



# DMG 7000

## Internet Distribution Gateway

---

### User Manual

## Copyright

© 2022 Sencore, Inc. All rights reserved.  
3200 Sencore Drive, Sioux Falls, SD USA  
[www.sencore.com](http://www.sencore.com)

This publication contains confidential, proprietary, and trade secret information. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any machine-readable or electronic format without prior written permission from Sencore. Information in this document is subject to change without notice and Sencore Inc. assumes no responsibility or liability for any errors or inaccuracies. Sencore, Sencore Inc., and the Sencore logo are trademarks or registered trademarks in the United States and other countries. All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries should be made directly to those companies. This document may also have links to third-party web pages that are beyond the control of Sencore. The presence of such links does not imply that Sencore endorses or recommends the content on those pages. Sencore acknowledges the use of third-party open source software and licenses in some Sencore products. This freely available source code can be obtained by contacting Sencore Inc.

## About Sencore

Sencore is an engineering leader in the development of high-quality signal transmission solutions for the broadcast, cable, satellite, IPTV, telecommunications, and professional audio/video markets. The company's world-class portfolio includes video delivery products, system monitoring and analysis solutions, and test and measurement equipment, all designed to support system interoperability and backed by best-in-class customer support. Sencore meets the rapidly changing needs of modern media by ensuring the efficient delivery of high-quality video from the source to the home. For more information, visit [www.sencore.com](http://www.sencore.com).

---

## Revision History

Date	Version	Description	Author
6/21/2019	0.1	First Draft	TDH
7/12/19	0.2	Updated draft	TDH
7/29/19	0.3	Revised draft	TDH
8/22/19	1.0	Initial Release	TDH
1/23/20	1.1	Correct latency range error in Zixi receive and transmit tables	TDH
6/5/2020	1.2	1.9.0 Feature Release	BCR
3/23/2021	1.3	1.10.0 Feature Release	BCR
10/19/2021	1.4	1.11.0 Feature Release	IWG
1/24/2022	1.5	1.12.0 Software Release	IWG

## Safety Instructions


- Read and follow all instructions
- Keep this manual
- Heed all warnings
- Do not use this apparatus near water
- Clean only with dry cloth
- Do not block any ventilation openings. Install in accordance with the manufacturer's instructions
- Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat
- Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
- Only use attachments/accessories specified by the manufacturer.
- Unplug this apparatus during lightning storms or when unused for long periods of time.
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
- Do not expose this apparatus to dripping or splashing liquids and ensure that no objects filled with liquids, such as vases, are placed on the apparatus.
- To completely disconnect this apparatus from the AC Mains, disconnect the power supply cord plug from the AC receptacle.
- The mains plug of the power supply cord shall remain readily operable.
- **Damage Requiring Service:** Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power-supply cord or plug is damaged.
  - If liquid has been spilled, or objects have fallen into the product.
  - If the product has been exposed to rain or water.
  - If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions as an improper adjustment of the controls may result in damage and will often require extensive work by a qualified technician to restore the product to its normal operation.
  - If the product has been dropped or damaged in any way.
  - The product exhibits a distinct change in performance.
- **Replacement Parts:** When replacement parts are required, be sure the service technician uses replacement parts specified by Sencore, or parts having the same operating characteristics as the original parts. Unauthorized part substitutions made may result in fire, electric shock or other hazards.

## SAFETY PRECAUTIONS

**There is always a danger present when using electronic equipment.**

*Unexpected high voltages can be present at unusual locations in defective equipment and signal distribution systems. Become familiar with the equipment that you are working with and observe the following safety precautions.*

- Every precaution has been taken in the design of your product to ensure that it is as safe as possible. However, safe operation depends on you the operator.
- Always be sure your equipment is in good working order. Ensure that all points of connection are secure to the chassis and that protective covers are in place and secured with fasteners.
- Never work alone when working in hazardous conditions. Always have another person close by in case of an accident.
- Always refer to the manual for safe operation. If you have a question about the application or operation email [ProCare@Sencore.com](mailto:ProCare@Sencore.com)
- **WARNING** – To reduce the risk of fire or electrical shock never allow your equipment to be exposed to water, rain or high moisture environments. If exposed to a liquid, remove power safely (at the breaker) and send your equipment to be serviced by a qualified technician.
- To reduce the risk of shock the power supply must be connected to a mains socket outlet with a protective earth ground connection.
- For the mains plug the main disconnect and should remain readily accessible and operable at all times.
- When utilizing DC power supply, the power supply **MUST** be used in conjunction with an over-current protective device rated at 50 V, 5 A, type: Slow-blow, as part of battery-supply circuit.
- To reduce the risk of shock and damage to equipment, it is recommended to ground the unit to the installation's rack, the vehicle's chassis, the battery's negative terminal, and/or earth ground. Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

 **Warning:** *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

## Package Contents

The following is a list of the items that are included in the shipping carton:

1. DMG 7000 Chassis
2. DMG 7000 Software
3. AC Power Cable
4. Quick Start Guide

If any of these items were omitted from the packaging, please email [ProCare@Sencore.com](mailto:ProCare@Sencore.com) to obtain a replacement.

## Table of Contents

<b>Section 1 Appliance Install and Overview .....</b>	<b>9</b>
1.1 Product Introduction.....	10
1.2 Power Connection .....	10
1.3 Maintenance .....	11
1.4 Network Setup via KVM.....	11
1.5 Front Panel Overview .....	11
1.6 Rear Panel Overview.....	13
<b>Section 2 Software Installation .....</b>	<b>15</b>
<b>Section 3 Web Interface Operation.....</b>	<b>18</b>
3.1 Logging into the DMG Web Interface .....	19
3.2 Control Panels .....	19
3.3 Title Ribbons .....	20
3.4 Buttons and Status Indicators.....	20
3.5 System Details with Global View .....	22
<b>Section 4 Web Interface Control Panels .....</b>	<b>23</b>
4.1 Gateway Control Panel .....	24
4.1.1 Adding a Gateway .....	25
4.1.2 Gateway Receive Settings .....	26
4.1.2.1 MPEG/IP Receive Settings.....	27
4.1.2.2 SRT Receive Settings.....	30
4.1.2.3 Zixi Receive Settings .....	33
4.1.2.4 HLS Receive Settings.....	36
4.1.2.5 Seamless RTP Receive Settings.....	38
4.1.2.6 RIST Receive Settings.....	40
4.1.3 Gateway Transmit Settings .....	43
4.1.3.1 MPEG/IP Transmit Settings.....	44
4.1.3.2 SRT Transmit Settings.....	46
4.1.3.3 Zixi Transmit Settings .....	49
4.1.3.4 RIST Transmit Settings.....	53
4.1.4 Additional Receive Instances .....	56
4.1.5 Configuring Active Inputs and Failover.....	57
4.1.6 Additional Transmit Instances .....	58
4.2 Admin Control Panel.....	59
4.2.1 Changing Unit Password .....	59
4.2.2 Profiles.....	60
4.2.3 SNMP MIB files .....	60
4.2.4 Diagnostics .....	61
4.2.5 Security Manager .....	62
4.2.5.1 Enabling DTLS.....	64
4.2.6 Updating the System Software .....	65
4.2.7 Reboot the Unit.....	66
4.2.8 Reset to Defaults .....	67
4.2.9 Unit Alias.....	67
4.2.10 Configuring the Unit Networks and VLANs .....	68
4.2.11 SSH Tunnels .....	71
4.2.12 License Information .....	73
4.2.13 Setting Unit Time and Date .....	73
4.2.14 Configuring SNMP.....	74
4.2.15 Syslog.....	75
4.3 Reporting Control Panel .....	76

---

4.3.1	Alarms.....	76
4.3.2	Configuring the Alarms .....	77
4.3.3	Event Logs.....	79
4.3.4	Configuring the Logs .....	80
4.4	About Panel .....	80
4.4.1	System Information.....	80
4.4.2	Contact Information .....	80
4.4.3	Options .....	81
4.4.4	Third Party Software Information.....	81
<b>Section 5 Appendices.....</b>		<b>82</b>
<b>Appendix A</b>	<b>– Specifications.....</b>	<b>83</b>
<b>Appendix B</b>	<b>– Error and Event List.....</b>	<b>86</b>
<b>Appendix C</b>	<b>– Internet Transport Protocol Explanation .....</b>	<b>88</b>
<b>Appendix D</b>	<b>– Acronyms and Glossary.....</b>	<b>90</b>
<b>Appendix E</b>	<b>– Warranty .....</b>	<b>91</b>
<b>Appendix F</b>	<b>– Support and Contact Information .....</b>	<b>92</b>
<b>Appendix G</b>	<b>– Open Source Software.....</b>	<b>93</b>



# Section 1 Appliance Install and Overview



## Introduction

This section includes the following topics:

1.1	Product Introduction.....	10
1.2	Power Connection .....	10
1.3	Maintenance .....	11
1.4	Network Setup via KVM.....	11
1.5	Front Panel Overview .....	11
1.6	Rear Panel Overview.....	13

## 1.1 Product Introduction

The DMG 7000 Internet Distribution Gateway is a software-based platform from Sencore aimed at transporting video/audio content over the internet. It bridges the gap between unmanaged and managed networks with protocols like MPEG/IP, RIST, SRT, Zixi, and HLS

The DMG 7000 can be purchased from Sencore as an appliance or installed as software on Ubuntu 18. Initial configuration can be done from mouse/keyboard/monitor or SSH. Once the management IP parameters are configured, the DMG 7000 can be operated and monitored via web interface, SNMP or Rest API over ethernet.

The DMG 7000 maintains the long standing Sencore tradition of coupling ease of use, with a straight-forward web interface to give the user complete control of the unit and signals being processed.

To obtain the associated documentation from the server manufacturer or detailed information regarding front of chassis indicator lights email [ProCare@Sencore.com](mailto:ProCare@Sencore.com)

## 1.2 Power Connection

The DMG 70010 Mini Unit will come with the necessary AC adaptor and power cord provided. To make the power connection, the user will

1. Insert the power cord to the adaptor;
2. Insert the adaptor to the DC power jack on the back of the DMG 7000 mini
3. Insert mate the power plug to a protected AC outlet

The DMG 70020 Field Unit has a single AC power connection provided on the chassis. To make the power connection, the user will

1. Locate the single AC power cord that is provided
2. Insert the female end into the DMG 7000 chassis
3. Insert the male end into a protected AC outlet

The DMG 70030 Headend unit will provide the user with a redundant AC power input. To make the power connection for this system, the user will

1. Locate the two (2) AC power cords that are provided
2. Insert the female ends into the two (2) open connections on the back of chassis
3. Insert the male ends of each AC power cord into separate protected AC outlets.

NOTE: Both AC connections should be active and complete or the system will sound an alarm indicating a power supply concern exists.

## 1.3 Maintenance

The DMG 7000 is a maintenance-free piece of equipment. There are no user serviceable parts on the inside of the unit. However, if the user has a need to pursue maintenance of any DMG 7000, please send an email request to one of our Sencore Pro Care members ([ProCare@sencore.com](mailto:ProCare@sencore.com)) asking for the documentation of their specific platform.

This same contact should also be used to request a copy of the latest DMG 7000 software, release notes, or other documentation.

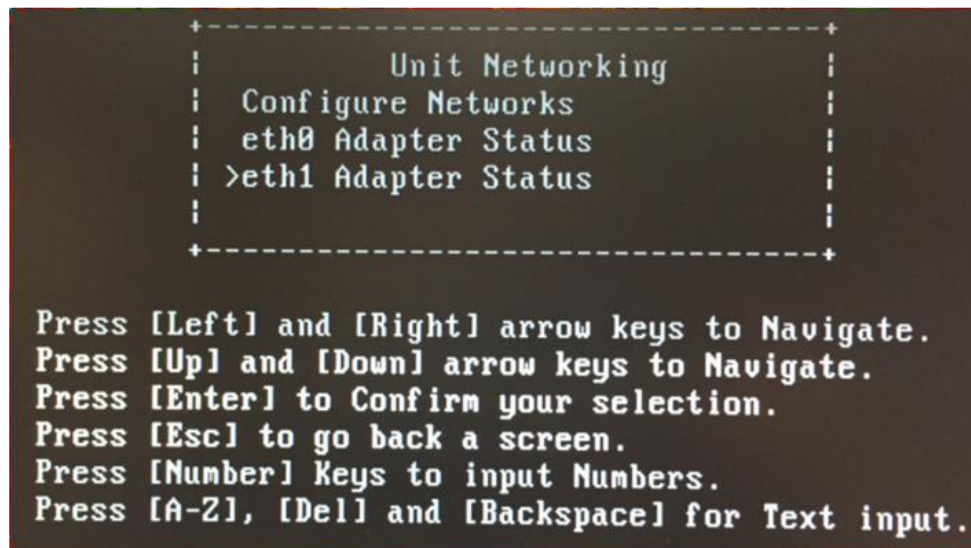
## 1.4 Network Setup via KVM

Connect the VGA (D-SUB) cable to a monitor and a USB keyboard.

The VGA will display the current Ethernet settings and provide a text-based menu to configure IP addressing, Subnet Mask, Gateway, and DNS settings.

Sencore recommends configuring the Eth0 port (Leftmost NIC when facing the rear of the unit) is set to a static IP for web-interface access. Ensure the user machine is also on the same network.

For additional information on initial network configuration menu see the Sencore DMG 7000 Quick-Guide documentation.



## 1.5 Front Panel Overview

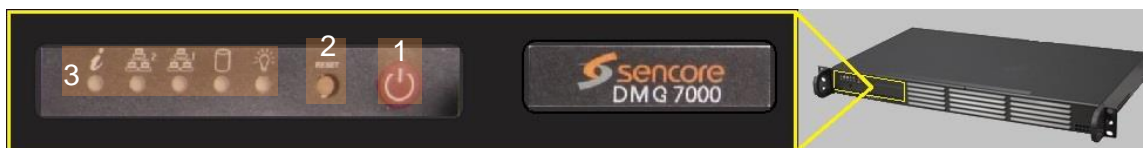
There are three form factors for the DMG 7000. There are details below for each front panel. Note that connectors without highlighting and description are not used by the DMG 7000 and should not be connected.

## The DMG 70010 Mini Unit



1. Power button
2. Status indicators for Power (PWR), Hard drive activity (SATA)
3. Two (2) USB 3.0 ports for keyboard and mouse connectivity

## DMG 70020 Field Unit



1. Power button
2. Reset button
3. Status indicators for Power (💡), Hard drive activity (💾), Management network activity (🌐), video network activity (🌐), and system status information (🔧).

## The DMG 70030 Headend unit



1. Power button
2. Reset button
3. Status indicators for Power, Hard drive activity, Management network activity, video network activity, and system status information.

## 1.6 Rear Panel Overview

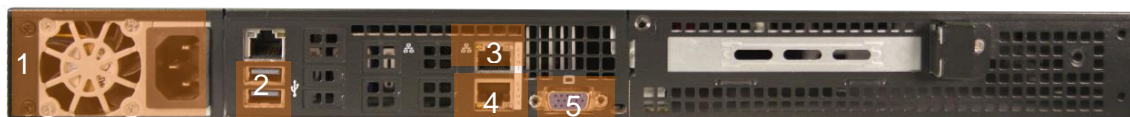
The DMG 7000 form factors back panels are described in the figures below. Note that connectors without highlighting and description are not used by the DMG 7000 and should not be connected.

### The DMG 70010 Mini Unit



1. RJ45 Ethernet ports for management of MPEG/IP
2. Two (2) USB 3.0 ports
3. USB 2.0 port
4. System Video Output ports – (1) HDMI, (1) Display port and (1) VGA port
5. Power input port (19VDC)

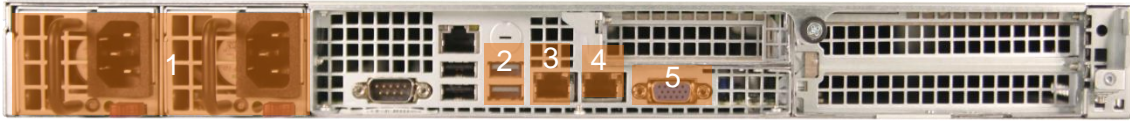
### The DMG 70020 Field Unit



1. Power supply (120/240 AC switching power supply)
2. USB ports (two) for keyboard and mouse connectivity
3. Eth0: One of two available RJ45 Ethernet ports for management or MPEG/IP
4. Eth1: One of two available RJ45 Ethernet ports for management or MPEG/IP
5. Local monitor output uses VGA (D-SUB) connector

---

### The DMG 70030 Headend unit



1. Redundant Power supplies (two 120/240 AC switching power supply)
2. USB ports (two) for keyboard and mouse
3. Eth0: One of two available RJ45 Ethernet ports for management or MPEG/IP
4. Eth1: One of two available RJ45 Ethernet ports for management or MPEG/IP
5. Local monitor output uses VGA (D-SUB) connector

## Section 2 Software Installation

This procedure is for customer's that are buying and installing DMG7000 software onto their own server and not one purchased from Sencore. The software can be loaded onto any server that meets the minimum server requirements listed in Appendix A. In order to enable the software, the customer will need to reach out to [sales@sencore.com](mailto:sales@sencore.com) to buy or get demo licenses.

### Installation Prerequisites

Before the installation can take place, prepare the hardware and network to be used with the DMG 7000.

1. Physically install (racked or mounted) the server hardware.
2. Install Ubuntu 18 operating system at:  
<https://ubuntu.com/download/server#releases>
  - a. It is recommended to install OpenSSH as well
3. Configure network ports and ensure connectivity to other devices in the network.
4. Setup a method for transferring installation files and licenses to the DMG 7000.  
This could be done remotely via SCP or physically via USB. WinSCP can be downloaded here: <https://winscp.net/eng/download.php>
5. Email the Sencore ProCare team at [procare@sencore.com](mailto:procare@sencore.com) for the DMG 7000 installation file.

**NOTE:** Tutorial for installing Ubuntu can be found at: <https://ubuntu.com/tutorials>

### DMG 7000 – Minimum Requirements

For 100Mbps of throughput

CPU:	Intel Quad-Core 1.1Ghz, up to 2.4Ghz
RAM:	4GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

For 250Mbps of throughput

CPU:	Intel Xeon 4-core 2.2Ghz
RAM:	8GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

For 850Mbps of throughput

CPU:	Intel Xeon 6-core 3.6Ghz
RAM:	16GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

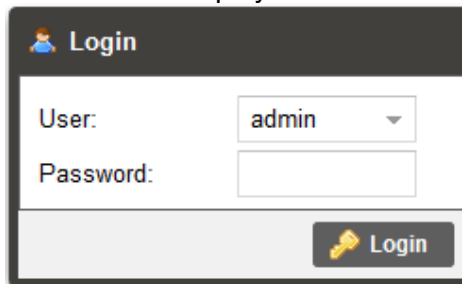
### Installation of DMG 7000 software

1. Transfer the DMG 7000 “.run” installation file to the /tmp/ directory onto the hardware prepared after the “Installation Prerequisites” steps.
2. From command prompt, use the following commands, without quotes, to install the DMG 7000 software. *Depending on OS settings, it may be necessary to run install commands as root or superuser.*
  - a. Type “cd /tmp” and press Enter
  - b. Type “sudo chmod +x DMG7000XXX.run” and press Enter
  - c. Type “sudo ./DMG7000XXX.run” and press Enter
    - i. NOTE: The install will begin, and the unit should reboot automatically.
  - d. Type “reboot” and press Enter if the machine does not reboot automatically.

## Request and Install Licenses

Request License for DMG 7000

1. Logging into the web gui.
2. Type the management IP address of the DMG 7000 in the browser URL field and press ENTER.
3. The DMG 7000 login screen will be displayed.

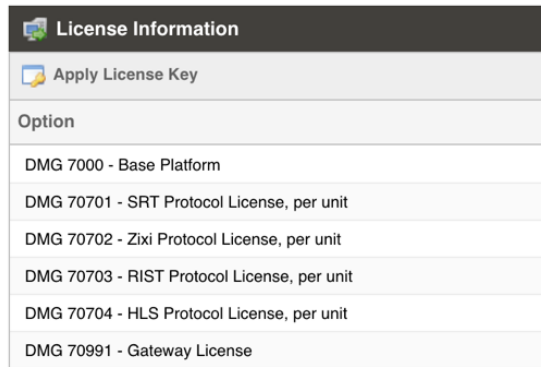
A screenshot of the DMG 7000 login interface. It features a dark header with a user icon and the word "Login". Below this is a white box containing a "User:" label with a dropdown menu showing "admin", and a "Password:" label with an empty text input field. At the bottom right of the white box is a dark button with a key icon and the word "Login".

4. The default user is **admin** and the default password is **mpeg101**.
5. Click login to continue.
6. Retrieve UUID from DMG 7000 user interface by navigating to the About tab.
7. Email the UUID to [sales@sencore.com](mailto:sales@sencore.com) to retrieve demo license or purchase license.

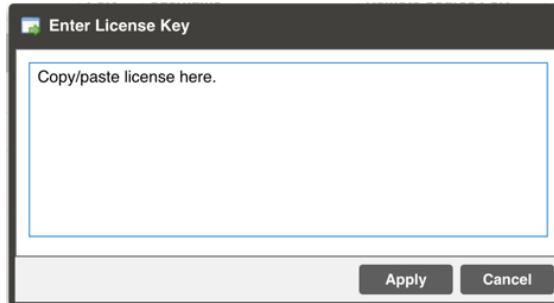
Install license for DMG 7000

1. Navigate to the Admin tab in the DMG 7000 user interface
2. Click the “Apply License Key” button in the License Information section.





3. Copy/paste the license key into the dialog box and click Apply.



4. The DMG 7000 will display the new licenses being added. Reboot. After the unit reboots, you will find the new licenses are applied.

# Section 3 Web Interface Operation

## Introduction

This section includes the following topics:

3.1	Logging into the DMG Web Interface .....	19
3.2	Control Panels .....	19
3.3	Title Ribbons .....	20
3.4	Buttons and Status Indicators.....	20
3.5	System Details with Global View .....	22

### 3.1 Logging into the DMG Web Interface

To open the DMG 7000 web interface use one of the following supported browsers and navigate to the unit's IP address:

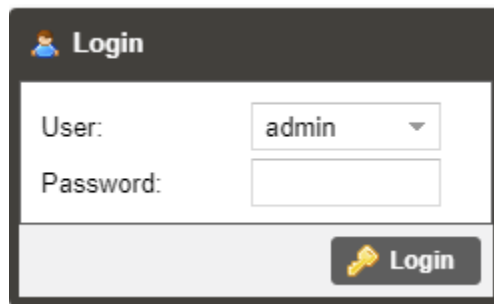
- Internet Explorer 11 & above
- Microsoft Edge 42 & above
- Firefox 77 & above
- Google Chrome 83 & above

The user will need to login to the web interface. By default the admin user account is available with “mpeg101” as the password. After entering the password, press the enter key or click the login button to login to the web interface.

#### Default Credentials

User: admin

Password: mpeg101



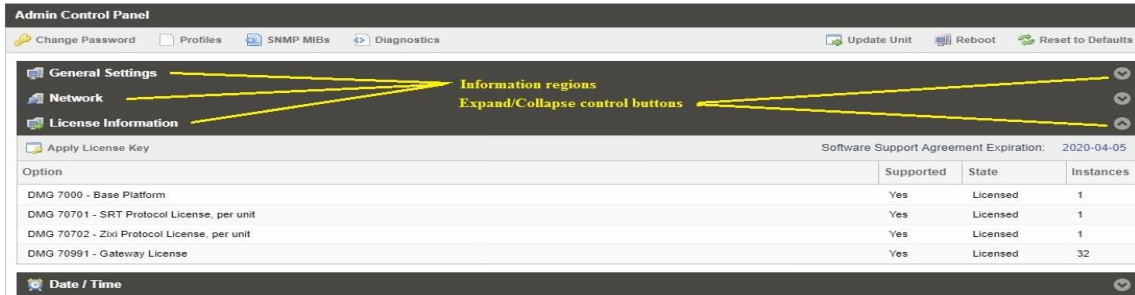
### 3.2 Control Panels

The web interface will provide complete control of unit configuration and process monitoring with four (4) separately defined control panels. Each control panel will be made up of unit features that are similar to each other to help the user easily locate the unit features they seek. The control panels are:

<b>Gateway</b>	This control panel is where the majority of the video stream processing configurations are managed.
<b>Admin</b>	This control panel is where unit hardware and administrative settings will be configured and monitored.
<b>Reporting</b>	This control panel is where alarms & logs are reported, configured and maintained.
<b>About</b>	This control panel is where unit software and hardware details are found.


### 3.3 Title Ribbons

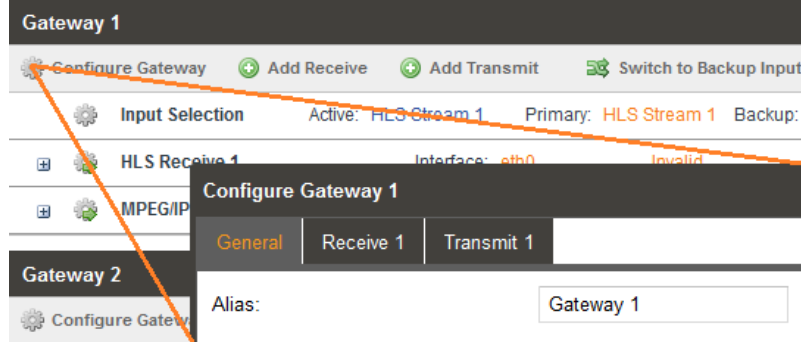
The “Gateway”, “Admin” and “About” control panels will group feature specific settings together under a title ribbon. Each ribbon presents an icon and description of settings that are offered. Each section can be expanded/collapsed with buttons at the right end as shown in the figure on the next page.




**Title Ribbons**

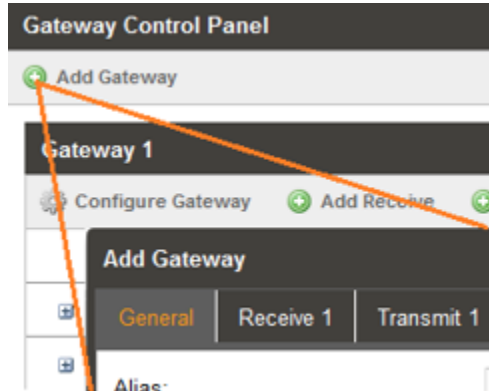
### 3.4 Buttons and Status Indicators

When the  icon is shown user configuration is available. Clicking this button will open menus where settings can be changed by the user.





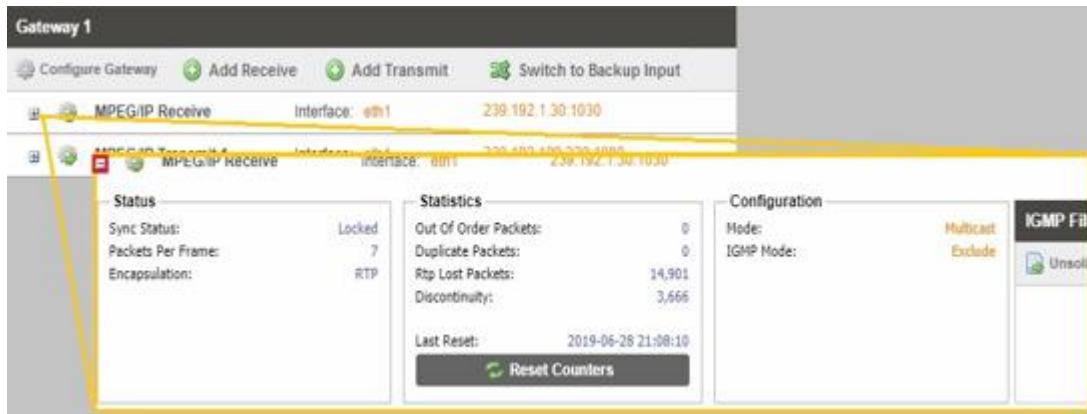
**Gateway Configuration Menu**

The green Add button  will allow the user to add new gateways or transmit paths to existing gateways. Similar to the configuration cog show above.






**Add Gateway Icon**

When the  icon is shown additional status information can be viewed. Click this button will expand the menu to display the additional status information. All text in status menus shown in **ORANGE** are **user configurable settings**. Text shown in **BLUE** report **status and details about the stream being processed**. Clicking the collapse icon  will close the details viewing window.



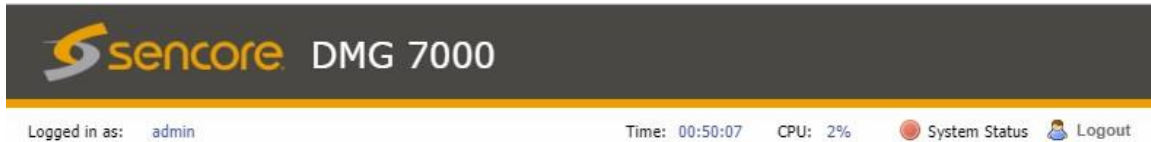
**Configurable Text vs Display Text**

Status in the DMG 7000 web interface is shown with LED status indicators:

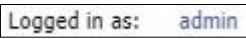
Green LED		Status is good. No errors are present and function is operating normally.
Red LED		Status indicates function is affected by active error. To view the errors, navigate to Alarms panel to view Active Errors.
Grey LED		Status is inactive. Function is currently disabled or unavailable.

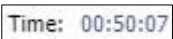
### 3.5 System Details with Global View

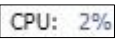
Some details are 'global' and can be viewed at all times when logged into the web client. These are displayed at the top of the page immediately under the model banner.





#### Global System Information

At the right (  ) is displayed the username currently accessing the web client.

Time (  ) is the next detail as you move to the left and it displays the current system time. This is a user defined setting and configuration of it is located on the Admin tab. The time value will be applied to reported system and alarm conditions found on the Reporting tab and in the log files.

The next detail is CPU status (  ) and is shown as a percentage. It reflects the amount of processing capacity that is currently being used.

Next is System Status (  System Status ) which reports the current status of the system. Green indicates the system operation is Good while Red indicates there is some detail about the system that is currently in Alarm condition. A Red condition prompts the user to seek further information about the Alarm condition by viewing the Reporting tab.

Finally, the Logout button (  Logout ) is provided and will allow the user to log out of the web client, returning them to the Login display page.

# Section 4 Web Interface Control Panels

**Introduction**

This section includes the following topics:

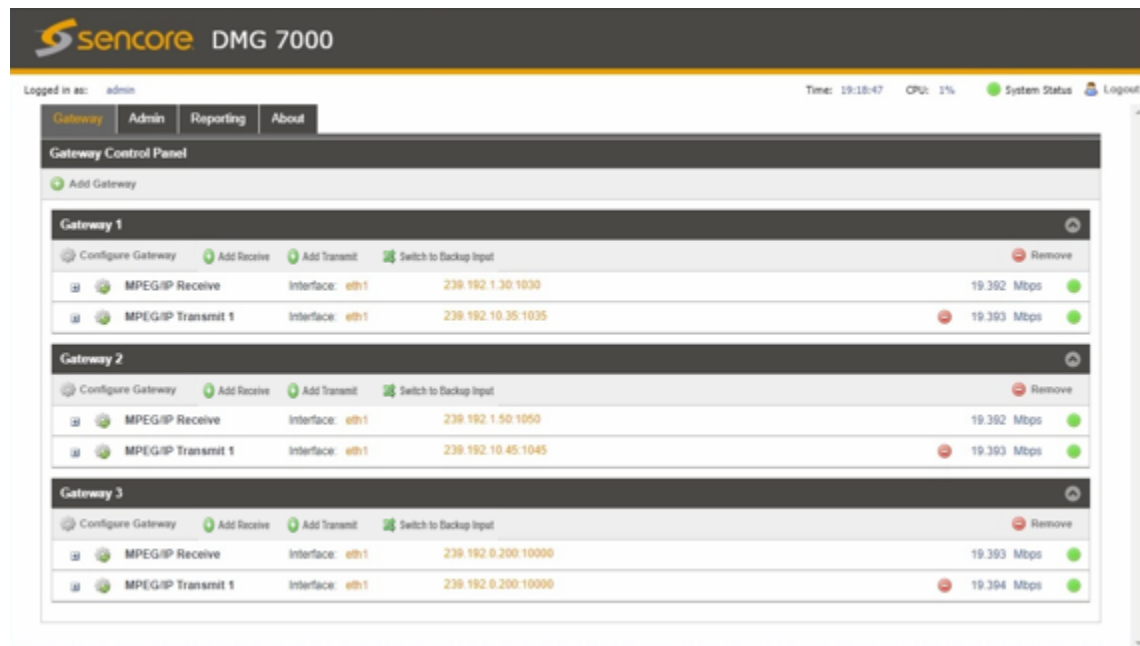
4.1	Gateway Control Panel .....	24
4.2	Admin Control Panel .....	59
4.3	Reporting Control Panel .....	76
4.4	About Panel .....	80

## 4.1 Gateway Control Panel

The Gateway control panel of the DMG 7000 web interface is used to configure the video processing details. This will include signal direction (transmit, receive or both), addresses to be received or delivered to and labeling of the gateways to help the user distinguish gateways from one another.

The number of available gateways will depend upon the physical DMG hardware as well as the license key that is applied. The chart below will show what an off the shelf unit will give the user, with a second column that will define the maximum number of gateway paths that can be attained with licensing.


Hardware	Provided Gateways	Maximum Gateways (with license)
DMG 70010 (Mini)	1	5
DMG 70020 (Field)	8	14
DMG 70030 (Head end)	32	50

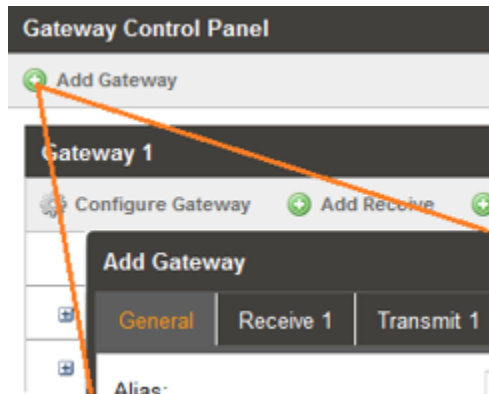


Gateway Tab



### 4.1.1 Adding a Gateway

To create a new or additional gateway, the user will click on the  button in the upper left area of the page. This will open a configuration window and allow the user to define the 'Alias' or label for the gateway; the receive and/or transmit addresses



**Add Gateway Icon**

The configuration window that opens will provide the user with three tabs: General, Receive and Transmit.

The General tab will hold the name of the created gateway. By default, it will be "Gateway (numeric value)" beginning with 1 and incrementing with each additional gateway that is added. The user can change this by editing the text in the text entry box.

The Receive tab is where the user will define the details for the stream to be received and any IGMP filtering. The Transmit tab(s) will define the details for the stream(s) to be sent out of this gateway.

### 4.1.2 Gateway Receive Settings

This menu is used to configure IP receive settings for MPEG/IP, SRT, Zixi, HLS, Seamless RTP (SMPTE 2022-7 for Hitless Switching) and RIST inputs. Based upon the type of protocol the user selects, the available configuration settings will adapt to provide the best fit.

Three settings that are common to all protocols are “Receive”, which can be set to Enabled or Disabled, “Interface”, which can be set to eth0 or eth1 (options may change depending on the number of interfaces and user defined interface name) and “VLAN”, which will filter incoming streams for VLAN tags as defined in [Section 4.2.9](#).

**Add Gateway**

General

Receive 1

Transmit 1

Receive Type:

MPEG/IP

Receive:

Enabled

Interface:

eth1

Mode:

Multicast

Destination IP:

239.192.0.200

Destination Port:

10000

FEC:

Disabled

IGMP Filter Mode:

Exclude

+

Add IGMP Address

−

Remove All

IGMP Address

Remove

Apply

Cancel

## Universal Gateway Receive Settings

*Note: when the “Receive” option is enabled for a given protocol (MPEG/IP, SRT, Zixi, HLS, Seamless RTP or RIST), the gateway will be capable of receiving incoming bitrate for that protocol. When using multiple receive instances on the same gateway, the “Receive” setting will not engage the newly configured receive instance as the active input by itself. To configure the additional receive as the active input, please review [Section 4.1.5](#).*

### 4.1.2.1 MPEG/IP Receive Settings

The figure below shows the options available when the “Receive Type” is set to “MPEG/IP”.

The screenshot shows the 'Add Gateway' configuration window with the 'Receive 1' tab selected. The settings are as follows:

Setting	Value
Receive Type:	MPEG/IP
Receive:	Enabled
Interface:	eth1
Mode:	Multicast
Destination IP:	239.192.0.200
Destination Port:	10000
FEC:	Disabled
IGMP Filter Mode:	Exclude



Below the settings, there is a section for IGMP addresses with a table:



IGMP Address	
	Remove

At the bottom of the window are 'Apply' and 'Cancel' buttons.

MPEG/IP Receive Settings

Setting	Range	Description
<b>Mode</b>	Multicast Unicast	<i>Multicast</i> setting allows the unit to receive multicast streams. Multicast streams originate from the IP range 224.0.0.0 – 239.255.255.255. <i>Unicast</i> allows the unit to receive unicast streams. Unicast streams originate directly from a source device.
<b>Destination IP</b>	224.0.0.0 – 239.255.255.255	This setting is only available when receiving a multicast stream. This is the address the unit will attempt to join.
<b>Destination Port</b>	0 - 65535	This is the UDP port the source device is sending to. This is the only setting required to receive a unicast stream but is also required for multicast.
<b>FEC</b>	Enabled Disabled	Sets the port to accept FEC on the incoming MPEG/IP stream
<b>IGMP Filter Mode</b>	Exclude Include	Used on networks supporting IGMPv3. If this setting is set to <i>Exclude</i> , any streams originating from the user defined IP addresses will be included in the IGMP messages and the network will not forward these streams to the device. If this setting is set to <i>Include</i> , any streams originating from the user defined IP addresses will be included in the IGMP messages and the network will only forward these streams to the device.

Click the  icon by the MPEG/IP input to view information about the incoming stream. Clicking the  icon will hide the IP statistics.

  **MPEG/IP Receive 1**

Interface: **eth1** **239.192.1.50:1050**

**Status**

Sync Status: **Locked**

Packets Per Frame: **7**

Encapsulation: **RTP**

FEC Rows: **0**

FEC Columns: **0**

**Statistics**

Out Of Order Packets: **0**

Duplicate Packets: **0**

Rtp Lost Packets: **0**


Discontinuity: **0**

FEC Corrected Packets: **0**


FEC Uncorrected Packets: **0**

FEC Corrected Packets / Period: **0**

Last Reset: **2021-03-23 21:03:02**

 **Reset Counters**

### MPEG/IP Receive Statistics

The  **Reset Counters** button is used to reset all the statistics for incoming IP packets and establish a new point of reference.

#### 4.1.2.2 SRT Receive Settings

The figure below shows the options available when the “Receive Type” is set to “SRT”



The screenshot shows a dialog box titled "Add Gateway" with three tabs: "General", "Receive 1", and "Transmit 1". The "Receive 1" tab is selected. The settings are as follows:



Setting	Value
Receive Type:	SRT
Receive:	Enabled
Interface:	eth1
Call Mode:	Caller
Remote Host:	1.0.0.2
Remote Port:	10000
Local Port Mode:	Auto
Local Port:	10000
Discovery Timeout (seconds):	3
Latency (ms):	20
Passphrase:	.....

At the bottom right of the dialog box are two buttons: "Apply" and "Cancel".

**SRT Receive Settings**

Setting	Range	Description
<b>Call Mode</b>	Caller Listener Rendezvous	Defines the 'handshake' mechanism to be used when establishing connection.
<b>Remote Host</b>	xxx.xxx.xxx.xxx	Defines the IP address of the stream on the remote device
<b>Remote Port</b>	0 – 65535	Defines the port of the stream on the remote devices
<b>Local Port Mode</b>	Auto Manual	In <i>Auto</i> mode, the local port number will be assigned automatically  In <i>Manual</i> mode, the local port number will be defined by the user
<b>Local Port</b>	1 – 65535	Defines the local port number
<b>Discovery Timeout (seconds)</b>	1 – 100, use 0 for infinite	Defines the length of time to wait for the stream to be discovered
<b>Latency (ms)</b>	1 – 8000	Defines buffer size in milliseconds
<b>Passphrase</b>	10 – 79 characters	Defines the encryption passphrase

Click the  icon by the SRT input to view information about the incoming stream. Clicking the  icon will hide the SRT receive statistics.


  **SRT Receive 1** Interface: **eth1**

**Status**


Connection State:	Connected
Up Time:	00:00:00:14
Local Port:	10000
Encryption Mode:	Disabled
Decryption State:	Unsecured
Round Trip Time (ms):	0
Buffer Size (ms):	121
Latency (ms):	125
Link Bandwidth:	37.677 Mbps
TS Packets Per SRT Packet:	7

**Statistics**

Reconnections:	0
Received Packets:	25,858
Received Bytes:	33.538 MB
Lost Packets:	0
Lost Bytes:	0 Bytes
Skipped Packets:	0
Skipped Bytes:	0 Bytes
Last Reset:	2021-03-23 21:19:55

 **Reset Counters**

### SRT Receive Statistics

The  **Reset Counters** button is used to reset all the statistics for incoming SRT packets and establish a new point of reference.



#### 4.1.2.3 Zixi Receive Settings

The figure below shows the options available when the “Receive Type” is set to “Zixi”.



The screenshot shows a web-based configuration interface titled "Add Gateway". It has three tabs: "General", "Receive 1" (which is selected and highlighted in orange), and "Transmit 1". The "Receive 1" tab contains the following settings:



Setting	Value
Receive Type:	Zixi
Receive:	Enabled
Interface:	eth1
Remote Host:	
Alternate Remote Host:	
Remote Port:	2077
Stream ID:	
Remote ID:	
Password:	
Ignore TLS Certificate Error:	Do Not Ignore
Maximum Latency (ms):	4000
Decryption Mode:	Disabled
Decryption Key:	*****
FEC Overhead (%):	30

At the bottom right of the dialog are two buttons: "Apply" and "Cancel".

**Zixi Receive Settings**

Setting	Range	Description
<b>Remote Host</b>	xxx.xxx.xxx.xxx Domain Name	Defines the host of the remote broadcast using IP address or domain name
<b>Alternate Remote Host</b>	xxx.xxx.xxx.xxx Domain Name	Defines the alternate host of the remote broadcast using IP address or domain name
<b>Remote Port</b>	0 – 65535	Defines the port of the stream on the remote device
<b>Stream ID</b>	User entry	Defines the Zixi stream ID to be received
<b>Remote ID</b>	User entry	Specify the Zixi Broadcaster or Feeder ID that will push the stream
<b>Password</b>	User entry	Provides the password to allow specific Stream ID entered to be received
<b>Ignore TLS Certificate Error</b>	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
<b>Maximum Latency (ms)</b>	30 – 10,000	Defines the maximum latency or buffer size (in milliseconds)
<b>Decryption Mode</b>	Disabled AES-128 AES-192 AES-256 Automatic	Defines if a decryption of the received signal is needed, which decryption standard to use, or if the DMG 7000 will automatically detect these
<b>Decryption Key</b>	User entry	Provides the key to allow signal processing if decryption is to be done
<b>FEC Overhead (%)</b>	0 – 50	Defines the amount of static overhead to be used to accommodate FEC

Click the  icon by the Zixi input to view information about the incoming stream.  
Clicking the  icon will hide the Zixi receive statistics.

  **Zixi Receive 1**

Interface: **eth1**

**Status**

Connection State:

Up Time:

Decryption State:

Round Trip Time (ms):

Jitter (ms):

TS Packets Per Zixi Packet:

Connected

00:00:00:17

Unsecured

5

2

7

**Statistics**

Reconnections:

Received Packets:

Received Bytes:

Dropped Packets:

Not Recovered Packets:

FEC Packets:

FEC Recovered Packets:

ARQ Packets:

ARQ Recovered Packets:

ARQ Duplicate Packets:

ARQ Requests:

0

30,421

36.947 MB

0

0

0

0

0


0

0


0

Last Reset:

2021-03-23 21:38:25

 **Reset Counters**

### Zixi Receive Statistics

The  **Reset Counters** button is used to reset all the statistics for incoming Zixi packets and establish a new point of reference.

#### 4.1.2.4 HLS Receive Settings

The figure below shows the options available when the “Receive Type” is set to “HLS”.

**Add Gateway**

General

Receive 1

Transmit 1

Receive Type:

HLS

Receive:

Enabled

Interface:

eth1

HLS Mode:

Pull

HLS Network Location:

Apply and Refresh

Profile Name	Bandwidth

Decryption Mode:

Disabled

Decryption Key:

\*\*\*\*\*

Discovery Timeout (seconds):

3

Apply

Cancel

**HLS Receive Settings**

Setting	Range	Description
<b>HLS Mode</b>	Push Pull	Determines if the HLS receives through a local or network location
<b>HLS Network Location</b>	User Entry	Defines address of the HLS stream to be received
<b>Profile / Bandwidth</b>	User Selected	After entering an HLS network location and clicking “Apply and Refresh”, a list of available profiles will be displayed
<b>Decryption Mode</b>	Disabled AES128	Defines if a decryption of the received signal is needed, AES 128 standard
<b>Decryption Key</b>	User Entry	Provides the key to allow signal processing if decryption is to be done
<b>Discovery Timeout (seconds)</b>	1 – 100, use 0 for infinite	Defines the length of time to wait for the stream to be discovered

#### 4.1.2.5 Seamless RTP Receive Settings

The figure below shows the options available when the “Receive Type” is set to “Seamless RTP”.

The screenshot shows the 'Add Gateway' configuration window with the 'Receive 1' tab selected. The settings are as follows:

- Receive Type:** Seamless RTP (dropdown)
- Receive:** Enabled (dropdown)
- Path 1 Interface:** eth1 (dropdown)
- Path 1 Destination IP:** 239.192.0.200 (text input)
- Path 1 Destination Port:** 10000 (spin box)
- Path 1 IGMP Filter Mode:** Exclude (dropdown)

Below these settings is a section for adding IGMP addresses:

- Add IGMP Address** (green plus icon) and **Remove All** (red minus icon) buttons.
- A table with the following structure:

IGMP Address	Remove

Below this section are identical settings for Path 2:

- Path 2 Interface:** eth1 (dropdown)
- Path 2 Destination IP:** 239.192.0.200 (text input)
- Path 2 Destination Port:** 10000 (spin box)
- Path 2 IGMP Filter Mode:** Exclude (dropdown)

Below these settings is another section for adding IGMP addresses:



- Add IGMP Address** (green plus icon) and **Remove All** (red minus icon) buttons.
- A table with the following structure:



IGMP Address	Remove

At the bottom of the window are **Apply** and **Cancel** buttons.

**Seamless RTP Receive Settings**

Setting	Range	Description
<b>Path 1 or 2 Destination IP</b>	xxx.xxx.xxx.xxx	Defines the address of the first or second path to be received
<b>Path 1 or 2 Destination Port</b>	1 - 65535	Defines the port of the first or second path to be received
<b>Path 1 or 2 IGMP Filter Mode</b>	Include, Exclude	Defines filter to include or exclude addresses contained in IGMP list box
<b>Path 1 or 2 IGMP List Box</b>	The list box for each path will comprise the addresses entered by the user, and define the sources input signals can be accepted from (Include), or sources that input signals are not to be accepted from (Exclude)	

Click the  icon by the Seamless RTP input to view information about the incoming streams. Clicking the  icon will hide the Seamless RTP receive statistics.



**Seamless RTP Receive 1**

**Status**


Sync Status: Locked  
Active Path: 1  
Packets Per Frame: 7  
Encapsulation: RTP

**Path 1 Statistics**


Out of Order Packets: 0  
Duplicate Packets: 0  
Lost Packets: 0  
Discontinuity: 0  
Last Reset: 2021-03-23 21:38:25

**Path 2 Statistics**

Out of Order Packets: 0  
Duplicate Packets: 0  
Lost Packets: 0  
Discontinuity: 0  
Last Reset: 2021-03-23 21:38:25

 **Reset Counters**

### Seamless RTP Statistics

The  **Reset Counters** button is used to reset all the statistics for incoming Seamless RTP packets and establish a new point of reference.

#### 4.1.2.6 RIST Receive Settings

The figure below shows the options available when the “Receive Type” is set to “RIST”.

**Add Gateway**

**General** | **Receive 1** | **Transmit 1**

Receive Type:

RIST

Receive:

Enabled

Profile Mode:

Simple

Latency (ms):

1000

Decryption Mode:

Disabled

Passphrase:


\*\*\*\*\*


Seamless:

Disabled

Bonding:

Disabled

 Add Link

Host/IP	Port	Interface	Mode	Backup	Remove
239.192.0.200	10000	eth1	Multicast	<input type="checkbox"/>	



Apply



Cancel

**RIST Receive Settings**



Setting	Range	Description
<b>Profile Mode</b>	Simple Main	Specifies the RIST profile mode by which to receive the incoming stream
<b>Latency (ms)</b>	1 – 8000	Defines buffer size in milliseconds
<b>Decryption Mode</b>	Disabled DTLS PSK	Specifies if the incoming RIST stream needs to be decrypted. Can only be enabled when using <i>Main</i> Profile Mode.  DTLS Decryption will require public and private keys as configured in <a href="#">Section 4.2.5.1</a> .
<b>Passphrase</b>	User entry	Provides the key to allow signal processing if <i>PSK</i> decryption is to be done
<b>Seamless</b>	Disabled Enabled	Allows user to enable seamless mode
<b>Bonding</b>	Disabled Enabled	Allows user to enable bonding mode

Click the  icon by the RIST input to view information about the incoming stream. Clicking the  icon will hide the RIST receive statistics.


  **RIST Receive 1** Interface: **eth1**

**Status**


Connection State:	Connected
Up Time:	00:15:35:18
Decryption State:	Unsecured
Round Trip Time (ms):	1
Buffer Size (ms):	1000
Jitter (ms):	5
Latency (ms):	1000
Link Bandwidth:	19.389 Mbps
FEC Cols:	0
FEC Rows:	0
TS Packets per RIST Packet:	7

**Statistics**

Reconnections:	1
Received Packets:	103,378,658
Received Bytes:	128.241 GB
Lost Packets:	0
FEC Uncorrected Packets:	0
FEC Recovered Packets:	0
RTCP NAKs:	0
RTCP Recovered Packets:	0
Last Reset:	2021-03-23 21:19:55

 **Reset Counters**

### RIST Receive Statistics

The  **Reset Counters** button is used to reset all the statistics for incoming RIST packets and establish a new point of reference.

### 4.1.3 Gateway Transmit Settings

This menu is used to configure IP transmit settings for MPEG/IP, SRT, Zixi and RIST. The DMG 7000's Gateway Transmit available configuration options will change based on the protocol the user selects for the "Transmit Type" field.

There are three settings common to all protocols: "Transmit", which can be set to Enabled or Disabled, "Interface", which can be set to eth0 or eth1 (options may change depending on number of interfaces and user defined interface name) and "VLAN", which will add VLAN tags as defined in [Section 4.2.9](#) to outbound streams.

**Add Gateway**

General | Receive 1 | **Transmit 1**

Transmit Type: MPEG/IP

Transmit: Enabled

Interface: eth1

Destination IP: 239.192.0.201

Destination Port: 10000

Source IP Mode: Auto

Source IP: 0.0.0.0

Source Port: 3020

Source MAC Mode: Auto

Source MAC: 00:00:00:00:00:00

TS Packets Mode: Auto

TS Packets Per IP Packet: 7

Encapsulation: UDP

Apply Cancel

**Universal Transmit Settings**

#### 4.1.3.1 MPEG/IP Transmit Settings

The figure shows the options available when the “Transmit Type” is set to “MPEG/IP”.

The screenshot shows a web-based configuration interface titled "Add Gateway". It has three tabs: "General", "Receive 1", and "Transmit 1". The "Transmit 1" tab is selected and highlighted in orange. Below the tabs, there are various configuration fields for transmitting MPEG/IP data. The fields are arranged in two columns. The first column contains labels for each setting, and the second column contains the current value or a dropdown menu. At the bottom right, there are "Apply" and "Cancel" buttons.

Setting	Value
Transmit Type:	MPEG/IP
Transmit:	Enabled
Interface:	eth1
Destination IP:	239.192.0.201
Destination Port:	10000
Source IP Mode:	Auto
Source IP:	0.0.0.0
Source Port:	3020
Source MAC Mode:	Auto
Source MAC:	00:00:00:00:00:00
TS Packets Mode:	Auto
TS Packets Per IP Packet:	7
Encapsulation:	UDP

**MPEG/IP Transmit Settings**

Setting	Range	Description
<b>Destination IP</b>	224.0.0.0 – 239.255.255.255	This setting is only available when receiving a multicast stream. This is the address the unit will attempt to join
<b>Destination Port</b>	0 – 65535	This is the UDP port the source device is sending to. This is the only setting required to receive a unicast stream but is also required for multicast
<b>Source IP Mode</b>	Auto Manual	When set to <i>Auto</i> , the source IP address on the output stream will match the corresponding local interface. When set to <i>Manual</i> , a user entered address can be assigned to the output stream
<b>Source IP</b>	xxx.xxx.xxx.xxx	Defines the Source IP address to be assigned to the output stream
<b>Source Port</b>	0 – 65535	Defines the source IP port to be assigned to the output stream
<b>Source MAC Mode</b>	Auto Manual	When set to <i>Auto</i> , the source MAC address of the output stream will match the corresponding local interface. When set to <i>Manual</i> , a user entered address can be assigned to the output stream
<b>Source MAC</b>	xx:xx:xx:xx:xx:xx	The user defined MAC for when using <i>Manual</i> MAC Mode
<b>TS Packets Mode</b>	Auto Manual	In <i>Auto</i> mode, the source will define the number of TS packets per IP packet. In <i>Manual</i> mode, the user will define the number of TS packets per IP packet
<b>TS Packets Per IP Packet</b>	1-7	The number of TS packets that are contained with a single IP packet. Default is 7. Lowering this value below default increases network overhead
<b>Encapsulation</b>	UDP RTP	Sets the Encapsulation to UDP or RTP

### 4.1.3.2 SRT Transmit Settings

The figure below shows the options available when the “Transmit Type” is set to “SRT”.



The screenshot shows the 'Add Gateway' dialog box with the 'Transmit 1' tab selected. The settings are as follows:



Setting	Value
Transmit Type:	SRT
Transmit:	Enabled
Interface:	eth1
Call Mode:	Caller
Remote Host:	1.0.0.3
Remote Port:	10000
Local Port Mode:	Auto
Local Port:	10000
Discovery Timeout (seconds):	3
Latency (ms):	125
Bandwidth Overhead (%):	25
TS Packets Mode:	Auto
TS Packets Per SRT Packet:	7
Time To Live (hops):	64
Type Of Service:	0
Encryption Mode:	Disabled
Passphrase:	*****

At the bottom right of the dialog are 'Apply' and 'Cancel' buttons.

**SRT Transmit Settings**

Setting	Range	Description
<b>Call Mode</b>	Caller Listener Rendezvous	Defines the 'handshake' mechanism to be used when establishing connection.
<b>Remote Host</b>	xxx.xxx.xxx.xxx	Defines the IP address of the stream on the remote device
<b>Remote Port</b>	0 – 65535	Defines the port of the stream on the remote devices
<b>Local Port Mode</b>	Auto Manual	In <i>Auto</i> mode, the local port number will be assigned automatically  In <i>Manual</i> mode, the local port number will be defined by the user
<b>Local Port</b>	1 – 65535	Defines the local port number
<b>Discovery Timeout (seconds)</b>	1 – 100, use 0 for infinite	Defines the length of time to wait for the stream to be discovered
<b>Latency (ms)</b>	1 – 8000	Defines buffer size in milliseconds
<b>Bandwidth Overhead (%)</b>	0 – 50	Defines the amount of bandwidth overhead to allow for
<b>TS Packets Mode</b>	Auto Manual	In <i>Auto</i> mode, the source will define the number of TS packets per SRT packet. In <i>Manual</i> mode, the user will define the number of TS packets per SRT packet
<b>TS Packets Per SRT Packet</b>	1 – 7	Defines the number of TS packets per SRT packet when mode is <i>Manual</i>
<b>Time To Live (hops)</b>	1 – 254	Defines the number of network devices the transmission is allowed to pass through
<b>Type of Service</b>	0 – 255	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 stream.
<b>Encryption Mode</b>	Disabled AES-128 AES-256	Defines which encryption standard to use or if the DMG 7000 will automatically detect this.
<b>Passphrase</b>	10 – 79 characters	Defines the encryption passphrase

Click the  icon by the SRT transmit instance to view information about the about stream. Clicking the  icon will hide the SRT transmit statistics.

  **SRT Transmit 1** Interface: **eth1**


**Status**

Connection State:	Connected
Up Time:	00:00:00:10
Local Port:	10000
Encryption Mode:	Disabled
Remote Decryption State:	Unsecured
Round Trip Time (ms):	0
Buffer Size (ms):	2
Latency (ms):	125
Maximum Bandwidth:	25.062 Mbps
Path Maximum Bandwidth:	27.668 Mbps


**Statistics**

Reconnections:	4
Sent Packets:	16,560
Sent Bytes:	21.478 MB
Resent Packets:	0
Resent Bytes:	0 Bytes
Dropped Packets:	0
Dropped Bytes:	0 Bytes
Received ACKs:	867
Received NAKs:	0

Last Reset: 2021-03-23 21:09:28

 **Reset Counters**

### SRT Transmit Statistics

The  **Reset Counters** button is used to reset all the statistics for outbound SRT packets and establish a new point of reference.



### 4.1.3.3 Zixi Transmit Settings

The figure below shows the options available when the “Transmit Type” is set to “Zixi”.

Add Gateway

General
Receive 1
Transmit 1

Transmit Type:
Zixi

Transmit:
Enabled

Interface:
eth1

Remote Host:

Alternate Remote Host:

Remote Port:
2088

Stream ID:

Password:

Ignore TLS Certificate Error:
Do Not Ignore

Maximum Latency (ms):
4000

Encryption Mode:
Disabled

Encryption Key:

Maximum Bitrate (Mbps):
8

FEC Overhead (%):
30

TS Packets Mode:
Auto

TS Packets Per Zixi Packet:
7

Bonding Mode:
Disabled

Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary
eth1	8	Primary

Apply
Cancel

**Zixi Transmit Settings**

Setting	Range	Description
<b>Remote Host</b>	xxx.xxx.xxx.xxx Domain Name	Defines the host of the remote broadcast using an IP address or domain name
<b>Alternate Remote Host</b>	xxx.xxx.xxx.xxx Domain Name	Defines the alternate host of the remote broadcast using an IP address or domain name
<b>Remote Port</b>	0 – 65535	Defines the port of the stream on the remote device
<b>Stream ID</b>	User entry	Defines the Zixi stream ID to be transmitted
<b>Password</b>	User entry	Provides the password to allow specific Stream ID entered to be received
<b>Ignore TLS Certificate Error</b>	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
<b>Maximum Latency (ms)</b>	30 – 10,000	Defines the maximum latency or buffer size (in milliseconds)
<b>Encryption Mode</b>	Disabled AES-128 AES-192 AES-256 Automatic	Defines which encryption standard to use or if the DMG 7000 will automatically detect this
<b>Encryption Key</b>	User entry	The key to be used by downstream decryption devices
<b>FEC Overhead (%)</b>	0 – 50	Defines the amount of static overhead to be used to accommodate FEC
<b>TS Packets Mode</b>	Auto Manual	In <i>Auto</i> mode, the source will define the number of TS packets per Zixi packet. In <i>Manual</i> mode, the user will define the number of TS packets per Zixi packet.
<b>TS Packets per Zixi Packet</b>	1 – 7	User defined value for when <i>Manual</i> mode is enabled.
<b>Bonding Mode</b>	Disabled All interfaces One Interface Any Interface	Specifies which interfaces, if any, are to be set to bonding mode.

<b>Interface Bonding Box</b>	Available for One Interface Mode Any Interface Mode	Allows user to define parameters and details about the port(s) when bonding
------------------------------	--	---



Zixi transmissions can be configured to use multiple interfaces simultaneously (Port Bonding). By defining the maximum bitrate for that interface, the unit will only send up to that rate on that interface. A Primary and Backup interface may also be chosen if redundant links should be used.



Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary
eth1	8	Primary

Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary
eth1	8	Primary

Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary
eth1	8	Primary

**Interface Bonding Boxes**

Click the  icon by the Zixi transmit instance to view information about the outbound stream. Clicking the  icon will hide the Zixi Transmit statistics.

  **Zixi Transmit 1**

Interface: **eth1**

**Status**

Connection State:

Up Time:

Round Trip Time (ms):

Jitter (ms):

Maximum Bandwidth:

Connected

00:00:01:39

0

3

0.000 Mbps

**Statistics**

Reconnections:

Sent Packets:

Sent Bytes:

Dropped Packets:

Not Recovered Packets:

FEC Packets:

FEC Recovered Packets:

ARQ Packets:

ARQ Recovered Packets:

ARQ Duplicate Packets:

ARQ Requests:

0

235,930

289.724 MB

0

0

54,427

0

0


0

0


0

Last Reset:

2021-03-23 21:09:28

 **Reset Counters**

### Zixi Transmit Statistics

The  **Reset Counters** button is used to reset all the statistics for outbound Zixi packets and establish a new point of reference.

#### 4.1.3.4 RIST Transmit Settings

The figure below shows the options available when the “Transmit Type” is set to “RIST”.

**Add Gateway**

General

Receive 1

Transmit 1

Transmit Type:

RIST

Transmit:

Enabled

Profile Mode:

Simple

Tunneling Mode:

Full Datagram

Latency (ms):

1000

Encryption Mode:

Disabled

Passphrase:

\*\*\*\*\*

Ignore TLS Certificate Error:

Do Not Ignore

Seamless:

Disabled

Bonding:

Disabled

+

Add Link

Dest Host/IP	Dest Port	Source Port	Interface	Bandwidth Limit (Mbps)	Backup	Remove
239.192.0.200	10000	3020	eth1	100	<input type="checkbox"/>	<div>⊖</div>

Apply

Cancel

**RIST Transmit Settings**

Setting	Range	Description
<b>Profile Mode</b>	Simple Main	Specifies the RIST profile mode for the transmit instance. The <i>Simple</i> profile mode will output with the same packet structure as an RTP packet. The <i>Main</i> profile mode will add more header information for use with the tunnel function
<b>Tunneling Mode</b>	Full Datagram Reduced Overhead	When set to <i>Full Datagram</i> , the IP header and UDP header will be re-added to each packet to help identify the channel. When set for <i>Reduced Overhead</i> , the source port and destination port will be added to the header to help identify the channel. Exclusive to <i>Main</i> Profile Mode.
<b>Latency (ms)</b>	1 – 8000	Specifies buffer size in milliseconds
<b>Encryption Mode</b>	Disabled DTLS PSK	Defines which encryption standard the RIST transmit instance will use. Exclusive to <i>Main</i> Profile Mode.  DTLS encryption will require uploading public and private keys as configured in <a href="#">Section 4.2.5.1</a> .
<b>Passphrase</b>	User entry	The encryption passphrase. Exclusive to <i>PSK</i> Encryption Mode.
<b>Ignore TLS Certificate Error</b>	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
<b>Seamless</b>	Disabled Enabled	Allows user to enable seamless mode
<b>Bonding</b>	Disabled Enabled	Allows user to enable bonding mode



RIST transmissions can be configured to use multiple interfaces simultaneously (Port Bonding). By defining the maximum bitrate for that interface, the unit will only send up to that rate on that interface. A Primary and Backup interface may also be chosen if redundant links should be used.

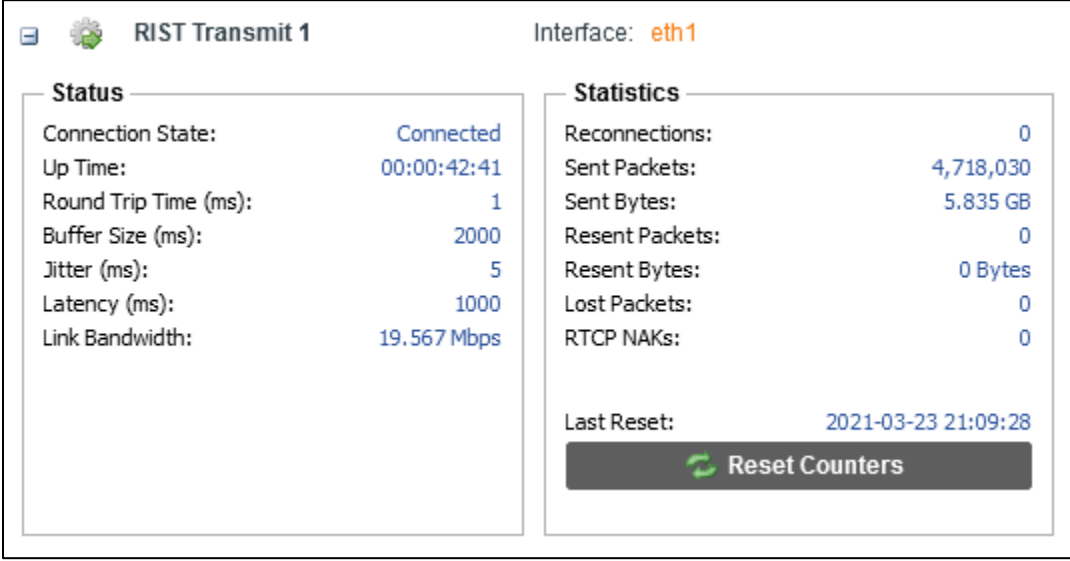
Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary
eth1	8	Primary

Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	<input type="text" value="8"/>	Primary
eth1	8	Primary

Interface ↑	Bandwidth Limit(Mbps)	Priority
eth0	8	Primary ▾
eth1	8	Primary
		Backup

Interface Bonding Boxes

Click the  icon by the RIST transmit instance to view information about the outbound stream. Clicking the  icon will hide the RIST transmit statistics.

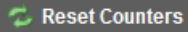


The screenshot shows the 'RIST Transmit 1' configuration window. At the top, it says 'Interface: eth1'. The window is divided into two main sections: 'Status' and 'Statistics'.

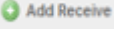
Status		Statistics	
Connection State:	Connected	Reconnections:	0
Up Time:	00:00:42:41	Sent Packets:	4,718,030
Round Trip Time (ms):	1	Sent Bytes:	5.835 GB
Buffer Size (ms):	2000	Resent Packets:	0
Jitter (ms):	5	Resent Bytes:	0 Bytes
Latency (ms):	1000	Lost Packets:	0
Link Bandwidth:	19.567 Mbps	RTCP NAKs:	0

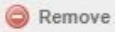

At the bottom right, there is a 'Last Reset:' timestamp of '2021-03-23 21:09:28' and a 'Reset Counters' button with a circular arrow icon.

### RIST Transmit Statistics

The  button is used to reset all the statistics for incoming RIST packets and establish a new point of reference.

#### 4.1.4 Additional Receive Instances

Each gateway on the DMG can be configured for multiple receive instances. To add an additional receive instance, click on the  button in the top left corner of the gateway section. The gateway configuration window will open with a new "Receive 2" tab, offering the same settings as the initial receive tab.

Removing a gateway from the configuration can be done by clicking on the  button located at the right side of the gateway ribbon. Any configured receive instance can also be removed by clicking on the red  19.394 Mbps button located within the receive row. When either of the red icons are clicked, the system will prompt the user with confirmation of intent to remove the item from the configuration.

Only one additional receive instance can be added, so the option becomes gray as shown below after the second path is added.

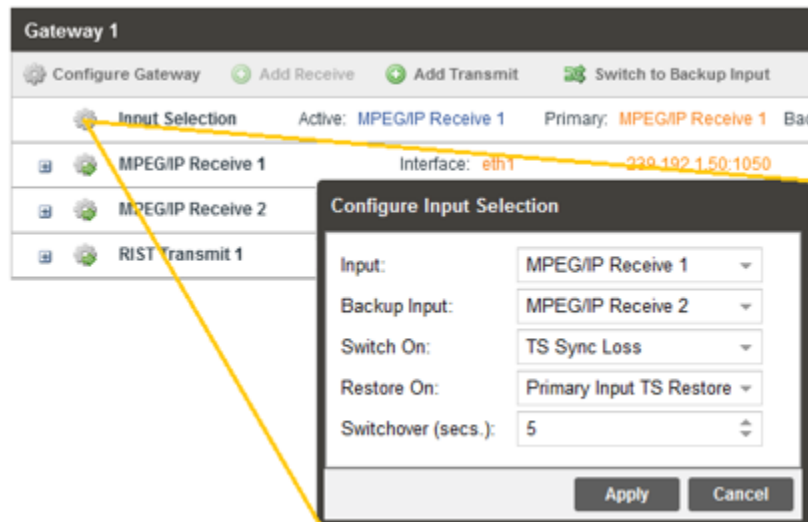


Gateway 4						
Configure Gateway	Add Receive	Add Transmit	Switch to Backup Input	Remove		
Input Selection	Active: MPEG/IP Stream 1		Primary: MPEG/IP Stream 1		Backup: None	
MPEG/IP Receive 1	Interface: eth1	239.192.1.50:1050	FEC: Present	19.394 Mbps		
MPEG/IP Transmit 1	Interface: eth1	239.192.0.200:8000		19.394 Mbps		
MPEG/IP Receive 2	Interface: eth1	239.108.108.36:35110	FEC: Not Present	9.552 Mbps		

## Multiple Receive Instances

### 4.1.5 Configuring Active Inputs and Failover



When two receive instances are configured as per [Section 4.1.4](#), only one of them can be assigned to the transmit instances. The Input Selection menu is used to determine which receive instance is the primary and backup.


















Input Selection Menu

Setting	Range	Description
<b>Input</b>	Receive 1 Receive 2	Used for both normal operation and input failover settings. During normal operation, this input will be the active input
<b>Backup Input</b>	Receive 1 Receive 2	During failover operation this input will become the active input. The catalyst for the unit to switch to this input is configured in the following setting.


<b>Switch On</b>	Manual Only TS Sync Loss	Choose the event that triggers the switch from the primary to the backup input
<b>Restore On</b>	Manual Only Primary Input TS Restored Backup Input TS Sync Loss	Choose the event that triggers a switch back to the primary input
<b>Switchover (secs)</b>	1 – 20	The amount of time the gateway must remain in the “Switch On” or “Restore On” state before automatic failover or switchback occurs



Clicking the  **Switch to Backup Input** option under the gateway will prompt the user for confirmation of intent to change the receive instance assigning the transmit instances to source from receive instance 2. Clicking  **Switch to Primary Input** will assign the transmit instances to return to sourcing from receive instance 1.

Gateway 1						
 Configure Gateway  Add Receive  Add Transmit  Switch to Primary Input  Remove						
 Input Selection	Active: MPEG/IP Receive 2    Primary: MPEG/IP Receive 1    Backup: MPEG/IP Receive 2					
 MPEG/IP Receive 1	Interface: eth1	239.192.150:1050	FEC: Not Present		19.392 Mbps	
 MPEG/IP Receive 2	Interface: eth1	239.192.108.35:10120	FEC: Not Present		5.250 Mbps	
 RIST Transmit 1	Interface: eth1	Connected to 192.168.108.11:10000 on port 3020			5.250 Mbps	

### Active Backup Input

#### 4.1.6 Additional Transmit Instances

The DMG 7000 will allow the user to configure a single gateway for multiple transmission paths. To add an additional transmission path, click on the  **Add Gateway Transmit** button in the top left corner of the Gateway section. The gateway configuration window will open with an additional Transmit tab. The new tab will offer the same settings as the initial transmit tab.

Removing a gateway from the configuration can be done by clicking on the  **Remove** button located at the right side of the gateway ribbon. Any configured transmit path can also be removed by clicking on the red  **19.394 Mbps** button located within the transmit row that the user wishes to remove. When either of the red icons are clicked, the system will prompt the user with confirmation of intent to remove the item from the configuration.

Which receive instance the transmit instances will source from is dependent on settings from [Section 4.1.4](#) and [Section 4.1.5](#).

Gateway 4						
Configure Gateway   Add Receive   Add Transmit   Switch to Backup Input   Remove						
Input Selection	Active: MPEG/IP Stream 1		Primary: MPEG/IP Stream 1		Backup: None	
MPEG/IP Receive 1	Interface: eth1	239.192.1.50:1050	FEC: Present		19.394 Mbps	
MPEG/IP Transmit 1	Interface: eth1	239.192.0.200:8000			19.395 Mbps	
MPEG/IP Transmit 2	Interface: eth1	239.192.0.200:8200			19.390 Mbps	

### Multiple Transmit Instances

## 4.2 Admin Control Panel

To access the Admin Control Panel, click on the Admin tab. This page will offer the user to control many global settings and maintenance tasks on the DMG 7000.

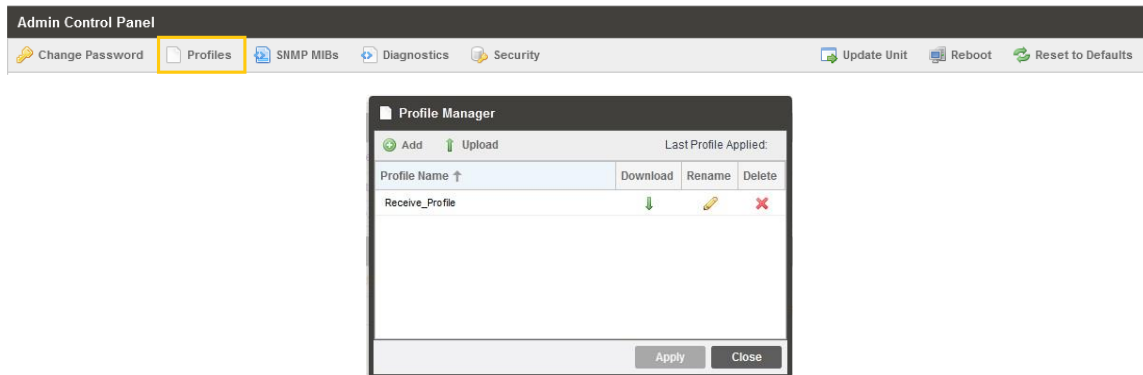
### 4.2.1 Changing Unit Password

The screenshot shows the 'Admin Control Panel' interface. The 'Change Password' button in the ribbon is highlighted with a yellow box. Below the ribbon, a 'Change Password' dialog box is displayed. It contains two input fields: 'New Password:' and 'Confirm Password:'. At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.


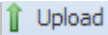




### Password Change Menu

The configuration button for this feature will be found under the Admin Control Panel title ribbon. This feature provides the DMG 7000 user management control of the web interface access password. In order to make changes to passwords, click the change password button. A window will appear to enter the current password and new password. Click “Apply” to save and exit.

## 4.2.2 Profiles



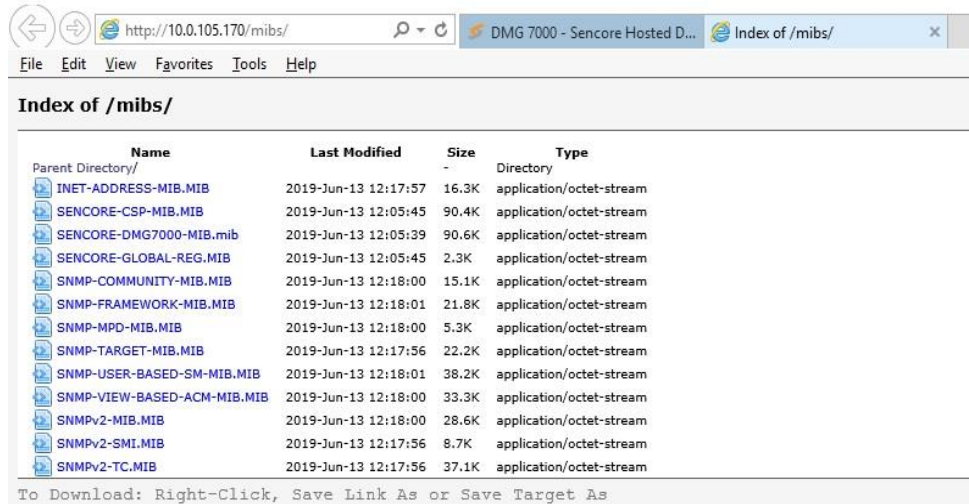
The DMG 7000 has the ability to save all configured settings to multiple profiles. Profiles can be saved locally, renamed and saved to external storage to be used on other DMG 7000. Profiles can be used to quickly and easily change the configuration of a DMG 7000 to suit different inputs and decoding requirements.

Add New Profile		Used to create or add a new profile to the profile list
Upload Profile		Used to upload a profile to the DMFG7000 from the user pc
Apply Profile		Used to apply a profile selected from profile list to the DMG7000
Rename Profile		Used to edit the selected profile name
Delete Profile		Used to delete a profile from the profiles list
Download Profile		Used to download a profile selected from the list to the user pc

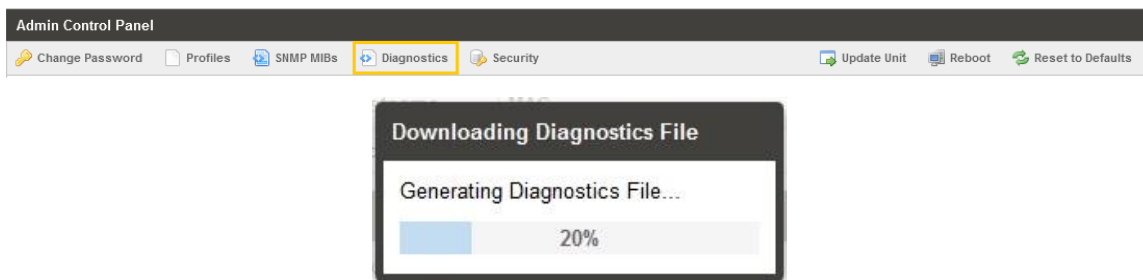
## 4.2.3 SNMP MIB files



The SNMP MIB files for the DMG 7000 can be obtained by clicking on the SNMP MIBs button at the top of the page. This will open a new tab within the current web browser and give the user a list of all available MIB files. Directions on how to save them to an external storage location are provided at the bottom of the list.



## 4.2.4 Diagnostics

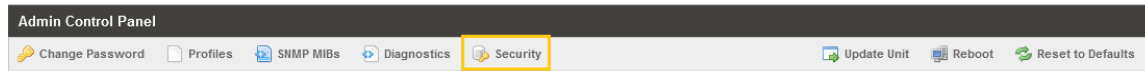


The DMG 7000 provides the user the ability to take a snapshot of the ALL current unit settings, reported values, active alarms, and the alarm and log file history. This snapshot will be downloaded as an .XML format file that can be attached in an email or opened for viewing.

Click the 'Diagnostics' button and a window will open showing the diagnostic file creation progress.

This window is replaced with a download file window when file creation is complete. The user will be asked to 'Open' or 'Save' the file. Selecting the Save option will download the .XML file to the pc 'downloads' location.

## 4.2.5 Security Manager

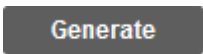

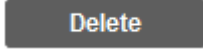
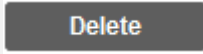





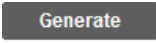
The Security Manager is used to configure self-signed certificate information.

Additionally, using public and private keys, this menu is used to enable DTLS encryption and decryption on RIST receive and transmit instances as described in [Section 4.2.5.1](#).

The image shows a window titled 'Security Manager'. It contains a 'Certificate Signing Request' section with the following fields: 'Country Name' (US), 'State or Province Name' (Delaware), 'Locality Name' (Wilmington), 'Organization Name' (Sencore Inc), 'Organizational Unit Name' (empty), 'Common Name' (empty), and 'Email Address' (empty). Below these fields are buttons for 'Generate New CSR File' (Generate), 'Download Generate CSR File' (Download), 'Delete Old CSR File' (Delete), and 'Delete Old Local Private Key File' (Delete). At the bottom, there are three 'Upload' buttons for 'Local Certificate File', 'Local Private Key File', and 'Remote Certificate File'. A 'Close' button is located at the bottom right of the window.

**Security Manager Menu**

Setting	Range	Description
<b>Country Name</b>	User entry	Country Name for generated CSR file
<b>State or Province Name</b>	User entry	State/Province Name for generated CSR file
<b>Locality Name</b>	User entry	Locality Name for generated CSR file
<b>Organization Name</b>	User entry	Organization Name for the generated CSR file
<b>Organizational Unit Name</b>	User entry	Organizational Unit Name for the generated CSR file
<b>Common Name</b>	User entry	Common Name for the generated CSR file
<b>Email Address</b>	User entry	Email Address for reference on the generated CSR file
<b>Generate New CSR File</b>		This icon will generate a new Certificate Signing Request file (CSR) using the configured IP from eth0 for the CSR file name. Additionally, the Security Manager will generate a local private key file to be used with the downstream
<b>Download Generated CSR File</b>		This icon will download the locally generated CSR file onto a remote machine
<b>Delete Old CSR File</b>		This icon will delete the locally generated CSR file
<b>Delete Old Local Private Key File</b>		This icon will delete the locally generated private key file
<b>Local Certificate File</b>		Use this icon to upload the local certificate file.
<b>Local Private Key File</b>		Use this icon to upload the local private key file
<b>Remote Certificate File</b>		Use this file to upload the remote certificate file

Upon clicking , the system will generate a new CSR file and local private key for use with the downstream receiver.

Certificate Signing Request File Name:	10.0.108.10.csr
Generate New CSR File:	<button>Generate</button>
Download Generate CSR File:	<button>Download</button>
Delete Old CSR File:	<button>Delete</button>
Delete Old Local Private Key File:	<button>Delete</button>
Local Certificate File:	<button>↑ Upload</button>
Local Private Key File: private_key.pem	<button>↑ Upload</button>
Remote Certificate File:	<button>↑ Upload</button>

**Generated Private Key and CSR Files**

#### 4.2.5.1 Enabling DTLS

In order to make a successful DTLS connection when enabling encryption and decryption on RIST receive and transmit instances, a “Local Certificate File”, “Local Private Key File” and “Remote Certificate File” must be uploaded to the Security Manager ([Section 4.2.5](#)).

As shown in the figure, the same Certificate File may be uploaded to both the Local and Remote Certificate File fields.

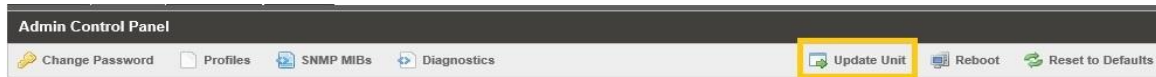
Local Certificate File:	server-cert.pem	<button>↑ Upload</button>
Local Private Key File:	server-key.pem	<button>↑ Upload</button>
Remote Certificate File:	server-cert.pem	<button>↑ Upload</button>

**Uploaded Key and Certificate Files**

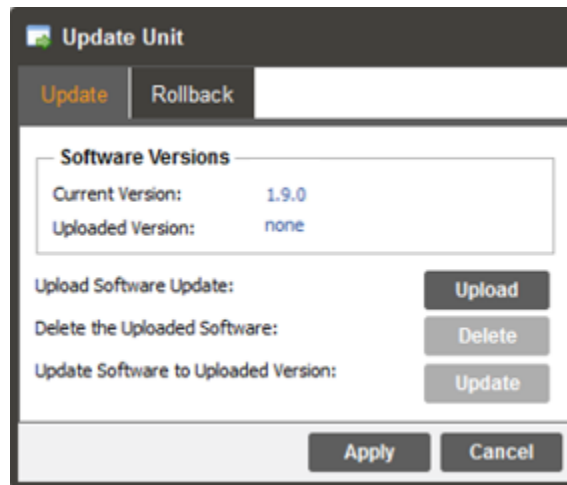
When making a DTLS connection between a DMG 7000 that is transmitting RIST and a DMG 7000 that is receiving RIST, these same files must be uploaded to both units. Additionally, both the transmit and receive instance on each unit must have *Profile Mode* configured for “Main” and *Encryption Mode* configured for “DTLS” as described in [Section 4.1.2.6](#) and [Section 4.1.3.4](#).



## 4.2.6 Updating the System Software

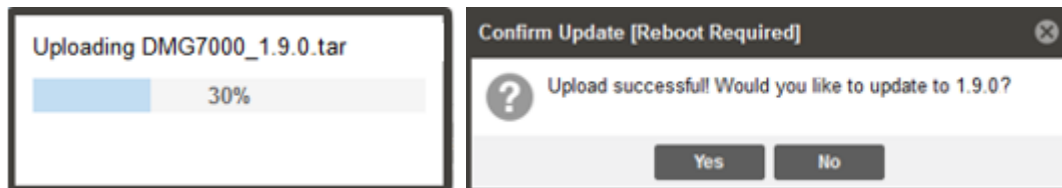




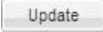
Updates to the DMG 7000 are performed through the web interface. A software update file is provided by Sencore and then uploaded to the unit. To request the latest software version or a copy of the release notes please send an email to [ProCare@Sencore.com](mailto:ProCare@Sencore.com). The 'Update Unit' button is in the top right corner of the Admin control panel. When opened this feature will allow the user to advance the software version the DMG 7000 operates on, or rollback the software version that the DMG 7000 operates on.



### Applying software updates

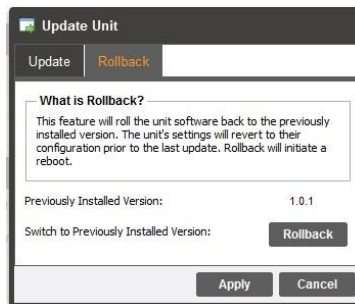
1. Click Upload button and browse to the appropriate software file
2. A progress bar will show uploading status
3. Once the file is uploaded click on Yes when prompted to update
4. The DMG will reboot after a software update is complete.
5. The DMG 7000 will reboot after a software update is complete.



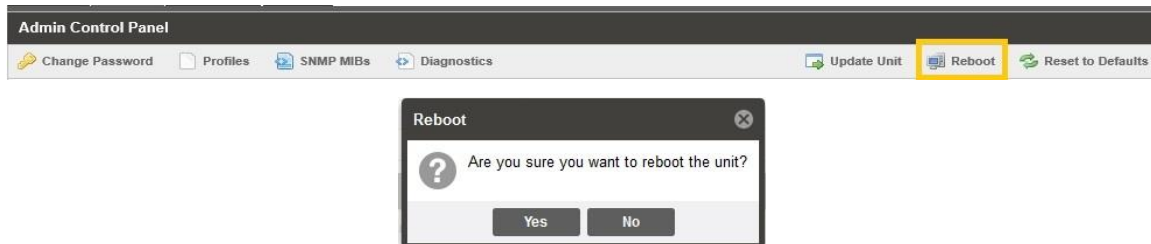
Upload Software Update		To upload software updates to the DMG 7000 click this button. The user will be prompted to navigate to an update file. The file will then upload to the DMG 7000. When complete the DMG 7000 will prompt the user to either apply the update or cancel
Delete the Uploaded Software		Clicking this button prompts the user to confirm the deletion of the software update from the DMG 7000. This will also clear the Uploaded Version status of the Software Versions section.
Update Software to Uploaded Version		Clicking the button starts the software update process. The DMG 7000 will prompt the user to confirm the update. Click Yes to continue or No to cancel.

### Rollback software updates

The DMG is capable of reverting back to a previous version of software using the Rollback feature. The DMG accomplishes this by maintaining two separate software images; one is the most current version of software with all current settings and the other is the previous version of software with all of the previous settings. To perform a rollback, click the Update Unit button and then click the Rollback tab. The DMG will reboot after the rollback process is complete.



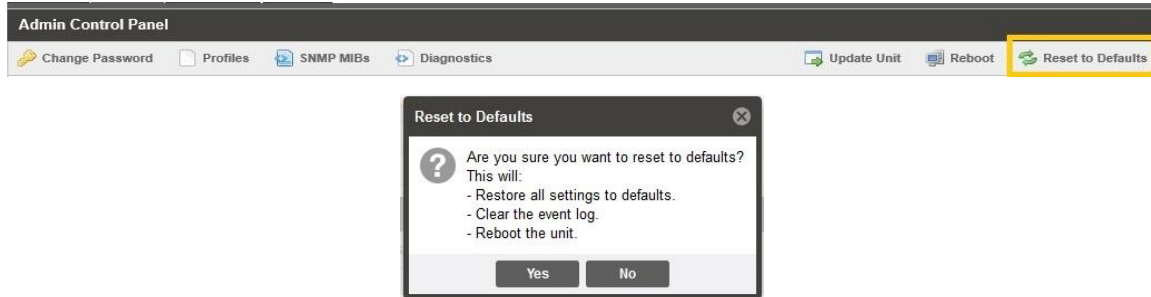
## 4.2.7 Reboot the Unit



The DMG 7000 can be rebooted from the web interface Admin page. The 'Reboot' button is located in the top right corner of the Admin Control Panel.

To perform a reboot, click the reboot button. The system will prompt the user to confirm the reboot request. Once confirmed, a status window with a progress bar will open be visible until the reboot is complete and the login window displayed.

#### 4.2.8 Reset to Defaults

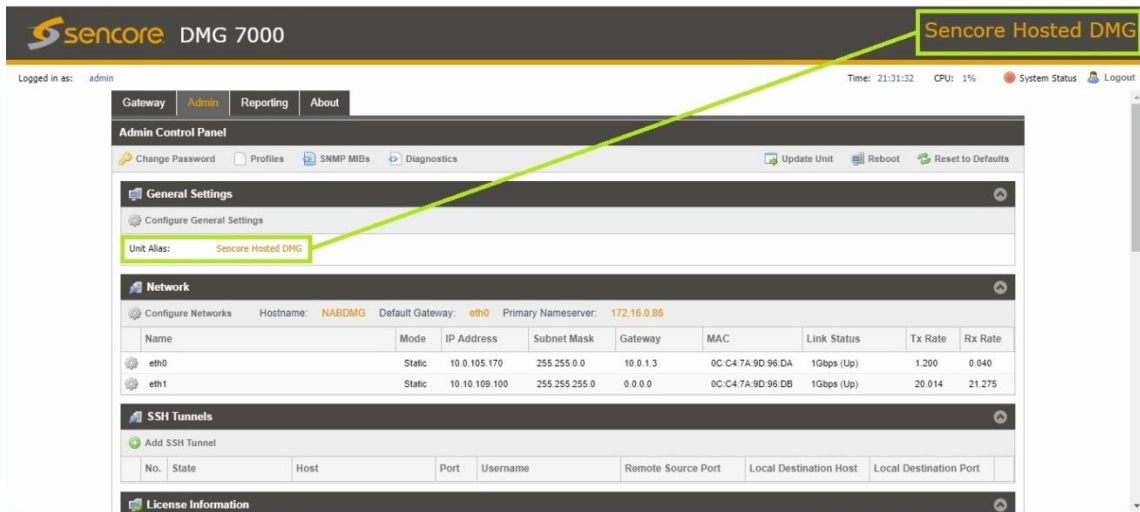


The DMG settings can be reset to factory defaults. All settings will be returned to the factory defaults **except** the network management ports TCP/IP settings. All event logs will be cleared. To reset all settings to default, click the Reset to Defaults button on the Admin page. The DMG will prompt the user to confirm the reset.

#### 4.2.9 Unit Alias

The configuration button for this feature is found under the General Settings title ribbon of the Admin control panel. The Unit Alias is a unique name or description the user can assign to the DMG 7000. The 'Alias' will be available on the unit web client and front panel.

When selected, the user will be provided a text entry box to enter the alias. The user will then click the Apply button to save the changes made. The web client and front panel will update immediately.



#### 4.2.10 Configuring the Unit Networks and VLANs

##### System Network interface

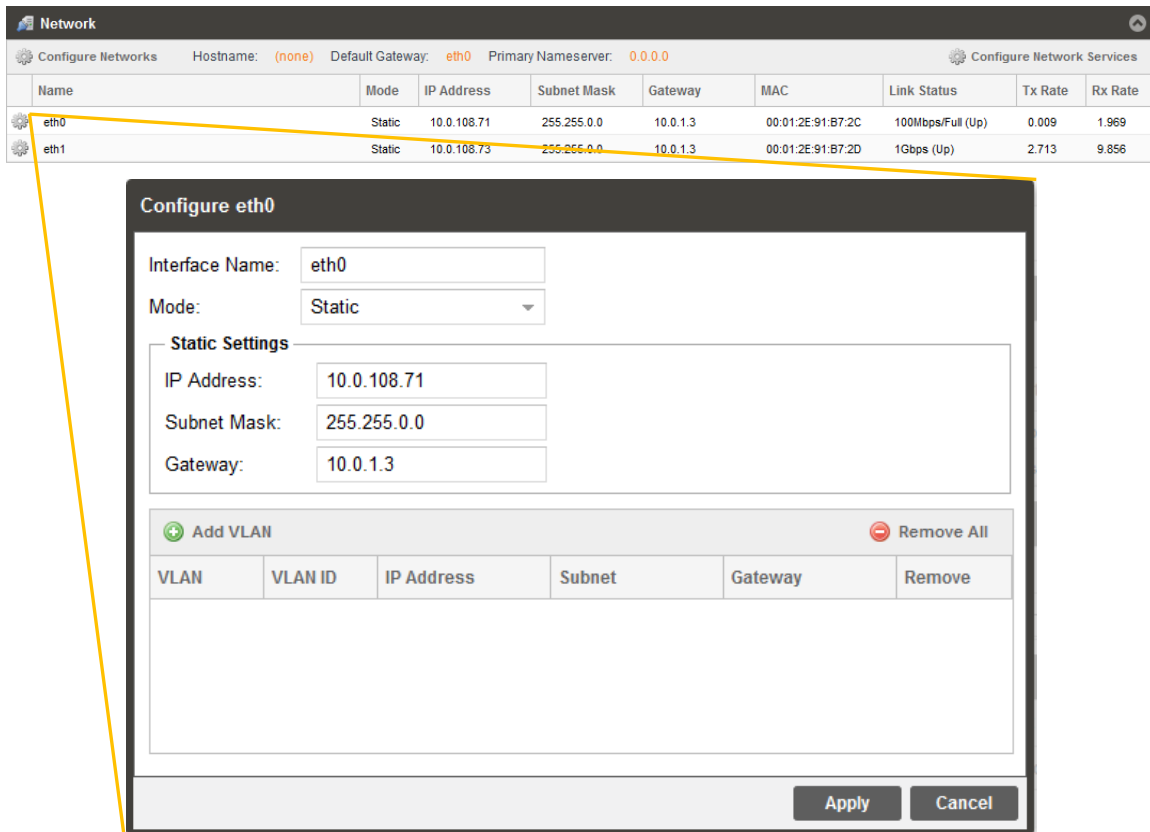
The DMG 7000 can be assigned a Hostname and DNS servers. To access this menu, click on the Configure Networks gear icon. Within the window that opens, the user can assign a Hostname to the DMG 7000, define which physical port (Eth0 or Eth1) the Default Gateway will use [The web-interface is accessible from the IP address of either Ethernet port; however, be sure to configure the two ports for separate subnets.], and provide addresses for Primary and Secondary Nameservers.




Setting	Available Selections	Description
Hostname	Alphanumeric, no spaces allowed	Defines optional system name
Default Gateway	Eth0, Eth1	Defines which physical port gateway address is to be used
Primary Nameserver	xxx.xxx.xxx.xxx	IP address of Primary (DNS) nameserver
Secondary Nameserver	xxx.xxx.xxx.xxx	IP address of Secondary (DNS) nameserver

## Management and Video/IP Ports

Each of the two physical NICs are identical in every way; either one can be configured for the management or Video/IP networks. As shown below, clicking the gear icon will open the settings for each NIC, including the name of the port, IP address and VLAN options. After finishing changes, click the apply button.



Setting	Available Selections	Description
Interface Name	User Entered (eth0 / eth1 by default)	User defined port names
Mode	DHCP, Static	DHCP allows network server to provide IP address Static requires the user to define the IP address to be used
IP Address	xxx.xxx.xxx.xxx	Static Mode IP address entry
Subnet Mask	xxx.xxx.xxx.xxx	Static Mode subnet mask entry
Gateway	xxx.xxx.xxx.xxx	Static Mode gateway entry

To add a VLAN to the NIC, click the  Add VLAN icon to bring up the “Add VLAN” menu as shown on the next page.

**Add VLAN**

VLAN Name:



VLAN Tag ID:

IP Address:

Subnet Mask:


Gateway:

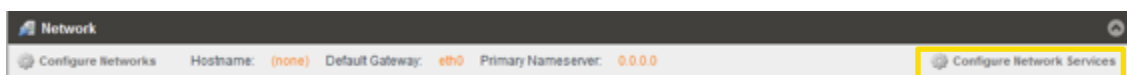
Setting	Available Selections	Description
VLAN Name	User Entered	User defined VLAN names
VLAN Tag ID	1 – 4094	The VLAN Tag to be assigned to outgoing streams and filtered for incoming streams
IP Address	xxx.xxx.xxx.xxx	Static Mode IP address entry
Subnet Mask	xxx.xxx.xxx.xxx	Static Mode subnet mask entry
Gateway	xxx.xxx.xxx.xxx	Static Mode gateway entry

After clicking “OK” to finish configuring the newly created VLAN, it will appear on the VLAN list as seen in the figure below. To remove individual VLANs, click the red  icon in the corresponding row. To remove all created VLANs, click the  Remove All button.

<

### Configuring Network Services

Both Physical NICs can have specific features enabled for functionality or disabled for security. To configure these settings, click on the  **Configure Network Services** as indicated in the figure below.



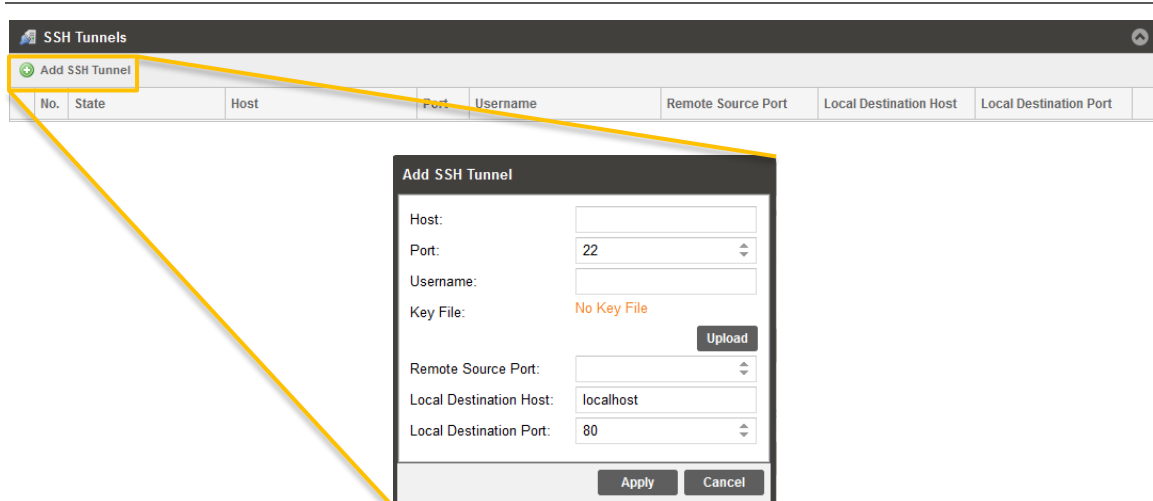
The “Configure Network Services” menu will then be shown. These are the default settings that allow for web access, ICMP contact through pinging and general stream input and output traffic. To enable or disable further settings, click to check the leftmost box as well as the box corresponding to the physical NIC (eth0, eth1) in the row of the intended service.

<input type="checkbox"/>	Service ↑	Protocol	Port	eth0 <input type="checkbox"/>	eth1 <input type="checkbox"/>
<input checked="" type="checkbox"/>	HTTP	TCP	80	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ICMP	ICMP	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SNMP	UDP	161	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	SNMP Traps	UDP	162	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	SSH	TCP	22	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Stream I/O	Unknown	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Syslog	UDP	514	<input type="checkbox"/>	<input type="checkbox"/>

Service	Protocol	Port	Description
HTTP	TCP	80	Allows access to the web interface via browser
ICMP	ICMP	N/A	Allows access to ICMP responses (such as pinging)
SNMP	UDP	161	Allows SNMP GET/SET commands
SNMP Traps	UDP	162	Enables SNMP traps to send upon system change
SSH	TCP	22	Allows for SSH access through port 22
Stream I/O	Unknown	N/A	Enables and disables all stream traffic for the physical interface (Zixi, MPEG/IP, SRT, HLS)
Syslog	UDP	514	Allows configuration of a syslog server for state triggered messages

#### 4.2.11 SSH Tunnels

The DMG 7000 can be remotely managed by using an SSH tunnel. In applications where Zixi ZEN Master is being used, an SSH tunnel is established to provide remote access to the web GUI of the DMG 2100.



**Figure 1: Adding SSH Tunnels**

The SSH tunnel configuration window will allow the user to define the connection to Zixi ZEN Master by providing the required details in the Add SSH Tunnel window. Most of the values for these settings can be found in your ZEN Master instance.

Setting	Range	Description
<b>Host</b>	IPv4 Address Valid Domain Name	The IP address or web link of the Zixi (ZEN Master) server
<b>Port</b>	0 – 65535	The IP port of the Zixi (ZEN Master) server
<b>Username</b>	User Entry	Account credential to log into Zixi (ZEN Master) server
<b>Key File</b>	N/A	Browse the local computer to select and upload a hashed key file used to open the secure connection to the Zixi (ZEN Master) server
<b>Remote Source Port</b>	0 – 65535	Remote port number the Zixi (ZEN Master) server is using for SSH communication
<b>Local Destination Host</b>	IPv4 Address Valid Domain Name	Address reporting to Zixi (ZEN Master) server. Localhost is the default.
<b>Local Destination Port</b>	0 – 65535	The port that is accessible to the Zixi (ZEN Master) server. Port 80 (DMG 7000 web client) is the default.

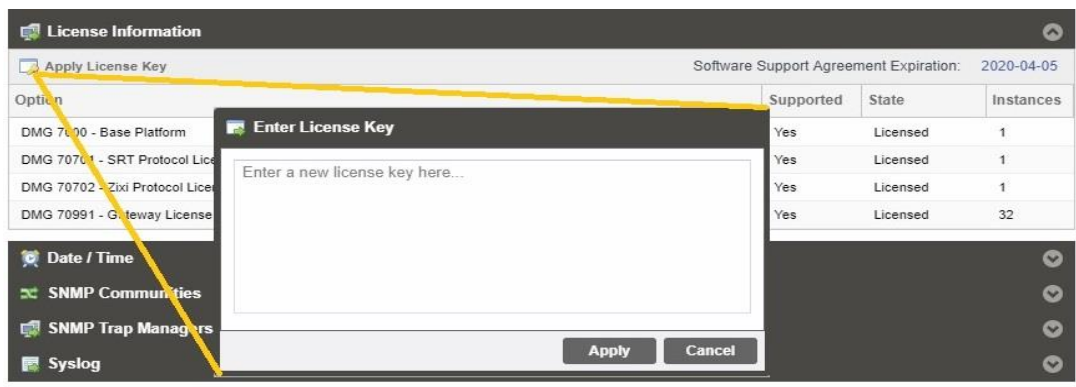


### 4.2.12 License Information

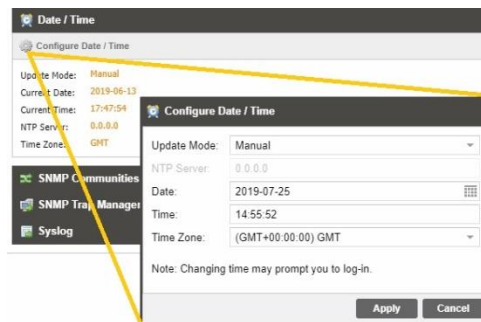
Certain features of the DMG 7000 require licenses in order to be functional. The interface displays all licenses available as well as the following status:

- License Locked or Unlocked
- License is Supported or Unsupported by the installed hardware


If licenses need to be applied to the DMG click Apply License Key button. The menu below will appear where the user can copy and paste the provided license key from Sencore.



### 4.2.13 Setting Unit Time and Date



The DMG 7000 can be set to synchronize with an NTP server or a manual data and time can be defined by the user. Click the “Configure Date/Time” cog icon to begin. These values are used to timestamp entries in the Alarm and Event logs under the Reporting tab.

Setting	Available selections	Description
Update Mode	NTP or Manual	NTP = user provides IP address of NTP server to synchronize system date and time with. Manual = user will define system date and time.
NTP Server	XXX.XXX.XXX.XXX Domain Name	Defines IP Address or Domain Name of the server to be used when in NTP mode.
Date	YYYY/MM/DD	Manual mode setting format for the system date. Calendar widget  can be used.
Time	00:00:00 – 24:00:00	Manual mode setting only - defines the system time. The time is based on a 24-hour clock.
Time Zone	-12:00:00 ~ +13:00:00	Applies a time offset to the value obtained from the NTP server

#### 4.2.14 Configuring SNMP

##### SNMP Communities

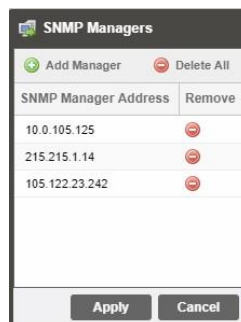


The screenshot shows the 'SNMP Community Strings' configuration window. It contains two text input fields: 'Read-Only Community' with the value 'public' and 'Read-Write Community' with the value 'private'. At the bottom, there are 'Apply' and 'Cancel' buttons.

SNMP Communities define whether users have read-only or read-write SNMP rights. These two communities are given unique names. The default names for these communities are:




- Read –Only Community: public
- Read- Write Community: private

##### SNMP Trap Managers



The screenshot shows the 'SNMP Managers' configuration window. It has a title bar with a plus icon and the text 'SNMP Managers'. Below the title bar are two buttons: 'Add Manager' (with a green plus icon) and 'Delete All' (with a red minus icon). There is a table with two columns: 'SNMP Manager Address' and 'Remove'. The table contains three rows of IP addresses: '10.0.105.125', '215.215.1.14', and '105.122.23.242'. Each row has a red minus icon in the 'Remove' column. At the bottom, there are 'Apply' and 'Cancel' buttons.

The SNMP trap managers are recipients of SNMP traps sent from the DMG 7000. The following menu allows the user to configure the recipient's IP addresses by adding or deleting target addresses of an SNMP Manager Address list.

<b>Add Manager</b>	 Add Manager	Adds IP address to SNMP Manager Address list
<b>Delete All</b>	 Delete All	Clears SNMP Manager Address list
<b>Delete Single Entry</b>		Removes single address from SNMP Manager list

#### 4.2.15 Syslog



The DMG 7000 can be configured to send error and event logs formatted in the syslog protocol to a remote user specified Syslog server.

<b>State</b>	Enabled or Disabled	Enabled = send message; Disabled = do not send
<b>Network Protocol</b>	UDP or TCP	Defines the protocol used to send the messages
<b>IP Address</b>	XXX.XXX.XXX.XXX	Defines the IP address of the Syslog server.
<b>Port</b>	0 - 65535	Defines the port of the Syslog server

### 4.3 Reporting Control Panel

The Reporting control panel in the DMG 7000 will provide the user with a list of active alarms, as well as a means to log the detected events. Active alarms are constantly updated to reflect the real-time state of the unit.

Once an error is no longer detected, it will be cleared from the active alarms window. The log files can be used to view alarm and event history. Both the active alarm and event logs can be configured for specific behavior based upon the user's needs.

Reporting Control Panel

Alarms **Logs** Configure

Refresh Clear Download

Severity	Timestamp	Transition	Location	Message
!	2019-07-08 01:54:48	+	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets OK
!	2019-07-08 01:54:48	+	Gateway Receive (Gatewa...	Zixi Receive Dropped Packets OK
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
!	2019-07-08 01:54:47	-	Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error

Gateway Admin **Reporting** About

Reporting Control Panel

Alarms **Logs** Configure

State	Name	Location	Last Changed
!	SRT Transmit Connection Error	Gateway Transmit 1 (Gateway 4)	2019-07-08 01:57:39
!	Ts Sync Loss Error	Gateway Receive (Gateway 4)	2019-07-08 01:57:34



#### 4.3.1 Alarms

Reporting Control Panel

Alarms **Logs** Configure

State	Name	Location	Last Changed
!	SRT Transmit Connection Error	Gateway Transmit 1 (Gateway 4)	2019-07-08 01:57:39
!	Ts Sync Loss Error	Gateway Receive (Gateway 4)	2019-07-08 01:57:34

Clicking on the Alarms button displays the Active Alarms menu. This list displays all of the *active alarms currently being reported* by the unit. There are four columns in the log that display different types of information.

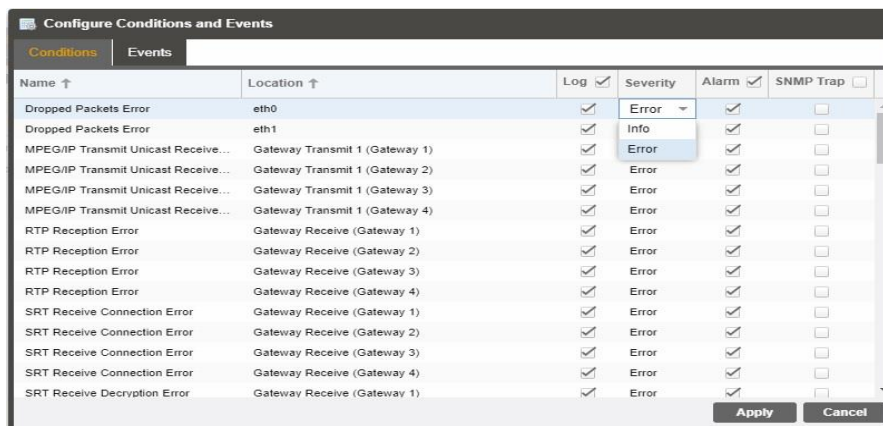
Alarms	
Column Name	Description
<b>State</b>	<p>This area displays an icon that will signify the importance of the event</p> <p>The  Info icon means the message is Informational and no error has been detected.</p> <p>The  Error icon means the message is an Alarm and the unit status has been set to 'Error'.</p>
<b>Name</b>	This column displays the description of the detected instance.
<b>Location</b>	This column displays the hardware or function that is experiencing the active error.
<b>Last Changed</b>	<p>This column displays the data and time the error was raised.</p> <p>Timestamps here are determined with the Date and Time settings configured in Section 4.2.11.</p>

### 4.3.2 Configuring the Alarms

The DMG 7000 monitoring points are divided into Conditions and Events and are managed separately. Configuration of these is done by clicking on the configuration cog in either the Alarms or Logs window.

#### Conditions

These instances are monitored within specific hardware and stream processing paths. How the DMG 7000 responds to the detection of the instance can be configured. Three 'checkbox' columns allow the user to define the system response. The checkbox at the top of the column can be used to enable or disable all instances in that column.



Logs	
Column Name	Description
<b>Name</b>	Defines the error message that will be provided if the instance is detected.
<b>Location</b>	This shows the user the specific hardware or stream processing path where the instance is detected.
<b>Log</b>	A checked box defines which instances will be recorded to the log file.
<b>Severity</b>	A dropdown box within the row allows the user to define the instance as an Error or Information event.
<b>Alarm</b>	A checked box defines which instances will raise an Alarm condition on the unit. This will cause the Error LED on the front of the unit and in the web client to illuminate.
<b>SNMP Trap</b>	A checked box defines which instances will trigger the DMG 7000 to send trap messages.

The APPLY button at the bottom of the window will commit the settings changes to the system, while the CANCEL button will ignore any settings changes and close the configuration window.

## Events

These instances are global to the system because they will have an impact on all hardware and stream processing areas of the DMG 7000. These instances can only be configured to be recorded in the log file and/or to be sent as SNMP Trap messages.

Configure Conditions and Events			
Conditions		Events	
Name ↑	Location ↑	Log <input checked="" type="checkbox"/>	SNMP Trap <input type="checkbox"/>
Date/Time Changed	Unit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
NTP Updated	Unit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Software Update Failed	Unit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Software Update Succeeded	Unit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unit Booted	Unit	<input checked="" type="checkbox"/>	<input type="checkbox"/>












Apply Cancel

Events	
Column Name	Description
<b>Name</b>	Defines the error message provided if the instance is detected.
<b>Location</b>	This will always be "Unit" since these instances are global
<b>Log</b>	A checked box defines which instances will be recorded to the log file.




**SNMP Trap**

A checked box defines which instances will trigger the DMG 7000 to send a trap message.






### 4.3.3 Event Logs

Gateway Admin Reporting About				
Reporting Control Panel				
Alarms		Logs		Configure
Refresh	Clear	Download		
Severity	Timestamp	Transition	Location	Message
	2019-07-09 01:48:27		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets OK
	2019-07-09 01:48:27		Gateway Receive (Gatewa...	Zixi Receive Dropped Packets OK
	2019-07-09 01:48:26		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
	2019-07-09 01:48:26		Gateway Receive (Gatewa...	Zixi Receive Dropped Packets Error
	2019-07-09 01:48:12		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets OK
	2019-07-09 01:48:12		Gateway Receive (Gatewa...	Zixi Receive Dropped Packets OK
	2019-07-09 01:48:11		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error
	2019-07-09 01:48:11		Gateway Receive (Gatewa...	Zixi Receive Dropped Packets Error
	2019-07-09 01:47:59		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets OK
	2019-07-09 01:47:59		Gateway Receive (Gatewa...	Zixi Receive Dropped Packets OK
	2019-07-09 01:47:58		Gateway Receive (Gatewa...	Zixi Receive Not Recovered Packets Error

The Logs window provides the user a display of the log file and management tools to streamline the data returned. There are three buttons that will manage the log file.

<b>Refresh</b>	 Refresh	Prompts the DMG 7000 to update the displayed logs.
<b>Clear</b>	 Clear	Clears the log file
<b>Download</b>	 Download	Exports the log file as a ".csv" extension file to the pc.

The log file itself is made up of five columns that explain each event, when it occurred, and the area of the system where the event was detected.

Column Name	Description
<b>Severity</b>	<p>The  Info icon means the message is Informational and no error has been detected.</p> <p>The  Error icon means the message is an Alarm and the unit status has been set to 'Error'.</p>
<b>Timestamp</b>	This is the DMG 7000 associated date and time of the instance. See Date/Time settings in Section 4.2.11.
<b>Transition</b>	<p>The  Went Bad icon means the instance entered into an Error state.</p> <p>The  Went Good icon means the instance entered into a Clear state.</p> <p>The  Event icon means a single point instance (such as NTP Time was updated) took place.</p>

<b>Location</b>	Defines the hardware or function that experienced the alarm or event.
<b>Message</b>	This displays the description of the specific path that experienced the instance.

#### 4.3.4 Configuring the Logs

Configuration of the logs will provide the user with the same configuration options as covered in section 4.3.2.

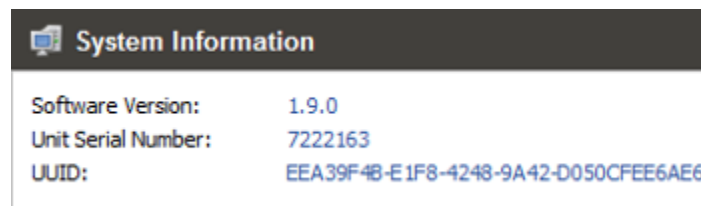
### 4.4 About Panel

Under the “About” panel, there is information about the current software version, hardware/software options, how to contact Sencore, and details on third party software being used.



#### 4.4.1 System Information

This area of the control panel gives the user the unit serial number and software version installed.



#### 4.4.2 Contact Information

This area of the control panel gives the user the physical address, web address and phone number as methods of contact.



### 4.4.3 Options

This area will provide details about both hardware and software contents of the DMG 7000 platform.

Options	
	DMG 70010 (DMG 70010 Single Channel)
+	DMG 7000 (DMG 7000 - Base Platform)
+	DMG 70701 (DMG 70701 - SRT Protocol License, per unit)
+	DMG 70702 (DMG 70702 - Zixi Protocol License, per unit)
+	DMG 70703 (DMG 70703 - RIST Protocol License, per unit)
+	DMG 70704 (DMG 70704 - HLS Protocol License, per unit)
+	DMG 70991 (DMG 70991 - Gateway License)

### 4.4.4 Third Party Software Information

This area of the control panel can be expanded to show the third-party software used by the DMG 7000. For more details see Section 5 – Appendix D for a complete list.

# Section 5 Appendices

## Introduction

This section includes the following appendices:

<b>Appendix A</b>	<b>– Specifications.....</b>	<b>83</b>
<b>Appendix B</b>	<b>– Error and Event List.....</b>	<b>86</b>
<b>Appendix C</b>	<b>– Internet Transport Protocol Explanation .....</b>	<b>88</b>
<b>Appendix D</b>	<b>– Acronyms and Glossary .....</b>	<b>90</b>
<b>Appendix E</b>	<b>– Warranty .....</b>	<b>91</b>
<b>Appendix F</b>	<b>– Support and Contact Information .....</b>	<b>92</b>
<b>Appendix G</b>	<b>– Open Source Software.....</b>	<b>93</b>

## Appendix A – Specifications

### DMG 7000 – Minimum Requirements

For 100Mbps of throughput

CPU:	Intel Quad-Core 1.1Ghz, up to 2.4Ghz
RAM:	4GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

For 250Mbps of throughput

CPU:	Intel Xeon 4-core 2.2Ghz
RAM:	8GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

For 850Mbps of throughput

CPU:	Intel Xeon 6-core 3.6Ghz
RAM:	16GB DDR4 2400MHz
HDD:	32GB SSD
Ethernet	2x 1GB RJ45 or SFP. Intel i350 chipset

### MPEG/IP Receive and Transmit

Receive –

Input Format:	UDP, RTP and RTP with extension headers Multicast and Unicast CBR SMPTE 2022/CoP3 FEC SMPTE 2022-7 Hitless Switching
Multicast Filtering:	Filters based on IP address VLAN Tagging IDs
Buffer size:	1 - 4000 KB, or 1 – 4000ms
Bitrate Range:	.25 – 200 Mb/s
Packets/IP Frame:	1-7 MPEG Packets/IP Frame
IGMP Compatibility:	Version 2 and 3

Transmit –

Output Format:	UDP and RTP
Bitrate Range:	.25 – 200 Mb/s
Packets/IP Frame:	1-7 MPEG Packets/IP Frame

### SRT Receive and Transmit

Receive –

Protocol and IP Range:	UDP, Unicast
Negotiation Modes:	Caller, Listener, Rendezvous
Latency:	20-8000ms, user configurable
Bitrate Range:	0.25 – 50 Mbps
Decryption:	AES-128, AES-256

---

Packets/IP Frame:	10-79 UTF-8 characters
Transmit –	Auto detect
Protocol and IP Range:	UDP, Unicast
Negotiation Modes:	Caller, Listener, Rendezvous
Latency:	20-8000ms, user configurable
Bandwidth Overhead:	0 – 50% of content bitrate
Bitrate Range:	0.25 – 50 Mbps
Encryption:	AES-128, AES-256
Packets/IP Frame:	10-79 UTF-8 characters
	1-7 MPEG Packets/IP Frame

**Zixi Receive and Transmit**

Receive –	
Protocol and IP Range:	UDP, Unicast
Latency:	30-10000ms, user configurable
Bitrate Range:	1 – 50 Mb/s
FEC Overhead:	0 – 50% of content bitrate
Decryption:	AES-128, AES-192, AES-256
Packets/IP Frame:	10-79 UTF-8 characters
Transmit –	Auto detect
Protocol and IP Range:	UDP, Unicast
Mode:	Feeder to Broadcaster
Latency:	30-10000ms, user configurable
Bandwidth Overhead:	0 – 50% of content bitrate
Bitrate Range:	0.25 – 50 Mbps
Encryption:	AES-128, AES-256
Packets/IP Frame:	10-79 UTF-8 characters
	1-7 MPEG Packets/IP Frame

**RIST Receive and Transmit**

Receive –	
Profile Mode	Simple, Main (Full Datagram), Main (Reduced Overhead)
Protocol and IP Range:	RTP, Unicast and Multicast
Latency:	1-8000ms, user configurable
Bitrate Range:	1 – 50 Mb/s
Decryption:	DTLS, PSK
Packets/IP Frame:	1-32 UTF-8 characters
Transmit –	Auto detect
Profile Mode	Simple, Main (Full Datagram), Main (Reduced Overhead)
Protocol and IP Range:	RTP, Unicast and Multicast
Latency:	1-8000ms, user configurable

---

Bitrate Range:	1 – 50 Mb/s
Decryption:	DTLS, PSK 1-32 UTF-8 characters
Packets/IP Frame:	1-7 MPEG Packets/IP Frame

**HLS Receive**

## Receive –

Protocol and IP Range:	HTTP, HTTPS, TCP, Unicast
Payload:	Chunked transport stream
Modes:	Pull, Push via WebDAV Push Mode supports up to 200GB or content
Profile Reception	Single profile selection
Bitrate Range:	0.25 – 50 Mbps
Decryption	AES-128 10-79 UTF-8 characters
Packets/IP Frame:	1-7 MPEG Packets/IP Frame

## Appendix B – Error and Event List

Events	Description
Date/Time Changed	The Date/Time setting of the system was changed
NTP Updated	The NTP Date/Time was updated
Software Update Failed	An attempted software update was unsuccessful
Software Update Succeeded	An attempted software update succeeded
Unit Booted	The system completed a boot process

Alarms	Description
Dropped Packet Error	The system has detected an instance of packets being dropped
HLS Receive Connection Error	The system encountered a connection error when receiving HLS transmission
MPEG/IP Transmit Unicast Receiver Not Found	The system was unable to detect the configured unicast receiver
NTP Server Unreachable	The system cannot connect to the configured NTP server
RIST Receive Connection Error	The system encountered a connection error when receiving RIST connection
RIST Receive Lost Packets Error	The system has detected lost packets in the received RIST signal
RIST Transmit Connection Error	The system has detected a connection error when transmitting SRT signal
RIST Transmit Lost Packets Error	The system has detected lost packets in the transmitted SRT signal
RTP Reception Error	The system has detected an error in RTP reception
SRT Receive Connection Error	The system encountered a connection error when receiving SRT transmission
SRT Receive Decryption Error	The system has errors when trying to decrypt SRT signal
SRT Receive Lost Packets Error	The system has detected lost packets in the received SRT signal
SRT Receive Skipped Packets Error	The system has detected skipped packets in the received SRT signal
SRT Transmit Connection Error	The system has detected a connection error when transmitting SRT signal
SRT Transmit Dropped Packets Error	The system has detected lost packets in the transmitted SRT signal
SRT Transmit NAK Received Error	The system has received a loss report from the receiver during the ARQ exchange and will retransmit packets
TS Sync Loss Error	The system has detected the loss of sync in the transport stream
Zixi Receive Connection Error	The system encountered a connection error when receiving Zixi transmission

Zixi Receive Decryption Error	The system has errors when trying to decrypt Zixi signal
Zixi Receive Dropped Packets Error	The system has detected dropped packets in the received Zixi signal
Zixi Receive Not Recovered Packets Error	The system is reporting that retransmitted packets were not recovered in the received Zixi signal
Zixi Transmit Connection Error	The system has detected an error when connecting to server to begin transmission
Zixi Transmit Dropped Packets Error	The receiving system is reporting that packets were dropped in the transmitted Zixi signal
Zixi Transmit Not Recovered Packets Error	The receiving system is reporting that retransmitted packets were not recovered in the transmitted Zixi signals

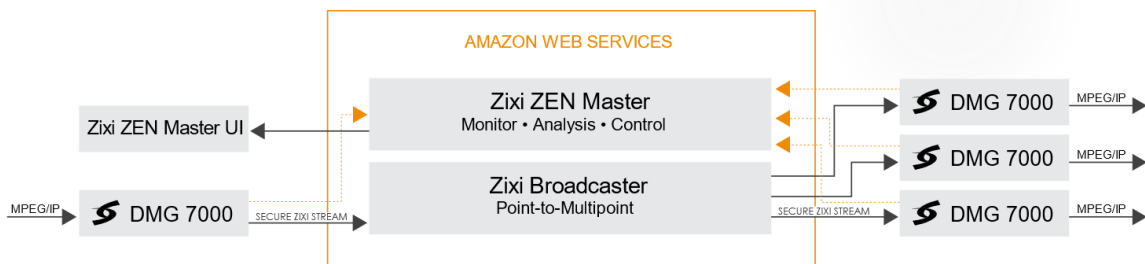
## Appendix C – Internet Transport Protocol Explanation

This section is intended to provide example system deployments of the DMG 7000 with all supported protocols. Each protocol can be used in different ways to accomplish the goal of distributing content reliability over unmanaged networks and internet connections. Generally speaking, each of these protocols uses a form of packet retransmission allowing receiving devices to request missing or corrupt packets from the source device. FEC (Forward error correction) is also used as an additional layer of protection at the expense of additional bandwidth overhead. When distributing content over unprotected networks, encryption becomes extremely important. AES-128 and AES-256 encryption is supported by the DMG 7000 to ensure content remains protected when sent across these networks.

In this first system the Zixi protocol is being used to transmit an MPEG/IP source over-the-internet to multiple destinations. This should could be used as point-to-point as well. A few keys points are important to understand.

- Streams being transmitted from the DMG 7000 must be sent to a Zixi Broadcaster.
- Streams being received on the DMG 7000 must be received from a Zixi Broadcaster.

This architecture ensures the “first-mile” and “last-mile” of the streams path through the internet are as short as possible. The Zixi Broadcaster and ZEN Master control system allow streams being distributed over the internet to achieve high reliability. The Zixi Broadcaster is an appliance or cloud instance function that ingests Zixi streams and enables additional functions such as transcoding, monitoring and analysis. The ZEN Master control system orchestrates these functions and allows remote access to the DMG 7000 via SSH tunnels. These systems utilize cloud systems such as Amazon Web Services, Microsoft Azure or Google Cloud Platform. Access to a Broadcaster and ZEN Master system must be arranged through Zixi.

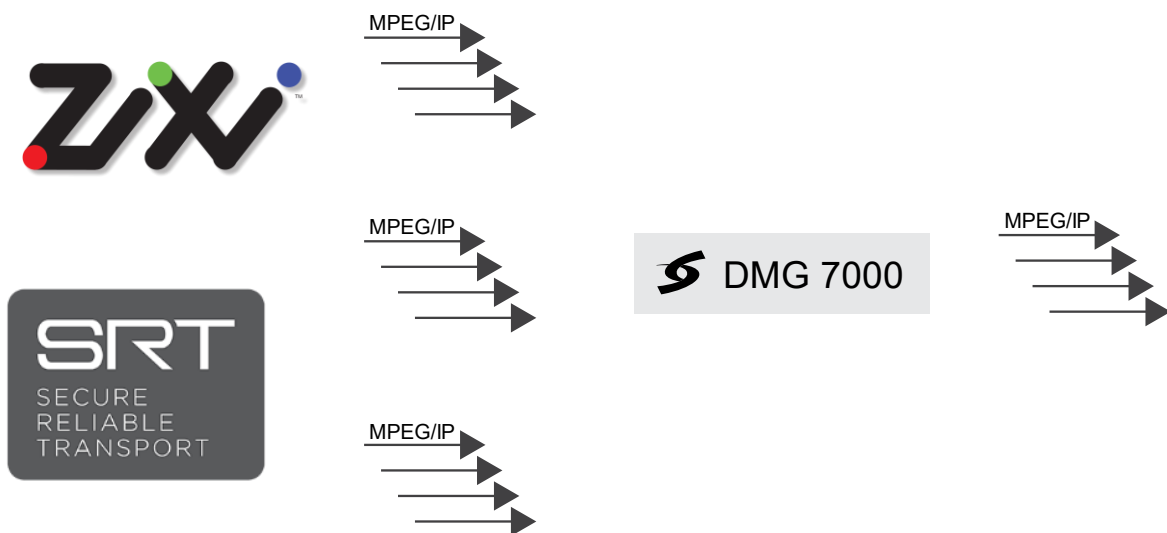


In this second system, the SRT protocol is being used for point-to-point transmission over the internet. The SRT protocol can be utilized without a central hub and transmit directly from a DMG 7000 to a receiving DMG 7000 over a consumer internet connection. Thanks to the DMG 7000’s ability to create multiple destinations from a single source one DMG 7000 can transmit to many end-points.





In this final example, the DMG 7000 is being used for signal acquisition from sources transmitted over an unmanaged network or internet connection. The goal of the DMG 7000 is to be protocol agnostic, allowing reception of MPEG/IP, SRT, Zixi and other protocols. This flexibility allows users to ingest streams sources from a variety of network architectures and turnaround these streams to MPEG/IP for use in typical broadcast networks.



## Appendix D – Acronyms and Glossary

**8VSB:** Vestigial sideband modulation with 8 discrete amplitude levels.  
**AAC:** Advanced Audio Coding  
**AC3:** Audio Coding Three  
**ADTS:** Audio Data Transport Stream  
**ASI:** Asynchronous Serial Interface  
**ATSC:** Advanced Television Systems Committee  
**AV:** Audio Video  
**Bit Rate:** The rate at which the compressed bit stream is delivered from the channel to the input of a decoder.  
**BPS:** Bits per second.  
**CAT6:** Category 6 – Cable standard for gigabit Ethernet  
**DHCP:** Dynamic Host Configuration Protocol  
**DMG 7000:** Digital Media Gateway  
**DVB:** Digital Video Broadcasting  
**FEC:** Forward Error Correction  
**GOP:** Group of Pictures  
**HD:** High Definition  
**HDMI:** High Definition Multimedia Interface  
**I/O:** Input/Output  
**IP:** Internet Protocol  
**LED:** Light Emitting Diode  
**MAC:** Medium Access Control  
**MIB:** Management Information Base  
**MPEG:** Moving Picture Experts Group  
**MPTS:** Multiprogram Transport Stream  
**NTP:** Networking Time Protocol  
**RIST:** Reliable Internet Stream Transport  
**RU:** Rack Unit  
**SD:** Standard Definition  
**SMPTTE:** Society of Motion Pictures and Television Engineers  
**SNMP:** Simple Network Management Protocol  
**SPTS:** Single Program Transport Stream  
**SRT:** Secure Reliable Transport  
**TS:** Transport Stream

## **Appendix E – Warranty**

### **Sencore One-Year Warranty:**

Sencore warrants this instrument against defects from any cause, except acts of God and abusive use, for a period of 1 (one) year from date of purchase. During this warranty period, Sencore will correct any covered defects without charge for parts, labor, or recalibration.

## Appendix F – Support and Contact Information

### Returning Products for Service or Calibration

The DMG 7000 server is a delicate piece of equipment and needs to be serviced and repaired by Sencore. Periodically it is necessary to return a product for repair or calibration. In order to expedite this process please carefully read the instructions below.

#### RMA Number

Before any product can be returned for service or calibration, an RMA number must be obtained. In order to obtain an RMA number, use the following steps.

Copy and paste, or enter the following link into a web browser:

<http://www.sencore.com/procare-support/service-repair>

Complete the on-line request form and click the Submit button at the bottom of the page

Once the RMA is generated it will be emailed to the address provided on the request. Shipping instructions will also be included.

#### Shipping the Product

Once an RMA number has been issued, the unit needs to be packaged and shipped back to Sencore. It's best to use the original box and packaging for the product but if this not available, check with the customer service representative for the proper packaging instructions.

Note: **DO NOT** return any power cables or accessories unless instructed to do so by the customer service representative.

## Appendix G – Open Source Software

The DMG 7000 includes:

Package	Version	License	Copyright
amibios dmi	75dce7b	GPL Version 2, June 1991	Claudio Matsuoka
BusyBox	1.24.2	GPL Version 2, June 1991	Erik Anderson, et.al.
Dropbear	2016.74	MIT-like	2002-2015 Matt Johnston, et.al (see license)
e2fsprogs	1.45.4	GPL Version 2, June 1991	Theodore Ts'o
ethtool	4.13	GPL Version 2, June 1991	David Miller, et.al.
FamFamFam Silk Icons	013	Creative Commons Attribution 2.5	Mark James
FastDB	3.71	MIT-like	Konstantin Knizhnik
FCGI	2.4.6	FastCGI	Open Market, Inc
FFmpeg	3.4	LGPL Version 2.1, February 1999	Fabrice Bellard
gptfdisk	1.0.3	GPL Version 2 June 1991	Roderick W. Smith
grub	2.00	GPL Version 3.29 June 2007	1994-2011 Free Software Foundation, Inc.
Lighttpd	1.4.30	BSD	2004, Jan Kneschke
libpcap	1.8.1	BSD	1993, 1994, 1995, 1996 The Regents of the University of California
Linux	5.3.5	GPL Version 2 June 1991	Linus Torvalds, et. Al.
Log4cpp	1.1.3	LGPL Version 2.1 February 1999	Bastiaan Bakker
Monit	5.1.1	GPL Version 3.29 June 2007	2010 Tildeslash Ltd.
Net-SNMP	5.7.1	BSD	1989, 1991, 1992 by Carnegie Mellon University, et.al (see license)
NTP	4.2.4p7	NTP License	1992-2009 David L. Mills
OpenSSL	1.0.1c	BSD-Like	1998-2008 The OpenSSL Project, 1995-1998 Eric Young
PCRE	8.30	BSD	1997-2012 University of Cambridge, et.al (see license)
POPT	1.16	MIT	1998 Red Hat Software
pureftpd	1.0.46	BSD	Frank Denis
qDecoder	12.0.4	BSD	2000-2012 Seungyoung Kim
samba	4.7.0	GPL Version 3.29 June 2007	Andrew Tridgell, et.al
Spawn-FCGI	1.6.3	BSD	Jan Kneschke, Stefan Bahler
srt	1.4.1	MPLv2.0 License	2018 Haivision Systems Inc.
TCLAP	1.2.0	MIT	2003 Michael E Smoot
tzdata	2017b	Public domain, BSD 3-clause	Arthur David Olson
Zlib	1.2.7	Zlib/libpng License	1995-2005 Jean-loup Gailly and Mark Adler

