the name, you must delete the entry and add a new one.	*Empty*
Transcoder	Specifies which transcoder the channel will use for its input. When in edit mode, the drop-down box is populated with the list of transcoders configured from the **CONFIGURATION > NODES > Transcoders** container.	*Unselected*
MBR / Group	**Optional.** Specifies the name of the VMG's MBR or another transcoder's Group ID output transport stream group that will be associated with the channel. This field is for reference only.	*Empty*
Stream container fields (Note: Click the "Streams" button to open the pop-up configuration window)		
IP Address	Specifies the multicast IP address(es) to which the transcoder is sending its output. Valid entries are: 224.0.0.1 – 239.255.255.254. Refer to iana.org for details. *Note:* If using Source Specific Multicasting (SSM), you *must* use only this range: 232.0.0.1 – 232.255.255.254.	*Empty*
Port	Specifies the UDP (User Datagram Protocol) port of the multicast source on which the transcoder is sending its output. If the *MBR / Group* field is used, the IP Address and Port entries will be auto-populated. Valid range is 1 – 65535	*Empty*
Published Video Bitrate	Specifies the video bit rate at which the transcoded stream is being published. Enter 0 (zero) or leave blank to have *RM* use the bit rate it detects from the input stream.	0
Enabled	Specifies whether the selected stream is enabled or disabled for channel recording.	True
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

Creating Channels and Streams

Creating a channel entails adding a row entry to the **Channels** sub-tab and configuring the streams within the channel.

To create a channel, proceed as follows:

1. From the **CONFIGURATION > CHANNELS** menu, click "**+**" to open the ADD menu.
2. Fill out the fields according to the descriptions for channels in Table 21 on page 84.
3. Click *Submit* to save and add the channel to the RM database.
4. Click the **Streams** button for the desired channel row entry.

   A pop-up **Streams** menu will open.
5. Click "**+**" to open the stream's ADD menu.
6. Fill out the fields according to the descriptions for streams in Table 21 on page 84.
7. Click *Submit* to save the stream to the RM database.
8. Click "**+**" in the same **Streams** pop-up to add additional streams to the channel.
9. Click "+" in the **Channels** container to add additional channels.

Schedules Sub-tab

The **SCHEDULES** sub-tab is where all event based recording (EBR) and continuous recording (CR) is scheduled. From here you can create new recording schedules, check the status of currently scheduled recordings, import and export recording schedules, and perform detailed search queries of all recordings.

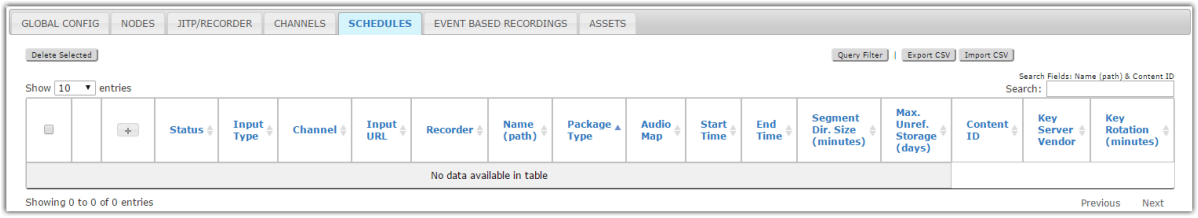
Schedules Sub-tab Tour

To view the **SCHEDULES** sub-tab, navigate as follows:

CONFIGURATION > SCHEDULES.

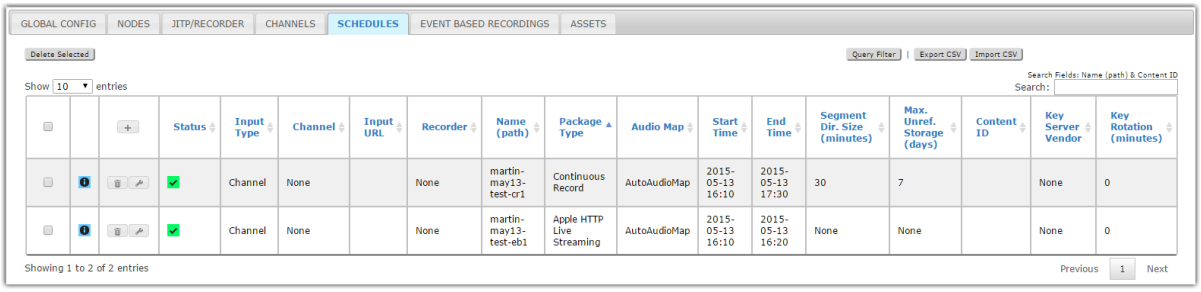
Default View

When you first view this menu, no recordings will be scheduled and the window will appear as follows:



Configured View

A configured **SCHEDULES** sub-tab will appear similar to the following:



Configuring Schedules

You can add( ), modify ( ), or delete ( ) a scheduled recording from this menu, using Table 22 below for guidelines.

Table 22. Schedules sub-tab fields

Name / Type		Description	Default
Fields			
	Status	Indicates the current status of the scheduled recording. Refer to Table 7 on page 44 for definitions.	*Read-only*
	Input Type	Indicates whether the program input originates via Channel or URL. If the Recorder is ingesting a UDP stream, select **Channel**. If the Recorder is ingesting HLSv2, select **URL**.	
	Input URL	Specifies the input URL location. Only used if Input Type is URL (i.e., the Recorder is ingesting HLSv2)	*Empty*
	Channel	Specifies the name of the channel on which the recording is scheduled. When creating a new schedule, a drop-down box of options that were defined in the CONFIGURATION > CHANNELS sub-tab will be displayed.	*Preselected with first channel configured*
	Recorder	Specifies the name of the Recorder on which the recording is scheduled. When creating a new schedule, a drop-down box of options that were defined in the CONFIGURATION > NODES > *Recorders* container will be displayed.	*Preselected with first Recorder configured*
	Name (path)	Specifies the unique directory path where the recording is placed. When creating a new schedule, this path must be defined. Valid entries ranges are 1 - 200 alphanumeric characters.	*Empty*

Table 22. Schedules sub-tab fields

Name / Type	Description	Default
Package Type	Specifies the type of package that is recorded. When creating a new schedule, choose one of the following from the drop-down box: • **Continuous Record** — For all package types where the recording will be CR *EBR Recordings:* • **Apple HTTP Live Streaming** • **MPEG Dash TS** • **RGB Packager Asset** • **Adobe HTTP Dynamic Streaming** • **Microsoft Smooth Streaming** • **Adobe HTTP Dynamic Streaming - HTTP File Format**	*Unselected*
Audio Map	Specifies the name of the Audio Map rules that the recording is using. When creating a new schedule, a drop-down box of options that were defined in the CONFIGURATION > JITP/RECORDER > Audio *Map* container will be displayed.	*Preselected with first Audio Map configured*
Start Time	Specifies the start time of the scheduled recording. When creating a new schedule, an interactive scheduling calendar will pop-up. Refer to "Scheduling Calendar" on page 89 for usage guidelines. Leaving this field empty will start the recording immediately upon clicking the *Save* icon.	*Empty*
End Time	Specifies the end time of the scheduled recording. When creating a new schedule, an interactive scheduling calendar will pop-up. Refer to "Scheduling Calendar" on page 89 for usage guidelines. Leaving this field empty will record content with no stop time, i.e., forever, upon clicking the *Save* icon. *Note:* The max length of an EBR is 18 hours. The max length of a CR is only limited to the amount of disk space available on the storage server.	*Empty*
Segment Dir. Size (minutes)	**For CR only.** Specifies the duration (in minutes) of each recorded segment directory. For example, if you specify a Segment Duration of 30 minutes, then each segment directory will contain 30 minutes worth of chunked TS files. When creating a new schedule, this field is optional; if left blank, the numbers specified in the *Configuration* > *Main* > *Global* container are used. Any value entered here will override the defaults from the *Global* container.	*Empty*

Table 22. Schedules sub-tab fields

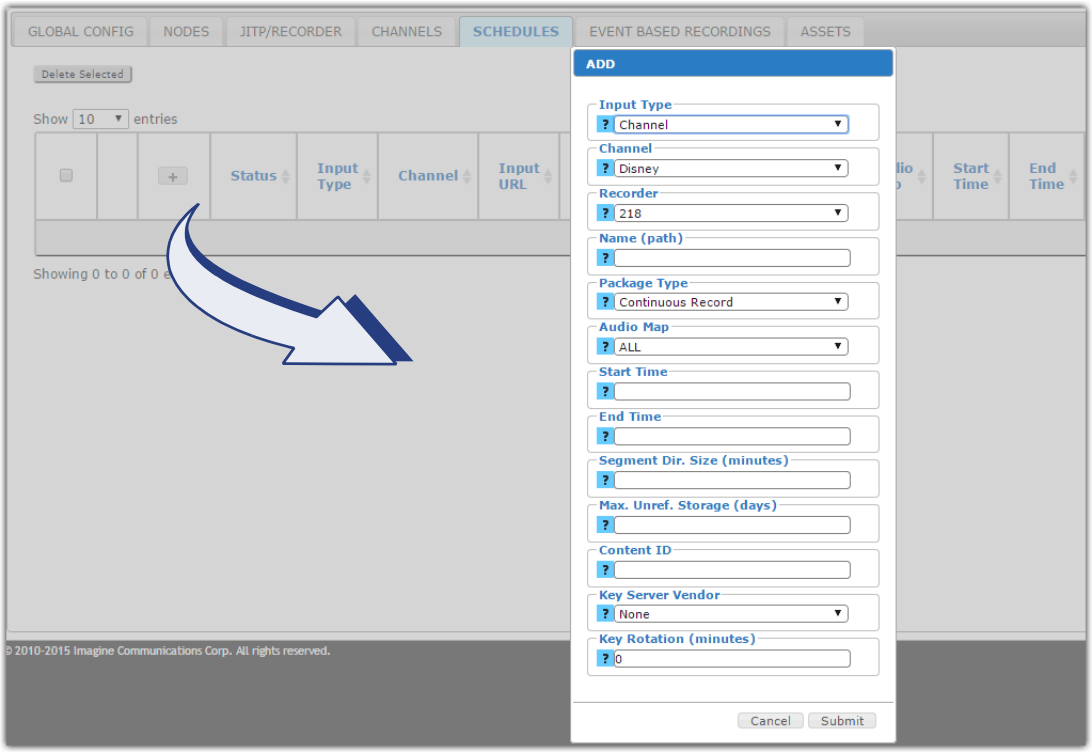
Name / Type	Description	Default
Max. Unref. Storage (days)	**For CR only.** Specifies the maximum number of days that an unreferenced CR segment directory (i.e., a segment of a recording that has not been used for asset creation) will be stored before it is automatically deleted. When creating a new schedule, this field is optional; if left blank, the number specified in the *Configuration* > *Main* > *Global* container is used. Any value entered here will override the defaults from the *Global* container.	*Empty*
Content ID	Specifies a description of encrypted content. This field is used by some key management servers to identify the content. Example: demo:RC001. Leave this field empty if no key server is used or if no Content ID for the key server is used.	*Empty*
Key Server Vendor	Specifies which key server vendor will be used for the channel. Choices from the drop-down box are: None, Verimatrix HLS, Nagra[a], Verimatrix PlayReady, Internal PlayReady, Mezzanine[b], KPN, and PlayReady Leaf.	None
Key Rotation *(minutes)*	Specifies the duration of time (in minutes) that a particular encryption key will be used. After the time period expires, a new encryption key will be required. Enter 0 or leave blank for no rotation.	0
Buttons		
Query Filter *button*	Clicking this button will open the *Query Filters* window in which you can search and filter an entry based on various parameters	n/a
Delete Selected *button*	When one or more scheduled recording entries are selected, clicking this button will delete the selected schedules. *Note:* You can select all rows at once to delete all, as shown in Figure 3 on page 43.	n/a
Export (CSV) *button*	Clicking this button will export the current list of all scheduled recordings to a Comma Separate Value (CSV) list that can be viewed in a program such as *Microsoft Excel*.	
Import (CSV) *button*	Clicking this button will import a desired list of scheduled recordings to a Comma Separate Value (CSV) list that can be viewed in a program such as *Microsoft Excel*. Any new schedules from this file will be appended to existing schedules.	
	Click this button to add a new entry.	n/a
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

a. This option is only available for use with HLSv2, which is a beta-only feature for this release.
b. For CR only: A choice of Mezzanine encryption will configure the Recorder to encrypt CR segments stored to disk.

Creating a Schedule

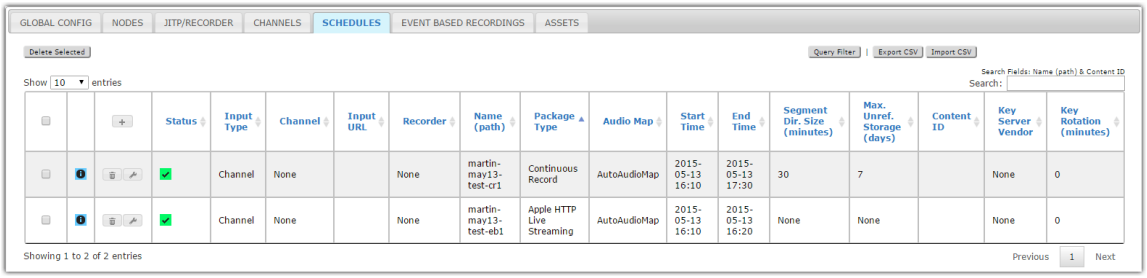
To create a new recording schedule, proceed as follows:

1. From the **CONFIGURATION > SCHEDULES** menu, click "**+**" to open the ADD menu.



2. Fill out the fields according to the descriptions for channels in Table 22 on page 86.
3. Click *Submit* to save and add the schedule to the RM database.

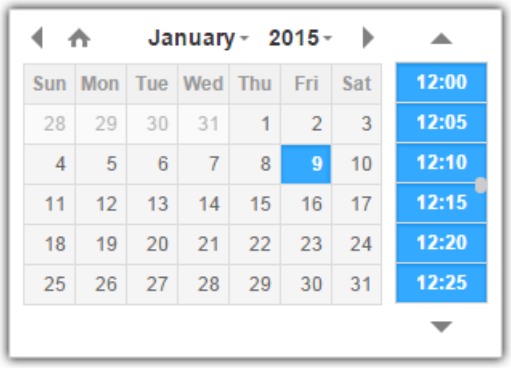
   A new row entry container and its recording status will be added to the **SCHEDULES** menu.

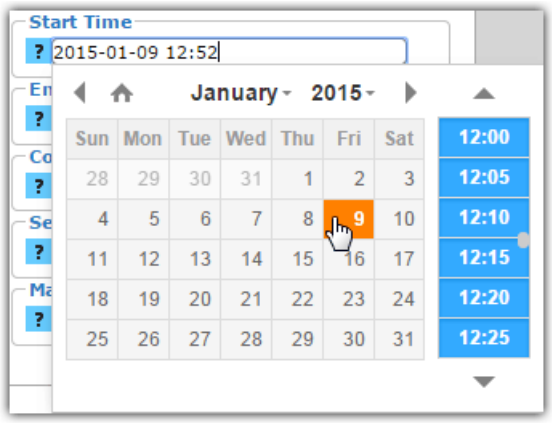


Scheduling Calendar

When creating a new recording schedule or asset, you can specify the start and end time of the EBR or CR. For CR, leaving the start and end times blank will start recording immediately and record indefinitely once the values have been saved. you can leave this field blank to either automatically start the recording once the values have been saved When the **Create Schedule** or **Create Asset** window is

displayed, clicking on the **Start Time** or **End Time** field produces an interactive calendar for ease of scheduling:





You can enter start and end times in one of two ways:

- Typing the date and time manually in the relevant fields;
- Clicking the highlighted current date, which will automatically enter the current date and time.
- Clicking on the desired date and using the time slider to the right of the date to adjust start/end time.

For Continuous Record only:

- In addition to the above three options, if you are scheduling a CR from the **SCHEDULES** tab, leaving the start time empty will automatically start the recording as soon as the schedule is saved, and leaving the end time empty will record content indefinitely with no stop time.

Or, you can use a combination of all of the above as suits your needs.

Note: *When clicking the current date in order to start the recording immediately, we recommend that you adjust the time up by one minute in order to ensure the current time does not pass before you save the schedule. For example: if you have scheduled the recording to start at 12:10 PM and the current time is 12:10 PM, if the time changes to 12:11 PM before you save the schedule, you will receive an error that the start time has passed when trying to save the schedule.*

Modifying a Recording Schedule

You can modify various aspects of a recording schedule depending on whether the recording has begun. To modify a recording schedule, proceed as follows

1. From **CONFIGURATION > SCHEDULES**, locate the recording you wish to modify and click the "wrench" icon to modify.
2. If the recording has not yet begun you can modify any field as described in Table 22 on page 86.

   If the recording has already begun, but not yet ended, the only parameter you can modify is the **End Time** (refer to the "Scheduling Calendar" on page 89).
3. Click *Submit* to save changes to the RM database.

Deleting a Recording Schedule(s)

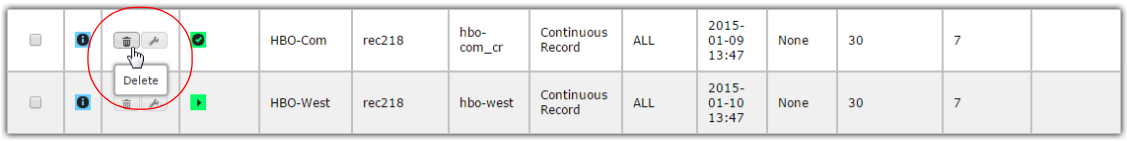
You can delete one or more recording schedules at any time, regardless of whether the recording has begun.

Note: *Deleting a recording schedule does not delete the actual recording. When you delete a schedule after recording has begun, the recording is effectively stopped.*

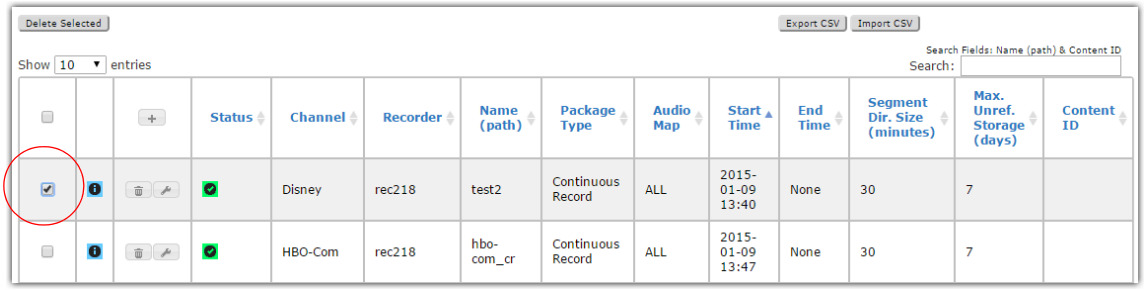
To delete one or more schedules, you can do one of three things from **CONFIGURATION > SCHEDULES** tab:

- *To delete a single schedule*, locate the schedule(s) you wish to delete and click the "trash" icon next to the row entry.
  -or-
- *To delete multiple schedules* at once, click to check the deletion box next to the row entries you wish to delete, then click the **Delete Selected** button.
  -or-
- *To delete all schedules*, click the selection box at the top of the **SCHEDULES** window to select all schedule, then click the **Delete Selected** button.

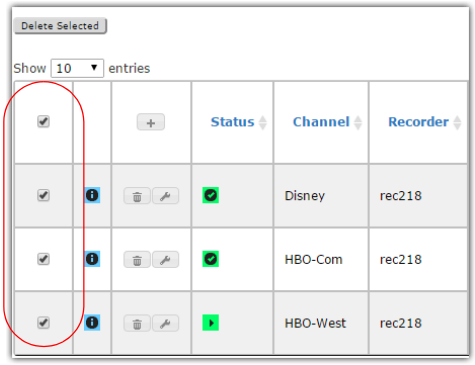
Delete single schedules



Delete one or more schedules



Delete all schedules



Event Based Recordings Sub-tab

The **Event Based Recordings** sub-tab provides information about completed EBR programs. From here you can view storage links for recordings. No configuration is performed from this sub-tab; it is for viewing or deleting only.

Event Based Recordings Sub-tab Tour

To view the **Event Based Recordings** sub-tab, navigate as follows:

CONFIGURATION > EVENT BASED RECORDINGS.

EBR items whose recordings have been completed or are in process will appear in this window. Below is an example:

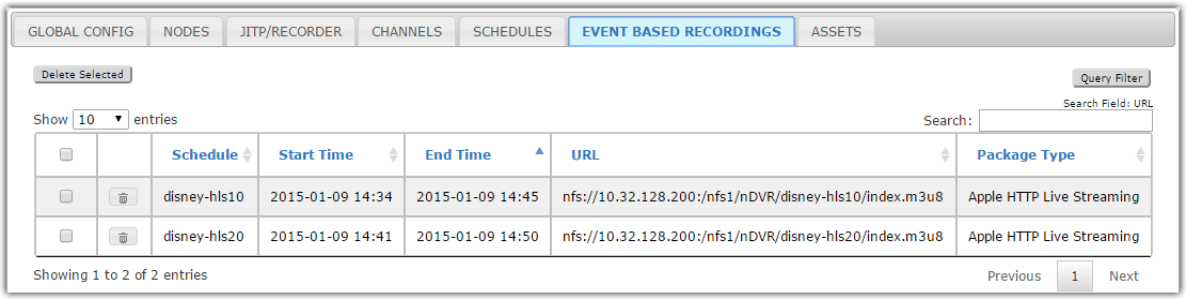


Table 23 describes the fields and buttons in the **Event Based Recordings** sub-tab.

Table 23. Scheduler sub-tab fields

Name / Type	Description
Channel Name	Displays the name of the recorded channel.
Start Time	Displays when the recording started.
End Time	Displays when the recording ended.
URL	Displays the path, on the storage server, where the recording stream can be found.
Package Type[a]	Displays the type of EBR package that has been recorded. One of the following options will be displayed in this column: • Apple HTTP Live Streaming • MPEG Dash TS • RGB Packager Asset • Adobe HTTP Dynamic Streaming • Microsoft Smooth Streaming • Adobe HTTP Dynamic Streaming - HTTP File Format
Delete Selected *button*	When one or more recorded entries are selected, clicking this button will delete the recording from the storage server. *Note:* You can select all rows at once to delete all as shown in Figure 3 on page 43.
Query Filter *button*	Clicking this button will open the *Query Filters* window in which you can search and filter an entry based on various parameters.

a. In order to record a particular Package Type, the Recorder(s) must have the proper Package Type licensing.

Using the EBR URL to View a Recording

You can use the URL provided in the Event Based Recording sub-tab to view a recording on a media player that supports the package type. To view the event based recording using the URL, do one of the following:

- For links with **HTTP** in the URL (and no Mezzanine encryption), the URL provided in the tab can be used as is.
- For links with **NFS** in the URL (or with Mezzanine encryption), the URL can be viewed from the JITP server, and the link must be modified as follows:

  ```
  http://[JITP Source Server Pattern]/[schedule name]/index.[manifest type]
  ```

  For example:
  ```
  http://ndvr-jitp3.lab.ripcode.com/dec22/testeb1/index.m3u8
  ```

Note: *When using MSS as an output format, a "/Manifest" must be added to the "index.ism" portion as follows: index.ism/Manifest*

Deleting a Recording(s) from RM

You can delete recordings from the RM's database.

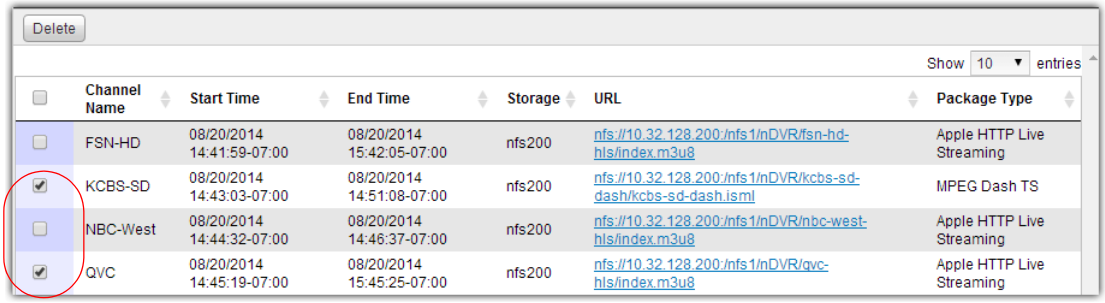
Note: *Deleting a recording from the* RM's database does not delete the recording from the storage server; it only deletes the reference from the database. To delete a recording form the storage server, you must delete the relevant files directly from the storage server.

To delete one or more recordings from the ,RM's database, proceed as follows:

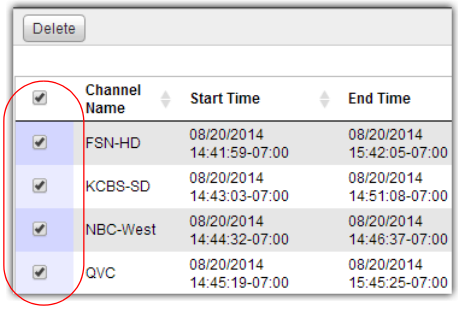
1. From **Configuration > Event Based Recording**, locate the recording(s) you wish to delete and click the selection box next to the row entry.

   Or, if you want to delete all schedules, click the selection box at the top of the *Scheduler* window.

Delete single recordings



Delete all recordings



2. Click the **Delete** button.
3. Confirm the deletion message by clicking **OK**.

Assets Sub-tab

The **Assets** sub-tab is where you can create viewable assets from segments that have been or are in the process of being continuously recorded.

Prerequisite

Prior to creating a CR asset, you must have first created a recording schedule for the intended asset as described in "Schedules Sub-tab" on page 85.

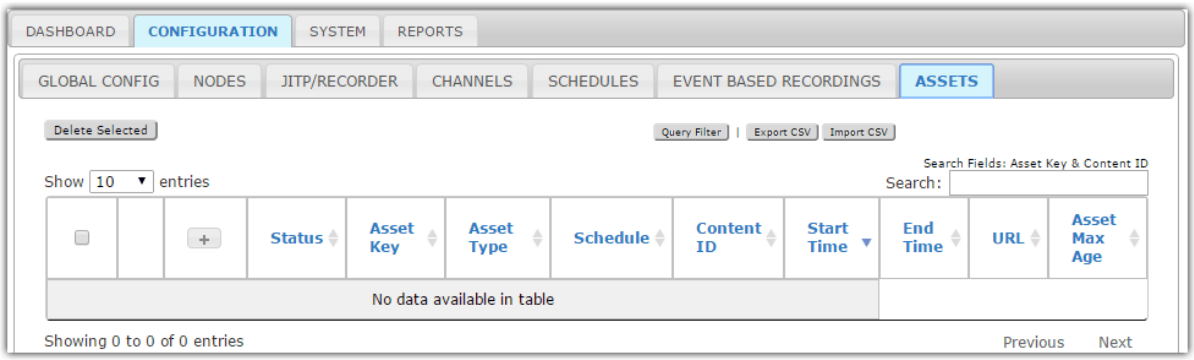
Assets Sub-tab Tour

To view the **Assets** sub-tab, navigate as follows:

Configuration > Assets.

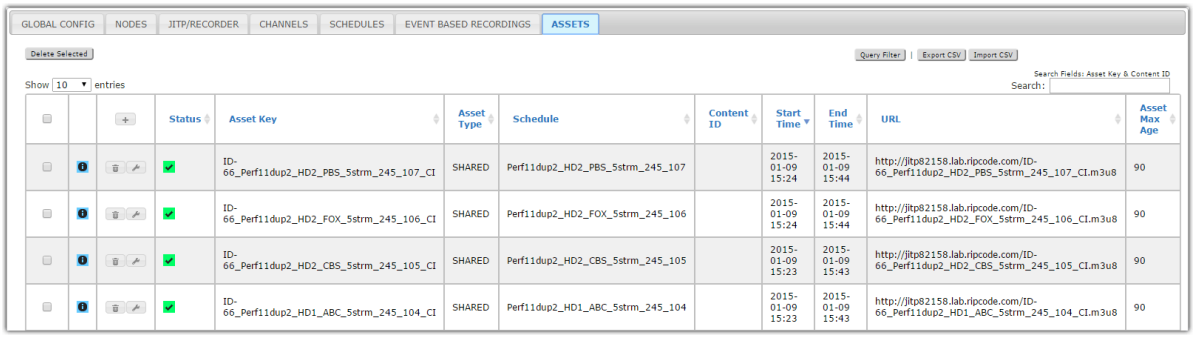
Default View

When you first view this menu, no assets will be listed and the window will appear as follows:



Configured View

A configured **Assets** sub-tab can look like this:



Configuring Assets

You can add(+), modify (🔧), or delete (🗑) an asset from this menu, using Table 24 below for guidelines.

Table 24. Assets sub-tab fields

Name / Type	Description	Default
Fields		
Status	Indicates the current status of the scheduled CR assets. One of four status icons will be displayed. Refer to Table 7 on page 44 for definitions.	*Read-only*
Asset Key	Specifies the unique directory path under which the asset is placed. When creating a new asset, this path must be defined. Valid entries ranges are 1 - 200 alphanumeric characters.	*Empty*
Asset Type	Specifies whether the asset will be shared (one recording available for all subscribers) or unique (one unique recording for each requesting subscriber). Choices are: SHARED or UNIQUE	Shared

Table 24. Assets sub-tab fields

Name / Type	Description	Default
Schedule	Specifies the name of the schedule from which the asset is being created. When creating a new asset, a drop-down box of options that were defined in the **CONFIGURATION > SCHEDULE** sub-tab will be displayed[a].	*First schedule in table*
Content ID	If the **CONFIGURATION > JITP/RECORDER > Profile** container was configured to use a key encryption server, the value here specifies the Content ID that the asset will use for encryption by the JITP server. This field is alphanumeric.	*Unselected*
Start Time	Specifies the start time of the created asset. When creating a new asset, an interactive scheduling calendar will pop-up. Refer to "Scheduling Calendar" on page 89 for usage guidelines. *Note:* In order for an asset to be created, the CR segments must either be present or scheduled to be present for the asset's start / end time range. For example, assume you have created a CR schedule on the channel named *Disney* from the present day at 1:00 PM to the following day at 1:00 PM. If you attempt to create an asset from this recording that starts or ends outside of this range (starting or ending, for example, at 12:00 PM on the present day), the asset will fail to be created.	*Empty*
End Time	Specifies the end time of the created asset. When creating a new schedule, an interactive scheduling calendar will pop-up. Refer to "Scheduling Calendar" on page 89 for usage guidelines. *Note:* The max length of a CR is only limited to the amount of disk space available on the storage server.	*Empty*
URL	Displays the path, on the JITP server, where the asset stream can be found.	*Read-only*
Buttons		
Query Filter *button*	Clicking this button will open the *Query Filters* window in which you can search and filter an entry based on various parameters.	*n/a*
Export (CSV) *button*	Clicking this button will export the current list of all assets to a Comma Separate Value (CSV) list that can be viewed in a program such as *Microsoft Excel*.	
Import (CSV) *button*	Clicking this button will import a desired list of assets to a Comma Separate Value (CSV) list that can be viewed in a program such as *Microsoft Excel*. Any new assets from this file will be appended to existing assets. *NOTE*: If the start time of the asset occurs in the past, the asset will **not** be imported.	
Delete Selected *button*	When one or more asset entries are selected, clicking this button will delete the selected asset(s). *Note:* You can select all rows at once to delete all as shown in Figure 3 on page 43.	
	Click this button to add a new entry.	n/a

Table 24. Assets sub-tab fields

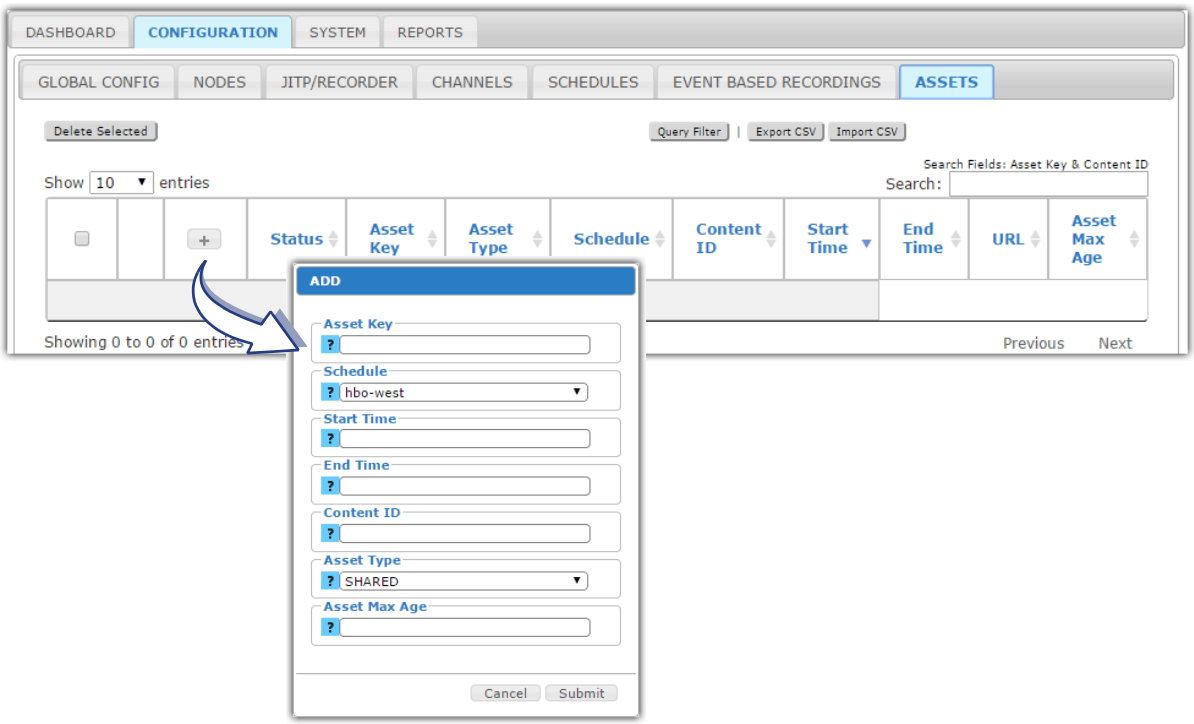
Name / Type	Description	Default
	Click this button next to an entry you wish to delete.	n/a
	Click this button to modify parameters for an existing entry.	n/a

a. When creating a new asset from a newly created schedule, you must refresh the browser in order to populate the *Schedule* drop-down box with the new schedule.

Creating an Asset

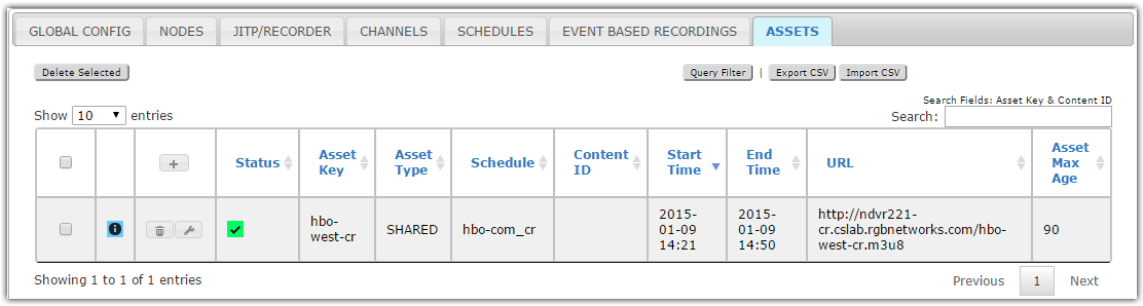
To create a new asset, proceed as follows:

From the **CONFIGURATION > ASSETS** menu, click "**+**" to open the ADD menu:



1. Fill out the fields according to the descriptions for channels in Table 24 on page 95.
2. Click *Submit* to save and add the asset to the RM database.

   A new row entry container and its recording status will be added to the **ASSETS** menu.



Scheduling Calendar

Refer to "Scheduling Calendar" on page 89 for instructions on using the **ASSETS** *Scheduling Calendar*.

Modifying an Asset

In this release, only the end time can be modified once an asset has been created. In order to change other parameters, you must delete the asset.

Deleting an Asset(s)

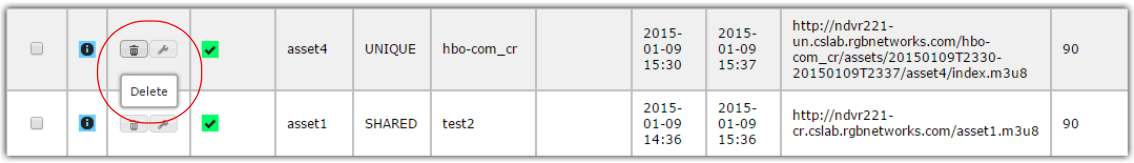
You can delete one or more assets at any time.

Note: *Deleting an asset does not delete the asset from the storage server; it only deletes the reference to the recorded segments. Continuous Record assets can only be automatically deleted by the RM according to the parameters set up from either the GLOBAL CONFIG tab or for the individual asset.*

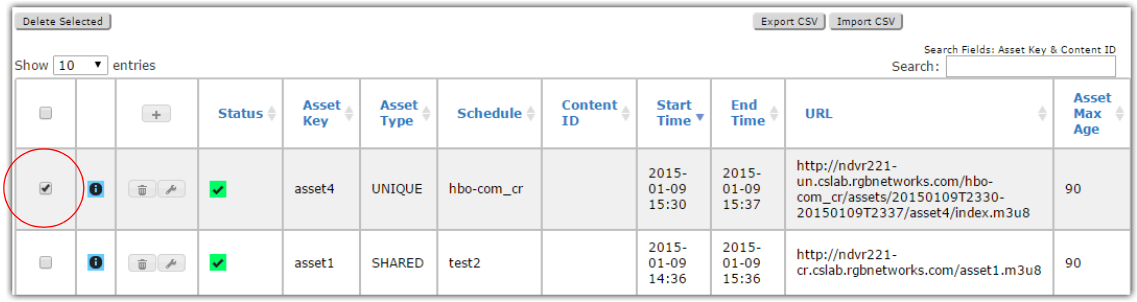
To delete one or more assets from the RM, you can do one of three things from the **CONFIGURATION > ASSETS** tab:

- *To delete a single asset*, locate the schedule(s) you wish to delete and click the "trash" icon next to the row entry.
  -or-
- *To delete multiple assets* at once, click to check the deletion box next to the row entries you wish to delete, then click the **Delete Selected** button.
  -or-
- *To delete all assets*, click the selection box at the top of the **ASSETS** window to select all assets, then click the **Delete Selected** button.

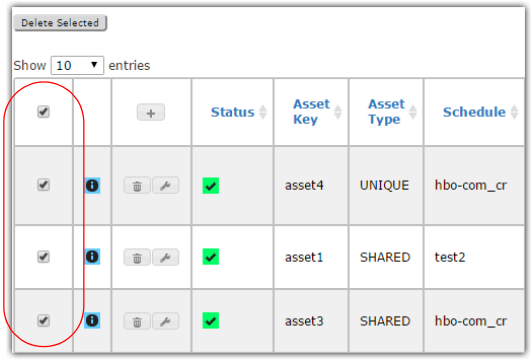
Delete single asset



Delete one or more assets



Delete all assets



Using the Assets URL to View a Recording

You can use the URL provided in the Assets sub-tab to view a completed or in-progress asset on a media player that supports the package type. To view the asset on a media player using the URL, you will need to modify the provided URL as follows (depending on whether encryption is being used):

For links where no Mezzanine encryption is used and HLS is the desired output format, one of two options is available:

- Copy the relevant link as shown in the **ASSETS** tab and paste it into a media player[3]
  -Or-
- Use the following format:
  `http://[JITP Source Server Pattern]/[Asset Key].[manifest type]`[4]

For links where Mezzanine encryption is used, the following format must be used:

3. When content is recorded using direct NFS access instead of HTTP access, you must formulate the link using the JITP source server pattern.
4. When using MSS as an output format, a "`/Manifest`" must be added to the "index.ism" portion as follows: **`index.ism/Manifest`**

`http://[JITP Source Server Pattern]/[Asset Key].[manifest type]`[5]

Content Management

The RM is responsible for removing unused or out-of-date recordings.

How content is deleted depends on whether the recordings are event-based or continuous record. If the recording is event-based, you must delete the content manually from the storage server; if the recording is CR, the content is automatically deleted based on how you have configured your system.

How EBR Content is Stored

Event-based recording content must be manually deleted from the storage server. To delete EBR content, you must delete the relevant files from the storage server you configured in the **CONFIGURATION > NODES > Storage Mounts** menu.

EBR Storage Structure

For NFS or GPFS, when manually deleting EBR content, you should delete the EBR-based directory and all its contents, including sub-directories.

For example, assume you have created an EBR schedule named, "Program-1." The file structure for this EBR schedule will look like this:

`../<Storage Mount Location>/`**`Program-1/`**`<Segment Directories & manifest>/<content>.ts`

The files in the *Program-1* directory will contain manifest files and content directories that will look similar to the following:

```
# pwd
/nfs1/nDVR/Program-1
# ls -l
drwxr-xr-x 2 678 678 4096 Oct 17 16:26 01
-rwxrwxrwx 1 678 678 3255 Oct 17 16:26 01.m3u8
drwxr-xr-x 2 678 678 4096 Oct 17 16:26 02
-rwxrwxrwx 1 678 678 3256 Oct 17 16:26 02.m3u8
drwxr-xr-x 2 678 678 4096 Oct 17 16:26 03
-rwxrwxrwx 1 678 678 3295 Oct 17 16:26 03.m3u8
drwxr-xr-x 2 678 678 4096 Oct 17 16:26 04
-rwxrwxrwx 1 678 678 3295 Oct 17 16:26 04.m3u8
drwxr-xr-x 2 678 678 4096 Oct 17 16:26 A1
-rwxrwxrwx 1 678 678 3243 Oct 17 16:26 A1.m3u8
-rwxrwxrwx 1 678 678  650 Oct 17 16:22 index.m3u8
```

5. When using MSS as an output format, a "`/Manifest`" must be added to the "index.ism" portion as follows: **`index.ism/Manifest`**

Drilling down into one of the numbered directories will show video content files similar to the following:

```
# pwd
/nfs1/nDVR/Program-1/01
# ls -l
-rwxrwxrwx 1 678 678 579040 Oct 17 16:23 20141017T182217-01-10vod.ts
-rwxrwxrwx 1 678 678 546704 Oct 17 16:23 20141017T182217-01-11vod.ts
-rwxrwxrwx 1 678 678 546892 Oct 17 16:23 20141017T182217-01-12vod.ts
-rwxrwxrwx 1 678 678 545012 Oct 17 16:23 20141017T182217-01-13vod.ts
-rwxrwxrwx 1 678 678 587500 Oct 17 16:23 20141017T182217-01-14vod.ts
-rwxrwxrwx 1 678 678 556292 Oct 17 16:23 20141017T182217-01-15vod.ts
-rwxrwxrwx 1 678 678 480152 Oct 17 16:23 20141017T182217-01-16vod.ts
-rwxrwxrwx 1 678 678 546140 Oct 17 16:23 20141017T182217-01-17vod.ts
-rwxrwxrwx 1 678 678 560240 Oct 17 16:24 20141017T182217-01-18vod.ts
-rwxrwxrwx 1 678 678 531664 Oct 17 16:24 20141017T182217-01-19vod.ts
-rwxrwxrwx 1 678 678 495568 Oct 17 16:24 20141017T182217-01-20vod.ts
-rwxrwxrwx 1 678 678 510984 Oct 17 16:24 20141017T182217-01-21vod.ts
```

Assume you wish to delete the recording whose schedule/path you named "Program-1." You must remove the schedule name directory and its contents as shown in red below:

`/nfs1/nDVR/`**`Program-1/`**`<Segment Directories & manifest>/<content>.ts`

How CR Content is Deleted

Continuous Record content can only be deleted automatically, the method of which is performed based on how you have configured the global or schedule-based deletion parameters as defined below.

CR Storage Parameters

These parameters can be found in the **Configuration > Main > Global** container, or via the **CONFIGURATION > ASSETS -> *ADD*** menu on a per-schedule basis (which overrides what is configured in the Global container).

- Segment Directory Size (minutes)—A segment directory contains individual content fragments, which include transport stream chunks and manifest files. When you set this value for a duration (for example, 30 minutes) the size of the segment directories that contain the content fragments will not exceed the equivalent of 30 minutes (or whatever value is set).
- Segment Unreferenced Age (days)—If there have been no assets created from any of the individual content fragments in the segment directory, the entire directory will be deleted after the number of days you specify (for example, 7 days). If one or more of the content fragments has been referenced as an asset, the entire segment directory is considered referenced and follows the deletion rules for the *Asset Max Age* parameter.
- Asset Max Age (days)—If an asset has been created from any of the individual content fragments in the segment directory, the segment directory associated with the asset will be deleted after the number of days you specify (for example, 90). Setting the *Asset Max Age* to a period longer than the *Segment Unreferenced Age* will ensure any unreferenced segments are deleted before asset-referenced segments.

Deletion Mechanism Functionality

The CR automatic content deletion mechanism runs as a cron job on the RM and is performed every 24 hours at a set time[6], at which point the RM will perform a calculation from the prior 24 hours to determine the age and reference status of all segments. The mechanism then deletes the segments according to the parameters described above. Schedule-based deviations in parameters will override global parameters for schedules in which the values differ.

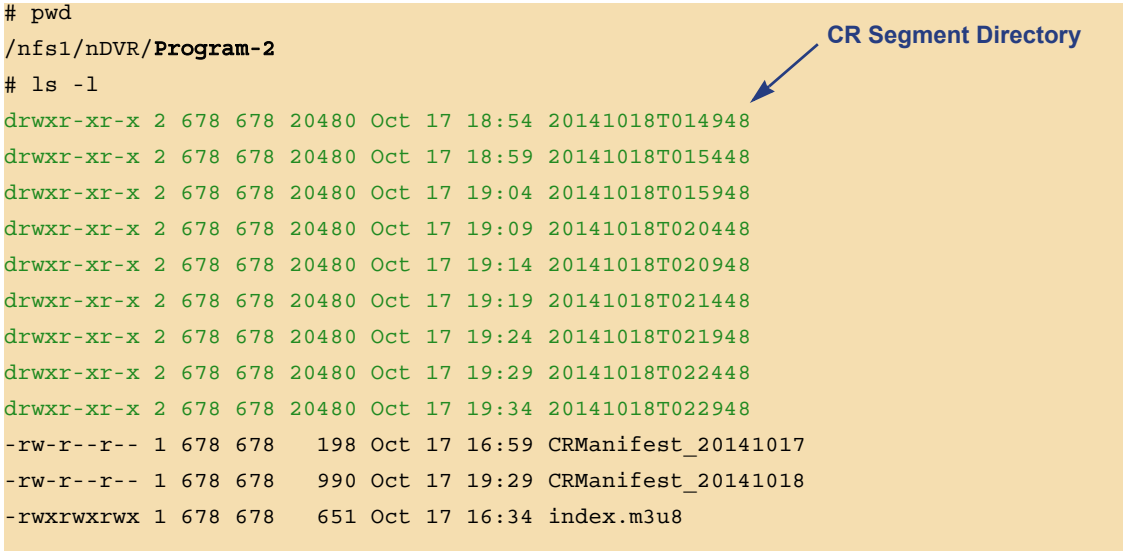
The deletion mechanism operates at the segment directory level. That is to say, if a particular segment directory contains both referenced and unreferenced fragments, the mechanism does not drill down to this level and remove only the applicable fragments. The segment directory and all its fragments are either recursively deleted or fully preserved.

What is Deleted

For NFS or GPFS, as an example, assume you have created a CR recording under a schedule named, "Program-2." The file structure for this CR schedule will look like this:

```
../<Storage Mount Location>/Program-2/<Segment Directories & manifest>/<.ts files & manifests>
```

The files in the *Program-2* directory will contain manifest files and segment directories that will look similar to the following:




```
# pwd
/nfs1/nDVR/Program-2
# ls -l
drwxr-xr-x 2 678 678 20480 Oct 17 18:54 20141018T014948
drwxr-xr-x 2 678 678 20480 Oct 17 18:59 20141018T015448
drwxr-xr-x 2 678 678 20480 Oct 17 19:04 20141018T015948
drwxr-xr-x 2 678 678 20480 Oct 17 19:09 20141018T020448
drwxr-xr-x 2 678 678 20480 Oct 17 19:14 20141018T020948
drwxr-xr-x 2 678 678 20480 Oct 17 19:19 20141018T021448
drwxr-xr-x 2 678 678 20480 Oct 17 19:24 20141018T021948
drwxr-xr-x 2 678 678 20480 Oct 17 19:29 20141018T022448
drwxr-xr-x 2 678 678 20480 Oct 17 19:34 20141018T022948
-rw-r--r-- 1 678 678   198 Oct 17 16:59 CRManifest_20141017
-rw-r--r-- 1 678 678   990 Oct 17 19:29 CRManifest_20141018
-rwxrwxrwx 1 678 678   651 Oct 17 16:34 index.m3u8
```

6. Currently, this time may not be changed.

Drilling down into one of the numbered segment directories will show video content and manifest files similar to the following:

```
# pwd
/nfs1/nDVR/Program-2/20141017T233448
# ls -l
-rwxrwxrwx 1 678 678    6321 Oct 17 16:39 01.m3u8
-rwxrwxrwx 1 678 678    6322 Oct 17 16:39 02.m3u8
-rwxrwxrwx 1 678 678    6318 Oct 17 16:39 03.m3u8
-rwxrwxrwx 1 678 678    6318 Oct 17 16:39 04.m3u8
-rwxrwxrwx 1 678 678  515496 Oct 17 16:35 20141017T183448-01-10vod.ts
-rwxrwxrwx 1 678 678  515872 Oct 17 16:35 20141017T183448-01-11vod.ts
-rwxrwxrwx 1 678 678 1013320 Oct 17 16:36 20141017T183448-02-21vod.ts
-rwxrwxrwx 1 678 678 1015952 Oct 17 16:36 20141017T183448-02-22vod.ts
-rwxrwxrwx 1 678 678 1962156 Oct 17 16:37 20141017T183448-03-24vod.ts
-rwxrwxrwx 1 678 678 1897484 Oct 17 16:37 20141017T183448-03-25vod.ts
-rwxrwxrwx 1 678 678 1915908 Oct 17 16:37 20141017T183448-03-26vod.ts
-rwxrwxrwx 1 678 678 2403392 Oct 17 16:39 20141017T183448-04-47vod.ts
-rwxrwxrwx 1 678 678 2570712 Oct 17 16:39 20141017T183448-04-48vod.ts
-rwxrwxrwx 1 678 678   48692 Oct 17 16:35 20141017T183448-A1-5vod.ts
-rwxrwxrwx 1 678 678   48692 Oct 17 16:35 20141017T183448-A1-6vod.ts
-rwxrwxrwx 1 678 678   48692 Oct 17 16:35 20141017T183448-A1-9vod.ts
-rwxrwxrwx 1 678 678    6269 Oct 17 16:39 A1.m3u8
-rwxrwxrwx 1 678 678     651 Oct 17 16:35 index.m3u8
```

Based on the parameters you set up in "CR Storage Parameters" on page 101, the CR automatic content deletion mechanism will determine whether the content files are asset-based or unreferenced. For CR, deletion occurs at the segment directory level (unlike manual EBR deletion where deletion occurs at the schedule/name level). Using the example above, if any of the .ts or .m3u8 files are associated with an asset, the entire segment directory one level up (for example, the directory named "20141018T014948") will either be preserved or deleted depending on how the age parameters were configured.

In other words, everything in red below will either be deleted or preserved, and everything in black will never be deleted (unless done so manually on the storage server itself):

`/nfs1/nDVR/Program-2/<Segment Directories & manifest>/<.ts files & manifests>`

CHAPTER 8

System Configuration

This chapter covers all maintenance and system-related tasks for Telurio Recording Manager, such as licensing, networking parameters, redundancy configuration, software upgrades, database backups, and configuring SNMP and syslog servers. All tasks in this chapter are performed from the **System** tab in the GUI.

System configuration that is necessary prior to configuring cDVR is listed at the beginning of this chapter

In This Chapter:

Prerequisite System Configuration

Before performing any other cDVR component configuration (from the **Configuration** tab), ensure the *system* parameters listed in Table 25 are configured on the RM.

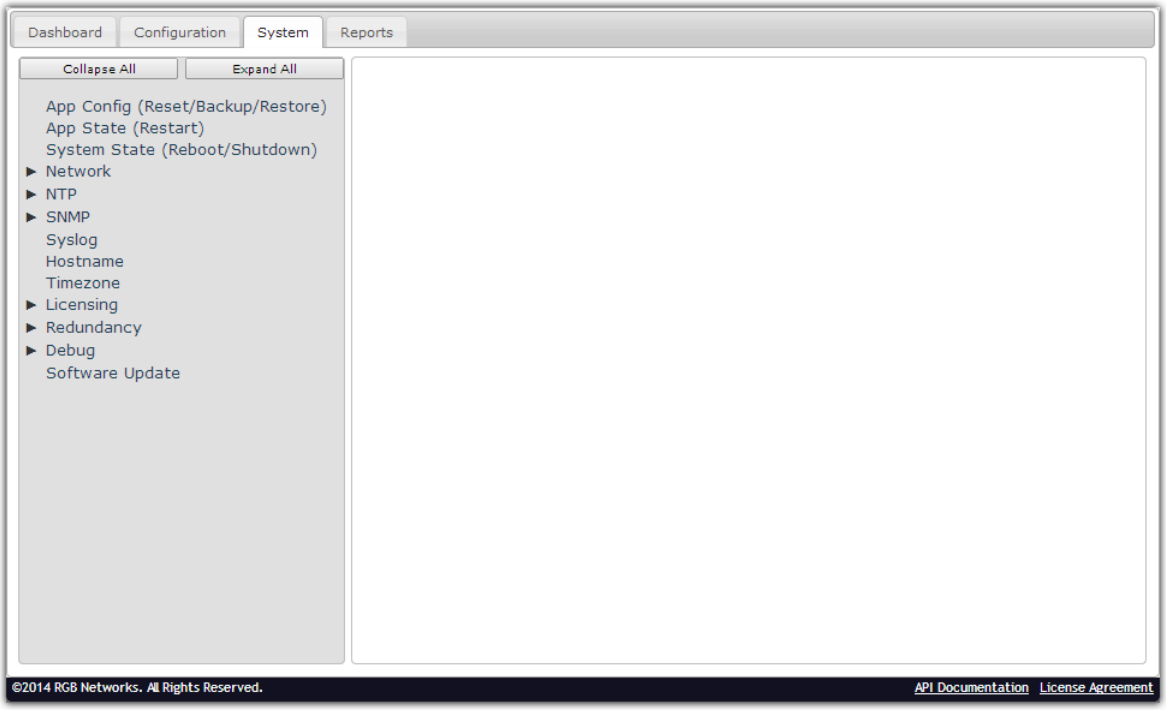
Table 25. Required system configuration before configuring RM

Parameter	For more information, see:	Requirement
RM IP address	"IP Branch" on page 114	Required
Network interface assignment	"Network Interfaces Branch" on page 118	Required
Network routes	"Routes Branch" on page 120	Required
DNS	"DNS Branch" on page 122	Required
NTP server(s)	"NTP Tree" on page 127	Optional, but recommended
Syslog server	"Syslog" on page 135	Optional, but recommended
Hostname	"Hostname" on page 137	Optional, but recommended
Timezone	"Timezone" on page 138	Required if not using NTP server
License key	"License Tree" on page 138	Required
Redundancy	"Redundancy Tree" on page 143	Required if using node-level redundancy

System Tab Navigation

The RM **System** tab is structured in a tree-branch category fashion. Within each main or sub-menu are various configuration options pertinent to its category.

The **System** tab's default view is shown below:



Menu Tree Layout

Table 26 provides an overview of the **System** tab menu tree layout..

Table 26. System tree menu layout

Menu Options			Description
App Config (Reset/Backup/Restore)			Reset, backup, or restore the RM database
App State (Restart)			Restart the RM service application
System State (Reboot/Shutdown)			Reboot or power down the RM
Network			
	IP		
		IP Address Configuration	Configure IP parameters for Ethernet interfaces
		IP Restart	Restart IP services for all Ethernet interfaces
	Ethernet Ports		Displays information about the system Ethernet ports
	Network Interfaces		Configure network interfaces for management or external comm.
	Routes		Configure network routing tables for the RM's Ethernet interfaces
	DNS		Configure a domain name, server, or search path
NTP			
	Server Config		Configure NTP server IP address for system timing
	Server State		Display status parameters of all configured NTP servers
	Server Restart		Restart an NTP server
SNMP			
	Settings		Configure SNMP trap parameters

Table 26. System tree menu layout

Menu Options		Description
	Trap Sink	Set parameters for which type of traps are sent to the server
Syslog		Add or remove a syslog server
Hostname		Set the hostname of the RM
Timezone		Set the timezone the system will use (not required if using NTP)
Licensing		
	Details	Display RM licensing information
	Server	Configure one or more license servers
	Lock Code	Display the license lockcode (required for obtaining a license)
	Update	Configure a new license key for the RM
	Refresh	Set the RM to retrieve new license key details from the server
Redundancy		
	Group	Configure group parameters for the RM's node-level redundancy
	Hosts	Add a redundancy peer to the RM redundancy group
	Failover	Execute a command that causes a failover to another node
	Recover	Execute a command that causes a recovery to the original node
	Registered Apps	Lists applications registered for redundancy message notification
Debug		
	Info	Execute a command to collect or delete system debug information
	Trace	Displays and allows editing for debug log levels
Software Update		Execute a command to update software (or view upgrade status)

System Tab Icons

While navigating in the **System** tab, you will come across various icons as described below in Table 27.

Table 27. System tab icon and button meanings

Symbol	Relevant Tab	Meaning
	Dashboard & System	Indicates more information is available for a particular row entry. **In the Dashboard tab** — only appears when the Events container is expanded. **In the System tab** — appears when more information is available for a particular row entry.
Expand All (button)	System & Reports	Expands all menu trees to their smallest branch
Collapse All (button)	System & Reports	Collapses all branch menus into their menu trees
	System	Clicking directly on the triangle next to the menu tree will expand the menu out one level.
	System	Clicking this button will open a pop-up window for configuration of various fields pertaining to the tree or branch category.
	System	Clicking this button will cause a command to be executed, such as a backup, a restart, or polling for information.

Table 27. System tab icon and button meanings

Symbol	Relevant Tab	Meaning
	System	Clicking this button will add a new row entry to the tree or branch category.
	System	Clicking this button will delete an existing row entry from the tree or branch category.
	System & Reports	Appears when a pop-up box requires input values. Hovering over the question mark will open a tool tip box that gives input information for the relevant field.
	System	Clicking the arrows will either add or remove an entry from a table that will be saved to the RM database.
	System	Clicking the arrows will either move an entry up or down in priority level in a table that will be saved to the RM database.

Contextual Menus

The configuration menus within the **System** tab are contextually based; that is, upon choosing a specific entry from a drop-down box, the remaining menu options will provide only those additional fields relevant to your selection.

App Config (Reset/Backup/Restore)

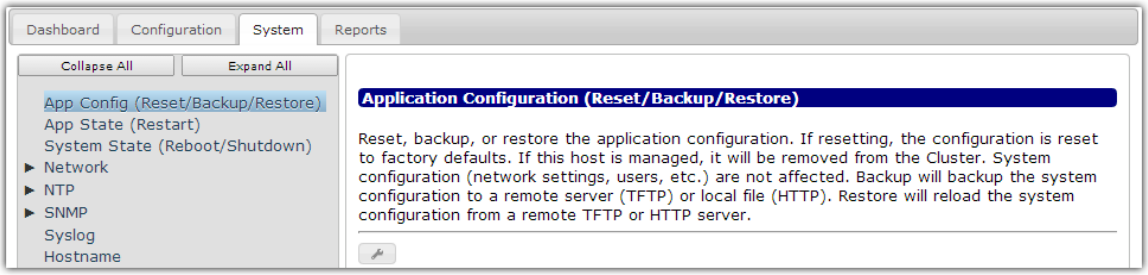
The RM has a database where it stores its system configuration. You can manage the database application configuration in three ways:

- **Reset** application configuration to factory defaults; this action does not reset the entire system to factory defaults, and only resets the License Server configuration if that configuration is stored in `/var/ripcode/DB`.
- **Backup** the system configuration to either a remote Trivial File Transfer Protocol (TFTP) server or via HTTP (which places the backup file on the RM).
- **Restore** system configuration to an RM from a remote TFTP server or via HTTP (from the RM or from an HTTP server).

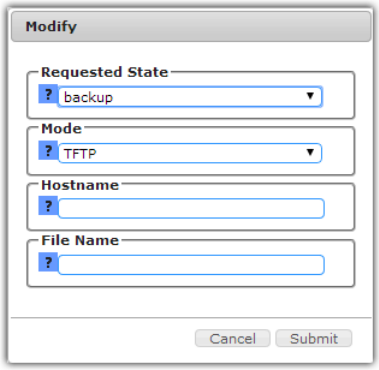
Menu Access and Usage

To access and use the **App Config** menu, proceed as follows:

1. From the **System** tab, click on the **App Config (Reset/Backup/Restore)** entry.



2. Click the wrench ( ) icon to open the *Modify* window:



3. From the **Requested State** field, choose the type of database management action you wish to perform (see Table 28 for details)
4. Select or enter the options relevant to the action you wish to perform from the remaining contextual drop-down fields.
5. Click **Submit** to execute the database task.

Menu Options

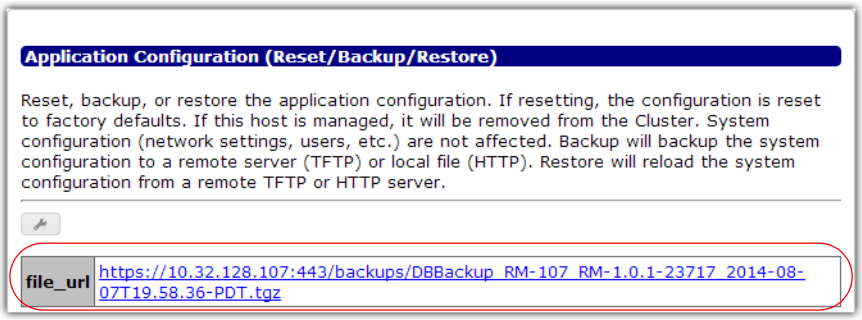
The menu options available in the **App Config** menu are described in Table 28.

Table 28. App Config menu options

Name	Description	Default
Requested State	Choose which type of database action you wish to perform. Choices from the drop-down menu are: *Backup, Restore*, and *Reset*	Backup
Mode	Select the mode to use for the database backup or restore. Choices are: TFTP or HTTP. For backup or restore: If you select **TFTP**, the backup files will be saved to or imported from the host and directory location you specify in the *Host* and *File Name* fields. For backup: If you select **HTTP**, there are no options for location or file name as the backup files will automatically be saved to RM's hard drive. *Note:* When using HTTP as a backup method, only one backup file (the most recent) is stored on the RM's hard drive at a time. Imagine Communications advises that you retrieve or download any existing backup file prior to executing another HTTP backup, otherwise it will be deleted. For restore: If you select HTTP, the backup files will be restored from the URL you specify in the *File Name* field.	TFTP
Hostname	**Required for TFTP.** The remote Trivial File Transfer Protocol (TFTP) server hostname or IP address to which the backup file should be sent or from which the backup file should be restored. *Not relevant for HTTP*	Empty
File Name	For TFTP backup: enter the name to assign to the backup file. The file will automatically be appended with .tgz. For TFTP restore: enter the name of the backup file to restore. If you do not specify a **.tgz** extension in this field, RM will append one. For HTTP restore: enter the full URL (including file name) of the backup file to restore. For example: `https://10.10.30.187/backups/DBBackup_jax-vm1_Packager-5.2-22183_2014-03-10T21.53.03-CDT.tgz`	Empty
Redundancy	Only appears when **restore** is chosen for *Requested State*: Choose whether redundancy settings (if found) from the backup file will be restored to the RM. Selecting **true** will restore all discovered redundancy settings to RM and will allow RM to join its configured Redundancy Group. Selecting **false** will not restore any discovered redundancy settings and will automatically configure RM as a standalone host.	False

View HTTP Backup File Location

If you used HTTP as the mode of backup, the link to the most recent backed up file will automatically be displayed in the **System > App Config** menu as shown below:



Note: *Only one backup file is maintained on the RM at a time. Subsequent HTTP backups will delete any existing backup file.*

Restoring a Database for Redundant RMs

A few extra steps are required in order to successfully restore a database to a redundant pair of RMs. These steps are listed below.

Caution: *Before restoring a database, ensure you have a backup file to use as the restore file. The backup must be performed from either the VIP or the physical IP address of the **Active** RM while the Standby and Active nodes were linked via their redundancy group. For information on setting up redundancy, refer to* "RM Redundancy Setup" on page 32.

1. Log in to the VIP of the redundancy group.
2. Navigate to the **System > Redundancy > Hosts** menu
3. Delete the entry for the *Standby* host. Do **not** delete the *Active* host's entry.

   The redundancy group should still be in tact, of which the Active host should still be its only member. The Standby host should come back online as a standalone system with an empty database.
4. From the **System > App Config (Reset/Backup/Restore)** menu, open the *Modify* window (click on the wrench), and select the following parameters:

   Requested State: **restore**
   Mode: **[Choose TFTP or HTTP]**
   Hostname: **[If using TFTP, enter the Hostname where the restore file is located]**
   File Name: **[Enter the name of the restore file]**
   Redundancy: **True**

Caution: *You must ensure the Redundancy flag is set to True, otherwise redundancy configuration will not be properly restored.*

5. Wait until the *Standby* (now a standalone) has finished its DB reset and has completely restarted as a standalone system.
6. Log in to the physical IP address of the *Standby*.

7. Repeat step 4 using the same file that you used to restore the *Active*.

   The Standby RM should now be part of the *Active's* redundancy group and in an Idle state when seen from the *Active's* **System > Redunancy > Group** menu.

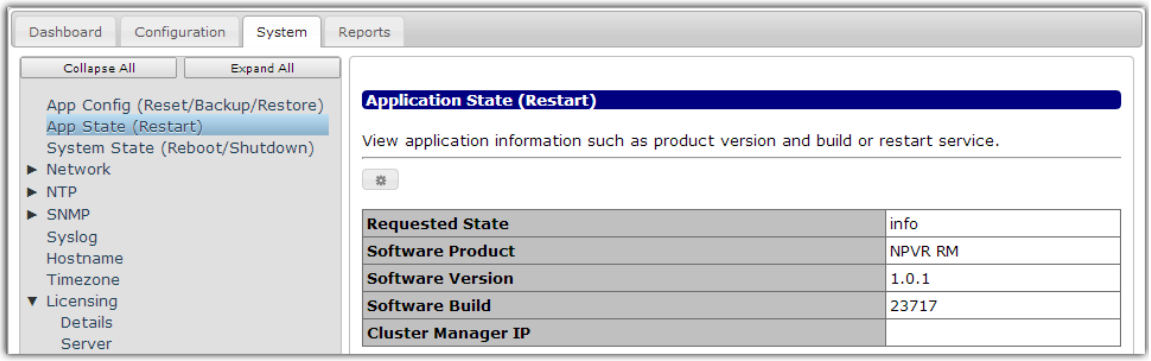
App State (Restart)

You can view key information about the RM as well as restart the RM application, which will restart all application-related services. An application restart does not restart the device on which the RM is loaded, however, all RM-related management activities will be stopped and started again.

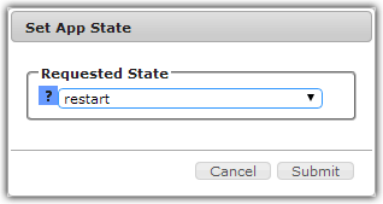
Menu Access and Usage

To access and use the **App State** menu, proceed as follows:

1. From the **System** tab, click on the **App State (Restart)** entry.



2. Click the execute ( ) icon to open the **Set App State** window:



3. From the **Requested State** field, the **Restart** value will already be chosen.
4. Click **Submit** to execute the restart immediately.

Menu Options

The menu options available in the **App State** menu are described in Table 29.

Table 29. App State menu options

Name	Description	Default
Requested State	Displays the current state of the application. When viewing the *Application State (Restart)* window, this will be set at *Info*. When opening the *Set App State* window, the **restart** option will be chosen.	info / restart
Software Product	Displays the type of application product	NPVR RM
Software Version	Displays the software version of the RM	Auto-filled
Software Build	Displays the software build number of the RM	Auto-filled
Cluster Manager IP	Displays whether this node belongs to a redundancy cluster and which node is the cluster's leader.	n/a

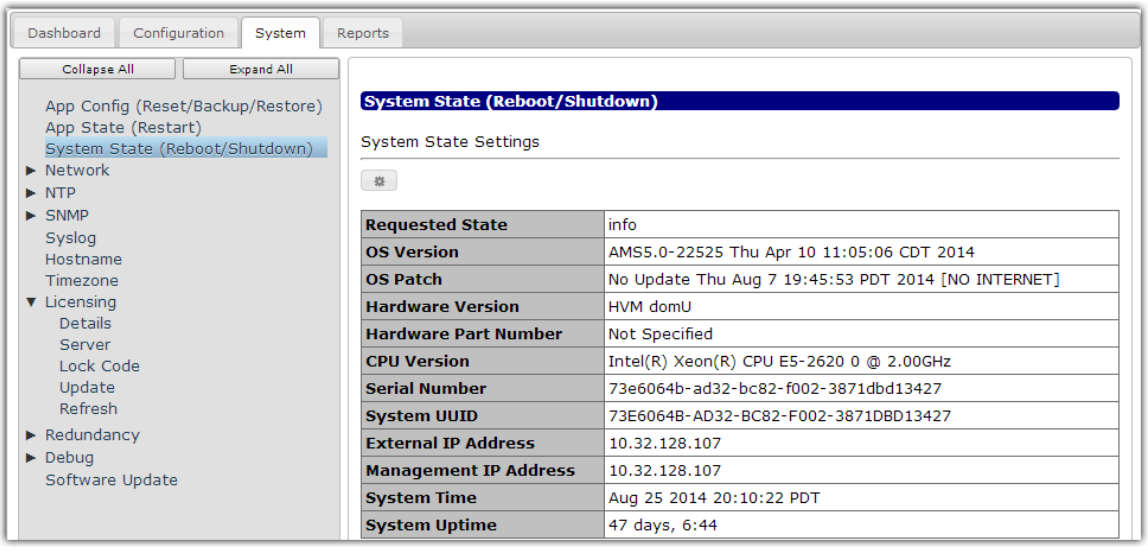
System State (Reboot/Shutdown)

You can view key information about the device on which RM is running as well as reboot or power down the device.

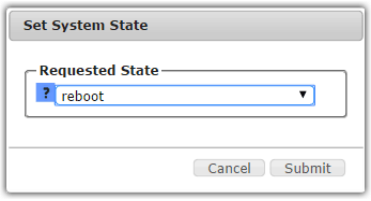
Menu Access and Usage

To access and use the **System State** menu, proceed as follows:

1. From the **System** tab, click on the **System State (Reboot/Shutdown)** entry.
   System status information is displayed in the menu.



2. To initiate a reboot or shutdown, click the execute ( ) icon to open the **Set System State** window:



3. From the **Requested State** field, select whether to Reboot or Shutdown the hardware (or virtual machine).
4. Click **Submit** to execute the reboot or shutdown immediately.

Network Tree

The **Network** tree contains branch menus for viewing, configuring, and performing the following RM networking-related parameters:

- IP Branch
- Ethernet Ports Branch
- Network Interfaces Branch
- Routes Branch
- DNS Branch

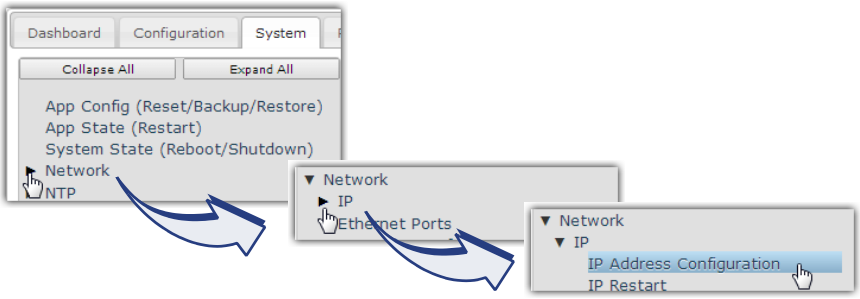
IP Branch

The **IP** branch allows you to restart IP services and configure IP address parameters for the RM's Ethernet interfaces.

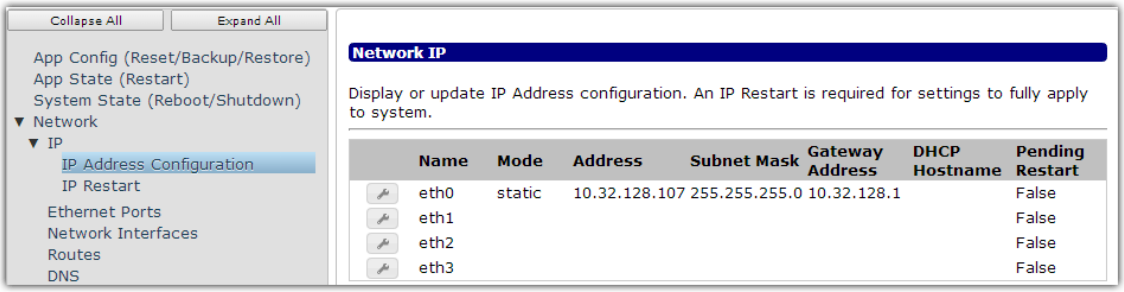
IP Address Configuration — Menu Access and Usage

To access and use the **IP Address Configuration** branch, proceed as follows:

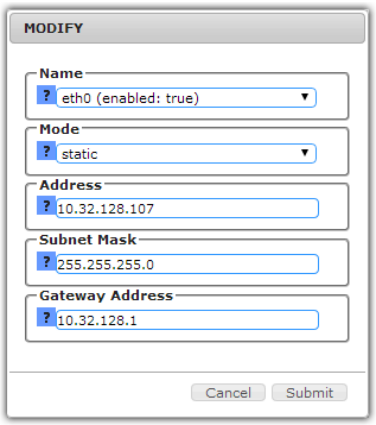
1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.
2. Click on the triangle next to the **IP** branch to expand out one level.



3. Click the **IP Address Configuration** entry to open the *Network IP* window:



4. For configuration, click the wrench ( ) icon next to the desired Ethernet entry to open the *MODIFY* window.



5. Choose values according to your preferences and guidelines as described in Table 30 on page 116.
6. Click **Submit** to saves changes to the database.
7. Perform an IP Restart for changes to take effect.

Menu Options

The menu options available in the **IP Address Configuration** menu are described in Table 30.

Table 30. IP Address Configuration menu options

Name	Description	Default
Name	Specifies the interface to which the configuration applies. When configuring, valid choices are automatically populated based on available interfaces.	n/a
Mode	Specifies the method used to set the IP address. Choices are: • **static**—Recommended. Manually configures the external management IP address of the RM, and optionally sets the subnet mask and gateway address[a]. When this option is issued, the IP address change is stored and takes effect when the network service is restarted. You will need to reconnect to the GUI using the new IP address. • **default_gateway**—If the system has multiple interfaces, select default_gateway and choose a specific interface to be used for the default gateway from the **Interface** field. If multiple DHCP interfaces are configured, the subsystem will use the first interface to be configured for the default gateway. • **dhcp**—Configures the RM to use DHCP (Dynamic Host Configuration Protocol) to automatically obtain its IP address and network settings.	static
Address	Only displayed when **static** is chosen. Specifies the host name or IP address to be assigned to the RM.	*auto-populated*
Subnet Mask	Only displayed when **static** is chosen. Specifies the subnet mask address for subnetwork to which the RM is being added. For example, 255.255.255.0.	*auto-populated*
Gateway Address	Only displayed when **static** or **default_gateway** is chosen. Specifies the IP address for the network node through which this subnetwork is accessed. When **static** configuration is chosen, this field is used for configuring an iptable rule for the interface. When **default_gateway** is chosen, the value in this field specifies the default gateway route to the host.	*auto-populated*
DHCP Hostname	Only displayed when **dhcp** is chosen. For DHCP assignment of IP address, specifies a name to use for uniquely identifying this RM to the DHCP server.	*Empty*
Pending Restart	Only displayed in the Network IP status window. Indicates whether an IP configuration change has been made without having restarted IP services; the change will take effect once the IP restart has been executed.	False

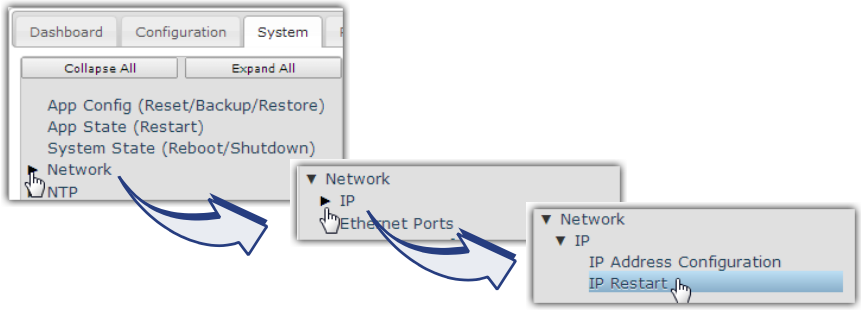
a. When configured in **static** mode, the **Gateway Address** field is used for the Linux OS' iptable rule and not for the RM's default gateway.

IP Restart — Menu Access and Usage

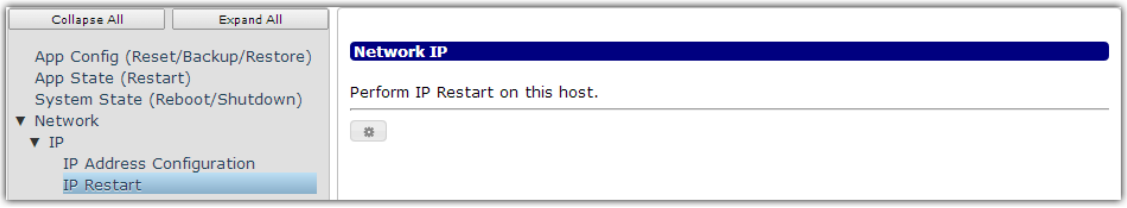
To access and use the **IP Restart** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.

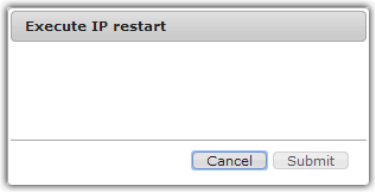
2. Click on the triangle next to the **IP** branch to expand out one level.



3. Click the **IP Restart** entry to open the *Network IP* configuration window:



4. Click the execute ( ) icon to open the *Execute IP restart* window.



5. Click **Submit** to perform an immediate restart.

Ethernet Ports Branch

The **Ethernet Ports** branch displays key information about the physical state of the Ethernet ports on the physical device running RM. No configuration is performed in this menu; it is for informational purposes only.

To access the **Ethernet Ports** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.
2. Click the **Ethernet Ports** entry to open the *Ethernet Ports* display window:

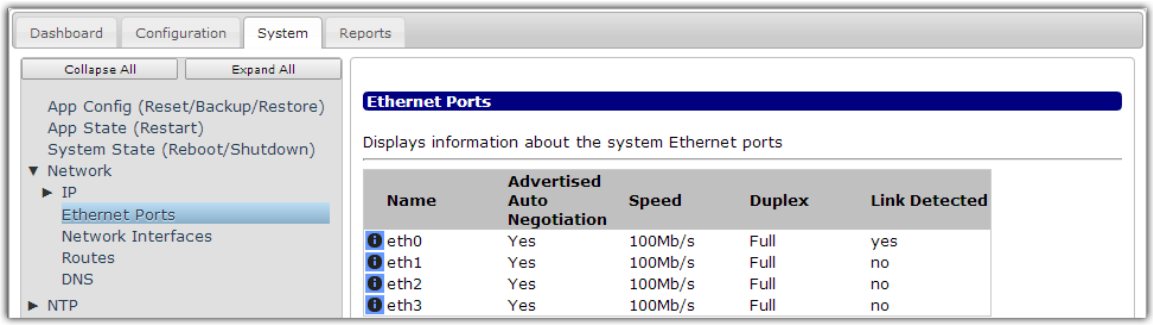


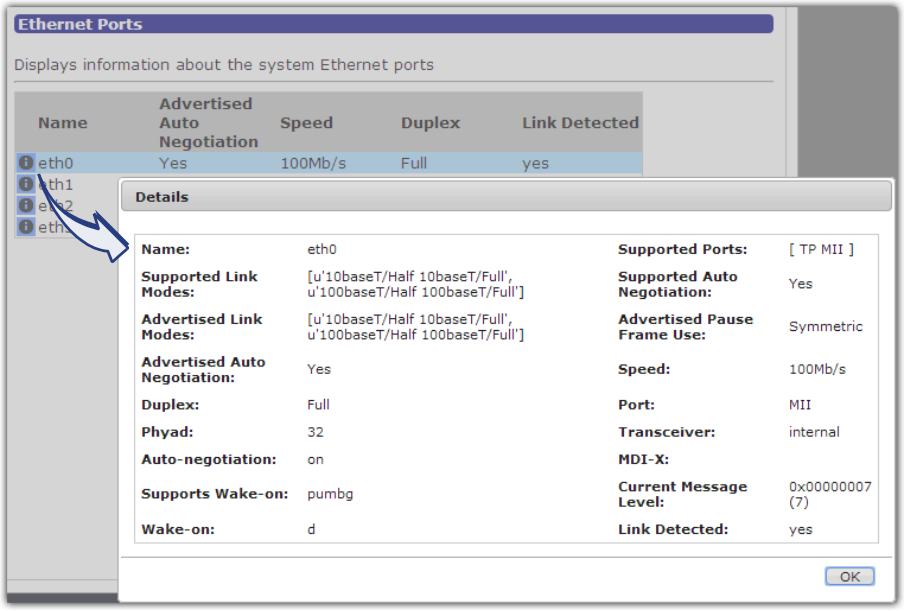
Table 31 describes the fields in the Ethernet Ports menu.

Table 31. Ethernet Ports menu descriptions

Name	Description
Name	Displays the Ethernet interface port.
Advertised Auto Negotiation	Displays whether the Ethernet port is enabled for auto negotiating transfer rates of connected devices.
Speed	Displays the transfer speed that has either been auto negotiated or manually set.
Duplex	Displays whether the port is full or half-duplex
Link Detected	Displays whether the port has detected a connection to another device.

More Information

To obtain additional information about a specific Ethernet port, click the info ( ) icon next to the port's row entry. A detailed information window will open as shown below.



Network Interfaces Branch

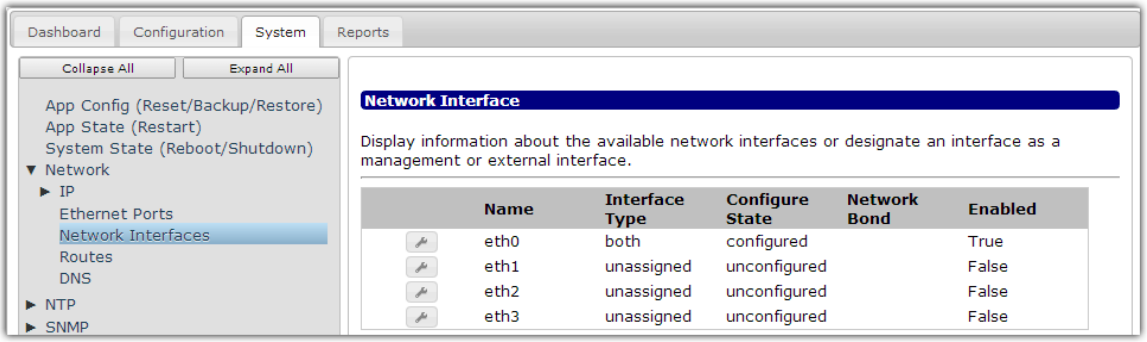
The **Network Interfaces** branch provides the ability to designate an Ethernet port as a management or externally facing port, or both.

Menu Access and Usage

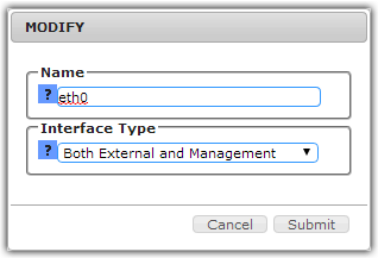
To access and use the **Network Interfaces** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.

2. Click the **Network Interfaces** branch to open the window of the same name.



3. For configuration, click the wrench ( ) icon next to the desired Ethernet port entry to open the *MODIFY* window.



4. Choose values according to your preferences and guidelines as described in Table 32 on page 120.
5. Click **Submit** to saves changes to the database.
6. Perform an Application Restart for changes to take effect.

Menu Options

The menu options available in the **Network Interface** menu are described in Table 32.

Table 32. Network Interfaces menu options

Name	Description	Default
Name	Specifies the interface to which the configuration applies. When configuring, valid choices are automatically populated based on available interfaces.	n/a
Interface Type	Specifies what type of communication the Ethernet interface can accept. When configuring the interface from the *Modify* window, choices are: **External (public facing)** — The interface will be used for generating URLs, links, etc, and external traffic to and from other non-management devices (such as Recorder or JITP traffic) **Management (internal)** — The interface will be used for management traffic, such as webGUI or API management of RM. Additionally, the interface is used for all multicast traffic, and is the designated interface for communication between the RM and Recorder/JITP. **Both External and Management** — The interface will be used for both External and Internal (management) communication. Note: by default, RM always configures the eth0 (or equivalent) port as both management and external. **Not explicitly assigned** — The interface is not manually set for either management or external traffic. This setting appears when an Ethernet port has not yet been configured / enabled from the *System > Network > IP > IP Address Configuration* menu.	eth0 (or equivalent) defaults to *External and Management*
Configure State	Only displayed as a read-only option in the status window. Indicates whether the Ethernet interface has been configured with IP information via the *System > Network > IP > IP Address Configuration* menu.	*Read-only*
Network Bond	Only displayed as a read-only option in the status window. Indicates whether the interface has been configured as part of a network bond. *This release does not support data population in this field.*	*Read-only*
Enabled	Only displayed as a read-only option in the status window. Indicates whether the Ethernet interface is enabled for communication (i.e., cable connected, disabled by external tools, etc.).	*Read-only*

Routes Branch

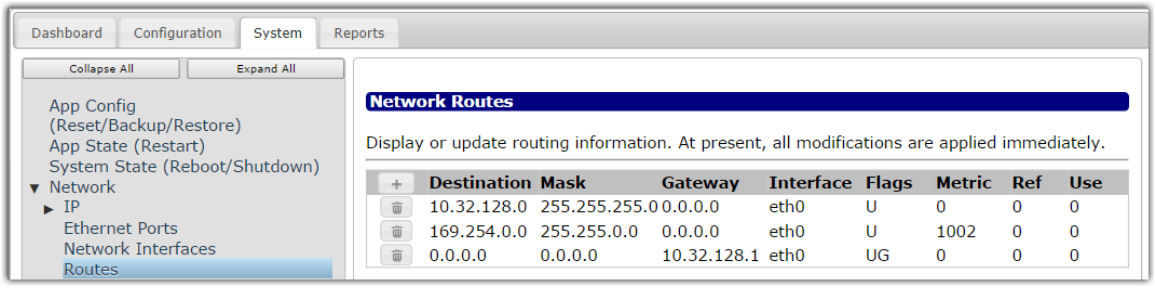
The **Routes** branch allows you to manage network routing by adding and removing entries in the network routing table of the RM.

Note: *Adding a network route via the RM GUI only adds a route for the RM, not the JITP or Recorder. To add network routes in order for all devices to communicate with each other, a network route must also be set from the JITP/Recorder GUI (i.e,. The Packager GUI).*

Menu Access

To access and use the **Routes** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.
2. Click the **Routes** branch to open the window of the same name.



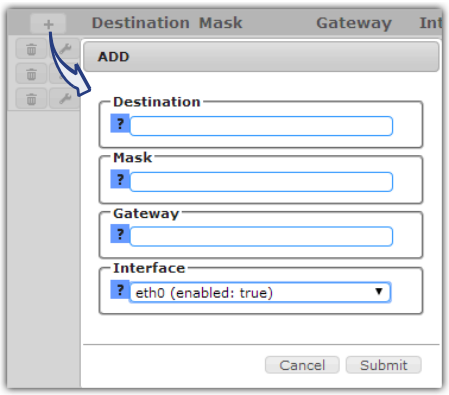
Menu Usage

Two types of actions are available from the *Network Routes* menu:

- Add a route
- Delete a route

To **Add** a route, proceed as follows:

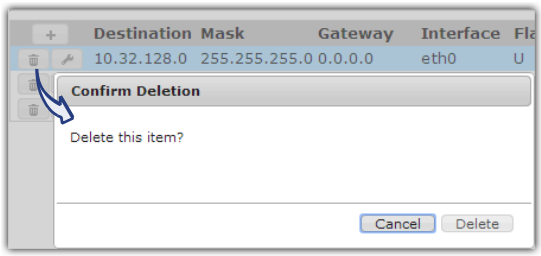
1. Click the add (+) icon at the top of the status table to open the *ADD* window.



2. Choose values according to your preferences and guidelines as described in Table 33 on page 122.
3. Click **Submit** to saves changes to the database. The change takes effect immediately.

To **Delete** a route, proceed as follows:

1. Click the trash ( ) icon at the top of the status table to open the *DELETE* window.



2. Choose values according to your preferences and guidelines as described in Table 33 on page 122.
3. Click **Delete** to delete the entry from the database.

Menu Options

The menu options available in the **Routes** menu are described in Table 33.

Table 33. Routes menu options

Name	Description	Default
Destination	Specifies the network address of the destination sub-network for the route. Valid entry is a 32-bit network IP address only.	*Empty*
Mask	Specifies the subnet mask of the destination network for the route. Valid entry is a 32-bit subnet mask address.	*Empty*
Gateway	Specifies the gateway address to use for the network route. When configuring, if this entry is left blank, the default gateway specified in *System* > *Network* > *IP Address Configuration* > *default_gateway* will be used.	*Empty*
Interface	Specifies the network interface to which the route will be applied. Choices from the drop-down menu are automatically populated based on valid and available interfaces.	*n/a*
Flags	Information here is an “as-is” display of the Linux `route` command. Please refer to the route manpage for further details.	*Read-only*
Metric	Information here is an “as-is” display of the Linux `route` command. Please refer to the route manpage for further details.	*Read-only*
Ref	Information here is an “as-is” display of the Linux `route` command. Please refer to the route manpage for further details.	*Read-only*
Use	Information here is an “as-is” display of the Linux `route` command. Please refer to the route manpage for further details.	*Read-only*

DNS Branch

The **DNS** branch allows you to view and configure the RM with Domain Name System (DNS) server addresses and domain entries. From the **DNS** menu, you can:

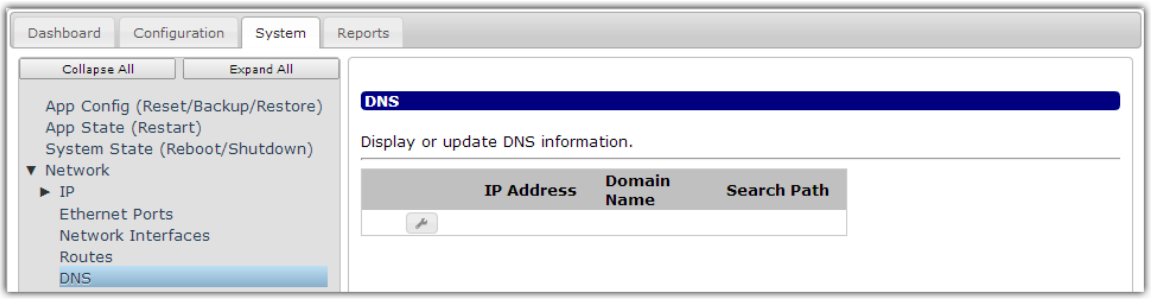
- Configure / reorder DNS server
- Configure Domain Name
- Configure / reorder Search Path

This section describes menu access and usage; for a description of the fields available in the **DNS** menu, refer to Table 34 on page 127.

Menu Access

To access and use the **DNS** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Network** branch to expand out one level.
2. Click the **DNS** branch to open the window of the same name.

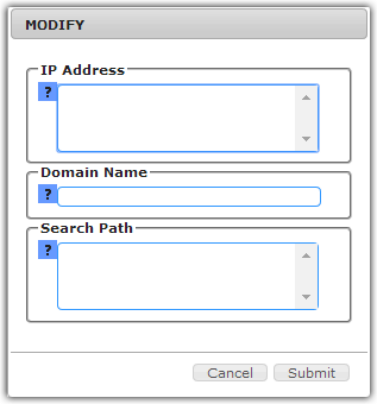


Menu Usage

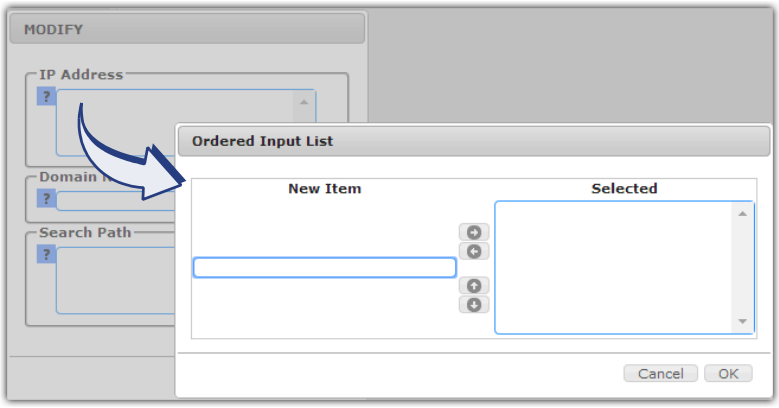
This section provides instructions for all available settings in the *System* > *Network* > *DNS* menu.

To **Configure a DNS server,** proceed as follows:

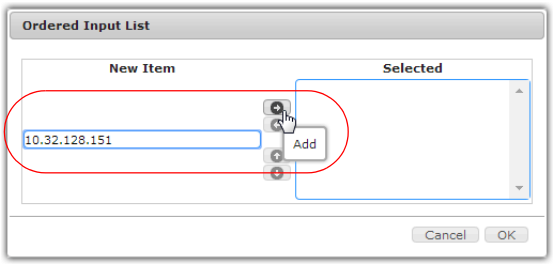
1. Click the wrench ( ) icon at the top of the status table to open the *MODIFY* window.

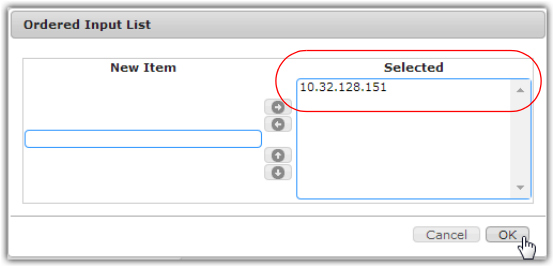


2. Click in the **IP Address** field to open the *Ordered Input List* window.

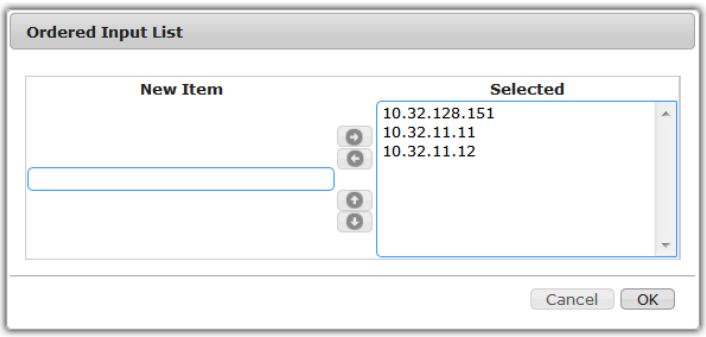


3. In the **New Item** field, enter the desired DNS server IP address and click the right arrow button to place the entry in the **Selected** field.



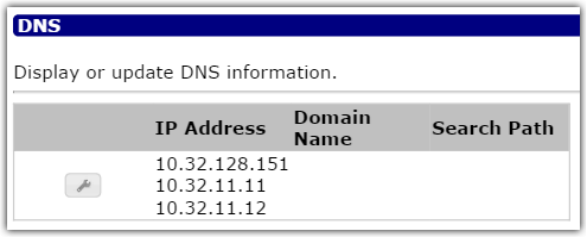


4. Repeat Step 3 for each additional DNS server you wish to add.



5. If you wish to change the order in which the servers are prioritized, select the server IP you wish to move and use the up/down arrow buttons to place as desired.
6. Click **OK** to save the DNS server to the list.
7. Click **Submit** to save and add the DNS server to the RM.

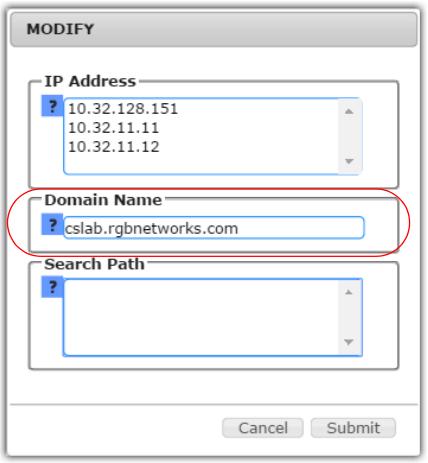
   The new DNS entries or orders will be displayed in the *System* > *Network* > *DNS* status menu.



Note: *To modify an existing DNS entry, simply click the wrench icon in the status window and follow these steps above.*

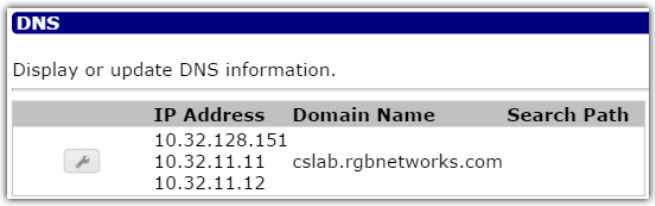
To **Configure a Domain Name,** proceed as follows:

1. Click the wrench ( ) icon at the top of the status table to open the *MODIFY* window.
2. Type the name of the domain in the **Domain Name** field



3. Click **Submit** to save and add the domain to the RM.

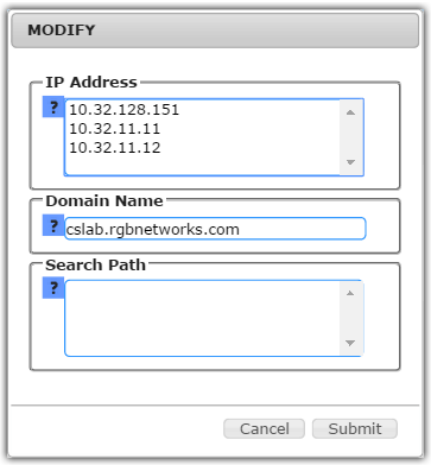
   The new domain name will be displayed in the *System* > *Network* > *DNS* status menu.



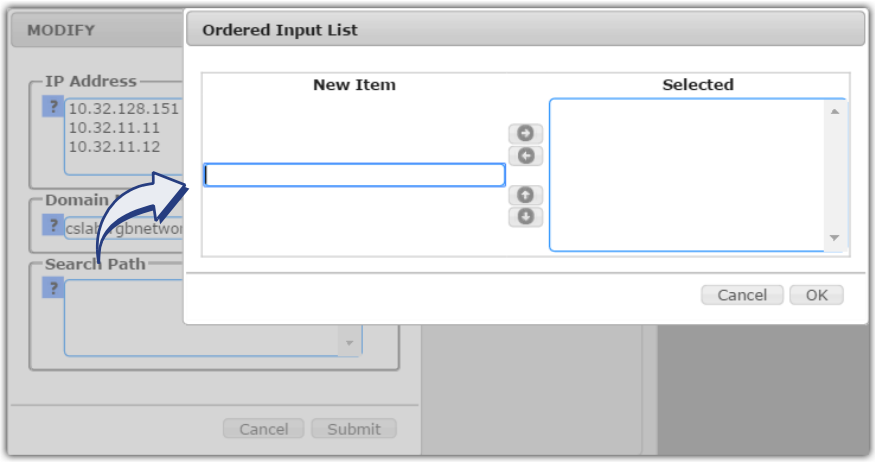
Note: *To modify an existing domain name, simply click the wrench icon in the status window and follow these steps above.*

To **Configure a Search Path** proceed as follows:

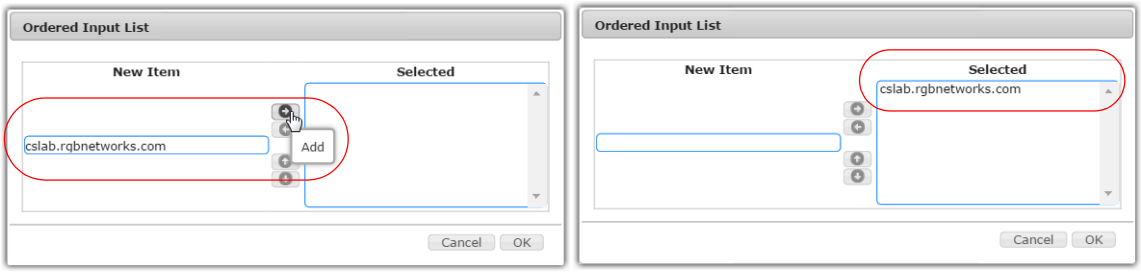
1. Click the wrench ( ) icon at the top of the status table to open the *MODIFY* window.



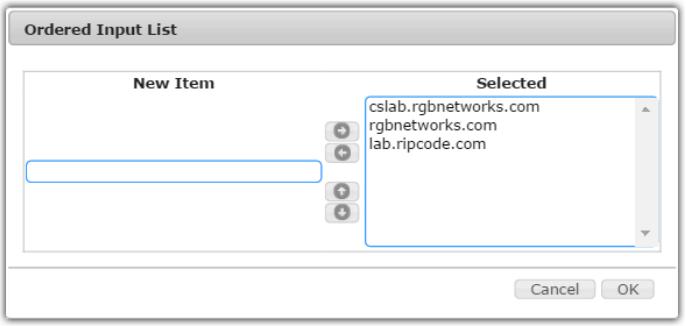
2. Click in the **Search Path** field to open the *Ordered Input List* window.



3. In the **New Item** field, enter the desired domain address and click the right arrow button to place the entry in the **Selected** field.

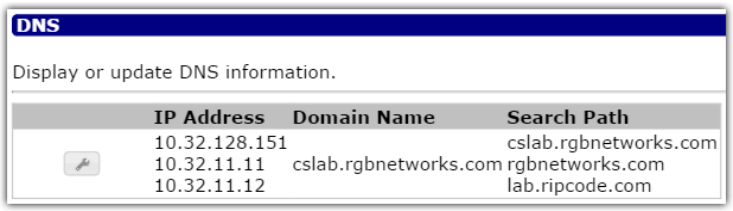


4. Repeat Step 3 for each additional domain you wish to add.



5. If you wish to change the order in which the search paths are prioritized, select the domain you wish to move and use the up/down arrow buttons to place as desired.
6. Click **OK** to save the search path to the list.
7. Click **Submit** to save and add the search path to the RM.

   The new search paths or order will be displayed in the *System* > *Network* > *DNS* status menu.



Note: *To modify an existing search path entry, simply click the wrench icon in the status window and follow these steps above.*

Menu Options

The menu options available in the **DNS** menu are described in Table 34.

Table 34. DNS menu options

Name	Description	Default
IP Address	Specifies the IP address(es) that the RM will use for its DNS	*Empty*
Domain Name	Specifies the domain in which RM resides. This entry must include the Fully Qualified Domain Name (FQDN). For example, if the domain in which RM resides is named, “fargo.mylab.com” you may not enter “fargo” or “mylab.com.” You must enter the FQDN of `fargo.mylab.com`	*Empty*
Search Path	Specifies additional domain search paths to use for resolving DNS as well as the priority to use for searching.	*Empty*

NTP Tree

The **NTP** tree contains branch menus for viewing, configuring, and restarting NTP server information for system timing.

- Server Config Branch
- Server State Branch
- Server Restart Branch

Server Config Branch

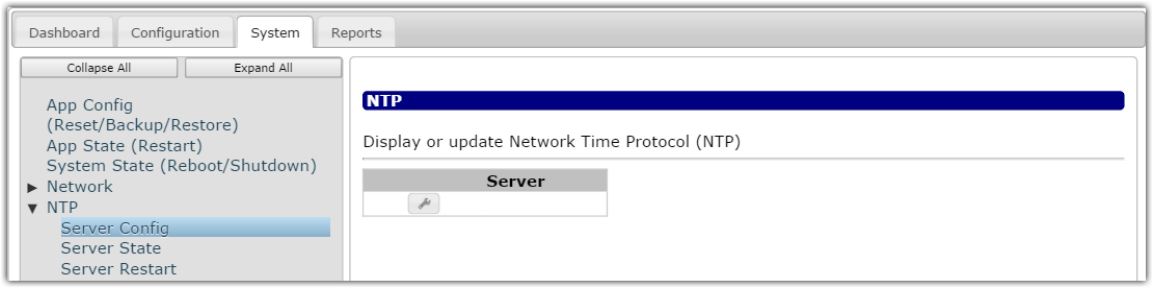
The **Server Config** branch allows you to view and specify which NTP server(s) the RM will use for its system timing reference.

Menu Access and Usage

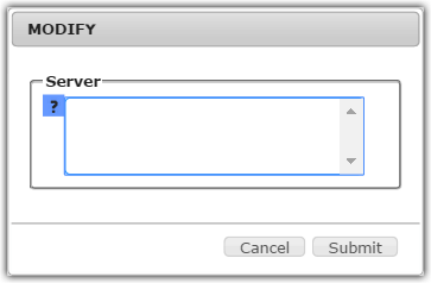
To access and use the **Server Config** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **NTP** tree to expand out one level.

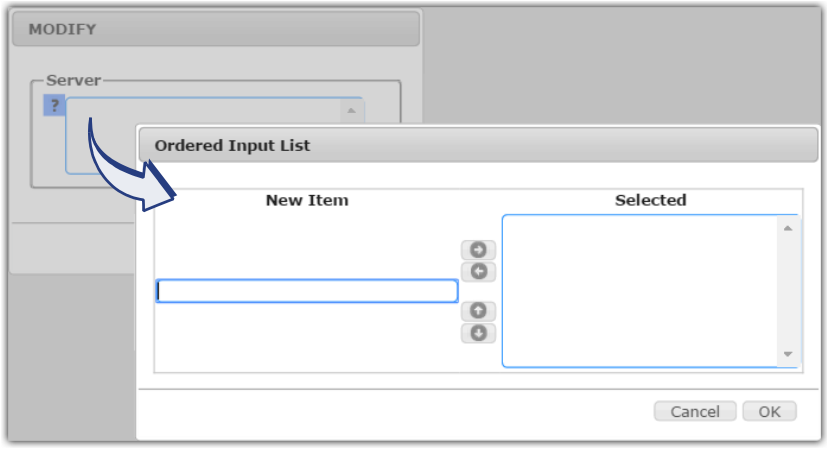
2. Click the **Server Config** branch to open the **NTP** window.



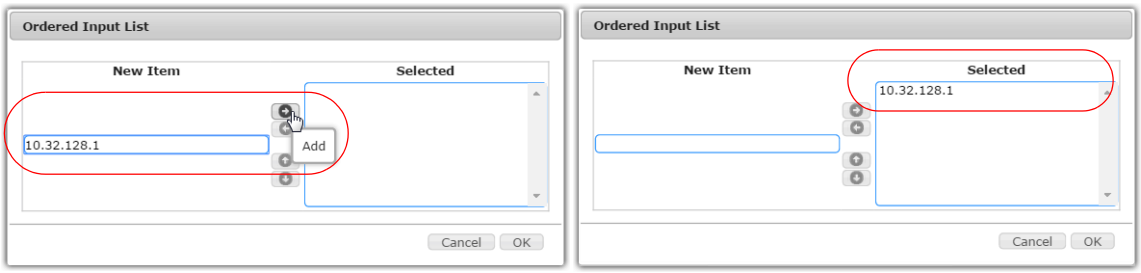
3. Click the wrench ( ) icon at the top of the status table to open the *MODIFY* window.



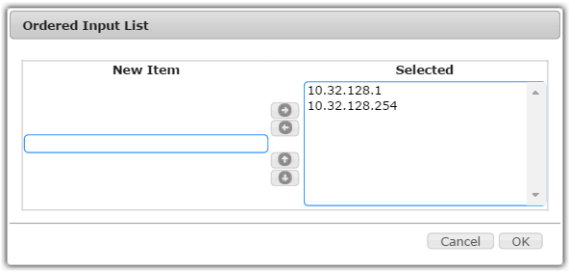
4. Click in the **Server** field to open the *Ordered Input List* window.



5. In the **New Item** field, enter the desired NTP server IP address and click the right arrow button to place the entry in the **Selected** field.

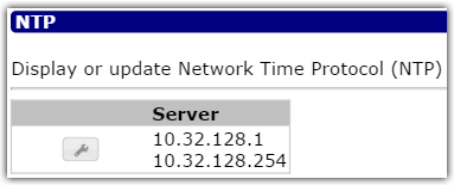


6. Repeat Step 5 for each additional DNS server you wish to add.



7. If you wish to change the order in which the servers are prioritized, select the server IP you wish to move and use the up/down arrow buttons to place as desired.
8. Click **OK** to save the NTP server to the list.
9. Click **Submit** to save and add the NTP server to the RM.

   The new NTP entries or orders will be displayed in the *System* > *NTP* > *Server Config* status menu.



Note: *To modify an existing NTP entry, simply click the wrench icon in the status window and follow these steps above.*

Server State Branch

The **Server State** branch displays key statistical information about the NTP server(s) that the RM is using. No configuration is performed in this menu; it is for informational purposes only.

To access the **Server State** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **NTP** tree to expand out one level.
2. Click the **Server State** entry to open the *NTP State* status window:

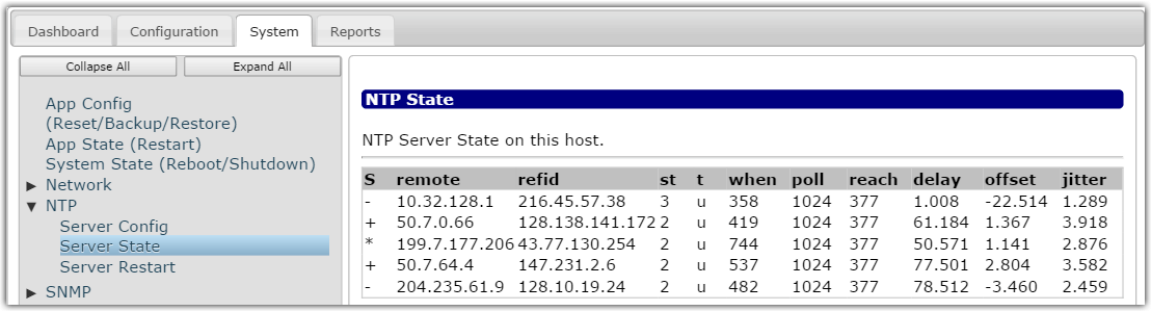


Table 35. Server State menu descriptions

Name	Description
S	Indicates the status of the NTP's remote peers. Options are: [*blank*] — Reject. Peer is unreachable **x** — Falsetick. Peer has been discarded due to intersection algorithm **.** — Excess. Peer has been discarded due to synchronization distance **-** — Outlyer. Peer has been discarded due to clustering algorithm **+** — Candidate. Peer is a survivor and candidate for the combining algorithm **#** — Selected. Peer is a survivor, but not among first 6 peers for synchronization distance ***** — Peer. Peer has been declared a winner. **o** — pps.peer. Peer is a winner, but its timing is derived from pulse-per-second signal.
remote	Displays the NTPs' IP addresses or first 15 characters of its hostname.
refid	Displays the IP address or host that the NTP server is using as the source for its timing.
st	Displays the accuracy of time sync to the reference clock, or stratum. The lower the score, the better. The RM should register at most at 2 or 3 in order to function effectively. If this number is 16, the RM is not getting timing service from the server.
t	Shows the type of peer for the entry. One of the following letters will be displayed: l = local peer u = unicast peer m = multicast peer b = broadcast peer
when	Reports when the last time service packet was received (in seconds).
poll	Shows the polling interval (in seconds)
reach	Displays the octal bitmap of results from the last eight polls from the NTP server. A value of 377 means the last 8 attempts were successful. A value of 0 means the last 8 attempts failed (i.e., timing is unavailable for this server).
delay	Displays the number of milliseconds it is taking for NTP packets to make a round-trip from the RM to the NTP server and back to the RM. It is advisable to pick NTP servers that are physically close to the RM.
offset	Display the number of milliseconds difference between the NTP server clock and the RM's clock
jitter	Also known as dispersion. Displays the dispersion in milliseconds of successive time values from the NTP server. Jitter is a measure of the network's stability (in terms of time) from the RM to the NTP server. It is an important factor used by NTP to determine the "best" server.

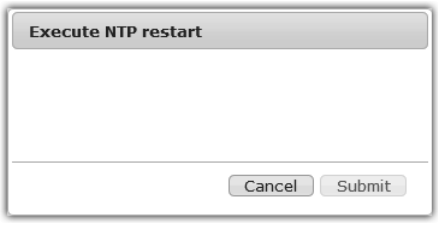
Server Restart Branch

The **Server Restart** branch allows you to restart the NTP service on the RM.

To access and use the **Server Restart** menu, proceed as follows:

1. From the **System** tab, click on the triangle next to the **NTP** branch to expand out one level.
2. Click the **Server Restart** entry to open the *NTP* restart window.

3. Click the execute ( ) icon to open the **Execute NTP restart** window:



4. Click **Submit** to execute the restart immediately.

SNMP Tree

The SNMP tree allows you to configure settings for the RM's Simple Network Management Protocol (SNMP) service. When SNMP is enabled, all events that are shown in the GUI's **Dashboard > Events** container are also forwarded to the SNMP trap server. Up to 16 trap servers may be configured per RM system.

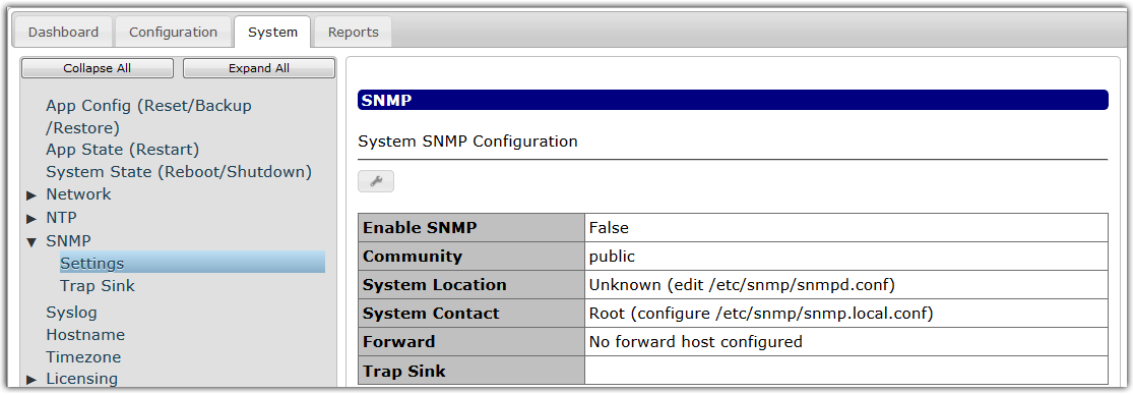
Note: *Only SNMP trap forwarding is supported; management of the RM can not be done via SNMP.*

Settings Branch

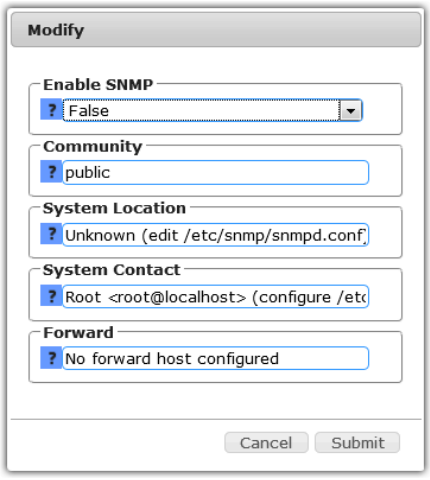
The **Settings** branch configures system-wide parameters for the RM's SNMP service.

To access and use the **Settings** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **SNMP** tree to expand out one level.
2. Click the **Settings** branch to open the *SNMP* settings window.



3. For configuration, click the wrench ( ) icon in the SNMP status window open the *Modify* window.



4. Choose values according to your preferences and guidelines as described in Table 30 on page 116.
5. Click **Submit** to saves changes to the database.

Menu Options

The menu options available in the SNMP **Settings** menu are described in Table 36.

Table 36. SNMP Settings menu options

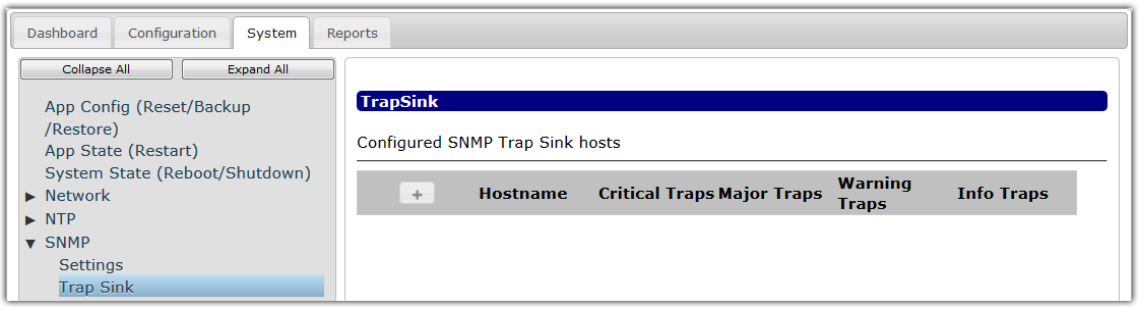
Name	Description	Default
Enable SNMP	Specifies whether to enable or disable RM's SNMP service.	False
Community	Specifies the SNMP community string to use. This field defaults to public (read-only), but can be changed to a secure alphanumeric string that the SNMP servers will use for communication.	public
System Location	Specifies an alphanumeric string that identifies the location (or name) of the RM system that will be sending traps. This string is then sent as part of the response to an SNMP get request from a trap server.	Unknown (edit /etc/snmp/snmpd.conf)
System Contact	Specifies an alphanumeric string that identifies the contact (person or group) for the RM system that will be sending traps. This string is then sent as part of the response to an SNMP get request from a trap server.	Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
Forward	Specifies the hostname or IP address of a device if you wish to use it as a proxy trap server for forwarding traps from this system. To disable trap forwarding, select None.	No forward host configured
Trap Sink	Available only in the Settings status window. Specifies the IP address of a trap server to which traps will be sent.	*read-only*

Trap Sink Branch

The **Trap Sink** branch allows you to add, remove, and configure parameters for individual trap server.

To access the **Trap Sink** branch, proceed as follows:

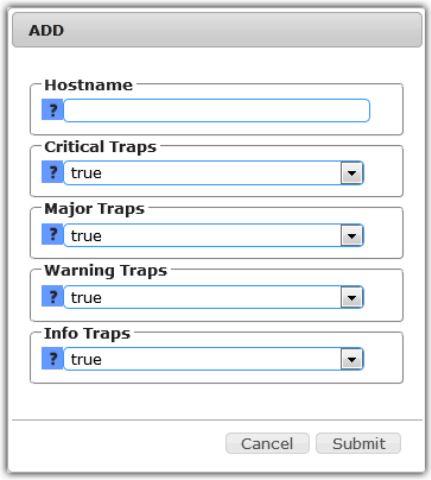
1. From the **Trap Sink** tab, click on the triangle next to the **SNMP** tree to expand out one level.
2. Click the **Trap Sink** branch to open the *TrapSink* settings window.



Add a Trap Server

To add a trap server:

1. Click the add (+) icon in the *TrapSink* status window to open the *ADD* window.

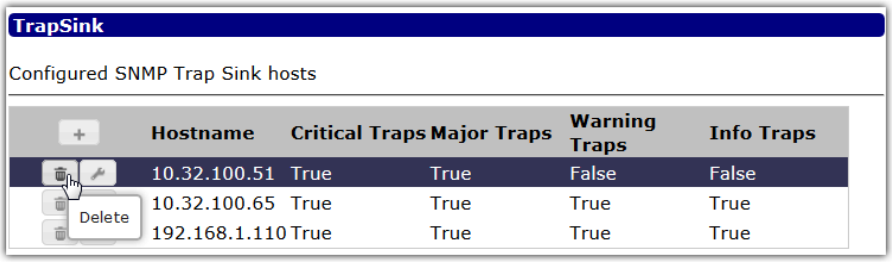


2. Choose values according to your preferences and guidelines as described in Table 37 on page 134.
3. Click **Submit** to saves changes to the database.

Delete a Trap Server

To delete a trap server:

1. Click the trash (🗑) icon in the *TrapSink* status window in the row entry of the trap server you wish to delete.

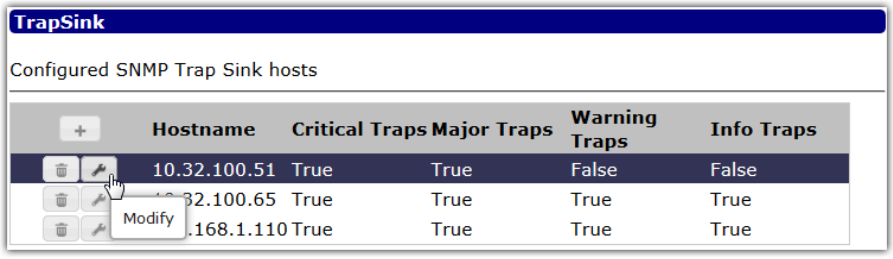


2. From the *Confirm Deletion* pop-up, click **Delete**.

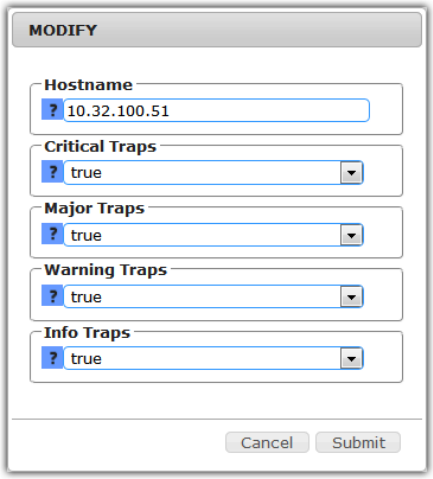
Modify a Trap Server

To modify a trap server:

1. Click the wrench ( ) icon in the *TrapSink* status window in the row entry of the trap server you wish to modify.



The trap server's *Modify* window will open..



2. Choose values according to your preferences and guidelines as described in Table 37 on page 134.

Note: *When modifying a trap server, the hostname (either IP address or name) cannot be modified.*

3. Click **Submit** to saves changes to the database.

Menu Options

The menu options available in the SNMP **Trap Sink** menu are described in Table 37.

Table 37. SNMP Trap Sink menu options

Name	Description	Default
Hostname	Specifies the hostname or IP address of the trap server. Up to 16 trap servers may be configured for each RM system[a]. *Note: You may not change the hostname / IP address of an existing trap server. You must first delete the hostname / IP entry and then re-add it with the desired name or IP change.*	*Empty*
Critical Traps	Specifies whether to send critical-level traps to the server.	true

Table 37. SNMP Trap Sink menu options

Name	Description	Default
Major Traps	Specifies whether to send major-level traps to the server.	true
Warning Traps	Specifies whether to send warning-level traps to the server.	true
Info Traps	Specifies whether to send informational-level traps to the server.	true

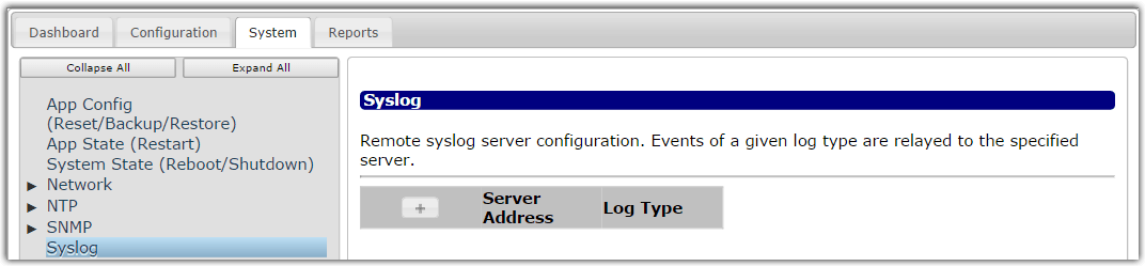
a. The only special character supported in the SNMP Trap Server Hostname / IP field is "." For example, a hostname of `host1.rgbnetworks.com` is accepted; a hostname of `host-1.rgbnetworks.com` is not accepted.

Syslog

Adding a Syslog server to the RM allows you to specify whether events and informational messages generated by RM will be sent to a remote server rather than stored locally. You can configure up to 16 separate Syslog servers.

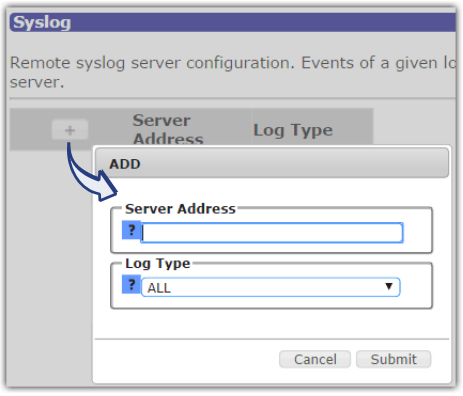
Menu Access

To access the **Syslog** menu, from the **System** tab, click on the **Syslog** entry.



Add a Syslog Server

1. From the **Syslog** menu, click the plus (+) icon to open the *ADD* window:



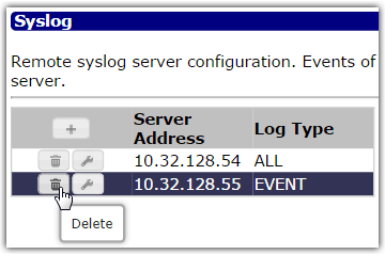
2. In the **Server Address** field, enter the hostname or IP address of the Syslog server to add.
3. In the **Log Type** field, select which messages to forward to the Syslog server.

4. Click **Submit** to save and add the Syslog server.
5. Repeat **steps 1-4** to add additional Syslog servers.

Note: *The Syslog server must be reachable by the RM in order to be added to its database.*

Delete a Syslog Server

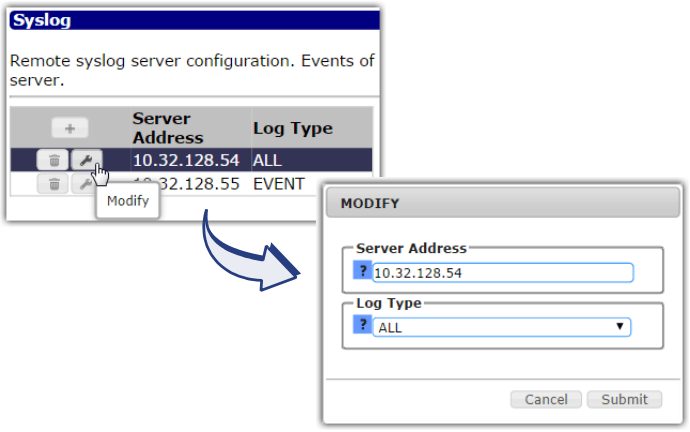
1. From the **Syslog** menu, click the trash ( ) icon.



2. Click **Delete** to confirm the deletion.

Modify a Syslog Server

1. From the **Syslog** menu, click the wrench ( ) icon to open the *ADD* window:



2. Change values according to your preferences and as defined in Table 38 on page 137.
3. Click **Submit** to save modifications to the Syslog server.

Menu Options

The menu options available in the **Syslog** menu are described in Table 38.

Table 38. Syslog menu options

Name	Description	Default
Server Address	Specifies the hostname or IP address of the Syslog server.	*Empty*
Log Type	From the drop-down menu, choose which types of messages should be forwarded to the Syslog server. Choices are: *ALL* — Forwards all messages (info & events) to the server. *INFO* — Forwards informational log entries only to the server; this includes internal RM related application trace, debug, and error messages. These events are sent to the Syslog server tagged as Error, Info, and Debug. *EVENT* — Forwards application log entries that are of only Critical, Major, or Warning severity level. Entries that are informational in severity will only be included if the entry was a clearing event from an earlier failure condition. These events are sent to the Syslog server tagged as Critical, Alert, Warning, and Info.	ALL

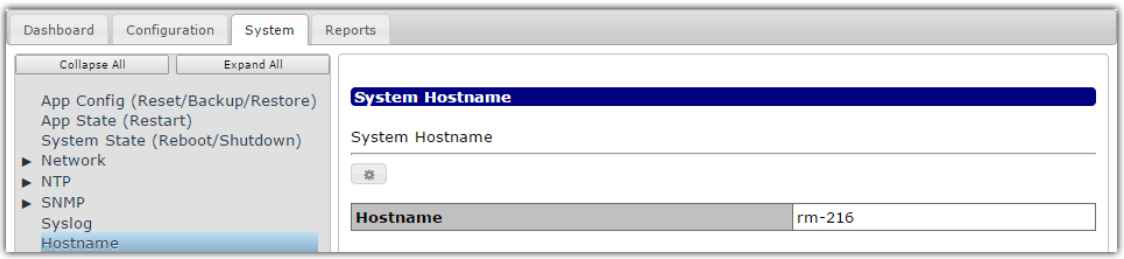
Hostname

Most likely, the hostname for the RM was already configured during operating system installation. However, you can set or change the hostname from the RM GUI as well.

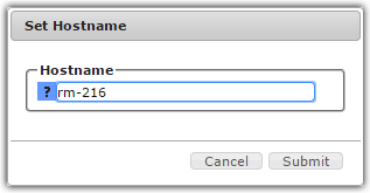
Menu Access and Usage

To access and use the **Hostname** menu, proceed as follows:

1. From the **System** tab, click on the **Hostname** entry.



2. Click the execute ( ) icon to open the **Set Hostname** window:



3. From the **Hostname** field, enter or change the hostname as desired (up to 255 characters).

Caution: *The Hostname must not contain any uppercase letters. You may only use lowercase letters for this entry.*

4. Click **Submit** to execute the change.
5. Perform an IP Restart for the changes to take effect.

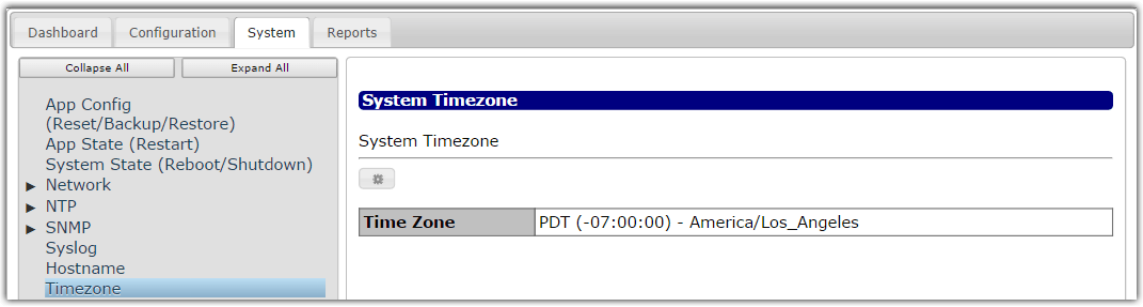
Timezone

If you are not using an NTP server for system timing reference, you can set the RM's time zone manually.

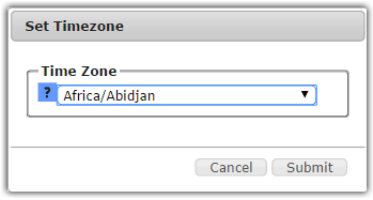
Menu Access and Usage

To access and use the **Timezone** menu, proceed as follows:

1. From the **System** tab, click on the **Timezone** branch.



2. Click the execute ( ) icon to open the **Set Timezone** window:



3. Click the **Time Zone** field and select the desired time zone from the drop-down list.
4. Click **Submit** to execute the change.

License Tree

The **License** tree contains branch menus for viewing, configuring, updating the RM license. This section describes usage and fields for each branch menu. For detailed instructions on how to install the RM license, please refer to "RM Licensing" on page 29.

The **License** tree contains the following branches:

- Server Config Branch
- Server State Branch
- Network Interfaces Branch

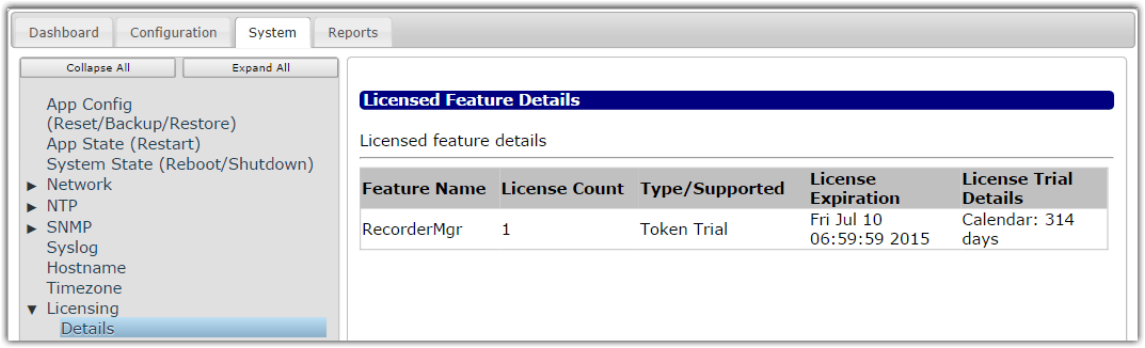
Details Branch

The license **Details** branch provides important information for the current RM license. No configuration is done in this menu; it is informational only.

Menu Access

To access the **Details** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Licensing** branch to expand out one level.
2. Click the **Details** branch to open the **License Feature Details** window.



Menu Options

Information available in the **Details** menu is described in Table 39.

Table 39. Details menu options

Name	Description
Feature Name	Displays the product name for which the license applies.
License Count	Displays the number of licenses available for this product. Note that for RM, this number will always be “1,” even when the RM is operating in redundancy mode as each RM must have its own license.
Type / Supported	Displays the type of license supported for the RM. Options are **Token** or **Token Trial**.
License Expiration	Displays the expiration date of the license.
License Trial Details	If the license is a trial license, this field will display the number of days for which the license is valid.

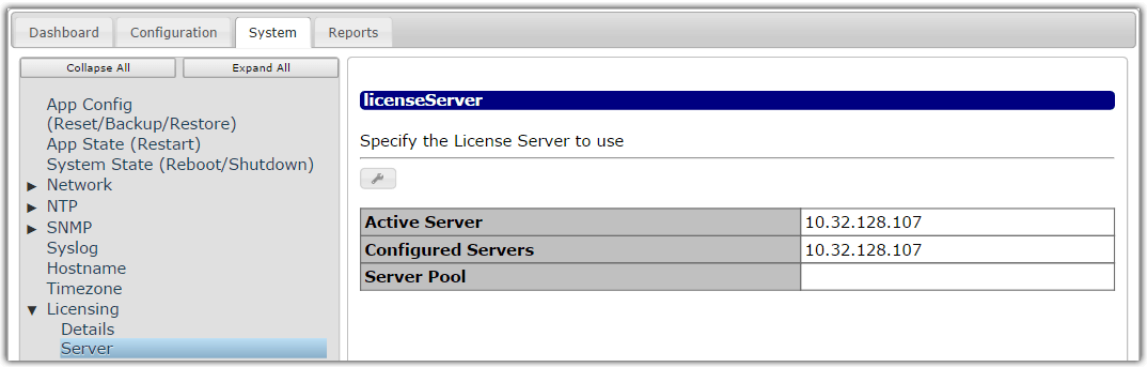
Server Branch

The license **Server** branch allows you to configure a license server to use for the RM.

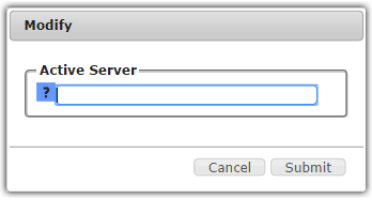
The RM has a built-in License Server that manages licenses for management. If desired, the RM can use an external License Server; in this case, you must configure the RM to point to the IP address or host name (DNS name) for the external server where the Licensing Application is installed.

To access and use the **Server** branch, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Licensing** tree to expand out one level.
2. Click the **Server** entry to open the *licenseServer* status window:



3. For configuration, click the wrench ( ) icon to open the *Modify* window.



4. Enter the IP address or hostname of the license server according to the guidelines described in Table 40 on page 140.
5. Click **Submit** to saves changes to the database.

Note: *The license server must be reachable by the RM in order to be added to its database.*

Menu Options

Table 40 describes the fields in the *licenseServer* / *Modify* windows.

Table 40. Server State menu descriptions

Name	Description
Active Server	Specifies the IP address or host name of the License Server that will manage licensing for the RM. When configuring this field, you can enter either the IP address of the license server, or the FQDN. You can also enter the word, “localhost” if you wish to use the RM’s as its own licensing server.

Table 40. Server State menu descriptions

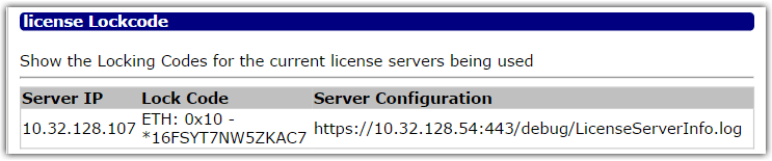
Name	Description
Configured Servers	For non-redundant license servers: this value should be the same as the *Active Server*. For redundant license servers, the *Active Server* will show the current member of the group in use and the *Configured Servers* field will show all of the servers. *Note:* If a different server has been configured, but the Safenet Client library is still trying to use the previous server, this value may be different.
Server Pool	For redundant license server pool: this field will show all of the of the servers in the pool.

Lockcode Branch

The licensing **Lockcode** branch displays the unique key that identifies your RM and its characteristics. If you want to change or add a license, you will need to contact the licensing administrator at Imagine Communications Customer Support and provide the lock code for the RM.

To access the **Lockcode** menu, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Licensing** tree to expand out one level.
2. Click the **Lockcode** entry to open the *license Lockcode* status window.:



3. If you are requesting a new license, copy the contents of the **Lock Code** field in order to send this data to the Imagine Communications Customer Support license administrator.

Menu Options

Information available in the **Lockcode** menu is described in Table 41.

Table 41. Lockcode menu options

Name	Description
Server IP	Displays the IP address of the RM's active license server.
Lock Code	Displays the RM's lockcode, unique to the device.
Server Configuration	Displays a link to a file containing details for the server. This file may then be used when contacting the Imagine Communications license administrator.

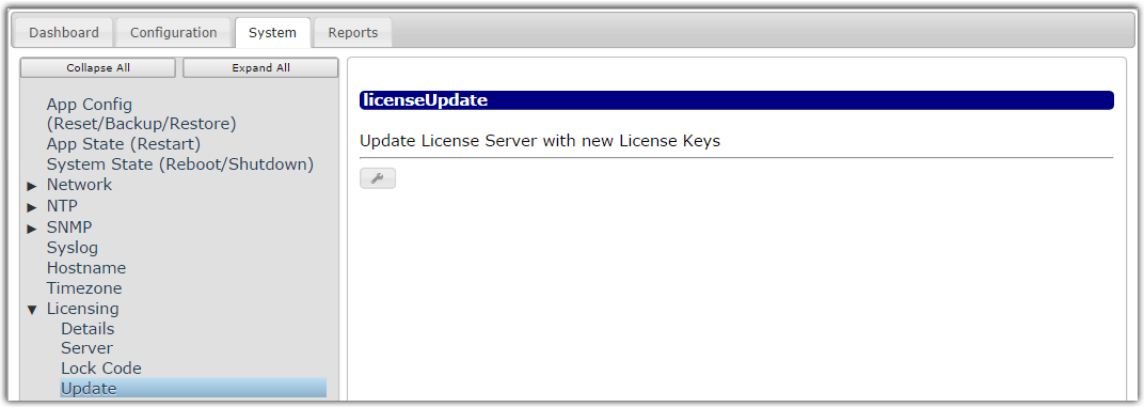
Update

The **Update** branch allows you to update or add a new license for the RM.

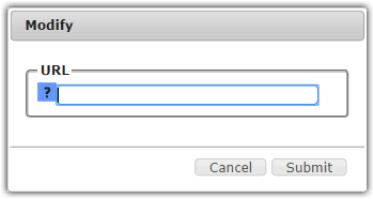
Menu Access and Usage

To access and use the **Update** menu, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Licensing** tree to expand out one level.
1. Click the **Update** entry to open the *license Update* status window.:.



2. Click the wrench ( ) icon to open the *Modify* window:



3. In the **URL** field, enter either the URL where the license can found or the license key itself (see Table 42 for details)
4. Click **Submit** to enter the new license, which will take effect immediately.

Menu Options

The menu options available in the **Update** menu are described in Table 42.

Table 42. License Update menu options

Name	Description	Default

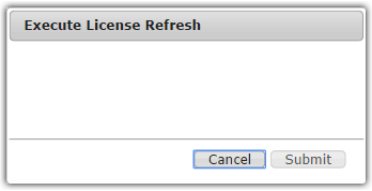
URL	Enter the full HTTP or TFTP URL to the remote license key file. For example:
	`http://remotehost/path/to/licenseFile.key`
	`tftp://remotehost/path/to/licenseFile.key`
	Notes:
	• This field can also accept a path to a file located on the local host. Format should be: `file://<full_path_to_file>` For example: `file:///tmp/file.key`
	• The easiest method of updating a license is to copy and paste the entire license key strings from the key file you received from Imagine Communications Customer Support
		Empty

Refresh Branch

The **Refresh** branch allows you to force the RM to update its license key from the device acting as its license server.

To access and use the license **Refresh** menu, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Licensing** branch to expand out one level.
2. Click the **Refresh** entry to open the *licensedFeatures* window.
3. Click the execute ( ) icon to open the **Execute License Refresh** window:



4. Click **Submit** to execute the license refresh immediately.

Redundancy Tree

To allow for the highest level of redundancy which minimizes downtime, Imagine Communications' cDVR solution provides node-level, 1+1 active/standby redundancy for the RM in which an RM redundancy group contains a Primary (or Active) RM and a Standby RM. The redundancy group provides a failover capability from the active RM to the standby RM. Each time the configuration database for the active RM is updated, the standby RM synchronizes its configuration database with the active RM's configuration database.

The **Redundancy** tree allows you to create a redundancy group with another RM. You can also execute manual failovers and recoveries form this menu.

Note: *This section describes menu access and usage for all branches in the **System > Redundancy** tree. This section does not provide detailed instructions on setting up or tearing down redundancy. Please refer to* Chapter 4, "RM Redundancy Setup" *detailed redundancy instructions.*

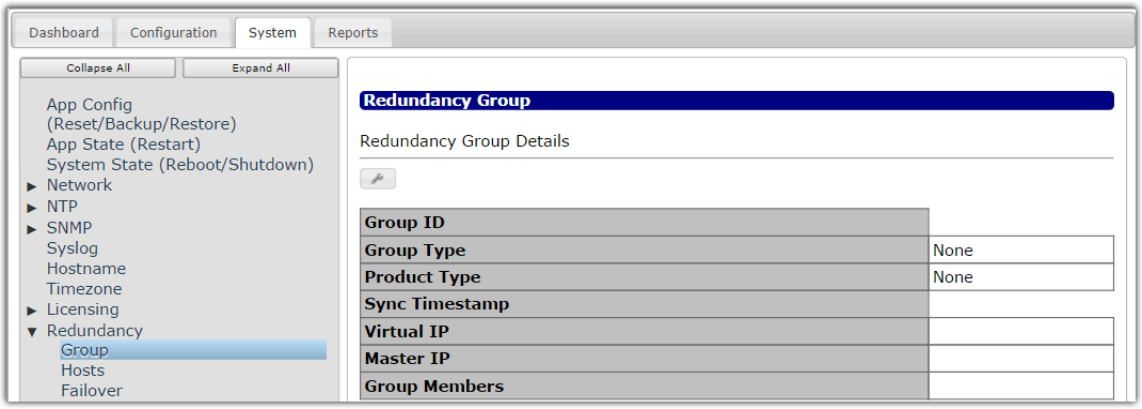
Group Branch

The **Group** branch configures an RM redundancy group so that a host can be added to it. Within this menu you can also find important status information for the RM's redundancy group.

To access and use the **Group** branch, proceed as follows:

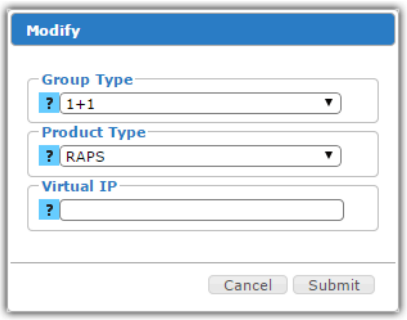
1. From the **System** tab, click on the triangle next to the **Redundancy** tree to expand out one level.

2. Click the **Group** branch to open the *Redundancy Group* window.



3. For configuration, click the wrench ( ) icon to bring up the *Modify* window.

   The **Group Type** and **Product Type** menus are preselected for *1+1* and *RAPS* respectively as shown below. :



4. In the **Virtual IP** field, enter the virtual IP address that will be assigned to both the Primary and Standby RMs.
5. Click **Submit** to save and add the redundancy group.

Menu Options

The menu options available in the Redundancy **Group** menu are described in Table 43.

Table 43. Redundancy Group menu options

Name	Description	Default
Group ID	Displays the system-assigned unique ID attributed to this redundancy group.	*Read-only*
Group Type	Specifies the type of redundancy for which the group is configured. This field is read-only, with *1+1* preselected.	1+1
Product Type	Specifies the type of product for which the group will apply. This field is read-only, with *RAPS* preselected.	RAPS
Sync Timestamp	Used internally for timestamping multicast messages.	*Read-only*
Virtual IP	Specifies the Virtual IP address that will be used for the redundancy group. Once configured, this IP address should be used for all subsequent access to the RM cluster. When configuring, enter a valid, unused IP address.	*Empty*

Table 43. Redundancy Group menu options

Name	Description	Default
Master IP	Indicates which physical IP address of the redundant RM pair is the master of the group (i.e., which RM is currently the active).	*Read-only*
Group Members	Indicates status information of all members of the redundancy group. Values returned are: *host_id* — the unique ID assigned to each host in the group. *host_ip* — IP address of the relative host *host_type* — Current redundancy type of the RM (Active or Standby) *host_state* — Current health state of the RM (Active, Failed, Degraded, Recovery, or Idle) *peer_id* — Not used for RM redundancy *host_version* — Software version running on the host **Host State Defnitions** **Active**: Host is running and is actively processing requests **Idle**: Host is running but not processing requests. It is ready to take over in the event of a failover. **Degraded**: Host is currently Active, but a failover has been requested and no standby is available to take over; this host will continue to run and process requests. When another host becomes available, this host will complete the failover operation. **Recovery**: This host is currently synchronizing with the Active host in the group. **Disabled**: Host is starting up, shutting down, or not running. Normal host state transitions: - Startup: Disabled-Recovery-Idle/Active - Shutdown: Idle/Active-Disabled - Failover: Active-Failed - Recovery: Failed-Recovery-Idle	*Read-only*

Caution: *Once you have successfully created a redundancy group, all further configuration should be performed by logging in to the Virtual IP address of the redundant pair to ensure proper configuration functionality..*

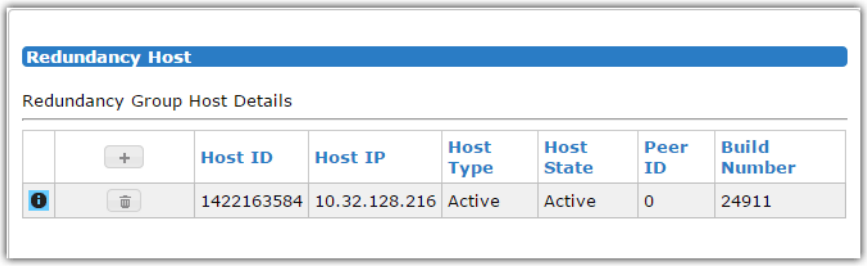
Hosts Branch

The **Hosts** branch allows you to add, remove, and configure parameters for a redundancy host.

To access the **Hosts** branch, proceed as follows:

1. Ensure you are logged into the VIP for the redundancy group.
2. From the **System** tab, click on the triangle next to the **Redundancy** tree to expand out one level.

3. Click the **Hosts** branch to open the *Redundancy Host* settings window.

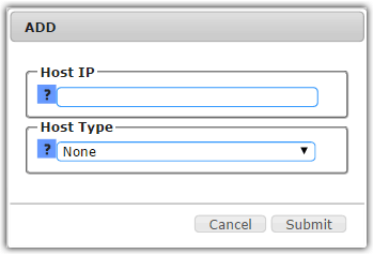


Note: *When you configure a group from the **System** > **Redundancy** > **Group** menu, a row entry for the active RM will automatically be added to the **System** > **Redundancy** > **Hosts** menu.*

Add a Redundancy Host

To add a redundancy host:

1. Click the add (+) icon in the *Redundancy Host* window to open the *ADD* window.



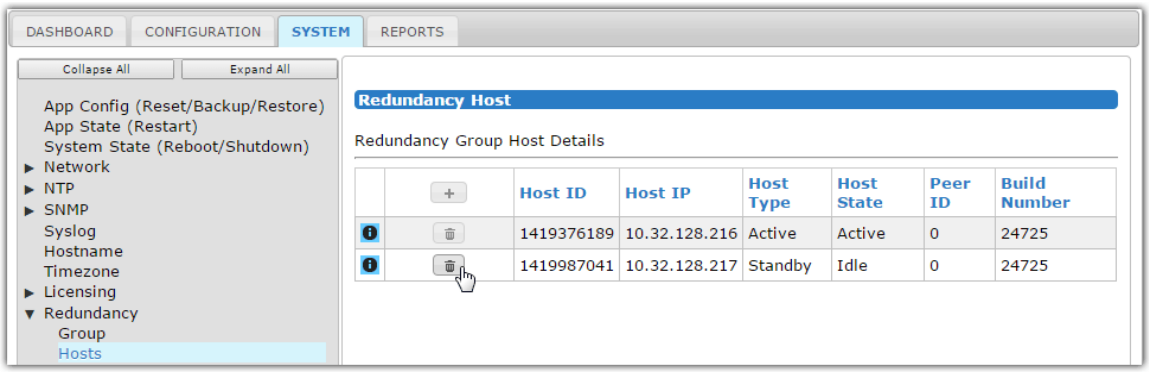
2. Choose values according to your preferences and guidelines as described in Table 44 on page 147.
3. Click **Submit** to saves changes to the database.

Caution: *You cannot add a host to a redundancy group unless the **System** > **Redundancy** > **Group** settings have been configured.*

Delete a Redundancy Host

To delete a redundancy host:

1. Click the trash (🗑) icon in the *Redundancy Host* status window in the row entry of the host you wish to delete.



2. From the *Confirm Deletion* pop-up, click **Delete**.

Caution: *You cannot delete an active host from a redundancy group unless the standby host has been deleted first.*

Menu Options

The menu options available in the **Hosts** menu are described in Table 44.

Table 44. Redundancy Hosts menu options

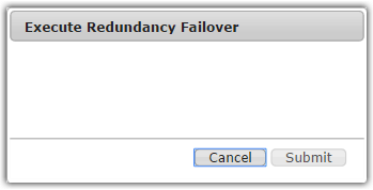
Name	Description	Default
Host ID	Displays the system-assigned unique ID attributed to the host.	*Read-only*
Host IP	Specifies the IP address of the redundant host. When configuring, enter a valid IP address that has a two-way communication path to the other RM host.	*Empty*
Host Type	Specifies the type of redundant host for which the RM is configured. When configuring, choose one of the following from the drop-down menu: None, Standby, or Active	None
Host State	Indicates the current redundancy status of the host. Options seen will be one of the following: Active, Idle, Failover, Recovery, Degraded ???	*Read-only*
Peer ID	Not used for RM redundancy.	*n/a*
Build Number	Indicates the software build number of the host. Note: Only the build number is displayed in this menu; the complete software version of the host is available in the *System* > *Redundancy* > *Group* menu.	*Read-only*

Failover Branch

The **Failover** branch allows you to force a manual failover from the currently active RM to the standby RM.

To access and use the redundancy **Failover** menu, proceed as follows:

1. Ensure you are logged into the VIP for the redundancy group.
2. From the **System** tab, click on the triangle next to the **Redundancy** branch to expand out one level.
3. Click the **Failover** entry to open the *Redundancy Host* window.
4. Click the execute ( ) icon to open the **Execute Redundancy Failover** window:



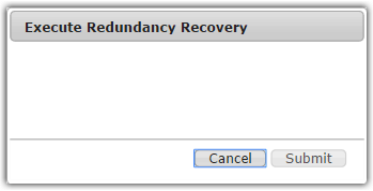
5. Click **Submit** to execute the failover immediately.

Recover Branch

The **Recover** branch allows you to force a manual recovery from the currently active RM to the standby RM.

To access and use the redundancy **Failover** menu, proceed as follows:

1. Ensure you are logged into the VIP for the redundancy group.
2. From the **System** tab, click on the triangle next to the **Redundancy** branch to expand out one level.
3. Click the **Recover** entry to open the *Redundancy Host* window.
4. Click the execute ( ) icon to open the **Execute Redundancy Recovery** window:



5. Click **Submit** to execute the recovery immediately.

Redundancy Switchover and Recovery Behavior.

Following are guidelines to how redundancy switchover and recovery behaves.

- Recovery is always manual, either from a application restart or using recovery command in the GUI.
- Recovery must always be done on the host your are attempting to recover (e.g. the failed RM). It cannot be done from the active RM.
- If a failover is attempted but the standby unit is also failed, then the failing unit will go from active to degraded. A switchover will *not* happen. When another RM becomes available, the failover will complete, the degraded host will enter a 'failed' state, and the standby RM enters the 'active' state.
- The *Degraded* state means that the host wants to fail, but cannot because the standby unit is not available. (additional note: a 'degraded' host can be manually recovered back to the active state).
- Once the standby unit becomes available, the failover operation will complete; thus the failing unit's 'degraded' state will move to a 'failed' state. The standby unit will now be the active unit.

Registered Apps Branch

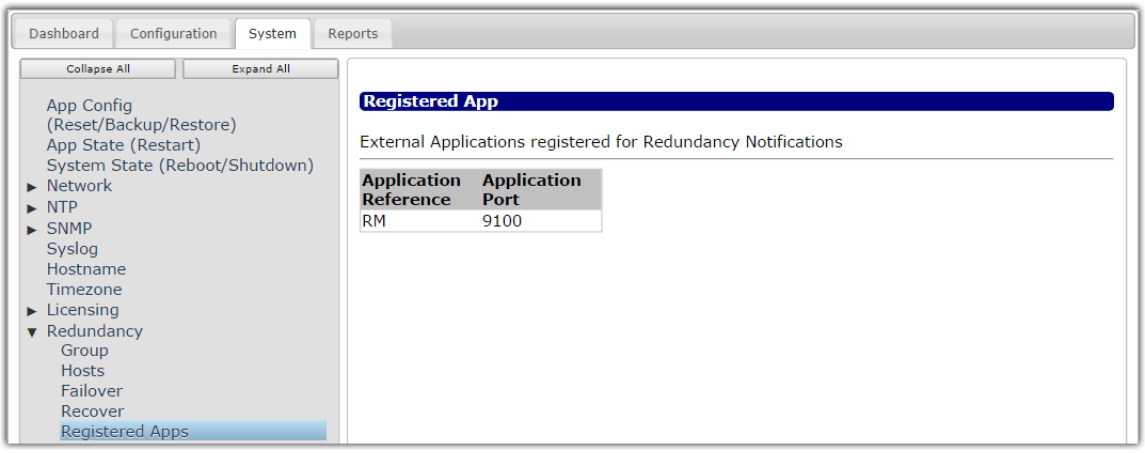
The **Registered Apps** branch provides information about external applications that are registered for Redundancy Notifications.

Note: *This menu is primarily for debugging when working with Imagine Communications Customer Support.*

To access the redundancy **Registered Apps** menu, proceed as follows:

1. Ensure you are logged into the VIP for the redundancy group.
2. From the **System** tab, click on the triangle next to the **Redundancy** branch to expand out one level.

3. Click the **Registered Apps** entry to open the *Registered App* window.



Menu Options

The read-only menu options available in the **Registered Apps** menu are described in Table 45.

Table 45. Redundancy Registered Apps menu options

Name	Description
Application Reference	Indicates which type of Telurio application is registered for redundancy in the redundancy group.
Application Port	Indicates the port number that is being used for redundancy communication.

Debug Tree

The **Debug** tree is a troubleshooting tool that you can use to collect important system diagnostics that you can provide to Imagine Communications Customer Support in the event your system malfunctions. There are two branches available from the Debug tree:

- **Info** — collects diagnostic information from multiple file locations for analysis and presents the results as a collection of files archived on the RM;
- **Trace** — sets debug trace levels for various applications.

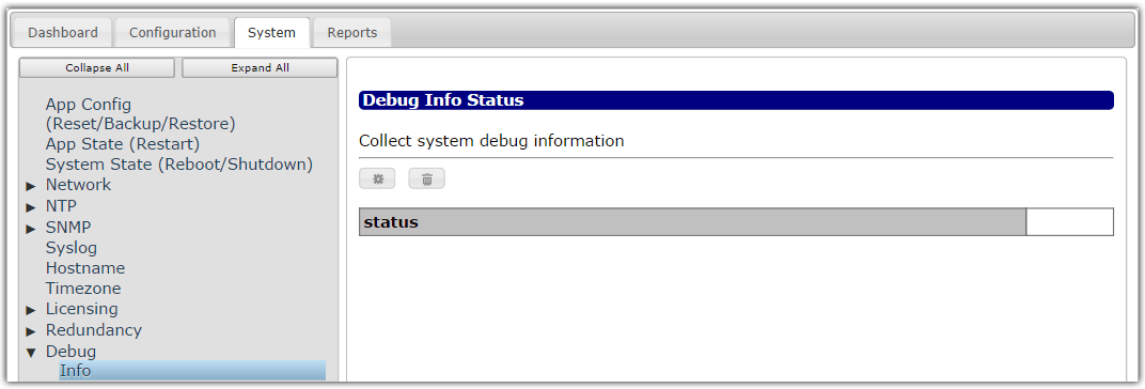
Menu Access and Usage

Both the *System* > *Debug* > *Info* and *System* > *Debug* > *Trace* menus should only be used under the direction of Imagine Communications Customer Support.

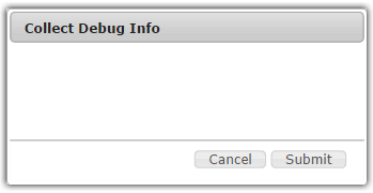
To collect diagnostic information in order to provide these file to Customer Support, proceed as follows:

1. From the **System** tab, click on the triangle next to the **Debug** branch to expand out one level.

2. Click the **Info** branch to open the *Debug Info Status* window.

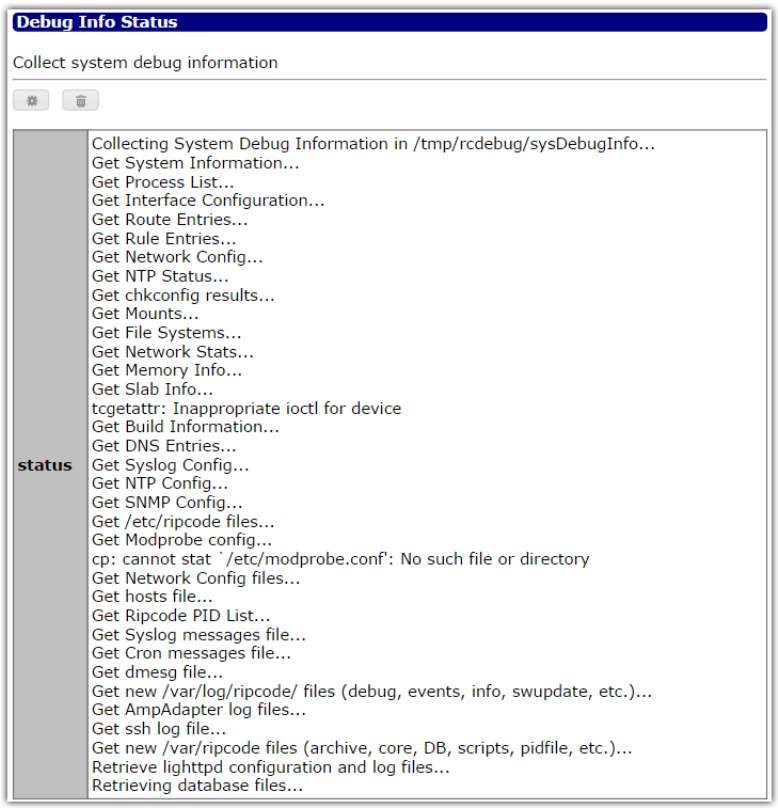


3. Click the execute ( ) icon to open the *Collect Debug Info* window.



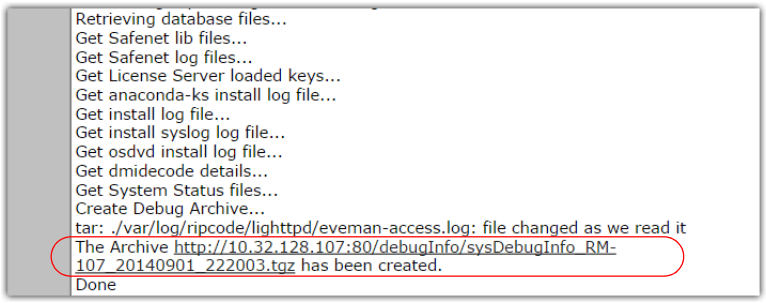
4. Click **Submit** to begin diagnostic collection.

   Progress will be shown in the status window as shown here:



5. Refresh your browser page (Shift+Enter, or right-click for refresh pop-up).

   The link to the debug info .tgz collection of files will be displayed at the bottom of the page:



Software Update

Software Update can perform both upgrades and downgrades for an RM and allows for in-process status monitoring.

This section briefly describes usage and fields in the **Software Update** menu.

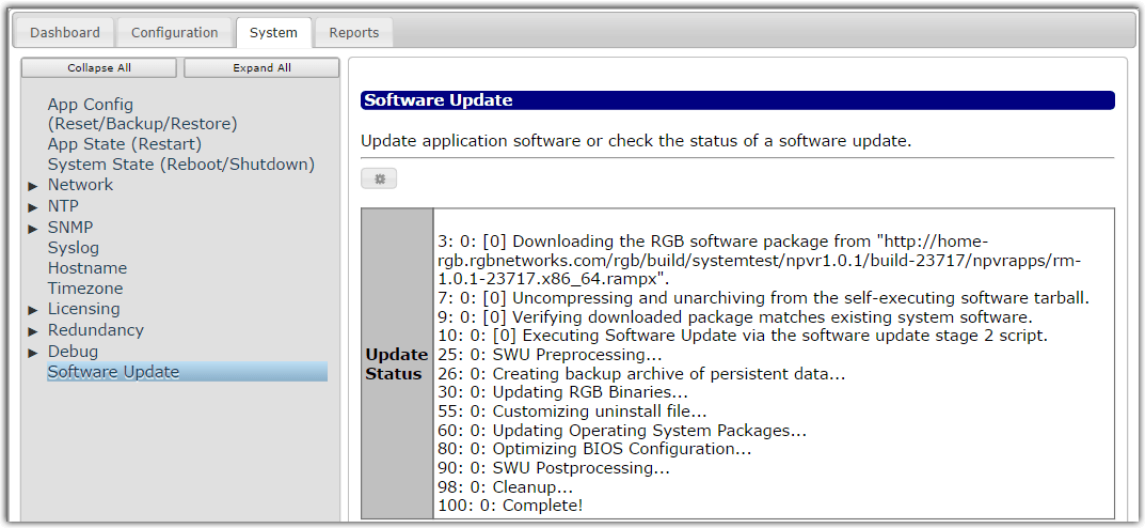
Note: *For detailed instructions on upgrading or downgrading either a standalone or redundant RM, please refer to the Recording Manager Software Installation, Setup, and Upgrade Guide for this release.*

Menu Access and Usage

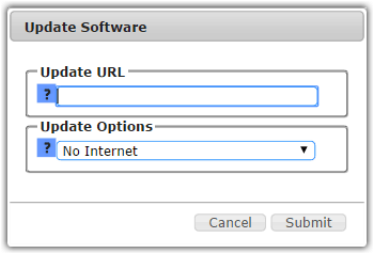
To access and use the **Software Update** menu, proceed as follows:

1. From the **System** tab, click on **Software Update**.

   If the system has been updated, the most recent software update status will be displayed in the menu.



2. To perform an update, click the execute ( ) icon to open the **Update Software** window:



3. In the **Update URL** field, enter the address to the location of the Imagine Communications software update package on your network. See Table 46.
4. From the **Update Options** drop-down, select whether to allow Internet connectivity during the update. See Table 46.
5. Click **Submit** to execute the software upgrade.

Menu Options

The options available in the **Update Software** menu are described in Table 46.

Table 46. Software Update menu options

Name	Description	Default

Update URL	Enter either an HTTP or TFTP URL indicating where the software is located. For example:
	`http://10.10.165.123/rip/rm-1.4-12345.x86_64.rampx`
	`-or-`
	`tftp://sw.rgb.com/rip/rm-1.4-12345.x86_64.rampx`
		Empty

Update Options	Select what kind of Internet connection, if any, the RM will use during the upgrade process. Choices are: No Internet — the system will not attempt to check if internet access is available for yum repos. No OS Update — only updates the Imagine Communications applications and will not update any OS-related packages. None — no extra options will be used.	No Internet

CHAPTER 9

Reports & Troubleshooting

This chapter describes how to use the **Reports** tab to obtain and display various reporting statistics on the RM, and provides contact information for Imagine Communications Customer Support.

In This Chapter:

Reports

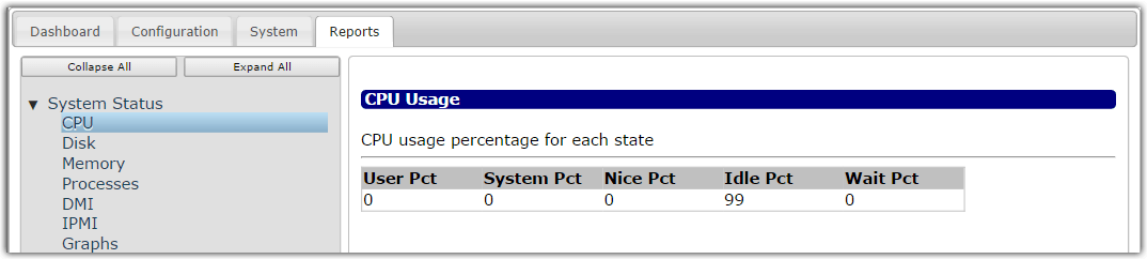
You can obtain several system statistics through the **Reports > System Status** tree, including Ethernet and hardware status, disk utilization, file storage capacity, and various statistical graphs.

The **System Status** tree contains the following branches, each of which will be discussed subsequently: CPU, Disk, Memory, Processes, DMI, IPMI, and Graphs. This section provides information on how to access each menu, and the menu's main function.

CPU

The **CPU** branch provides usage percentages for each state of the CPU on which RM is running. This menu presents similar statistics results as can be seen using the Linux "`top`" command.

Reports > System Status > CPU

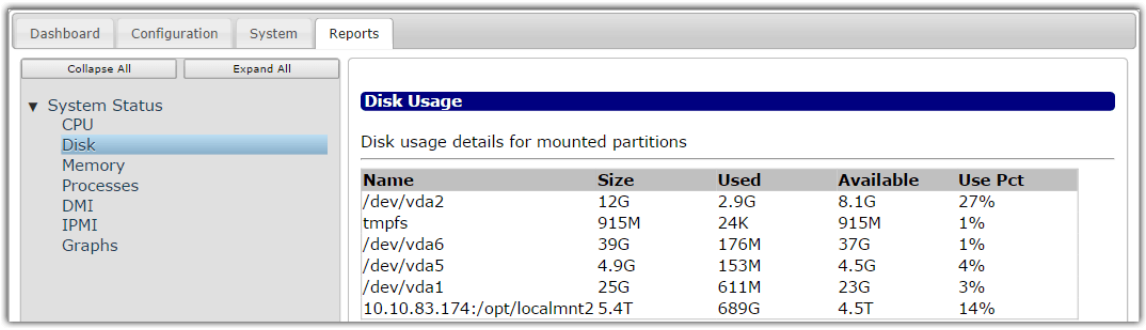


Disk

The **Disk** branch provides usage details for mounted disk partitions on which RM is running.

The operating system on which RM runs has several partitions. Using these partitions allows the system to continue to run even if one of the partitions is completely filled up; however, applications attempting to write to a full partition may behave erratically.

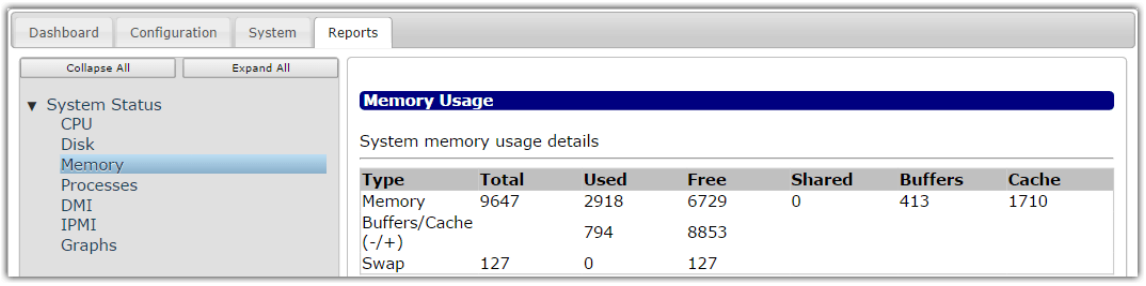
Reports > System Status > Disk



Memory

The **Memory** branch provides total amounts of free and used physical and swap memory for the device on which RM is running. All numbers are in Megabyte (MB) units.

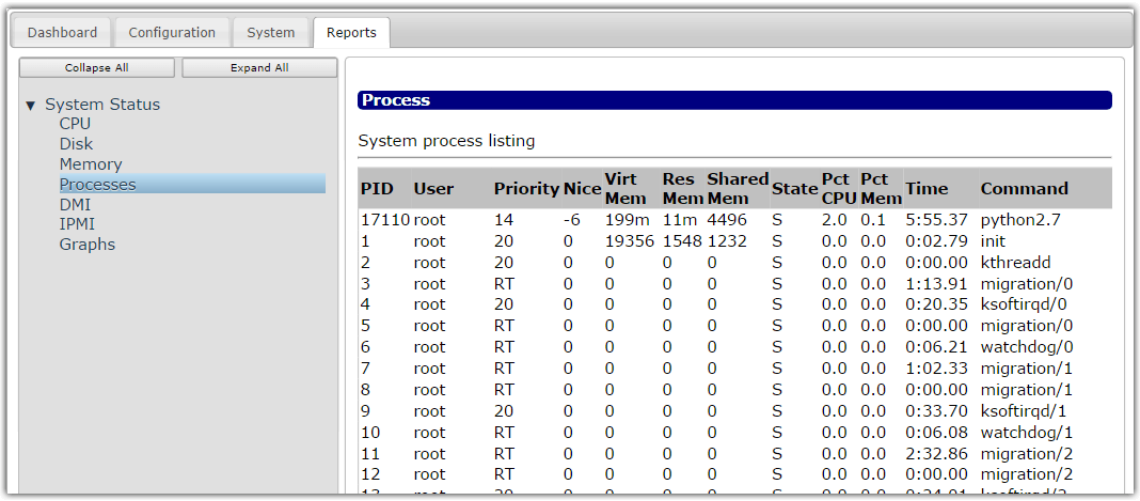
Reports > System Status > Memory



Processes

The **Processes** branch provides a list of all active processes that are currently running for the device on which RM is running.

Reports > *System Status* > *Processes*

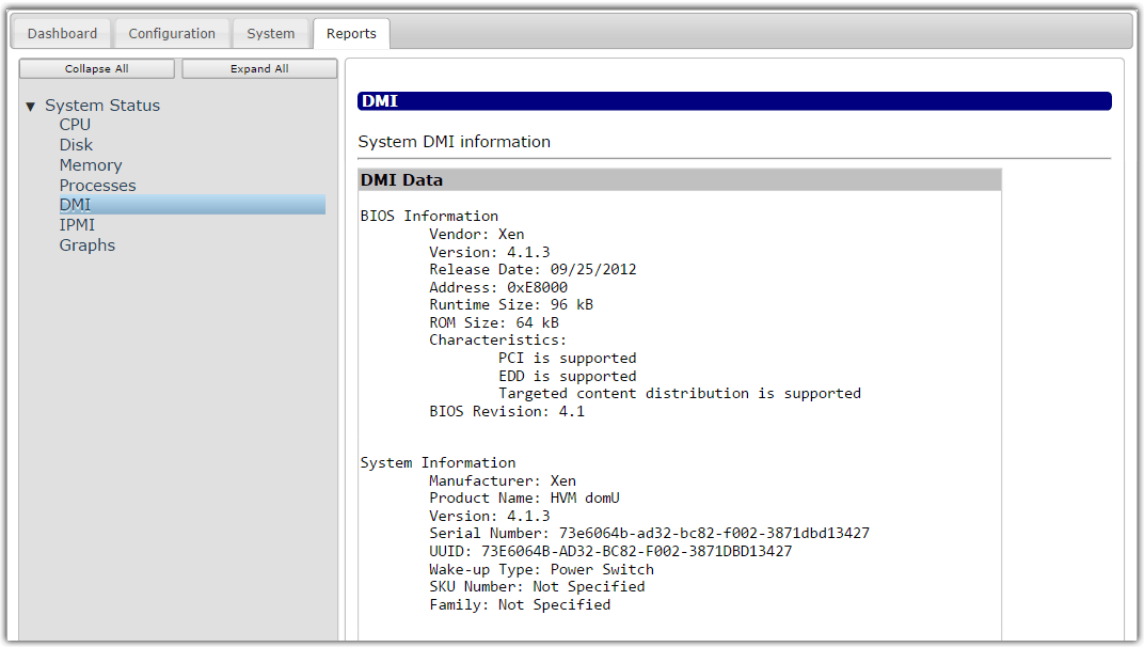


PID	User	Priority	Nice	Virt Mem	Res Mem	Shared Mem	State	Pct CPU	Pct Mem	Time	Command
17110	root	14	-6	199m	11m	4496	S	2.0	0.1	5:55.37	python2.7
1	root	20	0	19356	1548	1232	S	0.0	0.0	0:02.79	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	RT	0	0	0	0	S	0.0	0.0	1:13.91	migration/0
4	root	20	0	0	0	0	S	0.0	0.0	0:20.35	ksoftirqd/0
5	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
6	root	RT	0	0	0	0	S	0.0	0.0	0:06.21	watchdog/0
7	root	RT	0	0	0	0	S	0.0	0.0	1:02.33	migration/1
8	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/1
9	root	20	0	0	0	0	S	0.0	0.0	0:33.70	ksoftirqd/1
10	root	RT	0	0	0	0	S	0.0	0.0	0:06.08	watchdog/1
11	root	RT	0	0	0	0	S	0.0	0.0	2:32.86	migration/2
12	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/2

DMI

The **DMI** branch provides a status details list of the Direct Media Interface (DMI (SMBIOS)) table of hardware components for the device on which RM is running.

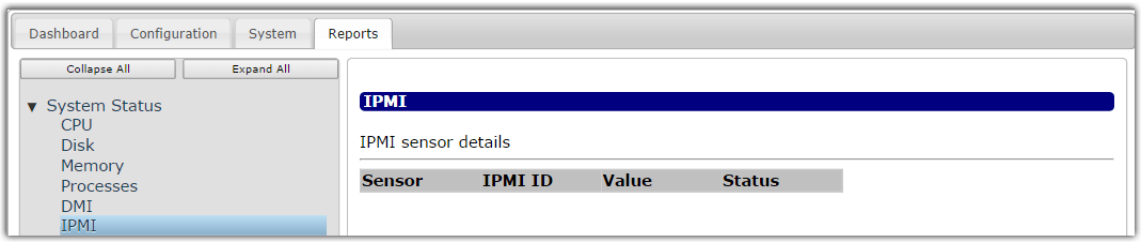
Reports > *System Status* > *DMI*



IPMI

The **IPMI** branch provides details on sensor data repository information (SDR) via Intelligent Platform Management Interface (IPMI). This field is only populated when the application is running on a hardware platform on which IPMI is enabled. A virtual machine displays no results for this menu.

Reports > *System Status* > *IPMI*



Graphs

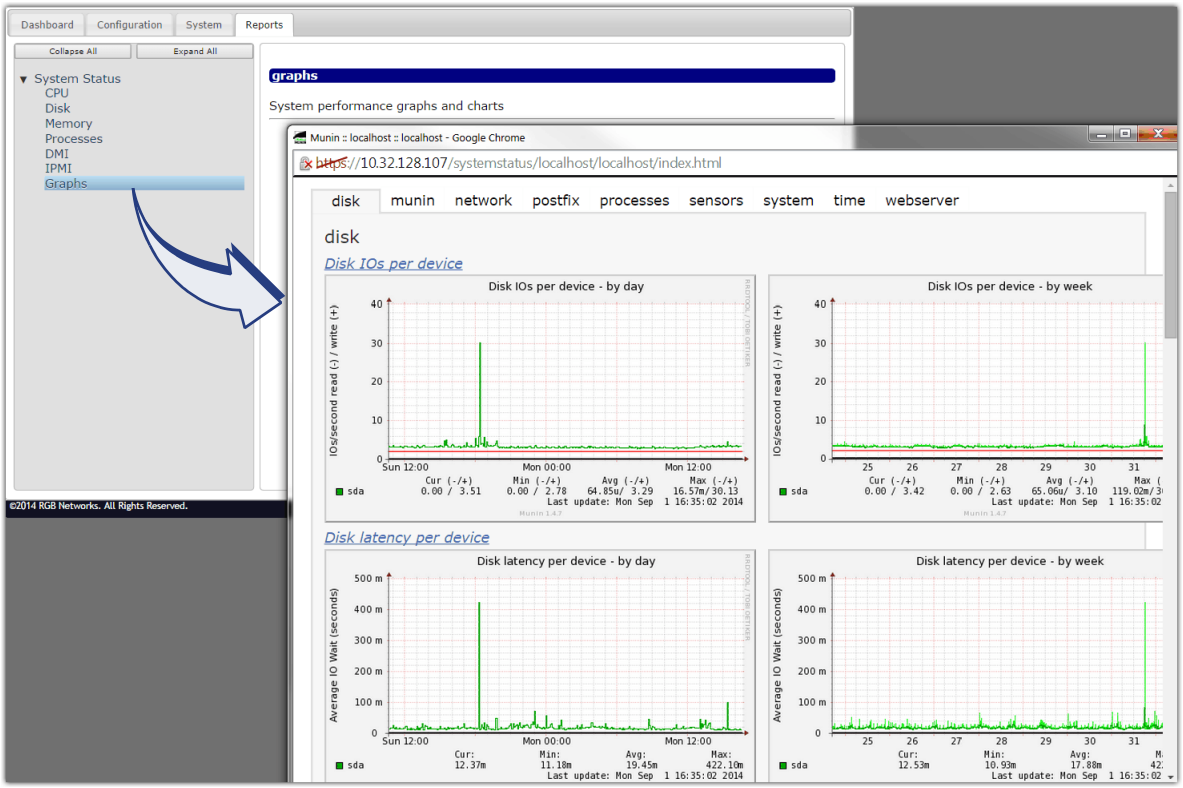
RM incorporates the Linux-based Debian archive tool "munin" to monitor and present system statistics in graphical form. Numerous statistics are collected through this tool including traffic stats, errors, bandwidth usage, processing percentage, hardware status, etc. The graphs are generated from plug-ins that provide system information. For each plug-in, several graphs are generated with different time-scales: day, week, month and year.

A number of graphs are available to view, each with detailed information on the following categories:

- **disk**—Provides statistics for the hard disk on which RM has been installed. 16 graphs available.
- **munin**—Provides statistics for the munin process running on RM. 2 graphs available.
- **network**—Provides statistics for RM's Ethernet interfaces. 30 graphs available.
- **postfix**—Provides statistics for message delivery. 4 graphs available.
- **processes**—Provides statistics for all processes running on RM's platform. 10 graphs available.
- **sensors**—Provides statistics for all hardware-related sensors such as fan speed and hardware temperature. 0 graphs available.
- **system**—Provides all system statistics such as CPU usage, logged in users, and system load. 22 graphs available.
- **time**—Provides statistics on the RM's interaction with an NTP server. 8 graphs available.
- **webserver**—Provides statistics on RM's webserver application. 4 graphs available.

Below is a sample of the type of graph that can be viewed from graph report menu. Up to 94 total graphs are available.

Reports > System Status > Graphs



Contacting Customer Support

Imagine Communications Customer Support is available 24x7. If after reviewing this section you still require assistance, please contact Customer Support via any of the following methods:

Table 47. Contacting Imagine Communications Customer Support

Method	Contact Information
E-mail	support@rgbnetworks.com
Internet	http://www.rgbnetworks.com/support/rgb-customer-portal.php
Inside North America	1.877.RGB.NETW // (1.877.742.6389)
Outside the North America	+1.408.701.2800

Information Required for Troubleshooting

Prior to contacting Customer Support, please collect diagnostics for the system as described in the section titled, "Debug Tree" on page 149.

APPENDIX A

RESTful API

This chapter provides information on how to access the Telurio Recording Manager's Application Programming Interface (API) in order to develop applications that access the RM software.

In This Appendix:

Overview

The RM uses Representation State Transfer (REST), an architectural paradigm that is used to create an interface using a client-server model.

Functionality

REST is not a specific protocol such as XML-RPC or Thrift. Typically, an HTTP infrastructure is used and assumed in the design of a RESTful API, but it is not required. Within the HTTP protocol specification a set of methods are designed that characterize the variation of client-server responses. For example, one method may be used to retrieve data while another may be used to create data.

Components

The *REST API* uses the following HTTP-based methods:

- HEAD
- OPTIONS
- GET
- POST
- PUT

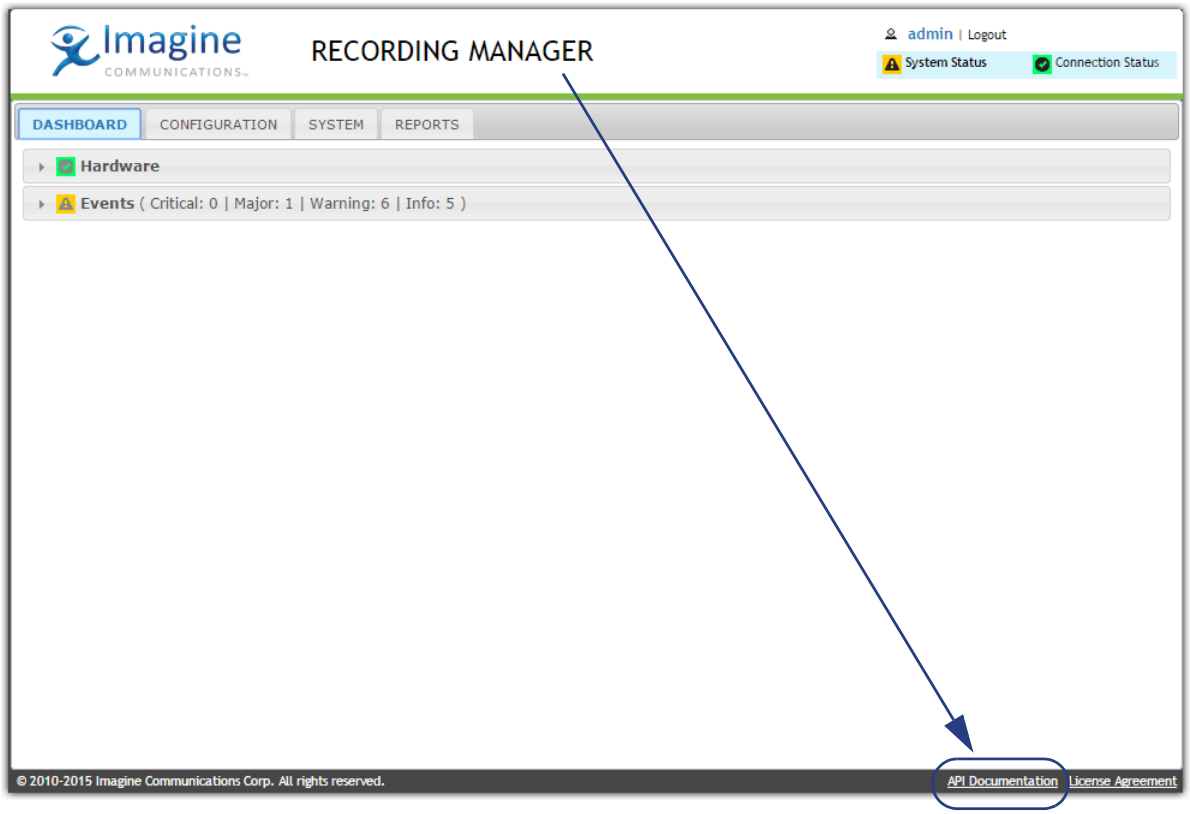
- PATCH
- DELETE

Since REST is not a protocol per se, the usage of these methods is not rigidly defined. However, there are certain expectations or conventions that are followed when using the various HTTP methods.

Access and Usage

For complete details on how to use the *RESTful API,* refer to the online help pages on your RM, which include API access and usage guidelines.

From the RM GUI, click on the **API Documentation** link at the bottom of any RM screen as shown here:



Or, enter the following address in your browser:

`http://<RM IP address or hostname>/rmdoc/index.html`

Where `<RM IP address or hostname>` = the IP address or hostname of your RM.