Haivision

Viper™

Multi-Stream Recording, Streaming & Publishing Appliance

Administration Guide Version 2.0

HVS-ID-AG-VIP-200
Issue 01

Copyright

Document Number: HVS-ID-AG-VIP-200
Version Number: v2.0-01

If you have comments or suggestions concerning this administration guide, please contact:

Technical Publications Department
Haivision
4445 Garand
Montréal, Québec, H4R 2H9 Canada

Telephone: 1-514-334-5445
info@haivision.com

Trademarks

Safety Guidelines

Use the following guidelines when unsafe conditions exist or when potentially hazardous voltages are present:

- Always use caution and common sense.
- To reduce the risk of electrical shock, do not operate equipment with the cover removed.
- Repairs must be performed by qualified service personnel only.

Antistatic Precautions

Electrostatic discharge (ESD) results from the buildup of static electricity and can cause computer components to fail. Electrostatic discharge occurs when a person whose body contains a static buildup touches a computer component.

The equipment contains static-sensitive devices that may be easily damaged, and proper handling and grounding is essential. Use ESD precautionary measures when installing systems or cards, and keep the parts and cards in antistatic packaging when not in use. If possible, use antistatic floorpads and workbench pads.

Improper handling and/or installation practices may VOID the warranty.

CAUTION When handling components, or when setting switch options, always use an antistatic wrist strap connected to a grounded equipment frame or chassis. *If a wrist strap is not available, periodically touch an unpainted metal surface on the equipment.* Never use a conductive tool, such as a screwdriver or a paper clip, to set switches.

Table of Contents

Safety Guidelines 3
Antistatic Precautions 3

About This Guide 9
About Haivision 10
Audience 10
Reliability of Information 10
Obtaining Documentation 10
Related Documents 11
Service Support 11
Document Conventions 11

New Product Features 1

Part I: Installation and Setup

Chapter 1: Introduction
Product Overview 8
Viper Features 9
Viper Applications 9
Viper Stand-Alone 10
Viper in a Furnace Realm – Distributed Recording and Publishing 11
Physical Description 12
Network Interfaces 12
Audio/Video Interfaces 13
Video Inputs 13
Audio Inputs 13
Video Outputs 14
PTZ Camera Control 14
LED Status Indicators 15

Chapter 2: Installing the Viper
Setting Up the Appliance 18
Safety First 18
Connecting the Viper to the Network 19

Viper Default Network Settings 19
Connecting the Viper to A/V Sources 21
Connecting the Video Inputs 21
Connecting the Audio Inputs 23
Connecting a PTZ Camera 24
Connecting the Viper to A/V Outputs 25
Powering Up the Viper 27

Part II: Administration

Chapter 3: Initial System Setup - Managing Users

Accessing the Administration Tools Portal 31
Creating and Managing Users and Groups 34
Default Usernames 34
Signing in to the Admin module 35
Configuring Users 37
Configuring Groups 40
Configuring Permissions for Groups or Users 43
Configuring Group Permissions 43
Hotmarks Entitlements 46
Configuring User Permissions 47
Setting a User's PIN 48
Configuring Guest Permissions 49
Configuring Touch Panel Guest Mode Permissions 51
Using Command Line Arguments to Manage Launch Preferences 52
Configuring LDAP Settings 54
LDAP Configuration Settings 57
Using Conditional Access for User Authentication 60
Channel Entitlements 62
Asset Entitlements 63
Keyword-based Entitlements 64
Managing Device Entitlements 65
Managing API Credentials 67
Creating a Credential 67
Associating the Credential With Viper Groups 68
Viewing the Consumer Key and Secret pair 69

Chapter 4: Admin Module - General System Configuration

General Configuration 71
General Configuration Options 73

Configuring the Launch Portal Theme 75
Guidelines for Changing the Launch Portal Theme 76
Re-Branding the InStream Interface 78
“Stretchable” Images 79
Branding Options 81
Customizing UI Labels 84
Encoder Configuration 86
Configuring the Video 86
Video Settings 87
Configuring the Audio 89
Audio Settings 90
Taking a System Snapshot 91
Server Manager 93
Managing the Server 93
Device States 96
Device Options 96
Configuring Network Settings 98
Network Settings 100
Advanced IP Settings 102

Chapter 5: Viper Integration into a Furnace Realm

Integration Overview 105
InStream 105
Conditional Access 105
Publishing 106
Authentication 106
Prerequisites 107
Summary of Steps 107
Setting Up Credentials 110
Create Viper Credentials (Furnace Credential Manager) 110
Assign Viper Credentials (Furnace Credential Manager) 112
Invitation Process 114
Invitation (Furnace Server Manager) 114
Accept the Invitation (Viper Server Manager) 115
Configure Viper Permissions (VF Admin) 118
Channel Configuration 119
Configure Viper Channels (Viper Channel Editor) 119
Output URLs for Encryption 122
Add Viper Channels to Furnace (Furnace Channel Editor) 123
Adding the Viper Channel to the Furnace Lineup 125
Publishing Options 126

Chapter 6: Configuring Channels

Channel Editor - Configuring Channels 129
Live Channels - Editing the Viper Channel 131
Channel Editor Settings 133
Setting Up InStream Talkback 135
Icon Manager - Managing Channel Icons 137
Lineup Editor - Managing the Channel Lineup 140
Creating Channel Lineups 140
Adding Viper Now On-Demand Titles to the Channel Lineup (STBs only) 141

Chapter 7: STB Image Provisioning

STB Imager - Managing STB Image Profiles 143
Adding a New STB Image Profile 143
Assigning a Profile to a STB 146
Creating a New Profile Assignment 147
Deleting a Profile Assignment 148

Chapter 8: Managing Reports

Viper Reports - Accessing Usage Statistics 150
Live Channel Stats Report 151
Past Channel Stats Report 152
Refining the Report 152

Part III: Asset Management

Chapter 9: Editing and Managing Assets

Viper Editor - Digitizing and Managing Assets 155
Creating Off-line Assets (Digitizing Assets) 155
Inserting Hotmarks 163
Adding or Modifying Asset Thumbnails 164
Merging Assets 166
Loading Assets 170
Exporting Assets 172
Deleting Assets 173
Publishing Assets 174

Chapter 10: Viewing and Deleting Recordings

NVR - Network Video Recorder 176
Viewing and Deleting Recorded Assets 178

Chapter 11: Managing Video on Demand

Viper NowAdmin - Making Assets Available On-Demand 180
Adding a New Viper Now Link 180
Viper Now Resource Link Fields 185
Adjusting Viper Now Server Configuration Settings 187
Viper Now Global Options Fields 188

Part IV: Reference

Appendix A: Glossary of Terms 190

Appendix B: Technical Specifications 193

A/V Input Specifications 194
A/V Output Specifications 195
Advanced Features 195
Video Encoding 196
Audio Encoding 196
IP Network Interfaces 197
Management Interface 197
Physical 198

Appendix C: Command Line Arguments 199

Syntax Conventions 200
Introduction 201
All Applications 202
InStream 203
InStream Multi-Stream Viewing 208
VF STB (Set Top Box) 209
VF NVR 211
VF Editor 212

Appendix D: Warranty Information 213

Haivision One (1) Year Limited Warranty 213
Haivision End User Software License Agreement 215

About This Guide

Welcome to the Administration Guide for Haivision's Viper™ Multi-Stream Recording, Streaming & Publishing Appliance, Version 2.0. This guide describes how to set up and manage systems using the administrative tools available via the Tools portal.

NOTE This guide is intended for system administrators and authorized site personnel only. Please see the Viper InStream User's Guide for information on the system interfaces that InStream users see, and the Viper Getting Started Guide for steps to operate the Touch Panel interface.

Topics In This Section

About Haivision 10
Audience 10
Reliability of Information 10
Obtaining Documentation 10
Related Documents 11
Service Support 11
Document Conventions 11

About Haivision

Haivision is a global leader in delivering advanced video networking, digital signage, and IP video distribution solutions. Haivision offers complete end-to-end technology for video, graphics, and metadata to help customers to build, manage, and distribute their media content to users throughout an organization or across the Internet. Haivision has specific expertise in the enterprise, education, medical/healthcare, and federal/military markets.

Haivision is based in Montreal and Chicago, with technical centers in Beaverton, Oregon; Austin, Texas; and Hamburg, Germany.

Audience

This guide is directed towards qualified service personnel such as technicians and network system administrators who have a basic knowledge of telecommunications equipment, and IP and LAN concepts and terminology.

Reliability of Information

The information contained in this administration guide has been carefully checked and is believed to be entirely reliable. However, as Haivision improves the reliability, function, and design of its products, the possibility exists that this administration guide may not remain current.

If you require updated information, or any other Haivision product information, contact:

Haivision
4445 Garand
Montréal, Québec, H4R 2H9 Canada

Telephone: 1-514-334-5445
Email: info@haivision.com

Or visit our website at: http://www.haivision.com

Obtaining Documentation

You may download the software, Release Notes, and user documentation, including this administration guide through Haivision's Download Center at: http://www.haivision.com/download-center/

NOTE All customers may access the Download Center; however, a login is required. If you do not have a login, select the link to create an account.

Related Documents

In addition to this administration guide, the following documents are also available through Haivision's Download Center (see link above):

- Viper Getting Started Guide
- Viper InStream User's Guide
- Viper API Integrator's Guide
- ViperData Ports and Security Policy

Service Support

Haivision is committed to providing the service support and training needed to install, manage, and maintain your Haivision equipment.

For more information regarding service programs, training courses, or for assistance with your support requirements, contact Haivision Technical Support via our Support Portal on our website at: http://www.haivision.com/support/

Document Conventions

The following document conventions are used throughout this administration guide.

TIP The light bulb symbol highlights suggestions or helpful hints.

NOTE Indicates a note, containing special instructions or information that may apply only in special cases.

IMPORTANT Indicates an emphasized note. It provides information that you should be particularly aware of in order to complete a task and that should not be disregarded. IMPORTANT is typically used to prevent loss of data.

CAUTION Indicates a potentially hazardous situation which, if not avoided, may result in damage to data or equipment, or minor to moderate injury. It may also be used to alert against unsafe practices.

New Product Features

Viper v2.0 introduces the following new features and enhancements:

User Interface Update (Touch Panel and Web Interface)

Viper v2.0 has updated its Touch Panel and Web user interfaces to match the new look and feel of the Haivision corporate user interface.

RTMP Support

The Viper now can create Real Time Messaging Protocol (RTMP) streams from Transport streams in order to send those streams to Flash enabled media servers. The following Flash-enabled CDNs are supported:

- Akamai 1st Generation and HD2 CDN.
- Generic FMS

For more information, see the Viper Getting Started Guide.

REST API

Viper v2.0 provides an XML Representational State Transfer (REST) Application Programming Interface (API) support to provide remote control of the Viper's functionalities from a third-party. The objective is to allow integrators knowledgeable with HTTP API (REST API) to send commands to the Viper to capture content.

Specifically, the API may be used to control tasks that would otherwise be accomplished through its Admin Web portal, including NVR (Network Video Recorder) commands for controlling a recording or the ability to start and stop video streams.

Viper administrators can select which recording interface should be available to users, either the REST API or the Touch Panel recording interface. This is done from the Admin Web portal (Admin>Configuration).

For more information, see the Viper API Integrator's Guide.

API Translator

Viper v2.0 also introduces an API Translator system to allow third party control systems to interface with the Viper REST API.

The API Translator serves as a proxy interface that accepts simple commands from a control system over a telnet connection, translates the commands into REST calls to the Viper API, and returns an easy-to-parse response back to the control system.

For more information, see the API Translator Installation and Reference Guide.

Embedded SDI Audio

The Viper now supports embedded SDI audio. This increases the number of accessible audio sources from three to five stereo pairs (SDI 1-2, SDI 3-4, 1/8” (3.5mm) Mini, RCA, and XLR).

For more information, see the Viper Getting Started Guide.

Audio Peak Meters

Viper v2.0 provides audio peak meters on the Touch Panel interface to provide a visual confirmation that the selected audio inputs have a valid feed prior to streaming or recording.

For more information, see the Viper Getting Started Guide.

Video Output Display

The previous Viper release introduced the ability to output (“mirror”) the visual content displayed in the Touch Panel via the HDMI 1 or VGA connector. Viper v2.0 may also be configured to display the video streams either with or without the Touch Panel user interface. This is done from the Touch Panel interface (Admin > Display Settings screen).

NOTE When you select Video:

- The display will be blank except when the Viper is displaying a stream (e.g., Select Inputs, Stream & Record, and Review & Publish>Review screens).
- You can select the display format, either: PIP, Source 1, or Source 2 only.

For more information, see the Viper Getting Started Guide.

Networking Configuration

The Viper now allows administrators to change the IP settings from the Touch Panel interface. Previously these settings could only be configured from the Admin Web portal (Admin>Server Manager page). This simplifies the initial integration of a Viper into the customer’s network and speeds up the access to the Viper functionalities.

For more information, see the Viper Getting Started Guide.

Stream Encryption

The Viper now allows administrators to set the encryption level for the two streams in order to secure their access from unauthorized users. This is done from the Admin Web portal (Channel Editor page).

There are three selectable levels: None, AES-128 and AES-256.

For information, see "Channel Editor - Configuring Channels" on page 129.

Remote Control for PTZ Camera

The Viper now supports remote control of video cameras with VISCA (Video Systems Control Architecture) – RS-232 Control protocol (commonly referred to as PTZ remote camera control).

Users can now control the PTZ (pan tilt and zoom) controls of the camera, by hand from the Touch Panel interface. The controls are available in the Select (Video) Inputs and Stream & Record Activity Screens.

For information on connecting the camera to the Viper, see "Connecting a PTZ Camera" on page 24. For information on controlling the camera from the Touch Panel interface, see the Viper Getting Started Guide.

NOTE The VISCA protocol supports up to seven PTZ cameras over the same interface. In this case, several cameras can be daisy-chained over the same RS-232 communication port.

Talkback Support

The Viper now allows end users monitoring a Viper session through an InStream software player to reply back (audio only) directly to the individuals at the video source, via a speaker or headphones connected to the Viper appliance.

NOTE This is only supported on InStream players running on Windows systems.

For information on setting up Talkback, see "Setting Up InStream Talkback" on page 135.

VoD for Set-Top Boxes (Stingray)

The current release introduces Viper Now into the Viper toolset to allow the asset to be displayed in Stingray set-top boxes. Including Viper Now allows access to VoDs, through the Admin Web portal, in the STB Guide listing.

For information on connecting the camera to the Viper, see "Viper NowAdmin - Making Assets Available On-Demand" on page 180.

Persistent Video, Audio and Metadata Settings

Viper v2.0 provides persistent settings selection for the Video, Audio, and Metadata Settings. The settings will be persistent throughout power cycle or appliance restart.

Once the Apply button is selected, the new settings will be permanent until a new selection is made.

HVC Support

Viper v2.0 supports exporting of Viper recorded assets via the Haivision Video Cloud (HVC) VCMS video platform to a folder located on an FTP server.

For information about setting up a new HVC account, please contact your Haivision sales representative or hvc-sales@haivision.com.

Guest Access

Viper v2.0 introduces a Guest profile to allow quick access to the Viper Touch Panel interface. Guest mode eliminates the need to enter a PIN code for user authentication, thereby reducing the time to start streaming and/or recording a session. Guest mode permissions are pre-defined by the Administrator from the Admin Web portal (under Guest Permissions on the Admin > Group Permissions or User Permissions page).

Touch Panel interface users can now enable Guest mode from the Info Screen (using a long hold from the Touch Panel Welcome screen). Once enabled, users can simply “Touch Anywhere To Begin” on the Welcome screen and the Viper will open the Stream & Record Activity screen.

See “Configuring Guest Permissions” on page 49.

Asian Font Support

Touch Panel labels can now be displayed with either Japanese, Chinese or Korean characters. Touch Panel interface users can now enable Asian Fonts from the Info Screen (using a long hold from the Touch Panel Welcome screen).

For more information, see the Viper Getting Started Guide.

NOTE The labels must be customized and uploaded from the Admin Web portal (see the following feature, “Touch Panel Label Localization”).

Touch Panel Label Localization

Viper v2.0 administrators can customize the text displayed on the InStream player, user portal, error messages, as well as the Touch Panel interface. This is done from the Admin Web portal (Configuration>UI Labels page).

See “Customizing UI Labels” on page 84.

Transfer/Export Asset(s) to an External USB Drive

Viper recorded assets can now be transferred directly to an external USB storage device connected to the one of the five USB ports. The supported drive format is FAT32 in order to allow for support across operating systems such as Windows, OSX, and Linux.

For more information, see the Viper Getting Started Guide.

File Format Conversion of Recorded Assets

When exporting recorded assets, the Viper can also transcode assets from H.264 (Transport Stream) to AVI, WMV, MOV (QuickTime), or MP4. The transcoded assets will be saved on USB storage devices.

Dual assets will be transcoded as two distinct assets.

For more information, see the Viper Getting Started Guide.

Hotmark Enhancements

Viper v2.0 supports up to 14 “live” Hotmarks with a 28 character length.

See “Hotmarks Entitlements” on page 46.

Viper MAX and Viper VF Merged

Viper MAX and Viper VF are now referred to as Viper, and Viper VF will have the same functionality of the former Viper MAX.

PART I: Installation and Setup

CHAPTER 1: Introduction

This chapter provides a brief overview of Haivision's Viper™ Multi-Stream Recording, Streaming & Publishing Appliance, along with a description of the main hardware components.

Topics In This Chapter

Product Overview 8
- Viper Features 9
- Viper Applications 9
- Viper Stand-Alone 10
- Viper in a Furnace Realm – Distributed Recording and Publishing 11

Physical Description 12
- Network Interfaces 12
- Audio/Video Interfaces 13
- LED Status Indicators 15

Product Overview

The Viper Multi-Stream Recording, Streaming & Publishing Appliance is the evolution of Haivision's Furnace VF Live Encoder and VF Stand-Alone Encoder. The Viper incorporates the live encoding capabilities of the Makito/Barracuda encoders, while addressing advanced applications requiring built-in storage and raw video frame processing.

The Viper combines encoding, storage, compute power, and a Touch Panel human-machine interface. The Viper can be used either as a stand-alone appliance or as a companion contribution appliance for the Furnace IP video distribution system. Within a Furnace environment, the Viper acts as an additional recording and encoding appliance, supporting and enhancing Haivision's ecosystem.

Figure 1-1 Viper Front view

Figure 1-2 Viper Rear view

Using the Touch Panel interface, Viper users can set up a multi-channel session, initiate simultaneous streaming and recording, and automatically make content available for on-demand viewing.

The Viper captures full resolution, full frame rate dual-channel content synchronously, thereby assuring contextual review. During the session, remote viewers can watch multi-stream HD content live simply by clicking a Web link and launching Haivision's browser independent InStream player. After recording the event, the operator can make the multi-stream asset available for direct on-demand viewing. When combined with the Viper's Conditional Access module, the operator can securely publish assets within the Viper portal.

Viper Features

- Dual-stream appliance
- Desktop and portable installations
- Touch Panel interface for simple operation
- Login + PIN code to manage access to Viper as well as user entitlements
- Intuitive recording and streaming of two signals (e.g., Video + Desktop)
- Local recording
- Streamlined Stream / Record / Review / Publish workflow
- Stand-alone or integrated within Furnace (managed through Furnace Portal)
- Audio Talkback from InStream player to host Viper

Viper Applications

The Viper was designed to capture presentations, situational training, and other forms of instruction – in which live, personal expression by a presenter is combined with dynamic media such as animations, real-time video, and information from software programs such as spreadsheets, CAD tools, and simulators.

In order to effectively transmit the in-room experience live via IP video streaming, both the live camera feed and any associated dynamic media must be available simultaneously to out-of-room viewers. The combined video stream should also be available to viewers who may wish to review the experience at a later time, on-demand.

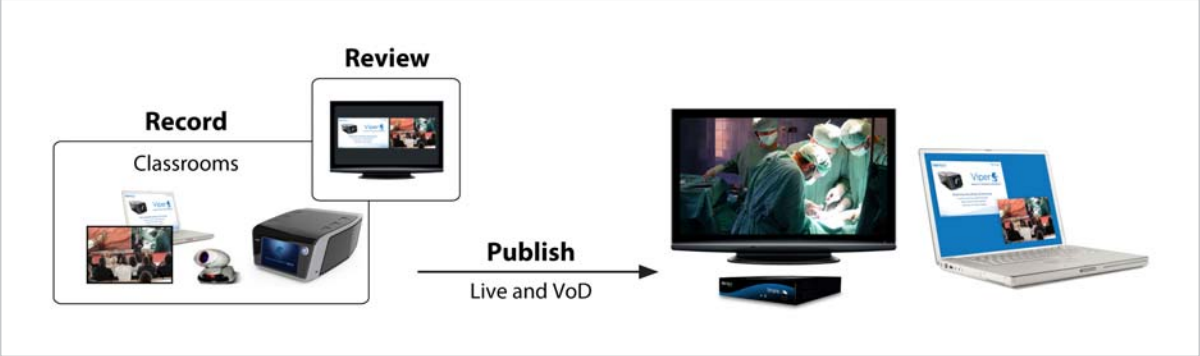
The Viper supports simultaneous capture and streaming of high-resolution sources, such as an HD camera and a computer. Either source can be high definition video or high-resolution computer graphics encoded in real-time to H.264. During live viewing or replay of the "event", the streams remain associated and synchronized. Both media streams are always available at full resolution, and viewers can select the most appropriate display layout, using Haivision's InStream player.

A PTZ camera, with VISCA protocol, may also be connected to the Viper to allow users to remotely control the camera's Pan Tilt and Zoom controls from the Touch Panel interface.

Viper Stand-Alone

Viper can be used as a stand-alone user operated appliance for recording, streaming, and video-on-demand, providing dual-stream HD and metadata capabilities. The following diagram illustrates a typical Viper stand-alone scenario.

Figure 1-3 Viper Stand-Alone Scenario



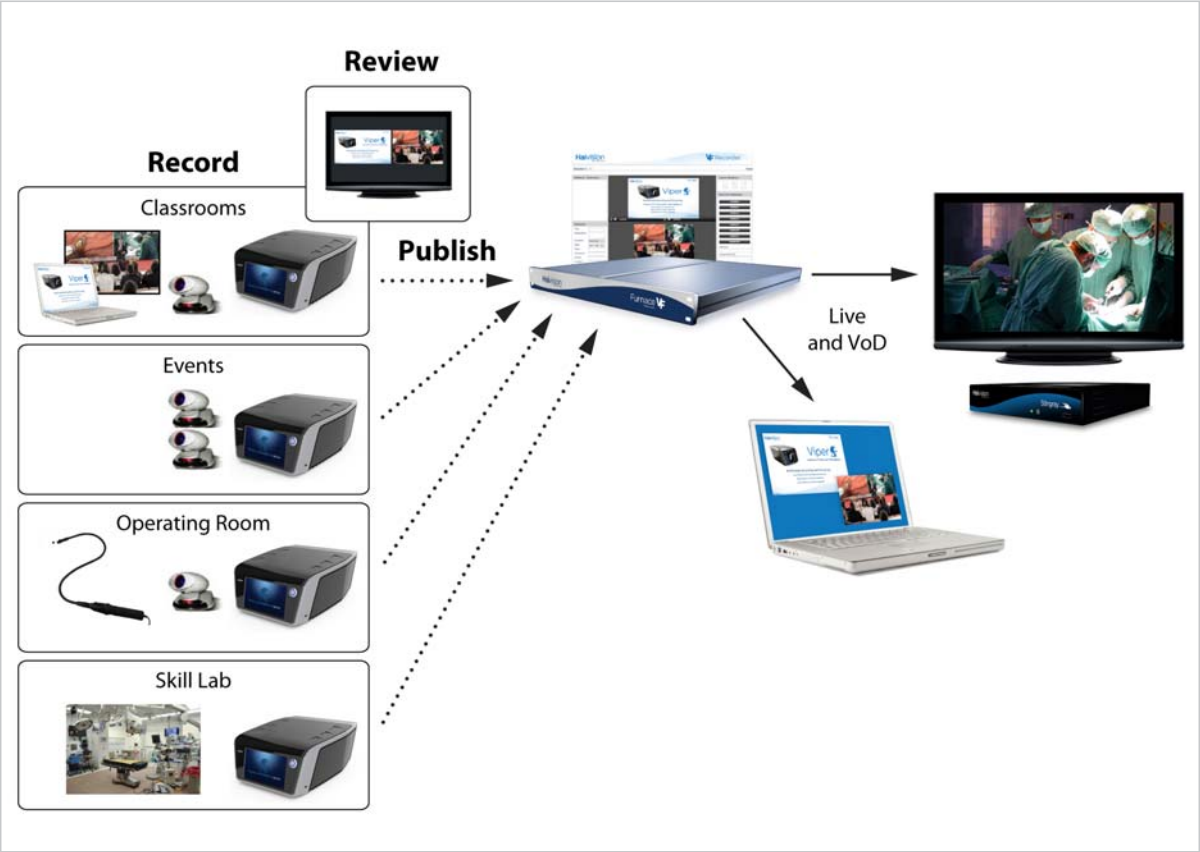
Related Topics

- "Integration Overview" on page 105
- "Viper Integration into a Furnace Realm" on page 104

Viper in a Furnace Realm – Distributed Recording and Publishing

Viper may also be used as a satellite streaming and recording appliance residing within the network realm of a hosted Furnace server (Furnace v6.2.2 or later). The following diagram illustrates a Viper scenario in a Furnace realm.

Figure 1-4 Viper in a Furnace Realm



Related Topics

- "Integration Overview" on page 105
- "Viper Integration into a Furnace Realm" on page 104

Physical Description

The Viper comes delivered as a compact, integrated appliance featuring a Touch Panel interface. Following is a description of the Viper interfaces, connectors, and LED status indicators.

Network Interfaces

The Viper comes with two 10/100/1000 Base-T Ethernet Network interfaces (RJ45, located at the back of the unit) for both traffic and management.

NOTE Viper units ship from the factory with the following network settings:

- Eth0 is configured using a static IP address (10.5.1.2) to allow you to connect directly to the unit from a 10.5.x.x domain.

  To configure the network settings from the Touch Panel interface (Admin>IP Settings screen), see “Changing the Viper’s IP Address” in the Viper Getting Started Guide.

- Eth1 is only used by Haivision support engineers and should *not* be used for normal operation.

Figure 1-5 Ethernet Connection

Ethernet Connection [**Eth0** must be configured with a valid IP address and gateway to work in your environment. See Note above.]

Related Topics

- “Connecting the Viper to the Network” on page 19

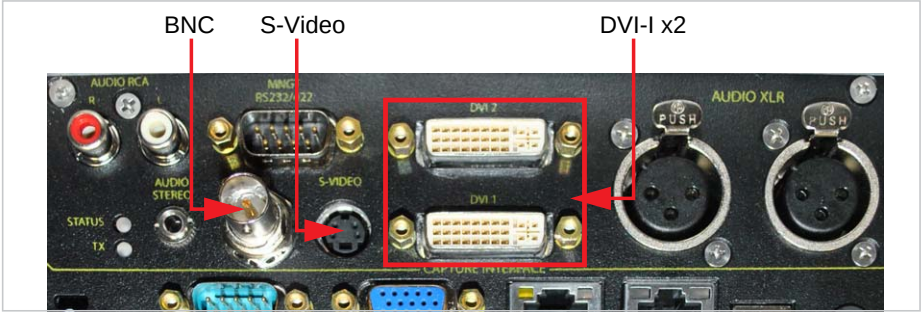
Audio/Video Interfaces

Video Inputs

The Viper supports the following Video inputs:

- DVI-D and Component (Analog): 2x DVI-I (DVI-Integrated) connectors
- 3G/SD/HD SDI: BNC connector
- Composite NTSC or PAL (CVBS): BNC connector
- S-Video: 4-pin Mini-DIN connector

Figure 1-6 Video Input Connections

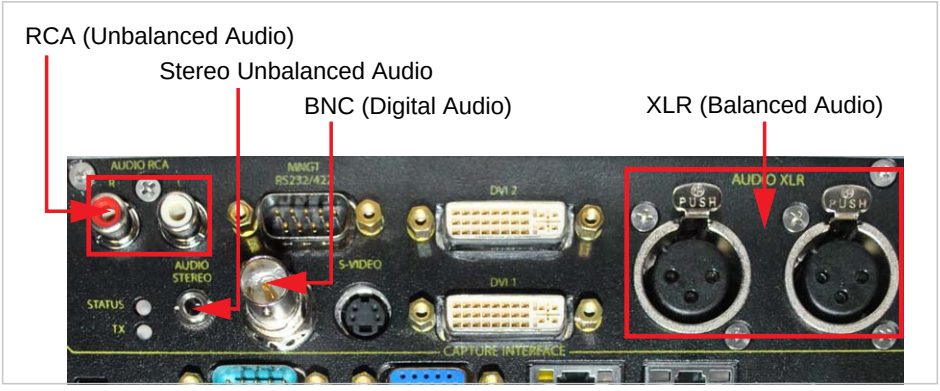


Audio Inputs

The Viper supports the following Audio inputs:

- Stereo Unbalanced: 1/8” Jack Audio Stereo connector (TRS 3.5 mm).
- Balanced Audio: XLR Right and Left connectors
- Unbalanced Audio: RCA Right and Left connectors
- Digital Audio: SDI via BNC connector (Channels 1-2 or 3-4)

Figure 1-7 Audio Input Connections

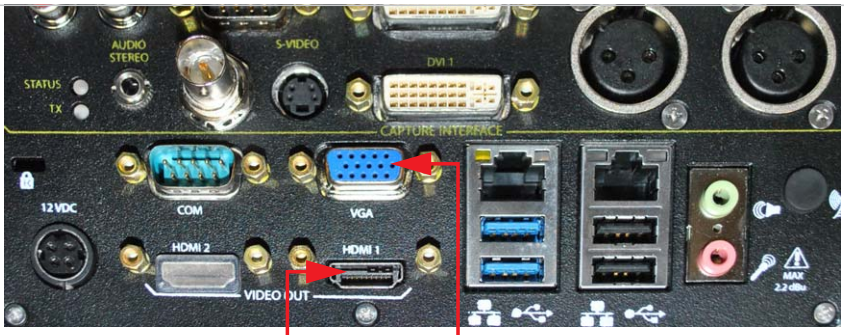


Video Outputs

The Viper supports the following Video outputs:

- HDMI 1
- VGA

Figure 1-8 Video Output Connections



PTZ Camera Control

A PTZ camera, with VISCA protocol, may be connected to the Viper's RS-232 ("COM") port to provide remote PTZ camera control from the Touch Panel interface.

Figure 1-9 PTZ Camera Connection

Related Topics

- "Connecting the Viper to A/V Sources" on page 21
- "Connecting the Viper to A/V Outputs" on page 25
- "Connecting a PTZ Camera" on page 24

LED Status Indicators

The LED colors and flashing (blinking) speed indicate the status (operational state) of the appliance.

Figure 1-10 LED Status Indicator (Front panel)

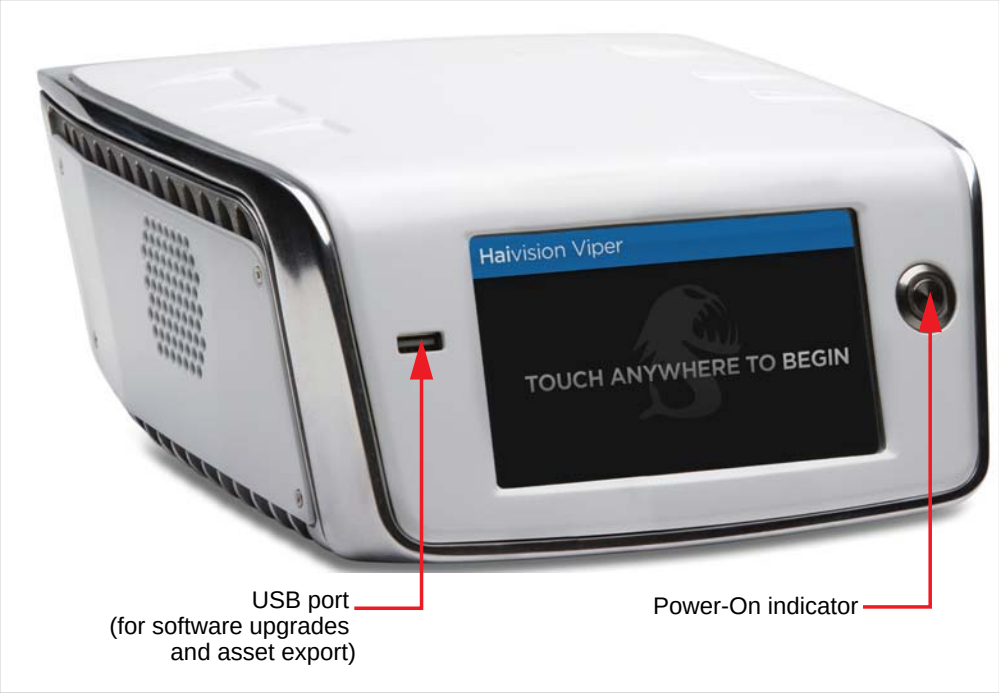


Table 1-1 LED Status Indicator – Front Panel

Function	Color	Description	Indication
Power-On	Blue	OFF	No power
		BLUE Solid	Blue LED integrated in the Power button indicates when the appliance power is On.

Figure 1-11 LED Status Indicators (Rear view)

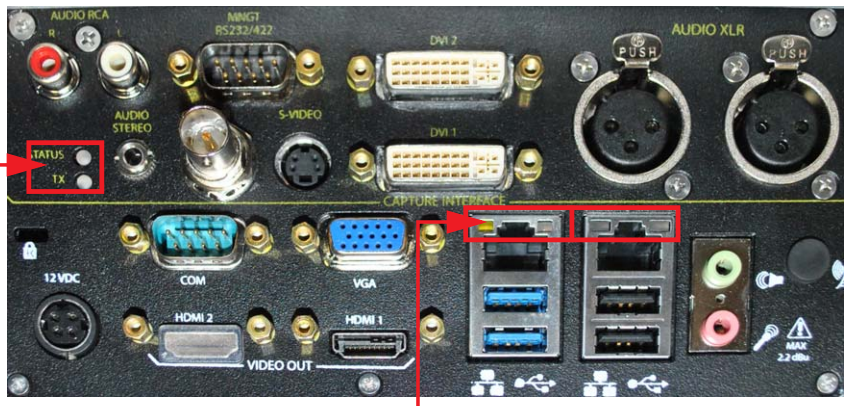


Table 1-2 LED Status Indicators – Rear Panel

Function	Color	Description	Indication
STATUS	RED/ GREEN	OFF	No power
		RED Solid	Error / Fault (capture card)
		GREEN Blinking	Booting / Initialization (capture card)
		GREEN Solid	No Fault / OK
TX	AMBER/ GREEN	AMBER Solid	At least one of the conditions below is sufficient to turn the LED AMBER: • Capture card not NOT ready, or • Valid video input NOT detected
		GREEN Solid	Valid video input detected from "Primary" encoder.
Network [Eth1 and Eth0] ports			
ACT	YELLOW	OFF	No activity.
		YELLOW Blinking	Active network traffic detected.
LINK	AMBER	OFF	Not connected.
		AMBER Solid	Valid link present.

Related Topics

- "Powering Up the Viper" on page 27

CHAPTER 2: Installing the Viper

This chapter explains how to set up and connect the Viper.

Topics In This Chapter

Setting Up the Appliance 18
Safety First 18
Connecting the Viper to the Network 19
Viper Default Network Settings 19
Connecting the Viper to A/V Sources 21
Connecting the Video Inputs 21
Connecting the Audio Inputs 23
Connecting a PTZ Camera 24
Connecting the Viper to A/V Outputs 25
Powering Up the Viper 27

Setting Up the Appliance

Always read the instructions carefully and keep this administration guide for future reference.

Please choose a suitable, well-ventilated location for operating the appliance. By doing so you will preserve long lifesaving and stability of the unit(s).

Set up the unit on a reliable and flat surface, or mount in a rack which has active ventilation.

TIP Make sure that there is sufficient air flow around the unit and that there are no foreign bodies blocking the air exhaust fan.

When mounting in a rack, it is recommended to leave a minimum of 6 inches (15cm), between Vipers if you intend to place them next to each other.

Safety First

Please pay particular attention to the following points in order to help protect yourself and the appliance:

- Refer to "Safety Guidelines" on page 3.
- The Viper is an indoor appliance and should be kept in a dry, dust free environment.
- There are no user-serviceable parts inside the unit. Making unauthorized changes will void the warranty.
- Only connect the unit to a compatible power source.
- If an electrical fault occurs, disconnect the unit and contact Haivision Technical Support.
- Never try to force the connections when setting up the system as this may damage the unit.

Connecting the Viper to the Network

When you receive your Viper, you will need to change the factory default network configuration to work in your environment. Before you can begin streaming and recording, you *must* re-configure Eth0 with a valid IP address and gateway for full network functionality.

Viper Default Network Settings

By default, Eth0 is configured using a static IP address (10.5.1.2) to allow you to connect directly to the unit from a 10.5.x.x domain.

- You can configure the network settings from the Touch Panel interface (Admin>IP Settings screen). For details, see “Changing the Viper’s IP Address” in the Viper Getting Started Guide.
- You can also communicate with the Viper Eth0 interface by setting up a switch with the Viper connected to Eth0 and a computer configured with a 10.5.X.X/255.255.0.0 IP address or IP alias.

  Once your computer is configured for the Viper network, you can configure the Viper network settings by accessing https://10.5.1.2/admin in your Web browser.

On the Viper Touch Panel interface, both the Info screen and the Admin screen display the Eth0 IP address.

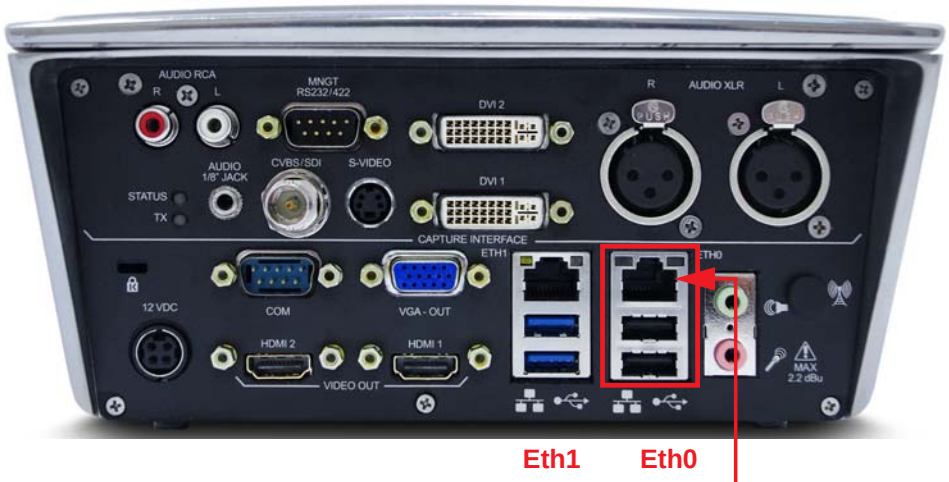
IMPORTANT Eth1 is only used by Haivision support engineers and should *not* be used for normal operation.

To connect the Network Interface:

1. To get started, connect the Viper's Eth0 port to the IP network using an Ethernet UTP cable (Type Cat 5 or higher grade). See "Viper Default Network Settings" above to re-configure Eth0 with a valid IP address and gateway.

   This will allow you to connect to the unit via the Web Admin portal.

Figure 2-1 Network Connection



Connect Ethernet cable to Eth0 [**Eth0** must be configured with a valid IP address and gateway to work in your environment.]

Connecting the Viper to A/V Sources

You can connect multiple video inputs on the Viper and then select the two inputs to use from the Touch Panel interface. This allows you to easily switch between analog and digital video inputs without having to plug and unplug cables.

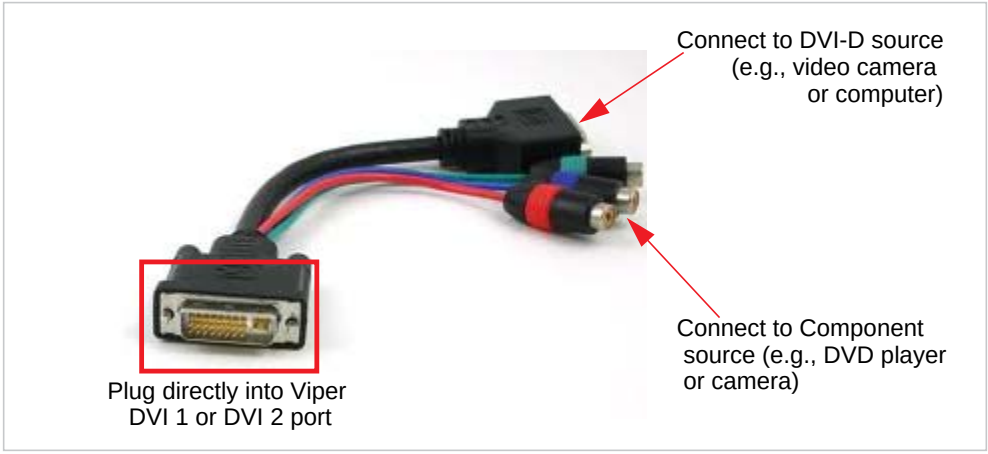
Connecting the Video Inputs

Connect one or more of the Viper's Video Inputs to Video Sources (such as a video camera, DVD player, or computer video card), using the appropriate connector(s):

To connect Digital DVI or Component Analog Video, or Computer Graphic Inputs:

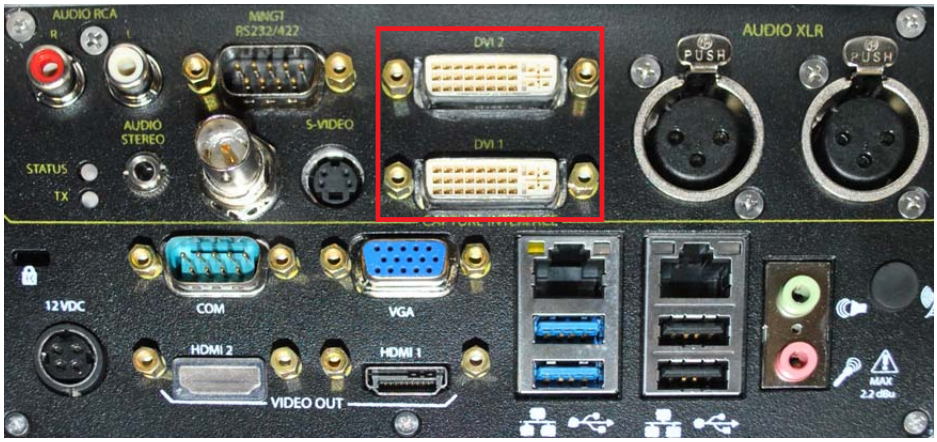
1. Plug the DVI-I male connector on the DVI and Component to DVI Adapter (shown in Figure 2-2, provided with the unit) directly into either the DVI 1 or DVI 2 input on the Viper (shown in Figure 2-3).

Figure 2-2 DVI and Component to DVI Adapter



NOTE This adapter allows you to connect both digital DVI-D and Component video sources to the Viper DVI input connector.

Figure 2-3 Component Analog/Digital Video/Computer Graphics Connections

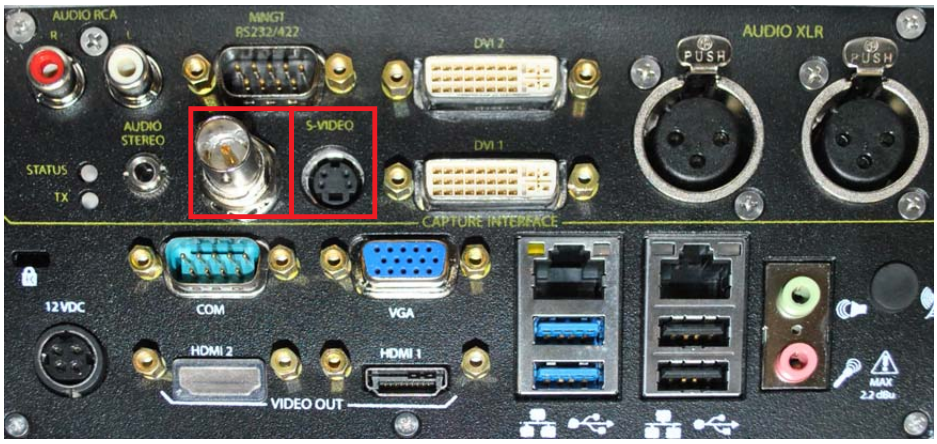


2. Then connect the DVI-D female connector and/or Component connectors on the adapter (shown below) to your video sources.

To connect S-Video or SD/Composite Video Inputs:

1. Connect your Video Source cables to the Viper's Video Inputs, using the appropriate connector(s):
   - S-Video: Use the 4-pin mini-DIN connector.
   - Composite (CVBS) Video: Use the BNC connector.
   - SDI Video/Audio (either SD or HD): Use the BNC connector.

Figure 2-4 SDI/Composite or S-Video Connections



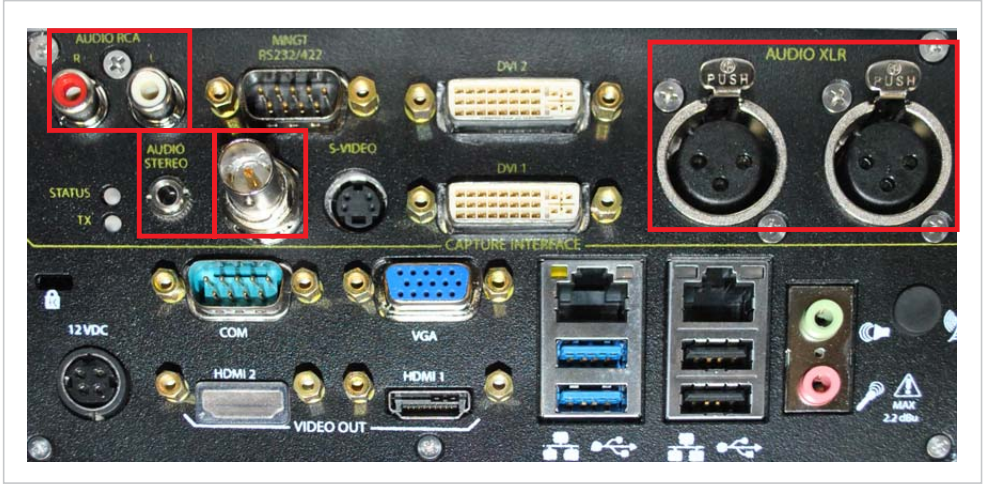
Connecting the Audio Inputs

You can also connect multiple audio inputs on the Viper and then switch audio sources from the Touch Panel interface.

To connect Audio Inputs:

1. Connect the Viper's Audio Inputs to Audio Sources, using the appropriate connector(s):
   - 1/8" Jack (Unbalanced): Use the Audio Stereo connector (TRS 3.5 mm).
   - XLR (Balanced) Audio: Use the XLR Right and Left connectors.
   - RCA (Unbalanced) Audio: Use the RCA Right and Left connectors.
   - SDI 1-2 (Digital): Use the BNC connector.
   - SDI 3-4 (Digital): Use the BNC connector.

Figure 2-5 Audio Connections



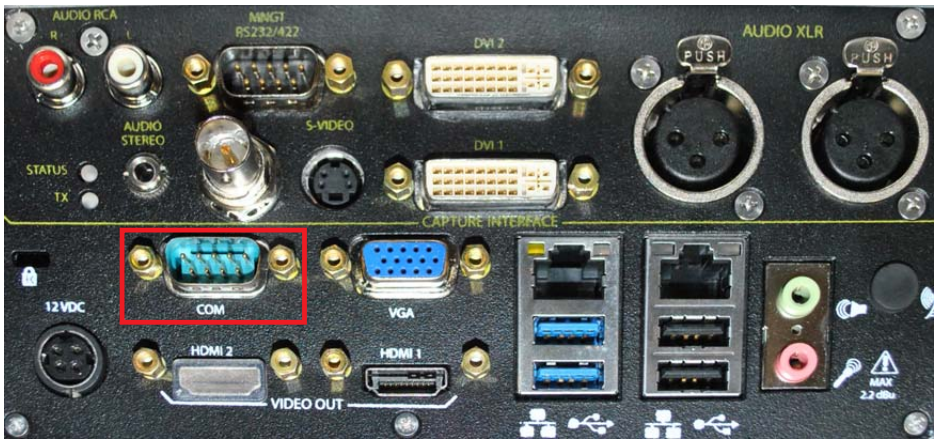
Connecting a PTZ Camera

You can also (optionally) connect a PTZ camera, with VISCA protocol, to the Viper to allow users to remotely control the camera's Pan Tilt and Zoom controls from the Touch Panel interface. You will need a cable appropriate for your camera.

The Viper supports the VISCA (Video Systems Control Architecture) – RS-232 Control protocol (referred to as PTZ remote camera control).

To connect a PTZ camera to the Viper:

1. Connect the cable from the camera to the Viper's RS-232 ("COM") port located next to the VGA port.



Connecting the Viper to A/V Outputs

The local HDMI 1 or VGA output ports may (optionally) be used to mirror the Touch Panel interface or display video during Streaming, Recording, and Reviewing. When a monitor is connected on one of those ports, it will show either the same Viper application display as the Touch Panel interface, or only the video streams without the user interface (configurable from the Touch Panel interface).

To connect HDMI or VGA Video Outputs:

1. (Optional) Connect one of the Viper's Video Outputs to a computer monitor or other display, using the appropriate connector:
   - HDMI: Use a Type-A 19-pin HDMI connector.
   - VGA: Use an HD-15 D-Sub connector.

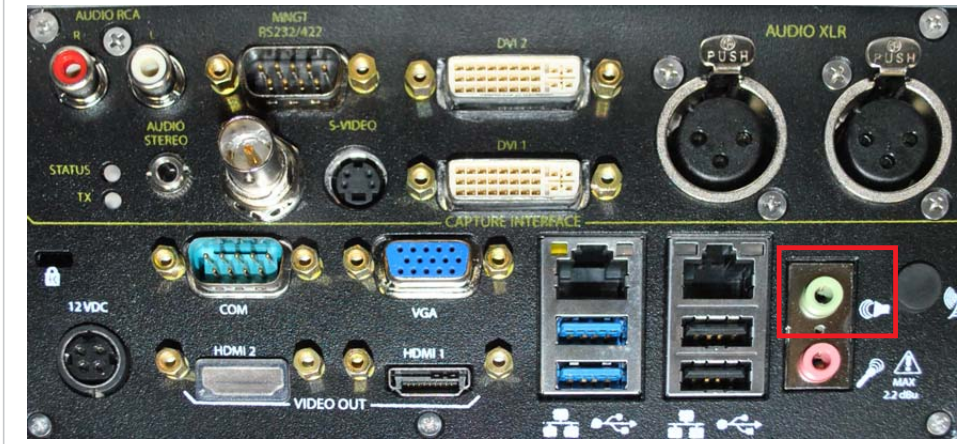
Figure 2-6 Video Output Connections

NOTE Video cannot be output on both ports simultaneously.

To set up Audio Talkback or Audio Preview:

1. (Optional) To set up Audio Talkback or Audio Preview, connect the green Audio Output connector to a speaker.

Figure 2-7 Video Output Connections



Powering Up the Viper

To power up the Viper:

1. Connect the power cable to the Viper chassis (insert arrow side up).

Figure 2-8 Power Connection (Rear view)

2. Plug the other end of the power cable into a grounded electrical outlet or a separate power source such as an uninterrupted power supply (UPS) or a power distribution unit (PDU).
3. Press the Power button on the front of the appliance.

Figure 2-9 Power Switch (Front panel)

The Power indicator LED should light and you will see the boot progress bar.

PART II: Administration

CHAPTER 3: Initial System Setup - Managing Users

This chapter describes how to access the Administrative Tools portal and get started setting up and managing Viper using the Admin module.

NOTE The procedures described in this chapter assume that you have administrative privileges.

For information on the system interfaces that InStream users see, please refer to the InStream User's Guide.

Topics In This Chapter

Accessing the Administration Tools Portal 31
Creating and Managing Users and Groups 34
- Default Usernames 34
- Signing in to the Admin module 35
- Configuring Users 37
- Configuring Groups 40

Configuring Permissions for Groups or Users 43
- Configuring Group Permissions 43
- Configuring User Permissions 47
- Setting a User's PIN 48
- Hotmarks Entitlements 46
- Configuring Guest Permissions 49
- Configuring Touch Panel Guest Mode Permissions 51
- Using Command Line Arguments to Manage Launch Preferences 52

Configuring LDAP Settings 54
- LDAP Configuration Settings 57

Using Conditional Access for User Authentication 60
- Channel Entitlements 62
- Asset Entitlements 63
- Keyword-based Entitlements 64

Managing Device Entitlements 65

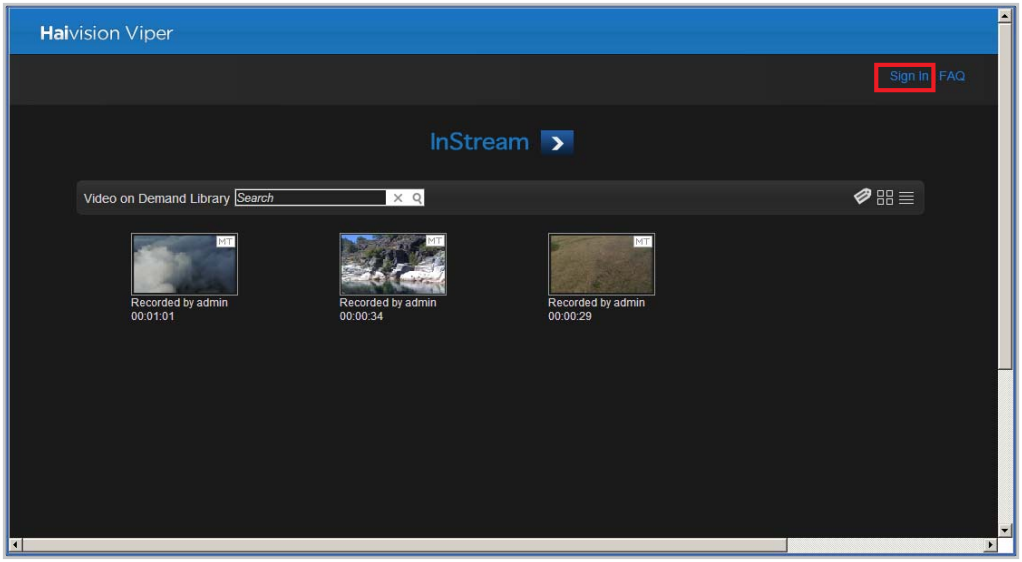
Managing API Credentials 67
Creating a Credential 67
Associating the Credential With Viper Groups 68
Viewing the Consumer Key and Secret pair 69

Accessing the Administration Tools Portal

To access the Administration Tools portal:

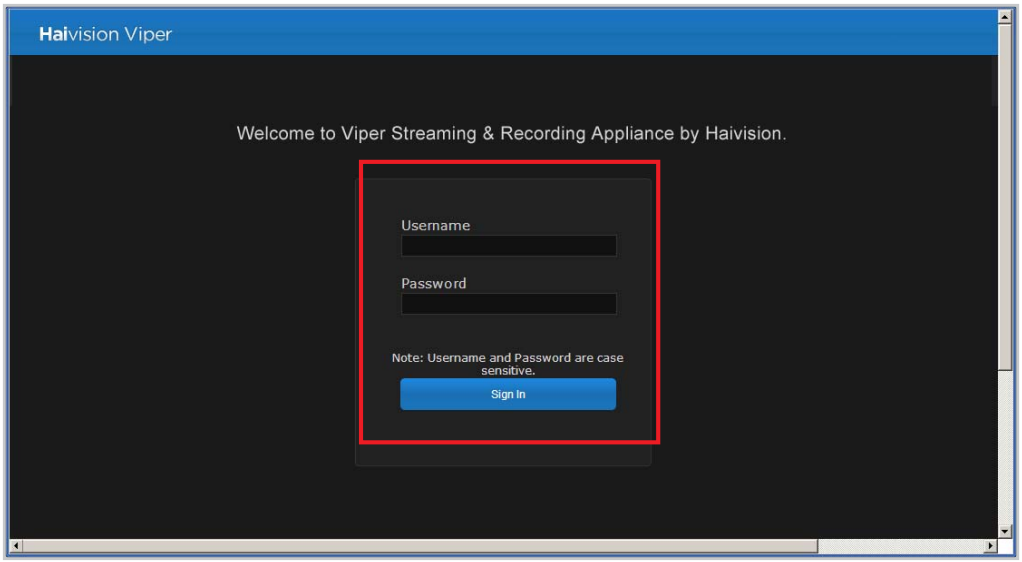
1. Launch a Java-enabled Web browser of your choice (such as Internet Explorer, Firefox, Chrome, or Safari).
2. Type the URL or IP address for the Viper in the browser's address bar and press ENTER.

   The Viper Launch portal appears, listing the available video assets for your system, as shown in the following example.



3. Click Sign In from the navigation bar.
4. If you see a Security Certificate warning, click Proceed anyway (or equivalent) to accept the certificate and continue to the Login page.

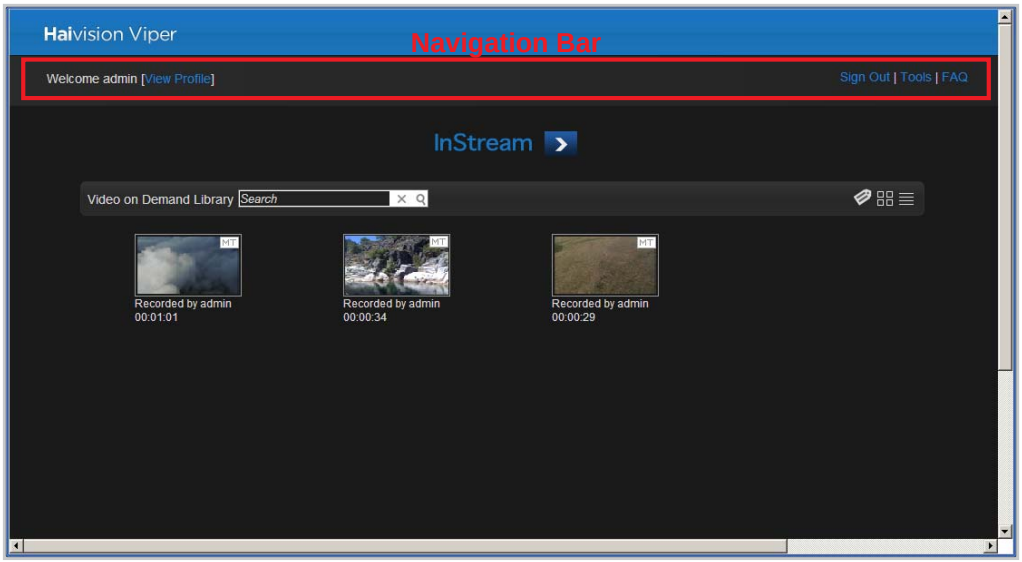
5. On the Sign In page, sign in with the username and password supplied by Haivision. Then press ENTER or click Sign In.



NOTE If the Sign In page does not appear, verify the address of your server and make necessary corrections to the address you are entering in your Web browser.

Also check to make sure that the Viper network configuration, as provided on your site survey at the time of purchase, is compatible with your current network settings.

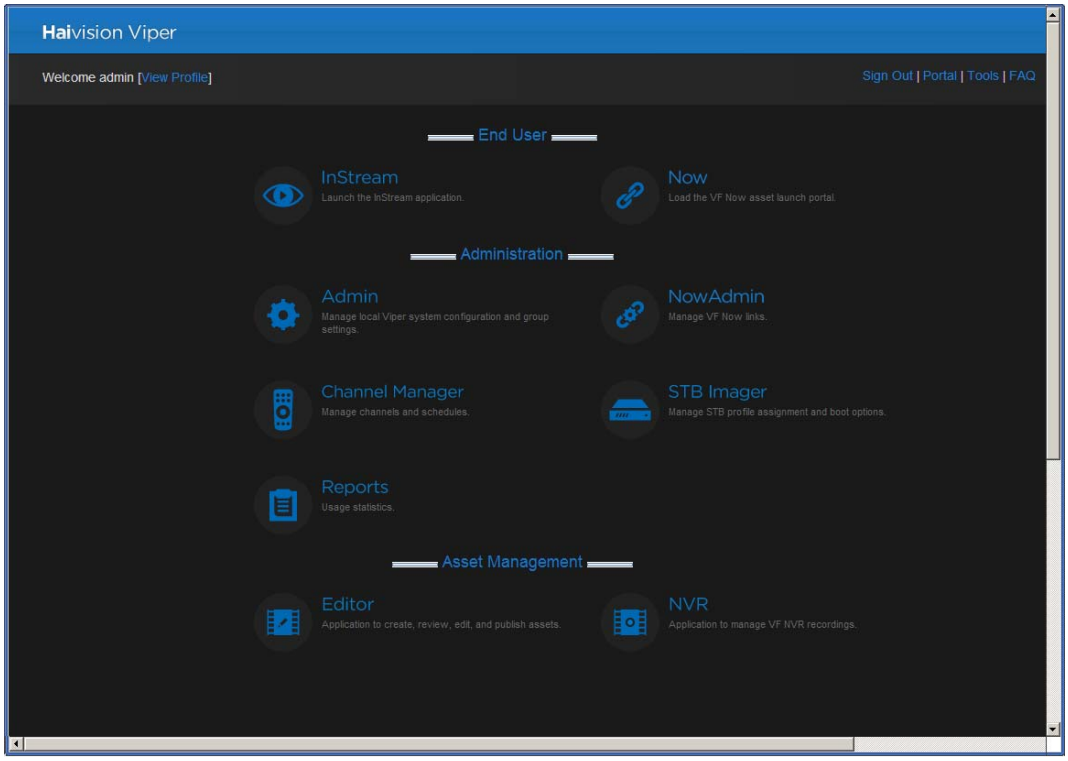
Once you have successfully signed in, the Launch portal re-appears with your account information and the Tools button added to the navigation bar (sample shown in the following example).



6. Click Tools.

Next you will see the Tools page (shown in the example on the following page). This is the central administration portal page used to administer the Viper system.

When the Tools page appears, the Viper system is ready for administrative access.



NOTE The Tools page is intended for administrators and authorized site personnel only. End users should be directed to the Launch portal for viewing purposes.

The Web browser must be Java enabled in order to launch Viper player clients. You can find the latest java plug-in at http://www.java.com.

Creating and Managing Users and Groups

The Admin module is used by system administrators for a range of Authentication, General, and Service Configuration tasks. The initial setup tasks for Authentication depend on whether or not the system uses the Conditional Access module.

The Conditional Access module provides several components to manage user and group settings, including Conditional Access (group or user entitlements to channels and assets), Device Manager (to assign set top boxes to groups), and LDAP Configuration.

NOTE LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to look up information from a server. LDAP directories are used for authentication, permissions, and directory lookups for information such as user name, email, phone number, or address.

If the Conditional Access module has been purchased, you can (optionally) configure Viper to connect to your company or organization's LDAP server to store and streamline the retrieval of user permissions and login credentials.

With Conditional Access, you can also use the Device Manager to add and remove devices from groups. (The entitlements are still managed through the Conditional Access tool.)

If you do not have Conditional Access – or if you have Conditional Access but are not using LDAP or Active Directory – you can use the Admin module to directly manage users and groups.

Default Usernames

The default admin username/password is haiadmin/manager. haiadmin is a special system user intended primarily for initial setup purposes. It is not intended for permanent use and has a limited permission set that cannot be changed. For access to all Viper features, create a regular (administrative) user with a secure password.

As a security measure, be sure to change the default password for the haiadmin account.

Please note that your admin credentials may have been set differently if requested. In this case, please contact Haivision Technical Support to retrieve this information.

In addition, the Viper provides the following default usernames and passwords. These are intended to serve as examples showing typical levels of authentication based on Viper workflows. Each one also includes a default PIN for the Touch Panel interface:

- Username: admin
  Password: admin
  PIN: 9999
- Username: creator
  Password: creator
  PIN: 1111

- Username: consumer
  Password: consumer
  PIN: 2222

When you sign in to the Admin module using the haiadmin account, you can view the permissions defined for each of these accounts.

Signing in to the Admin module

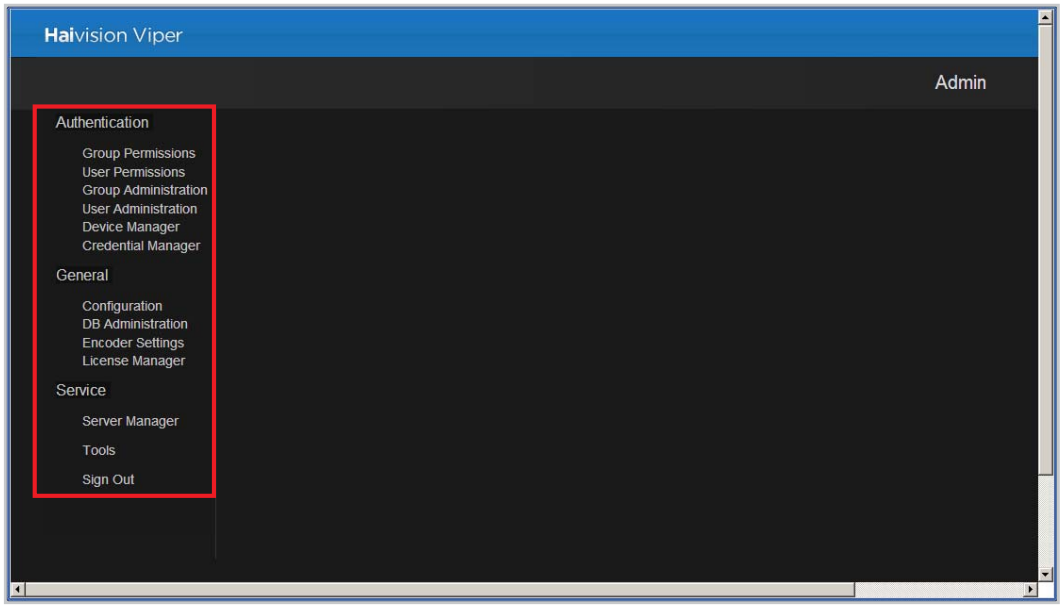
To start using the Admin module:

1. Open the Web browser of your choice and browse to the IP Address provided on your System Details sheet.

NOTE If you haven't changed the factory presets, and if not specified elsewhere in the shipment, the Viper's IP Address on port Eth0 is set by default to: 10.5.1.2. For information on the Viper's default network settings, see "Connecting the Viper to the Network" on page 19.

2. On the Launch portal, click Sign In from the navigation bar.
3. Sign in with the default admin username and password: haiadmin/manager.

The Admin Welcome page appears, with links to the Authentication, General, and Service Configuration sections on the left side of the page.



The available Authentication links depend on your system and the permissions assigned to your account. Following are three typical setups:

- Conditional Access, but *not* connected to LDAP server: All Authentication links are available: LDAP Configuration, Conditional Access, Group Permissions, User Permissions, Group Administration, User Administration, and Device Manager.
- Conditional Access and connected to LDAP server: Group Administration and User Administration links are no longer available since the Viper is now connected to the LDAP user list.
- No Conditional Access: Group Administration and User Administration links are available to manage user and group settings. The LDAP Configuration and Conditional Access links are not available.

The following sections describe how to use the Admin module to directly manage user and group settings.

TIP To configure your system to use an LDAP service, see "Configuring LDAP Settings" on page 54.

Configuring Users

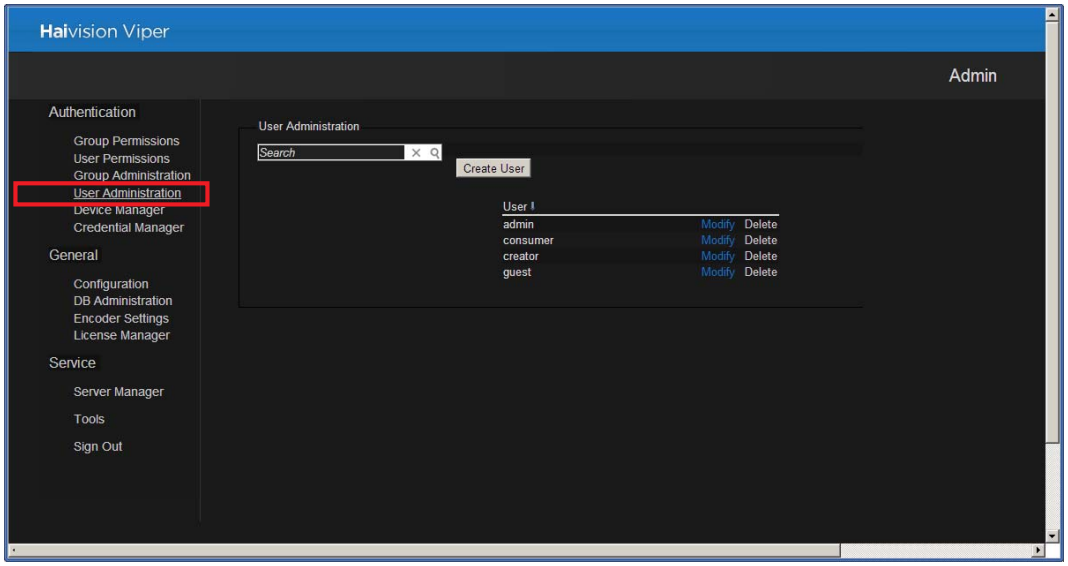
The Admin User Administration module allows you to create and manage the users for your system.

NOTE That this module is only available if you have *not* configured the Viper to connect to an LDAP server.

To configure user accounts:

1. Click the User Administration link on the left side of the Admin page.

   The User Administration page opens (shown in the following example) displaying the current list of users for your system.



   From here you can browse through the list, search for users, add and delete users, and modify existing user accounts. This includes modifying user information, enabling or disabling accounts, and changing passwords.

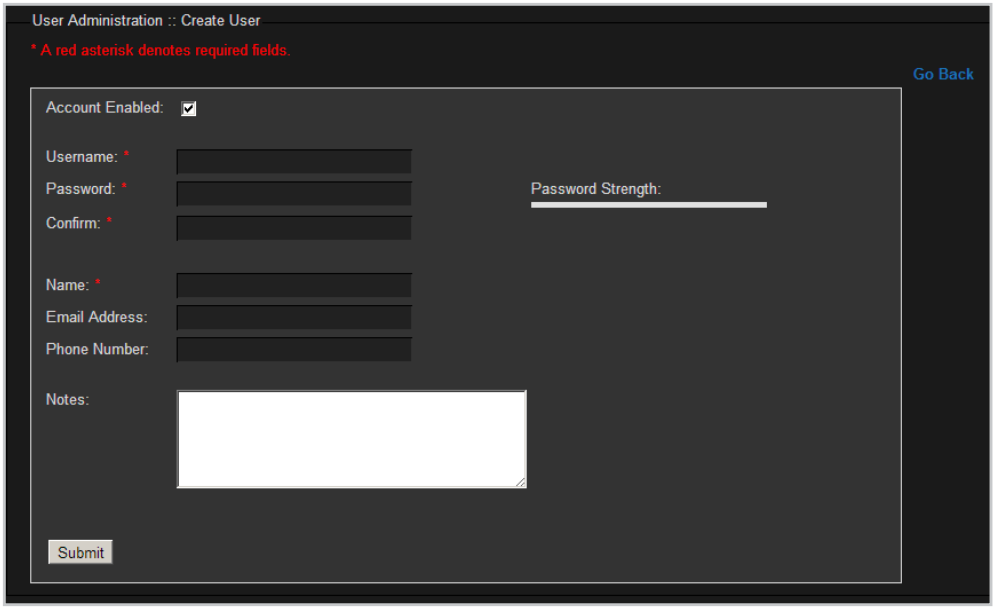
2. To search for a user, type the name or part of the name in the Search field and click .

   This will filter the list to show only users whose names contain the search text.

TIP You can also change the sort order of the list by clicking User↓.

3. To clear your search, click ✕.

4. To add a user, click Create User.
5. On the Create User page (shown below), fill in the fields to set up the new user account.



a. To enable or disable this user account, check or uncheck the Account Enabled checkbox.

b. Type in the Username and Password. (Both the username and password are case sensitive.)

   User passwords require a minimum length of 6 characters (uppercase/lowercase letters, numbers, punctuation and symbols), with no maximum length. The Admin module prompts you to improve the password security as you type in characters.

NOTE Viper user password requirements differ depending on whether they are admins or non-admins. Viper admins can set a password to something less secure than regular users can (i.e., minimum one character).

c. Type in any descriptive information to identify this user such as the full name, email address, phone number, and notes. (The user name will be modified accordingly on the navigation bar.)

d. Click Submit to save the changes.

You will be returned to the User Administration page, and the name will be added to the User list.

TIP You can either assign Group Permissions to this user, by adding the user to a group (see "Configuring Groups": Step #8 on page 41), or you can define the permissions for the user (see "Configuring User Permissions" on page 47).

6. To modify user information, including enabling or disabling the account or changing the password, click Modify next to the user name.

   The Modify User page displays the basic user information and lists any groups to which the user has been assigned.

7. Enter your modifications and click Submit to save the changes.

8. To remove a user, on the User Administration page, click Delete next to the user name. This permanently deletes the user from the system.

Your changes take effect immediately. When you have completed all sections, you can either navigate to another module or click Sign Out to exit the Admin module.

Configuring Groups

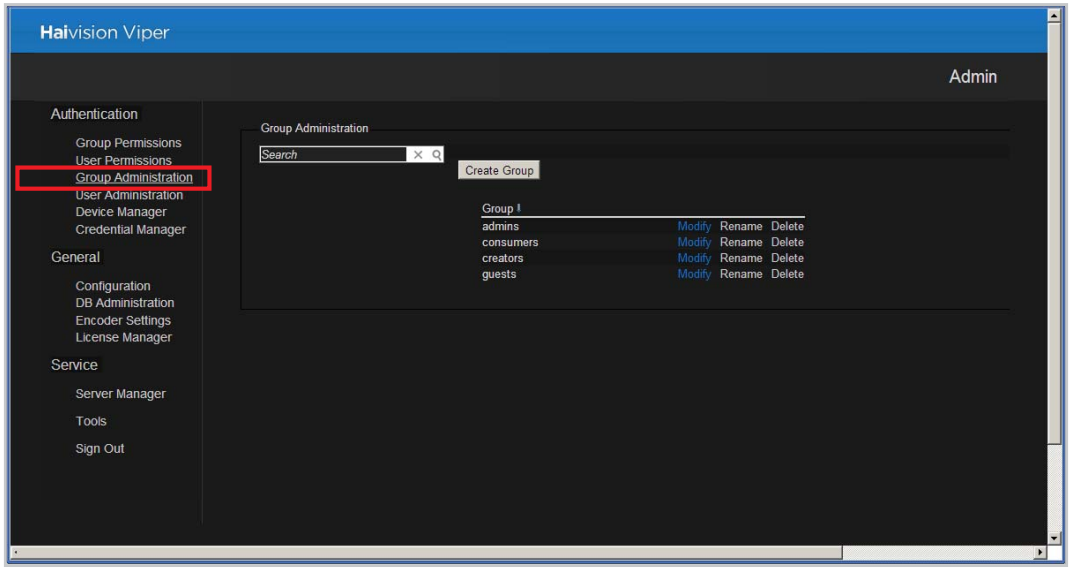
The Admin Group Administration module allows you to create and manage the user groups for your system. (Note that this module is only available if you have *not* configured the Viper to connect to an LDAP server.)

NOTE Groups may also be used to assign viewing entitlements to set top boxes (STBs). This requires the Device Manager, which is included in the Conditional Access module.

To configure user groups:

1. Click the Group Administration link on the left side of the Admin page.

   The Group Administration page opens (shown in the following example) displaying the current list of groups defined for your system.



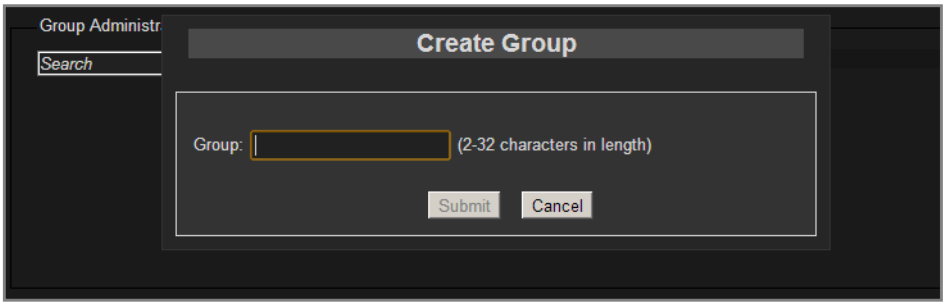
   From here you can browse through the list, search for groups, create new groups, and modify existing groups. This includes renaming groups, deleting groups, as well as adding and removing users to/from the group.

2. To search for a group, type the name or part of the name in the Search field and click .

   This will filter the list to show only groups whose names contain the search text.

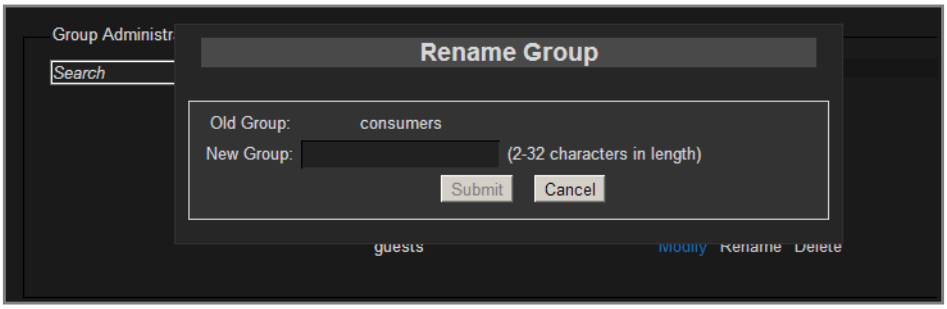
TIP You can also change the sort order of the list by clicking Group↓.

3. To clear your search, click ✕.
4. To create a new group, click Create Group.
5. On the Create Group popup (shown below), type the new group name into the text box and click Submit.



The name will be added to the Group list.

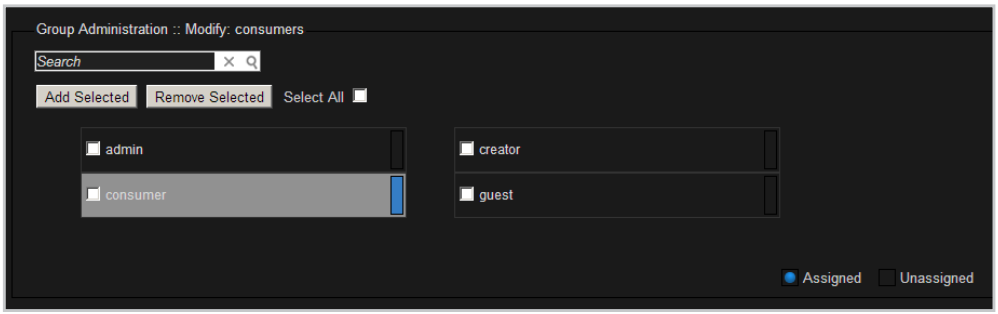
6. To rename a group, on the Group Administration page, click Rename next to the group name.
7. On the Rename Group popup (shown below), type the new group name into the text box and click Submit.



The name will be modified on the Group list.

8. To add and remove users from the group, click Modify next to the group name.

The Modify Group page opens (shown in the following example) displaying the current list of available users for your system. Users that are part of the group are highlighted in blue.



a. To add users to the group, check the names of the users and click Add Selected.

b. To remove users from the group, check the names of the users and click Remove Selected.

TIP You can check the Select All checkbox and then click Add Selected or Remove Selected to either add all names to or delete all names from the group. You can also use the CTRL or SHIFT keys to select multiple names.

To return to the Group Administration page, click the Group Administration link on the left side of the page.

9. To remove a group, on the Group Administration page, click Delete next to the group name.

Your changes take effect immediately. When you have completed all sections, you can either navigate to another module or click Sign Out to exit the Admin module.

Configuring Permissions for Groups or Users

The Admin module provides two complementary methods for defining user access permissions and entitlements. You can either:

- Define Group Permissions and then add users to groups, or
- Define User Permissions on a per user basis.

In either case, "permissions" include user account permissions, access to Viper applications such as InStream, administrative permissions for specific tools and clients, as well as assigning command line arguments to specify InStream launch preferences. You can also define the Hotmarks that will be available for the group or user on the Touch Panel interface.

The two methods are not mutually exclusive and can be used in any combination for entitlement.

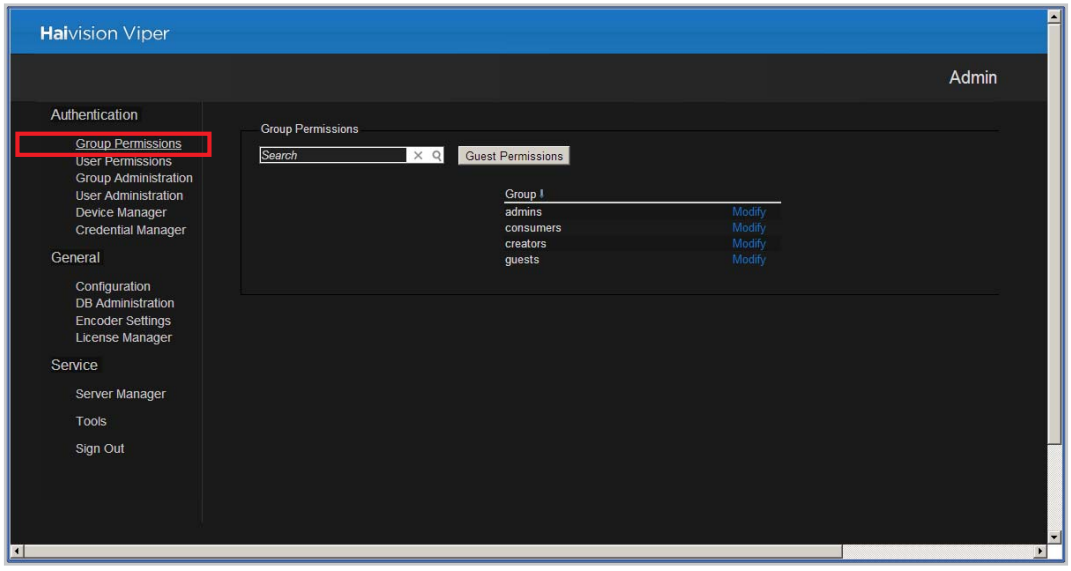
NOTE Permissions are additive, meaning that a user can perform all actions granted to any of their assigned roles.

Configuring Group Permissions

To configure group permissions:

1. Click the Group Permissions link on the left side of the Admin page.

   The Group Permissions page opens (shown in the following example) displaying the current list of groups defined for your system.



From here you can browse through the list, search for groups, and modify the administrative privileges and user permissions for groups. You may also define the "Guest" Permissions for the system, which will apply to unauthenticated users (i.e., users who are not signed in). See "Configuring Guest Permissions" on page 49.

2. To search for a group, type the name or part of the name in the Search field and click .

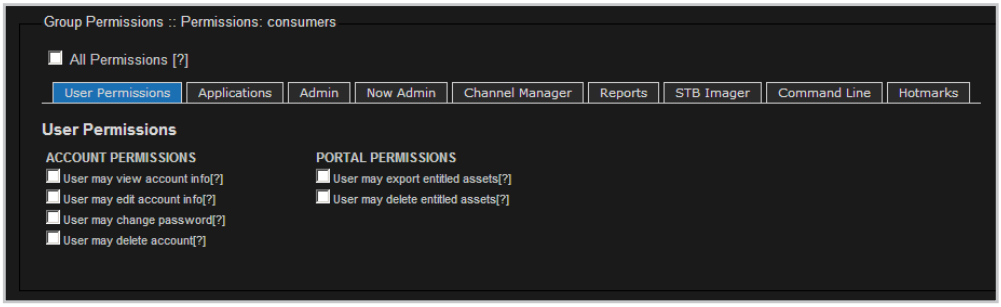
   This will filter the list to show only groups whose names contain the search text.

TIP You can also change the sort order of the list by clicking Group↓.

3. To clear your search, click .

4. To modify administrative privileges and/or user permissions for a group, click Modify next to the group name.

   The Modify Group Permissions page opens (example below, showing User Permissions tab).

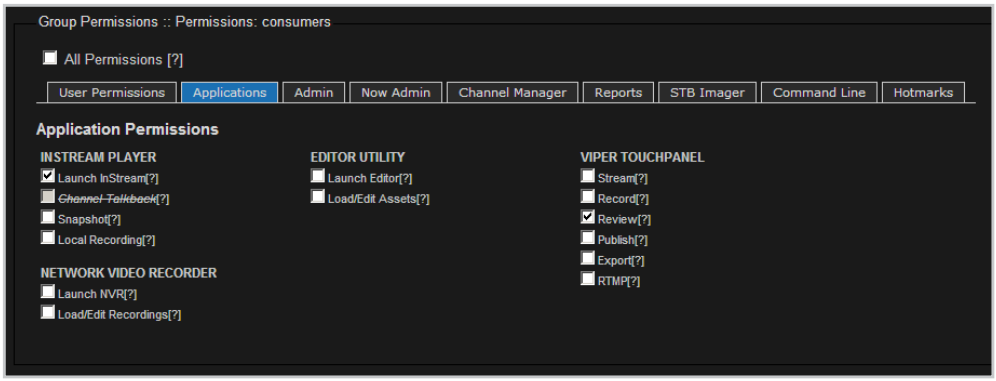


   The Modify Group Permissions page provides tabbed sections to define user permissions and access to Viper applications. From here, you can configure access to the tools that this group will need.

TIP To give the group "administrative" permissions, i.e., access to all Viper applications and Web tools, as well as full control over user and system administration, check the All Permissions checkbox.

5. For each tabbed section, check all boxes that apply to define the group privileges and user permissions. For example:

   - To give the group access to the VF Editor tool and allow group members to load and edit assets, click the Applications tab (shown below). Then under EDITOR UTILITY, check the Launch Editor and Load/Edit Assets checkboxes.



   - To give the group access to the InStream player, on the Applications tab under INSTREAM PLAYER, check the Launch InStream checkbox.
   - To give the group access to the Viper Touch Panel interface, on the Applications tab under VIPER TOUCHPANEL, check the appropriate checkbox(es): Stream, Record, Review, and/or Publish.

TIP When a Viper is joined to a realm, the authentication is made against the database.

Your changes take effect immediately. When you have completed all sections, you can either navigate to another module or click Sign Out to exit the Admin module.

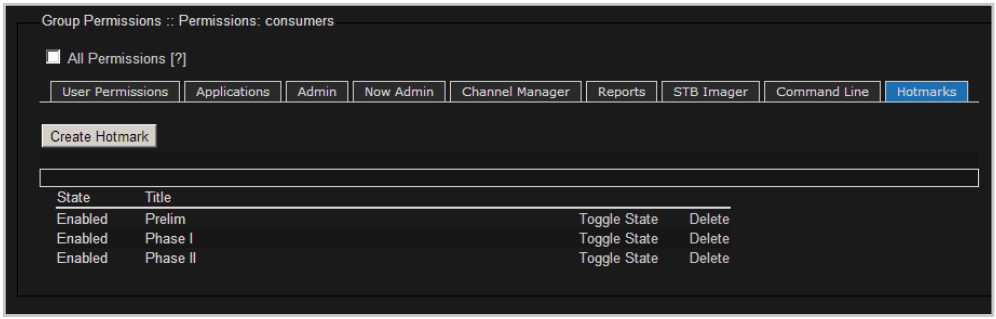
Hotmarks Entitlements

You can define the Hotmarks available for the group or user (on the Touch Panel interface).

To define the available Hotmarks:

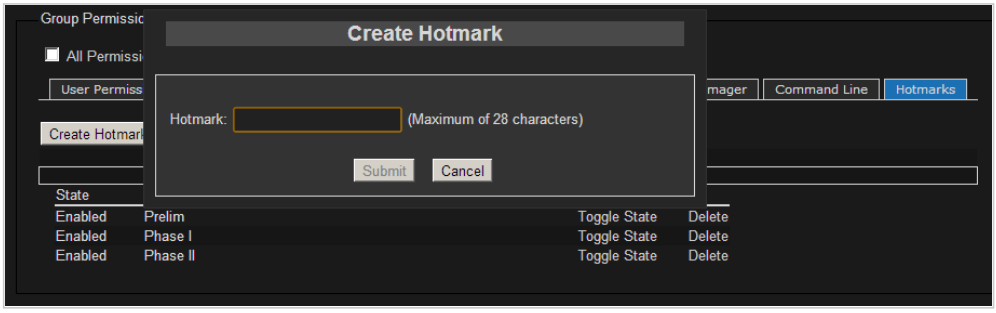
1. Click the Hotmarks tab.

   The Hotmarks tab (shown below) displays the current list of available Viper Hotmarks for your system.



2. To create a Hotmark, click Create Hotmark.

3. On the Create Hotmark popup (shown below), type the new Hotmark name (up to 28 characters) into the text box and click Submit.



4. Repeat as necessary for all Hotmarks (a maximum of 14 “live” Hotmarks may be available at a time in the Touch Panel interface).

   The new Hotmarks are added to the list and will be available when this group or user accesses the Viper Touch Panel interface.

5. To enable and/or disable a Hotmark, click Toggle State in the row containing the Hotmark.

   This allows you to define a repository of Hotmarks and then enable or disable them for particular situations.

6. To remove a Hotmark from the group’s authorized resources, click Delete in the row containing the Hotmark to delete.

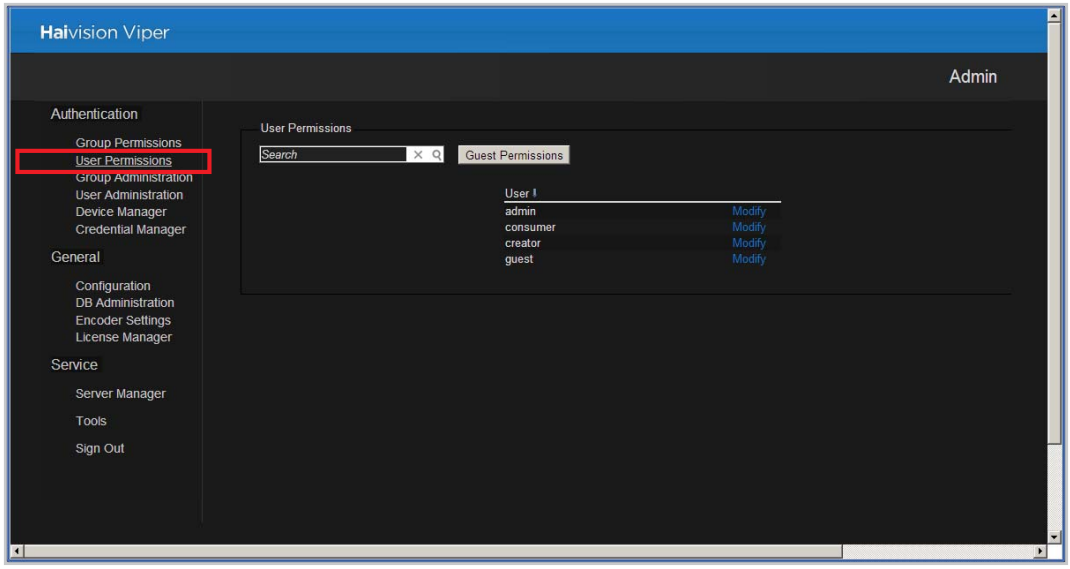
Configuring User Permissions

User-based permissions allow you to set access to Viper features on a user-by-user basis. The selections for user-based permissions are the same as those for group-based permissions. You can also set the user's PIN from the User Permissions page.

To configure user permissions:

1. Click the User Permissions link on the left side of the Admin page.

   The User Permissions page opens (shown in the following example) displaying the current list of users defined for your system.



   From here you can browse through the list, search for users, and modify the administrative privileges and user permissions for individual users. You may also define the "Guest" Permissions for the system, which will apply to unauthenticated users (i.e., users who are not signed in). See "Configuring Guest Permissions" on page 49.

   For details on modifying administrative privileges and/or user permissions, see "Configuring Permissions for Groups or Users" on page 43.

Setting a User's PIN

When configuring user permissions, you can also assign a 4 to 12 digit PIN (Personal Identification Number) which can be used to authenticate the user to the Touch Panel interface.

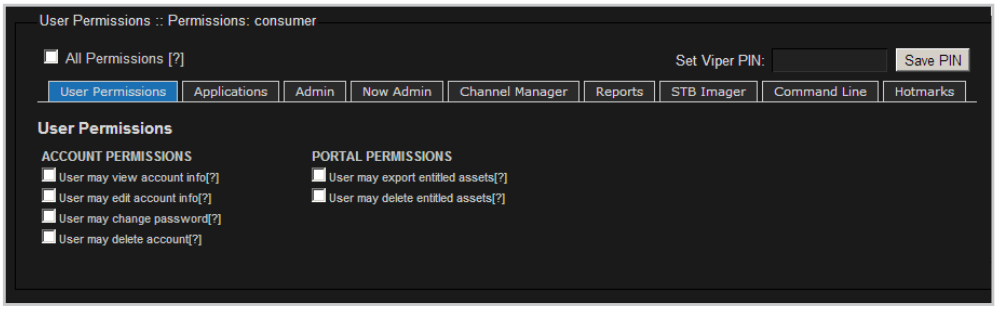
NOTE When setting up the Viper, you need to select the Authentication Mode for the Touch Panel. You can choose between PIN and Password (which requires users to enter a PIN followed by their username and password to gain access) or PIN only (which allows users to gain access simply by entering their PIN). For details, see "General Configuration" on page 71.

PINs are only stored on the Viper. This means that if the Viper is joined to a Furnace realm, then any valid Viper PIN will unlock the Touch Panel and take the user to the Username/Password screen. At that point the user must enter a valid Furnace username and password.

To set a user's PIN:

1. On the User Permissions page, click Modify next to the user name.

   The Modify User Permissions page opens (example below).



2. Type the new PIN in the Save Viper PIN text box.
3. Click Save PIN.

   If the PIN is already in use, the system will prompt you with a Failed assignment message, and you will need to enter a different PIN.

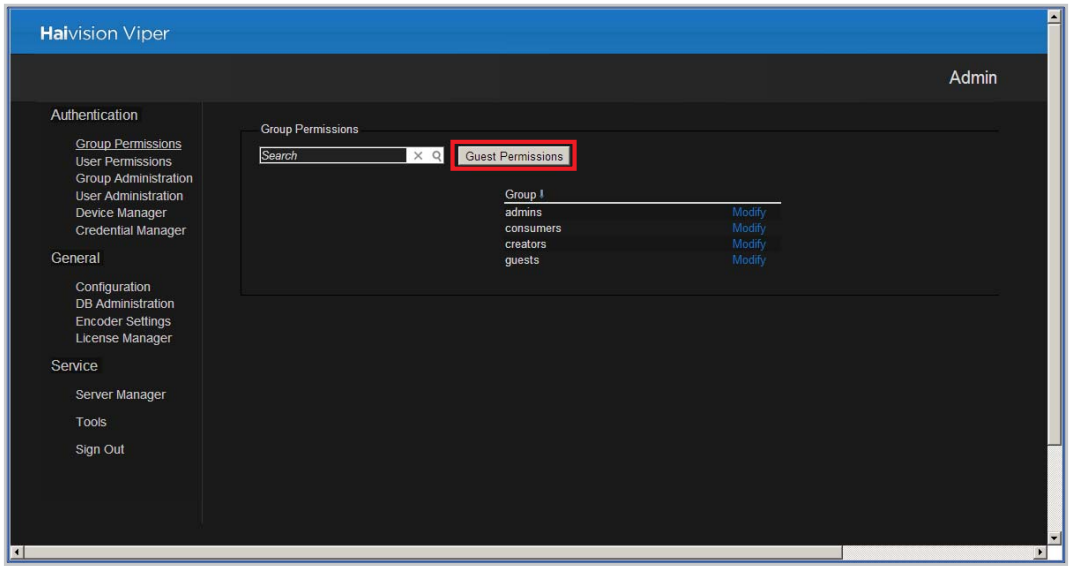
Configuring Guest Permissions

You can also define Guest Permissions for your system. Guest Permissions are used when a user has not signed in. For example, you may choose to allow visitors to the Viper portal to launch the InStream player and view the contents of the VoD page, without requiring them to sign in. The Guest permissions apply to these users.

IMPORTANT Guest permissions are not “default” permissions. Authenticated users (i.e., users who have signed in) will only get the permissions assigned to their account (based on the group or groups to which they are assigned). Guest permissions are never assigned to users who are signed in.

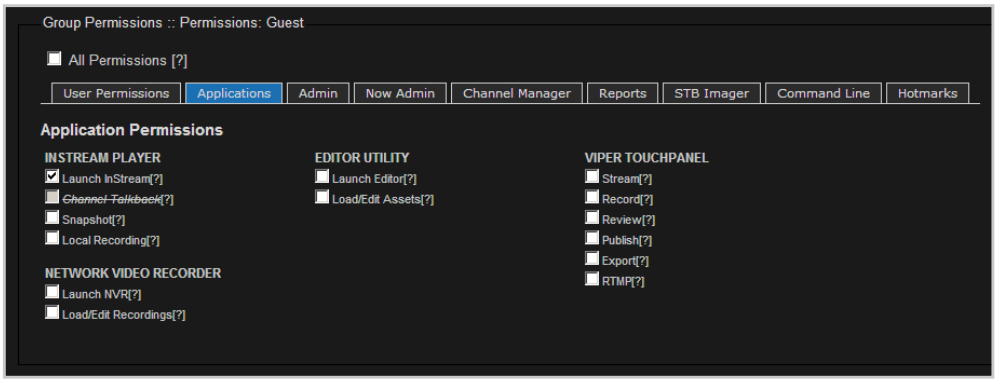
To define Guest Permissions:

1. On either the Group Permissions or User Permissions page, click Guest Permissions.



2. On the Guest Permissions page, click the Applications tab.

   The Applications tab opens (shown below).



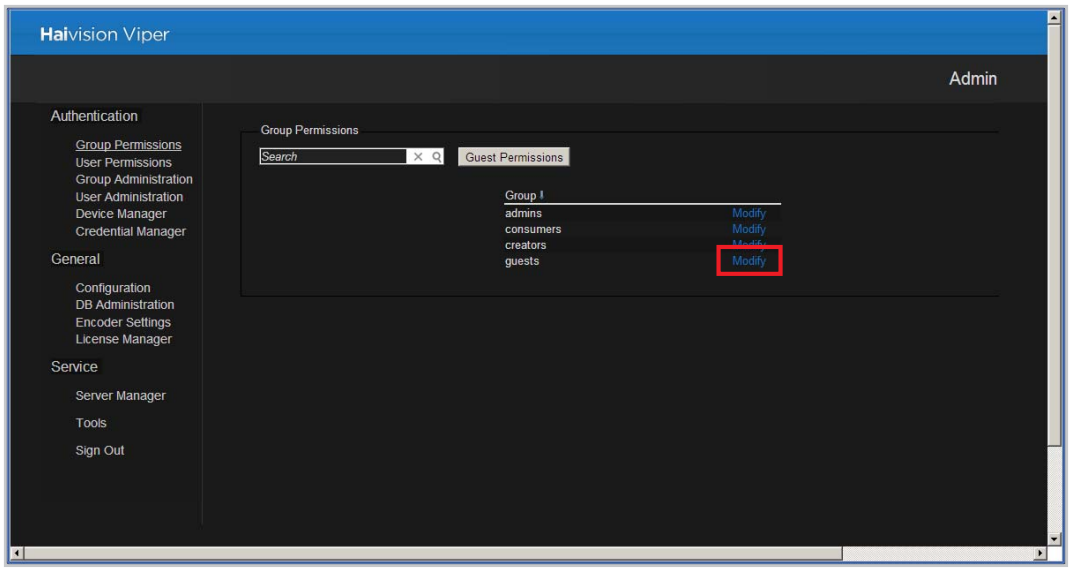
3. For each tabbed section, check all boxes that apply to define the privileges and user permissions for guest users. For more information, see "Configuring Permissions for Groups or Users" on page 43.

Configuring Touch Panel Guest Mode Permissions

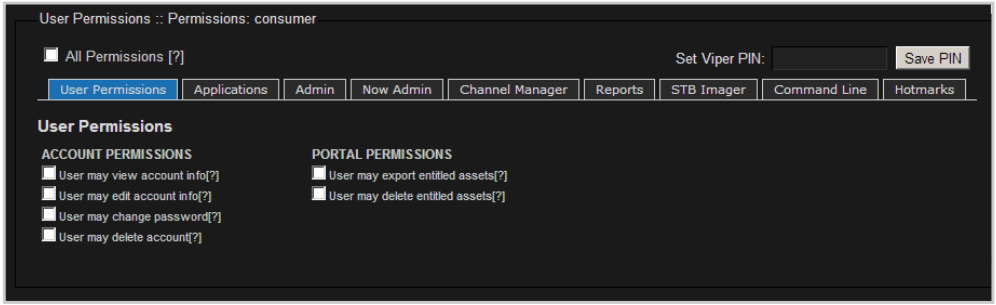
Viper also provides a Guest mode to allow users and groups quick access to the Viper Touch Panel interface. When secure access is not required, Guest mode can be enabled from the Touch Panel Info Screen. This allows users to simply "Touch Anywhere To Begin" on the Touch Panel Welcome screen without entering a PIN or password. Guest mode functionality is limited to the permissions defined for the Guest profile (see following).

To define Touch Panel Guest Mode Permissions:

1. On either the Group Permissions or User Permissions page, click Modify next to the Guest group or user name.



The Modify User or Group Permissions page opens (example below).



2. For each tabbed section, check all boxes that apply to define the privileges and user permissions for Touch Panel Guest Mode. For more information, see "Configuring Permissions for Groups or Users" on page 43.

When you have completed all sections, you can either navigate to another module or click Sign Out to exit the Admin module.

Using Command Line Arguments to Manage Launch Preferences

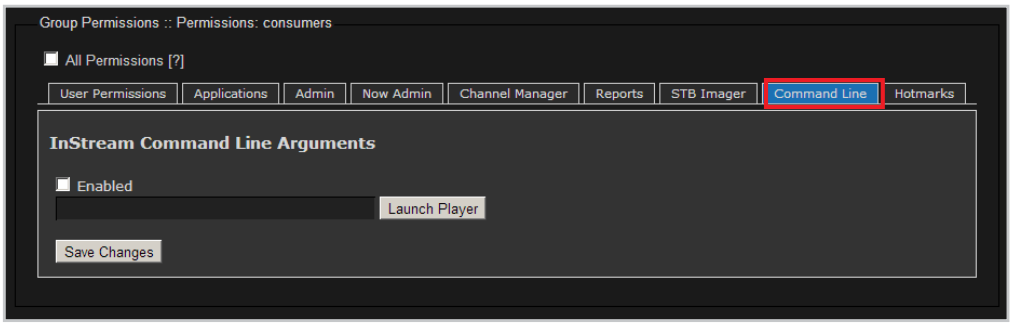
You can also assign command line arguments (CLAs) to specify InStream launch preferences and other behaviors. For example, the system can be configured to hide the player window upon startup, mute the audio, or disable loading of existing preferences and saving of preferences on exit.

For a list of InStream launch preferences that may be managed via command line arguments, see Appendix C: “Command Line Arguments”.

NOTE CLAs are only applied when InStream is launched from the main portal page (example shown on in “Accessing the Administration Tools Portal” on page 31). They do not apply with launching VOD assets from the portal, or launching InStream from the Tools page.

To define InStream launch preferences using command line arguments:

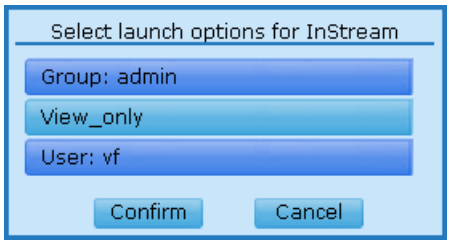
1. On either the Group Permissions or User Permissions page, click Modify next to the group or user name to assign the preference(s).
2. On the Modify Group/User Permissions page, click the Command Line tab.



3. Type in the command line argument(s) and values (using spaces to separate multiple arguments, if required) for each application.

   Refer to the list of command line arguments in Appendix C:.
4. Check the Enabled checkbox.
5. Click Launch Player to test the display.
6. Click Save Changes to save these preferences.

IMPORTANT Users may be assigned to more than one group, which may have conflicting launch preferences assigned using command line arguments. In this case, when such a user tries to launch the player, the Viper will provide an option dialog prompting the user to select which launch options to use (shown in the following example).



Configuring LDAP Settings

NOTE LDAP Configuration is an option, which is included in the Conditional Access module, and must be purchased separately.

If you are not using an LDAP service, see "Creating and Managing Users and Groups" on page 34.

If your company or organization uses an LDAP server, you can configure the Viper to access this server. This will allow you to take advantage of your existing LDAP directory for access control, account management, and user authentication.

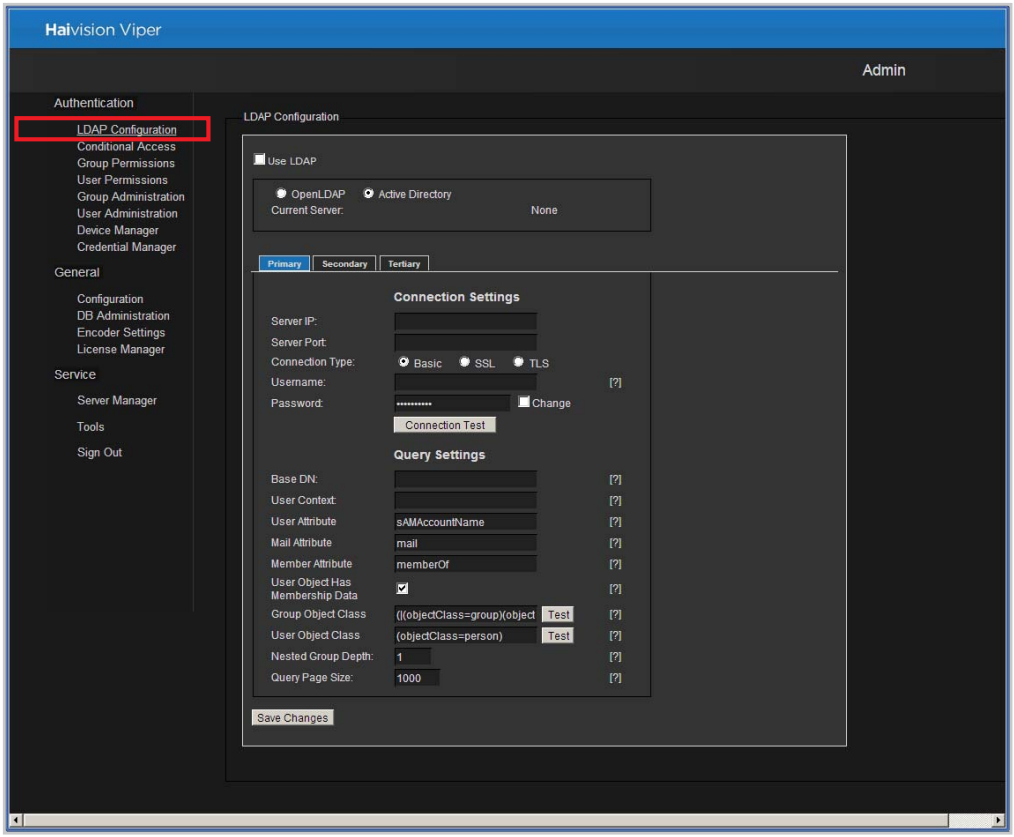
From the LDAP Configuration page, you can configure up to three LDAP servers: typically, a Primary server with optional Secondary and Tertiary backups. The system provides automatic failover switching; you may also manually switch the current server.

You may also define and save LDAP server settings for future use without enabling LDAP.

To configure LDAP settings:

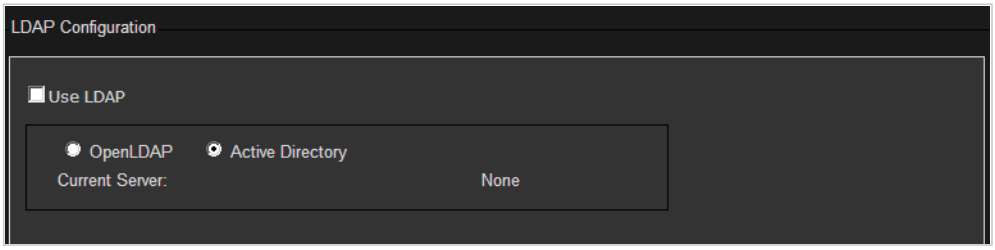
1. Click the LDAP Configuration link on the left side of the Admin page.

   The LDAP Configuration page opens (shown in the following figure).



The LDAP Configuration page displays the panes for configuring multiple LDAP servers (Primary, Secondary, and Tertiary). It also provides a button to test a connection to the defined LDAP server.

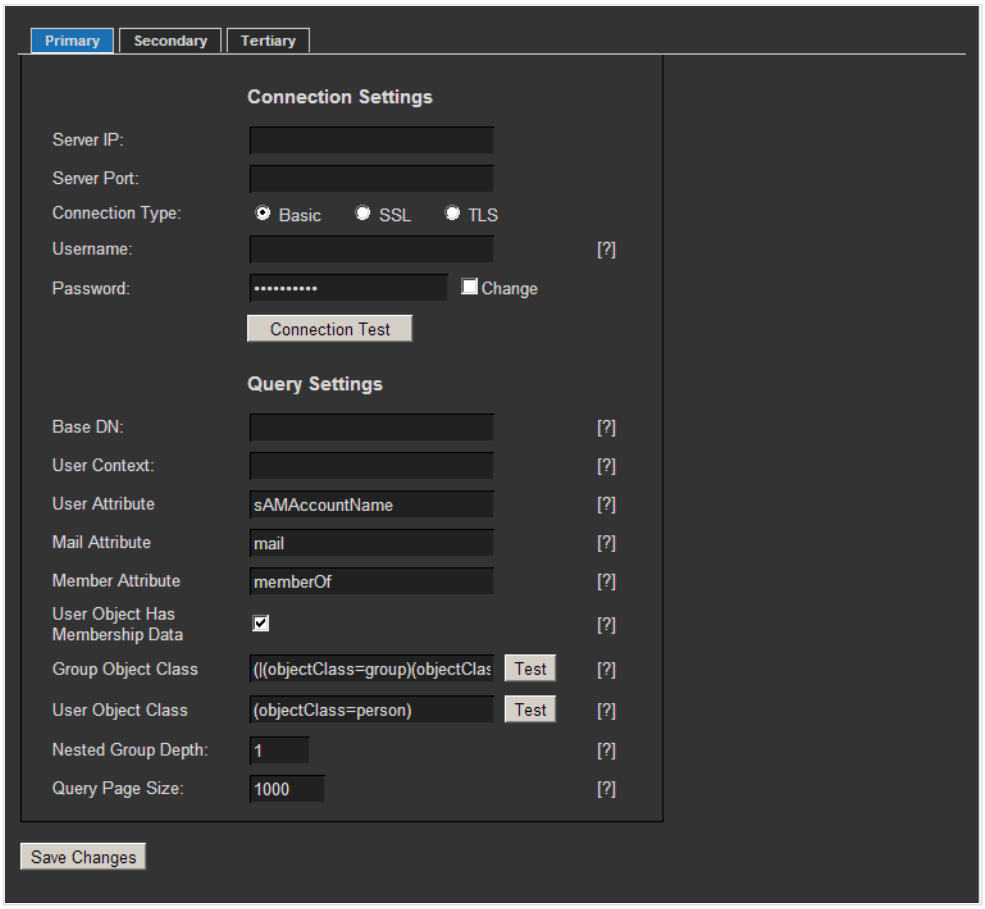
2. To configure the Viper to use your LDAP service, check the Use LDAP checkbox.



3. Select the type of LDAP implementation for your system, either:

- Open LDAP: An open source implementation of LDAP directory services.
- Active Directory: An implementation of LDAP directory services by Microsoft.

4. To configure either a Secondary or Tertiary backup system, click the associated tab. (The default is Primary.)



5. Fill in the fields to configure the server connection. See the following section "LDAP Configuration Settings".

6. (Optional) To configure another backup server (i.e., Secondary or Tertiary), repeat Steps #4 and #5.

7. (Optional) To switch the active server, click either Primary, Secondary or Tertiary. Then click Continue to confirm the change.

8. Click Save Changes to save the LDAP settings.

IMPORTANT When LDAP is engaged, the Viper server no longer recognizes any users or groups defined while LDAP was not enabled. This means that when you configure the Viper to use LDAP, you will need to sign in again using an LDAP user

account (unless you are using haiadmin, which does not get “kicked out” when the LDAP settings change). The list of valid PINs will change when the LDAP setting is toggled. However, the Viper Touch Panel session remains active.

When you configure the Viper to use LDAP, you must still assign permissions to your groups or users. See “Configuring Permissions for Groups or Users” on page 43.

LDAP Configuration Settings

The following table lists the LDAP Configuration Settings.

LDAP Field	Description
Connection Settings	
Server IP	The IP address or domain name of the server that hosts the LDAP server.
Server Port	The communications port that the LDAP service uses. The default value is 389 (the standard port used for LDAP connections), or 636 for SSL connections.
Connection Type	Select the encryption protocol: • Basic: Unencrypted connection • SSL: Secure Socket Layer (recommended) • TLS: Transport Layer Security
Username	The username for Viper to connect to your LDAP system and query it for the required information. The user account needs to have permission to connect to the server and read the information in the LDAP directory.
Password	The password that corresponds with the user name provided for the Username field. To change the password, check the Change checkbox and then type in the new password. NOTE: You must check the checkbox in order to change the password. This allows you to update other information on the page without re-entering the password.
Connection Test	Click to test the connection from Viper to your LDAP system. If the test is successful, click Save Changes. NOTE: If you get the message “Anonymous Connection Succeeded,” this means that Viper has found the server, but the Username and/or Password is most likely wrong. IMPORTANT: If you get the message “Connection Test Succeeded,” this means that the Server IP, Server Port, Username and Password are correct.

LDAP Field (Cont.)	Description (Cont.)
Query Settings	
Base DN	The Base DN (Distinguished Name) used by your LDAP system. You can think of this as where (i.e., the folder) in the file system (i.e., the domain tree) you have put the files relevant to Viper. For example, ou=Groups,dc=haivision,dc=com NOTE: Spaces are not allowed unless they are part of the path. IMPORTANT: If the Base DN is wrong, Viper will not be able to access the groups. To verify that the Base DN is correct, you must check the available groups on the Group Permissions page.
User Context	The context under which your LDAP users can be found. You can think of this as what to append to the user name to make it work. For example, ou=People,dc=haivision,dc=com NOTE: You may omit the ou portion and specify the dc portion only. IMPORTANT: If the User Context is wrong, users will not be able to log in correctly. For example, they may only have the anonymous privileges or even a blank screen.
User Attribute	The user attribute your directory system uses. OpenLDAP systems normally use “cn” or “uid”, while Active Directory systems normally use “sAMAccountName”.
Mail Attribute	The mail attribute your directory system uses. OpenLDAP and Active Directory systems normally use “mail”.
Member Attribute	The member attribute your directory system uses. OpenLDAP systems normally use “member” or “memberUid”, while Active Directory systems normally use “memberOf”.
User Object Has Membership Data (checkbox)	Indicates that your directory system stores group membership data on the user object (memberOf). Check this box if you are using Active Directory or an OpenLDAP extension that supports memberOf.
Group Object Class	Object class query for groups. Default: (|(objectClass=group)(objectClass=groupOfNames)). The default will work with almost all directory servers.
User Object Class	Object class query for users. Default: (objectClass=person). The default will work with almost all directory servers.

LDAP Field (Cont.)	Description (Cont.)
Nested Group Depth	Sets the maximum recursion level for nested group support (i.e., defines the depth of the nesting) for user permissions and entitlements. This should be a low number, or 1 to disable nesting.
Query Page Size	Sets the size of a page for paged results. Paged results are typically supported, but the supported page size may need to be configured for your site. If the requested size is not supported by the LDAP server, a non-paged query will be attempted. The default on most directory servers is 1000.

Using Conditional Access for User Authentication

NOTE Conditional Access is an optional module and must be purchased separately.

If you are not using Conditional Access to manage user and group settings, see "Creating and Managing Users and Groups" on page 34.

The Conditional Access module provides a range of selections you can use to manage conditional access entitlements to the Viper system. For example, you can:

- Assign access to channels and Video on Demand (VoD) assets to specific groups and users. (Groups or users that are not given access to either channels or VoD assets will not be able to view either.)
- Create entitlement rules based on keywords in the asset's Title, Description and Tag metadata.

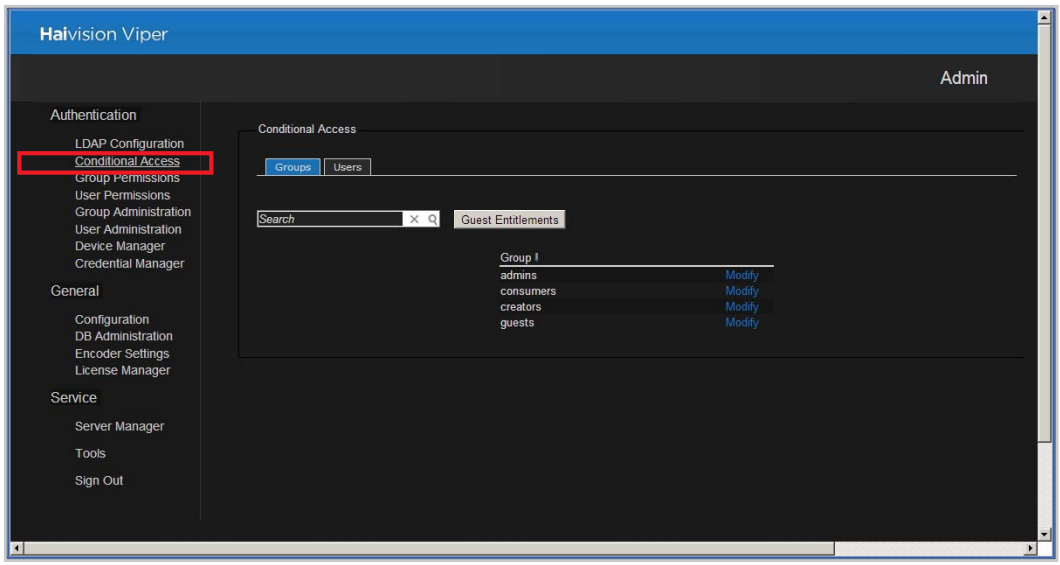
You may also define the "Guest" Entitlements for the system, which will apply to unauthenticated users (i.e., users who are not signed in). The selections for defining Guest entitlements are the same as those for groups and users.

TIP To enable Conditional Access entitlements, you need to select On for Conditional Access Method on the Configuration page. See "General Configuration" on page 71.

To configure Conditional Access Entitlements:

1. Click the Conditional Access link on the left side of the Admin page.

   The Conditional Access page opens (shown in the following example) displaying the current list of groups defined for your system.



The Groups tab is selected by default.

2. First select whether you want to modify the entitlements for a group, or a user, or for guests.

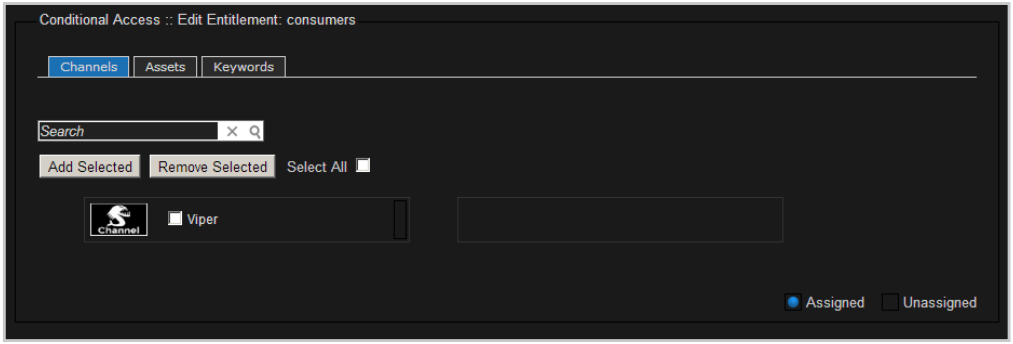
Channel Entitlements

There is only one channel by default in the Viper. By default, the Viper channel is not entitled to any user.

1. To modify the authorized resources:
   a. For a group, click Modify next to the group name.
   b. For a user, first click the Users tab and then click Modify next to the user name.
   c. For Guest entitlements, first click Guest Entitlements.

NOTE The steps that follow apply equally to group, user or Guest entitlements.

The Edit Entitlements page opens (shown in the following example) displaying the current channel for your system. If the channel is authorized, it will be highlighted in blue.



   a. To add the Viper's channel to the group's authorized resources, check the channel and click Add Selected.
   b. To remove the Viper's channel from the group's authorized resources, check the channel and click Remove Selected.

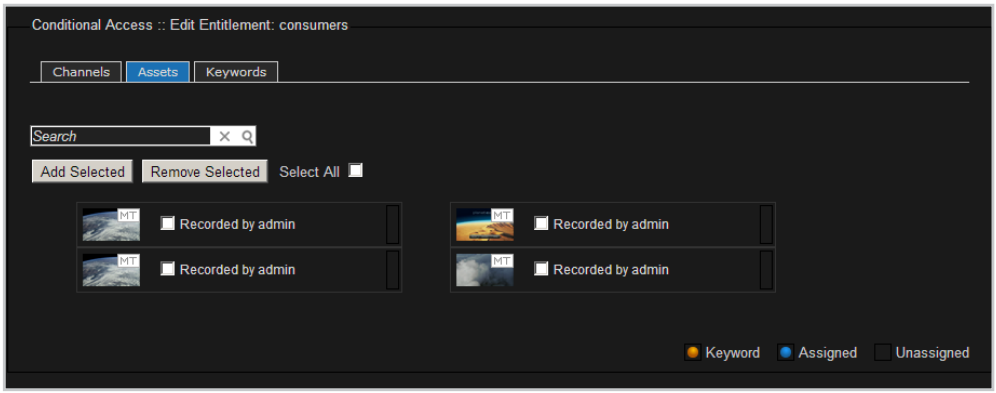
TIP You can check the Select All checkbox and then click Add Selected or Remove Selected to either add all names to or delete all names from the group. You can also use the CTRL or SHIFT keys to select multiple names.

Asset Entitlements

1. To modify the authorized Viper assets for the group or user, click the Assets tab.

   The Asset Entitlements page (shown in the following example) displays the current list of available Viper assets for your system.

TIP Authorized assets for the group are highlighted in blue. In addition, the color of the smaller rectangle to the far right indicates the entitlement method. It is blue for assets that have been selected "manually" from this page, and orange for assets that are keyword-entitled. See "Keyword-based Entitlements" on page 64.



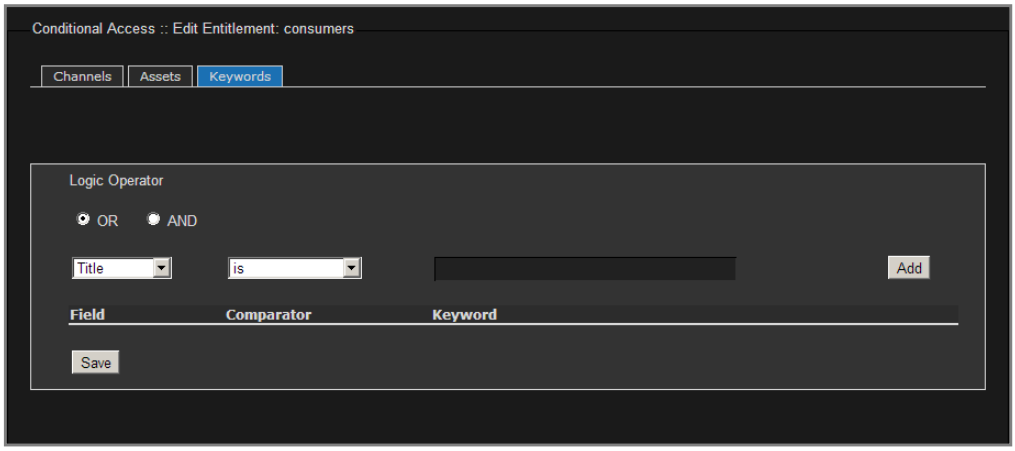
   a. To add assets to the group's authorized resources, check the names of the assets and click Add Selected.

   b. To remove assets from the group's authorized resources, check the names of the assets and click Remove Selected.

Keyword-based Entitlements

1. To create entitlement rules for the group or user based on keywords in the asset's Title, Description and Tag metadata, click the Keywords tab.

   On the Keyword Entitlements page (shown below), you can build entitlement rule expressions that combine multiple rules using the Logic Operators OR or AND.



2. Select the Logic Operator:
   - OR: Only one rule needs to be met for the group of users associated with the rule to be entitled.
   - AND: All rules must be met for the group to be entitled.
3. For each rule, select the Metadata source ("Field"), either: Title, Description or Tag.
4. Select the Comparator, either: is, is not, contains, or does not contain.
5. Type the Keyword in the text field and click Add.
6. To view a preview of the asset list resulting from the keyword-based entitlement, click Preview.
7. Repeat Steps #2- #5 to enter additional rules (i.e., to build a rule expression).

   Each time you add a rule, any assets that met the conditions of the rule are displayed below the list (see examples on the following page).
8. Click Save to save the entitlement rules.

Your changes take effect immediately. When you have completed all sections, you can either navigate to another module or click Sign Out to exit the Admin module.

Managing Device Entitlements

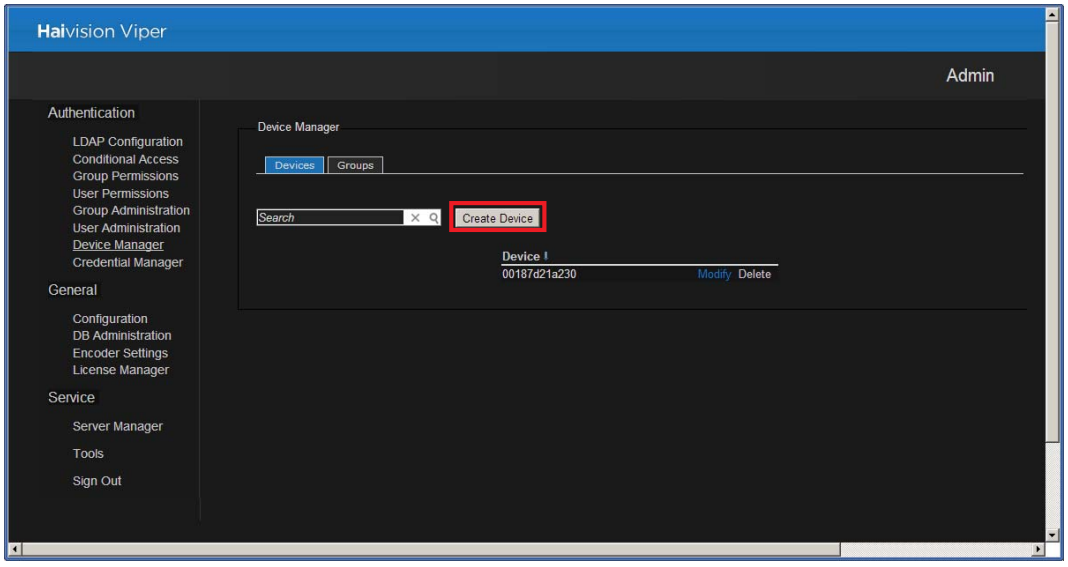
NOTE The Device Manager is included in the Conditional Access module.

The Device Manager allows you to “register” set top boxes (STBs) in your realm and then assign them to groups to control entitlements.

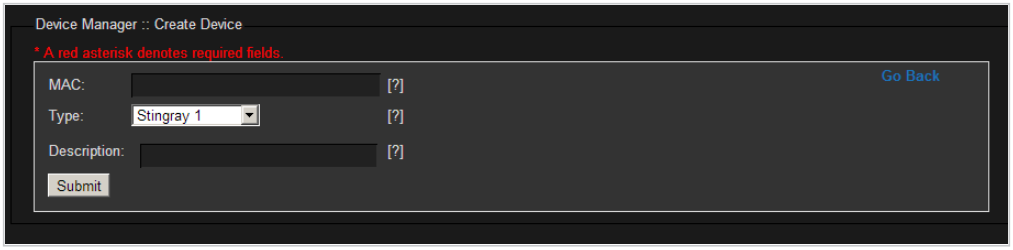
TIP can decode encrypted stations if it is invited and used as a integrated device in the realm, commanded by VF Command & Control. However, a decoder cannot decode encrypted stations if it is not invited.

To configure a device entitlement:

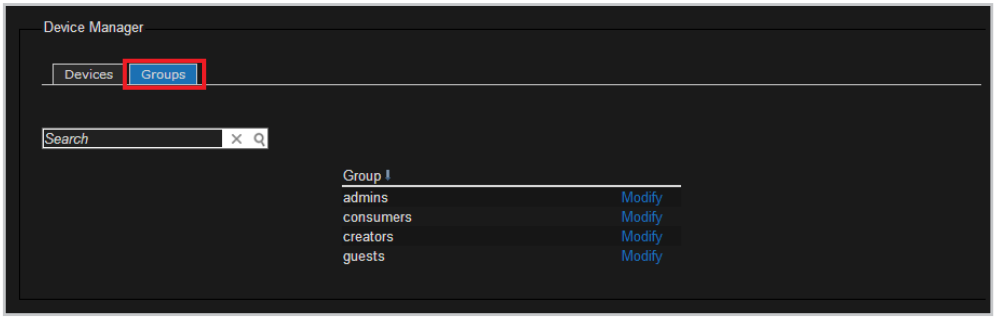
1. Click the Device Manager link on the left side of the Admin page.
2. On the Device Manager page, click Create Device.



3. On the Create Device page, type in the MAC address of the device (using hexadecimal digits without separators).



4. Select the device type, either Stingray 1, Stingray 2, or Makito Decoder.
5. (Optional) Type in a Description.
6. Click Submit.
7. On the Device Manager page, click the Groups tab.



8. To add the device to a group, click Modify next to the group name.

   The Modify Group page opens displaying the current list of defined devices for your system. Devices that are part of the group are highlighted in blue.
9. Check the name of the device to add to the group and click Add Selected.
10. Click the Device Manager link on the left side of the Admin page to return to the Devices tab.

Managing API Credentials

The Viper's REST API uses the OAuth standard to provide authentication to API clients. All clients accessing the API are required to authenticate.

To get started implementing API applications, you must generate an API credential for authentication.

This section provides the steps to accomplish this.

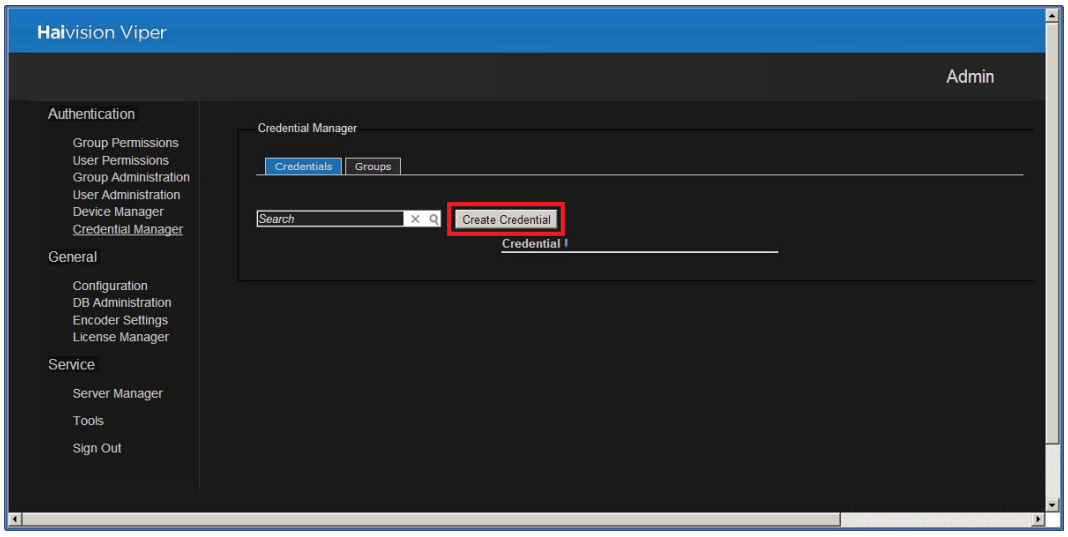
NOTE When joining one or more Vipers to a Furnace realm, the API credentials must be created on the Furnace, *not* the Viper(s). You are not required to create a credential for each Viper, although that is "Best Practices" for security.

You must set the Rest API Version to 2.0 on the Furnace Configuration page to allow the connection to the Viper to take place.

Creating a Credential

To create a credential for the Viper API or a Viper:

1. On the Admin page, click the Credential Manager link (on the left side under Authentication).
2. On the Credential Manager page, click Create Credential.



3. On the Create Credential page, type in a Name to associate with the credential and a Description.

4. Select the Expiration date and time (when the credential should expire and the system should deny access). Be sure to enter a complete date, including the hour, minute, and second.
5. Click Submit.

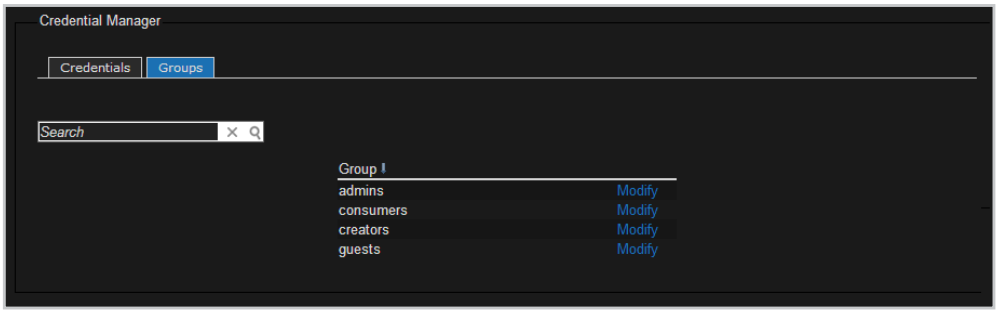
Associating the Credential With Viper Groups

Groups are used to restrict the permissions with which an API credential can operate. API actions are limited to the credential's assigned group permissions.

TIP In the case of Viper-Furnace integrations, the API credential created on the Furnace should always be assigned to a group with admin permissions.

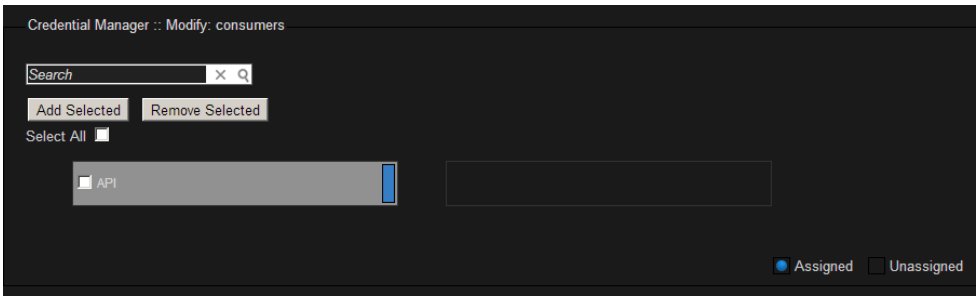
To associate a Credential with Viper User Groups:

1. On the Credential Manager page, click the Groups tab.



2. To add the credential to a group, click Modify next to the group name.

   The Modify Group page opens displaying the current list of defined credentials for your system. Credentials that are part of the group are highlighted in blue.



3. Check the name of the credential to add to the group and click Add Selected.

NOTE The group requires the All Permissions setting for API credentials to be allowed. See "Configuring Permissions for Groups or Users" on page 43.

Viewing the Consumer Key and Secret pair

You will need to copy the Consumer Key and Secret pair in order to use OAuth for your Viper APIs or to integrate a Viper in the realm of this Viper server.

To view the Consumer Key and Secret pair:

1. Click the Credential Manager link on the left side of the Admin page to return to the Credentials tab.
2. Find your credential in the list and click Modify next to the credential name.

   The Modify Credential page opens showing the Consumer Key and Consumer Secret generated for this credential (shown in the following example).

3. Select and copy this Consumer Key and Consumer Secret.

CHAPTER 4: Admin Module - General System Configuration

This chapter continues the Admin module, covering the General and Service Configuration tasks.

NOTE The procedures described in this chapter assume that you have administrative privileges.

Topics In This Chapter

General Configuration 71
- General Configuration Options 73
- Configuring the Launch Portal Theme 75
  - Guidelines for Changing the Launch Portal Theme 76
- Re-Branding the InStream Interface 78
  - "Stretchable" Images 79
  - Branding Options 81
- Customizing UI Labels 84

Encoder Configuration 86
- Configuring the Video 86
  - Video Settings 87
- Configuring the Audio 89
  - Audio Settings 90
- Taking a System Snapshot 91

Server Manager 93
- Managing the Server 93
  - Device States 96
  - Device Options 96
- Configuring Network Settings 98
  - Network Settings 100
  - Advanced IP Settings 102

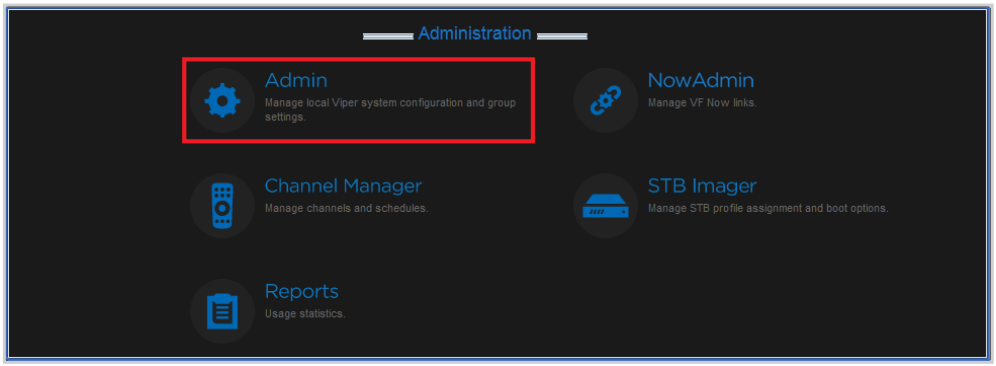
General Configuration

The Admin module provides General Configuration tools to configure the Viper Web tools and interface, as well as the Launch portal theme and the InStream player user interface. For example, you can:

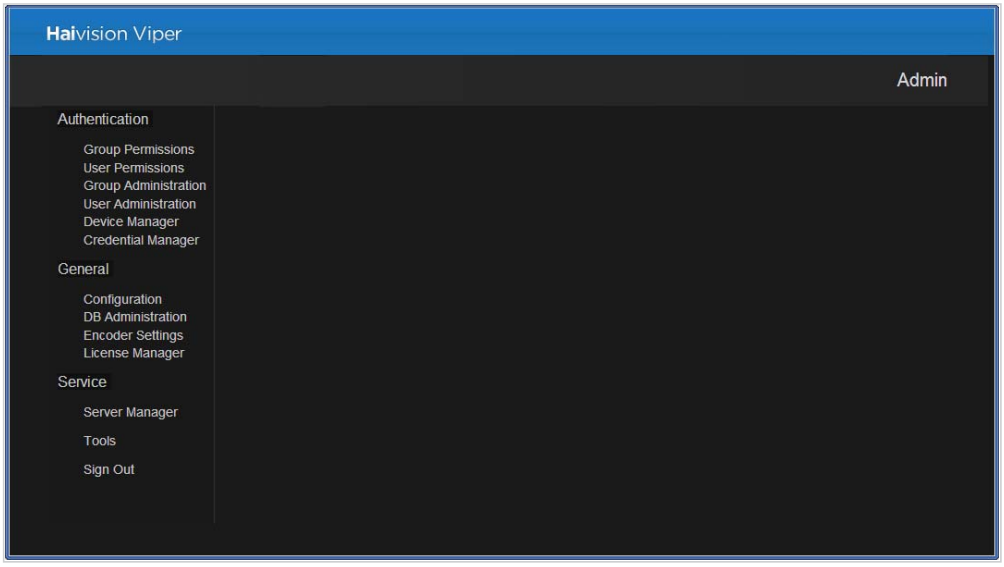
- Select the Viper Authentication Mode (PIN and Password, or PIN only, see page 73).
- Select the Viper Publishing Method (Automatic or Manual, see page 73).
- Select the Viper Publishing Destination (either Viper or a host Furnace, see page 73).
- Select the Conditional Access method (see page 73).
- Upload and select themes for the Launch portal (see page 75).
- Customize the InStream player user interface (including the company logo, player window, player controls, menu colors, and push-button look, see page 78). Note that this is a licensable option.
- Customize the text displayed on the user portal and InStream player user interface (including the labels and tooltips, see page 84).
- Select the Viper Control Status, either Local (from the Touch Panel interface) or External (from an external API, see page 74).
- View existing and update the system license (License Manager page).

To configure the Web tools and interface:

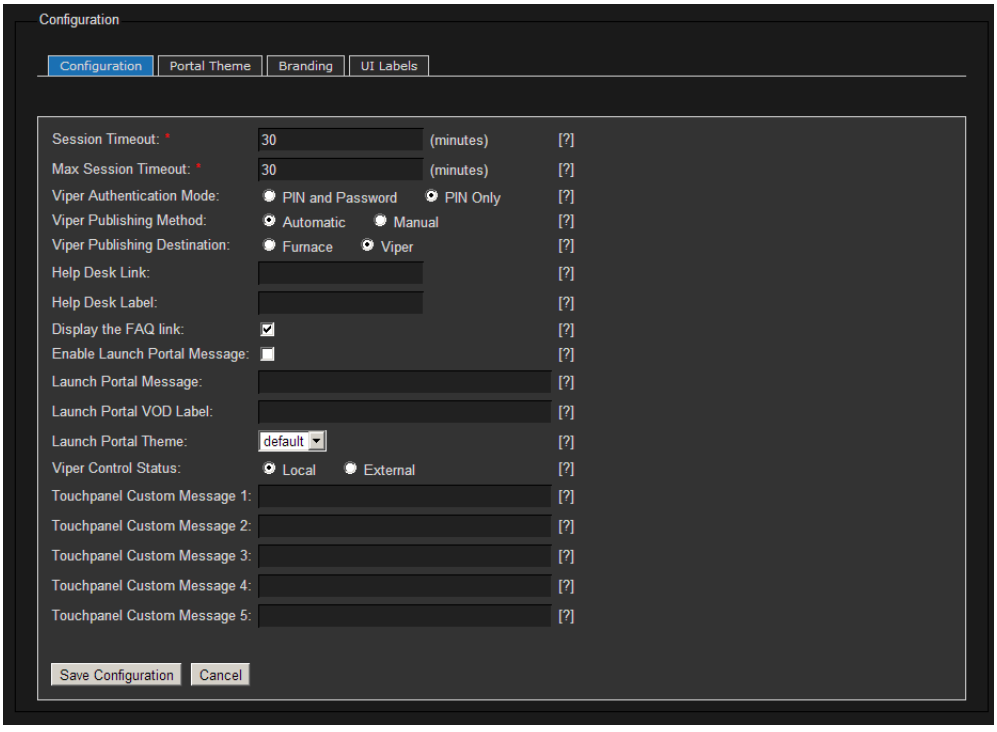
1. On the Tools page, click the Admin icon.



2. Click the Configuration link on the left side of the Admin page.



The Configuration page opens (shown in the following example).



3. Select or enter the new value(s) in the appropriate field(s). See the following section, "General Configuration Options".

4. Once you are finished with your changes, click Save Configuration.

General Configuration Options

The following table lists the Configuration options:

Configuration Option	Description
Session Timeout	Enter the time in minutes before active sessions expire: 1-60
Max Session Timeout	Enter the maximum time in minutes before active sessions expire: 1-360
Viper Authentication Mode	Select which authentication mode to use for the Touch Panel: • PIN and Password: Users must enter a PIN followed by their username and password to gain access. • PIN only: Users can gain access simply by entering their PIN. NOTE: "PIN only" is not available when using LDAP. For information on User PINs, see "Setting a User's PIN" on page 48.
Viper Publishing Method	Select which publishing method to use for the Touch Panel: • Automatic: Recordings will automatically be published when complete. • Manual: Recordings must be manually published after review. For more information, see "Publishing Options" on page 126.
Viper Publishing Destination	Select which publishing destination to use for the Touch Panel: • Furnace: Publish to a Furnace server if available. • Viper: Publish locally to the Viper. For more information, see "Publishing Options" on page 126.
Conditional Access Method	(Conditional Access optional module must have been purchased) Select to enable or disable the Viper Conditional Access module: • Off • On
Help Desk Link	Enter a full http:// or mailto: address to provide a Help link from the Launch portal.
Help Desk Label	Change the default Help Desk label on the Launch portal (navigation bar).

Configuration Option	Description
Display the FAQ Link	Check to display the FAQ Link on the Launch portal (navigation bar).
Enable Launch Portal Message (checkbox)	Check to display the Launch Portal Message.
Launch Portal Message	Message that will appear (in red) above the launch icons on the Launch portal.
Launch Portal VOD Label	Description of the VOD Library that will appear next to the Search field.
Launch Portal Theme	Select which theme to use for the Launch Portal. NOTE: To preview or modify the themes, see the following section "Configuring the Launch Portal Theme".
Viper Control Status	Select the Operational Mode for the Viper, either: • Local: from the Touch Panel interface. • External: from an external API. IMPORTANT: The Touch Panel application can only be locked from the Welcome screen. If the Touch Panel is not open to the Welcome screen when the Viper Control Status is set to External, the Touch Panel will be locked when it returns to the Welcome screen.
Touchpanel Custom Messages 1-5	This text will be displayed on the Touch Panel interface, and is useful when Viper Control Status is set to External. For example, it could be used to display contact information for system administrators

Configuring the Launch Portal Theme

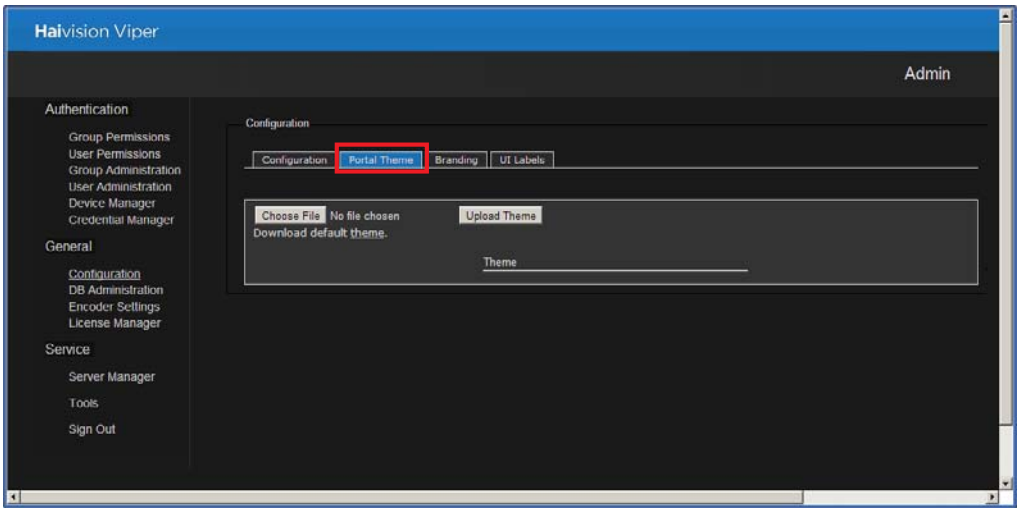
You can also configure the theme for your site's Launch portal. This is done by modifying the .css (Cascading Style Sheet) file provided with the Viper.

To get started, you need to download the Viper default theme and then adapt it (using a text editor) to suit your company or organization.

To adapt the default Viper portal theme:

1. On the Configuration page, click the Portal Theme tab.

   The Portal Theme tab opens, listing the themes available for your system.



2. Click Download default theme to open the default Viper .css file in a text editor on your local computer.
3. Type in your changes in the text editor and save the file under a new name. For guidelines, refer to "Guidelines for Changing the Launch Portal Theme" on page 76.
4. On the Portal Theme tab, click Choose File (or Browse, depending on your browser) to select the modified .css file, and then click Upload Theme to add it to the list of available themes.
5. Once a new or modified theme is included on the Theme List, you can click Preview next to it and a prototype launch page will open in a new window.
6. Once you are satisfied with the theme, click the Configuration tab and select it from the Launch Portal Theme drop-down list.
7. Click Save Configuration.

The modified Launch portal will take effect immediately. You may have to refresh your browser to see the changes.

Guidelines for Changing the Launch Portal Theme

This section suggests some general guidelines for changing the Launch portal theme.

IMPORTANT This section is intended for qualified web developers and therefore does not attempt to provide instructions on how to modify the .css (Cascading Style Sheet) file. Doing so would be beyond the scope of this document.

However, CSS is a well documented standard. For more information, please refer to the following resources:

- http://www.w3.org/TR/CSS2/
- http://www.w3schools.com/css/

To change the theme, you can upload either a .css file, or a .zip file. Using a .zip file enables you to upload your own images along with the .css file.

The .zip file must contain a style.css file (this is the theme itself). There is currently no limit as to the number of .gif, .jpg and .png files the .zip file can contain. However, the maximum upload size is 20MB.

NOTE Images that are uploaded should be defined in the .css file with a relative path.

For example, an image that already exists may be defined as:

```
background-image: url('/images/vf_instream_button.png');
```

An image uploaded with your changes should be defined as:

```
background-image: url('custom_instream_button.png');
```

NOTES:

- Keep in mind that CSS uses selectors to choose which html object to modify. Consider the following example (from the Viper default .css file):

```
#footer
{
height: 159px;
background-image: url('/images/launch_footer.png');
background-repeat: no-repeat;
background-position: center center;
width: 1000px;
margin: auto;
}
```

The #footer is the selector, i.e., it selects which html object to modify. Therefore, you should not change the selector, because the footer will no longer have an image. Instead, to change the image, you can just change the background-image line to contain a different url.

- To use an image that you uploaded in a .zip file, the url should look like this:

```
url('launch_footer.png')
```

NOTE There is no leading slash. This is important, because if you put a slash at the front, it won't work.

- To use an image from your own server, you can specify something like this:

```
url('http://www.google.com/logo.png')
```

- Do not switch to a blank profile, as it can be difficult to fix. The login page becomes basically unusable without a theme. If this occurs, you can enter a username and password and press ENTER. Or you can use the following url to view the page with the theme disabled:

```
https://servername.com/login.php?theme=&action=/admin/
```

- There can only be one active theme at a time.

Re-Branding the InStream Interface

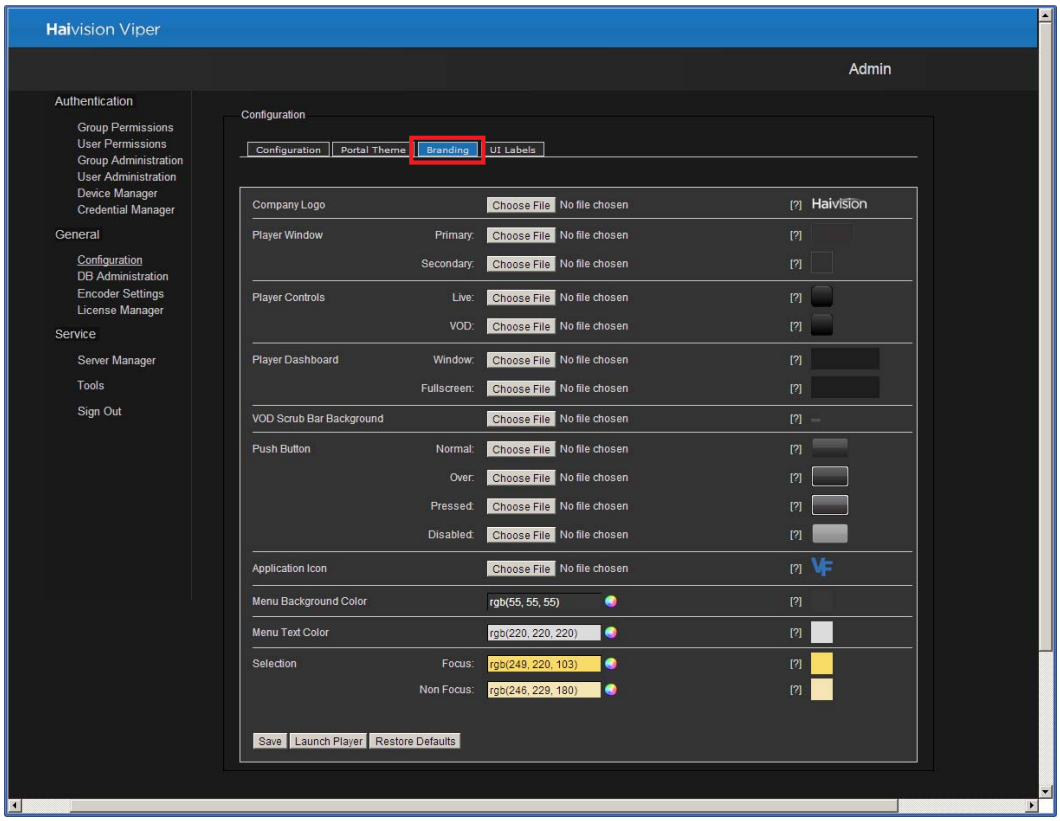
From the Configuration Branding page, you can customize the InStream player user interface components such as the company logo, player window, player controls, menu colors, and push-button look. From this page, you can view details about individual components such as the image filename or color value. You can upload image files to replace the default components, select new colors, save, and then launch the InStream player to preview the rebranded interface.

NOTE After upgrading a Viper server, you will need to reapply the branding by re-saving. However, you do not need to reload any of the individual components.

To customize the InStream player user interface:

1. On the Configuration page, click the Branding tab.

   The Branding tab opens (shown below).



   The Branding page consists of a list of components, either image files (in .PNG format) or colors (RGB values), that make up the InStream player user interface.

For each component, a thumbnail of the current image file or color value is displayed in the far right column. You can pass the cursor over the thumbnail to display the image filename or the RGB color value. Clicking [?] displays the information you need to know to replace the component, such as the image size, and for "stretchable" components, the xy coordinates and dimensions of the quadrants. (See the following section ""Stretchable" Images".)

2. Select the components to customize your InStream player user interface. (See "Branding Options" on page 81.)
   - For image files, click Choose File to locate the file, and then click Open to select the image to upload.
   - For colors, click the color wheel and select the color.
3. To preview your changes, click Save and then click Launch Player.

"Stretchable" Images

For components such as the player window, player controls, player dashboard, and push button, you can upload a small image which will be used as a background when the InStream application displays the window. Using a concept called "stretching" (Windows/Mac OS X), the application will take the image and stretch it across (and in some cases, down) to fill the space in your application window. (Note that Linux doesn't stretch the images; it repeats them, i.e., "tiling".)

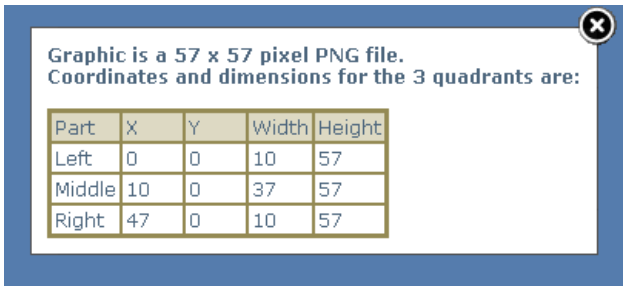
NOTE Logo images (i.e., the Company Logo and Application Icon) are not stretched.

Each "stretchable" component uses either a 3 or 9 quadrant grid: 3 quadrant images are only stretched horizontally, while 9 quadrant images are stretched both horizontally and vertically.

- With a 3 quadrant image, the two side quadrants of the image are displayed without change, while the space between is stretched horizontally to fill the space. See the following section "Example: 3 Quadrant Image".
- With a 9 quadrant image, the four corner quadrants of the image are displayed without change, while the space between the top and bottom, and left and right is stretched both horizontally and/or vertically to fill the space.

Example: 3 Quadrant Image

Clicking [?] for Player Controls: VOD displays the filesize (57 x 57 pixels) and the coordinates and dimensions for a 3 quadrant grid:



To continue the example, below is a simple 57 x 57 pixel .PNG graphic divided into three quadrants, with the “stretchable” area indicated between the two white lines:

The following image shows the above .PNG graphic after it has been stretched horizontally. Note that the two side quadrants are displayed without change.

Branding Options

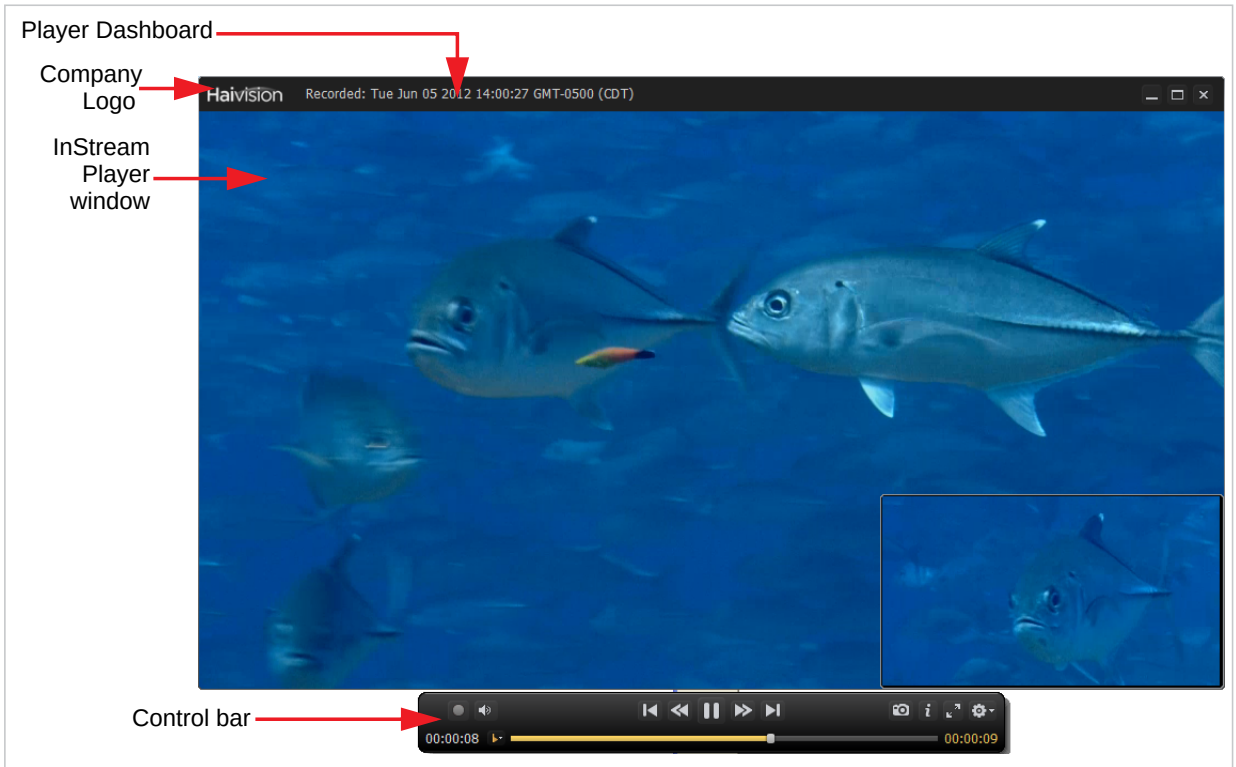
The following table lists the Branding options. [For an illustration of the components in the InStream player window, see Figure 4-1 on page 83.]

User Interface Component	Description
Company Logo	Select a PNG file to display as the logo. [Top left, within Player Window dashboard, *not* stretched.] The height must be less than or equal to 32 pixels so it will fit within the player dashboard. The logo can be as wide as needed. NOTE: The Haivision graphic is a 74 x 18 pixel PNG file.
Player Window	These images will be stretched both horizontally and vertically to fit the Player Window. For the xy coordinates and dimensions of the 9 quadrants, click [?].
Primary	Select a 300 x 150 pixel PNG file to display for the Primary player window.
Secondary	Select a 75 x 75 pixel PNG file to display for the Picture-In-Picture (PIP) window.
Player Controls	These items define the player control bar below the Player Window. These images will only be stretched horizontally. For the xy coordinates and dimensions of the 3 quadrants, click [?].
Live	Select a 35 x 35 pixel PNG file to display for the Live video control bar.
VOD	Select a 57 x 57 pixel PNG file to display for the VoD control bar.
Player Dashboard	These items define the “dashboard” at the top of the InStream player. These images will only be stretched horizontally. For the xy coordinates and dimensions of the 3 quadrants, click [?].
Window	Select a 100 x 32 pixel PNG file to display for the dashboard.
Fullscreen	Select a 100 x 32 pixel PNG file to display when the player window is in Fullscreen mode.

User Interface Component	Description (Cont.)
VOD Scrub Bar Background	Select a 13 x 5 pixel PNG file to display for the VOD scrub bar background.
Push Button	These items define the Watch and Close push buttons. These images will be stretched both horizontally and vertically. Select a 49 x 28 pixel PNG file for each. For the xy coordinates and dimensions of the 9 quadrants, click [?].
Normal	This graphic will be displayed when the push button is in the Normal state.
Over	This graphic will be displayed when the cursor hovers over the push button.
Pressed	This graphic will be displayed when the push button is pressed.
Disabled	This graphic will be displayed when the push button is disabled.
Application Icon	Select a 49 x 28 pixel PNG file to be displayed on the InStream button on the taskbar. NOTE: The Application Icon is not stretched. (Does not apply to Mac OS X, only Windows and Linux.)
Menu Background Color	Select the background color for menu windows (e.g., Player Settings and Multi-viewer Settings windows).
Menu Text Color	Select the color for the text in menu windows.
Selection	Select the color to indicate selection.
Focus	Select the color for the selected item while the focus is in that window.
Non Focus	Select the color for the selected item while the focus is not in that window.
Save	Click to save your selections. You must save *before* launching the player in order to preview your changes in the rebranded interface. NOTE: This causes the Defaults button to appear to allow you to toggle the thumbnails between system defaults and your saved selections. TIP: Because some browsers cache images, you may need to refresh your browser if an uploaded image doesn't show in the thumbnail.

User Interface Component	Description (Cont.)
Launch Player	Click to launch the InStream player to see your (saved) changes (i.e., preview the rebranded interface).
Defaults / User Defined	These buttons become available once you have saved changes. Click to toggle the thumbnails between the system defaults and your saved selections. This is helpful when comparing your rebranded components to the defaults.
Restore Defaults	Click to restore the InStream player to its default look. NOTE: Your changes will be discarded.

Figure 4-1 Components of InStream Player Interface (Player window)



Customizing UI Labels

From the Configuration UI Labels page, you can customize the text displayed on the InStream player, user portal, error messages, and Touch Panel interface. The text that you can replace includes labels as well as tooltips (which appear when the user hovers the cursor over an item).

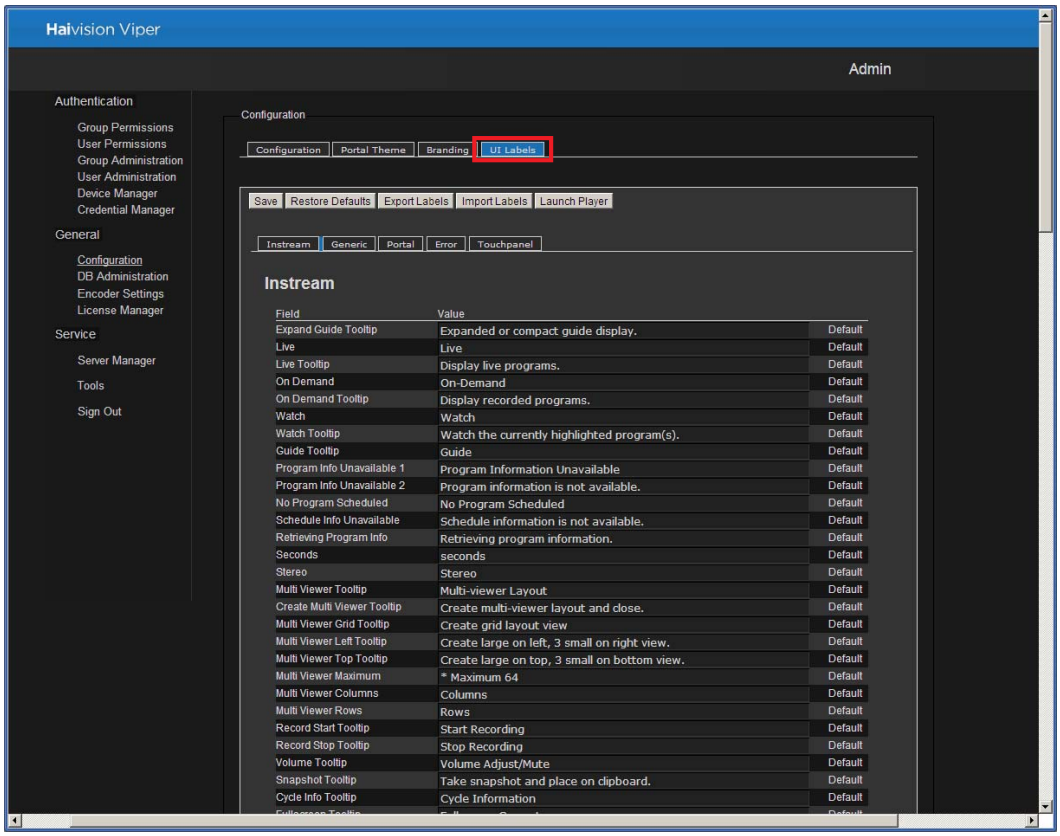
This allows you to adapt the interface to your requirements, including translating the interface into other languages. For example, you can create customized versions in French, German, and Spanish. You would export each version and then distribute it to be imported on other Viper systems.

As you work, you can launch the InStream player to preview the customized labels. At any time, you can restore a label to its default or restore all labels to their default values.

To customize the InStream player user labels:

1. On the Configuration page, click the UI Labels tab.

   The UI Labels tab opens (shown in the following example).



2. For each label or tooltip to customize, type the new text in the Value field.
3. To customize the Touch Panel interface text, click the Touchpanel tab.
4. To preview your changes, click Save and then click Launch Player.

5. To restore a label to its default, click the Default button to the right of the Value field.
6. To restore all labels to the defaults, click Restore Defaults.
7. When you are satisfied with your customized interface, you can export it. To do so, click Save and then click Export Labels. The interface labels and tooltips are saved in a proprietary file entitled labels.data in your default Downloads folder. You can modify the filename as required to distinguish different customized versions.
8. To import a saved interface customization, click Import Labels and select the customized .data file to load onto the current Viper system.

Encoder Configuration

From the Encoder Settings page, you can specify the Video and Audio settings for the Primary and Secondary built-in encoders. You can also generate an Encoder system snapshot for troubleshooting purposes.

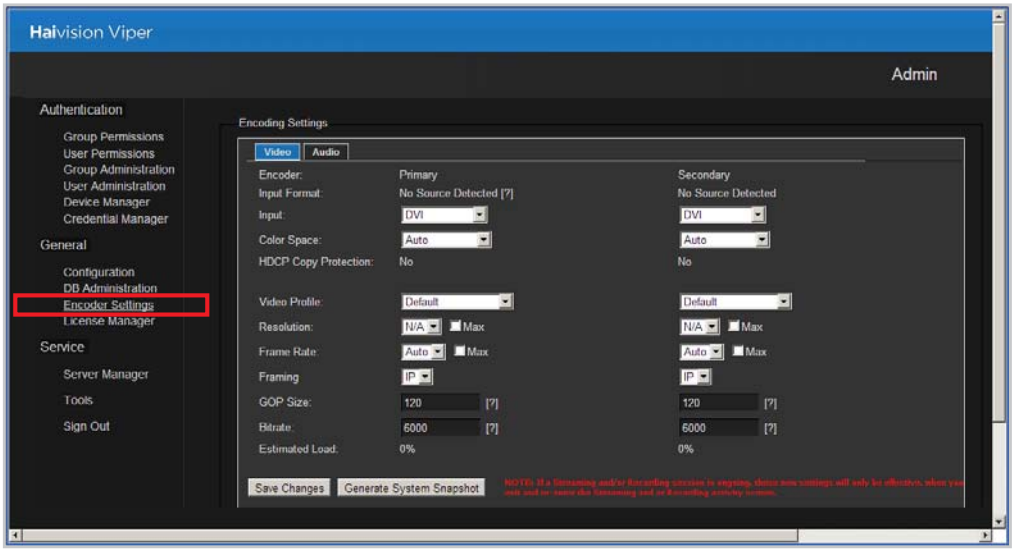
NOTE If the Touch Panel interface is being used for streaming and/or recording, the Encoder Inputs must be selected from the Touch Panel interface.

Configuring the Video

To configure the video settings for the built-in encoders:

1. Click the Encoder Settings link on the left side of the Admin page.

   The Encoder Settings page opens to the Video tab (shown below), displaying the configurable video encoding settings for your Viper.



2. Fill in the fields to configure the video encoder settings for your Viper. See the following section "Video Settings".

3. Click Save Changes.

NOTE If a streaming and/or recording session is ongoing, you must exit and re-enter the Stream & Record Activity screen (on the Touch Panel interface) before your changes will take effect.

Video Settings

The following table lists the configurable Viper Encoder Video Settings. Each setting is selected on a per stream basis, so you need to configure the settings for both inputs.

Video Setting	Description
Encoder	Primary or Secondary.
Input Format	(Read-only) This is the input signal detected from the video source. It includes the number of pixels per line and the number of frames per second. This is auto-detected by the system and cannot be changed. If the signal cannot be detected (or is outside the supported range), the Viper Touch Panel will display a static color bar, and the Web Interface Input Format will be No Source Detected.
Input	Select the type of Video Input for the appliance: • Digital (DVI) • Digital (DVI 2) • Analog (Component) • Analog (Component 2) • S-Video • Composite • SDI
Color Space	Select the color space to use while capturing the content. Matching the appliance input color space to the source enhances and optimizes color reproduction. This is useful with source formats such as graphics cards outputting HDTV resolutions. Select either: • Auto: The encoder determines the appropriate color space to use. • YCbCr: Forces the encoder to use Y,Cb,Cr • RGB (Full Range): Forces the encoder to use RGB Full Range [0..255] • RGB (Limited Range): Forces the encoder to use RGB Limited Range [16..235] TIP: Once the color space has been modified, re-select the Input Sources from the Viper Touch Panel to ensure the modification has taken effect.
HDCP Copy Protection	(Read-only) Indicates whether an HDCP stream is copy-protected. If Yes, the stream will not be encoded.

Video Setting (Cont.)	Description (Cont.)
Video Profile	(Optional) Select a Video Profile to control the video quality for the encoder. The list provides a selection of video presets or “Profiles” defined for different contexts: • ComputerGraphics • Default • Movies • News • Outdoors • Sports • VirtualPresence
Resolution	This is the stream output resolution. Select the number of lines per frame and pixels per line to be encoded. Options depend on the Input Format detected, and may include: • 1920x1080p • 1920x1080i • 1440x1080p • 1440x1080i • 960x1080p • 960x1080i • 1280x720p • 720x480p NOTE: This is a dynamic set of resolutions generated by the Viper’s encoder. Any formats allowed to be downscaled will be auto-displayed by the Viper’s encoding functions.
Frame Rate	Select the video frame rate per second: • Auto: Encodes at the same frame rate as the input • 60..1 fps
Framing	Select the Video Compression Mode: • IP: I and P frames only
GOP Size	Enter the Group of Pictures size for the encoded video. 0..1000 Default = 120. NOTE: The GOP Size is the same for both inputs.

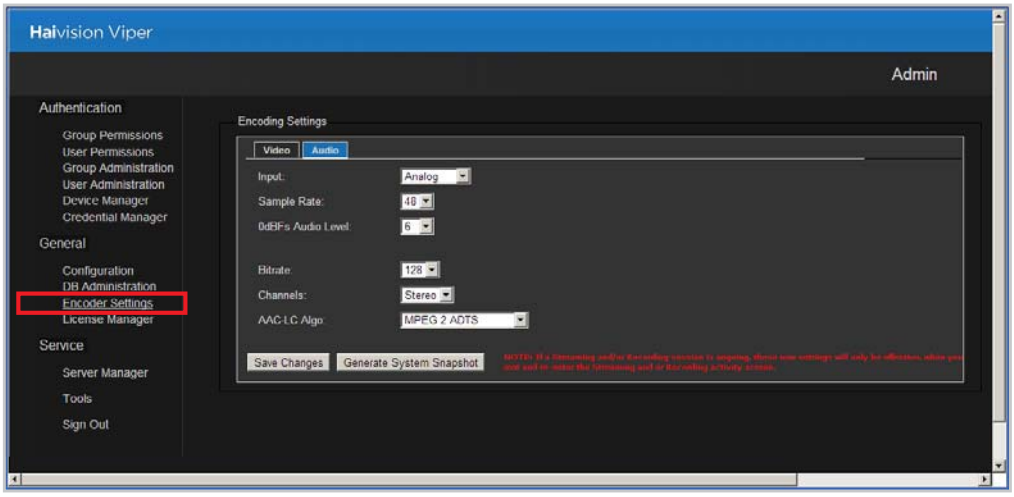
Video Setting (Cont.)	Description (Cont.)
Bitrate	Enter the Video Bitrate (numeric values only) for the encoded video: • HD: 150..15000 kbps • SD: 150..8000 kbps Default = 6000.
Estimated Load	(Read-only) The video encoding processor usage of the stream instance in percentage%. This value is included to help administrators manage the overall load of the encoder services, to prevent the encoders from exceeding their processing capacity, which can cause image degradation and poor encoding quality. NOTE: The combined estimated loads should not exceed 100%.

Configuring the Audio

To configure the audio settings:

1. On the Encoder Settings page, click the Audio tab.

   The Audio tab opens (shown below), displaying the audio encoding settings defined for your Viper.



2. Fill in the fields to configure the audio encoder settings for your Viper. See the following section "Audio Settings".

3. Click Save Changes.

NOTE If a streaming and/or recording session is ongoing, you must exit and re-enter the Stream & Record Activity screen (on the Touch Panel interface) before your changes will take effect.

Audio Settings

The following table lists the configurable Viper Encoder Audio Settings. Each setting is selected on a per stream basis, so you need to configure the settings for both inputs.

Audio Setting	Description
Input	Select the type of Audio Input for the encoder: • Analog • RCA • XLR • SDI1Ch12 • SDI1Ch34
Sample Rate	The number of audio samples per second taken from the incoming signal. 48 kHz only.
0 dBFS Audio Level	(Analog Input only) Adjusts the maximum analog Audio Input level (0 dBfs) from +5dBU up to +20dBU. NOTE: This is useful in applications such as broadcast and streaming to allow higher audio headroom.
Bitrate	Select the Audio Bitrate for the encoder: 32, 64, 96, 128, 192, 256, or 384 kbps. Default = 128
Channels	Select the number and type of audio channels to encode. Mono, Stereo If you set the Audio Bitrate to 32 kbps, use Mono.
AAC-LC Algo	The audio compression algorithm: • MPEG2 ADTS - Encodes audio using the ISO/IEC 13818-7 MPEG-2 AAC-LC algorithm with an ADTS header. (Default) • MPEG4 ADTS - Encodes audio using the ISO/IEC 14496-3 MPEG-4 AAC-LC algorithm with an ADTS header. • MPEG4 LOAS/LATM - Encodes audio using the ISO/IEC 14496-3 MPEG-4 AAC-LC algorithm with a LOAS/LATM header.

Taking a System Snapshot

Taking a system snapshot can be useful for troubleshooting and may be forwarded to Haivision Technical Support if you are requesting technical support for the Viper.

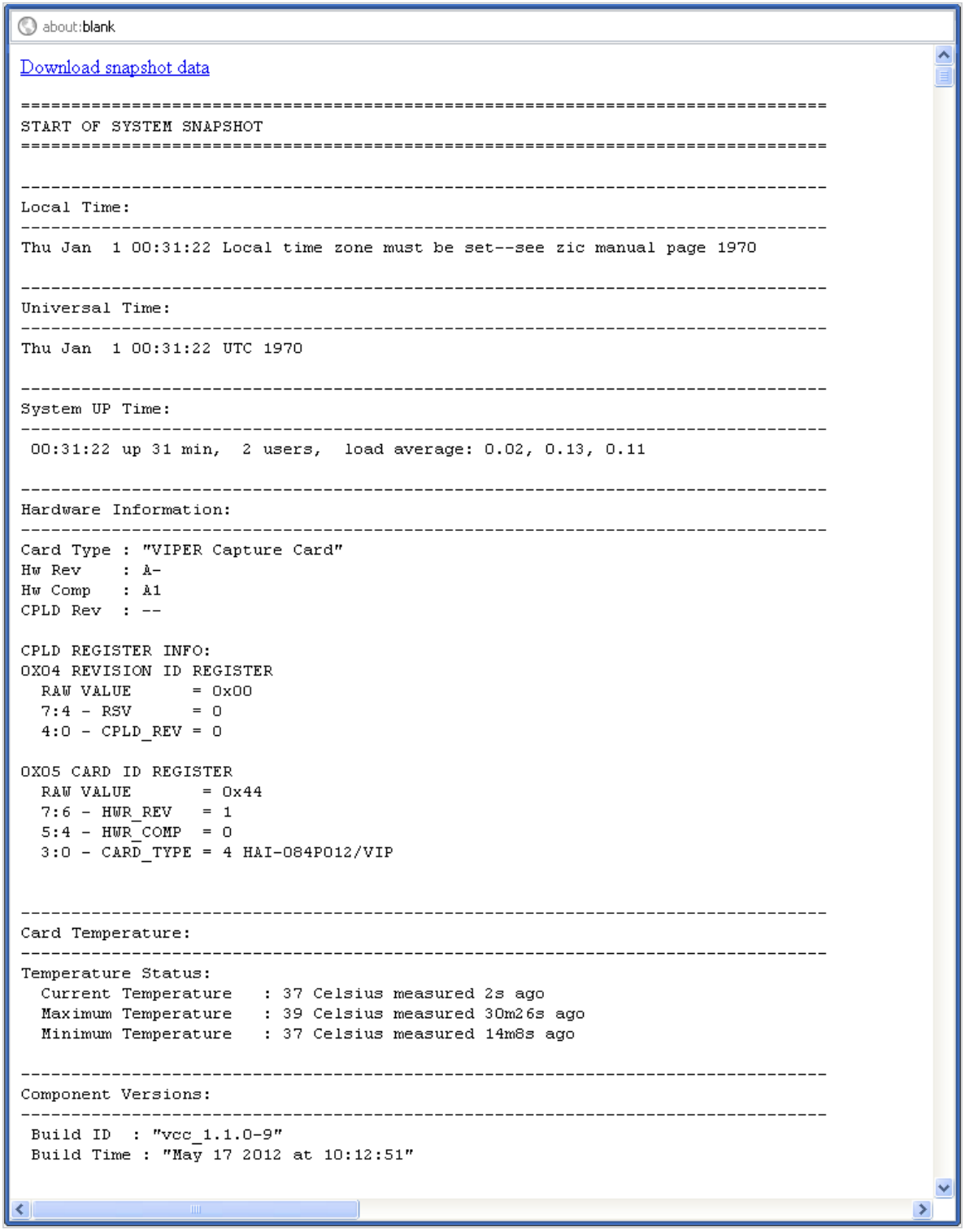
The system snapshot lists information such as system uptime, hardware information, component versions, network settings, loaded modules, running processes, system traces, configured streams and stream status checks, configured video encoders and status checks, configured audio encoders and status checks, startup config file contents, global settings file contents, debug logging settings file contents, downloaded software packages, last software update log, and OS statistics.

To take a system snapshot:

1. From the Encoder Settings page (either Video or Audio tab), click Generate System Snapshot.

   The system will display a snapshot of system information in a new window, as shown in the following example.

2. To download the file to your computer, click Download snapshot data and save the file on your computer.


about:blank
Download snapshot data
==========
START OF SYSTEM SNAPSHOT
==========

Local Time:

Thu Jan 1 00:31:22 Local time zone must be set--see zic manual page 1970

Universal Time:

Thu Jan 1 00:31:22 UTC 1970

System UP Time:

 00:31:22 up 31 min, 2 users, load average: 0.02, 0.13, 0.11

Hardware Information:

Card Type : "VIPER Capture Card"
Hw Rev   : A-
Hw Comp   : A1
CPLD Rev : --
CPLD REGISTER INFO:
0X04 REVISION ID REGISTER
  RAW VALUE   = 0x00
  7:4 - RSV   = 0
  4:0 - CPLD_REV = 0
0X05 CARD ID REGISTER
  RAW VALUE   = 0x44
  7:6 - HWR_REV   = 1
  5:4 - HWR_COMP = 0
  3:0 - CARD_TYPE = 4 HAI-084P012/VIP

Card Temperature:

Temperature Status:
  Current Temperature   : 37 Celsius measured 2s ago
  Maximum Temperature   : 39 Celsius measured 30m26s ago
  Minimum Temperature   : 37 Celsius measured 14m8s ago

Component Versions:

 Build ID   : "vcc_1.1.0-9"
 Build Time : "May 17 2012 at 10:12:51"

Server Manager

Managing the Server

In order to get started using the Viper, you must configure your system or “local realm”. The Server Manager page lists all the network-reachable VF-compatible devices it can see through its service discovery feature.

The devices on the Server Manager list are divided into three sections: Local Realm, Unassigned Devices, and Foreign Realms. Your “local” realm is the Viper to which you are currently connected, while “foreign” realms are devices that can be seen but are not managed by the Viper (because they belong to a different Portal Server). Unassigned devices are still searching for and have not joined a realm.

From the Server Manager page, you can perform the following key functions:

- View the server name, IP address, realm status, and “Last Seen” date of devices; also view the MAC address for unassigned devices and devices in foreign realms.
- Modify the network settings for the Viper.
- Select the Join Method for a Viper that is invited into a Furnace realm and confirming the invitation.
- Change the host name of a device in the local realm, in particular, to give meaningful, descriptive names to associate with encoders and servers.
- Reboot the Viper.

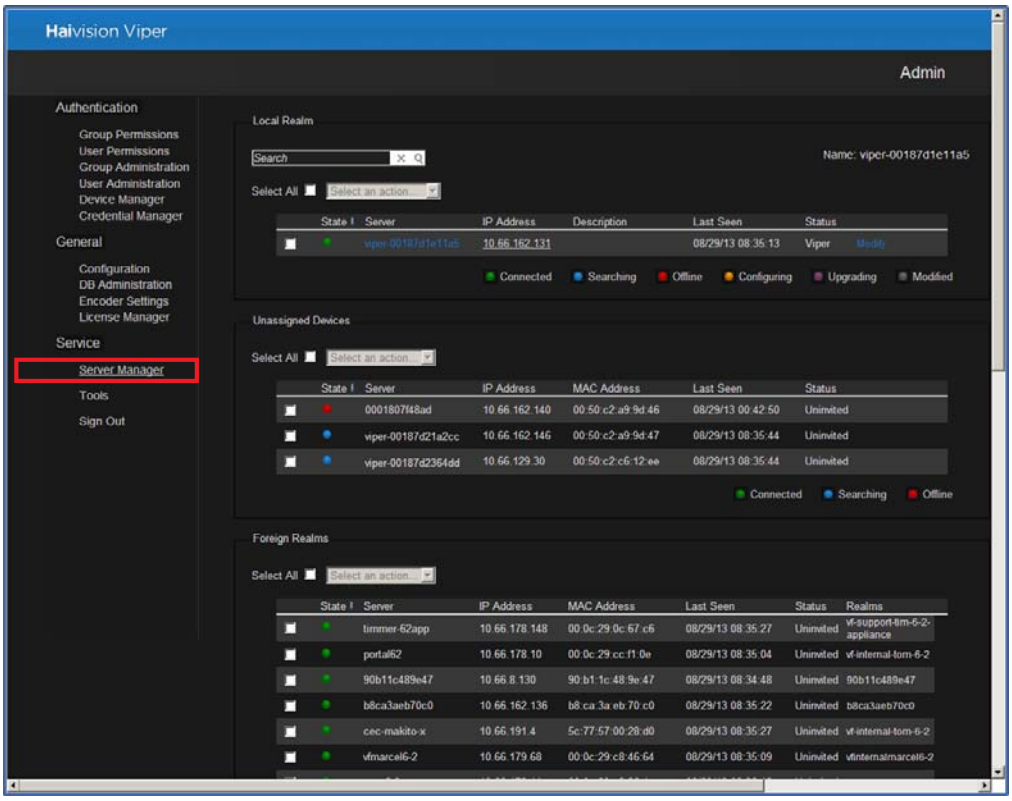
From the Server Manager page, you can also check the status of devices, i.e., to see whether a device is active (“Connected”), turned off (“Offline”), or attempting to locate and join its realm (“Searching”). For more information, see “Device States” on page 96.

NOTE A server will attempt to locate and join its realm for approximately 10 minutes.

To access the Server Manager list:

1. Click the Server Manager link on the left side of the Admin page.

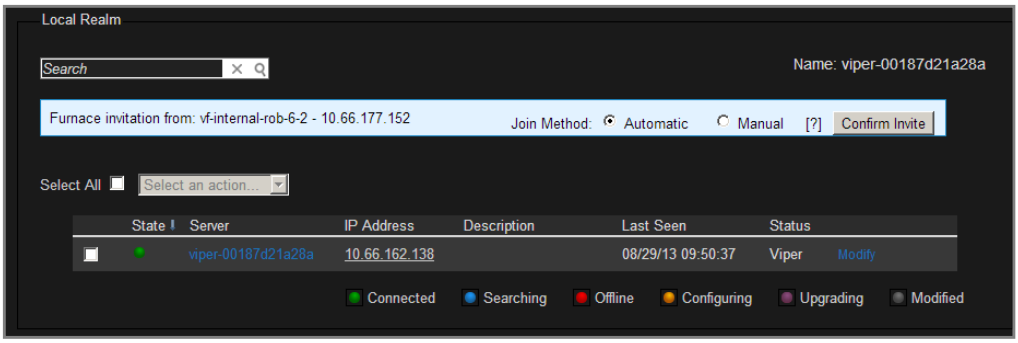
   The Server Manager page opens (shown in the following example).



   The Server Manager page lists all the VF-compatible devices available on the network, including their IP address and their status on the network/realm. The server list is derived from the License key on the Portal Server, but shows the realm status of all servers. This is important when you are adding hardware or if you have been shipped servers where the realm isn't properly set up.

2. If the Viper is to be integrated into a Furnace realm, the first step is to accept the invitation from a Furnace device.

   Each Viper to which an invitation has been sent from the Furnace will display an Invitation message highlighted in a blue box located at the top of its Server Manager page (as shown in the following example).

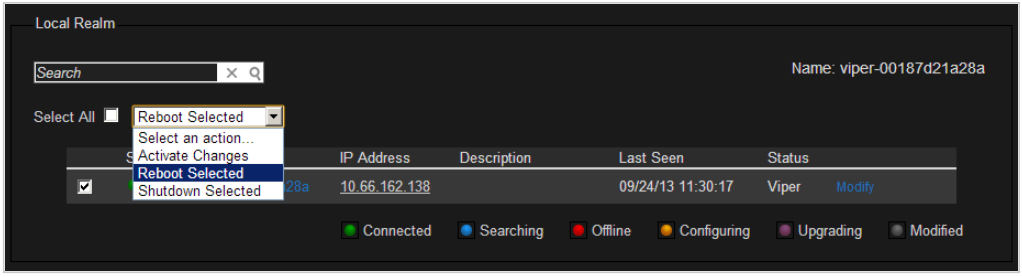


- To accept the Furnace invitation, select the Join Method: either Automatic or Manual. This determines whether the Viper will re-join the Furnace realm automatically or manually following future reboots.
- And then click Confirm Invite.

For more information, see "Accept the Invitation (Viper Server Manager)" on page 115.

3. To configure the network settings for the Viper, click the Modify button next to the Viper. See "Configuring Network Settings" on page 98.

4. To reboot the Viper, check the checkbox to select the Viper and select Reboot Selected from the Select an action… drop-down list. Note that there is a three-minute delay before the unit reboots.



5. When you have completed your changes, to activate the Viper, check the checkbox to select the Viper. Then select Activate Changes from the Select an action… drop-down list.

   Activating the Viper is only required when changing network settings; however, it is unnecessary when joining a realm.

Device States

The possible device states are as follows:

Device State	Description
Connected	Device is on network / communicating with Portal Server
Searching	Device is searching for a Portal Server to join. The server either does not have an active invitation to join, or has not heard from the server it wants to join.
Offline	Device is off network / not communicating with Portal Server
Configuring	(Local Realm only) Server has been told to reconfigure but has not yet done so (could indicate that server has accepted the configuration and is in process of reconfiguring, or server has rejected/denied the configuration and is not reconfiguring).
Upgrading	(Local Realm only) System upgrade is in progress.
Modified	(Local Realm only) Pending IP or Realm Settings changes.

Device Options

The server options are as follows:

Device Option	Description
Local Realm	
Activate Changes	Activates network and realm settings. You will be prompted to confirm the selection before the action is performed.
Evict Selected	Applies to a system that has joined your realm. This option removes it from the realm.
Invite Selected	Invites a system that has not yet joined the realm.
Reboot Selected	Reboots the Viper. You will be prompted to confirm the selection before the reboot is performed.

Device Option	Description
Shutdown Selected	Shuts down the Viper. You will be prompted to confirm the selection before the shutdown is performed.
Unassigned Devices / Foreign Realms	
Invite Selected	Applies to a system that is not in your realm yet.
Remove Selected	Applies to an offline system. This option allows you to delete records of a system that is no longer available, to help clean up the records of old systems which are no longer owned or have been replaced.
Uninvite Selected	Applies to a system that has been invited, but has not yet joined the realm.

Configuring Network Settings

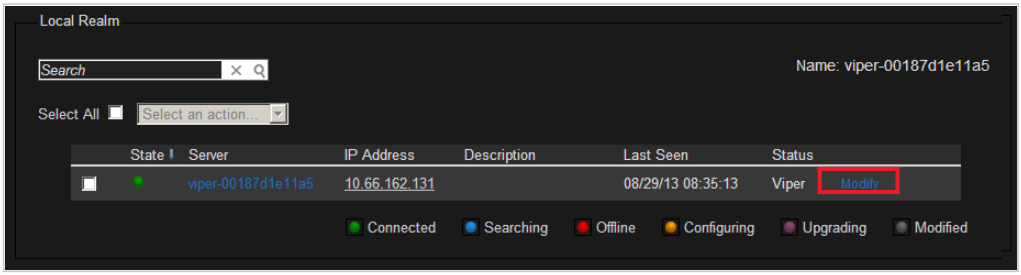
The Server Manager allows you to configure the network settings for the Viper. This includes modifying the IP address, subnet mask, gateway address, DNS server, and server hostname, as well as advanced settings such as NIC bonding, additional routes, and link negotiation settings.

NOTE This is only available to configure the Viper to which you are connected, *not* encoders or other devices in the realm. For the Viper's default network settings, see "Connecting the Viper to the Network" on page 19.

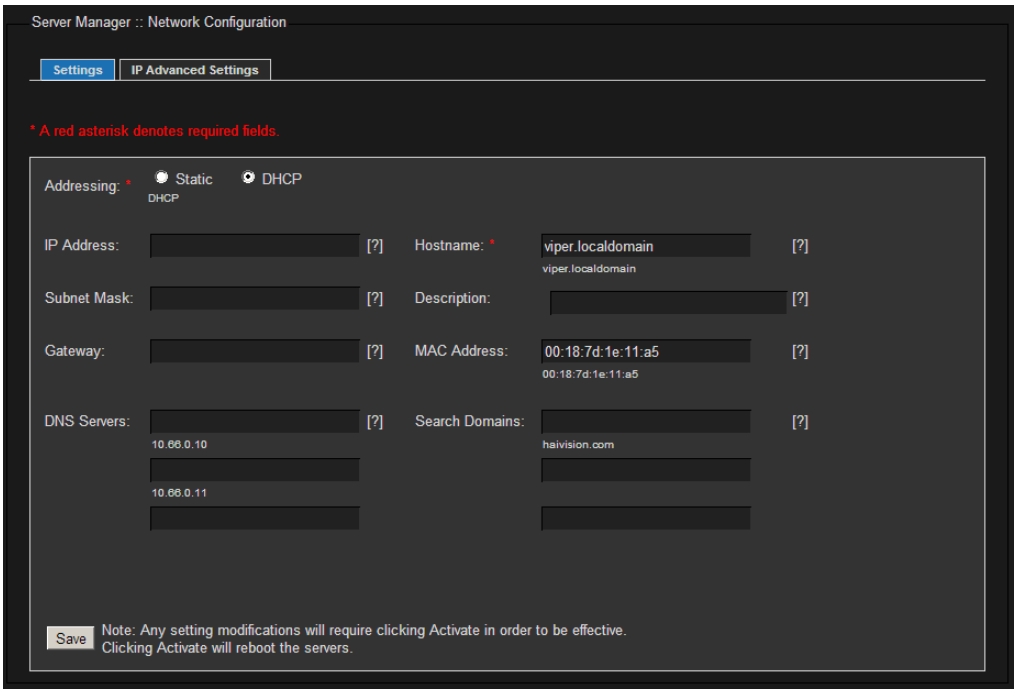
TIP You can also change the Viper's network settings from the Touch Panel interface. For details, see the Viper Getting Started Guide.

To configure the Network Settings:

1. On the Server Manager page, click the Modify button next to the Viper.



The Network Configuration page opens (shown in the following example).



2. Select either Static or DHCP to enable or disable the Dynamic Host Configuration Protocol.

NOTE When DHCP is enabled, the server will get an IP Address from a DHCP server on the network. When it is disabled, you must manually enter the server's IP Address, Netmask, and Gateway Address.

---

3. Make the required modifications and click Save. See the following section "Network Settings".

TIP To configure multiple network configurations, such as configuring bonding or setting up static routes, see "Advanced IP Settings" on page 102.

---

4. On the Server Manager page, select Activate Changes from the Select an action… drop-down list.

Network Settings

The following table lists the configurable Viper network settings. The current value is displayed below the text field (where applicable). A red asterisk denotes required fields, when static IP addressing is selected.

NOTE Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

IP Setting	Description
Addressing	Choose whether the Viper will use a static or dynamic IP address: • Static: Select to disable DHCP. When it is disabled, you must manually enter the IP Address, Netmask & Gateway Address. • DHCP: Select to enable the Dynamic Host Configuration Protocol. When DHCP is enabled, the Viper will receive an IP Address from a DHCP server on the network.
IP Address	Displays the IP Address for the Viper. This is a unique IPv4 address that identifies the unit in the IP network. NOTE: If DHCP is disabled, you may enter an IP address in dotted-decimal format (xxx.xxx.xxx.xxx).
Hostname	The hostname to be assigned to this Viper. This is a FQDN (Fully Qualified Domain Name); for example, myserver.mycompany.com.
Subnet Mask	Displays the IPv4 network mask for the Viper. This is the 32-bit mask used to determine the IP addresses of the local network. NOTE: If DHCP is disabled, you may enter a Netmask in dotted-decimal format (e.g., 255.255.0.0).
Description	The name to be assigned to the Viper in Tools. This may match the hostname, but does not need to. For example, you can specify a more descriptive name to use across the toolsets.
Gateway	Displays the IPv4 default route to be assigned to this Viper. This is the gateway used to route traffic to destinations beyond the local network. This address must be reachable on your local subnet. NOTE: If DHCP is disabled, you may enter a gateway address in dotted-decimal format.

IP Setting	Description
MAC Address	(Read-only) The Media Access Control address assigned to the Viper's eth0 network interface. This is the physical address of the network interface and cannot be changed.
DNS Servers	(Optional) The IPv4 address of the Domain Name Servers to use.
Search Domains	(Optional) The search strings to use when attempting to resolve when accessing domain names.

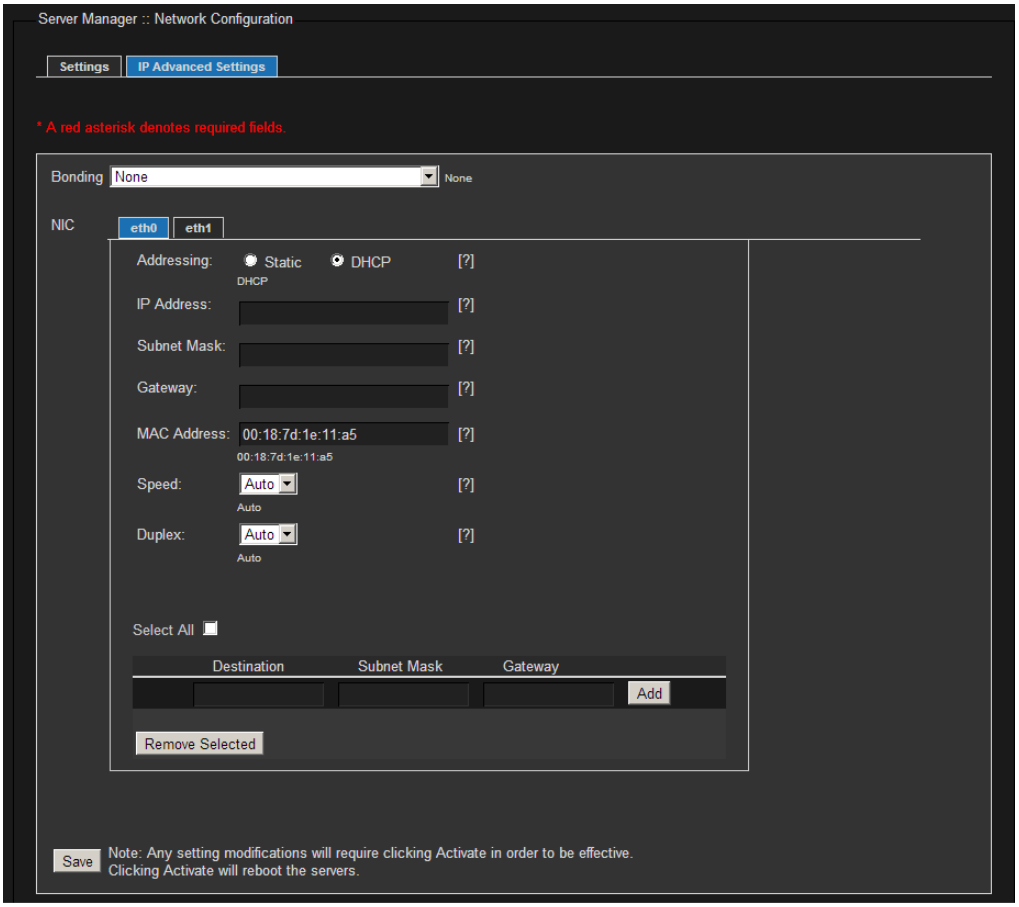
Advanced IP Settings

The Server Manager allows you to configure advanced IP settings for the Viper. This includes setting up multiple network interfaces, NIC bonding, and link negotiation settings, as well as static routes.

To configure advanced IP settings:

1. Click the IP Advanced Settings tab on the Network Configuration page.

   The IP Advanced Settings page opens (shown in the following example).



NOTE The basic IP settings (from the Network Settings page) are mirrored on the IP Advanced Settings page (under Eth0).

2. To configure bonding, select the option appropriate for your network.

TIP Bonding enables an administrator to use more than one physical network port as a single connection. This can be used to increase performance or redundancy of a server.

3. For each destination to add, type in the IP address, Subnet Mask, and Gateway and click Add.
4. To configure additional NICs (Network Interface Cards) for the server, click the next available eth tab and configure the required settings.
5. Click Save.
6. On the Server Manager page, click Activate Changes.

CHAPTER 5: Viper Integration into a Furnace Realm

This chapter provides the information you need to know to integrate a Viper into a Furnace realm.

Topics in this Chapter

Integration Overview 105
- InStream 105
- Conditional Access 105
- Publishing 106
- Authentication 106

Prerequisites 107
- Summary of Steps 107

Setting Up Credentials 110
- Create Viper Credentials (Furnace Credential Manager) 110
- Assign Viper Credentials (Furnace Credential Manager) 112

Invitation Process 114
- Invitation (Furnace Server Manager) 114
- Accept the Invitation (Viper Server Manager) 115
- Configure Viper Permissions (VF Admin) 118

Channel Configuration 119
- Output URLs for Encryption 122

Adding the Viper Channel to the Furnace Lineup 125

Publishing Options 126
- Local Media Server – Playback Review 126
- Publishing 126
- Manually Transferring Assets from a Viper to a Furnace 127

Integration Overview

Viper provides the same Record, Stream and Review capabilities, regardless of whether it is used as a stand-alone appliance or integrated into the Furnace IP video distribution system.

Stored assets still residing in the Viper local media library can be played locally by launching the InStream player from the Viper portal.

The key differences between the two modes involve how Conditional Access is applied, Publishing behaviors, and the enforcement of Username and Password Authentication in a Furnace realm, as discussed in the following sections.

InStream

Once a Viper is part of a Furnace realm, multiple users can view the outgoing streams in the InStream player(s) launched by the Furnace server. The number of players depends on whether the Viper is playing a Multicast stream or a VoD asset:

- While streaming, a stand-alone Viper can launch as many InStream players as there are users (since it is a Multicast stream).
- While playing a VoD (Unicast) asset, a stand-alone Viper can offer up to a maximum of 100Mbits of playback. So the number of InStream players that can be launched depends on the bitrate of the assets being played.

  For example, if the asset is 1Mbit, then 100 InStream players can be launched from the Viper. If the asset is 5Mbits then 20 players can be launched, and so on. If one user launches a 1Mbit asset and another user launches a 10Mbit asset, this would come to a total of 11MBits, leaving 89Mbits remaining to be used by the rest of the users.

Conditional Access

When a Viper is in a Furnace realm, its Conditional Access (CA) entitlements are enforced by the Furnace. If CA is enabled on the Furnace, then administrators will need to set entitlement rights for local Viper assets in the Viper Admin module. When a Viper is not connected to a Furnace, CA is not available (unless the Viper has its own optional CA license).

If an asset is entitled via the Viper Admin module, the entitlement is saved into the Furnace system and when the asset is published to the Furnace, it will still be entitled. Keyword entitlements are not shared between the Furnace and Viper, so if you want to use keywords they must be configured the same on the Furnace and Viper (there is no Viper support).

See “Assign Viper Credentials (Furnace Credential Manager)” on page 112.

Publishing

Viper can be configured to either automatically or manually publish its recorded assets from the Touch Panel to the host Furnace server to which it is associated. This allows a wider audience to review VoD assets through the means of multiple InStream players launched from the host Furnace server.

When a Viper is part of a Furnace realm, assets can also be published from the Web portal to the hosted Furnace server. When the user hovers over a thumbnail or a row in the Viper VoD portal, the information dialog that opens includes a new “VF” option to publish the asset to the hosted Furnace server.

See “Publishing Options” on page 126.

Authentication

The Authentication process is the same for Viper stand-alone and in a Furnace realm when the PIN is used to unlock the Touch Panel.

However, the Authentication behavior for End Users and/or Groups varies, depending on whether the Viper is operating in or outside a Furnace realm.

- When a Viper is joined to a Furnace realm, the authentication is made against the Furnace database. Therefore, authentication on the Touch Panel always requires a PIN + Username and Password, even if the Viper was originally configured for PIN only authentication.
- When a Viper is out of the Furnace realm, the Username and Password are authenticated with the internal database of the Viper. Thus, it behaves the same as a Viper stand-alone in regard to authenticating its end users.

NOTE In the current release, when Viper is part of a Furnace realm, in order to use Guest mode, a “guest” user must exist on the Furnace.

Prerequisites

NOTE Haivision recommends that anyone undertaking the configuration of Viper streams have a basic knowledge of Internet Protocol (IP) Multicast.

These configuration steps require that you have access to both the Viper and Furnace Tools portals.

In the Furnace, you will need to access the following modules:

- Credential Manager located under: Tools > VF Admin > Authentication
- Server Manager located under: Tools > VF Admin > General
- Channel Editor located under: Tools > VF Channel Manager
- Lineup Editor located under: Tools > VF Channel Manager

For each Viper to integrate, you will need to access the following modules:

- Server Manager located under: Tools > Viper Admin > General
- Channel Editor located under: Tools > Viper Channel Manager
- Lineup Editor located under: Tools > Viper Channel Manager

Summary of Steps

This section summarizes the steps you need to follow in order to integrate one or more Viper(s) into the realm of a Furnace server. As required, this section provides links to detailed sections.

Set REST API Version to 2.0 (from the host Furnace)

- From the Furnace that will invite the Viper into its realm, set the Select Rest API Version to 2.0 (Authentication Enabled) (from VF Admin > Configuration) to allow the Viper to connect to the Furnace.

Set Up Credentials (from the host Furnace; then the Viper)

- Create Viper Credentials (Furnace Credential Manager):
  From the Furnace that will invite the Viper into its realm, create credentials for authorization (from VF Admin > Credential Manager).

  Later from the Viper, you will need to enter these credentials (consisting of a Consumer Key and Secret pair) when confirming the invitation.

- Assign Viper Credentials (Furnace Credential Manager):
  Assign Viper credentials to a group with administrative permissions (from VF Admin > Credential Manager).

Invite the Viper into the Furnace Realm (from the host Furnace)

- Invitation (Furnace Server Manager):
  From the host Furnace server, invite the Viper appliance into its realm (from VF Admin > Server Manager).

Join the Furnace Realm (from Viper)

- Accept the Invitation (Viper Server Manager):
  From the Viper, accept the invitation to join the Furnace realm (from Viper Admin > Server Manager). This includes selecting the Join Method (either Automatic or Manual).

  Once the Viper accepts the invitation, you will need to log in again (i.e., log out and then re-authenticate after joining the realm) using the Furnace Username and Password.

Configure the Viper Permissions (from the Furnace)

- Configure Viper Permissions (VF Admin):
  Next from the Furnace, assign the appropriate Viper Touch Panel permissions to individual users or groups (from Furnace > VF Admin > Group or User Permissions).

Configure the Viper Channels (from the Viper)

- Configure Viper Channels (Viper Channel Editor):
  From the Viper (Channel Manager > Channel Editor), modify the Output URL (i.e., the broadcast IP) for each of the Viper channels to avoid conflicts with multiple Vipers.

Add/Configure Viper Channels (from the Furnace)

- Add Viper Channels to Furnace (Furnace Channel Editor):
  From the Furnace (VF Channel Manager > Channel Editor), add and configure the Viper Channels.

Create the Channel Lineup (from the Furnace)

- Adding the Viper Channel to the Furnace Lineup:
  From the Furnace (VF Channel Manager > Lineup Editor), add the Viper channel to the Furnace Channel Lineup.

Define the Publishing Method and Destination (from the Viper)

- From the Viper (Admin > Configuration), define the Viper Publishing Method (either Automatic or Manual: Automatic goes to the Viper Publishing Destination; Manual lets users decide). If set to Automatic, next define the Viper Publishing Destination (either Furnace or Viper).

Define PIN and Password vs. PIN only (from the Viper)

- From the Viper (Admin > Configuration), define whether users can access the Touch Panel by entering both a PIN and Password, or PIN only. Note that if the Viper is integrated into a Furnace realm, PIN and Password is always required. (The Viper will use the Username and Password of the host Furnace in order to complete its authentication procedures.)

Setting Up Credentials

Create Viper Credentials (Furnace Credential Manager)

To get started, from the Furnace, you need to generate API credentials for authentication for each Viper to integrate into the Furnace realm.

To create Credentials for a Viper:

1. Open the Furnace Launch portal and sign in using an administrative account.
2. Click Tools to open the Furnace Tools page.

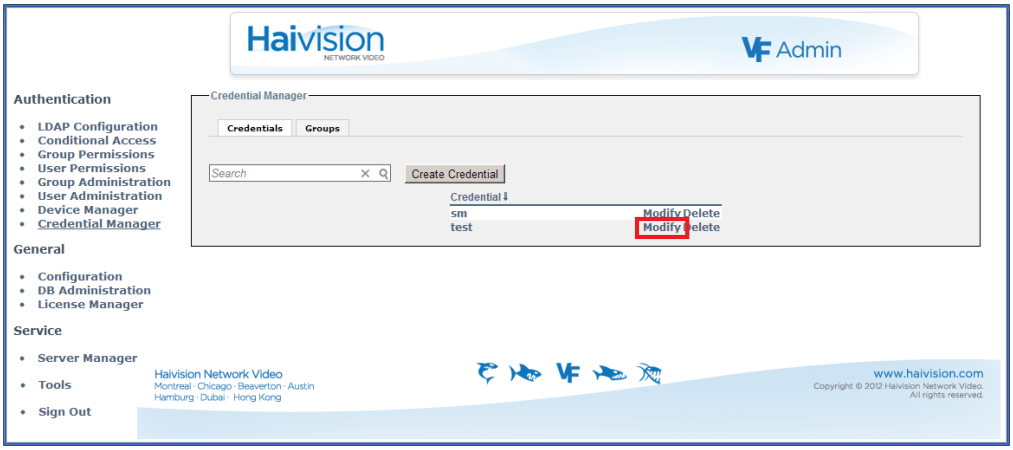
3. On the Tools page, click the VF Admin icon.
4. On the VF Admin page, click the Credential Manager link (on the left side under Authentication).

5. Follow the steps to create an API credential in the Furnace Administration Guide in the section “Managing API Credentials”.

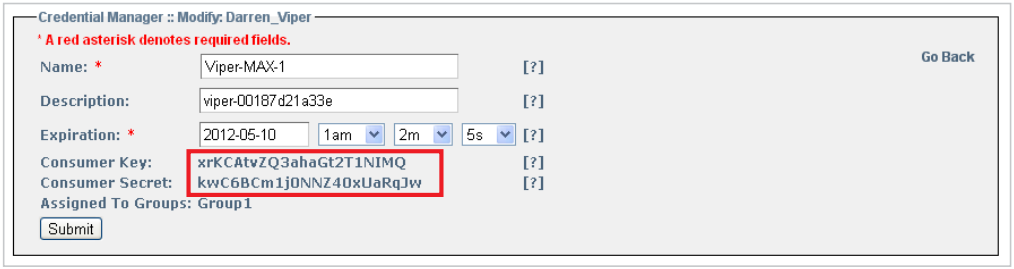
TIP We recommend that you give each credential a name and description that indicates the Viper to which it is dedicated.

You will need to copy the Consumer Key and Secret pair for each credential that you create.

6. To view the Consumer Key and Secret pair for a credential, on the Credential Manager page, click Modify next to the credential name.



The Modify Credential page opens showing the Consumer Key and Consumer Secret generated for this credential (shown in the following example).



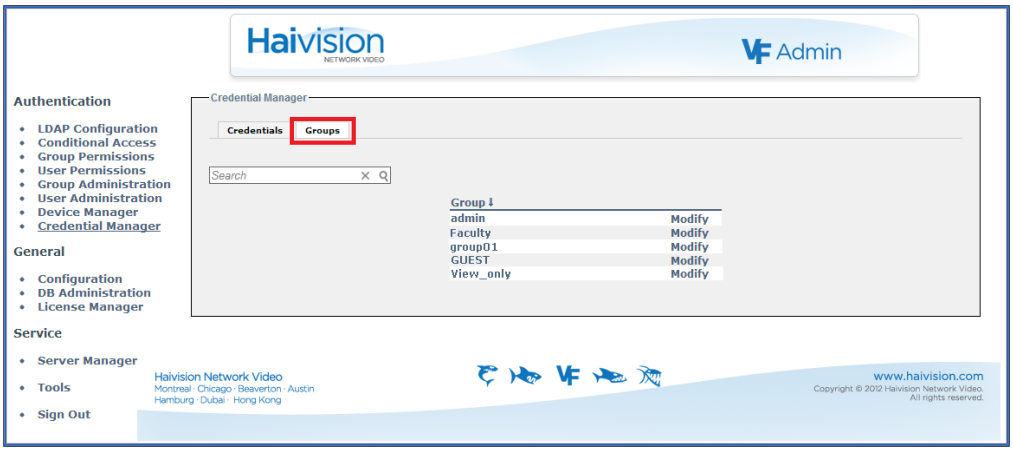
7. Jot down or make a copy of the Consumer Key and Consumer Secret. They will be needed when the targeted Viper accepts the invitation from the Furnace server.

Assign Viper Credentials (Furnace Credential Manager)

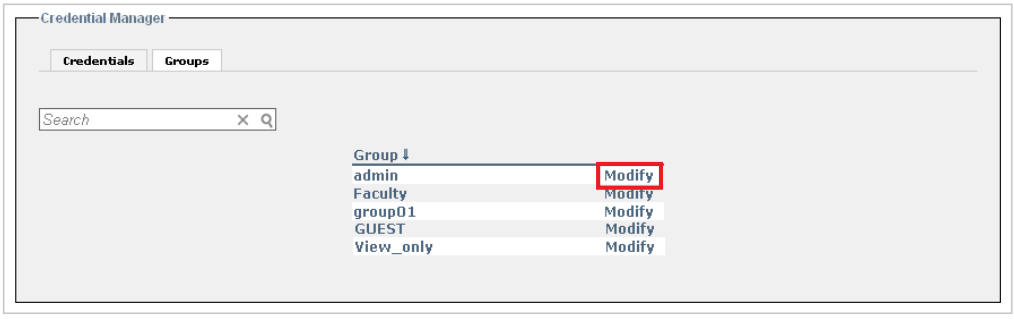
Next you need to assign the Viper credentials to a Furnace group with administrative permissions.

To assign the Viper Credentials to a Furnace Group:

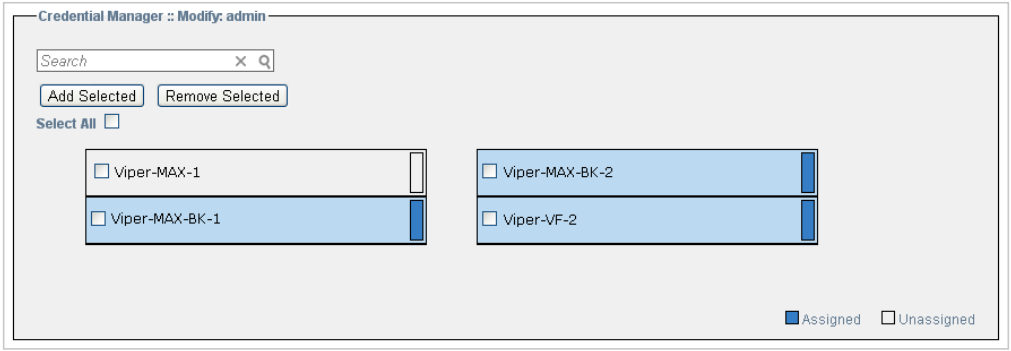
1. On the Furnace Credential Manager page, click the Groups tab and locate the group to which your Users are assigned in VF Admin.



2. To add the credential to the group, click Modify next to the group name.



The Modify Group page opens displaying the current list of defined credentials for your system. Credentials that are part of the group are highlighted in blue (as shown in the example on the following page).



3. Check the name of the credential to add to the group and click Add Selected.

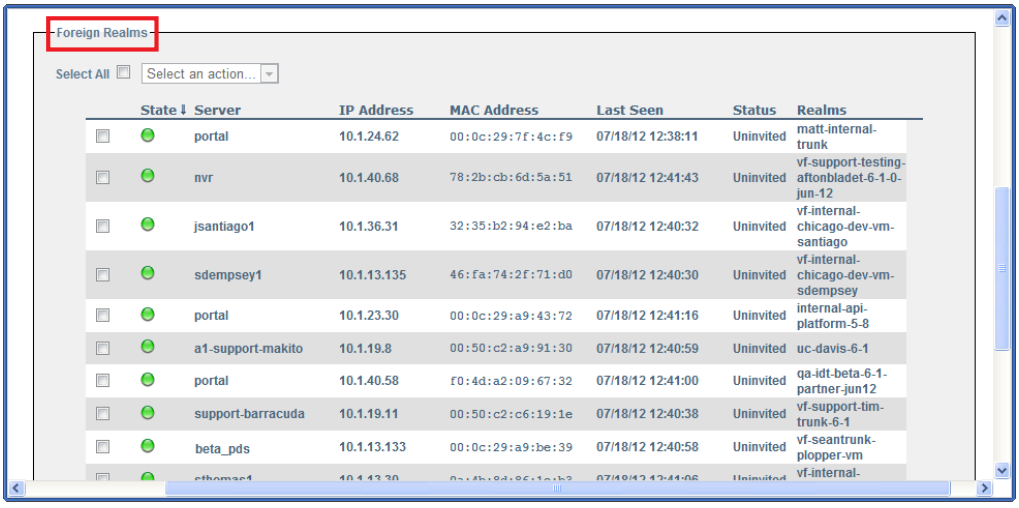
Invitation Process

Invitation (Furnace Server Manager)

The next step is to invite the Viper into the Furnace realm from the Furnace Server Manager module.

1. On the Furnace Tools page, click the VF Admin icon.
2. On the VF Admin page, click the Server Manager link (on the left side under Service).

3. Locate the name of the Viper (or Vipers) in the Foreign Realms section at the bottom of the Server Manager page.



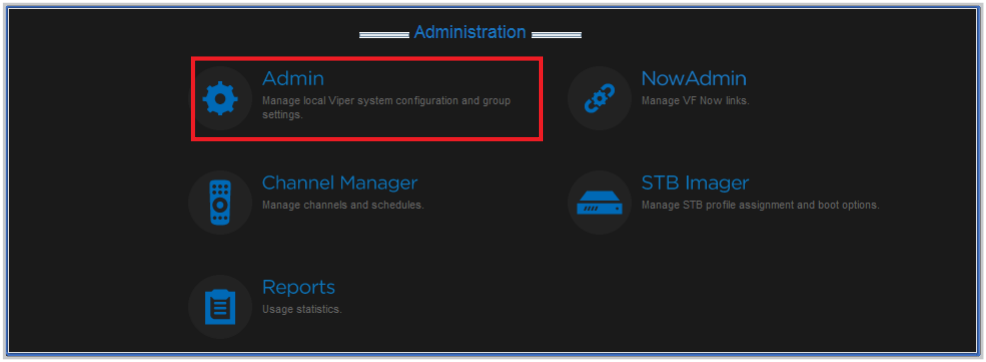
4. Select the Viper(s) to invite into the Furnace realm and click the Invite Selected button.

Accept the Invitation (Viper Server Manager)

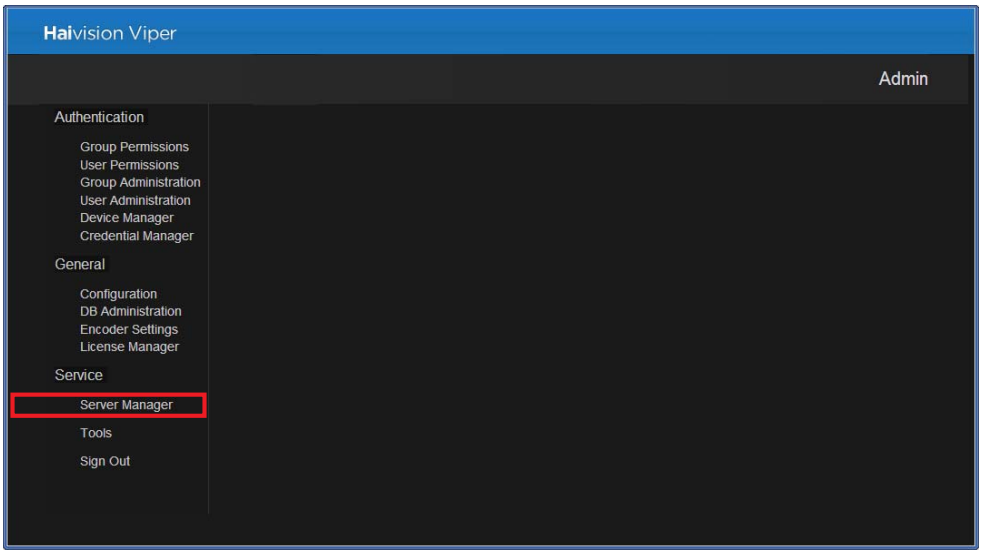
Now you can accept the invitation from the Viper Server Manager module.

TIP It may take a minute or two for the invitation to show up in the Viper. You may need to refresh the page until the invitation is available.

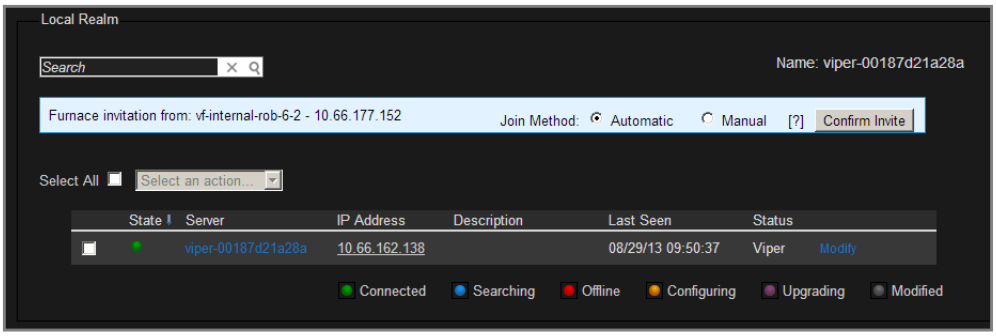
1. Open the Viper Launch portal and sign in using an administrative account.
2. Click Tools to open the Viper Tools page.
3. On the Tools page, click the Admin icon.



4. On the Admin page, click the Server Manager link (on the left side under Service).



Each Viper to which an invitation has been sent from the Furnace will display an Invitation message highlighted in a blue box located at the top of the Server Manager page (as shown in the following example).



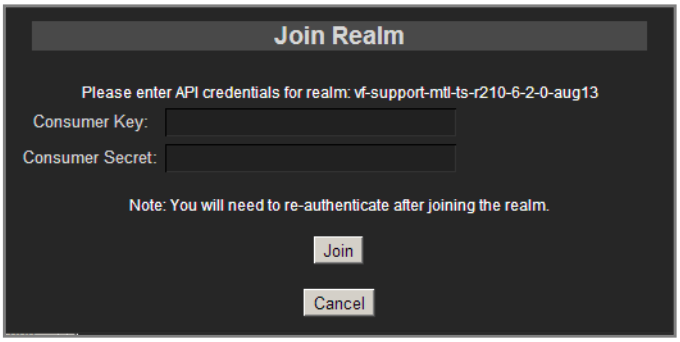
5. To accept the Furnace invitation, select the Join Method: either Automatic or Manual. This determines whether the Viper will re-join the Furnace realm automatically or manually following a reboot.

   - Automatic: You will not need to "re-accept" another Furnace invitation to re-join the Furnace realm.
   - Manual: The acceptance process will need to be confirmed manually every time.

   You will need to restart the Viper Touch Panel application in either mode when you first join.

6. Click Confirm Invite.

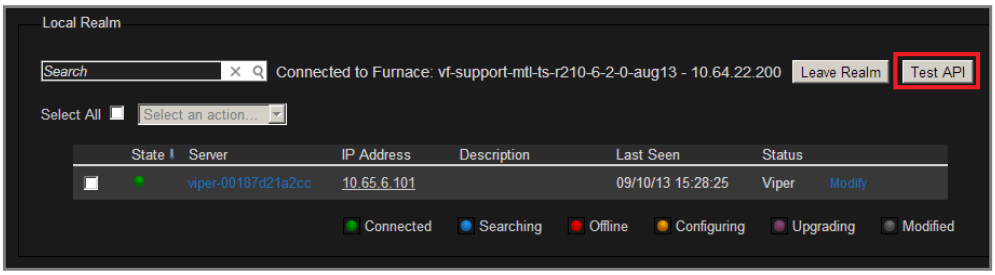
7. At the confirmation stage, on the Join Realm dialog, paste in the Consumer Key and Consumer Secret previously created in the Furnace Credential Manager (copied in Step #7 in the section "Create Viper Credentials (Furnace Credential Manager)").



8. Click Join.

9. You will need to log in to the Viper again (i.e., to re-authenticate after joining the realm) using the Furnace Username and Password.

10. To test the API credentials, at the top of the Server Manager page, click Test API.



TIP If the test fails, make sure you have correctly completed the steps in the section "Assign Viper Credentials (Furnace Credential Manager)".

11. To leave the realm, at the top of the Server Manager page, click Leave Realm and then click Yes on the dialog.

If you leave the realm from the Viper Admin page, the Viper will disassociate itself from the Furnace realm and clear the stored API credentials. This step should only be necessary if the Viper is permanently leaving the Furnace realm.

NOTE Leaving the realm from the Viper Admin page does not clear the invitation on the Furnace side. The next time the page is loaded, it should once again show an open Furnace invitation.

Configure Viper Permissions (VF Admin)

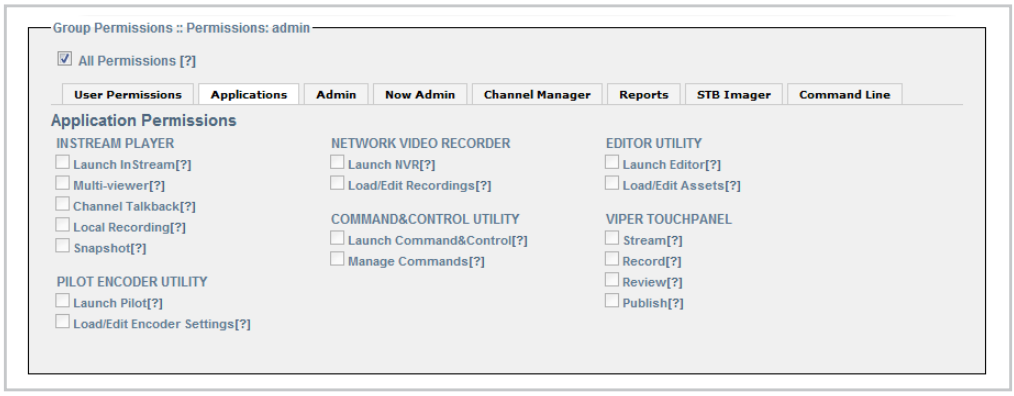
To assign Viper Touch Panel Permissions to a Furnace User:

1. From the Furnace Tools page, click the VF Admin icon.
2. Click the User Permissions link on the left side of the VF Admin page.
3. Click Modify next to the user name.

   The Modify User Permissions page opens (showing the User Permissions tab).
4. For each tabbed section, check all boxes that apply to define the user permissions.

NOTE When Viper is joined to a Furnace realm, non-admin Furnace users or groups require additional permissions to be able to publish to the Furnace.

5. Click the Applications tab (shown below). Then under EDITOR UTILITY, check the Load/Edit Assets checkbox.



For more information, please refer to the Furnace Administration Guide, Chapter 3 “Initial System Setup: Configuring Permissions for Groups or Users”

Channel Configuration

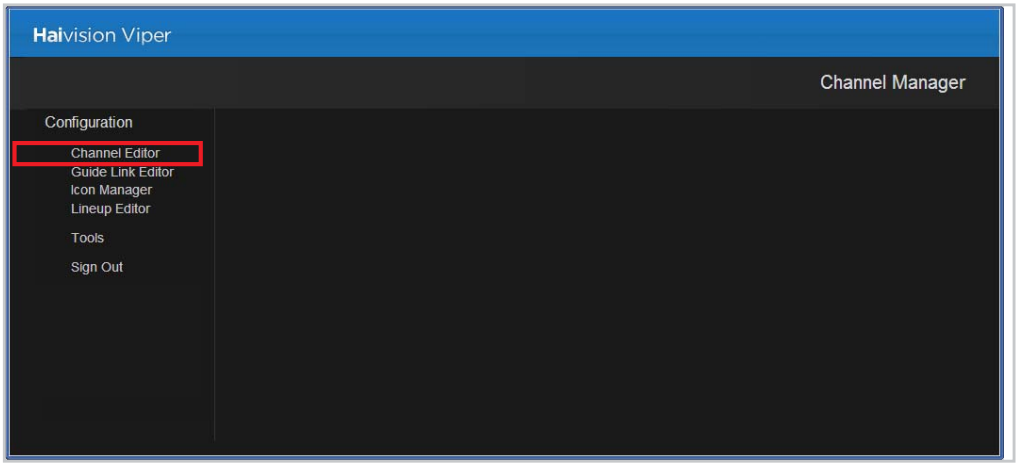
Configure Viper Channels (Viper Channel Editor)

In this step, you will modify the default Viper channel configuration to meet your system and network requirements.

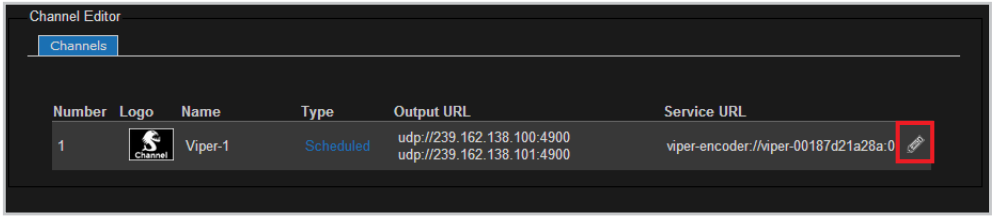
IMPORTANT Make sure that each Channel has its own unique Output URL.

To edit the Viper channel:

1. From the Viper Tools page, click the Channel Manager icon.
2. On the Channel Manager Welcome page, click the Channel Editor link (on the left side).

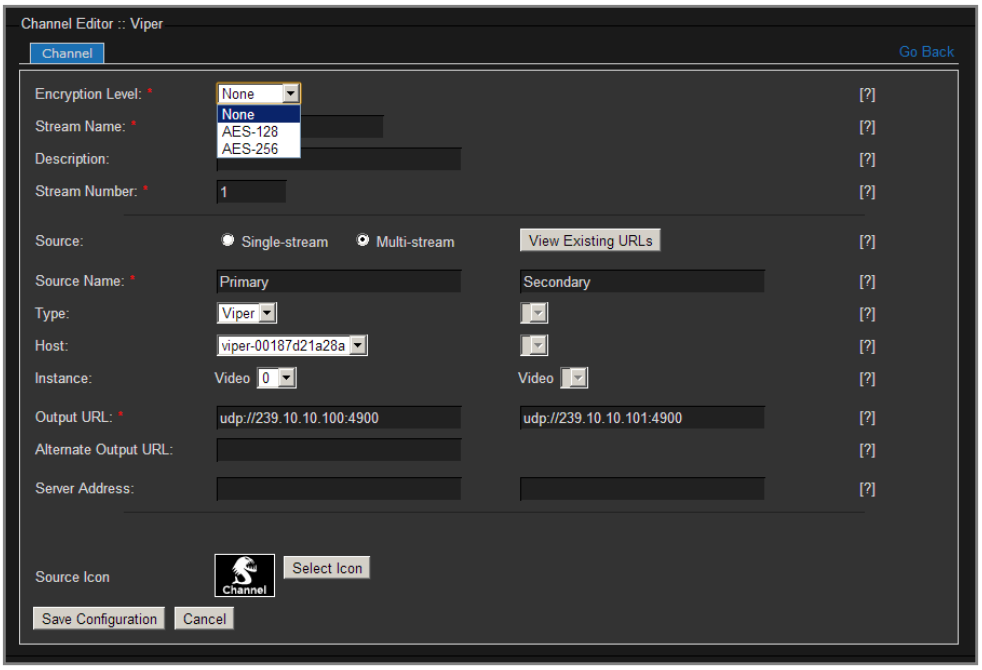


The Channel List (shown in the example below) displays the Viper channel and Output URL links that are defined on the license server.



3. Click the Edit icon .

The Channel Editor page opens (as shown on the following page).



4. Select the Encryption Level for the stream: [AES refers to Advanced Encryption Standard.] See "Output URLs for Encryption" on page 122.
   - None: Encryption is disabled.
   - AES-128: 10 cycles of repetition for 128 bit keys.
   - AES-256: 14 cycles of repetition for 256 bit keys.
5. Enter unique values for:
   - Stream Name
   - Stream Number
6. For the Source, select either Single-stream or Multi-stream. By default, the Viper is set in Multi-stream mode.

   It is recommended to keep the Viper configured to Multi-stream Source as it is the standard way of using a Viper channel. However, if you switch to Single-Stream, keep in mind that this will only provide a single channel.
7. For the source Type, select Viper, if not already selected.

NOTE Audio and video sources must be physically connected to the Viper.

8. For the Host, select the server name of the Viper you want to configure. Typically it is the only server name in the list since you are still configuring the Viper and not yet on the Furnace Channel Editor page.

NOTE In the current release, Viper in a Furnace realm cannot use Talkback. Only Viper Stand-Alone can use Talkback.

9. For the Output URLs, you will need to change the default addresses to meet your network environment requirements.

   The Vipers are shipped with Default addresses of Primary channel udp://239.10.10.100:4900 and Secondary channel udp://239.10.10.101:4900.

   Modifying these addresses will create distinct channels for each Viper and allow for them to be monitored from an InStream player launched from a Furnace server.

10. Click Save Configuration. (Do not exit the page without saving; otherwise, the new information will be lost.)

Output URLs for Encryption

The following table lists the supported Output URLs when enabling encryption on the Viper's channel:

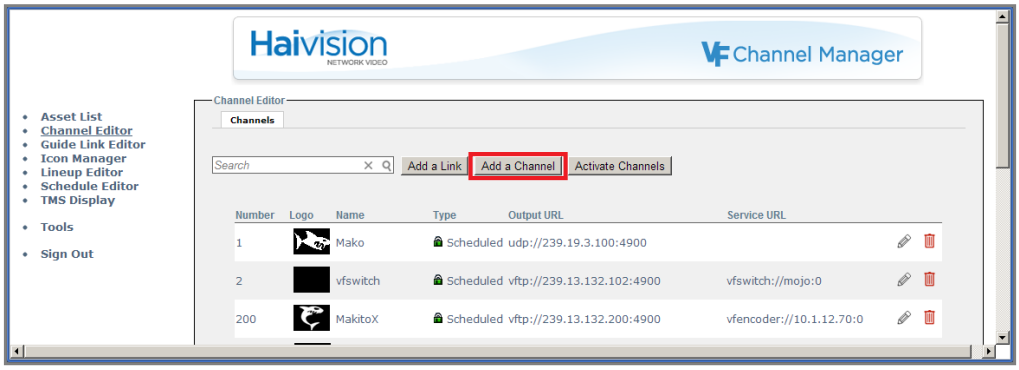
Application Mode	URL Type	Usage and Example
Touch Panel – Stand-Alone	udp://	Use when Encryption is enabled on the Viper channel (from the Viper Channel Editor). udp://239.100.100.100:4900
Touch Panel – Furnace Realm	udp://	Use when Encryption is enabled on the Viper channel (from the Furnace Channel Editor). udp://239.100.100.100:4900
REST API – Stand-Alone	vfudp://	Use when Encryption is enabled on the Viper channel (from the Viper Channel Editor). vfudp://239.100.100.100:4900
REST API – Furnace Realm	vfudp://	Use when Encryption is enabled on the Viper channel (from the Furnace Channel Editor). vfudp://239.100.100.100:4900

NOTE Encrypted streams from the Touch Panel application are not compatible with Furnace services such as Bridge, which require encrypted streams to be sent using VFUDP.

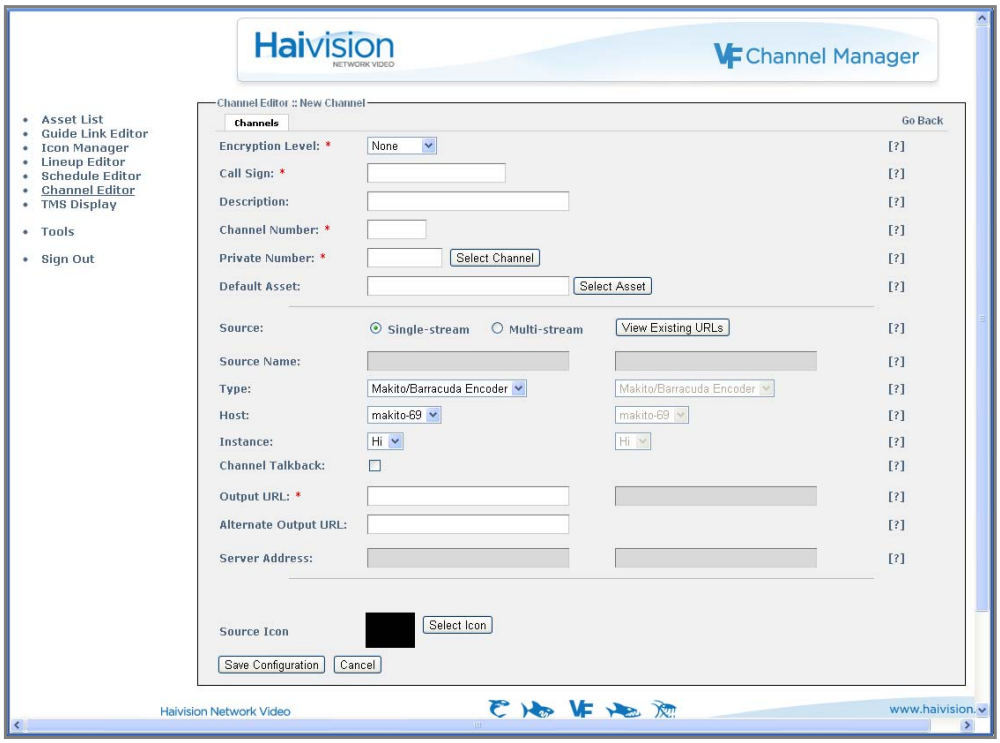
Add Viper Channels to Furnace (Furnace Channel Editor)

Next you need to add the Viper Channels to the Furnace.

1. From the Furnace Tools page, click the VF Channel Manager icon.
2. On the VF Channel Manager Welcome page, click the Channel Editor link (on the left side).
3. On the Channel List page, click Add a Channel.



You will see a page similar to the Viper Channel Editor. Except here, there is no information already filled-in. You will need to add the information relevant to each Viper stream.



4. Set the Encryption Level to either None, AES-128, or AES-256. See "Output URLs for Encryption" on page 122.
5. Enter a Call Sign. This is a short Channel name that will appear in the InStream channel guide.
6. Set the Channel Number. This can be any number that fits into your Lineup.
7. Set a Private Channel Number. This is a number starting at 10000 and beyond.
8. Enter a Source Name for each channel. This is the name which will show up in the Lineup of the Furnace InStream player.
9. For the Type, select Viper.
10. Select the Host corresponding to the Viper from which the streams are to be pulled.

    You will have more than one instance to select if you have a group of Vipers integrated with the Furnace server.

    The Hostname should be sufficiently descriptive to allow the end user to select the correct Viper.
11. Type in the Output URL in order to match the address conventions of your network.
12. Click Save Configuration.

Adding the Viper Channel to the Furnace Lineup

Next you need to add the Viper channel to the Furnace Channel Lineup. This step allows InStream players launched from the Furnace server to include in their Lineup the channels of the Vipers integrated into the Furnace realm.

1. On the VF Channel Manager page, click the Lineup Editor link (on the left side).

   The Lineup Editor page opens with the “default” lineup selected.

2. Select the Lineup to modify from the Lineup Name drop-down menu on the right. In most cases, you should edit the “default” lineup.
3. Drag the new Viper channel from “Source Items” to “Current Lineup”
4. Click Save Lineup.

To test the Lineup selection:

1. Launch InStream.

   At this stage, you will see the new channels in the InStream Lineup (but no video in the player(s)).

2. From the Viper Touch Panel interface, select the Source input.(Follow the steps in the Viper Getting Started Guide to set up streaming.)
3. On the Stream & Record Activity screen, touch the Stream button.

If the lineup selection is successful, you should see the Streams coming out of the Viper via the InStream player.

Publishing Options

Local Media Server – Playback Review

From the Touch Panel interface, users can review stored assets still residing in the Viper local media library, which have yet to be published to a host Furnace.

Once a recording is completed, users can review the content in order to decide if it is worth publishing, storing locally, or simply deleting (see NOTE below). The Touch Panel interface provides “trick play/DVR” capabilities (such as Fast Forward, Rewind, and Pause) and a “scrub” bar to navigate the recordings.

NOTE There is no Delete button in the Touch Panel interface. The only way to delete an asset from a Viper is through the Web portal. When the user hovers over a thumbnail or row in the Viper VoD portal, the information dialog that opens includes an “X” icon, representing the Delete function (if the user has been given permissions).

Assets which are automatically published to a Furnace are not deleted from the Viper.

Publishing

In order to share the recorded assets from a Viper in a Furnace realm with a wider audience, those assets have to be “published” to a Furnace server. The assets will then be available for viewing through multiple InStream players launched from the Furnace server.

The Viper can be configured (Admin > Configuration) to either automatically or manually publish its recorded assets to its host Furnace server.

- If configured to Manual, once a recording session on a Viper is completed, on the Touch Panel interface, you will see a Publish button on the Browse Assets screen. Select the asset to publish and touch Publish.
- On the Publish screen, you will see either a Viper> button or two buttons (Viper> or Furnace>, depending on whether the Viper is part of a Furnace realm).
- When you select one of these buttons, the asset will be published and you will see a new screen with a Publishing progress bar. [Note that publishing to the Viper is fast, while publishing to the Furnace is rate limited.]

NOTE The host Furnace server is the master repository of all the available VoD assets, if and when, several Vipers are included in its realm.

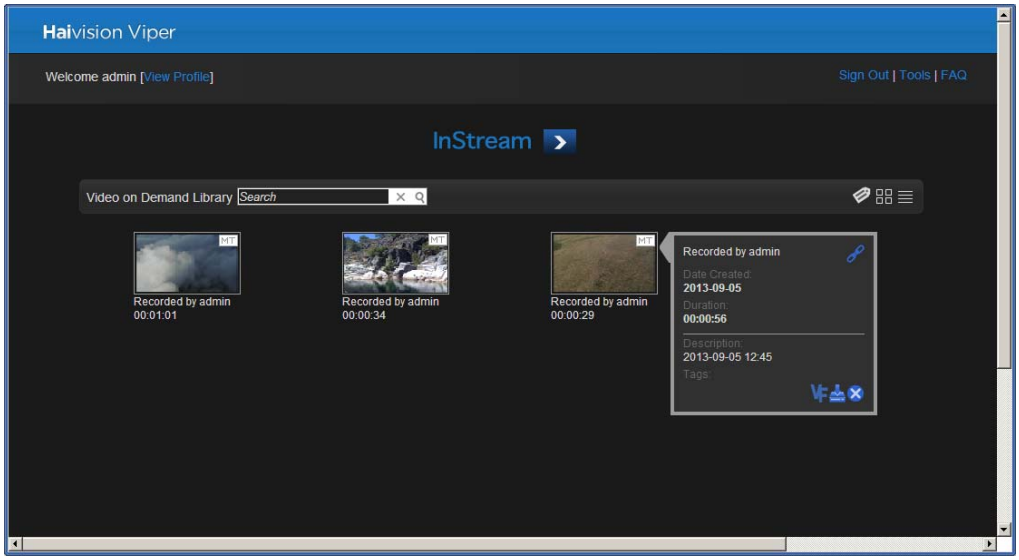
Manually Transferring Assets from a Viper to a Furnace

From the Touch Panel

To manually transfer assets from the Viper Touch Panel (on a Viper in a Furnace realm), please refer to the Viper Getting Started Guide.

From the Web Portal

To transfer an asset from the Web portal page, you can use the Export/Publish function available when you hover over a thumbnail or a row. If your Viper is part of a Furnace realm, the information dialog that opens includes an additional option to “publish” the asset to the host Furnace server.



When you click the  option, the selected asset will be published to the host Furnace media server.

CHAPTER 6: Configuring Channels

Viper provides a full suite of remote administration tools via the Tools portal. This chapter describes the tools available to system administrators to configure channels for live video.

Topics In This Chapter

Channel Editor - Configuring Channels 129
Live Channels - Editing the Viper Channel 131
Channel Editor Settings 133
Setting Up InStream Talkback 135
Icon Manager - Managing Channel Icons 137
Icon Manager Error Messages 138
Lineup Editor - Managing the Channel Lineup 140
Creating Channel Lineups 140

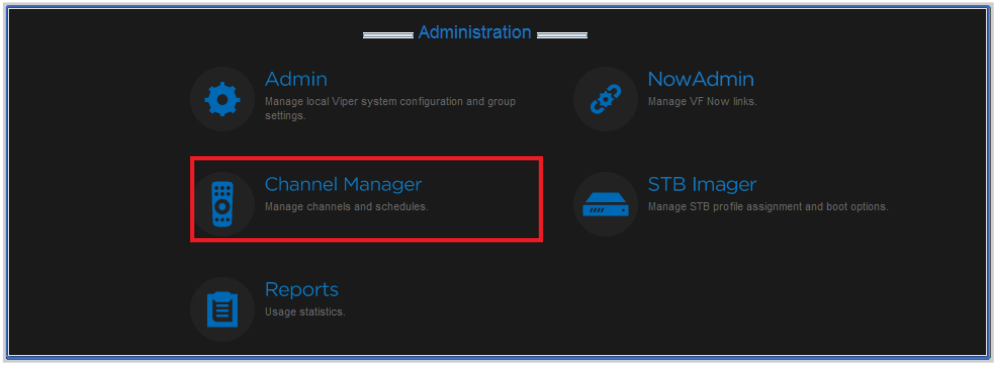
Channel Editor - Configuring Channels

The Channel Editor is used modify the default Viper channel configuration to meet your system and network requirements.

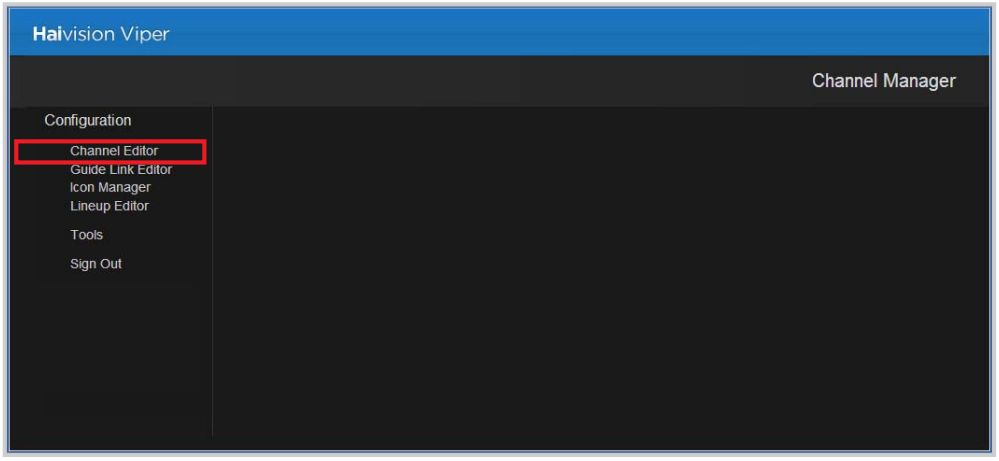
IMPORTANT Make sure that each Channel has its own unique Output URL.

To display the channel list:

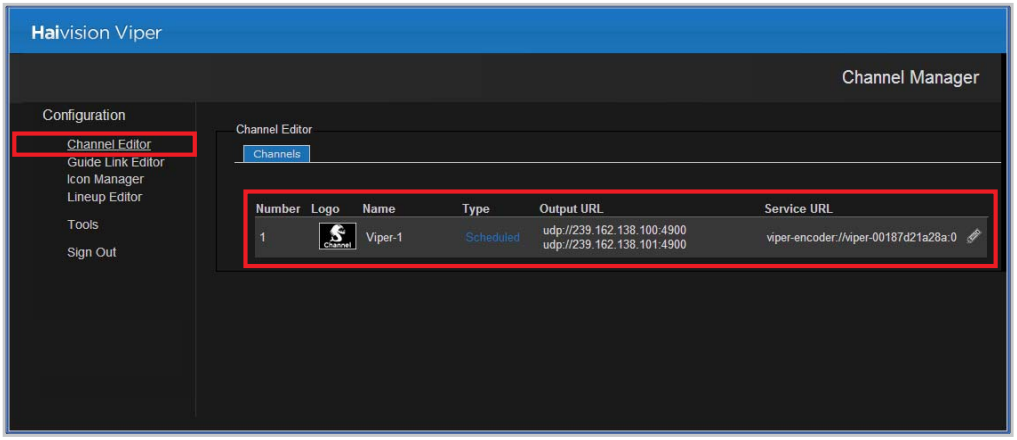
1. On the Tools page, click the Channel Manager icon.



2. Click Channel Editor on the left side of the Channel Manager Welcome page.



The Channel List (shown in the following example) displays the Viper channel and Output URL links that are defined on the Viper.

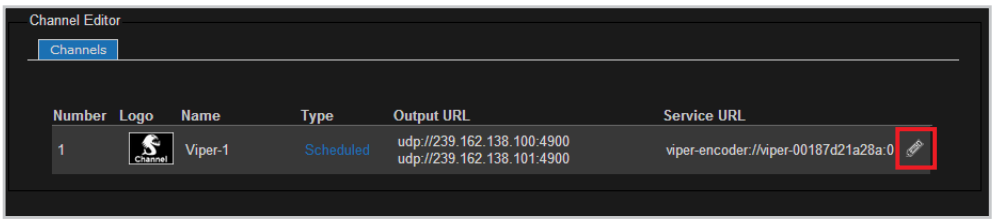

Haivision Viper
Channel Manager
Configuration
Channel Editor
Guide Link Editor
Icon Manager
Lineup Editor
Tools
Sign Out
Channel Editor
Channels
Number
Logo
Name
Type
Output URL
Service URL
1
Viper-1
Scheduled
udp://239.162.138.100:4900
udp://239.162.138.101:4900
viper-encoder://viper-00187d21a28a:0

Live Channels - Editing the Viper Channel

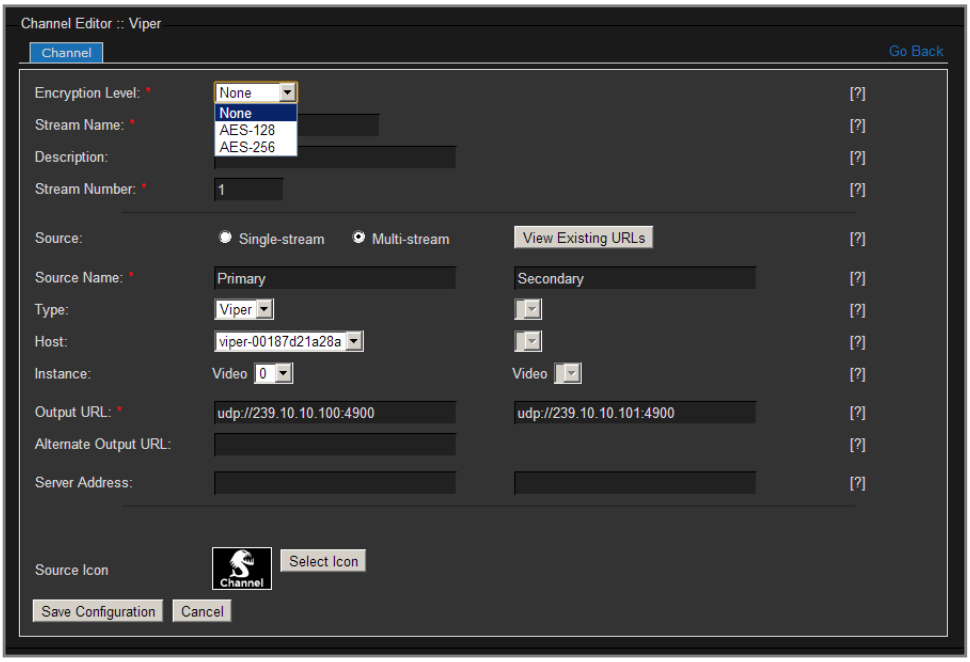
This section describes how to edit the Viper channel. For example, to configure more than one Viper on the same network, you need to assign a unique multicast stream address to each Viper (from each Viper's Channel Editor).

To edit the Viper channel:

1. On the Channel List page, click the Edit icon .



The Channel Editor page opens.



2. Follow these steps to edit the channel. For details, see "Channel Editor Settings" on page 133.
3. Select the Encryption Level for the stream: [AES refers to Advanced Encryption Standard.] See "Output URLs for Encryption" on page 122.
   - None: Encryption is disabled.
   - AES-128: 10 cycles of repetition for 128 bit keys.
   - AES-256: 14 cycles of repetition for 256 bit keys.

4. Enter unique values for:
   - Stream Name
   - Stream Number
5. For the Source, select either Single-stream or Multi-stream. By default, the Viper is set in Multi-stream mode.

   It is recommended to keep the Viper configured to Multi-stream Source as it is the standard way of using a Viper channel. Note that the Touch Panel settings override the Single-stream/Multi-stream setting in the Channel Editor (e.g., if you stream two inputs, you always get multi-stream). However, the REST API uses the Single-stream/Multi-stream setting.
6. To enable Audio Talkback to the Viper, check the Channel Talkback checkbox. For more information, see "Setting Up InStream Talkback" on page 135.

NOTE In the current release, Viper in a Furnace realm cannot use Talkback. Only Viper in stand-alone mode can use Talkback.

7. For the Output URLs, you will need to change the default addresses to meet your network environment requirements.

   The Vipers are shipped with Default addresses of Primary channel udp://239.10.10.100:4900 and Secondary channel udp://239.10.10.101:4900.

   Modifying these addresses will create distinct channels for each Viper on a network. See "Output URLs for Encryption" on page 122.
8. Click Save Configuration. (Do not exit the page without saving; otherwise, the new information will be lost.)

NOTE For a Viper residing in a Furnace realm, the Viper channels are expected to be monitored from the InStream players launched from the Furnace server.

Channel Editor Settings

The following table lists the Channel Editor fields:

Channel Editor Field	Description
Encryption Level	The encryption level for the stream. Select either None, AES-128 or AES-256.
Stream Name	Type in a brief channel name that will appear in the Channel Lineup and Set-Top Box channel guide.
Description	(Optional) Enter a short description for the channel.
Stream Number	A traditional channel number that will appear in the Set-Top Box channel guide.
Source	Select either Singlestream or Multi-stream. A Multistream channel will combine the output of two encoded sources connected to the Viper interfaces. TIP: Clicking View Existing URLs opens the Channel Display list. From here you can check the URLs currently in use by the system, which is helpful when entering the Output URLs.
Source Name	(Multistream channels only) Type in a unique name for each Multistream source. NOTE: These names will be listed in the Set-Top Box channel guide.
Type	(Read-Only) The device type is Viper. Sources must be physically connected to the Viper.
Host	Select the host name from the list of connected servers in the realm that provide the desired service. (Read-Only) The Host is the server name of the Viper you are configuring.
Instance	(Read-Only) The encoder Instance to use for the service assignment.
Channel Talkback (checkbox)	Check to enable Audio Talkback to the Viper that is streaming the content that InStream users are viewing. For more information, see "Setting Up InStream Talkback" on page 135.
Output URL	Defines the multicast output address and stream parameters for this service. Enter a UDP URL (e.g., udp://239.1.1.100:4900). (Multistream channels) Enter a secondary output URL.

Channel Editor Field (Cont.)	Description
Alternate Output URL	Enter an additional channel output address.
Server Address	The channel's service assignment.

Setting Up InStream Talkback

NOTE In the current release, Talkback does not work when the Viper is part of a Furnace realm.

Talkback allows end users monitoring a Viper session through an InStream software player to reply back (audio only) directly to the individuals at the video source, via a speaker or headphones connected to the Viper appliance.

The audio will be encoded and sent via unicast UDP to the Viper sourcing the stream they are viewing (as shown in the following diagram). The audio will play out of the Viper's audio output device. Talkback is "First-In/First Served", meaning that only one user can use the return audio channel at a time.

The audio is only sent to the source Viper. It is *not* distributed to other viewers of the stream.

Talkback features and requirements include:

- Supported by InStream on Windows 7 only. (Linux, Mac OS X and Stingray STBs are not supported.)
- InStream users must have direct network access to the Viper sourcing the stream, over UDP port 9177. Note that InStream does not allow for port changes. Also, the Talkback feature needs to be enabled on the Viper (using the Viper's Channel Editor).
- Entitlement for Talkback use can be restricted to certain groups or users by an administrator using Viper Admin. (Groups/users with Talkback permissions are authorized to talk back on the Viper's Channel.)

To Set Up InStream Talkback:

1. Make sure Viper users are entitled for Talkback. (Open Viper Admin and modify the relevant User or Group Permissions: under Applications> INSTREAM PLAYER, check the Channel Talkback checkbox.)
2. Enable Talkback on the Channel. (In Viper Channel Manager, edit the Viper's Channel and check the Channel Talkback checkbox.
3. Connect a speaker or headphones to the Viper's audio output.

   The following picture illustrates a sample signal path from the Audio Source through the Viper's audio output when using the InStream Talkback feature.

Figure 6-1 Audio Talkback Signal Path

CAUTION Unplugging or disabling the microphone while using InStream Talkback could cause InStream stability issues. Users should not unplug or disable their microphones while holding down the Talkback button (on the InStream player window). However, there is no problem with unplugging the microphone while using InStream as long as they are not actively using Talkback.

Icon Manager - Managing Channel Icons

The Icon Manager provides a tool to view, add, replace and delete your own custom Channel icons.

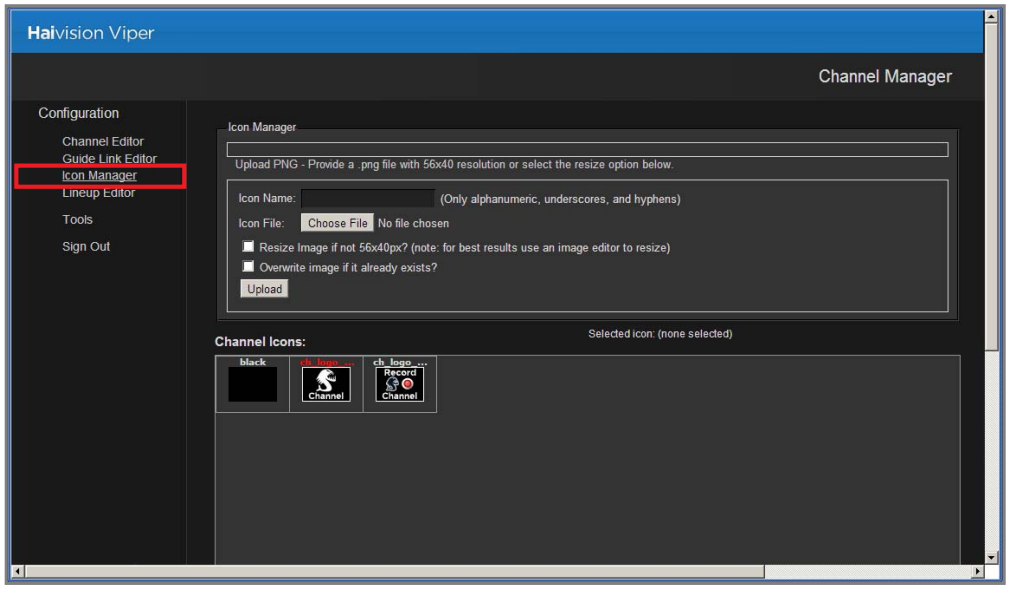
The required resolution for each channel icon is 56 pixels wide by 40 pixels high, and the required icon file type is portable network graphics (PNG) format. The file size must be less than 300 kilobytes.

The Icon Manager provides options to replace an existing image or resize a larger image to the required dimensions. If greater control over image quality is desired, scale the image to the proper dimensions with an image editor before uploading.

To view the Channel icons for your system:

1. Click Icon Manager on the left side of the Viper Channel Manager page.

   The Icon Manager page opens.



To upload a new icon:

1. Type in a name for the icon in the Icon Name field.
2. Click Browse to select a valid icon file.

TIP If your icon file image resolution is different than 56 x 40px or unknown, check the Resize Image checkbox to enable the Icon Manager to scale the image to the required size.

---

3. Click Upload to upload your icon.

When the icon has been successfully uploaded, an “Icon uploaded successfully” status message appears at the top of the page and the icon appears in the Channel Icons list.

The Icon Manager lists custom icons ahead of the default system icons in the Channel Icons grid. The icon is now available for assignment to a channel using Channel Editor.

When your icon has been uploaded properly, the Icon Manager displays a success message, as shown in the previous image. Otherwise an error message displays (list of possible error messages shown in the following section “Icon Manager Error Messages”).

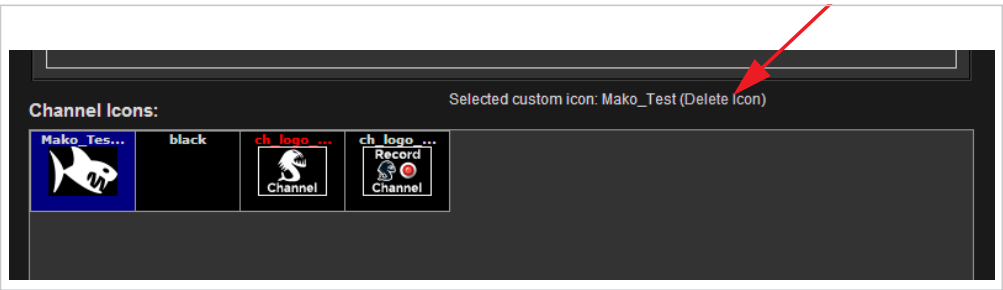
The Icon Manager prevents you from overwriting the default system icons.

To delete an icon:

On the Channel Icons grid, the selected icon is blue, as shown in the following image. Above the grid, a prompt displays the icon name and whether it is in use.

Icons that are assigned to a channel may not be deleted until they become unassigned. If the icon is unassigned, the prompt displays the icon name and a Delete Icon link.

1. To delete an unassigned icon, click the associated Delete Icon link.



2. On the confirmation dialog, click Delete Icon to delete the icon from the system.

If an error occurs during deletion, an error message displays at the top of the page.

The Icon Manager prevents you from removing default system icons.

Icon Manager Error Messages

The following table lists the Icon Manager error messages:

Icon Manager Error Message	Description
Error: Empty Icon Name Field	The Icon Name field was empty when the Upload button was clicked.
Error: Icon File unspecified	The Icon File field was empty or contains a bad filename.
Error: Icon File is invalid	The Icon File field contained an irresolvable file path or URL.

Icon Manager Error Message	Description
Error: Icon File must be PNG format	The icon file provided was not a PNG formatted file.
Error: Icon File is larger than 300KB	The icon file is larger than 300KB (the maximum size allowed).
Error: Icon File exists, no overwrite specified	The Icon already exists.
Error: Icon File is empty	The icon file itself is empty or truncated.
Error: Incorrect resolution in icon file	The icon file resolution is not correct.

Lineup Editor - Managing the Channel Lineup

The Lineup Editor is used to control the output address of EPG data as well as enable VF Now entries to show in the lineup for STBs.

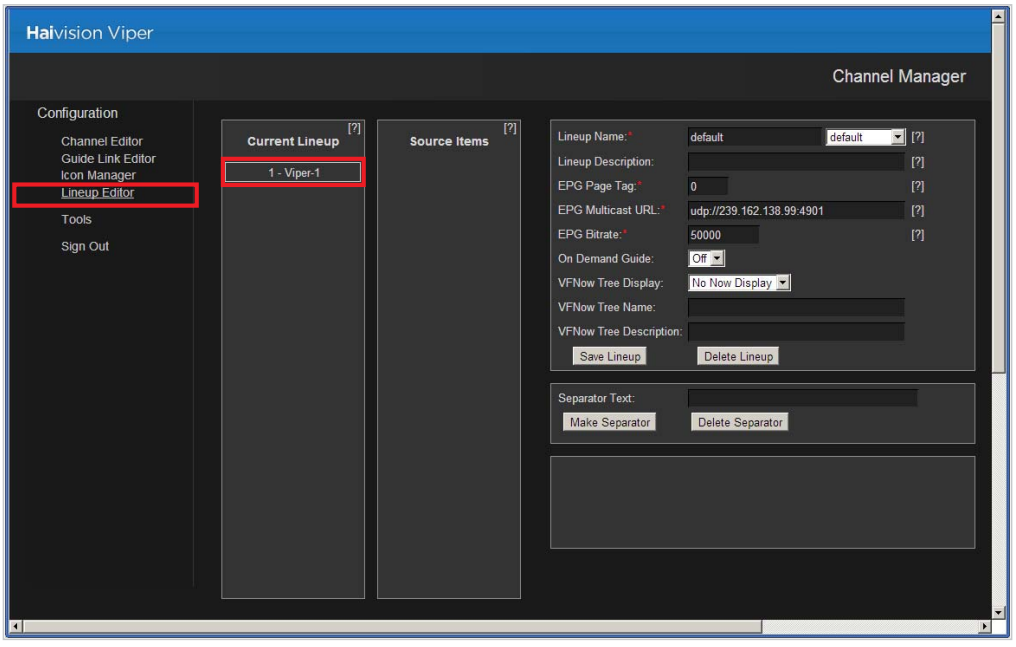
NOTE The default EPG address must be changed on all Vipers during initial setup. Otherwise, if two Vipers with the same EPG address are on the same network, the streams cannot be viewed in InStream or on a STB.

Creating Channel Lineups

To edit the Current Lineup:

1. Click Lineup Editor on the left side of the Viper Channel Manager page.

   The Lineup Editor page opens.



   By default, the channel named “Viper” is in the Current Lineup.

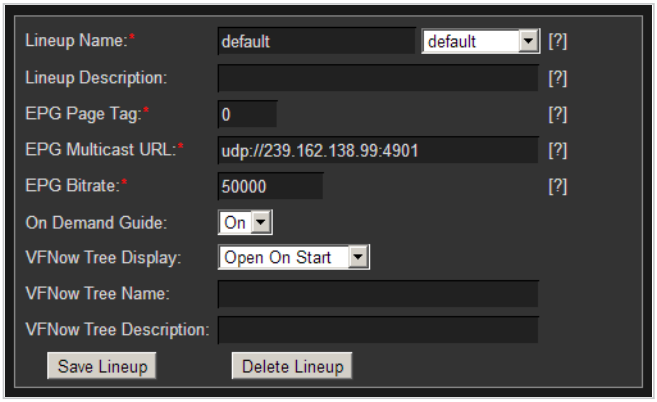
Adding Viper Now On-Demand Titles to the Channel Lineup (STBs only)

NOTE In order to get Viper Now links to display on the STB, you need to enable On Demand Guide and Viper Now Tree Display on the Lineup Editor page.

This section shows how to add Viper Now titles to the channel lineup displayed by the Guide on STBs.

To add Viper Now titles to the STB channel lineup:

1. On the Lineup Editor page, set On Demand Guide to “On” as shown in the following image.



2. Set the Viper Now Tree Display to either “Open on Start” or “Closed on Start” (typically “Closed on Start”).
3. (Optional) Enter a Viper Now Tree Name, for example, “VOD”.
4. (Optional) Enter a Viper Now Tree Description.
5. Click Save Lineup.

A Viper Now entry must also be configured for the channel lineup (see “Adding a New Viper Now Link” on page 180).

CHAPTER 7: STB Image Provisioning

This chapter describes the Viper STB Imager provisioning utility.

Topics In This Chapter

STB Imager - Managing STB Image Profiles 143
- Adding a New STB Image Profile 143
- Assigning a Profile to a STB 146
- Creating a New Profile Assignment 147
- Deleting a Profile Assignment 148

STB Imager - Managing STB Image Profiles

Viper STB Imager

Stingray STBs automatically provision themselves from the network and accept an operating image and configuration based on the image profile assigned to the MAC address of the STB. In most cases, the default profile is used.

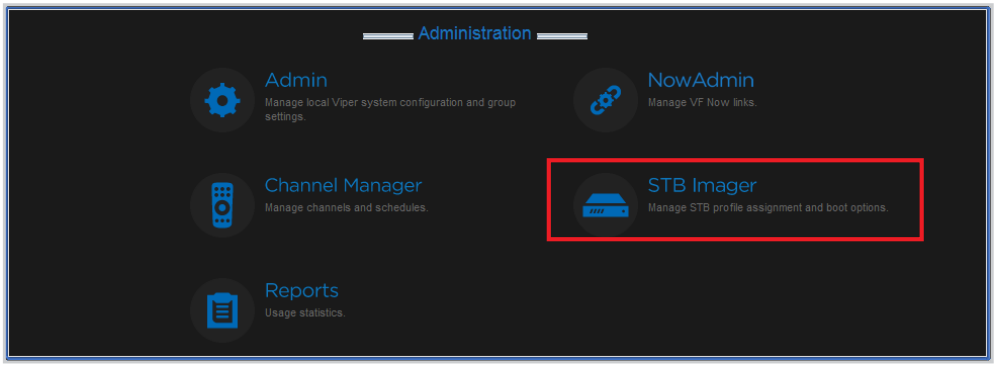
The STB Imager provisioning utility is used to create profiles that are unique to one or more STB applications. A profile sets up specific behaviors for certain applications such as kiosks, conference rooms, or digital signage.

Adding a New STB Image Profile

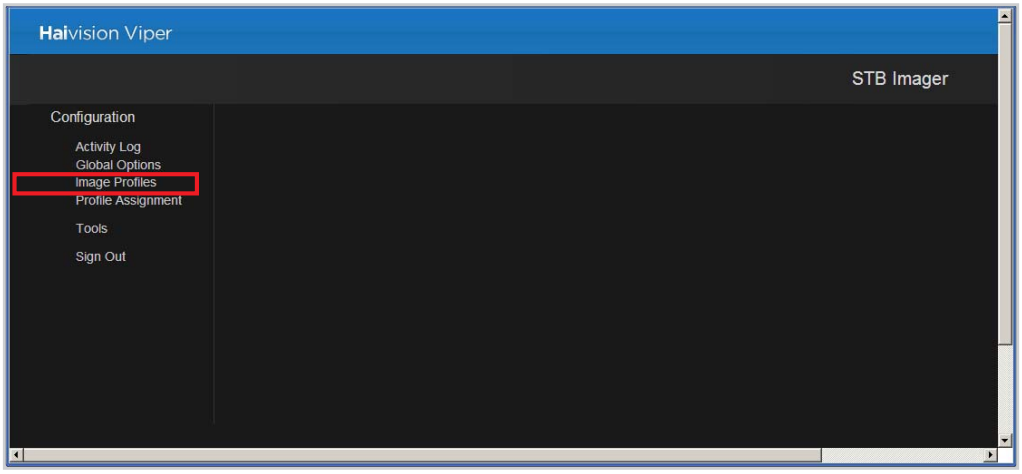
This section explains how to create an STB Imager profile.

To add a new STB Image Profile:

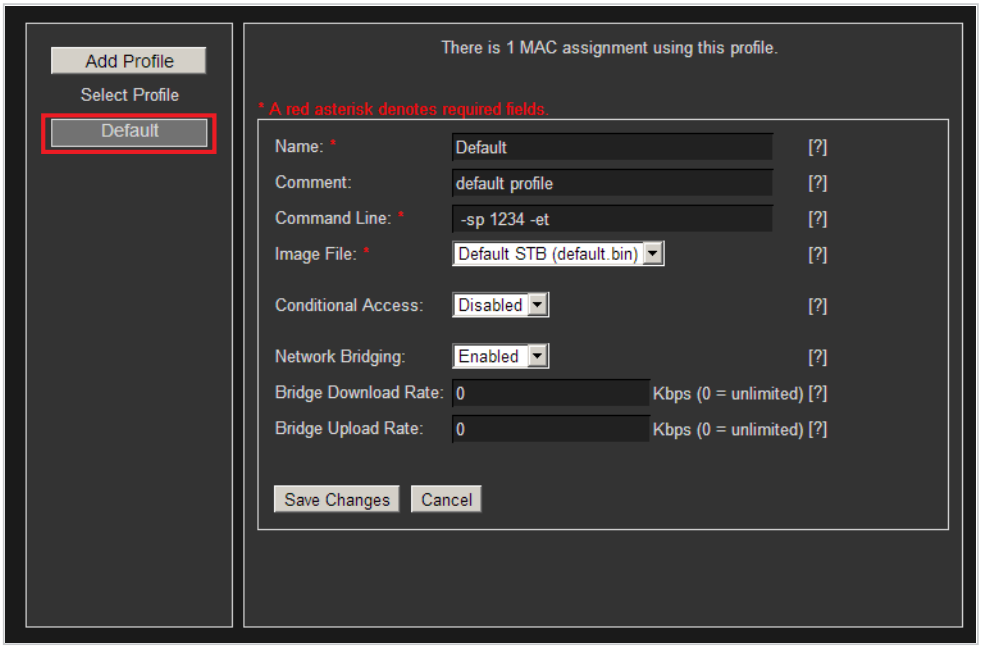
1. On the Tools page, click the Viper STB Imager icon under the Administration Section.



2. Click Image Profiles on the left side of the STB Imager Welcome page.



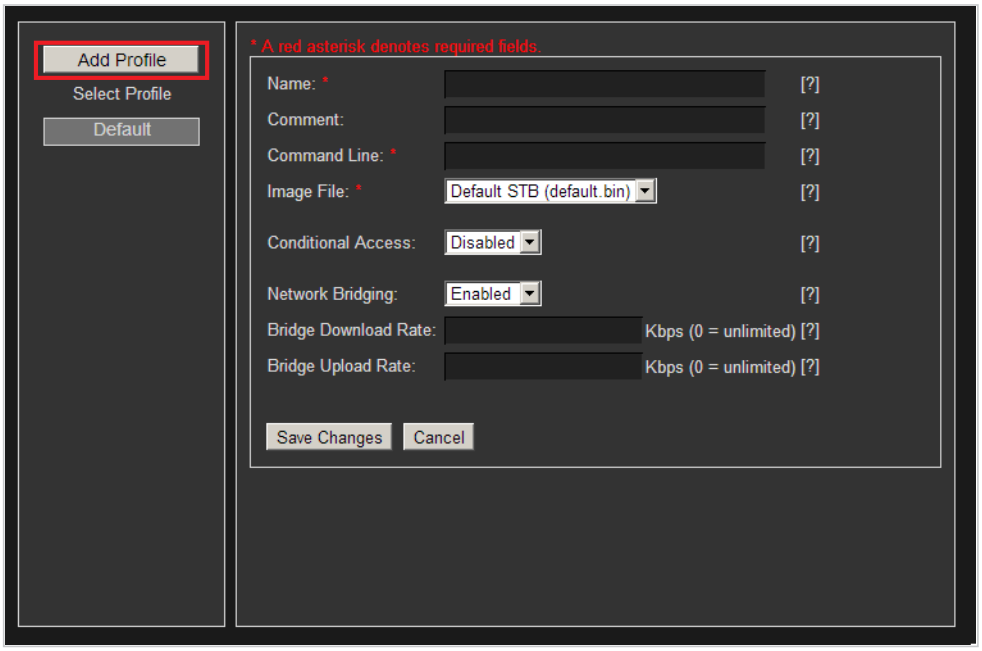
3. To view the default profile, click Default.



The default profile details are displayed in the Profiles pane (right side).

4. To add a new profile, click Add Profile.

   The Profile fields are cleared for you to enter the new information.



5. Enter the Name for the profile and (optionally) a comment that describes the purpose of the profile.

6. Specify a command line, for example:

   ```
   -l udp://10.1.3.104:4902 -sp 1234 –et
   ```

   This sample command line string specifies the license server to which the STB should communicate, sets the setup password to 1234, and instructs the STB to show and use the system time broadcast in the EPG rather than its real-time clock.

7. Select the default image file.

8. To enable Conditional Access, select Enabled.

   When Conditional Access (CA) is enabled on an STB profile, you can assign specific STBs to groups and then use CA to control what Video on Demand assets those groups can view. This requires a Viper license with CA entitlement. For more information, see "Using Conditional Access for User Authentication" on page 60 and "Managing Device Entitlements" on page 65.

9. To enable the network bridge on dual NIC Set Top Boxes, select Enabled for Network Bridging.

   Network bridging allows you to daisy-chain multiple devices off a single network drop: main network <=[STB eth0]=> STB <=[STB eth1]=> local switch or other device.

10. To specify the Network Bridge Download and Upload Rates (i.e., the upload and download rates when bridging is enabled, enter the rates in Kbps (range is 0 to unlimited).

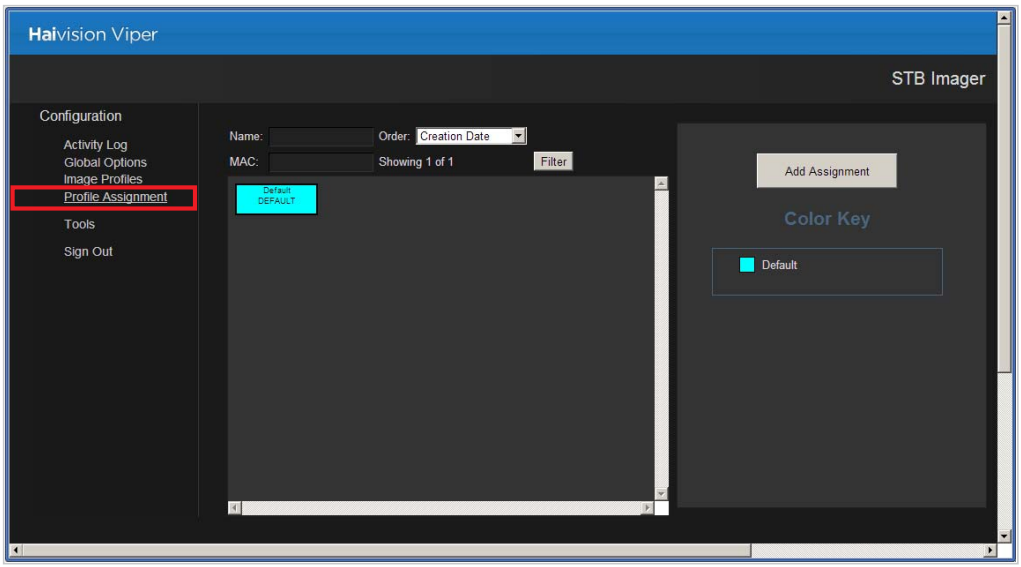
    This allows you to rate-limit the traffic bridged through the STB when Network Bridging is enabled.

11. Click Save Changes to save the profile.

Assigning a Profile to a STB

This section explains how to assign your new profile to one of your STBs:

1. Click Profile Assignment on the left side of the STB Imager page.
2. From the list of STBs, click the box that matches the STB to be assigned a new profile.



NOTE If your system has many STBs listed with unique profiles, you can use the Filter to refine the list.

You can either type a string in the **Name** field, or type the MAC address for the STB in the **MAC** field, and then click Filter.

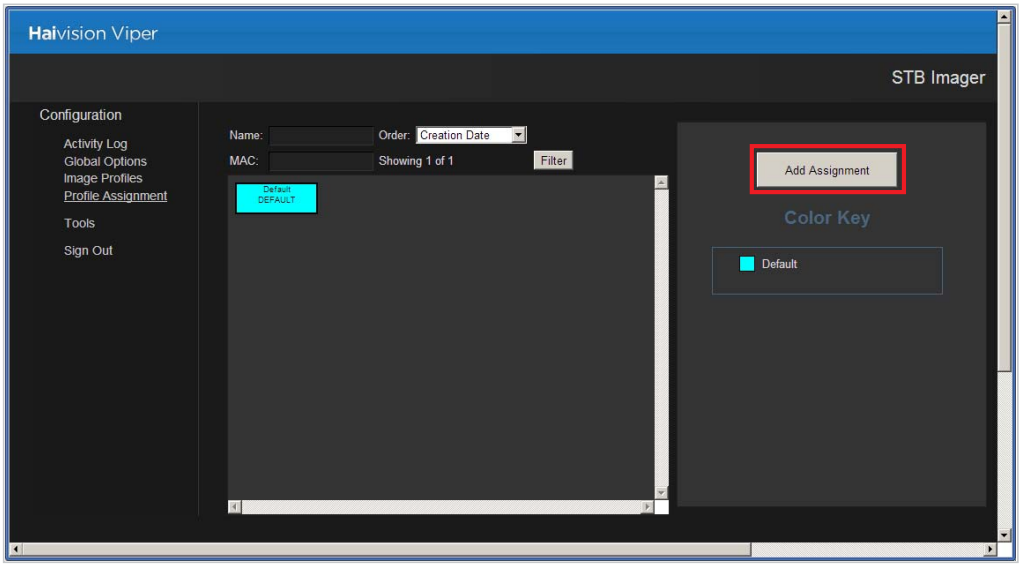
The selected profile details are displayed in the Profiles pane (right side).

3. Click Save Changes.

Creating a New Profile Assignment

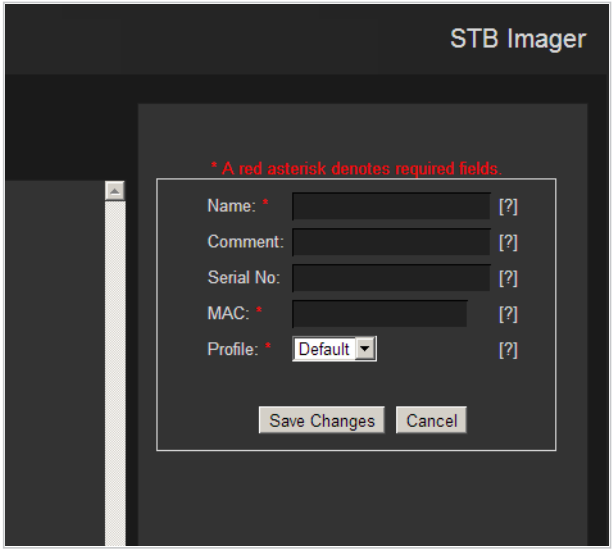
This section explains how to assign a profile for an STB.

1. On the STB Profile Assignment page, click Add Assignment.



The Profile Assignment fields appear in the right pane.

2. In the Name field, enter a name for this STB.



3. (Optional) For future reference, type a comment in the Comment field that describes the purpose of the STB.
4. (Optional) Type the Stingray STB serial number in the Serial No. field.
5. Enter the Stingray MAC address in the MAC field (e.g., 00:22:19:58:6A:03). A value of default is used for all MAC addresses without an entry.

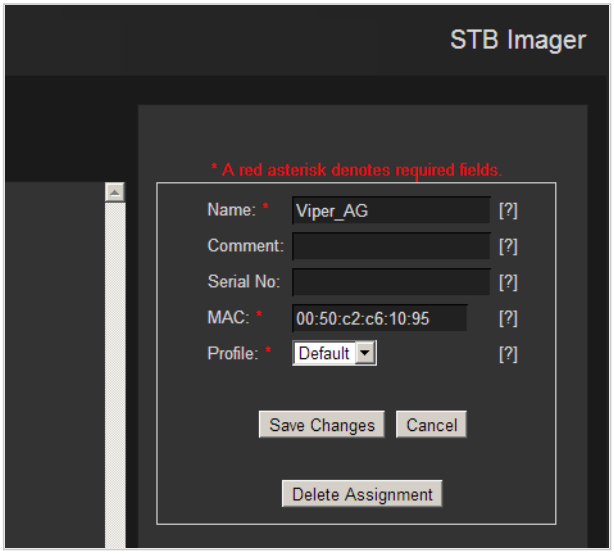
6. Select the profile to assign from the Profile drop-down list.
7. Click Save Changes to assign the profile.

Deleting a Profile Assignment

When a specific STB is relocated or the unique profile is no longer relevant to the STB, deleting the profile assigned to the STB will enable the STB to become provisioned with the default system profile when the STB is power cycled (either by unplugging it or holding the front panel power button pressed for approximately five seconds).

To delete a profile assignment:

1. On the STB Profile Assignment page, click the profile assignment box for the STB for which the profile assignment should be deleted.
2. Then click Delete Assignment.



CHAPTER 8: Managing Reports

This chapter describes the Viper Reports tool available to system administrators to enable real-time and past usage reporting.

Topics In This Chapter

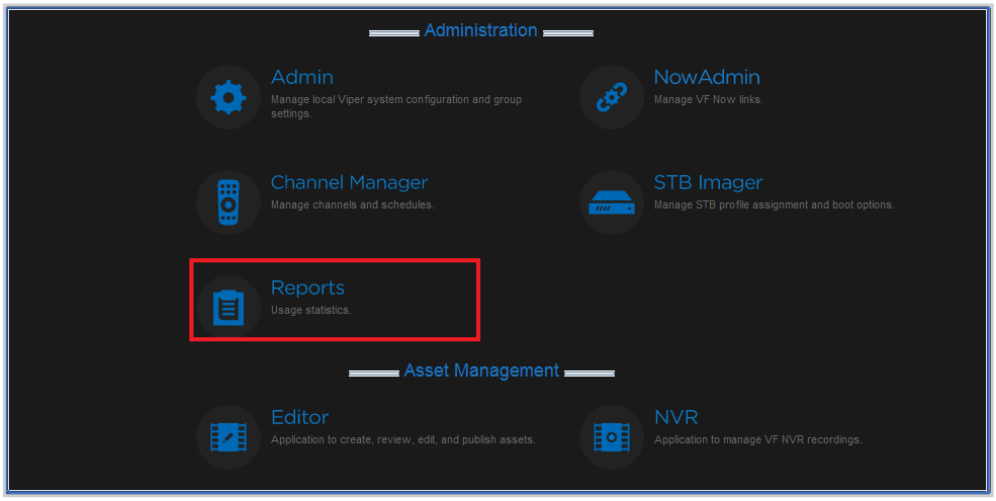
Viper Reports - Accessing Usage Statistics 150
- Live Channel Stats Report 151
- Past Channel Stats Report 152
  - Refining the Report 152
  - Viewing Daily and Hourly Usage 230

Viper Reports - Accessing Usage Statistics

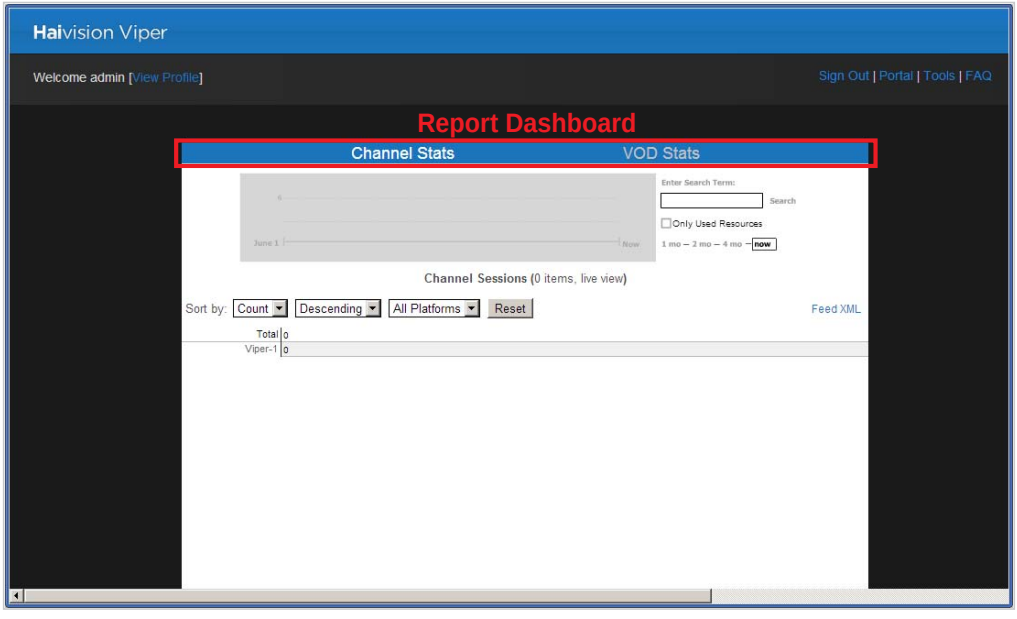
Viper provides a Reports portal to enable access to real-time and past usage data. Usage details are separately available for both channel usage and Viper VOD on-demand usage by InStream and Stingray STB users. For each type of report, both real-time usage and past usage reporting is available.

To access the Viper Reports portal:

1. On the Tools page, click the Viper Reports icon under the Administration Section.



The Reports portal opens as shown in the example below.



When you access the Viper Reports portal, it displays the current aggregate real-time viewing statistics for the Viper channel. The start page shows the aggregate usage per channel for all InStream and Stingray STB clients and provides the ability to customize or filter the report by platform and sort order as well as show hourly details for past usage.

Two types of reports are available in the Reports Portal: Channel Stats and Viper VOD Stats. The following sections explain how to display these reports.

NOTE The features described in the following sections work the same way for both Channel Stats and VOD Stats.

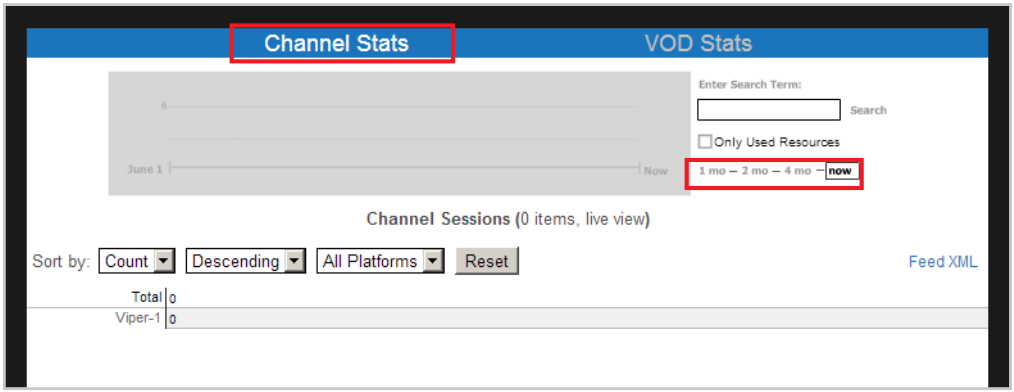
Live Channel Stats Report

To generate a live Channel Stats report:

1. First, select the report type by clicking either Channel Stats or VOD Stats in the Reports dashboard.

Channel Stats	Shows usage data such as how many users over what time span have tuned into the Viper channel, as well as what platform is prominent on the system.
VOD Stats	Shows usage of the VOD assets in your system.

2. Next, select the time frame by clicking either now to report real-time usage from active clients, or 1 mo, 2 mo, or 4 mo to show statistics of past usage for up to 4 months in the past.



For example, to show active real-time usage of multicast channels, select Channel Stats and now.

TIP You can click the drop-down lists to sort the reports by [Count] or [Name], in [Ascending] or [Descending] order. You can also filter the results by platform.

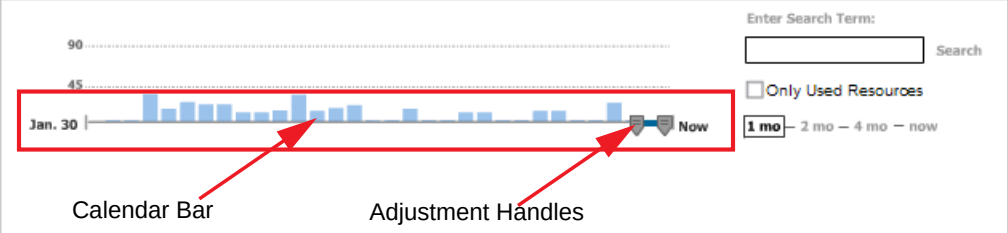
Sorting by [Name] performs an alpha sort by channel name in either ascending or descending order depending on the menu selection.

Past Channel Stats Report

To generate a past Channel Stats report:

1. Select either a 1 mo, 2 mo, or 4 mo activity window to report on viewing statistics up to 4 months in the past.

   The figure below shows that a 2 month activity window was selected.



Refining the Report

This section discusses options to refine the report.

Option	Description
Enter Search Term	Type an optional search term to include only resources that contain this text in the report.
Only Used Resources	Click this checkbox to report only resources that had been watched during the report period. Changing this criterion generates a new report.
1 mo – 2 mo – 4 mo – now	Click the **1 mo**, **2 mo**, or **4 mo** activity window to report on past usage. Changing this criterion generates a new report. Click **now** to report real-time usage from active clients.

After selecting the activity window, you can modify the window to a single day or multiple days by clicking the calendar bar and moving the adjustment handles to frame the activity window to the range of interest.

PART III: Asset Management

CHAPTER 9: Editing and Managing Assets

This chapter describes the Viper Editor utility available to system administrators to digitize and manage assets for on-demand viewing with Viper Now.

Viper Editor allows administrators to record a Viper stream while the unit is actively streaming. Viper Editor also provides basic editing and metadata tools as well as the ability to import third party MPEG assets and export dual- or single-stream assets.

IMPORTANT Recording on the Viper is handled primarily from the Touch Panel interface. The Editor module is included with the Viper to enable users to import and export dual- or single-stream assets.

Topics In This Chapter

Viper Editor - Digitizing and Managing Assets 155
- Creating Off-line Assets (Digitizing Assets) 155
  - Inserting Hotmarks 163
  - Adding or Modifying Asset Thumbnails 164
- Merging Assets 166
- Loading Assets 170
- Exporting Assets 172
- Deleting Assets 173
- Publishing Assets 174

Viper Editor - Digitizing and Managing Assets

Viper Editor is the asset creation and editing application for the Viper tools. Viper Editor provides features such as the ability to digitize analog assets while adding user metadata (i.e., information about the asset, tags, or a thumbnail image), or to edit an existing asset and post it to the master digital asset library. It also includes a real-time video "clipper" feature for cleaning up the front and back of video assets or clipping a portion of video from a larger asset and making a new asset.

Only single-stream assets can be recorded in Viper Editor. However, Viper Editor supports editing of dual-stream assets, along with exporting of dual-stream assets to standard transport streams.

Creating Off-line Assets (Digitizing Assets)

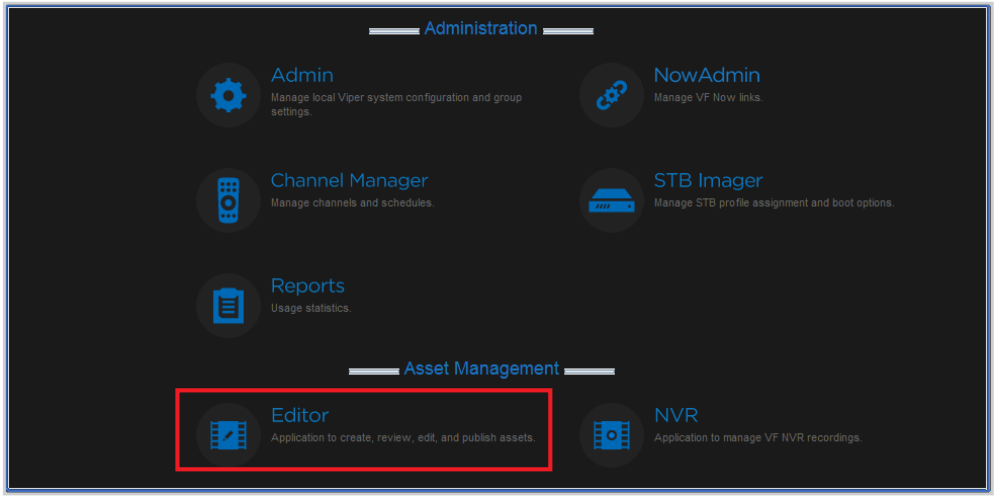
This section walks through a simple four-step approach to digitizing and publishing an asset that can be available for on-demand viewing Viper Now).

NOTE The Viper must be actively streaming in order to use Editor to record a Viper stream.

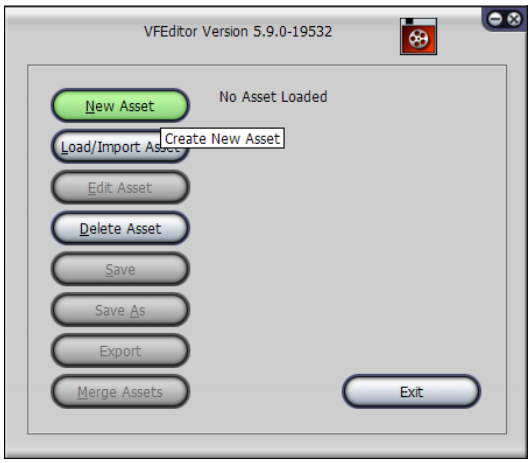
- Step 1: Connect your video and audio source to the encode channel.
- Step 2: Log in to the encoder and record the audio/video stream.
- Step 3: Review and edit your recording.
- Step 4: Publish the digitized video asset to the Asset Manager.

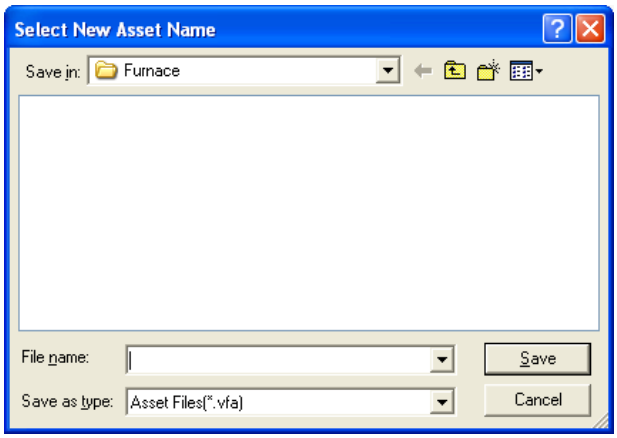
Step 1: Connect your video and audio source to the encode channel.

1. On the Tools page, click the Viper Editor icon under the Asset Management section.



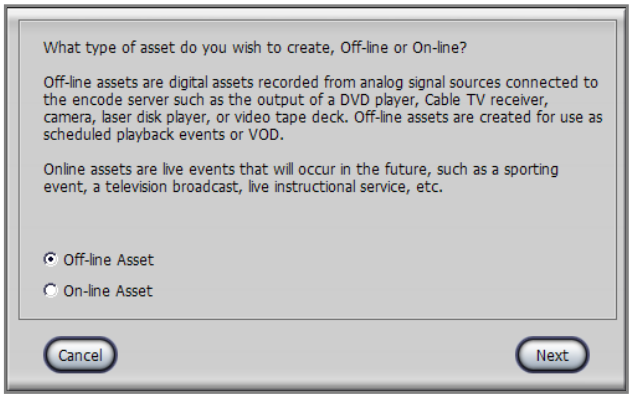
2. On the Viper Editor dialog box (shown below left), click New Asset.





3. In the Select New Asset Name dialog box (shown above right), select a folder, type in a filename for the asset, and click Save.

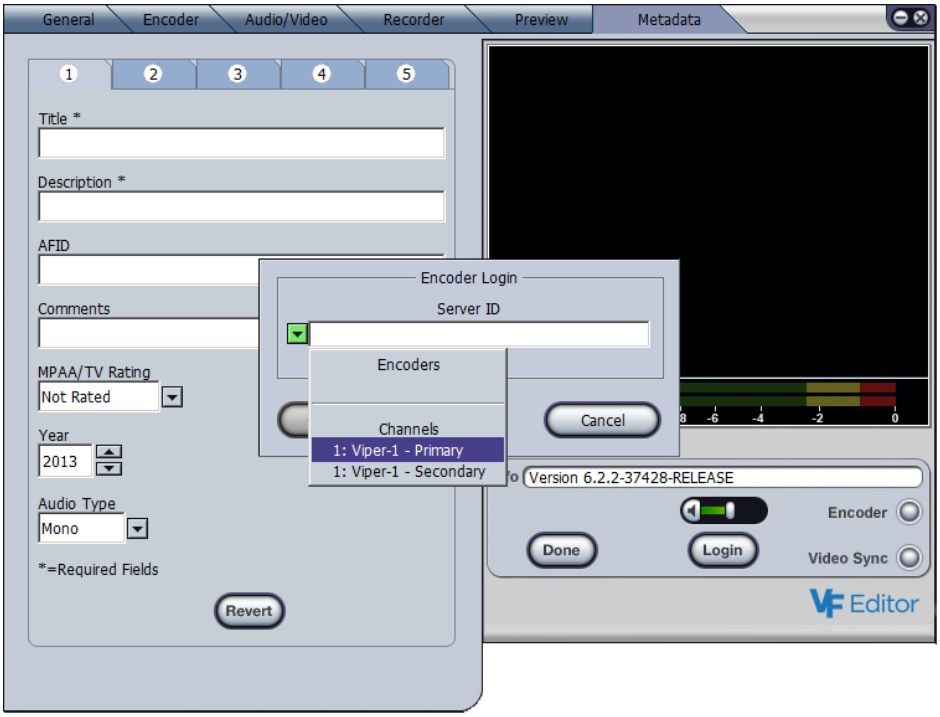
4. On the Asset Type dialog box, check Off-line Asset (meaning it is stored off-line) and click Next.



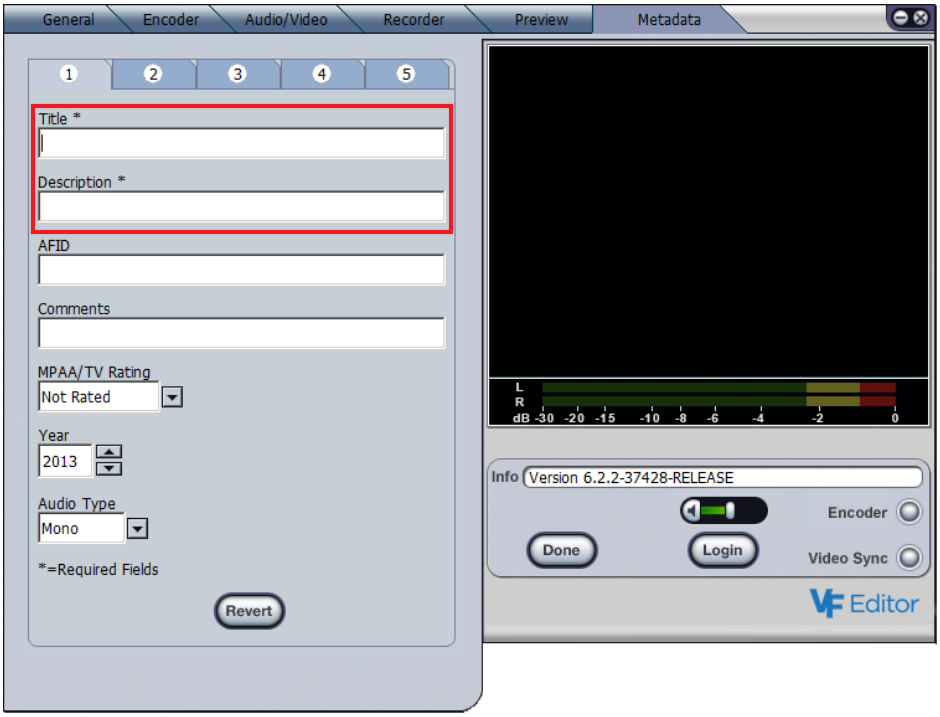
The Viper Editor window opens displaying the Metadata tab.

Step 2: Log in to the encoder and record the audio/video stream.

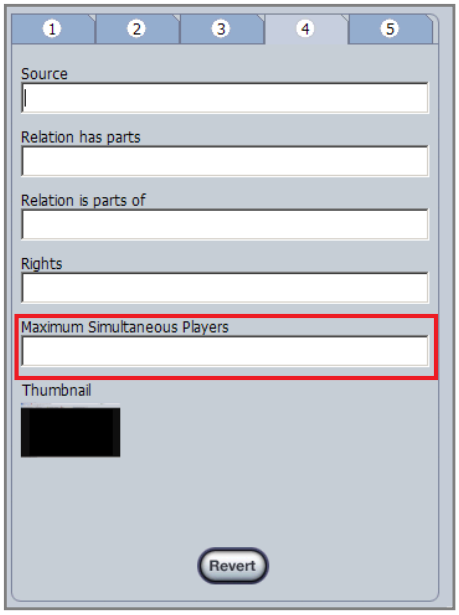
1. On the Viper Editor window, click Login, select the Viper channel from the Encoder Login drop-down list, and click Connect.



2. Complete the required Metadata fields (Title and Description).

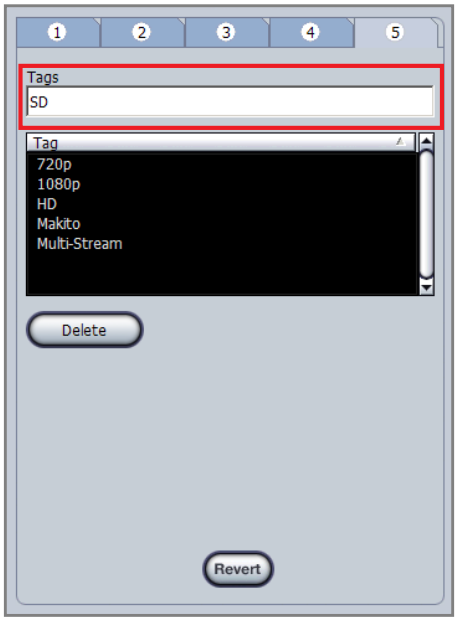


3. If concurrent player limits are required, click tab 4 and type in the number of Maximum Simultaneous Players (shown below).



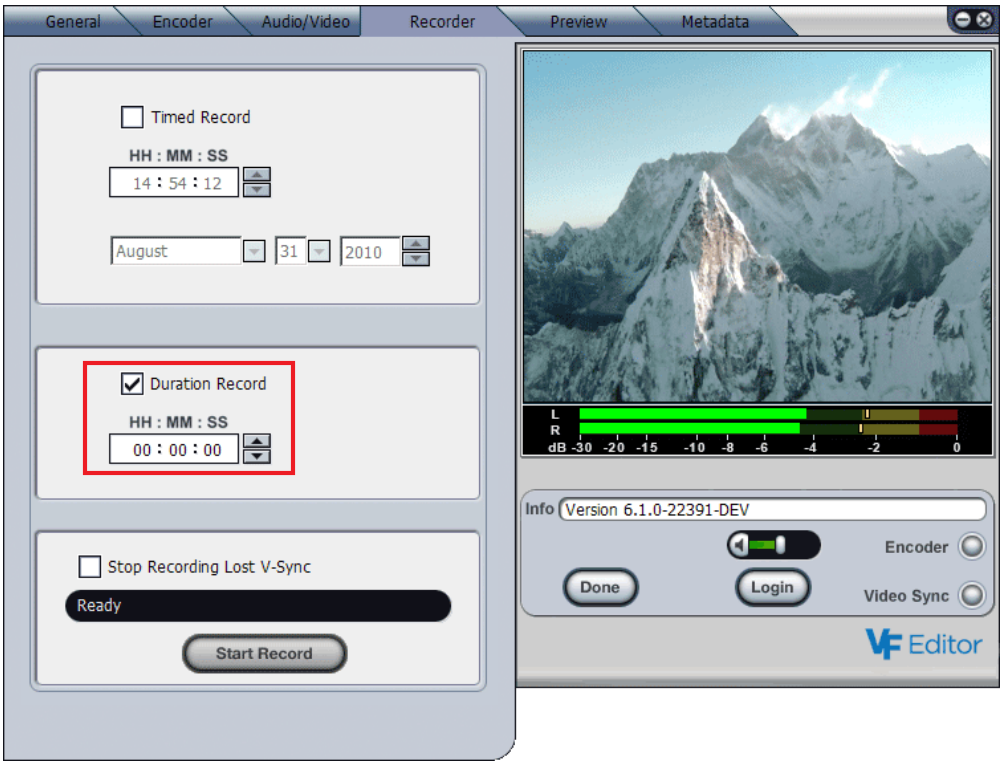
TIP To capture or modify a thumbnail snapshot of a video frame from the asset, see "Adding or Modifying Asset Thumbnails" on page 164.

4. To assign Tags to the asset (which users can use to categorize and search for the asset), click tab 5, type the word or phrase in the **Tags** field (shown below), and press ENTER.



5. Click the Recorder tab.

6. Check the Duration Record checkbox, and set the duration to at least 1 minute by double-clicking in the minute field (under ":MM") and entering 1.



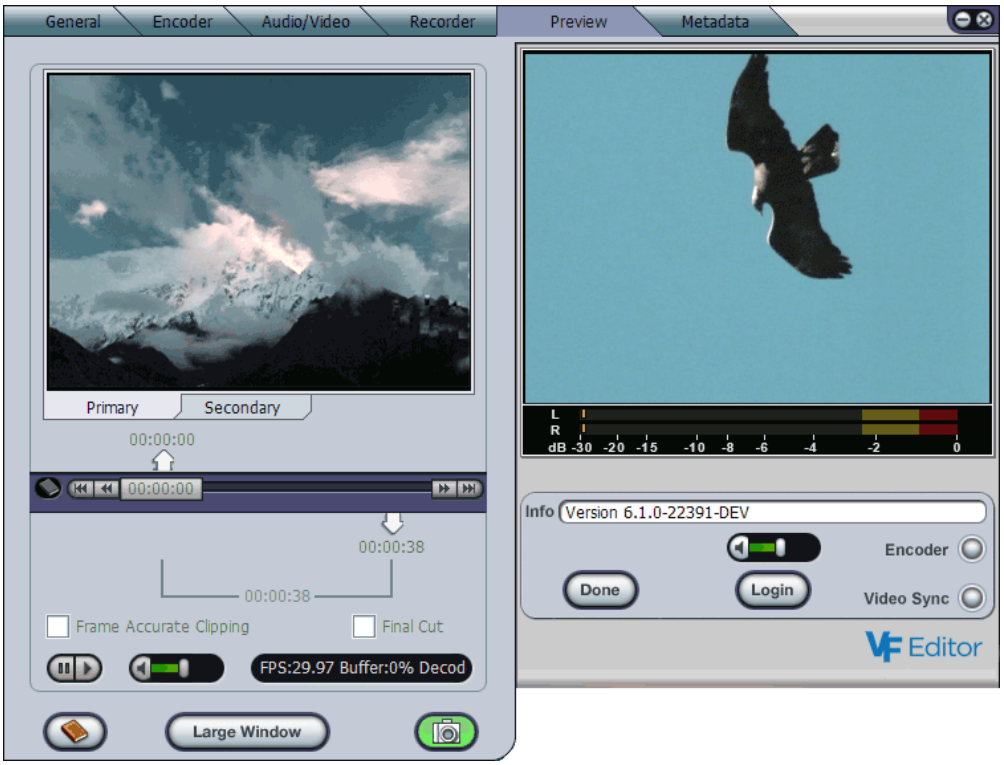
7. Click Start Record.

When the duration counts down to 0, recording will terminate automatically (you may stop the recording any time before that if desired).

Step 3: Review and edit your recording.

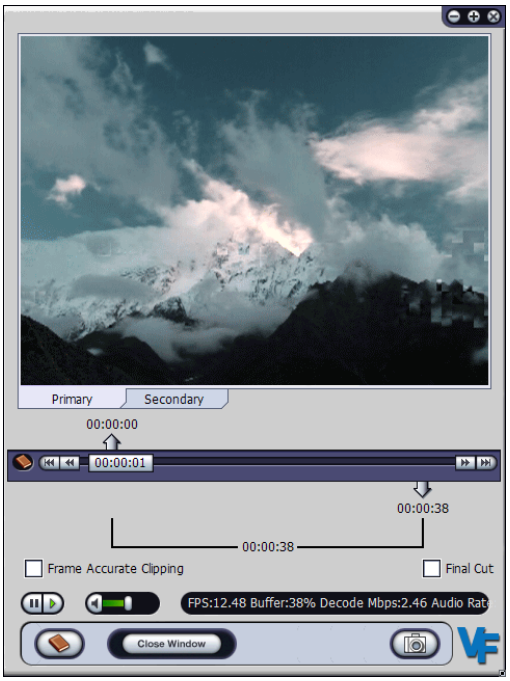
This step also applies to editing any asset loaded into Viper Editor.

1. Click the Preview tab.



2. If the asset is multi-stream, choose which track to edit by clicking either the Primary or Secondary tab below the viewing pane.

3. (Optional) Launch the “clipper” window by clicking Large Window (shown in the following example), or you may edit the video start and end points directly from the Preview viewing pane.



The Large Window or “clipper” mode allows you to stretch the size of the clipper work area with your mouse. Or you can press the + or - key on the numeric keypad to increase or decrease the clipper window size.

4. From either the **Preview** tab on the Viper Editor window or the clipper window, click the Pause button, and then move the scrub bar 00:00:00 where you want your video to start.

   If a fine scrub bar adjustment is needed to position the video more precisely, press and hold the SHIFT key, then click and drag the scrub bar.

   Or click the or button to step the video frame forward or in reverse.

5. When the video is positioned properly, double-click the **start marker** (up arrow) to move it to the scrub bar position (the start marker will position itself to the closest MPEG I-Frame).

6. Now position the scrub bar to the video frame where you want your video clip to end. Double-click the **end marker** (down arrow) to move it to the scrub bar position.

7. When you are finished adjusting the start and end clip markers, check the Final Cut checkbox.

   You have successfully specified a clipped segment of the video delineated by the start and end clip markers.

8. To review your changes, click the Play  button.

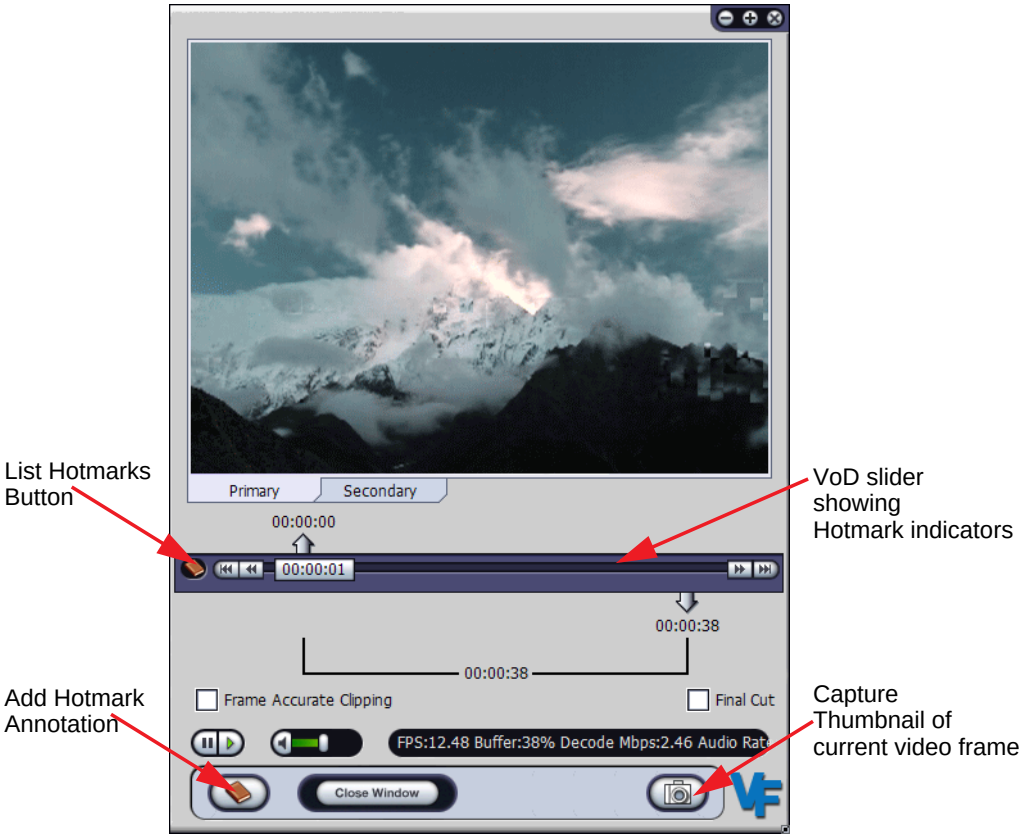
   To return to the Viper Editor **Preview** tab from the clipper window, click Close Window or the X button in the upper right corner.

Inserting Hotmarks

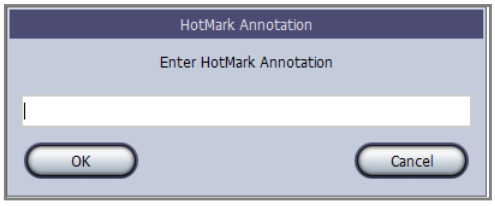
From either the **Preview** tab or the clipper window, you can insert "Hotmarks" with annotations to index and store reference points in the video.

To insert a Hotmark reference point:

1. Load an asset into Viper Editor and click the Preview tab.
2. Click the Add Hotmark button (lower left).



3. In the Annotation dialog, type in the Hotmark description and click OK.



The Hotmark is inserted in the clip and added (along with the annotation) to the Hotmarks menu.

4. To view, edit the annotation, or delete Hotmarks previously saved in the asset, click the List Hotmarks button.
   - Selecting one of the Hotmark entries from the list shows a yellow Hotmark locator icon on the VoD slider corresponding to the video index location saved for the Hotmark.
   - Clicking the Hotmark locator icon positions the video scrub bar to the video corresponding to the Hotmark index location.
5. To capture a thumbnail snapshot of the current video frame to include as metadata for the asset, click the Capture Thumbnail button.
6. When you have completed editing the metadata and/or video, click Done to close the window and return to the Viper Editor dialog box.

Adding or Modifying Asset Thumbnails

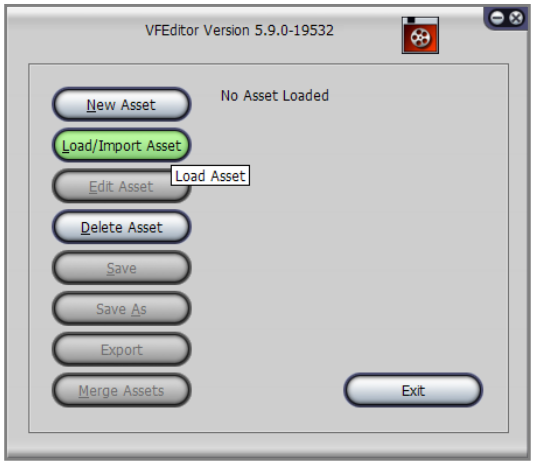
During a recording session, the Viper automatically generates a thumbnail from the first valid frame of the recorded asset (for either Dual- or Single-stream recordings). A thumbnail is a single image captured from the recorded content.

These thumbnails are displayed in the Touch Panel's Review & Publish screen to provide visual feedback of the content. Thumbnails are also associated with the assets listed in the VoD portal page as well as within the Conditional Access module listing under the Assets tab.

The steps that follow show how to use the Editor to add or modify a thumbnail after an asset has been recorded.

To add or modify the thumbnail for an asset:

1. On the Editor dialog box, click Load/Import Asset.

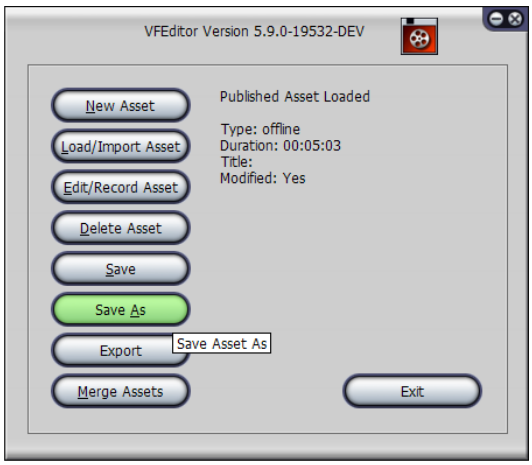


2. On the Load Asset dialog, click the Published asset button.

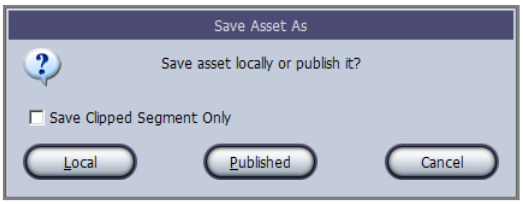
3. On the Load Asset list, select the asset to add the Thumbnail to and then click Load (or double-click the asset).
4. On the Editor dialog box, click Edit/Record Asset.
5. On the Editor window (Preview tab), use the Scrub bar to drag to the image that you want to use as the asset Thumbnail.
6. Click the Camera icon at the bottom right of the application window.
7. Click Done.
8. Click Exit. When asked to Save the changes, click OK.
9. Go back to the Portal to confirm that the thumbnail has been associated with the asset.

Step 4: Publish the digitized video asset to the Asset Manager.

1. On the Viper Editor dialog box, click Save As.



The Save Asset As dialog opens.



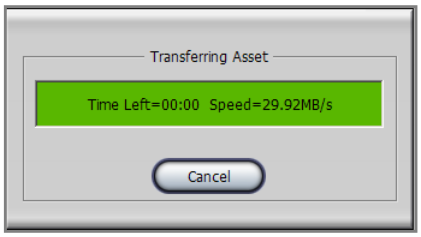
2. To save only the video portion between your clipping points, check the “Save clipped segment only” checkbox.

   To save the *whole* asset including the clipped segment, leave the checkbox unchecked.

3. Click Published.

   Asset publishing across the network begins immediately.

A progress dialog opens showing the publish status.



You have successfully digitized an asset and published the video to the Viper.

This asset is now available to the Viper Channel Manager and will available for viewing on the Viper portal using InStream and Viper Now systems. You can now create a Viper Now resource link in the Viper Now system to enable on-request viewing of this asset.

Merging Assets

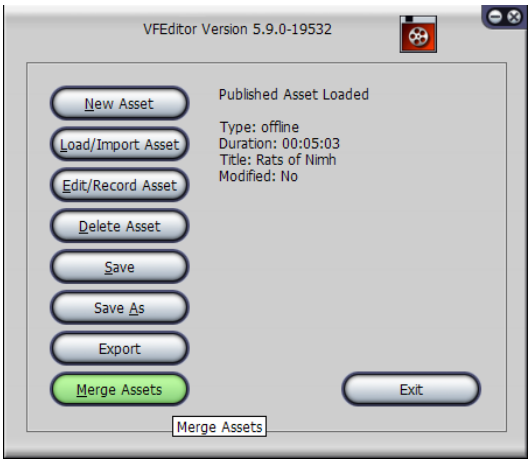
Viper Editor provides the option to merge a collection of local or published assets to one monolithic asset.

The process of merging assets requires that you first select or create a target asset to accept the resulting merged list of assets. Merging assets replaces the media contents of the asset to which the other assets are merged.

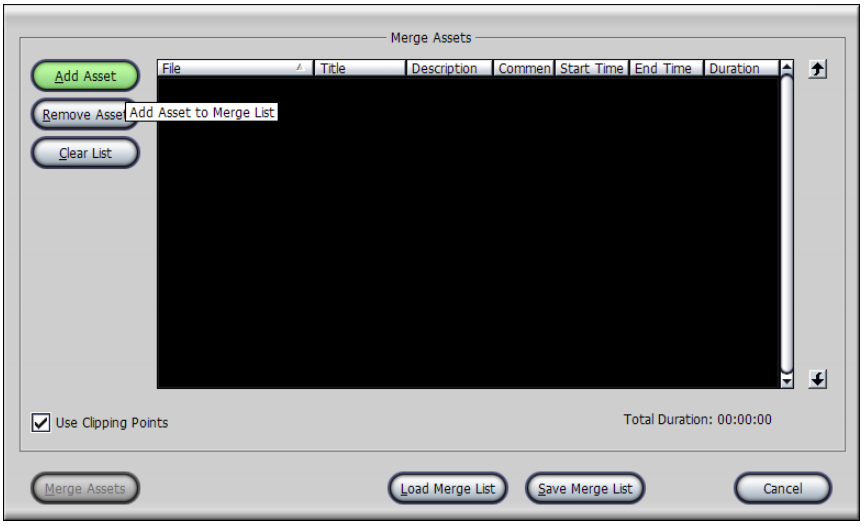
NOTE Merging is not currently supported for dual-stream assets.

To merge assets:

1. Create a new target asset, following the steps in "Creating Off-line Assets (Digitizing Assets)" on page 155. Or you may also use an existing asset as the target asset.
2. On the Viper Editor dialog box, click Merge Assets.



3. On the Merge Assets dialog, click Add Asset to select the first asset to merge.



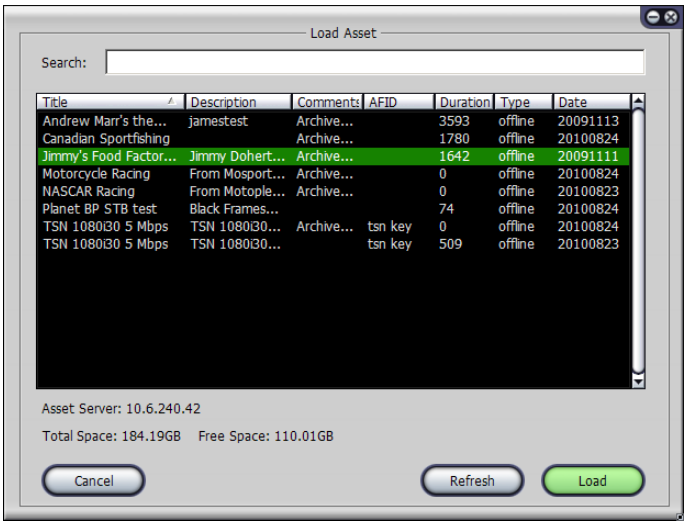
The Add Asset dialog opens.

4. To select an asset from the local hard drive (or mapped network drive storage listed by your file manager), click Local and then select the asset from the list.

-or-

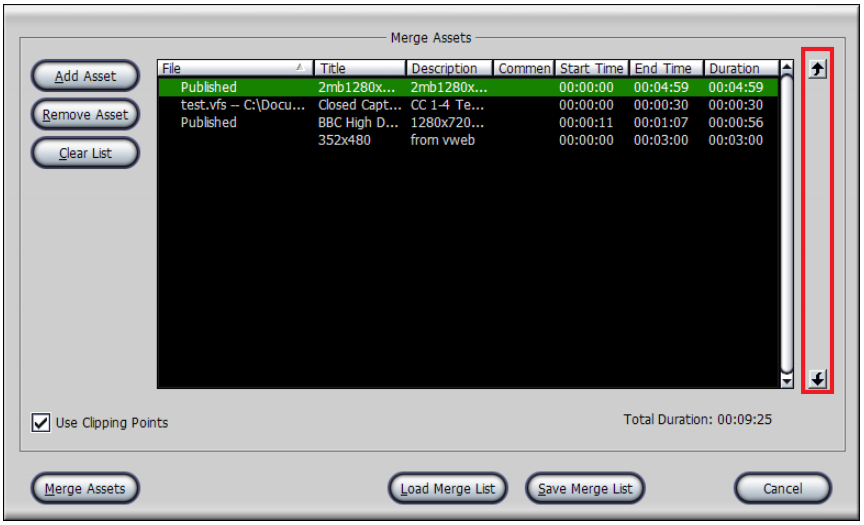
To select a published asset from the server, click Published.

5. On the Load Assets list dialog, highlight the asset in the list and click Load.



6. Repeat this process (i.e., Steps #3 through #5) until you have selected all of the assets you wish to merge together.

TIP To change the order of the assets, click an asset and then click the Move Asset Up or Down arrows to the right of the list (as shown in the following example).

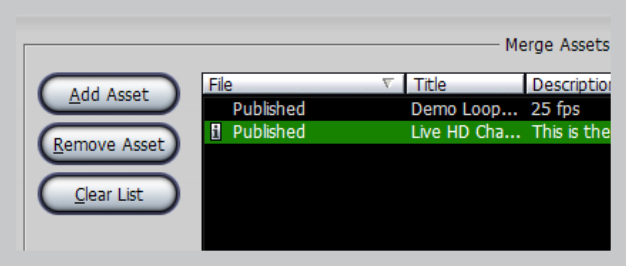


7. (Optional) To overwrite the metadata that you entered for the "merged asset" with the metadata from one of the assets in the merge list, double-click the preferred asset to select it.

-or-

Right-click the preferred asset and select “Use this Asset’s Metadata” from the pop-up menu. You can also select “Edit Clipping” to launch the “clipper” window to edit the asset.

The “info” icon will appear to indicate the Metadata selection as shown in the following image.



8. To deselect the Metadata assignment, double-click the asset again or double-click another asset to choose its Metadata.

   Remember that the Guide will use this Metadata, so be certain to assign Metadata from the appropriate asset or manually enter the correct text.

TIP You can change the Metadata after the merge by clicking Edit/Record Asset on the Viper Editor dialog box.

---

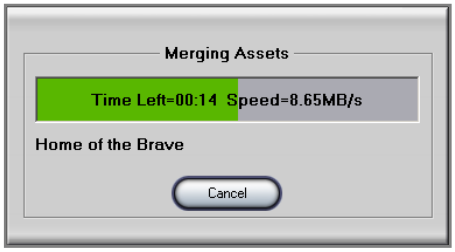
9. To merge each asset according to the start and end clip points saved in the asset, check the Use Clipping Points check box.

10. To save the merge list for future use, click Save Merge List.

11. To load a previously saved merge list, click Load Merge List and select the list in the Select List dialog box.

12. When you have completed arranging your list of assets in the preferred order, click Merge Assets.

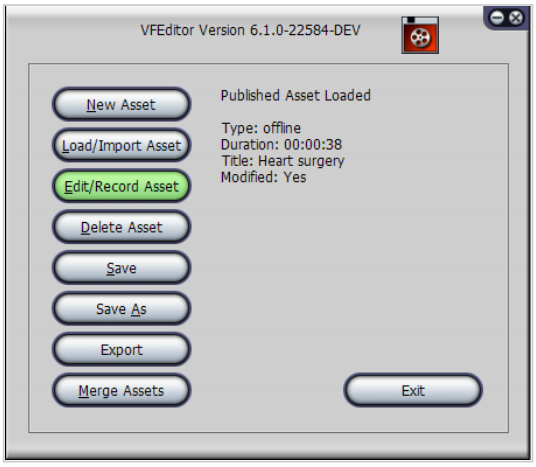
    A progress dialog opens showing the merge status.



After merging has completed, Viper Editor returns to the main dialog box that shows the asset file name, asset title, and duration.

To change the Metadata:

1. Click Edit/Record Asset.

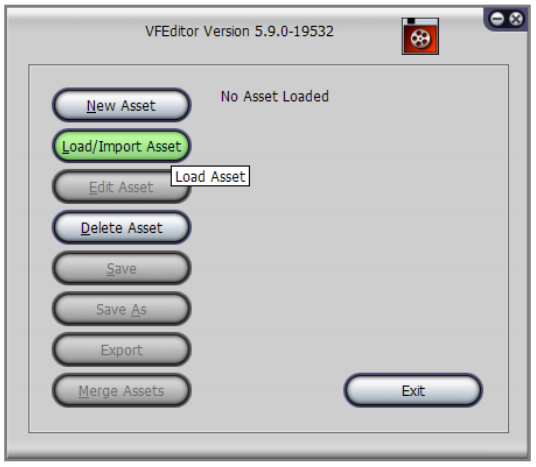


Merged assets can be viewed, edited, exported or published the same as any other asset.

Loading Assets

To load an asset for review:

1. On the Viper Editor dialog box, click Load/Import Asset.

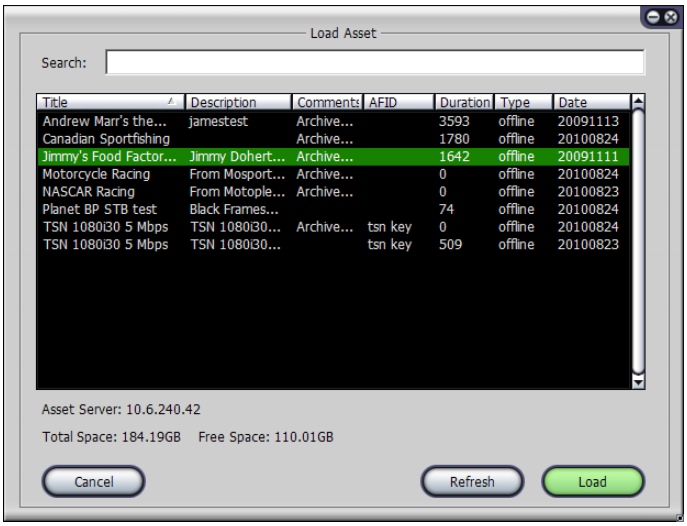


The Load Asset dialog opens.

2. To load an asset from your local hard drive (or mapped network drive storage), click Local and then select the asset from the list.

-or-

To select a published asset from the server, click Published, click an asset in the list, and then click Load or double-click the asset.



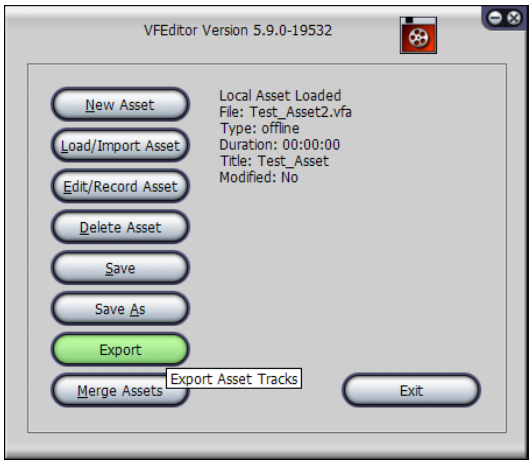
The asset loads to Viper Editor and is now available for editing, publishing, export or review.

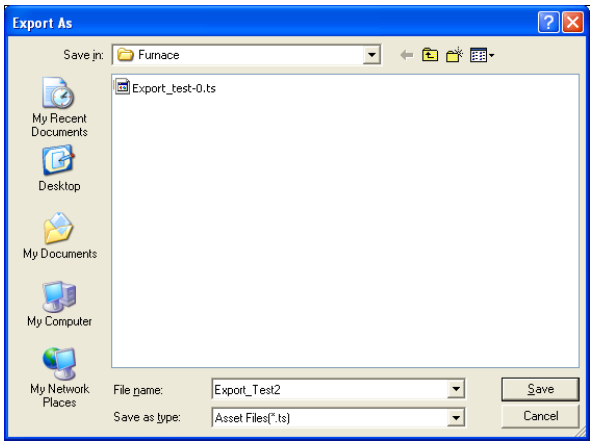
Exporting Assets

Viper Editor provides the option to export an asset to a standard transport stream in a folder on your desktop.

To export an asset to a standard transport stream:

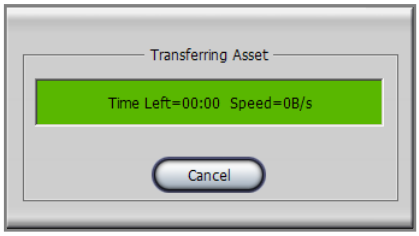
1. Create a new target asset, or load an existing asset.
2. On the Viper Editor dialog box (shown below left), click Export.





3. In the Export As dialog box (shown above right), select a folder, type in a filename for the stream, and click Save.

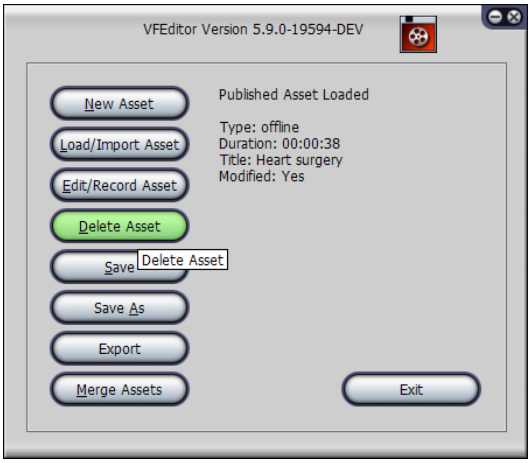
   The export begins immediately, and a progress dialog opens showing the export status.



Deleting Assets

To delete an asset and associated storage:

1. On the Viper Editor dialog box, click Delete Asset.



The Delete Asset dialog opens.

2. To delete an asset from the local hard drive (or mapped network drive storage), click Local and then select the asset from the list on the Select Asset dialog box.

   -or-

   To delete a published asset from the server, click Published, click an asset in the list, and then click Delete or double-click the asset.

3. On the warning dialog, click Yes to delete the asset.

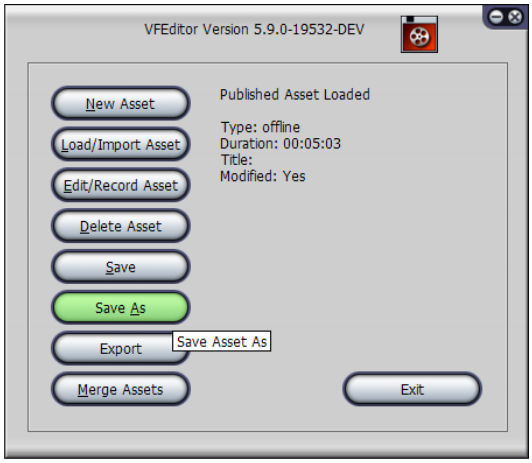
   The asset is deleted and you are returned to the Viper Editor dialog box.

Publishing Assets

To publish the on-line asset:

NOTE This assumes you have already saved the asset as a Published Asset to the Asset Manager (covered in "Step 4: Publish the digitized video asset to the Asset Manager." on page 165).

1. On the Viper Editor dialog box, click Save As.



2. On the Save Asset As dialog, click Published.

   A progress dialog shows the transfer of your asset to the Asset Manager, and your asset is now ready for use.

3. When the transfer has completed, close the Viper Editor application by clicking Exit or the X button in the upper right corner.

CHAPTER 10: Viewing and Deleting Recordings

This chapter describes NVR, the Viper's Network Video Recorder.

IMPORTANT Recording on the Viper is handled from the Touch Panel interface. However, the NVR module is provided to enable users to delete recordings. Although published assets can be deleted from the Web portal, you must use NVR to delete recordings that have not yet been published.

Use of NVR for any other purpose is *strongly* discouraged because the NVR and Touch Panel applications will compete with each other for recorder resources. Furthermore, if a recording is started via NVR, it will be automatically stopped when a new session is started from the Touch Panel.

Topics In This Chapter

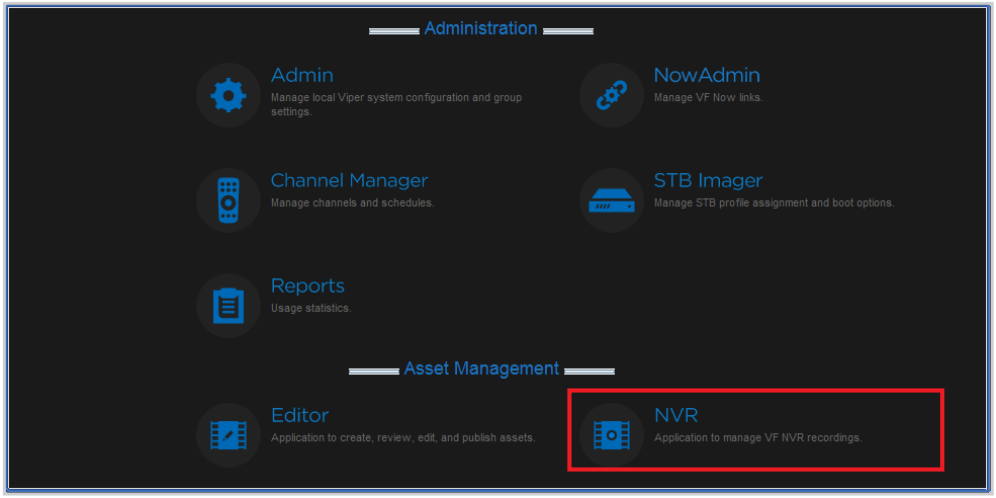
NVR - Network Video Recorder 176
Viewing and Deleting Recorded Assets 178

NVR - Network Video Recorder

From the Viper NVR window, you can view a list of the assets that have previously been recorded (Assets tab) and delete assets from the list.

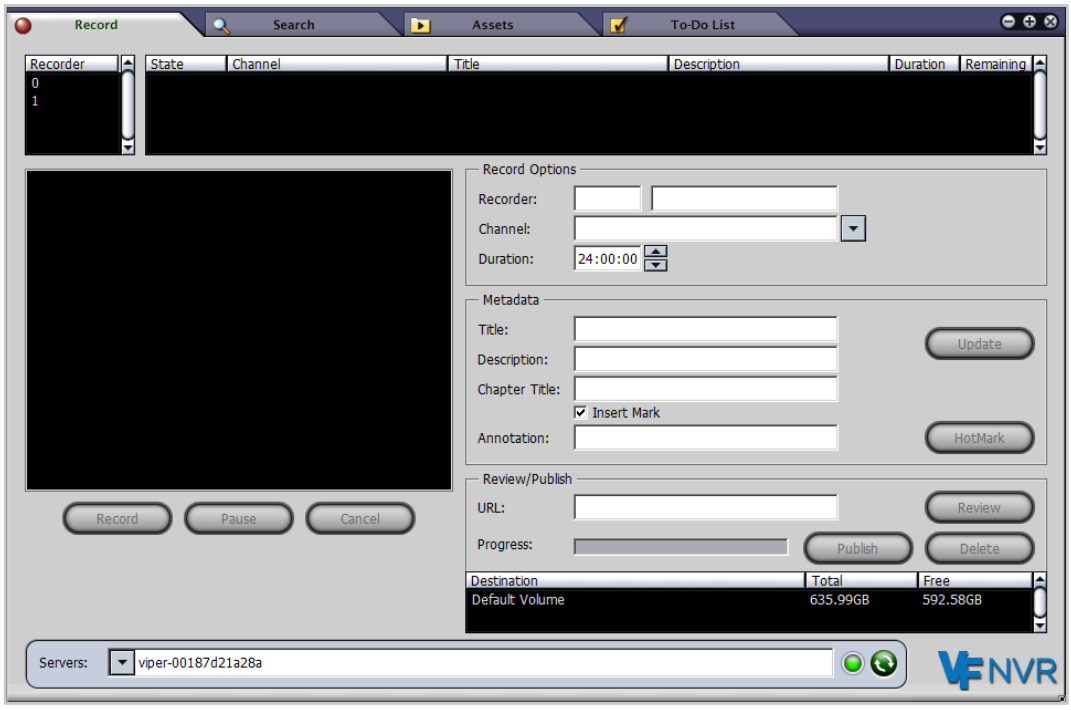
To launch Viper NVR:

1. On the Tools page, click the Viper NVR icon under the Asset Management section.



Once the application has launched, the Viper NVR window opens.

The Viper NVR window opens to the Record tab (shown below).



The server active indicator is illuminated green when the connection to the Viper is active. If the indicator is red, the connection has been lost.

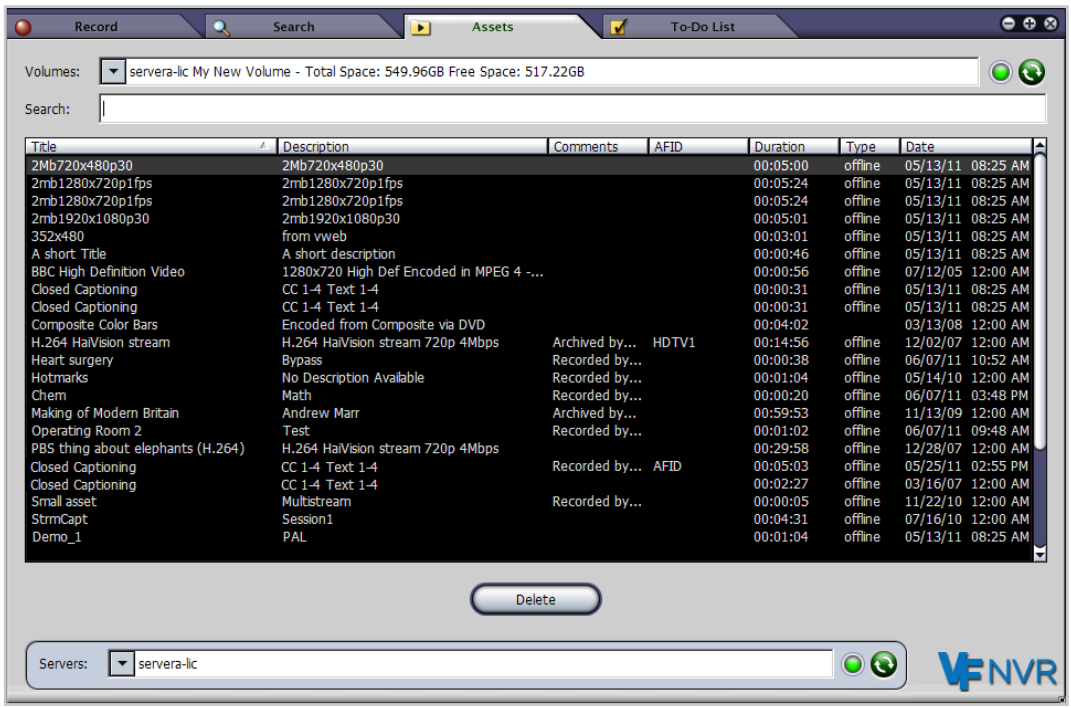
Viewing and Deleting Recorded Assets

From the Assets tab, you can view a list of the assets or shows that have previously been recorded. You can search the list to find a previously recorded asset, as well as delete assets from the list.

To view the previously recorded assets:

1. Click the Assets tab.

   The Assets tab also displays the list of volumes that contain assets as well as the contents of the volume on the NVR server.



TIP If an asset that has recently been recorded has not yet shown up in the Asset List, click the Assets Refresh button (next to the Volumes).

---

2. To delete an asset from the list, highlight the asset and click Delete.

CHAPTER 11: Managing Video on Demand

This chapter describes the Viper NowAdmin Web interface tool available to system administrators to manage system-wide Viper Now (Video on Demand) resources.

Topics In This Chapter

Viper NowAdmin - Making Assets Available On-Demand 180
Adding a Viper Now Link 180
Viper Now Resource Link Fields 185
Adjusting Viper Now Server Configuration Settings 187
Viper Now Global Options Fields 188

Viper NowAdmin - Making Assets Available On-Demand

Viper NowAdmin is an asset management tool used to make video assets available for on-request viewing.

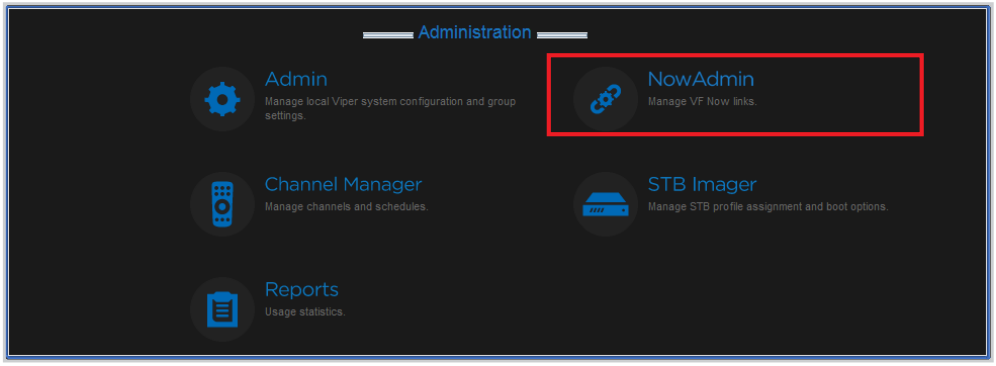
Assets stored in the system are not made available to users for viewing from Viper Now by default. Assets published to Viper still appear in the portal's Video on Demand Library. However, they will not appear in the STB's VoD list unless they have a Viper Now link created.

To enable a user to see the video on-demand, the asset must be assigned to a unique "link" which users can visit to launch and view the asset. This link can be edited, disabled or deleted at any time via the Viper NowAdmin tool to better control access to the asset.

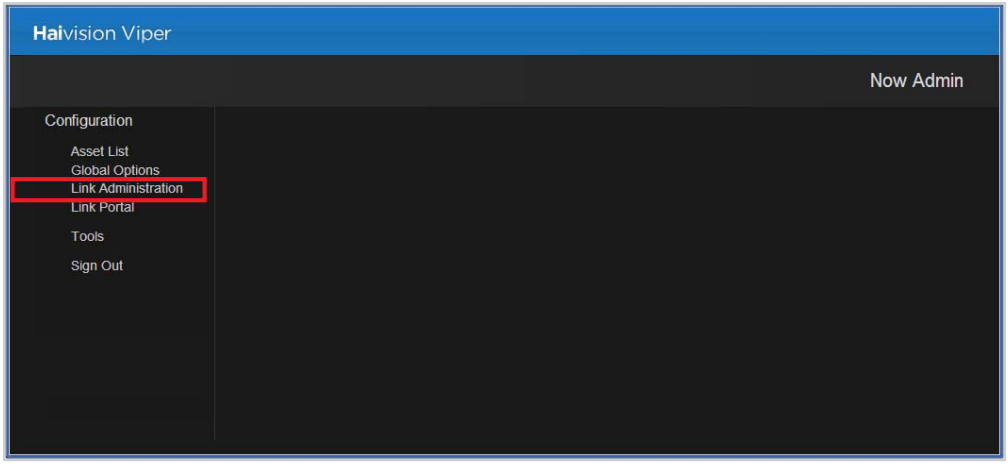
Adding a Viper Now Link

To add a Viper Now Link

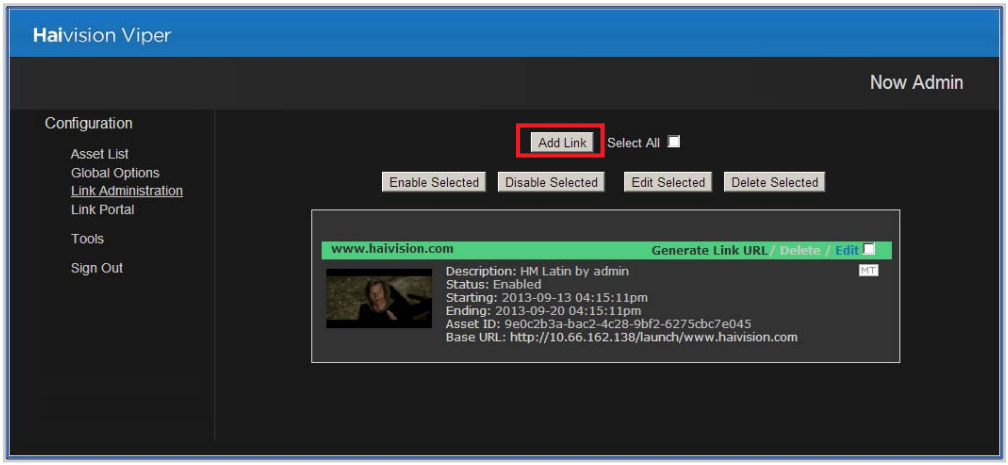
1. On the Tools page, click the Viper NowAdmin icon under the Administration section.



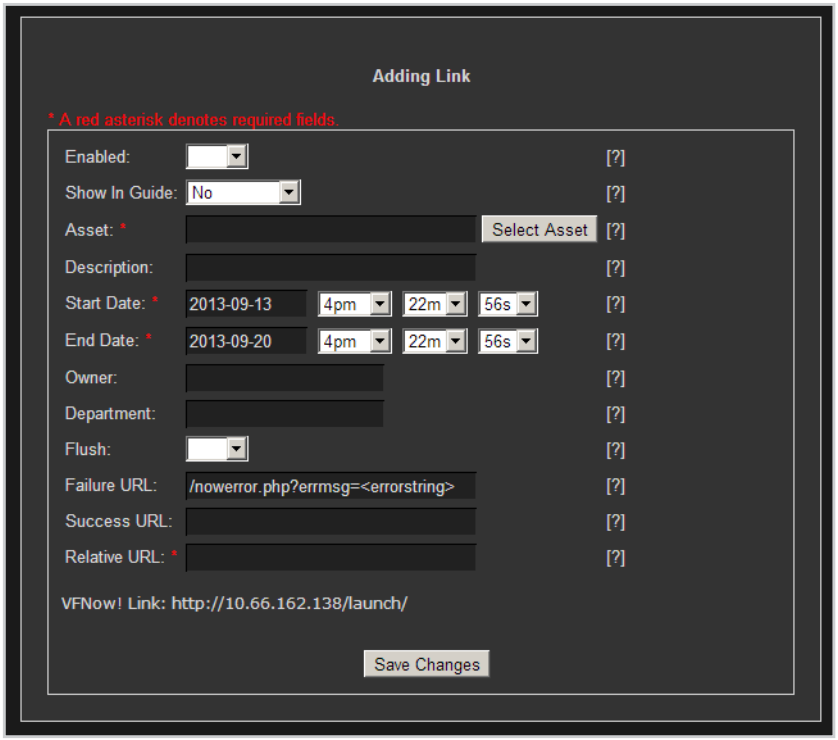
2. Click Link Administration on the left side of the Viper NowAdmin Welcome page.



3. On the Link Administration page, click Add Link.



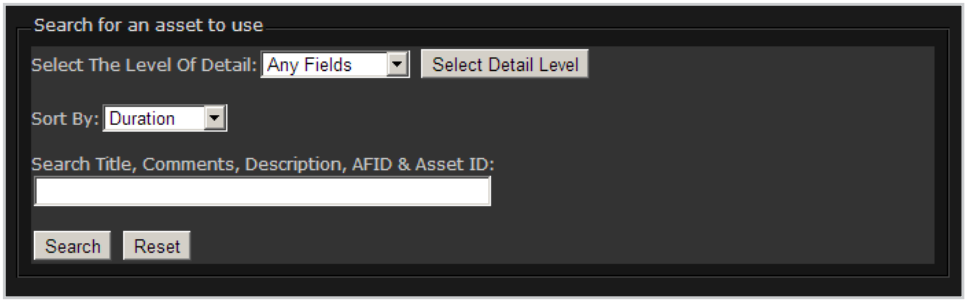
The Adding Link page opens with fields for you to define the link.



TIP For information on the Adding Link fields, see "Viper Now Resource Link Fields" on page 185.

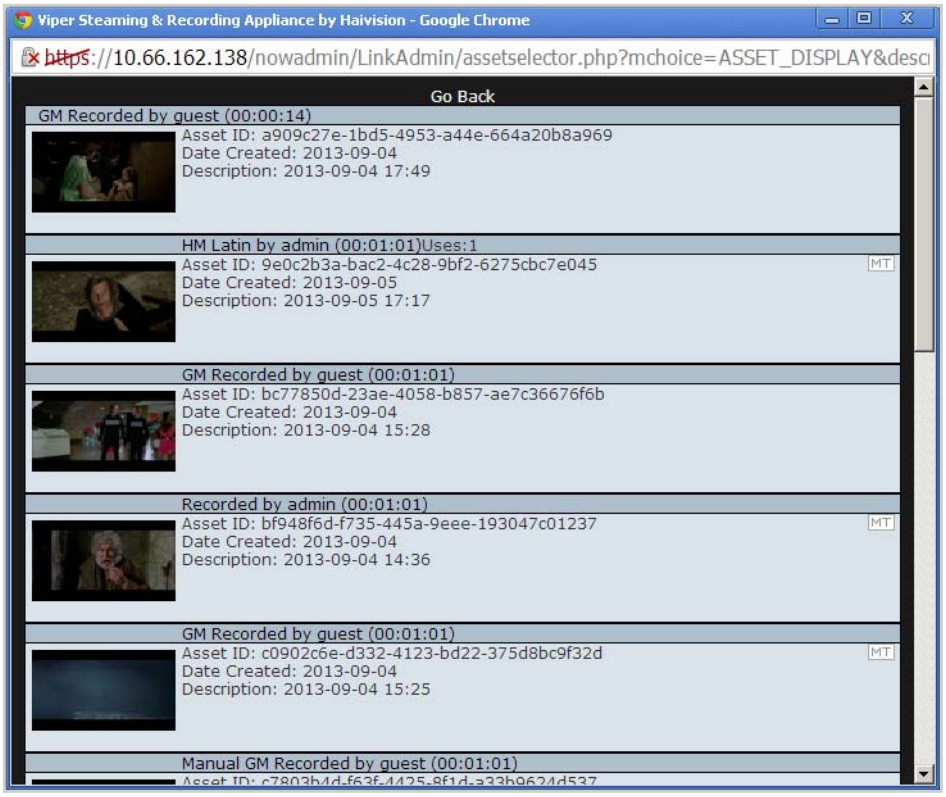
4. Select Yes for Enabled to enable the link. (If set to Disabled, viewers will be directed to the Failure URL when they attempt to launch the link.)

5. Show In Guide controls whether the asset is shown in the STB program listings. Assets may be available on the Viper Now page without being shown for on-demand launching within the live InStream player.
   - Select No to limit it to the Viper Now page only.
   - Select All Lineups to allow all users to launch the video from the InStream player's listing.
   - If your system contains multiple lineups, you may select one particular lineup (if available on your system) to which the link will be limited. (See "Lineup Editor - Managing the Channel Lineup" on page 140.)
6. Click Select Asset to choose the asset.
7. On the Search Asset window (shown below), you can either click Search to show all defined assets or you can filter your search.



You can also sort the display of your search results. For example, select a criterion such as Title from the Sort By drop-down list and then click Search (still leaving the Search field empty to show all assets in the database).

8. On the Asset List page, scroll down the list until you find the asset to assign and click that asset to select it.



This asset is now assigned to the Viper Now resource link that you are creating. The Asset List page closes and you are returned to the Adding Link page.

9. In the Description field, type a short descriptive name.

10. (Optional) To change the end date to your preferred expiration date, adjust the date and time of the End Date fields. (The default “End” date of the Viper Now link is one week in the future.)

    Regardless of where it is referenced (i.e., your own or a third party portal), the link will only be active and will only be displayed in the Viper Now demo portal between the start and end dates you specify.

11. Type the name of the asset in the Relative URL field, and press the ENTER key (or click elsewhere on the page). This is a name for the URL that Viper NowAdmin will use in generating the Viper Now resource link to refer to the selected asset.

    The URL below the input fields will update automatically as you type to include this name to complete the URL. As long as the VoD Link has not been deleted, the system will either launch the video or display the appropriate failure page when users attempt to visit that link.

12. To activate the link for use per the configured start and end dates, click Save Changes.

NOTE After you save your new link, the portal shows the list of active links with your new link at the top of the list as shown in the following image. Observe that the link name, status, creator, start/end dates, asset ID, and the URL are displayed here too. The URL displayed here is the same as the URL shown in the Add a Now Link dialog box above and may be copied and pasted to your own custom web portal. This is the same link used in the Now launch portal shown on the following page. Only the creator of the link may edit or delete it.

13. Click Sign Out at the left of the page and close the browser session.

The Viper Now portal shows the new link you created to make your video available for on request viewing. The link shows in this portal until you delete it or it expires.

NOTE The Viper Now portal displays only *active* resource links. If the current time is outside the bounds of the configured Start and End Date for the link, it will be absent from the portal. When links have expired, viewers who try to reach the link are directed to an error page which states that the link has expired. The Viper Now server settings must be correct to enable launching and playing of the titles from the established links.

For information on the proper Viper Now server settings, refer to "Adjusting Viper Now Server Configuration Settings" on page 187.

TIP To customize the Viper Now viewing experience for your end users, click Generate Link URL on any existing Viper Now link as shown below and then click the **(help)** link on the Viper Now URL Generator page.

Viper Now Resource Link Fields

The following table describes the fields and drop-down lists displayed while creating or editing a Viper Now link.

Field Name	Description
Enabled	Enables or disables the link. The link will launch InStream to play the asset only if enabled. Selecting **[No]** disables the link from end-user access.
Show In Guide	Specifies whether to enable the link for access directly in the Guide. Select **[All Lineups]** to include the link in the Guide. TIP: Show In Guide must be enabled to make a Viper Now asset available to STBs for VoD viewing.
Created by	Indicates the user who created the link.
*Asset	Asset ID assigned to the Viper Now link. This is a required field.
Start Date	The first date and time that the link will be enabled to allow end users to launch the assigned asset.
End Date	The last date and time that the link will be enabled to allow end users to launch the assigned asset.
Owner	Text field to enter the name of the person who created the link.
Department	Text field to enter the department to which the link belongs, if any.
Flush	When set to **[Yes]**, the Viper Now link will be removed from the system when the date and time specified for the End Date occurs.
Failure URL	A fully qualified URL to which the end-user's Web browser will be directed upon a failure condition detected by the system. This provides the site with the ability to direct its users to a support web page tailored to the needs of the site for Viper Now session inaccessibility (such as bandwidth license exceeded). When left empty, the browser will return to the same portal page from which the Viper Now session was originally launched.
Success URL	A fully qualified URL to which the end-user's Web browser will be directed upon successful commencement of a Viper Now session. When left empty, the browser will return to the same portal from which the Viper Now session was launched.

Field Name	Description
*Relative URL	Type the text label that you wish to uniquely assign to the link created for this asset. Text typed in this field will be appended to the Viper Now link.
Viper Now Link	Read-only field that displays the URL that you need to put in your site's html portal if you would like to launch Viper Now services for this link outside of the Viper Now prototype portal. Simply copy and paste this link in your portal.
Save Changes	Clicking this button instructs the Viper Now system to create the link according to the configuration present when the button was clicked. Then changes are activated immediately and the link is made available per the configured start and end times identified.
Cancel	Clicking this button instructs the Viper Now system to abandon creation or modification of the link Viper Now link.

Please refer to "Adjusting Viper Now Server Configuration Settings" on page 187 for additional configuration details.

Adjusting Viper Now Server Configuration Settings

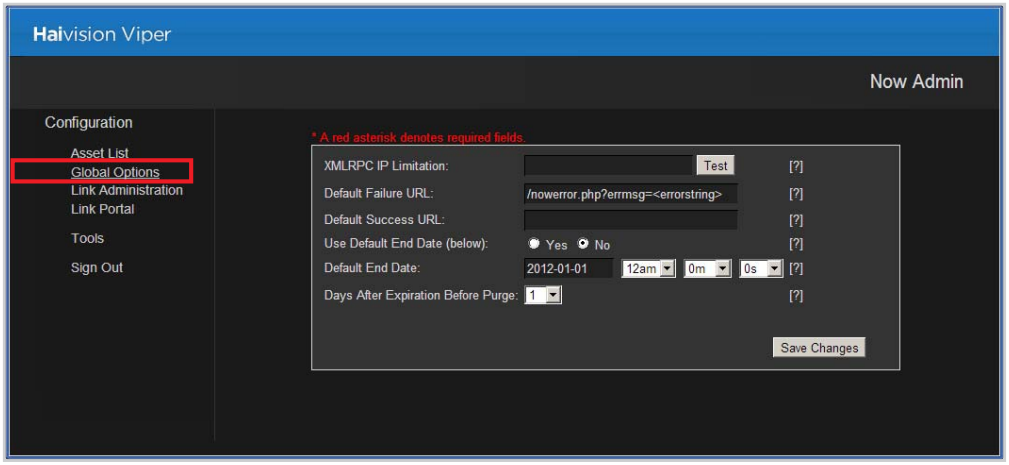
This section describes the Now server settings found in the Viper Now administration portal. These settings must be correct for a properly functioning Viper Now system.

If your Viper Now service seems unresponsive when you click a link on the Now launch page (e.g., 10.1.50.50/now), check whether the server settings match the syntax of those described below. Make necessary adjustments to your settings where they depart from the syntax below, keeping in mind that your server may have a different address than the examples that use “10.1.50.50”.

CAUTION Changing these settings to improper values will disable the Now service. This section uses a sample server address of “10.1.50.50” for the examples. Please refer to your site survey for the address of your Now server.

To adjust the Viper Now server settings:

1. Click Global Options on the left side of the Viper NowAdmin Welcome page.



   The Global Options page opens displaying the server settings.

   Under certain circumstances, server settings may need to be initialized or changed. However, do *not* make other changes without consulting Haivision Technical Support.

2. You may safely modify the Default Failure and Success URL fields, and the Default End Date and Time to suit your system.

3. To apply your changes to the server settings, click Save Changes.

CAUTION Please contact Haivision before changing any other settings. Changing these settings to erroneous values will disable Viper Now services.

Viper Now Global Options Fields

The following table lists the default settings and provides a description of each Global Options field.

SettingInStream	Description
Default Failure URL	The URL the browser is sent to if there is an error. May contain any URL even one of your own branded URLs. It is initialized to a Haivision error URL (e.g., /nowerror.php?errmsg=<errorstring>).
Default Success URL	The URL the browser is sent to after a successful launch.
Use Default End Date (below)	Enables or disables use/enforcement of default end date. If enabled, new assets will have their End Date pre-set to the Default End Date specified below. If this is not enabled, new links will default to expiring after 1 week (7 days).
Default End Date	Sets the default end date.
Days After Expiration Before Purge	The number of days to wait before removing expired links from the database.

Part IV: Reference

APPENDIX A: Glossary of Terms

AES	Advanced Encryption Standard
API	Application Programming Interface. For the purposes of this document, API refers to the collection of entities, operations and supporting materials provided with the Viper API.
Audio Bitrate	The number of bits used per unit of time to represent an audio stream. Measured in kilobits per second (kbps).
AVC	Advanced Video Coding. A standard for video compression, used for the recording, compression, and distribution of high definition video.
CBR	Constant Bit Rate. The encoder will generate a constant number of bits over a period of time.
CDN	Content Delivery Network.
CLI	Command Line Interface.
CRADA	Cooperative Research and Development Agreement.
FEC	Forward Error Correction.
Frame Rate	The video frame rate per second.
Furnace	Haivision's IP video management server.
GOP	Group of Pictures. In relation to the ViperViper, the GOP size specifies how often an I-Frame is sent.
HEVC	High Efficiency Video Coding. Also known as H.265 and MPEG-H Part 2. HEVC is a draft video compression standard, currently under development as a successor to H.264/MPEG-4 AVC (Advanced Video Coding).
Hi	Term use to refer to a high quality video encoding characterization of a given video input.
HLS	HTTP Live Streaming. An HTTP-based media streaming communications protocol created by Apple® Inc. as part of their QuickTime® and iPhone® software systems.

I-Frame	Intra Coded Picture, usually referred to as a reference frame. An I-Frame contains the full image of the picture (i.e., it is not a delta).
Input Presets	New set of input settings grouped under a central theme, which can be saved and recalled for later use.
JITC	Joint Interoperability Test Command.
JMIT	JITC Motion Imagery Tool.
Viper	Haivision's real-time stream-based video transcoder.
KLV	Key Length Value. Refers to metadata packets.
Lo	Term use to refer to a low quality video encoding characterization of a given video input.
MAC Address	Media Access Control address. A unique identifier assigned to a network interface card, usually assigned by the network card manufacturer.
MPEG TS	MPEG Transport Stream.
MTU	Maximum Transmission Unit. Specifies the maximum allowed size of IP packets for the encoded or transcoded stream.
NDPP	Network Device Protection Profile.
NIC	Network Interface Card.
OAuth	Open Authorization. An open standard for authorization.
PID	Packet Identification Number.
PIN	Personal Identification Number.
PMT	Program Map Table, a collection of PIDs available in a transport stream.
Resolution	The stream output resolution, i.e., the number of lines per frame and pixels per line to be encoded.
REST	Representational State Transfer. A style of software architecture for distributed hypermedia systems.
RTMP	Real Time Messaging Protocol. A protocol for streaming audio, video and data over the Internet, used primarily between an Adobe® Flash player and a server.
Session	New set of recording attributes grouped under a central theme, which can be saved and recalled for later use.
ST	Security Target.

SVC	Scalable Video Coding. An extension of the video compression standard H.264/MPEG-4 AVC.
ToS	Type of Service. Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams.
TTL	Time-to Live for stream packets. Specifies the number of router hops the Stream packet is allowed to travel/pass before it must be discarded.
UI	User interface.
VBR	Variable Bit Rate. VBR streams vary the amount of output data per time segment. VBR allows a higher bitrate to be allocated to the more complex segments of media streams while less space is allocated to less complex segments.
Video Bitrate	The number of bits used per unit of time to represent a video stream. Measured in kilobits per second (kbps).
Viper	Haivision's Multi-Stream Recording, Streaming & Publishing Appliance
VoD	Video On Demand. An interactive technology that allows users to select and view programming in real time or download programs and view them later.

APPENDIX B: Technical Specifications

This appendix lists the technical specifications for the Viper.

Topics In This Appendix

A/V Input Specifications 194
A/V Output Specifications 195
Advanced Features 195
Video Encoding 196
Audio Encoding 196
IP Network Interfaces 197
Management Interface 197
Physical 198

A/V Input Specifications

A/V Input Specifications	
Video (Inputs):	
	2 x DVI-I (Integrated)
	Y,Pb,Pr / RGBHV Component Analog
	Y,Cb,Cr / DVI Component Digital
	S-Video NTSC/PAL
	Composite NTSC/PAL
	SD-SDI SMPTE 259M-C
	HD-SDI SMPTE 292M, 274M, 296M
	3G-SDI SMPTE 424M, 425M
Video Resolutions:	
	1920x1080p 60/59.94, 50, 30/29.97, 25 Hz *
	1920x1080i 60/59.94, 50 Hz
	1280x720p 60/59.94, 50, 30/29.97, 25 Hz
	720x480/576p 60/59.94, 50 Hz
	720x480/576i ‘ 60/59.54/50 Hz *interlaced shown in fields per second
Computer Resolutions:	
	1920x1080 60 Hz *
	1280x1024 75/60 Hz*
	1280x768 85/75/60 Hz
	1280x720 60 Hz
	1024x768 85/75/60 Hz
Audio (Input):	
	1/8" (35mm) Mini Unbalanced stereo Analog Audio
	2 x RCA Unbalanced stereo Analog Audio

A/V Input Specifications (Cont.)	
	XLR Balanced Stereo Analog Audio
	BNC Embedded SDI Audio

*Dual stream high resolution (1080p) must fit within a 60 fps total budget

A/V Output Specifications

A/V Output Specifications	
Video (Outputs):	
	HDMI VGA, XVGA, SXVGA
Audio (Output):	
	1/8” (3.5mm) Mini Unbalanced stereo analog audio

Advanced Features

Advanced Features	
	Dual quality streaming
	HD SD De-interlacing
	Built-In Downscaling
	Deblocking Filter
	EIA-608-B Closed Captioning (NTSC Line 21)
	SO aspect ratio configuration
	SD AFD and WSS (HDSDI)
	Color space configuration (DVI) (Auto Detect)

Video Encoding

Video Encoding	
Compression Standards:	
	ITU H.264 AVC (MPEG-4 part 10) / ISO/IEC 14496-10 • Baseline / Main Profile • Level 4.2 and lower Intermediate Levels • I, IP framing only • Configurable Group of Picture (GOP) size • Configurable frame rate • Deblocking filter
Video Bitrates:	
	SD/HD from 150 kbps to 15 Mbps
Rate Control:	
	Constant (CBR) / Variable (VBR)
Encoding Latency:	
	Less than 100ms

Audio Encoding

Audio Encoding	
Compression Standards:	
	MPEG-2AAC-LC ISOIEI C 13818-7
	MPEG-4 AAC-LC ISOIEI C 14496-3
Audio Channels:	
	2 per video channel
Audio Bit Rates:	
	From 32 to 448 kbps per audio pair
Frequency Response:	
	From 20 Hz to 22 kHz

IP Network Interfaces

IP Network Interfaces	
Standard:	
	2x Ethernet 10110011000 Base-T, auto-detect, Half | Full-duplex
Connector:	
	RJ45
Networking Protocols:	
	Unicast Streaming
	Multicast Streaming (IGMP v3)
	MPEG Transport stream over UDP

Management Interface

Management Interfaces	
Standard:	
	RS-232 (future)
Management Protocols:	
	HTTPS (Web browser)
	LCD Touch Panel

Physical

Physical Specifications	
Dimensions (H x W x D):	
	108mm H x 219mm W x 267mm D (4.25“ x 8.62“ x 10.51“)
Weight:	
	Approximately 4.53 kg [10 lbs.]
Power:	
	100-240 VAC external locking power supply
Temperature:	
	Operating: 0° to 40° C [32° to 104° F]
	Non-operating: -40° to 70° C [-40° to 158° F]
Relative Humidity:	
	Up to 95% without condensation

APPENDIX C: Command Line Arguments

This alphabetical command reference lists and describes the available command line arguments that can be used with the Viper client applications.

Commands In This Appendix

Syntax Conventions 200
Introduction 201
All Applications 202
InStream 203
    InStream Multi-Stream Viewing 208
VF STB (Set Top Box) 209
VF NVR 211
VF Editor 212

Syntax Conventions

The following syntax conventions are used in this appendix:

Convention	Description
Courier font	Indicates command names and options, filenames and code samples.
italic font	Indicates variables that you replace with a user-defined value or name.
< >	Same as italics. Variables are enclosed in angle brackets in contexts that do not allow italics.
[ ]	Square brackets indicate optional items or parameters.
a | b	A vertical bar separates items in a list of options from which you must select one. If options are not separated by |, you may use combinations.
a - b	Items separated by a hyphen indicate a range of options from which you must select one.

Introduction

This command reference lists the command line arguments (CLA) that can be used with the Furnace client applications: Viper client applications: Viper (Desktop and STB), Editor, and NVR.

In most situations, it is not practical or advisable to launch the Viper applications directly from the command line. It is generally preferable to access the Viper software via the Web portal or Tools page, as this is the only way to be sure that the software will work correctly with the system.

CLA items may be set per user group, or for unauthenticated users launching Viper via the Launch Portal. These items are managed via the Admin module. This is the recommended method to utilize these command line arguments.

NOTE In the case of the Stingray Set Top Box (STB), these arguments are supplied to the STB via the “Command Line” field of the associated profile in the VF STB Imager tool. See “Using Command Line Arguments to Manage Launch Preferences” on page 52.

All Applications

Arguments	Description & Usage
-cu <URL>	Specifies the URL of a plain text file that contains additional command line options.
--date-format <0-5>	Sets the date and time format: NOTE: Date format is one of: • 0: 2011-01-25 • 1: 11-01-25 • 2: 25/01/11 • 3: 25/01/2011 • 4: 01/25/11 • 5: 01/25/2011 NOTE: Does not apply to NVR.
--date-long-format <0-3>	Sets the date and time format to one of the following long date formats: • 0: Wednesday, January 25 • 1: Wednesday, 25 January • 2: Wednesday 25 January • 3: Wednesday, 25.January NOTE: Does not apply to NVR.
-l <URL>, --license <URL>	Specifies the vfclam license server URL. NOTE: License server is typically at udp://<IP>:4902.
-pt <pagetag>, --page-tag <pagetag>	Loads the assigned channel lineup if available. When creating additional lineups, page tags are used to refer to each lineup. The page tag can be any numeric value, but each lineup *must* have a unique page tag in order to be used.
-u <ID>, --uuid <ID>	Specifies session or user UUID. NOTE: Normally done by PHP or part of CA integration.
-z <encoded text>	Encrypts the command line argument text for use in launch parameters. Makes the command line arguments unreadable for anyone watching packet traffic. NOTE: Custom text can be encrypted upon request.

InStream

Arguments	Description & Usage
-24	Sets the time display to 24-hour clock.
-at <asset-id> <track-id>	Plays the specific track of the asset specified. The first argument is the <asset-id> (identical to -a). The second is the <track-id> which usually starts at 0 (not guaranteed).
--bottomclip <val>, --leftclip <val>, --rightclip <val>, --topclip <val>	Specifies how much to clip off the video's border to hide overscan. NOTE: <val> specifies pixels. Default values are typically fine.
-cl --customer-logo-url	Specifies the URL of the PNG file containing a logo that will be displayed in upper left corner of the player. Can be used instead of Viper Branding options (see "Re-Branding the InStream Interface" on page 78). TIP: If you specify an invalid logo, e.g., "invalid_logo.png", the Haivision branding will be removed from the dashboard.
-ccd --closed-caption-disable	Disables access to the closed captioning controls.
--controls-disable	Disables all UI controls as well as mouse and keyboard interaction. NOTE: Should be used in conjunction with -x, -y, -w, -h to place to viewer window, as well as optionally --vubars and --status to monitor stream information.
-dc <cols>, --display-columns <cols> -dr <rows>, --display-rows <rows>	Changes the tiling patterns used for displaying streams. NOTE: Tiling pattern refers to the layout of rows and columns in the Multi-viewer grid.
--default-size <0-1>	Sets the window size on startup. NOTE: Size is one of: • 0 Minimized • 1 Fullscreen

Arguments	Description & Usage
-dip <param>, --decoder-init-parms <param>	Specifies decoder-specific parameters. NOTE: "D3D" is currently the only valid parameter – use Direct3D for video surfaces.
-h <val>, -w <val>	Sets the size of the window in pixels.
-hd --help-disable	Disables access to the Viper online Help (selectable from the Player Settings menu).
--hide	Hides the player window upon startup.
-hu <URL>, --help-url <URL>	Specific URL will launch in a Web browser if the "Technical Support" option is selected. NOTE: The "Technical Support" option is in the right-click context menu.
--layout <0-2>	Sets the multi-viewer layout. NOTE: Layout is one of: • 0 Normal • 1 Main Left • 2 Main Top
-ll <val>, --low-latency <val>	Adjusts latency response by setting buffer size. NOTE: Reasonable values are 0-2000. Correlates to "/;latency=" setting for stream URL.
-loop	Loops playback of stream/videos.
-m, --mute	Mutes audio on startup.
-ml, --mute-onlock	Mutes audio when locking the system. NOTE: Applies to: • Screensaver, power save, or screen lock (Windows); • Screensaver, or sleep from Apple menu (OS X).
-na, --no-audio	Disables audio.
-nd, --no-dashboard	Turns off the dashboard display on startup. NOTE: Hotkeys/menus are still accessible.

Arguments	Description & Usage
-ncc, --no-channel-changing	Channel cannot be changed by user. NOTE: The channel that is launched on startup will be the only channel visible in the guide for the duration of the player.
-nodnd, --no-drag-n-drop	Prevents the ability to drag-and-drop supported media files onto the player application for playback. NOTE: Typically configured by default at all installations in vfclamdcmdline.xml.
-oo, --overlay-on	Enables hardware overlays on startup. NOTE: Overlays are off by default.
-ot <pos> <size> <lum> <alpha> <text>, --overlaytext <pos> <size> <lum> <alpha> <text>	Starts the player with a text message being displayed as a video message. **Item: Meaning & Values:** • pos Screen position: 0-8 (see grid below) • size Text pt. size: 8-10 is a good range • lum Text brightness: 0-255 • alpha Text transparency: 0 (transparent) -255 (opaque) • text Message text: Special characters: %i = client IP, %m = client MAC address %D = date and time %I = IP address %M = MAC address %U = username NOTE: Screen positions correspond to the following locations: 0 1 2 3 4 5 6 7 8
-prd --preferences-disable	Disables the saving of player preferences that affect the layout. These include the location and size, layout, etc.

Arguments	Description & Usage
-r <URL>, --read <URL>	Tunes into specified URL on startup instead of a channel. NOTE: Typically a multicast stream (vftp://239.x.x.x:4900). May also be a published asset (uuid:<id>), or a local file: • absolute path (Windows): file:/C:/file.vfs • absolute path (linux): file:////home/user/file.vfs
-re <URL>, --read-exit <URL>	Launches InStream tuned to the specified asset at <URL>. Exits when the end of the video is reached. NOTE: Only applies to video assets that are launched as VoD. Typically a multicast stream (vftp://239.x.x.x:4900). May also be a published asset (uuid:<id>), or a local file: • absolute path (Windows): file:/C:/file.vfs • absolute path (linux): file:////home/user/file.vfs
-sap	Enables SAP (Secondary Audio Programming) mode upon startup.
-sm <0-9>	Specifies the monitor display to which the application will launch.
--station-logo	Enables the display of channel logos on top of the video feeds.
--status	Enables the text “status” line for stream display on startup.
-top	Enables “Video On Top” option on startup. The player window stays on top of other applications. NOTE: Does not apply to Mac OS X.
-url1	Tunes into the primary URL of channels as specified in Channel Editor. NOTE: This is the default behavior.
-url2	Tunes into the secondary URL of channels as specified in Channel Editor. NOTE: If there is no secondary URL configured, the player will present an error.

Arguments	Description & Usage
-v <0-100>, --volume <0-100>	Sets the volume level on startup.
--video-fullspeed <param>	Sets the behavior of stream playback upon startup. NOTE: <param> is one of: • all All streams play at full speed • active Only selected stream plays at full speed. Others show I-frames only • none No streams play at full speed - show I-frames only
-vot <time>, --vod-inactive-timeout <time>	Sets the VOD Idle timeout duration. NOTE: <time> specifies seconds.
--vubars	Enables the audio (Volume Unit) bars for stream display on startup.
-x <val>, -y <val>	Sets the startup position in pixels. NOTE: Top left corner of the screen is (0,0). Linux desktops: The player will not move past the boundaries of the screen with this option. May not work on Compiz-enabled Linux desktops.
-xp <0-100>, -yp <0-100>	Sets the startup position percentage. NOTE: Top left corner of the screen is (0,0). Linux desktops: The player will not move past the boundaries of the screen with this option. May not work on Compiz-enabled Linux desktops.

InStream Multi-Stream Viewing

Arguments	Description & Usage
-pd --pip-disable	Forces display of a multitrack stream using two viewers instead of display in a Picture-in-Picture window. NOTE: Only disables PIP for channels launched with -s. However, if a VoD asset is launched with -a, or if a VoD asset or a channel is selected from the Guide, it still launches with the PIP.
-ph, --pip-hide	Hides the Picture-in-Picture window on startup.
-pp <0-8>, --pip-position <0-8>	Sets the Picture-in-Picture window default position. NOTE: Window positions correspond to the following locations: 0 1 2 3 4 5 6 7 8
-ps <1-3>, --pip-size <1-3>	Sets the default Picture-in-Picture window size. NOTE: Size is one of: • 1 Small • 2 Medium • 3 Large
-pw, --pip-swap	Swaps the Primary and Picture-in-Picture windows on startup.

VF STB (Set Top Box)

Arguments	Description & Usage
-24	Sets the time display to 24-hour clock.
-a <asset-id>	Plays the specific asset id on startup. NOTE: <asset-id> is a UUID of a published asset that also is available as a current VOD link.
-cgmsa <0-3>	Copy Generation Management System Analogue level.
--disable-hdcp	Disables HDCP on the Stingray STB HDMI output port.
-dog, --dont-open-guide	Launches into “TV” mode by default, instead of “Guide” mode.
-dr	Disables remote control input.
-et, --epg-time	Sets the current time/timezone of the player to sync with the time of provided EPG data. NOTE: Typically set on STB profile command lines.
-g <URL>, --guide <URL>	Specifies the URL of the continuous guide data feed. NOTE: Typically a multicast address (udp://239.x.x.x:4901), specified in vfclamdcmdline.xml
-ll <val>, --low-latency <val>	Adjusts latency response by setting buffer size. NOTE: Reasonable values are 0-2000. Correlates to “/;latency=” setting for stream URL.
-loop	Loops playback of VoD video title.
-ls <pin>, --lock-screen <pin>	Locks screen on startup. NOTE: Accepts a 4-digit numeric pin code. The pin code must be entered in order to view content on a Stingray STB.
-m, --mute	Mutes audio on startup.

Arguments	Description & Usage
-mv <0-3>	Turns on Macrovision output for video display.
-r <URL>, --read <URL>	Tune into specified URL on startup instead of a channel. NOTE: Typically a multicast stream (vftp://239.x.x.x:4900). May also be a published asset (uuid:<id>).
-s <callsign>, --station <callsign>	Loads the specific channel as the default channel on startup.
-sap	Enables SAP (Secondary Audio Programming) mode upon startup.
-sp <password>, --setup-password <password>	Sets the password for accessing system setup menus. NOTE: Specified in the VF STB Imager Image Profiles Command Line field. Default is typically "1234".
-url1	Tunes into the primary URL of channels as specified in Channel Editor. NOTE: This is the default behavior.
-url2	Tunes into the secondary URL of channels as specified in Channel Editor. NOTE: If there is no secondary URL configured, the player will present an error.
-v <0-100>, --volume <0-100>	Sets the volume level on startup.
-vf <format>, --video-format <format>	Sets the output video format upon startup. NOTE: Typically used for configuring the STB for high definition televisions. Contact Haivision Technical Support for valid options.
-vot <time>, --vod-inactive-timeout <time>	Sets the VOD Idle timeout duration. NOTE: <time> specifies seconds.

VF NVR

Arguments	Description & Usage
-et, --epg-time	Sets the current time/timezone of the player to sync with the time of provided EPG data. NOTE: Typically set on STB profile command lines.

VF Editor

Arguments	Description & Usage
-dip <param>, --decoder-init-parms <param>	Specifies decoder-specific parameters. NOTE: "D3D" is currently the only valid parameter; use Direct3D for video surfaces.
-dp <path>, --default-path <path>	Specifies the file path that file selection dialogs will default to (open / save, etc.)
-scd, --save-clipped-default	"Saved Clipped Segment" is checked by default for "Save" functionality.

APPENDIX D: Warranty Information

Haivision One (1) Year Limited Warranty

Haivision warrants its hardware products against defects in materials and workmanship under normal use for a period of ONE (1) YEAR from the date of equipment shipment ("Warranty Period"). If a hardware defect arises and a valid claim is received within the Warranty Period, at its option and to the extent permitted by law, Haivision will either (1) repair the hardware defect at no charge, or (2) exchange the product with a product that is new or equivalent to new in performance and reliability and is at least functionally equivalent to the original product. A replacement product or part assumes the remaining warranty of the original product or ninety (90) days from the date of replacement or repair, whichever is longer. When a product or part is exchanged, any replacement item becomes your property and the replaced item becomes Haivision's property.

EXCLUSIONS AND LIMITATIONS

This Limited Warranty applies only to hardware products manufactured by or for Haivision that can be identified by the "Haivision" trademark, trade name, or logo affixed to them. The Limited Warranty does not apply to any non-Haivision hardware products or any software, even if packaged or sold with Haivision hardware. Manufacturers, suppliers, or publishers, other than Haivision, may provide their own warranties to the end user purchaser, but Haivision, in so far as permitted by law, provides their products "as is".

Haivision does not warrant that the operation of the product will be uninterrupted or error-free. Haivision does not guarantee that any error or other non-conformance can or will be corrected or that the product will operate in all environments and with all systems and equipment. Haivision is not responsible for damage arising from failure to follow instructions relating to the product's use.

This warranty does not apply:

(a) to cosmetic damage, including but not limited to scratches, dents and broken plastic on ports;

(b) to damage caused by accident, abuse, misuse, flood, fire, earthquake or other external causes;

(c) to damage caused by operating the product outside the permitted or intended uses described by Haivision;

(d) to a product or part that has been modified to alter functionality or capability without the written permission of Haivision; or

(e) if any Haivision serial number has been removed or defaced.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, HAIVISION SPECIFICALLY DISCLAIMS ANY AND ALL

STATUTORY OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. IF HAIVISION CANNOT LAWFULLY DISCLAIM STATUTORY OR IMPLIED WARRANTIES THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THIS EXPRESS WARRANTY AND TO REPAIR OR REPLACEMENT SERVICE AS DETERMINED BY HAIVISION IN ITS SOLE DISCRETION. No Haivision reseller, agent, or employee is authorized to make any modification, extension, or addition to this warranty. If any term is held to be illegal or unenforceable, the legality or enforceability of the remaining terms shall not be affected or impaired.

EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE EXTENT PERMITTED BY LAW, HAIVISION IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO OR CORRUPTION OF DATA; OR ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE HOWSOEVER CAUSED INCLUDING THE REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COSTS OF RECOVERING, PROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED OR USED WITH HAIVISION PRODUCTS AND ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF DATA STORED ON THE PRODUCT. THE FOREGOING LIMITATION SHALL NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS.

OBTAINING WARRANTY SERVICE

Before requesting warranty service, please refer to the documentation accompanying this hardware product and the Haivision Support Knowledge Base http://haivision.com/support/knowledge-base. If the product is still not functioning properly after making use of these resources, please contact your Authorized Reseller or Haivision at http://support.haivision.com using the information provided in the documentation. The Authorized Reseller or Haivision will help determine whether your product requires service and, if it does, will inform you how Haivision will provide it. You must assist in diagnosing issues with your product and follow Haivision's warranty processes.

Haivision may provide warranty service by providing a return material authorization ("RMA") to allow you to return the product in accordance with instructions provided by Haivision or Authorized Reseller. You are fully responsible for delivering the product to Haivision as instructed, and Haivision is responsible for returning the product if it is found to be defective. Your product or a replacement product will be returned to you configured as your product was when originally purchased, subject to applicable updates. Returned products which are found by Haivision to be not defective, out-of-warranty or otherwise ineligible for warranty service will be shipped back to you at your expense. All replaced products and parts, whether under warranty or not, become the property of Haivision. Haivision may require a completed pre-authorized form as security for the retail price of the replacement product. If you fail to return the replaced product as instructed, Haivision will invoice for the pre-authorized amount.

APPLICABLE LAW

This Limited Warranty is governed by and construed under the laws of the Province of Quebec, Canada.

This Limited Hardware Warranty may be subject to Haivision's change at any time without prior notice.

Haivision End User Software License Agreement

READ BEFORE USING

THE SOFTWARE PROGRAMS ARE PROTECTED BY NATIONAL AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES. READ THE TERMS OF THE FOLLOWING END USER (SOFTWARE) LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE PRODUCT. BY USING THE PRODUCT, YOU CONFIRM YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, HAIVISION IS UNWILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO INSTALL OR USE THE LICENSED SOFTWARES.

1. DEFINITIONS

1.1 Entitlement. The collective set of applicable documents authorized by Haivision Systems Inc. or its affiliate Haivision (collectively "Haivision) evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Licensed Software under this Agreement.

1.2 You (or Your). The individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.

1.3 License Fee. License Fee shall mean the consideration paid to Haivision for use of the Licensed Software. The License Fee is part of the price paid for the relevant Product.

1.4 Licensed Software. Licensed Software shall mean the executable version of Haivision's computer software, program or code, in object code format (specifically excluding source code), together with any related material including, but not limited to the Reference Manuals or database schemas provided for use in connection with the Licensed Software and including, without limitation, all Upgrades through the date of installation.

1.5 Reference Manuals. Reference Manuals shall mean the most current version of the documentation for use in connection with the Licensed Software provided by Haivision to You.

1.6 Updates. Updates shall mean any periodic software releases, additions, fixes, and enhancements thereto, release notes for the Licensed Software and related Reference Manuals, (other than those defined elsewhere in this section as Upgrades) which have no value apart from their operation as part of the Licensed Software and which add minor new functions to the Licensed Software, but none so significant as to warrant classification as an Upgrade, which may be provided by Haivision to fix critical or non-critical problems in the Licensed Software on a scheduled, general release basis. Updates to the Licensed Software ("Version") are denoted by number changes to the right of the decimal point for a version and revision number (for example going from 2.0.0 to 2.1.3).

1.7 Upgrades. Upgrades shall mean any modification to the Licensed Software made by Haivision, which are so significant, in Haivision's sole discretion, as to warrant their exclusion under the current license grant for the Licensed Software. Upgrades of Licensed Software are denoted by number changes to the left of the decimal point for a release number (for example going from 2.0 to 3.0).

2. RIGHTS GRANTED, RESTRICTIONS AND SUPPORT

2.1 License to Use.

(a) Subject to the terms and conditions set forth herein and subject to the terms of your Entitlement, Haivision hereby grants to You a non-exclusive, personal, limited and nontransferable right and license to use the Licensed Software in accordance with the terms of this Agreement. This license is granted to You and not, by implication or otherwise, to any parent, subsidiary or affiliate of Yours without Haivision's specific prior written consent. This license is for the limited use of the Licensed Software by You for the purpose of creating, managing, distributing and viewing IP Video assets. This license does not grant to You the right to use any Licensed Software in connection with any public broadcasting or broadcasting for home or residential purposes, or any license for content whatsoever. The license and rights granted to You in this Section (2.) do not include the right to sublicense to distributors, resellers and other third parties any of the rights granted to You in this Section (2.). All rights not expressly granted You in this Agreement are reserved to Haivision and no implied license results from this license.

2.2 Restrictions.

(a) Reproduction. You shall not copy, distribute, reproduce, use or allow access to any of the Licensed Software, except as explicitly permitted under this Agreement. You shall not modify, adapt, translate, export, prepare derivative works from, decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Licensed Software or any internal data files generated by the Licensed Software, or use the Licensed Software embedded in any third party hardware or software. You shall also not use the Licensed Software in an attempt to, or in conjunction with, any device, program or service designed to circumvent technological measures employed to control access to, or the rights in other work protected by copyright laws. You shall not remove, modify, replace or obscure Haivision's copyright and patent notices, trademarks or other proprietary rights notices affixed to or contained within any Licensed Software. No right is granted hereunder for any third party who obtains access to any Licensed Software through You to use the Licensed Software to perform services for third parties.

(b) Ownership. The Licensed Software is conditionally licensed and not sold. As between the parties, Haivision and/or its licensors owns and shall retain all right, title and interest in and to all of the Licensed Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein, and nothing in this Agreement shall be deemed to transfer to You any ownership or title to the Licensed Software. You agree that it will not remove, alter or otherwise obscure any proprietary rights notices appearing in the Licensed Software. All Haivision technical data and computer software is commercial in nature and developed solely at private expense.

3. TERM AND TERMINATION

3.1 Term. The license and service term are set forth in your Entitlement(s). Additionally, this Agreement may be terminated without cause by You upon thirty (30) days written notice to Haivision.

3.2 Termination for Breach. Your rights under this Agreement will terminate immediately without notice from Haivision if You materially breach it or take any action in derogation of Haivision's rights to Software. Haivision may terminate this Agreement should any Software become, or in Haivision's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation.

3.3 Termination; Effect; Survival. Upon the termination of this Agreement for any reason: (a) all license rights granted hereunder shall terminate; (b) You shall immediately pay to Haivision all amounts due and outstanding as of the date of such termination or expiration; and (c) You shall return to Haivision all Licensed Software and all Haivision Confidential Information not otherwise required under the terms of this Agreement or certify that all such Licensed Software and Confidential Information have been destroyed. Notwithstanding any termination of this Agreement, the following provisions of this Agreement shall

survive for the relevant period of time set forth therein, if any: Sections 2.2, 4.1, 4.2, and 6.

4. REPRESENTATIONS, DISCLAIMER AND LIMITATION OF LIABILITY

4.1 Haivision Warranty.

(a) Haivision warrants that the Licensed Software will operate substantially in accordance with the Reference Manuals provided for a term of ninety (90) days (the "Warranty Period") after its delivery date. As Your sole and exclusive remedy for any breach of this warranty, Haivision will use its commercially reasonable efforts to correct any failure of the Licensed Software to operate substantially in accordance with the Reference Manuals which is not the result of any improper or unauthorized operation of the License Software and that is timely reported by You to Haivision in writing within the Warranty Period, provided that in lieu of initiating commercially reasonable efforts to correct any such breach, Haivision may, in its absolute discretion, either (i) replace the Licensed Software with other software or technology which substantially conforms to the Reference Manuals or (ii) refund to You a portion of the fee paid for the relevant Product, whereupon this Agreement shall terminate. This warranty shall immediately terminate if You or any third party makes or attempts to make any modification of any kind whatsoever to the Licensed Software.

(b) All proprietary Hardware, if any, will be subject to the then current warranty terms of Haivision. All non-proprietary Hardware, if any, is sold "AS IS"; however, to the extent that Haivision has the legal right to do so, Haivision hereby transfers to You any and all warranties made by Haivision's vendors to Haivision with respect to such non-proprietary Hardware which was sold by Haivision or the Reseller to You, provided that You expressly acknowledge and agree that Haivision disclaims any and all liability in connection with any such non-proprietary Hardware, as set forth in Section 4.2(b) of this Agreement.

4.2 Warranty Disclaimers.

(a) THE EXPRESS WARRANTIES SET FORTH IN SECTION 4.1(a) ABOVE IN RESPECT OF THE LICENSED SOFTWARE ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING THE LICENSED SOFTWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANT-ABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS (ALL OF WHICH ARE DISCLAIMED). HAIVISION DOES NOT WARRANT THAT ANY OF THE LICENSED SOFTWARE WILL MEET ALL OF YOUR NEEDS OR REQUIREMENTS, OR THAT THE USE OF ANY OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE DETECTED OR CORRECTED.

(b) THE EXPRESS WARRANTIES SET FORTH IN HAIVISION'S WARRANTY TERMS IN RESPECT OF HAIVISION PROPRIETARY HARDWARE ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING ANY SUCH PROPRIETARY HARDWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALL NON-PROPRIETARY HARDWARE SOLD BY HAIVISION OR THE RESELLER TO YOU IS SOLD "AS IS" EXCEPT FOR HAIVISION'S AGREEMENT TO TRANSFER TO YOU ANY WARRANTY GIVEN TO IT BY ANY VENDOR FROM WHOM SUCH HARDWARE WAS PURCHASED FOR RESALE TO YOU HEREUNDER IN ACCORDANCE WITH THE PROVISIONS OF SECTION 4.1(b), AND HAIVISION DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING ANY SUCH NON-PROPRIETARY HARDWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

4.3 Liability Limitation. IN NO EVENT SHALL HAIVISION OR ITS OFFICERS, EMPLOYEES, AGENTS, REPRESENTATIVES, MEMBERS OF HAIVISION, NOR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED SOFTWARE, BE LIABLE TO YOU, YOUR CUSTOMERS OR TO ANY OTHER THIRD PARTY FOR CONSEQUENTIAL, INDIRECT, INCIDENTAL OR SPECIAL DAMAGES, LOST PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY DAMAGES FOR ANY BREACH OF THE TERMS OF THIS AGREEMENT OR FOR LOST OR CORRUPTED DATA ARISING FROM ANY CLAIM OR ACTION HEREUNDER, BASED ON CONTRACT, TORT OR OTHER LEGAL THEORY AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. HAIVISION SHALL NOT BE LIABLE FOR DAMAGES FOR ANY CAUSE WHATSOEVER IN AN AMOUNT IN EXCESS OF THE FEE PAID TO HAIVISION BY YOU FOR THE RELEVANT PRODUCT.

5. INDEMNIFICATION

5.1 Indemnification by Haivision.

(a) Haivision shall indemnify and hold You harmless against any and all actions, claims, losses, damages, liabilities, awards, costs and expenses (including reasonable attorneys' fees) ("Claims") arising out of i) any accusation or purported violation of any third person's US and copyright, trademark, patent rights or trade secrets, proprietary information on account of Your use of the Licensed Software when used in accordance with the terms of this Agreement, or (ii) relating to or arising out of any negligence or wilful misconduct on the part of Haivision or any breach by Haivision of the terms of this Agreement or any Maintenance and Support Agreement, or applicable law. You shall promptly notify Haivision in writing of any such Claim and promptly tender the control of the defense and settlement of any such Claim to Haivision. Haivision shall thereafter undertake the defense of any such Claim using counsel of its choice. You shall cooperate with Haivision, in defending or settling such Claim at the expense of Haivision; provided that Haivision shall not settle any Claim against You which would require the payment of money by You without the prior written consent of You, which consent shall not be unreasonably withheld. You shall have the right to consult and provide input into the defense with counsel of its choice at its own expense. Haivision shall not reimburse You for any expenses incurred by You without the prior written approval of Haivision, which approval shall not be unreasonably withheld.

(b) If any Licensed Software is, or in the opinion of Haivision may become, the subject of any Claim for infringement, then Haivision may, or if it is adjudicatively determined that any of the Licensed Software infringes in the manner described above (except to the extent that any translation, modification, addition or deletion or combination by You is the sole source of such Claim), then Haivision shall, at its option, either (i) procure for You the right to continue use of the Licensed Software for the term hereof, (ii) replace or modify the Licensed Software with other suitable and reasonably equivalent products so that the Licensed Software becomes non-infringing, or (iii) terminate this Agreement and refund to You a portion of the fee paid for the relevant Product.

(c) Haivision shall have no liability for: (i) the use of other than the then current release of the Licensed Software; (ii) the use of the Licensed Software other than as set forth in its accompanying documentation and as permitted herein; (iii) the modification of any of the Licensed Software by any party other than Haivision; or (iv) any infringement arising from the use of any Licensed Software by You after Haivision has issued a written notice to You requiring You to cease using such Licensed Software when Haivision exercises its option to terminate the License pursuant to Section 3.2 (collectively, "Exclusions"). SECTION 5.1 STATES HAIVISION'S ENTIRE OBLIGATION WITH RESPECT TO ANY CLAIM REGARDING THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

5.2 Indemnification by You. You shall indemnify and hold Haivision harmless against any and all Claims directly or indirectly arising out of, or in any manner whatsoever associated or connected with Your performance, purported performance or non-performance of its rights and obligations under this Agreement,

and against any and all Claims incurred by or on behalf of any of the foregoing in the investigation or defense of any and all such Claims.

6. OTHER PROVISIONS

6.1 Export and Other Restrictions. This Agreement, and all Your rights and Your obligations under this Agreement, are subject to all applicable Canadian and U.S. Government laws and regulations relating to exports including, but not limited to, the U.S. Department of Commerce Export Administration Regulations and all administrative acts of the U.S. Government thereunder. In the event the Licensed Software or the Hardware is exported from the United States or re-exported from a foreign destination, You shall ensure that the distribution and export/re-export of the Licensed Software or the Hardware is in compliance with all laws, regulations, orders, or other restrictions of the U.S. Export Administration Regulations. You agree that neither it nor any of its Affiliates will export/re-export any Licensed Software, Hardware, technical data, process, Products, or service, directly or indirectly, to any country for which the Canadian government or United States government (or any agency thereof) requires an export license, other governmental approval, or letter of assurance, without first obtaining such license, approval or letter.

6.2 Publicity. Neither party shall make or authorize or permit any other person to make any announcement or other like statement concerning this Agreement or the subject matter, terms or conditions hereof, without the other party's prior written consent.

6.3 Transfer and Assignment. Haivision may assign, sublicense, or transfer this Agreement and/or any or all of its rights or obligations hereunder. You may not assign, transfer or delegate any of its rights or obligations hereunder (whether by operation of law or otherwise) without the prior written consent of Haivision. Any unauthorized assignment, transfer or delegation by You shall be null and void. No other Person shall have or acquire any right under or by virtue of this Agreement.

6.4 Waiver and Amendment. No modification, amendment or waiver of any provision of this Agreement shall be effective. No failure or delay by either party in exercising any right, power or remedy under this Agreement, except as specifically provided herein, shall operate as a waiver of any such right, power or remedy. Without limiting the foregoing, any terms and conditions of the Entitlement or similar materials submitted by either party to the other shall be of no force or effect.

6.5 Enforcement by Third Party. For any Licensed Software licensed by Haivision from other suppliers, the applicable supplier is a third party beneficiary of this Agreement with the right to enforce directly the obligations set forth in this Agreement against You.

6.6 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Province of Québec, Canada and the Laws of Canada applicable therein (excluding any conflict of laws rule or principle, foreign or domestic).

6.7 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law and the remaining provisions of this Agreement shall remain in full force and effect.

6.8 Force Majeure. Neither party shall be liable to the other party for any failure or delay in performance to the extent that such delay or failure is caused by fire, flood, explosion, war, terrorism, embargo, government requirement, labor problems, export controls, failure of utilities, civil or military authority, act of God, act or omission of carriers or other similar causes beyond its control. If any such event of force majeure occurs, the party delayed or unable to perform shall give immediate notice to the other party, and the party affected by the other's delay or inability to perform may elect, at its sole discretion, to terminate this Agreement or resume performance once the condition ceases, with an option in the affected party to extend the period of this Agreement up to the length of time the condition endured. Unless written

notice is given within 30 calendar days after the affected party is notified of the condition, the latter option shall be deemed selected. During an event of force majeure, the affected party shall exercise reasonable effort to mitigate the effect of the event of force majeure.

If you have questions, please contact Haivision Systems Inc., 4445 Garand, Montréal, Québec, H4R 2H9 Canada.