



Centra Gateway Video Distribution Platform

User Manual

Copyright

© 2024 Sencore, Inc. All rights reserved.
3200 Sencore Drive, Sioux Falls, SD USA
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.

Revision History

Date	Version	Description	Author
9/29/2023	1.0	Initial Release (1.0.0 Software)	IWK

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 extended 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.

Unexpectedly 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
- **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 always remain readily accessible and operable.
- 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. Centra Gateway Chassis
2. Centra Gateway Software
3. AC Power Cable
4. Quick Start Guide

If any of these items were omitted from the packaging, please email ProCare@Sencore.com to obtain a replacement.

Table of Contents

Section 1 Appliance Install and Overview	9
1.1 Product Introduction.....	10
1.2 Power Connection	10
1.3 Maintenance	10
1.4 Network Setup via KVM.....	10
1.5 Front Panel Overview	11
1.6 Rear Panel Overview.....	12
Section 2 Software Installation	14
2.1 Installation Prerequisites.....	15
2.1.1 Centra Gateway – Minimum Requirements	15
2.2 Installation of Centra Gateway software	16
2.2.1 Installation via .run file	16
2.2.2 Installation via ISO.....	16
2.3 Request and Install Licenses.....	17
Section 3 Web Interface Operation.....	19
3.1 Logging into the Centra Web Interface	20
3.2 Navigation Pane	21
3.3 Search Bar	24
Section 4 Control Panels.....	26
4.1 Notifications Control Panel	27
4.2 Monitor Control Panel	28
4.2.1 Monitoring System Level Metrics and Performance.....	29
4.2.2 Monitoring Overall System Bandwidth	29
4.2.3 Monitoring Routes and Groups	31
4.3 Director Control Panel	32
4.4 Director Control Panel	33
4.4.1 Adding a Route	34
4.4.1.1 Route Options	36
4.4.1.2 Destination and Source Options	38
4.4.2 Source Node Settings.....	39
4.4.2.1 MPEG/IP Source Settings	41
4.4.2.2 SRT Source Settings	43
4.4.2.3 Zixi Source Settings	45
4.4.2.4 HLS Source Settings	48
4.4.2.5 Seamless RTP Source Settings	50
4.4.2.6 RIST Source Settings	52
4.4.2.7 Primary and Backup Failover Options	54
4.4.3 Destination Node Settings.....	57
4.4.3.1 MPEG/IP Destination Settings.....	59
4.4.3.2 SRT Destination Settings.....	62
4.4.3.3 Zixi Destination Settings	65
4.4.3.4 RIST Destination Settings.....	68
4.4.4 Route Statistics and Telemetry	71
4.4.4.1 MPEG/IP Telemetry Information.....	75
4.4.4.2 SRT Telemetry Information.....	80
4.4.4.3 Zixi Telemetry Information	86
4.4.4.4 RIST Telemetry Information.....	92
4.4.4.5 HLS Source Telemetry	98
4.4.4.6 Seamless RTP Source Telemetry	99
4.4.5 Groups.....	102

4.5	Analyze	105
4.5.1	TS Analyzer Settings	106
4.5.2	TS Analyzer Information	109
4.6	Templates	112
4.6.1	Viewing and Using Templates	113
4.6.2	Creating Route Templates.....	115
4.6.3	Creating Source Templates.....	116
4.6.4	Creating Destination Templates	116
4.7	Reporting Control Panel	117
4.7.1	Alarms.....	117
4.7.2	Log.....	118
4.8	System	120
4.9	Administration Control Panel	120
4.9.1	General	121
4.9.1.1	Setting Unit Label	121
4.9.1.2	Setting Unit Date and Time	122
4.9.2	Network.....	124
4.9.2.1	Configuring Hostname and DNS	124
4.9.2.2	Configuring Network Services	125
4.9.2.3	Management and Data Ports.....	127
4.9.3	SSH Tunnels	131
4.9.4	Security.....	133
4.9.4.1	Changing Unit Password	133
4.9.4.2	Security Manager.....	134
4.9.4.3	Enabling DTLS.....	137
4.9.5	Reboot the Unit.....	138
4.9.6	Updating the System Software	139
4.10	Licenses.....	141
4.11	About.....	142
4.11.1	System Information.....	142
4.11.2	Contact Information	143
4.11.3	Third Party Software Information.....	144
Section 5	Appendices.....	145
Appendix A	– Specifications.....	146
Appendix B	– Error and Event List.....	149
Appendix C	– Internet Transport Protocol Explanation	151
Appendix D	– 101 290 Descriptors	153
Appendix E	– Acronyms and Glossary	154
Appendix F	– Warranty	155
Appendix G	– Support and Contact Information	156
Appendix H	– Open Source Software.....	157

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	10
1.4	Network Setup via KVM.....	10
1.5	Front Panel Overview	11
1.6	Rear Panel Overview.....	12

1.1 Product Introduction

The Centra Gateway Video Distribution Platform 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 Centra Gateway can be purchased from Sencore as an appliance or installed as software on Alpine Linux. Initial configuration can be done from mouse/keyboard/monitor or SSH. Once the management IP parameters are configured, the Centra Gateway can be operated and monitored via web interface, SNMP or Rest API over ethernet.

The Centra Gateway 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

1.2 Power Connection

The Centra Gateway 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 Centra Gateway
3. Insert the power plug to a protected AC outlet

1.3 Maintenance

The Centra Gateway 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 Centra Gateway, please send an email request to one of our Sencore Pro Care members (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 Centra Gateway 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 the initial network configuration menu see the Sencore Centra Gateway Quick-Guide documentation.

1.5 Front Panel Overview

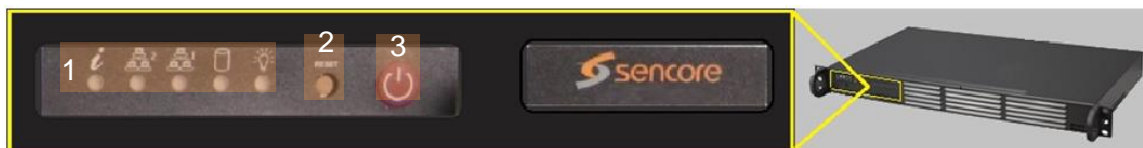
There are three form factors for the Centra Gateway. There are details below for each front panel. Note that connectors without highlighting and description are not used by the Centra Gateway and should not be connected.

CENTRA-GW-HW-MINI – Centra Gateway 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

CENTRA-GW-HW-FIELD – Centra Gateway Field Unit



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

CENTRA-GW-HW-HEADEND – Centra Gateway Headend Unit



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

1.6 Rear Panel Overview

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

CENTRA-GW-HW-MINI – Centra Gateway Mini Unit



1. RJ45 Ethernet Ports for Management or Data
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)

CENTRA-GW-HW-FIELD – Centra Gateway 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

CENTRA-GW-HW-HEADEND – Centra Gateway 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

Introduction

This procedure is for anyone installing Centra Gateway software onto a server that is not purchased from Sencore. The software can be loaded onto any server that meets the minimum server requirements listed in [Appendix A](#). To enable the software, the customer will need to reach out to sales@sencore.com to buy or get demo licenses.

This section includes the following topics:

2.1	Installation Prerequisites.....	15
2.2	Installation of Centra Gateway software.....	16
2.3	Request and Install Licenses.....	17

2.1 Installation Prerequisites

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

1. Physically install (racked or mounted) the server hardware.
2. Install Alpine Linux operating system at:
<https://alpinelinux.org/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 Centra Gateway. 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 for the Centra Gateway installation file.

NOTE: Tutorial for installing Alpine Linux can be found at:
<https://docs.alpinelinux.org/user-handbook/0.1a/Installing/medium.html>

2.1.1 Centra Gateway – 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 800Mbps 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

2.2 Installation of Centra Gateway software

2.2.1 Installation via .run file

1. Transfer the Centra Gateway “.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 Centra Gateway 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 CentraXXX.run” and press Enter
 - c. Type “sudo ./CentraXXX.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.

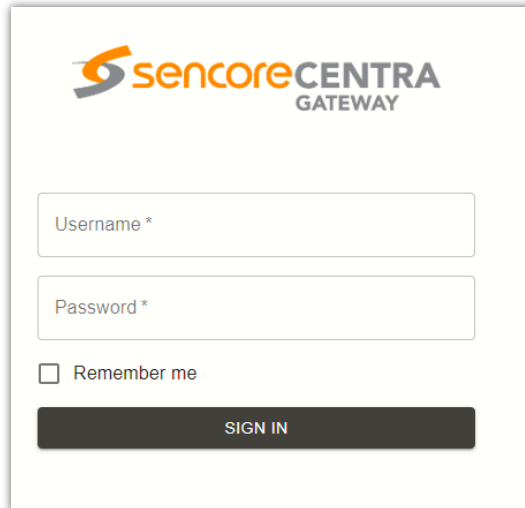
2.2.2 Installation via ISO

1. Download the installer ISO.
2. Use it to create a bootable USB flash drive (e.g. with Rufus).
3. Insert the installation media into device and boot to it.
 - a. By default it will install to the first detected hard disk.
 - b. If prompted, log in using these credentials
User: admin
Pass: mpeg101

2.3 Request and Install Licenses

Request License for Centra Gateway

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

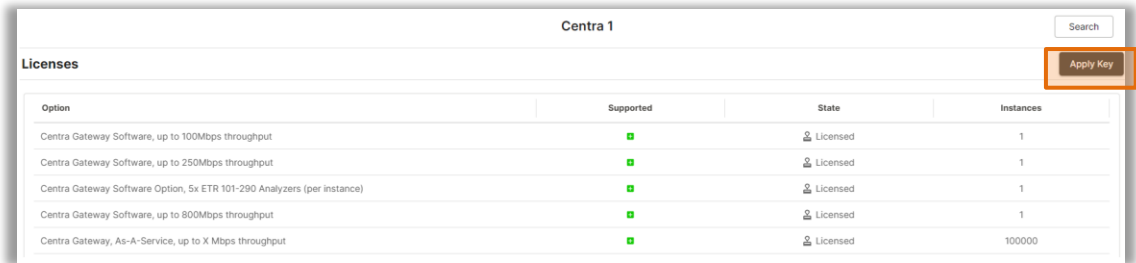
The image shows the login interface for the Sencore Centra Gateway. At the top, there is a logo consisting of a stylized orange 'S' followed by the text 'sencore' in orange and 'CENTRA GATEWAY' in grey. Below the logo, there are two input fields: 'Username *' and 'Password *'. Under the password field, there is a checkbox labeled 'Remember me'. At the bottom of the form is a dark grey button with the text 'SIGN IN' in white capital letters.

4. The default user is **admin** and the default password is **mpeg101**.
5. Click Sign In to continue.
6. Retrieve UUID from Centra Gateway user interface by navigating to the About tab.
7. Email the UUID to sales@sencore.com to retrieve demo license or purchase license.

Install license for Centra Gateway

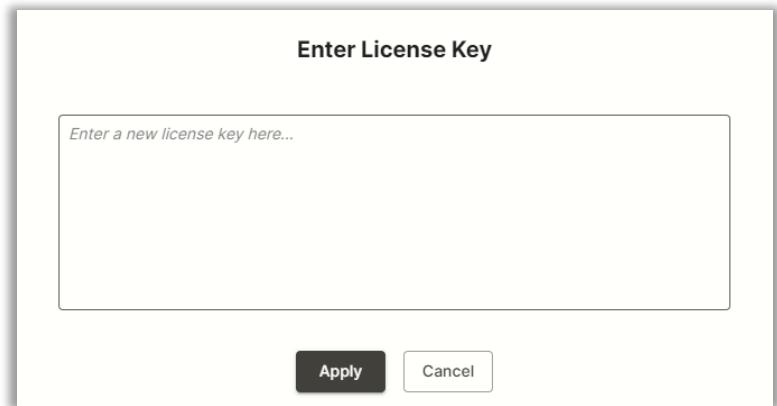
1. Click on the “System” drop down on the navigation pane in the Centra Gateway user interface
2. Navigate to the “Licenses” section

3. Click the “Apply Key” button in the top right of the Licenses section.



Apply Key Location

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



Enter License Key Menu

5. The Centra Gateway will display the new licenses being added. Reboot. After the unit reboots, the new licenses are applied.

Section 3 Web Interface Operation

Introduction

This section includes the following topics:

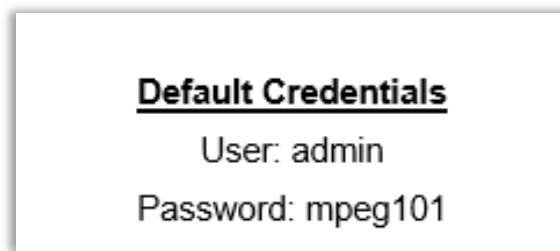
3.1	Logging into the Centra Web Interface	20
3.2	Navigation Pane	21
3.3	Search Bar	24

3.1 Logging into the Centra Web Interface

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

- Internet Explorer
- Microsoft Edge
- Firefox
- Google Chrome

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 sign in button to sign into the web interface.

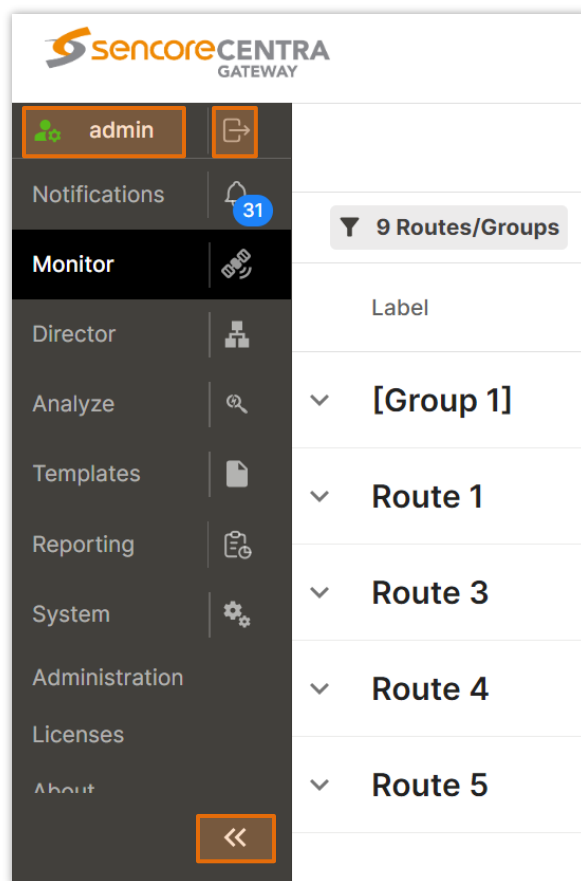


The login prompt features the Sencore CENTRA GATEWAY logo at the top. Below the logo are two input fields: 'Username *' and 'Password *'. Under the password field is a checkbox labeled 'Remember me'. At the bottom is a dark grey button with the text 'SIGN IN' in white capital letters.

Login Prompt


3.2 Navigation Pane



The navigation pane is the tab used for moving around the Centra interface. The web interface provides complete control of unit configuration and process monitoring with ten separately defined control panels inside the navigation pane. Each control panel has a distinct purpose to help locate the unit features



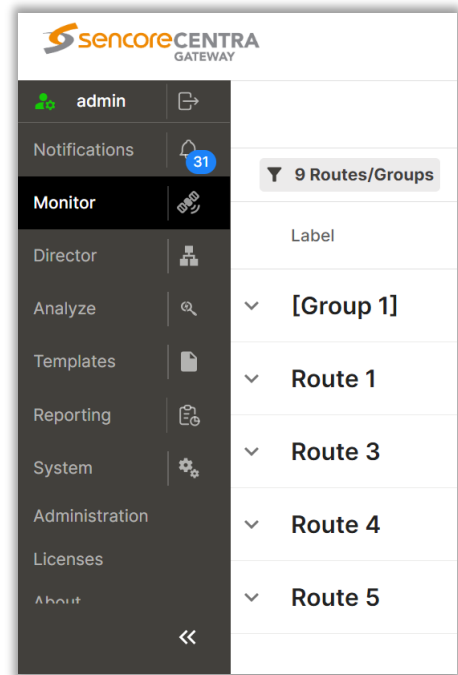
Navigation Pane

Where admin is indicated, this shows which User is currently logged into the GUI.

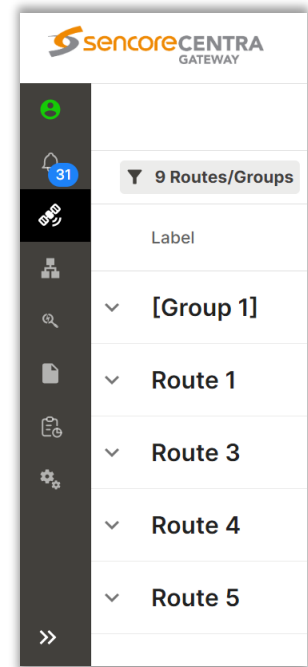
The logout icon, , allows the currently signed in user to logout.

The  and  icons can expand or collapse the “Navigation Pane”

Expanded Navigation Pane



Collapsed Navigation Pane



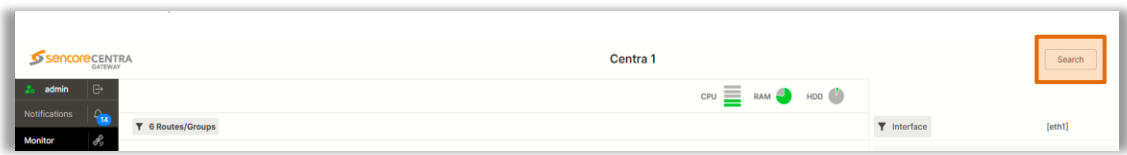
In general, ^ and v icons may be used throughout the control panels to similarly collapse and expand status and config menus.

Within the Navigation Pane, the control panels are:

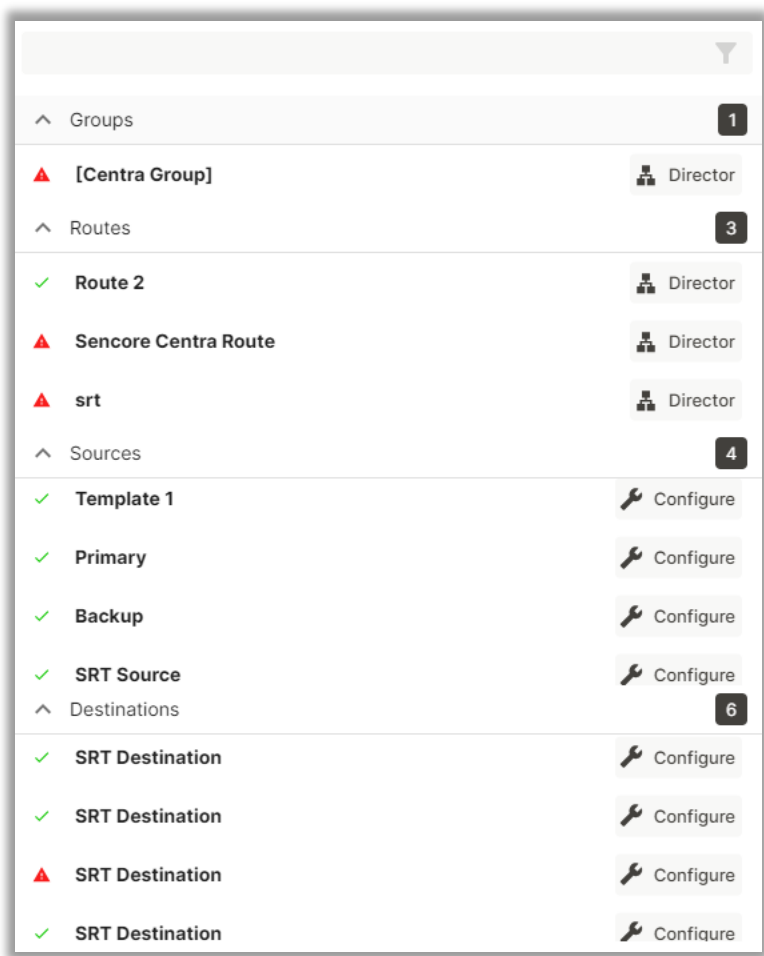
Control Panel	Description
Notifications	The notifications control panel can be expanded and retracted for a quick visual on alarms and can be used to navigate to alarming nodes
Monitor	Here the bitrate, bandwidth, and system performance can be viewed
Director	Where the video stream processing configurations are managed
Analyze	This control panel is used to control 101 290 Analysis on input and output nodes
Templates	This control panel allows a view of all saved route, source, and destination templates
Reporting	This control panel is where alarms & logs are reported, configured, and maintained
System	This control panel is where unit hardware and administrative settings will be configured and monitored. Software and unit details also shown under this panel
Administration	This control panel gives access to device settings. Access given: Date/Time, Network, SSH Tunnels, Security
Licenses	This control panel shows licenses applied and allows application of new license key
About	This control panel shows software version, serial number, support, and third party information

3.3 Search Bar



The search bar is in the top right corner of the page and can be used to look through all the flows.



Search Location



Search Dropdown

The  **Configure** button is for a single destination or source node and will open the hosting route as well as the configuration menu for that node. The  **Director** icon will navigate to a route or group without opening additional node configuration menus.

Section 4 Control Panels

Introduction

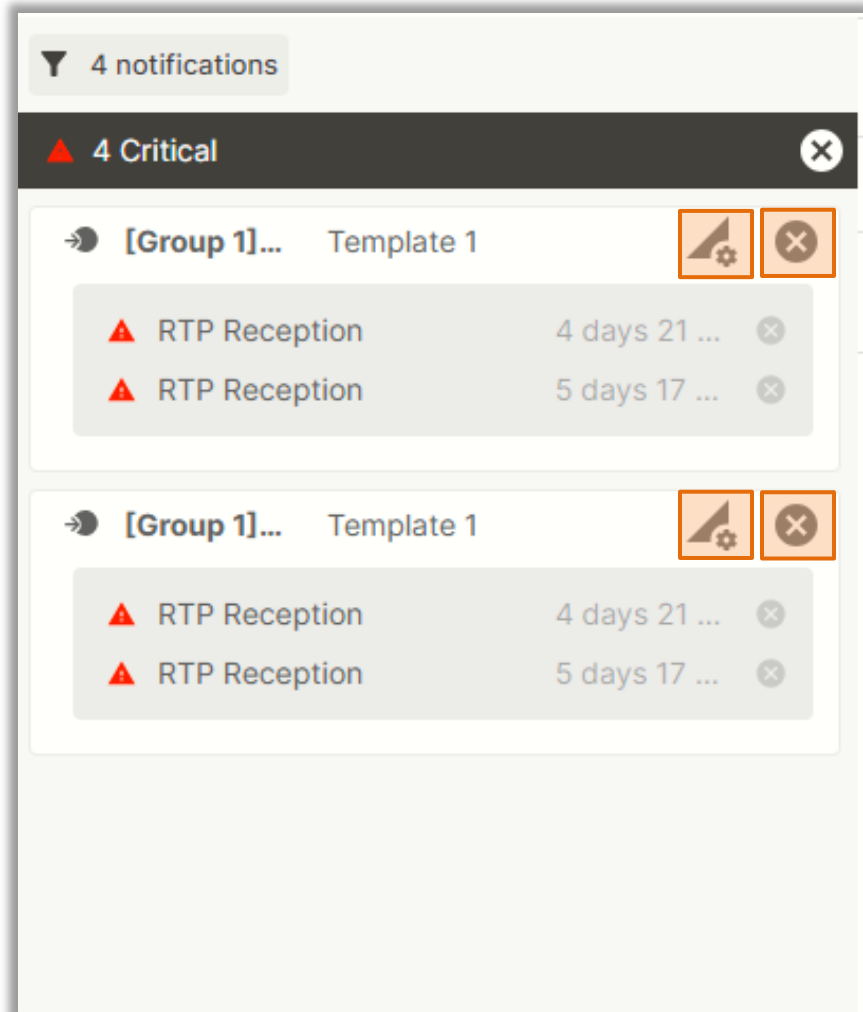
This section includes the following topics:

- 4.1 Notifications Control Panel27
- 4.2 Monitor Control Panel28
- 4.3 Director Control Panel32
- 4.4 Director Control Panel33
- 4.5 Analyze105
- 4.6 Templates112
- 4.7 Reporting Control Panel117
- 4.8 System120
- 4.9 Administration Control Panel120
- 4.10 Licenses141
- 4.11 About.....142





4.1 Notifications Control Panel

The Notifications control panel can be expanded or retracted and is used to view all current system alarms/alerts.



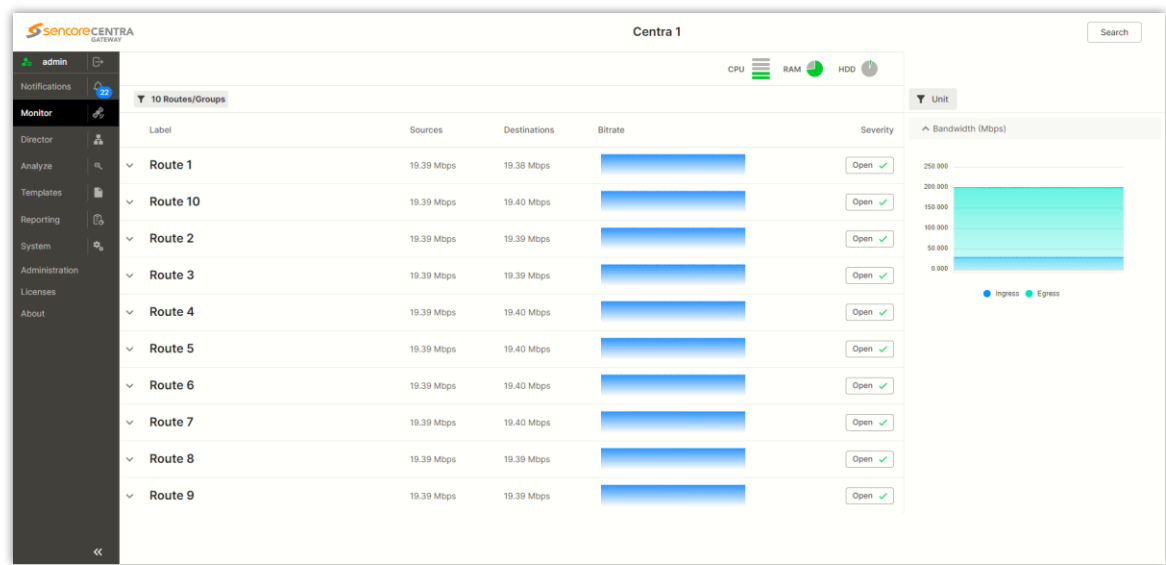
Notifications Panel

Clicking the  icon will automatically navigate to the alarming group or route.

Clicking on the  icon will remove the alert from the notification tab.

4.2 Monitor Control Panel

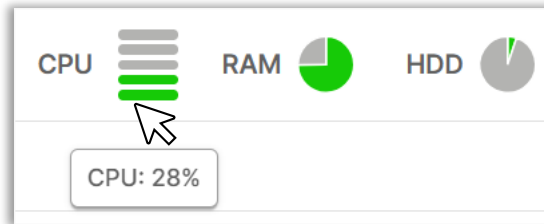
The Monitor control panel of the Centra Gateway web interface is used to view the system, route, and group performance details. This includes bitrate (destination, source), CPU, RAM, and disk usage.



Monitor Main Page

4.2.1 Monitoring System Level Metrics and Performance

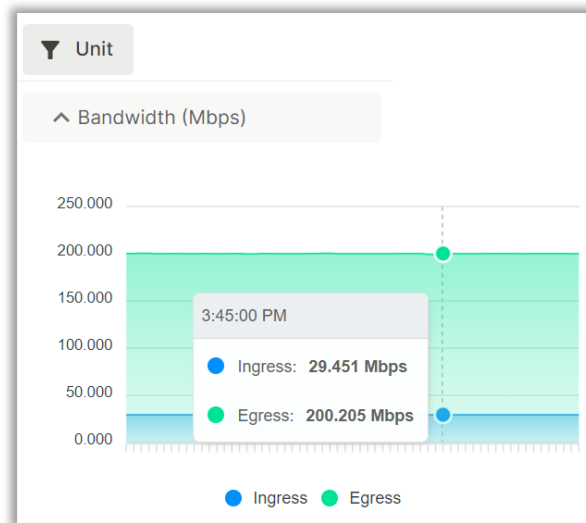
The CPU, RAM and HDD icons show overall system metrics and performance. Hover over the icons to expose the actual percent value used.



CPU represents the total percentage of processing power utilized by routes, groups, and other operations on the server. RAM is the total amount of available memory utilized across the on-board RAM disks, and HDD shows the total amount of storage utilized on-board the server.

4.2.2 Monitoring Overall System Bandwidth

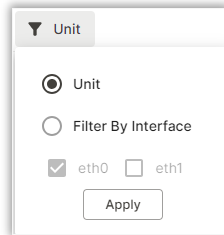
Upon loading the “Monitor” control panel, the “Bandwidth (Mbps)” graphics will begin collecting values for the aggregate ingress and egress bitrate throughout the whole system. Hover over the graph to show the values for Ingress and Egress bitrate in that moment.



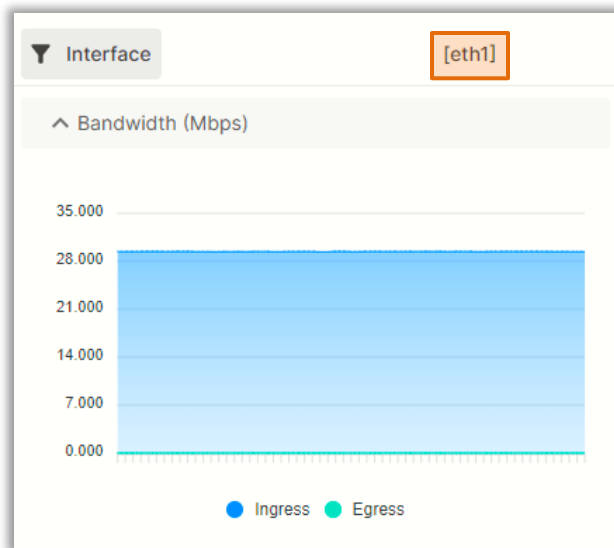
Bandwidth Section

The vertical axis represents bitrate in Mbps, while the horizontal axis represents up to the last five minutes of readings (collected in increments of five seconds).

The unit icon can be used to filter the aggregate bandwidth either for all NICs in the server or specific singular NICs.



When filtering by interface, the current selected interface(s) will be displayed at the top right.



4.2.3 Monitoring Routes and Groups

Routes are the main function of the Centra. When configured, a route will receive sources before outputting to one or more destinations. Groups are a collection of multiple routes.

9 Routes/Groups				
Label	Sources	Destinations	Bitrate	Severity
▼ [Group 1]	38.79 Mbps	38.78 Mbps	<div></div>	Open ✓
▼ Route 1	19.39 Mbps	19.38 Mbps	<div></div>	Open ✓

Monitoring Page and Route Level View

Click the drop-down arrow to view more information about the route/group.

^

[Group 1]

38.79 Mbps

0.0 Mbps

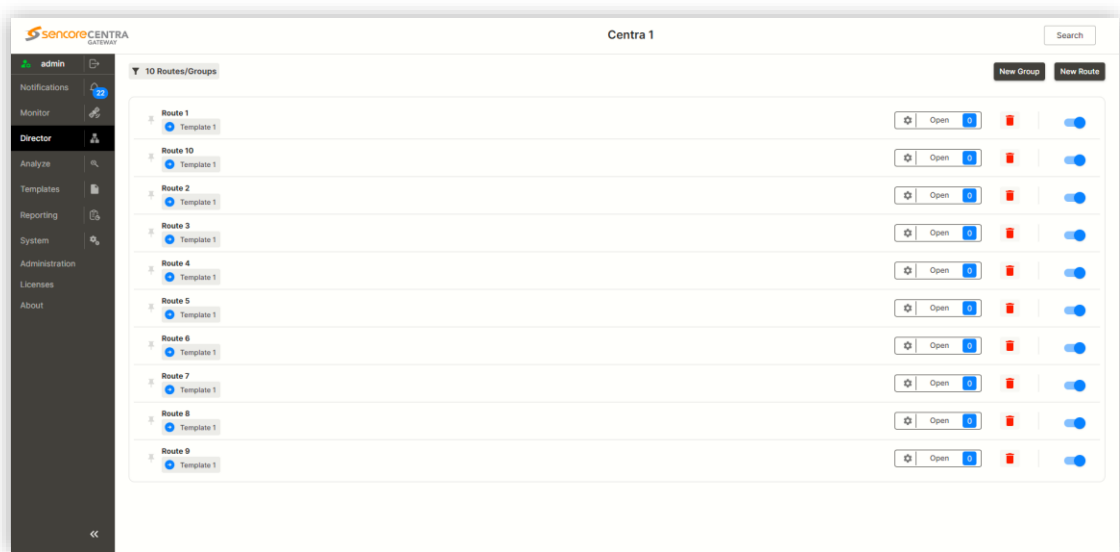
Open

Route	Direction	Label	Interface	Protocol	Address	TR 101 290
Route 1		Template 1	eth1	MPEG IP	239.192.1.50:...	
		Dest. Templ...	eth1	MPEG IP	239.192.105.1...	
Route 2		Template 1	eth1	MPEG IP	239.192.1.50:...	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>

Monitor Group (Multiple Routes in One Group)

4.3 Director Control Panel

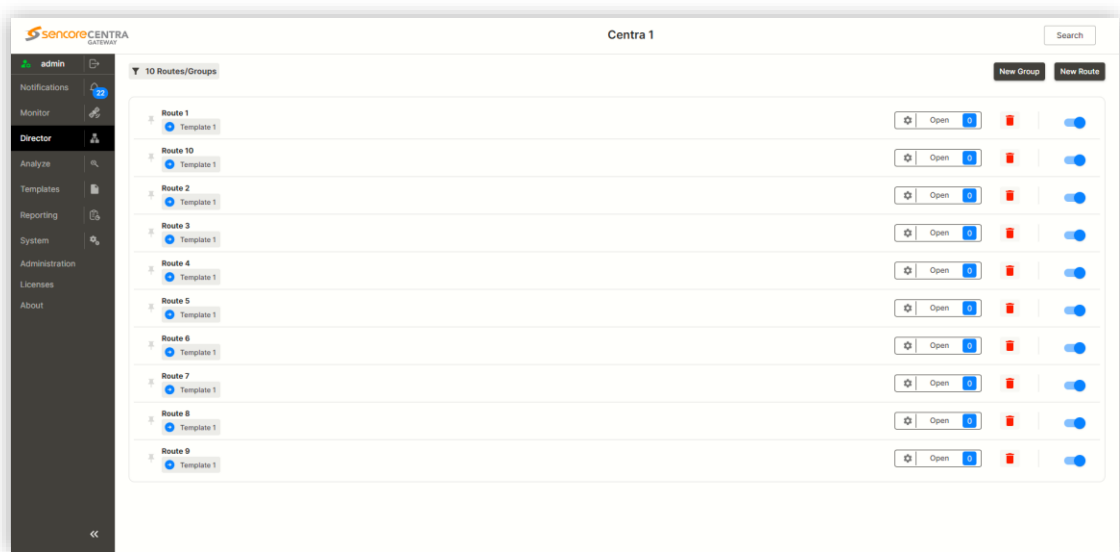
The Director control panel of the Centra Gateway web interface is used to configure the processing and distribution of video. This will include signal direction (destination, source, or both), addresses to be received or delivered to and labeling of the gateways to help the user distinguish gateways from one another. The number of available routes will depend upon the license key that is applied.



Director Main Page

4.4 Director Control Panel

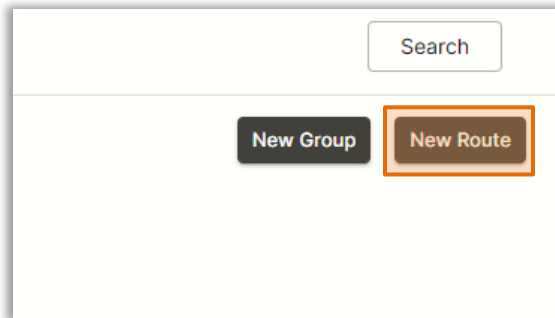
The Director control panel of the Centra Gateway web interface is used to configure the processing and distribution of video. This will include signal direction (destination, source, or both), addresses to be received or delivered to and labeling of the gateways to help the user distinguish gateways from one another. The number of available routes will depend upon the license key that is applied.



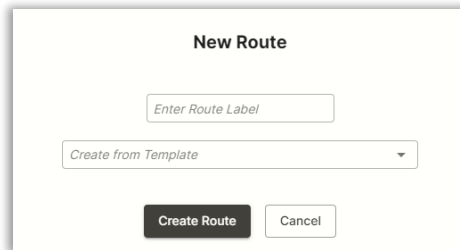
Director Main Page

4.4.1 Adding a Route

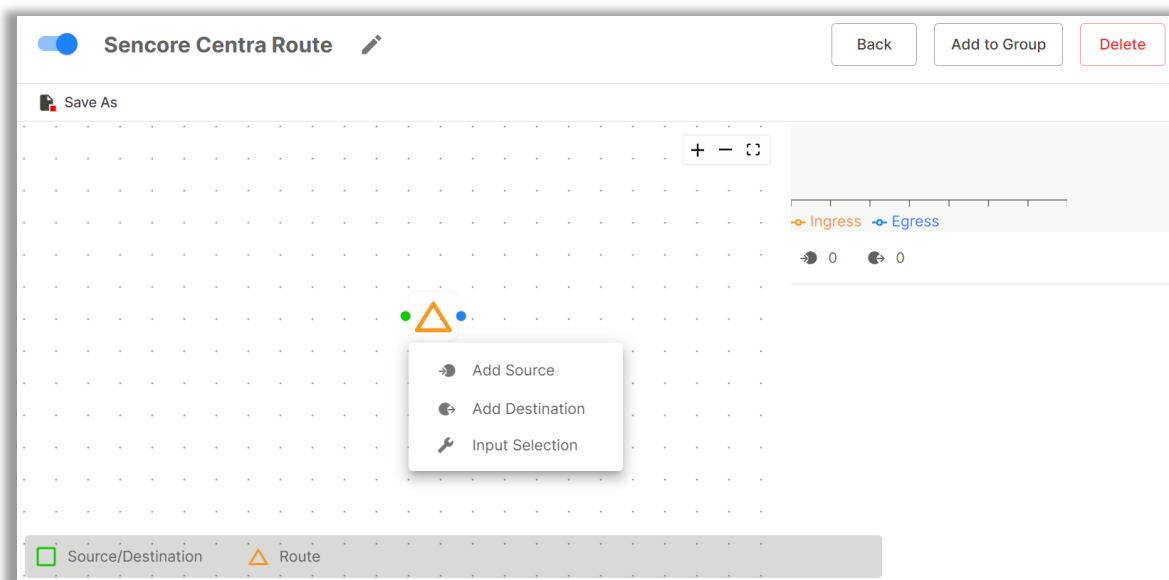
To create a new route, click on the “New Route” button in the upper right of the “Director” page. After entering the label for the route and clicking “Create Route”, the Director-level menu for the route will be opened automatically.



Add Route Button




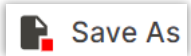


New Route Window



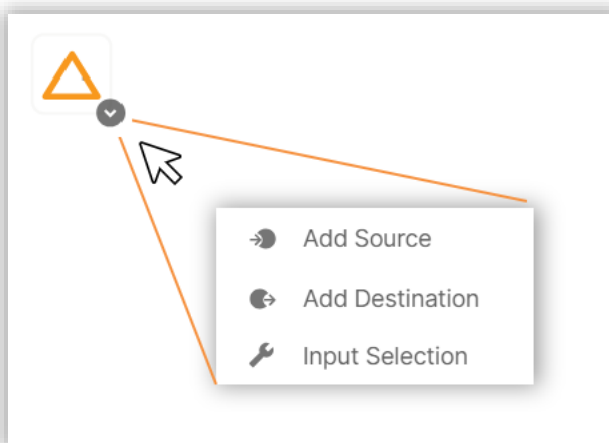
Route Example

Route Icons

Icon	Name	Description
	Route	This icon represents the focal point where sources enter, and destinations leave. The leftmost colored circle indicates source status, while the colored circle on the right indicates destination status
	Node Status Indicators	<i>Green</i> can indicate either an uncreated source or an existing source or destination that's free of errors. <i>Red</i> indicates an enabled source or destination in a failed state (unlocked signal or connection). <i>Blue</i> indicates that no destination is created. <i>Gray</i> indicates a disabled source or destination
	Source and Destination Nodes	Each square box represents a distinct source or destination and will be connected to the Route node. <i>Green</i> indicates an enabled and error-free Source or Destination. <i>Red</i> means the Source or Destination is enabled, but it is unlocked or disconnected. <i>Gray</i> indicates a disabled Source or Destination Node
	"Save As" icon	Use the "Save As" key to save the full route as a template. This is useful when configuring many similar routes. More information on Templates is available in Section 4.5 . Only ungrouped routes are eligible to be saved as Templates

4.4.1.1 Route Options

Upon creating a new route, the Route Dropdown Options will already be opened upon arrival (Add Source, Add Destination, Input Selection). To access the Route Dropdown Options outside of first time creation, hover over the route node to expose the gray dropdown arrow and then click the arrow to view the popout menu.

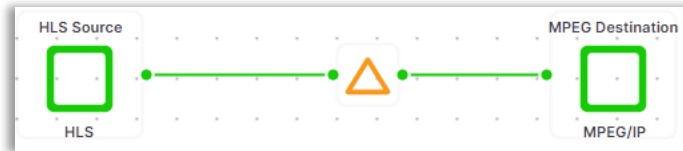


Route Dropdown Menu

Route Dropdown Options

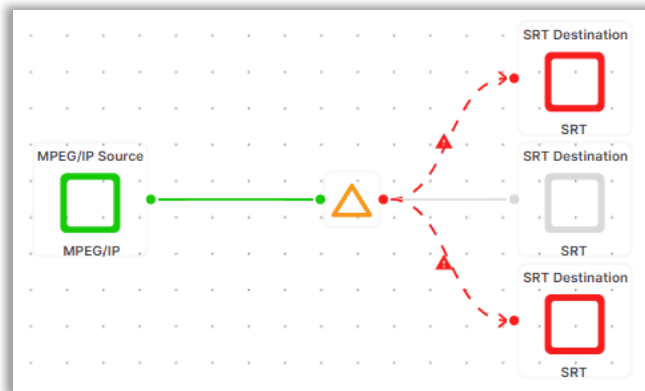
Option	Description
Add Source	Used to add Source Nodes to the Route; up to two distinct sources can be added to a Route (primary and backup). Information on Source Settings can be found in Section 4.3.2
Add Destination	Used to add Destination Nodes to the Route; many distinct destinations can be added to a Route. Information on Destination Settings can be found in Section 4.3.3
Input Selection	Once a backup source is added, this menu is used to configure failover and failback settings between the primary and backup inputs. Information on Primary and Backup Failover Options can be found in Section 4.3.2.7

After adding source and destination nodes, lines and status indicators will be added to the route to indicate connectivity pathing and overall condition. The left side of the route is reserved for sources while the right side of the route is used for destinations.



Route with Added Source and Destination Nodes

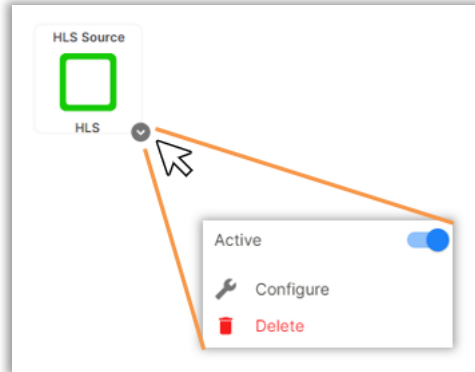
Line and status indicators will change depending upon configuration and status.



Route with Disabled and Disconnected Nodes

4.4.1.2 Destination and Source Options

To view the action options for a destination or source node, hover over the node to expose the gray dropdown arrow, and then click the arrow to expose the popout menu.



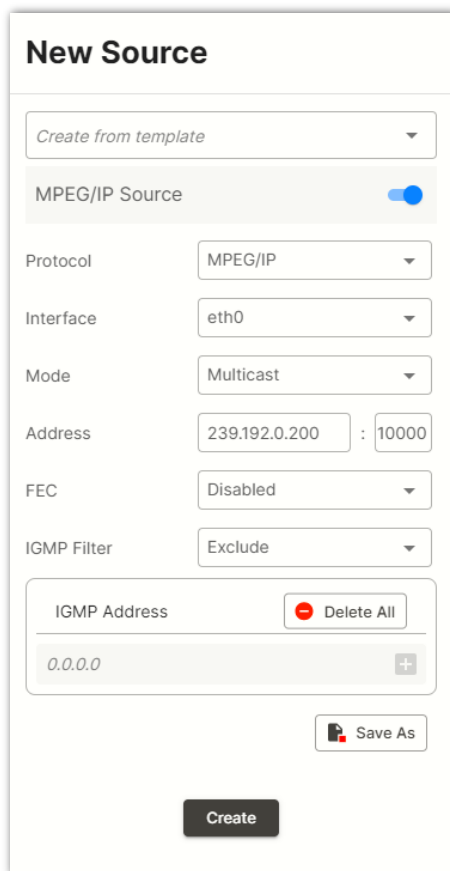
Node Action Menu

Node Dropdown Options

Option	Description
Active	Used to quickly enable and disable the source or destination node
Configure	Opens the source or destination settings, for use with Section 3.6.2 or Section 3.6.3
Delete	Removes the source or destination Node from the route

4.4.2 Source Node Settings

When adding or editing a source node using the Route Action Opens menu from [Section 4.3.1.1](#), the “New Source” or “Configure” option menu will be used to configure the receive properties of the input, such as interface, protocol, and address.



The "New Source" form contains the following fields and controls:

- Create from template**: A dropdown menu.
- MPEG/IP Source**: A toggle switch, currently turned on.
- Protocol**: A dropdown menu set to "MPEG/IP".
- Interface**: A dropdown menu set to "eth0".
- Mode**: A dropdown menu set to "Multicast".
- Address**: Two input fields containing "239.192.0.200" and "10000".
- FEC**: A dropdown menu set to "Disabled".
- IGMP Filter**: A dropdown menu set to "Exclude".
- IGMP Address**: A list with one entry "0.0.0.0" and a "Delete All" button.
- Save As**: A button with a floppy disk icon.
- Create**: A large button at the bottom.

Director Source Settings

The name/label of the node can be changed by clicking to the left of the  button.



This image shows a close-up of the node configuration bar. The text "MPEG/IP Source" is enclosed in an orange rectangular box, indicating it is the label that can be edited. To the right of the text is a blue toggle switch.

Name/Label Location

This menu is used to configure IP source settings for MPEG/IP, SRT, Zixi, HLS, Seamless RTP (SMPTE 2022-7 for Hitless Switching) and RIST inputs. Based upon the protocol selected, the available configuration settings will change. The next sections describe the available source options for each protocol.

4.4.2.1 MPEG/IP Source Settings

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

New Source

Create from template

MPEG/IP Source

Protocol

MPEG/IP

Interface

eth0

Mode

Multicast

Address

239.192.0.200

:

10000

FEC

Disabled

IGMP Filter

Exclude

IGMP Address

Delete All

0.0.0.0

+

Save As

Create

MPEG/IP Source Settings

Setting	Range	Description
Select Template	Dropdown of existing templates	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing multiple similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Mode	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
Address	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
Port	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
FEC	Enabled Disabled	Sets the port to accept FEC on the incoming MPEG/IP stream
IGMP Filter	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
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.2 SRT Source Settings

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

Configure

Create from template

SRT Source

Protocol

SRT

Interface

eth1

Call Mode

Caller

Remote Host

1.0.0.2

:

10000

Local Port Mode

Auto

Local Port

10000

Discovery Timeout (s)

3

Latency (ms)

20

Passphrase

.....

Save As

Update

SRT Source Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing multiple similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enable or disable the node
Call Mode	Caller Listener Rendezvous	Defines the ‘handshake’ mechanism to be used when establishing connection
Remote Host	xxx.xxx.xxx.xxx	Defines the IP address of the stream on the remote device
Port	0 – 65535	Defines the port of the stream on the remote devices
Local Port Mode	Auto Manual	In <i>Auto</i> mode, the local port number will be assigned automatically In <i>Manual</i> mode, the user will define the local port number
Local Port	1 – 65535	Defines the local port number
Discovery Timeout (seconds)	1 – 100, use 0 for infinite	Defines the length of time to wait for the stream to be discovered
Latency (ms)	1 – 8000	Defines buffer size in milliseconds
Passphrase	10 – 79 characters	Defines the encryption passphrase
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.3 **Zixi Source Settings**

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

Configure

Create from template

Zixi Source

Protocol

Zixi

Interface

eth0

Remote Host

:

2077

Alternate Remote Host

Stream ID

Remote ID

Password

Ignore TLS Certificate Error

Do Not Ignore

Maximum Latency (ms)

4000

Decryption Mode

Disabled

Decryption Key

.....

FEC Overhead (%)

30

Save As

Update

Zixi Source Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Remote Host	xxx.xxx.xxx.xxx	Defines the host of the remote broadcast using IP address or domain name
Port	0 – 65535	Defines the port of the stream on the remote device
Alternate Remote Host	xxx.xxx.xxx.xxx	Defines the alternate host of the remote broadcast using IP address or domain name
Stream ID	User entry	Defines the Zixi stream ID to be received
Remote ID	User entry	Specify the Zixi Broadcaster or Feeder ID that will push the stream
Password	User entry	Provides the password to allow specific Stream ID entered to be received
Ignore TLS Certificate Error	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
Maximum Latency (ms)	30 – 10,000	Defines the maximum latency or buffer size (in milliseconds)
Decryption Mode	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 Centra Gateway will automatically detect these
Decryption Key	User entry	Provides the key to allow signal processing if decryption is to be done
FEC Overhead (%)	0 – 50	Defines the amount of static overhead to be used to accommodate FEC

Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.4 **HLS Source Settings**

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

Configure

Create from template

HLS Source

Protocol

HLS

Interface

eth1

HLS Mode

Pull

HLS Network Location

Sencore

Apply and Refresh

Profile Name	Bandwidth(bps)
No rows	

Decryption Mode

Disabled

Decryption Key

.....

Discovery Timeout (s)

3

Save As

Update

HLS Source Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
HLS Mode	Push Pull	Determines if the HLS receives through a local or network location
HLS Network Location	User Entry	Defines address of the HLS stream to be received
Profile / Bandwidth	User Selected	After entering an HLS network location and clicking “Apply and Refresh”, a list of available profiles will be displayed
Decryption Mode	Disabled AES128	Defines if a decryption of the received signal is needed, AES 128 standard
Decryption Key	User Entry	Provides the key to allow signal processing if decryption is to be done
Discovery Timeout (seconds)	1 – 100 Use 0 for infinite	Defines the length of time to wait for the stream to be discovered
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.5 Seamless RTP Source Settings

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

Configure

Create from template

Seamless RTP Source

ProtocolSeamless RTP

Interfaceeth0

Address239.192.0.200 : 10000

IGMP FilterExclude

IGMP AddressDelete All

0.0.0.0

Interfaceeth0

Address239.192.0.200 : 10000

IGMP FilterExclude

IGMP AddressDelete All


0.0.0.0

Save As

Update

Seamless RTP Source Settings

Page 50 (158)



Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Address	xxx.xxx.xxx.xxx	Defines the address of the first or second path to be received
Port	1 - 65535	Defines the port of the first or second path to be received
Path 1 or Path 2 IGMP Filter	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
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 section to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.6 RIST Source Settings

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

Configure

Create from template

RIST Source

Protocol

RIST

Profile Mode

Simple

Latency (ms)

1000

Decryption Mode

Disabled

Passphrase

Seamless

Disabled

Seamless Buffer (ms)

450

Bonding

Disabled

Host/IP	Port	Interface	Mode	Backup
239.192.0.200	10000	eth0	Multicast	<div><input type="checkbox"/></div> <div></div>

Save As

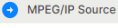
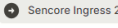
Update

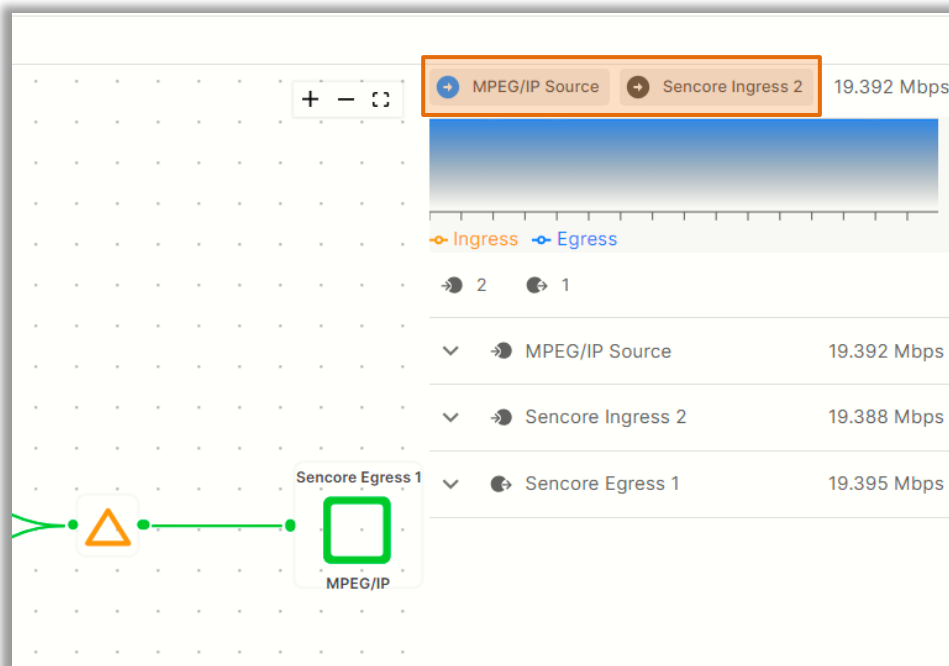
RIST Source Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Profile Mode	Simple Main	Specifies the RIST profile mode by which to receive the incoming stream
Latency (ms)	1 – 8000	Defines buffer size in milliseconds
Decryption Mode	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 Section 4.2.5.1
Passphrase	User entry	Provides the key to allow signal processing if <i>PSK</i> decryption is to be done
Seamless	Disabled Enabled	Allows user to enable seamless mode
Seamless Buffer	10 – 500	Set seamless buffer (ms)
Bonding	Disabled Enabled	Allows user to enable bonding mode
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.2.7 Primary and Backup Failover Options

Each route on the Centra can be configured for up to two source instances. The first is for the primary while the second is for backup. The primary and backup can be configured for automatic or manual failover. Only one of them may be assigned as the active source to the destination instances.

Use the Route Dropdown Opens menu from [Section 3.6.1.1](#) to add and configure the backup source with the “Add Source” key. In that same dropdown menu, the “Input Selection” options are used to determine which receive instance is the primary and backup as well as the failover options between them. This same menu can be opened by selecting the  button or  to quickly change the source input (note: blue shows active input).



Input Status

Input Failover

Active

+

Template 1

Primary

None

Backup

None

Switch

Manual Only

Restore


Manual Only

Switchover (Ms)

5000

Apply

Input Selection Menu

Setting	Range	Description
Active	N/A	Shows the current input in use. Use the  icon to switch the active input
Input	Receive 1 Receive 2	Used for both normal operation and input failover settings. During normal operation, this input will be the active input
Backup	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 Switch and Restore settings
Switch	Manual Only TS Sync Loss	Choose the event that triggers the switch from the primary to the backup input

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

4.4.3 Destination Node Settings

When adding or editing a destination node using the Route Action Opens menu from [Section 4.3.1.1](#), the “New Destination” or “Configure” option menu will be used to configure the transmit properties of the output, such as interface, protocol, and address.

New Destination

Create from template

MPEG Destination

Protocol

MPEG/IP

Interface

eth0

Destination

239.192.0.201

:

10000

Source IP Mode

Auto

Source IP

0.0.0.0

:

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

Save As

Create

Director Destination Settings

The name/label of the node can be changed by clicking to the left of the  button.



Name/Label Location

This menu is used to configure IP source settings for MPEG/IP, SRT, Zixi, and RIST outputs. Based upon the protocol selected, the available configuration settings will change. The next sections describe the available source options for each protocol.

4.4.3.1 MPEG/IP Destination Settings

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

New Destination

Create from template

MPEG Destination

Protocol

MPEG/IP

Interface

eth0

Destination

239.192.0.201

:

10000

Source IP Mode

Auto

Source IP

0.0.0.0

:

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

Save As

Create

MPEG/IP Destination Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates

On/Off Toggle	On Off	Enables or disables the node
Destination	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
:Port	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
Source IP Mode	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
Source IP	xxx.xxx.xxx.xxx	Defines the Source IP address to be assigned to the output stream
Port	0 – 65535	Defines the source IP port to be assigned to the output stream
Source MAC Mode	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
Source MAC	xx:xx:xx:xx:xx:xx	The user defined MAC for when using <i>Manual</i> MAC Mode
TS Packets Mode	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
TS Packets Per IP Packet	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
Encapsulation	UDP RTP	Sets the Encapsulation to UDP or RTP

Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.3.2 SRT Destination Settings

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

New Destination

Create from template

SRT Destination

Protocol

SRT

Interface

eth0

Call Mode

Caller

Remote Host

1.0.0.2

:

10000

Local Port Mode

Auto

Local Port

10000

Discovery Timeout (s)

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

.....

Save As

Create

SRT Destination Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Call Mode	Caller Listener Rendezvous	Defines the ‘handshake’ mechanism to be used when establishing connection
Remote Host	xxx.xxx.xxx.xxx	Defines the IP address of the stream on the remote device
Port	0 – 65535	Defines the port of the stream on the remote devices
Local Port Mode	Auto Manual	In <i>Auto</i> mode, the local port number will be assigned automatically In <i>Manual</i> mode, the user will define the local port number
Local Port	1 – 65535	Defines the local port number
Discovery Timeout (seconds)	1 – 100, use 0 for infinite	Defines the length of time to wait for the stream to be discovered
Latency (ms)	1 – 8000	Defines buffer size in milliseconds
Bandwidth Overhead (%)	0 – 50	Defines the amount of bandwidth overhead to allow for
TS Packets Mode	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
TS Packets Per SRT Packet	1 – 7	Defines the number of TS packets per SRT packet when mode is <i>Manual</i>
Time To Live (hops)	1 – 254	Defines the number of network devices the transmission is allowed to pass through

Type of Service	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
Encryption Mode	Disabled AES-128 AES-256	Defines which encryption standard to use or if the Centra Gateway will automatically detect this
Passphrase	10 – 79 characters	Defines the encryption passphrase
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.3.3 Zixi Destination Settings

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

Configure

Create from template

Zixi Destination

Protocol

Zixi

Interface

eth0

Remote Host

:

2088

Alternate Remote Host

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

Save As

Update

Zixi Destination Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Remote Host	xxx.xxx.xxx.xxx Domain Name	Defines the host of the remote broadcast using an IP address or domain name
Alternate Remote Host	xxx.xxx.xxx.xxx Domain Name	Defines the alternate host of the remote broadcast using an IP address or domain name
Remote Port	0 – 65535	Defines the port of the stream on the remote device
Stream ID	User entry	Defines the Zixi stream ID to be transmitted
Password	User entry	Provides the password to allow specific Stream ID entered to be received
Ignore TLS Certificate Error	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
Maximum Latency (ms)	30 – 10,000	Defines the maximum latency or buffer size (in milliseconds)
Encryption Mode	Disabled, AES-128, AES-192, AES-256, Automatic	Defines which encryption standard to use or if the Centra Gateway will automatically detect this
Encryption Key	User entry	The key to be used by downstream decryption devices
FEC Overhead (%)	0 – 50	Defines the amount of static overhead to be used to accommodate FEC
TS Packets Mode	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
TS Packets per Zixi Packet	1 – 7	User defined value for when <i>Manual</i> mode is enabled

Bonding Mode	Disabled	Specifies which interfaces, if any, are to be set to bonding mode
	All interfaces	
	One Interface	
	Any Interface	
Interface Bonding Box	Available for One Interface Mode	Allows user to define parameters and details about the port(s) when bonding
	Any Interface Mode	
Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.3.4 RIST Destination Settings

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

Configure

Create from template

RIST Destination

Protocol

RIST

Profile Mode

Simple

Tunneling Mode

Full Datagram

Maximum Latency (ms)

1000

Encryption Mode

Disabled

Passphrase

.....

Ignore TLS Certificate Error

Do Not Ignore

Seamless

Disabled

Bonding

Disabled

Dest Host/IP	Dest Port	Source Port	Interface	Bandwidth Limit (Mbps)	Backup
239.192.0.200	10000	3020	eth0	100	<div><div></div><div></div></div>

Save As

Update

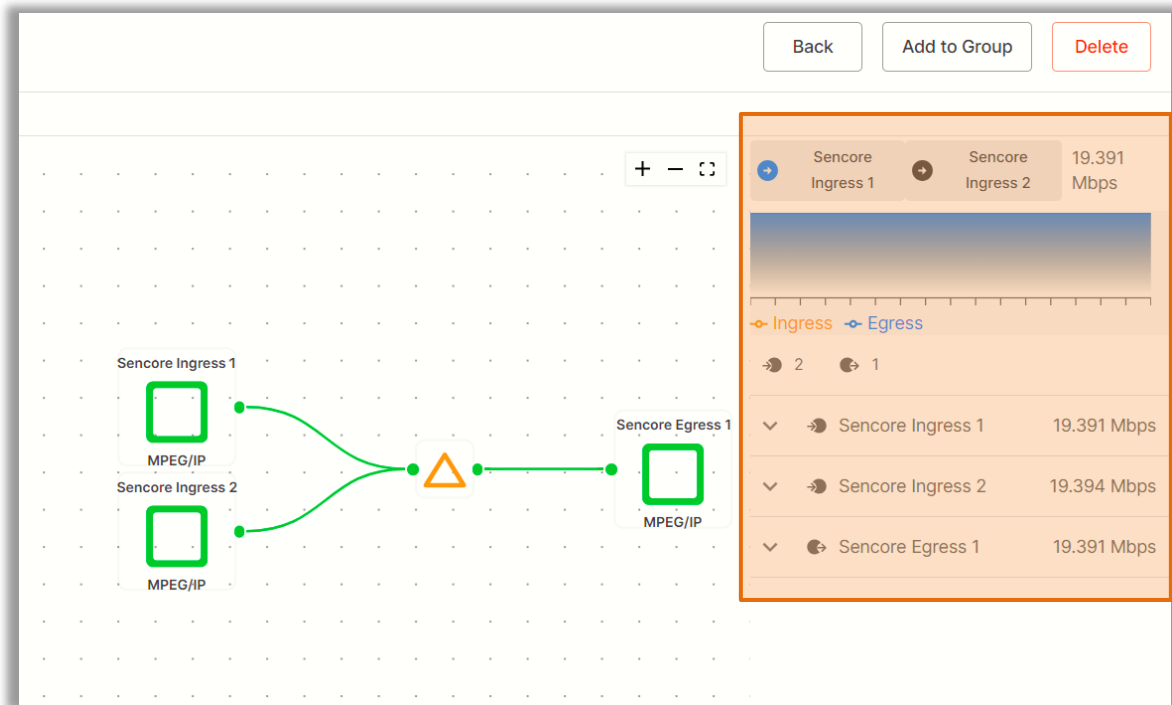
RIST Destination Settings

Setting	Range	Description
Select Template	0 – Many	Applies a copy of saved settings utilizing a template for reference. This can save time when creating or editing many similar flows. See Section 3.8 section for more information on templates
On/Off Toggle	On Off	Enables or disables the node
Profile Mode	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
Tunneling Mode	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
Latency (ms)	1 – 8000	Specifies buffer size in milliseconds
Encryption Mode	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 Section 4.2.5.1
Passphrase	User entry	The encryption passphrase. Exclusive to <i>PSK</i> Encryption Mode
Ignore TLS Certificate Error	Do Not Ignore Ignore	Defines whether to cease or continue processing if TLS Certificate Error is signaled
Seamless	Disabled Enabled	Allows user to enable seamless mode
Bonding	Disabled Enabled	Allows user to enable bonding mode

Save as	N/A	Saves a copy of the configuration as a template. See Section 3.8 to view templates
Create/Update	N/A	Create saves the initial configuration. Update applies the changes made

4.4.4 Route Statistics and Telemetry

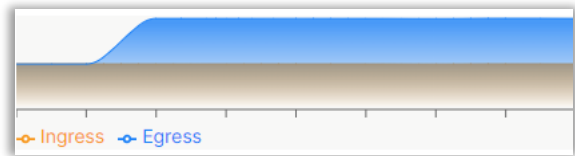
To view route telemetry data, under the Director page, enter a route or group. The menu on the right side of the page is the default view for telemetry data.






Default Route Statistics Page


The active and inactive source buttons, Sencore Ingress 1 Sencore Ingress 2 , show which input is being used. The blue icon shows the active input, the grey icon shows the inactive input. Selecting the active input will bring up the failover menu and clicking the black icon will switch the input (see [Section 4.3.2.7](#) for more details on the failover menu).

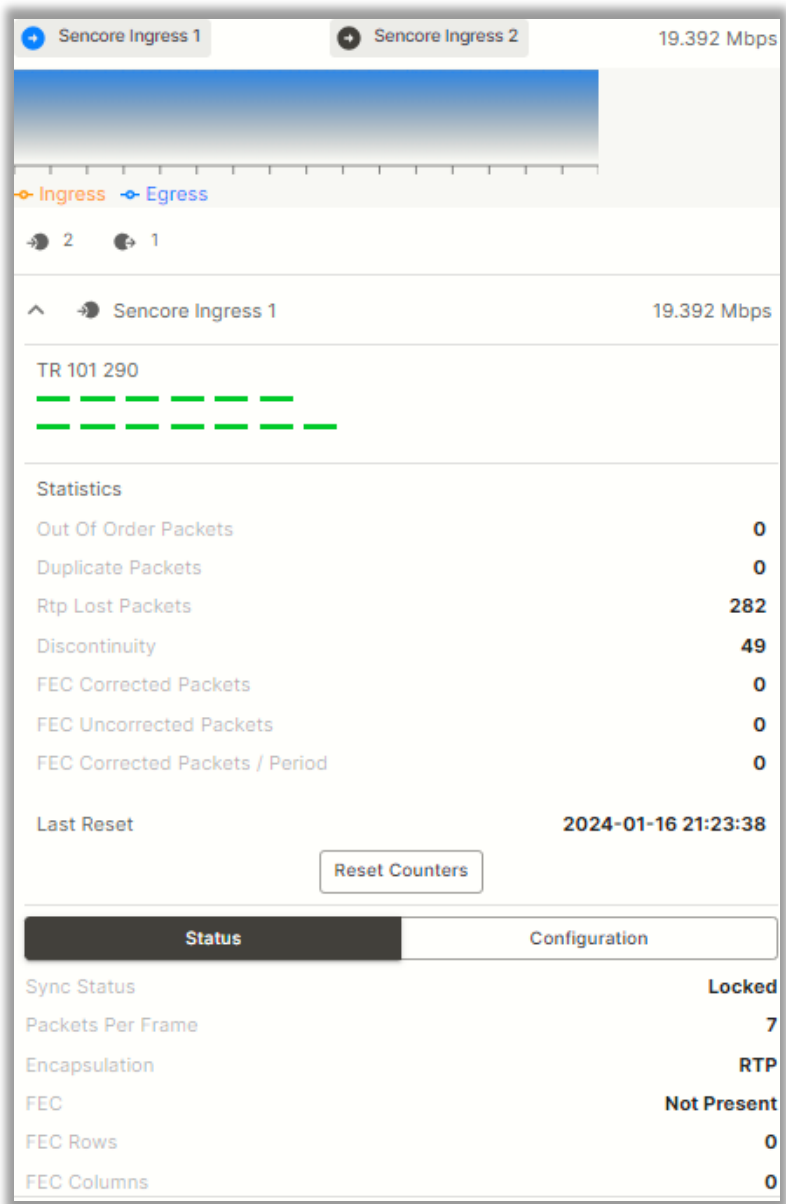
The bitrate chart shows aggregate flow rate for the active source and all destinations.



Bitrate Chart

The source/destination:  icons show the total number of source and destination nodes. The  is the source icon. The  icon is for the destination. dropdown options for source/destination nodes.

To view additional telemetry data, click on dropdown  for the given source or destination or the node itself.



Source Input Dropdown

If the source or destination is being monitored by an Analyze instance, the 101 290 statuses will be available here (see [Section 4.4](#) for more details):



101 290 Statuses

‘Statistics’ will encompass detailed IP layer information for the source or destination. Please note that this section is not present on destination nodes.

Statistics	
Out Of Order Packets	0
Duplicate Packets	0
Rtp Lost Packets	283
Discontinuity	49
FEC Corrected Packets	0
FEC Uncorrected Packets	0
FEC Corrected Packets / Period	0
Last Reset	2024-01-17 18:41:37
<button>Reset Counters</button>	

Statistics Section

For all types of IP, the Reset Counters button will reset all counts to 0.

Below Statistics, the ‘Status’ tab provides general info on the IP, such as encapsulation type and sync status

.

Status	Configuration
Sync Status	Locked
Packets Per Frame	7
Encapsulation	RTP
FEC	Not Present
FEC Rows	0
FEC Columns	0

Status Tab

The 'Configuration' tab provides a surface level view of the applied node settings, (for additional configuration information on the given node, see [Section 4.3.2](#) for Source Settings and [Section 4.3.3](#) for Destination Settings).

Status	Configuration
Mode	MULTICAST
Address	239.192.1.40
Port	1040
FEC	DISABLED
IGMP Mode	EXCLUDE
<div>IGMP Filter List</div> <div>Unsolicited IGMP Report</div>	

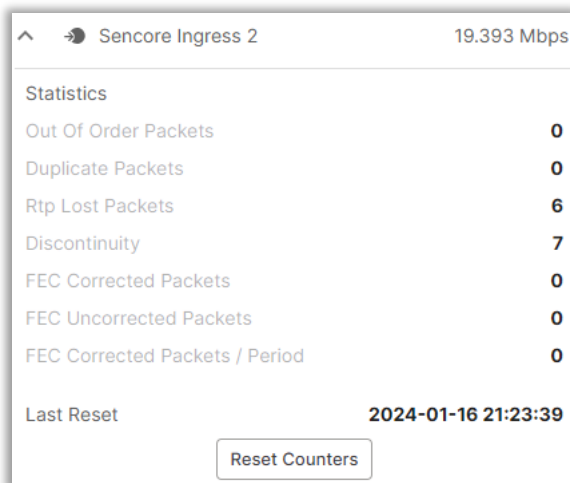
Configuration Tab

Depending on the IP protocol for the given source or destination, the statistics and status information will vary. The next sections describe the telemetry info for each protocol on the input and output sides.

4.4.4.1 MPEG/IP Telemetry Information

Use the information from [Section 4.4.4](#) to access the status and statistics for MPEG/IP sources and destinations.

MPEG/IP Source Statistics View:



MPEG/IP Source Statistics

Setting	Description
Out of Order Packets	Count of packets received, but in mismatched order
Duplicate Packets	Count of packets received more than once
Rtp Lost Packets	Count of packets not received
Discontinuity	Number of RTP Sequence errors
FEC Corrected Packets	Packets that have been recovered by Forward Error Correction
FEC Uncorrected Packets	Packets that could not be recovered by Forward Error Correction
FEC Corrected Packets / Period	Rate of correctable FEC errors per second

MPEG/IP Source Status View:

Status	Configuration
Sync Status	Locked
Packets Per Frame	7
Encapsulation	RTP
FEC	Not Present
FEC Rows	0
FEC Columns	0

MPEG/IP Source Status Tab


Setting	Range	Description
Sync Status	Locked, Unlocked	Detection of TS Sync
Packets per Frame	1 to 7	Number of TS Packets per IP Packet
Encapsulation	UDP or RTP	Detected IP Headers
FEC	Present, Not Present	Number of RTP Sequence errors
FEC Rows	0 to 10	Number of detected FEC Rows, will be 0 if "Not Present"
FEC Columns	0 to 10	Number of detected FEC Columns, will be 0 if "Not Present"

MPEG/IP Source Configuration Tab:

See [Section 4.4.2.1](#) for more information on node configuration settings.

Status	Configuration
Mode	MULTICAST
Address	239.192.1.50
Port	1050
FEC	DISABLED
IGMP Mode	EXCLUDE
<div>IGMP Filter List</div> <div>Unsolicited IGMP Report</div>	

MPEG/IP Source Configuration Tab

The  button will send an unsolicited IGMP report to force a join operation for each IP stream to be received.

MPEG/IP Destination Statistics View:

No statistics available or necessary for MPEG/IP destination nodes.

For MPEG/IP Destination Status:

Status	Configuration
Source IP	0.0.0.0
Source MAC	00:01:2E:96:6D:CB
Mode	MULTICAST
Receiver MAC	N/A

MPEG/IP Destination Status Tab

Setting	Range	Description
Source IP	xxx.xxx.xxx	IP address assigned to send from
Source MAC	xx:xx:xx:xx:xx:xx	MAC (media access control) address assigned to send from
Mode	MULTICAST or UNICAST	Selected IP send type
Receiver MAC	xx:xx:xx:xx:xx:xx	MAC (media access control) address assigned to send to

MPEG/IP Destination Configuration:

See [Section 4.4.3.1](#) for more information on node configuration settings.

Status	Configuration
Source IP Mode	AUTO
Source Port	3020
Source MAC Mode	AUTO
TS Packets Mode	AUTO
TS Packets	7

MPEG/IP Destination Configuration Tab

4.4.4.2 SRT Telemetry Information

Use the information from [Section 4.4.4](#) to access the status and statistics for SRT sources and destinations.

SRT Source Statistics View:

Statistics	
Reconnections	0
Received Packets	0
Received Bytes	0 Bytes
Lost Packets	0
Uncorrected Packets	0
Recovered Packets	0
SRT NAKs	0

SRT Source Statistics

Setting	Description
Reconnections	Number of reconnections since the stream started
Received Packets	Number of UDP packets received for that stream
Received Bytes	Number of bytes received for that stream
Lost Packets	Count of packets not received
Uncorrected Packets	Packets that could not be corrected
Recovered Packets	Packets that have been recovered
SRT NAKs	Total number of negative acknowledgment packets received from the destination device

SRT Source Status View:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Local Port	10000
Encryption Mode	DISABLED
Decryption State	UNSECURED
Round Trip Time (ms)	0
Buffer Size (ms)	0
Latency (ms)	20
Link Bandwidth	0.000 Mbps
TS Packets Per SRT Packet	0

SRT Source Status Tab

Setting	Range	Description
Connection State	VALID or INVALID	Link is working or link has failed
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Local Port	1 – 65535	Port to receive from
Encryption Mode	DISABLED or ENABLED	Whether the AES encryption is being used
Decryption State	SECURED or UNSECURED	Whether the connection is secure or not
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again
Buffer Size (ms)	0 - ∞	Contains stream packets received and waiting to be forwarded or decoded
Latency (ms)	0 - ∞	The maximum buffer size available for managing SRT packets

Link Bandwidth	0 - ∞	Estimated maximum bandwidth available as viewed from the destination device
TS Packets Per SRT Packet	1 to 7	Number of TS packets inside of an SRT packet

SRT Source Configuration Tab:

See [Section 4.4.2.2](#) for more information on node configuration settings.

Status	Configuration
Discovery Timeout (seconds)	3000
Call Mode	CALLER

SRT Source Configuration Tab

SRT Destination Statistics:

Statistics	
Reconnections	0
Sent Packets	0
Sent Bytes	0 Bytes
Resent Packets	0
Resent Bytes	0 Bytes
Lost Packets	0
SRT NAKs	0

SRT Destination Status Tab

Setting	Range	Description
Reconnections	0 -∞	Number of reconnections since the stream started
Sent Packets	0 -∞	Count of packets that have been sent
Sent Bytes	0 -∞	Count of bytes that have been emitted
Resent Packets	0 -∞	Count of packets that have re-emitted
Resent Bytes	0 -∞	Count of bytes that have re-emitted
Lost Packets	0 -∞	Count of packets not received
SRT NAKs	0 -∞	Total number of negative acknowledgment packets received from the destination device

SRT Destination Status View:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Local Port	10000
Encryption Mode	DISABLED
Remote Decryption State	UNSECURED
Round Trip Time (ms)	0
Buffer Size (ms)	0
Latency (ms)	125
Maximum Bandwidth	0.000 Mbps
Path Maximum Bandwidth	0.000 Mbps

SRT Destination Configuration Tab

Setting	Range	Description
Connection State	VALID or INVALID	Link is working or link has failed
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Local Port	1 – 65535	Port to send from
Encryption Mode	DISABLED or ENABLED	Whether the AES encryption is being used
Decryption State	SECURED or UNSECURED	Whether the connection is secure or not
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again
Buffer Size (ms)	0 - ∞	Contains stream packets received and waiting to be forwarded or decoded
Latency (ms)	0 - ∞	The maximum buffer size available for managing SRT packets
Maximum Bandwidth	0 - ∞	Maximum bandwidth used by the source device for this SRT stream
Path Max Bandwidth	0 - ∞	The destination device sends the value to the source device with an acknowledgment packet

SRT Destination Configuration:

See [Section 4.4.3.2](#) for more information on node configuration settings.

Status	Configuration
Discovery Timeout (seconds)	3000
Call Mode	CALLER
Bandwidth Overhead (%)	25
TS Packets Mode	AUTO
TS Packets	7
Time To Live (hops)	64
Type Of Service	0
Encryption Mode	DISABLED

SRT Destination Configuration Tab

4.4.4.3 Zixi Telemetry Information

Use the information from [Section 4.4.4](#) to access the status and statistics for Zixi sources and destinations.

Zixi Source Statistics View:

Statistics	
Reconnections	0
Received Packets	0
Received Bytes	0 Bytes
Dropped Packets	0
Not Recovered Packets	0
FEC Packets	0
FEC Recovered Packets	0
ARQ Packets	0
ARQ Recovered Packets	0
ARQ Duplicate Packets	0
ARQ Requests	0

Zixi Source Statistics

Setting	Description
Reconnections	Number of reconnections since the stream started
Received Packets	Number of UDP packets accepted for that stream
Received Bytes	Number of bytes accepted for that stream
Dropped Packets	Count of packets not received
Not Recovered Packets	Packets that have been recovered
FEC Packets	Count of total Forward Error Correction packet
FEC Recovered Packets	Packets that have been recovered by Forward Error Correction
ARQ Packets	Count of Automatic Repeat Request packets
ARQ Recovered Packets	Displays the number of dropped packets recovered via ARQ
ARQ Duplicate Packets	Displays the number of duplicate recovery packets received via ARQ
ARQ Requests	Displays the number of requests for retransmission of dropped packets made with ARQ

Zixi Source Status View:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Decryption State	UNSECURED
Round Trip Time (ms)	0
Jitter (ms)	0
TS Packets Per Zixi Packet	0

Zixi Source Status Tab

Setting	Range	Description
Connection State	INVALID or VALID	Detection of TS Connection
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Decryption State	Secured or unsecure	Shows whether the connection is encrypted
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again
Jitter (ms)	0 - ∞	The length of time the stream is actively streaming
TS Packets Per Zixi Packet	0 to 7	Number of TS packets contained in a Zixi Packet

Zixi Source Configuration Tab:

See [Section 4.4.2.3](#) for more information on node configuration settings.

Status	Configuration
Password	
Ignore TLS Certificate Error	DO_NOT_IGNORE
Maximum Latency (ms)	4000
Decryption Mode	DISABLED
FEC Overhead (%)	30

Zixi Source Configuration Tab

Zixi Destination Statistics View:

Statistics	
Reconnections	0
Sent Packets	0
Sent Bytes	0 Bytes
Dropped Packets	0
Not Recovered Packets	0
FEC Packets	0
FEC Recovered Packets	0
ARQ Packets	0
ARQ Recovered Packets	0
ARQ Duplicate Packets	0
ARQ Requests	0

Zixi Destination Statistics View

Setting	Description
Reconnections	Number of reconnections since the stream started
Sent Packets	Number of UDP packets emitted for that stream
Sent Bytes	Number of bytes emitted for that stream
Dropped Packets	Count of packets not received
Not Recovered Packets	Packets that have been recovered
FEC Packets	Count of total Forward Error Correction packets
FEC Recovered Packets	Packets that have been recovered by Forward Error Correction
ARQ Packets	Count of Automatic Repeat Request packets
ARQ Recovered Packets	Displays the number of dropped packets recovered via ARQ
ARQ Duplicate Packets	Displays the number of duplicate recovery packets received via ARQ.
ARQ Requests	Displays the number of requests for retransmission of dropped packets made with ARQ

Zixi Destination Status:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Round Trip Time (ms)	0
Jitter (ms)	0

Zixi Destination Status Tab

Setting	Range	Description
Connection State	INVALID or VALID	Detection of TS Connection
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again
Jitter (ms)	0 - ∞	The length of time the stream is actively streaming

Zixi Destination Configuration:

See [Section 4.4.3.3](#) for more information on node configuration settings.

Status	Configuration
Password	
Ignore TLS Certificate Error	DO_NOT_IGNORE
Maximum Latency (ms)	4000
Decryption Mode	DISABLED
Maximum Bitrate	8000000
FEC Overhead (%)	30
TS Packets Mode	AUTO
TS Packets	7
Bonding Mode	DISABLED

Zixi Destination Configuration Tab

4.4.4.4 RIST Telemetry Information

Use the information from [Section 4.4.4](#) to access the status and statistics for RIST sources and destinations.

RIST Source Statistics View:

Statistics

Reconnections

0

Received Packets

0

Received Bytes

0 Bytes

Lost Packets

0

RTCP NAKs

0

RTCP Recovered Packets

0

Last Reset

2024-01-19 15:37:22

Reset Counters

Link 1 Link Bandwidth

0.000 Mbps

Link 1 Received Packets

0

Link 1 Received Bytes

0 Bytes

Link 1 Last Reset

2024-01-19 15:37:22

Reset Link 1 Counters

RIST Source Statistics

Setting	Description
Reconnections	Number of reconnections since the stream started
Received Packets	Number of UDP packets accepted for that stream
Received Bytes	Number of bytes accepted for that stream
Lost Packets	Count of packets not received
RTCP NAKs	Total number of negative acknowledgment packets received from the destination device
RTCP Recovered Packets	Number of packets that have been corrected
Link # Link Bandwidth	Estimated maximum bandwidth available as viewed from the destination device
Link # Received Packets	Number of packets accepted for that link
Link # Received Bytes	Number of bytes accepted for that stream
Link # Last Reset	The date of last reset for that link

RIST Source Status View:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Decryption State	UNSECURED
Round Trip Time (ms)	0
Buffer Size (ms)	0
Jitter (ms)	0
Latency (ms)	0
Link Bandwidth	0.000 Mbps
Link 1 Connection State	DISABLED
Link 1 Up Time	00:00:00:00

RIST Source Status Tab

Setting	Range	Description
Connection State	VALID or INVALID	Link is working or link has failed
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Local Port	1 – 65535	Port to receive from
Encryption Mode	DISABLED or ENABLED	Whether the AES encryption is being used
Decryption State	SECURED or UNSECURED	Whether the connection is secure or not
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again
Buffer Size (ms)	0 - ∞	Contains stream packets received and waiting to be forwarded or decoded
Jitter (ms)	0 - ∞	The length of time the stream is actively streaming
Latency (ms)	0 - ∞	The maximum buffer size available for managing RIST packets
Link Bandwidth	0 - ∞	Estimated maximum bandwidth available as viewed from the destination device

Link # Connection State	ENABLED or DISABLED	Link is on or off
Link # Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming

RIST Source Configuration Tab:

See [Section 4.4.2.6](#) for more information on node configuration settings.

Status	Configuration
Profile Mode	SIMPLE
Latency (ms)	1000
Decryption Mode	DISABLED
Seamless	DISABLED
Seamless Buffer (ms)	450
Bonding	DISABLED

RIST Source Configuration Tab

RIST Destination Statistics View:

Statistics

Reconnections

0

Sent Packets

0

Sent Bytes

0 Bytes

Resent Packets

0

Resent Bytes

0 Bytes

Lost Packets

0

RTCP NAKs

0

Last Reset

2024-01-19 16:04:11

Reset Counters

Link 1 Link Bandwidth

0.000 Mbps

Link 1 Sent Packets

0

Link 1 Sent Bytes

0 Bytes

Link 1 Last Reset

2024-01-19 16:04:11

Reset Link 1 Counters

RIST Destination Statistics Tab

Setting	Description
Reconnections	Number of reconnections since the stream started
Sent Packets	Number of UDP packets accepted for that stream
Sent Bytes	Number of bytes accepted for that stream
Resent Packets	Count of packets not re-emitted
Resent Bytes	Count of bytes not re-emitted
Lost Packets	Count of packets not received at destination
RTCP NAKs	Total number of negative acknowledgment packets received from the destination device
Link # Link Bandwidth	Estimated maximum bandwidth available as viewed from the destination device
Link # Sent Packets	Number of packets emitted for that link
Link # Sent Bytes	Number of bytes emitted for that stream
Link # Last Reset	The date of last reset for that link

RIST Destination Status:

Status	Configuration
Connection State	INVALID
Up Time	00:00:00:00
Round Trip Time (ms)	0
Buffer Size (ms)	0
Jitter (ms)	0
Latency (ms)	0
Link Bandwidth	0.000 Mbps
Link 1 Connection State	DISABLED
Link 1 Up Time	00:00:00:00

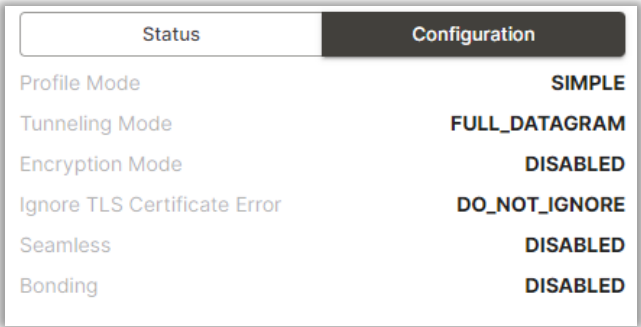
RIST Destination Status Tab

Setting	Range	Description
Connection State	VALID or INVALID	Link is working or link has failed
Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming
Local Port	1 – 65535	Port to send from
Encryption Mode	DISABLED or ENABLED	Whether the AES encryption is being used
Decryption State	SECURED or UNSECURED	Whether the connection is secure or not
Round Trip Time (ms)	0 - ∞	The time it takes for a packet to travel from a source to a destination and back again.
Buffer Size (ms)	0 - ∞	Contains stream packets received and waiting to be forwarded or decoded.
Jitter (ms)	0 - ∞	The length of time the stream is actively streaming
Latency (ms)	0 - ∞	The maximum buffer size available for managing RIST packets
Link Bandwidth	0 - ∞	Estimated maximum bandwidth available as viewed from the destination device

Link # Connection State	ENABLED or DISABLED	Link is on or off
Link # Up Time	xx:xx:xx:xx	The length of time the stream is actively streaming

RIST Destination Configuration:

See [Section 4.4.3.4](#) for more information on node configuration settings.



RIST Destination Configuration Tab

4.4.4.5 HLS Source Telemetry

The HLS source node does not contain any statistics. The status and configuration tabs are available for this node.

Status: Encryption mode (DISABLED or ENABLED)

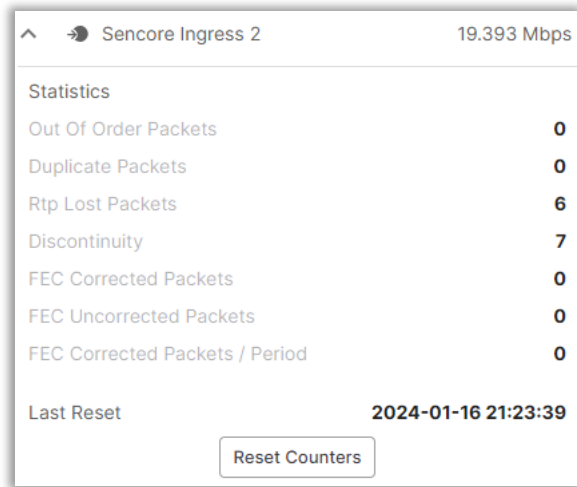
Configuration: Profile, Discovery timeout [in seconds] (0 - ∞)

For more information on HLS Settings, please view [Section 4.4.2.4](#).

4.4.4.6 Seamless RTP Source Telemetry

Use the information from [Section 4.4.4](#) to access the status and statistics for MPEG/IP sources and destinations.

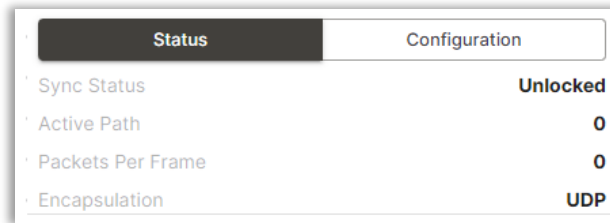
Seamless RTP Source Statistics View:



Seamless RTP Source Statistics

Setting	Description
Out of Order Packets 1 / 2	Count of packets received, but in mismatched order
Duplicate Packets 1 / 2	Count of packets received more than once
Rtp Lost Packets 1 / 2	Count of packets not received
Discontinuity 1 / 2	Number of RTP Sequence errors
Last Reset 1 / 2	Shows the last time the specific connection count has been reset

Seamless RTP Source Status View:



Seamless RTP Source Status Tab


Setting	Range	Description
Sync Status	Locked, Unlocked	Detection of TS Sync
Active Path	1 or 2	Which path is currently being used
Packets Per Frame	1 to 7	Number of TS Packets for each frame
Encapsulation	UDP or RTP	Type of IP header

Seamless RTP Source Configuration Tab:

See [Section 4.4.2.5](#) for more information on node configuration settings.

Status	Configuration
Physical Connector 1	eth0
IGMP Mode 1	EXCLUDE
Physical Connector 2	eth0
IGMP Mode 2	EXCLUDE
Path 1 IGMP Filter List	
Path 2 IGMP Filter List	
Unsolicited IGMP Report	

Seamless RTP Source Configuration Tab

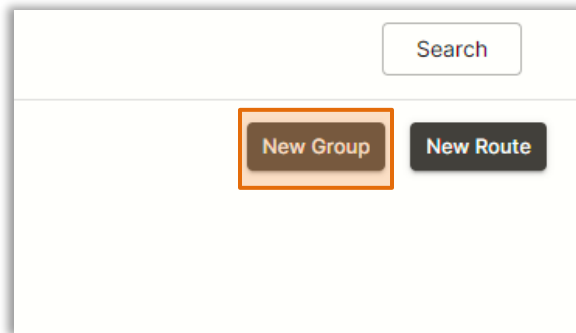
The  button will send an unsolicited IGMP report to force a join operation for each IP stream to be received.

Seamless RTP Destination Statistics:

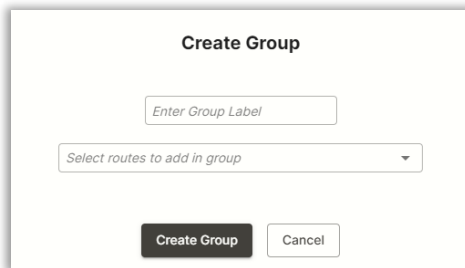
No statistics, status or configuration available or necessary for Seamless RTP destination nodes.

4.4.5 Groups

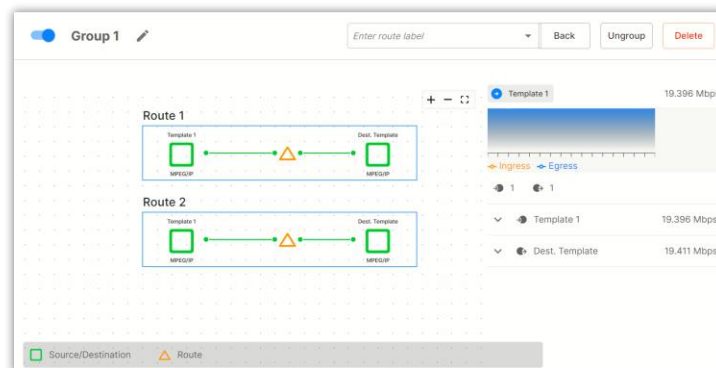
A group is a collection of routes. Categorize routes for easier management. To create a new group, click on the 'New Group' button at the top right of the Director panel. This configuration window is used to label the new group and add any previously created routes to the new group. It is not mandatory to have a pre-existing route to create a new group. A route can only be added to one group at a time.



New Group Button

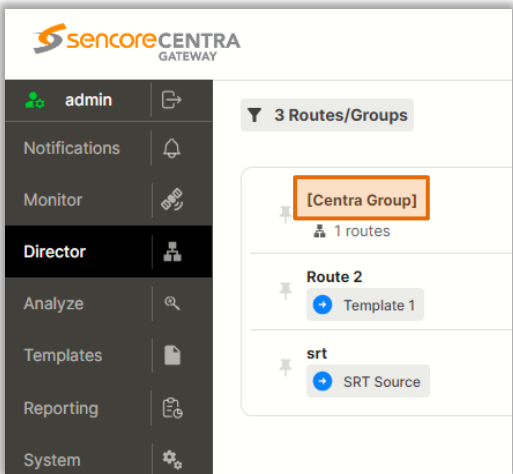


Create Group Window



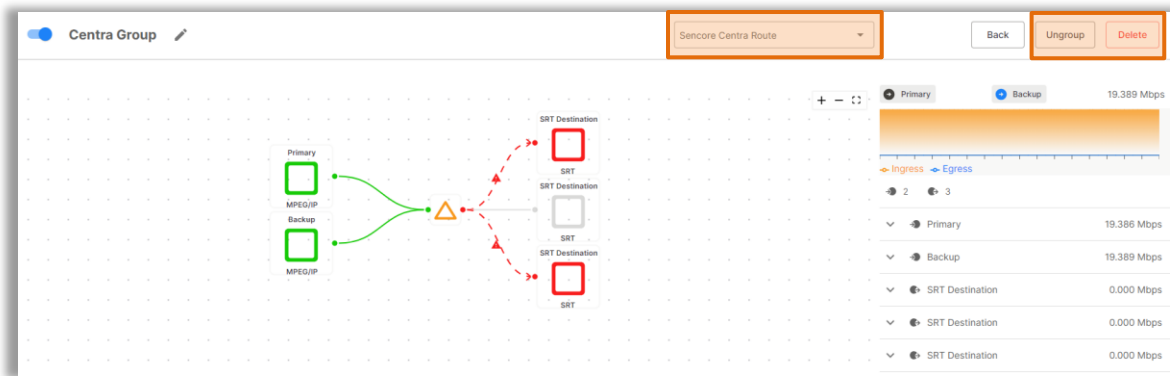
Group Example

On the Director tab, Groups are shown with [] around the group name. The example below shows how groups are displayed.

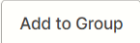


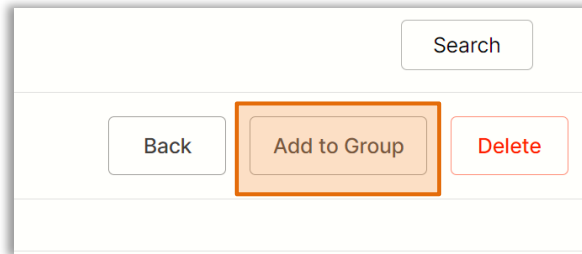
Created Group

After entering a group, select the dropdown, , to filter routes inside of a group. To remove a route from the group, click the button and select the routes to remove. Removing all routes will result in deletion of the group. Selecting the button will ungroup all associated routes and delete the group.

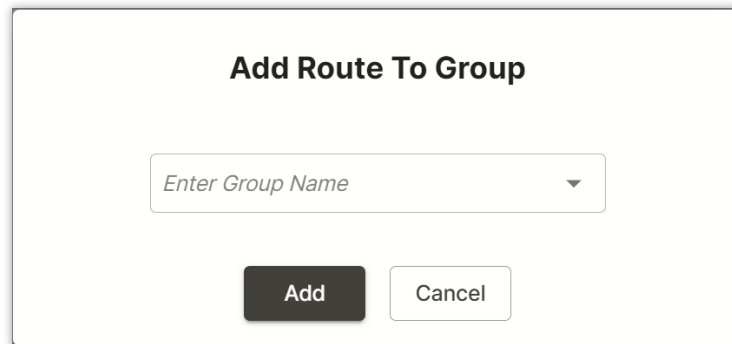


Group Navigation Icons

To add a route to an existing group, first select the route from the Director panel, then click the  button.



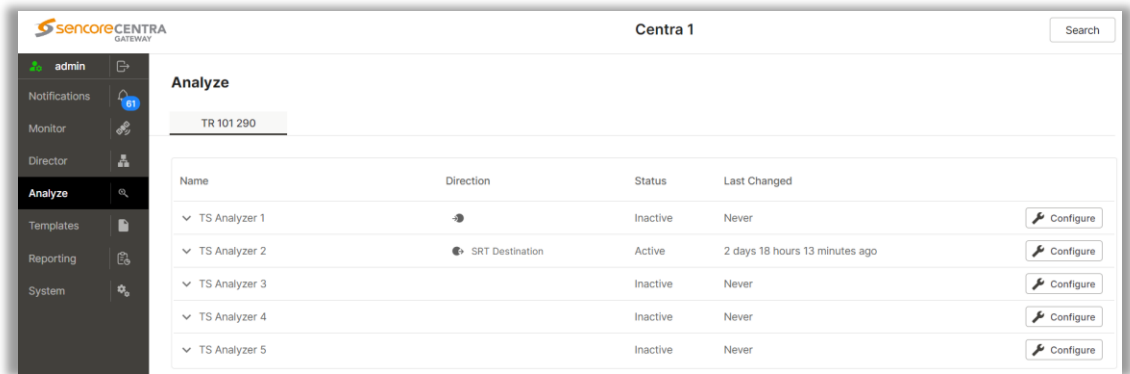
Add to Group Button



Add to Group Window

4.5 Analyze

To access the Analyze Control Panel, click on the ‘Analyze’ row on the leftmost Navigation Pane. So long as the “CENTRA-GW-SW-ANALYZE” license is added to the unit, this page can be used to engage one of up-to five independent 101 290 analyzer engines for transport stream validation on the Centra Gateway.



Analyze Main Page

Each 101 290 analyzer may be assigned to either a Source or Destination node to view the condition of the stream before or after routing through the Centra Gateway. 101 290 processing will occur after IP de-encapsulation on a Source Node and after IP re-encapsulation on a Destination Node.

4.5.1 TS Analyzer Settings

To configure the settings for a given TS Analyzer, click the corresponding button on the right side of the page.



Analyze

TR 101 290				
▼ TS Analyzer 1		Inactive	Never	Configure
▼ TS Analyzer 2	SRT Destination	Active	2 days 20 hours 44 minutes ago	Configure
▼ TS Analyzer 3		Inactive	Never	Configure
▼ TS Analyzer 4		Inactive	Never	Configure
▼ TS Analyzer 5		Inactive	Never	Configure

Configure Icon Location

The resulting menu is used to configure the 101 290 engine's target node and Priority 1 and 2 settings.

ETSI TR 101 290 monitoring

TS Analyzer 1

Enter Source/Destination to monitor

☒ Priority 1

TS Sync

☒ Sync Byte

☒ PAT

Continuity

☒ PMT

Missing PID

☒ Priority 2

☒ Transport

☒ CRC

☒ PCR Repetition

☒ PCR Discontinuity

☒ PCR Accuracy

☒ PTS

☒ CAT

Add All

Apply



Cancel

TS Analyzer Settings Window

Name	Range	Description
Label	1 character - many	Enter the name for the analyzer
Toggle	On/Off	Turn the analyzer on and off
Monitor Dropdown	Source/Destination Name	Use this dropdown to choose the source or destination to be monitored
Priority 1	TS Sync*	Enable/disable Priority 1: 101 290 attributes (see Appendix D for more information on attributes)
	Sync Byte	
	PAT	
	Continuity*	
	PMT	
	Missing PID*	
Priority 2	Transport	Enable/disable Priority 2: 101 290 attributes (see Appendix D for more information on attributes)
	CRC	
	PCR Repetition	
	PCR Discontinuity	
	PCR Accuracy	
	PTS	
	CAT	

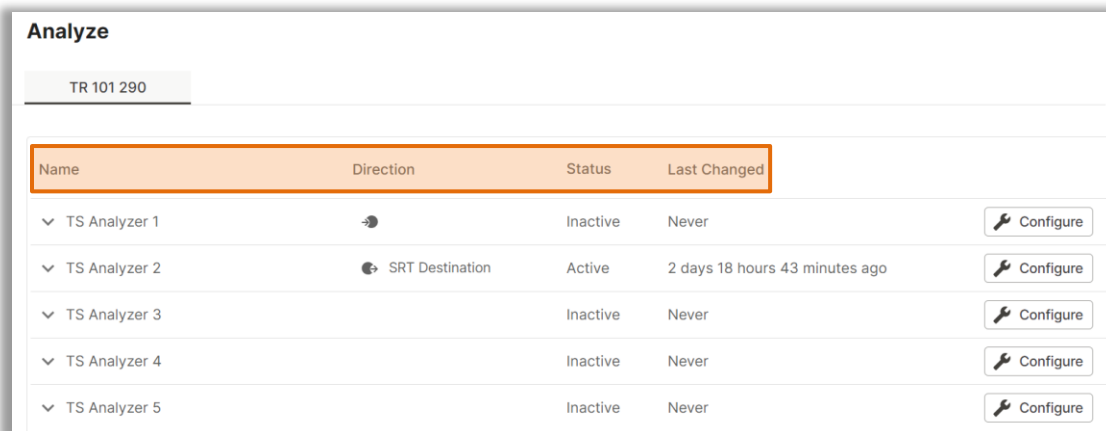
*Required, not able to be disabled.

Enable or disable a monitoring attribute, by clicking the name. All attributes are optional, except for TS Sync, Continuity, and Missing PID. Selecting the checkbox next to each priority will enable/disable all attributes under that priority. Clicking the button will select all attributes under both priorities.

When selecting nodes to monitor from the dropdown menu, the  icon is associated with a source node and the  icon is associated with a destination node.

4.5.2 TS Analyzer Information

When on the analyzer home menu, filter the analyzers by clicking on any of the headers (Name, Direction, Status, Last Changed).



Analyze				
TR 101 290				
Name	Direction	Status	Last Changed	
TS Analyzer 1		Inactive	Never	Configure
TS Analyzer 2	SRT Destination	Active	2 days 18 hours 43 minutes ago	Configure
TS Analyzer 3		Inactive	Never	Configure
TS Analyzer 4		Inactive	Never	Configure
TS Analyzer 5		Inactive	Never	Configure

Analyze Page Overview

Setting	Description
Name	Label of the analyzer
Direction	Node Source/Destination
Status	Shows whether the analyzer is enabled: Active/Inactive
Last Changed	Shows the last time the analyzer has been configured

To view the TS Analyzer status, click the drop-down on the left side of the row:

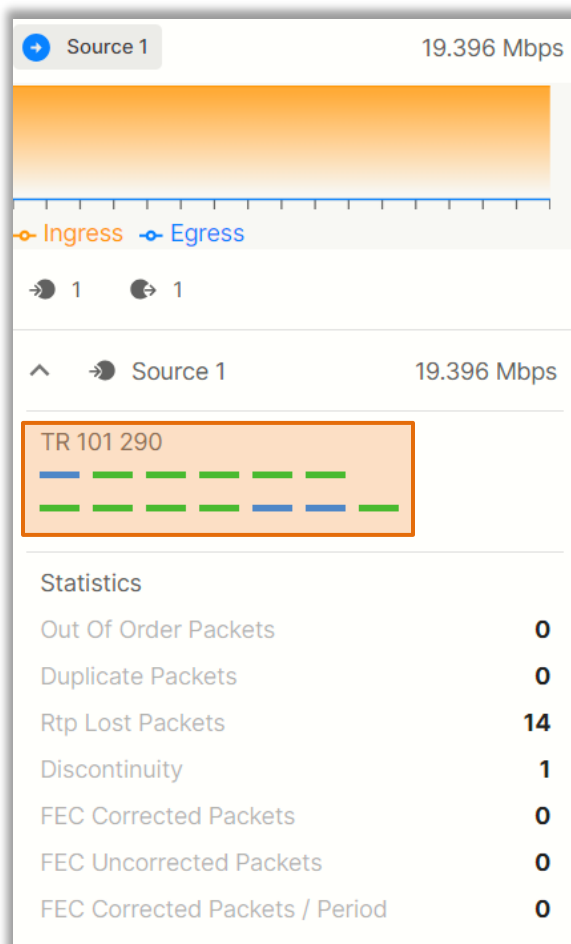
Name		Direction			
^ TS Analyzer 1		Template 1			
Priority 1	Status	Count	PID	Timestamp	
TS Sync Loss	✓				
Sync Byte	✓				
PAT	✓				
CC	✓	11749	97	2023-09-28 13:35:57	
PMT	✓	24	80	2023-09-28 13:34:33	
PID	✓				
Priority 2	Status	Count	PID	Timestamp	
Transport	✓				
CRC	✓				
PCR Repetition	✓				
PCR Discontinuity	✓				
PCR Accuracy	✓	24149	97	2023-09-28 13:35:57	
PTS	✓	41	49	2023-09-28 13:28:24	
CAT	✓				

TS Analyzer Information Page

Setting	Range	Description
Priority 1	TS Sync Loss	List of 101 290 priority 1 attributes available to be monitored
	Sync Byte	
	PAT	
	CC	
	PMT	
	PID	
Priority 2	Transport	List of 101 290 priority 2 attributes available to be monitored
	CRC	
	PCR Repetition	
	PCR Discontinuity	
	PCR Accuracy	
	PTS	
	CAT	

Status	Green, blue, red, and gray	Green = No Errors Blue = has previously been In Error Red = currently In Error Gray = not monitoring
Count	0 – many	Shows how many times the error has occurred
PID	0 – many	Affected PID(s)
Timestamp	Date	Date/time of last error occurrence

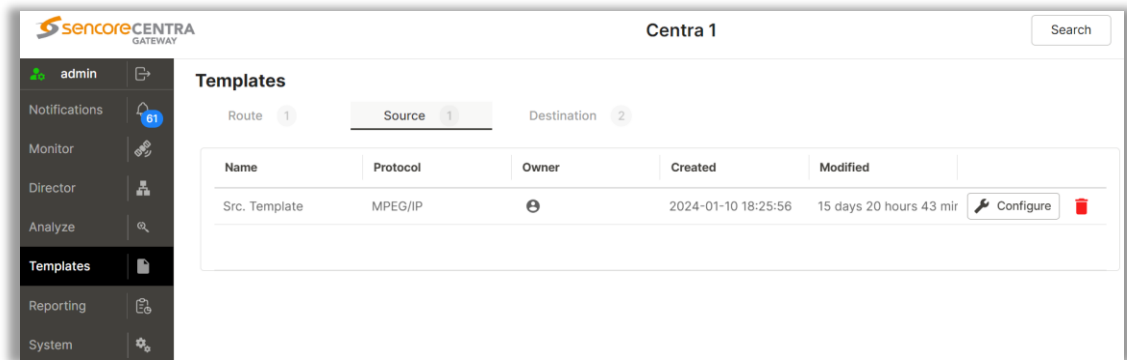
To access the 101 290 information from a route, select the node being monitored. The analyzer data will be shown above the statistics section the right (see [Section 4.3.4](#) for more info).



101 290 Information under Route

4.6 Templates

The Templates control panel is used to quickly apply configurations to any routes, sources or destinations based on pre-existing templates. To access the Templates Control Panel, click on the Templates tab on the left side of the page. This page provides access for viewing and editing saved templates for routes, sources, and destinations.




Templates Overview

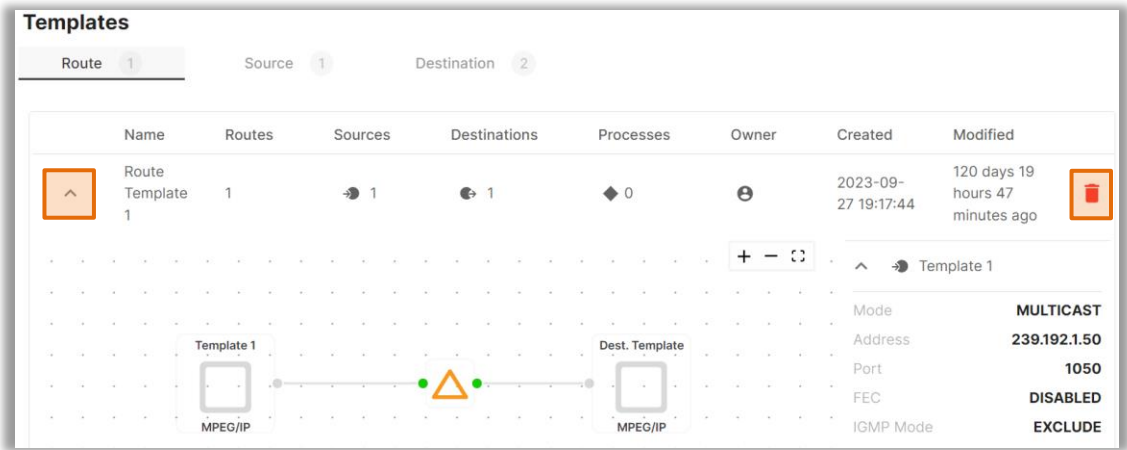
4.6.1 Viewing and Using Templates

There are 3 types of templates: Route Templates are Read-Only while Destination and Node Templates are Read-Write capable.

Route Templates

Click the down  arrow to view the route. Selecting any of the nodes will display the configuration contained in the node on the right side (see [Section 3.8](#) for more information on routes/nodes).

To delete a template, click the  button on the right hand of the row.



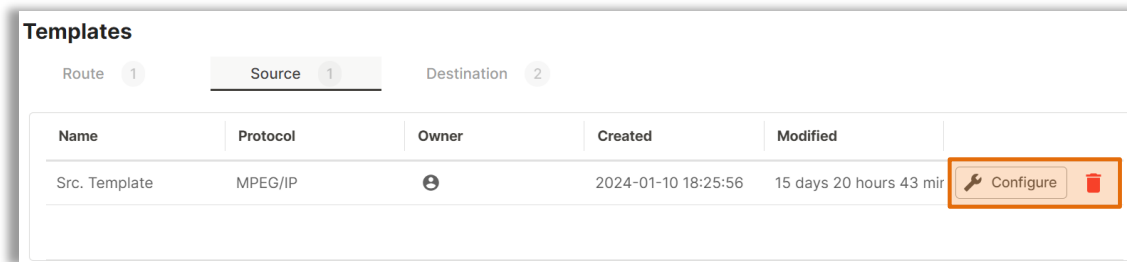
The screenshot shows the 'Templates' interface with the 'Route' tab selected. It displays a table with columns: Name, Routes, Sources, Destinations, Processes, Owner, Created, and Modified. A single row is visible for 'Route Template 1'. To the left of the table is a diagram showing a route from 'Template 1' (MPEG/IP) to 'Dest. Template' (MPEG/IP) via a central node. To the right of the table is a configuration panel for 'Template 1' with fields for Mode (MULTICAST), Address (239.192.1.50), Port (1050), FEC (DISABLED), and IGMP Mode (EXCLUDE). A trash icon is visible at the end of the row.

Route Template Overview

Source and Destination Templates

Under the appropriate tab, either a source or destination:

To edit a template, click the  Configure button under the last column of the row (see [Section 3.6.2](#) and [Section 3.6.3](#) for Source and Destination configuration options). To delete a template, click the  button on the rightmost side of the row.



The screenshot shows the 'Templates' interface with the 'Source' tab selected. It displays a table with columns: Name, Protocol, Owner, Created, and Modified. A single row is visible for 'Src. Template' with Protocol 'MPEG/IP'. At the end of the row are 'Configure' and 'trash' buttons.

Source/Destination Template Overview

Src. Template

Protocol

MPEG/IP

Interface

eth1

Mode

Multicast

Address

239.192.1.50

:

1050

FEC

Disabled

IGMP Filter

Exclude

IGMP Address

0.0.0.0

+

Delete All

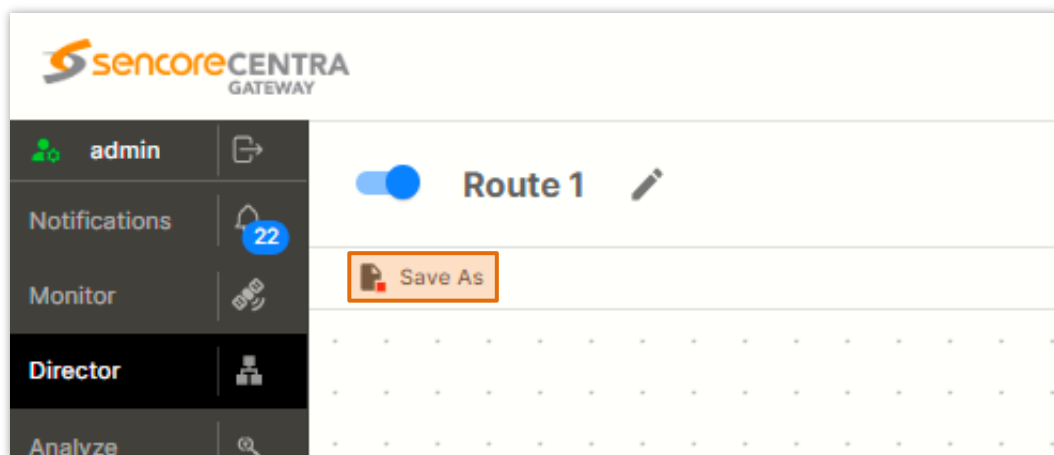
Update

Template Example

To use a template, select the template via drop-down to use when creating or configuring a route ([Section 3.6.1](#)), source ([Section 3.6.2](#)), or destination ([Section 3.6.3](#)).

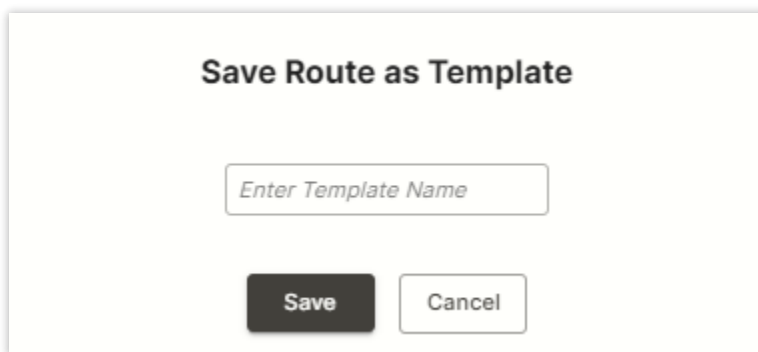
4.6.2 Creating Route Templates

To create a Route template, open any existing route on the “Director” panel. Under the enable icon, click the “Save As” button as shown below in the top left.



“Save As” Button Location

Enter the Template name into the subsequent prompt, and the route template will be saved and available for view on the “Templates” panel.



Save Route Template Window

4.6.3 Creating Source Templates

To create a Source template, navigate to the “Director” panel and open an existing route that’s configured with a source. Under the configuration page for that source ([Section 4.3.2](#)), click the “Save As” button in the bottom right and a prompt will be opened for the template name.



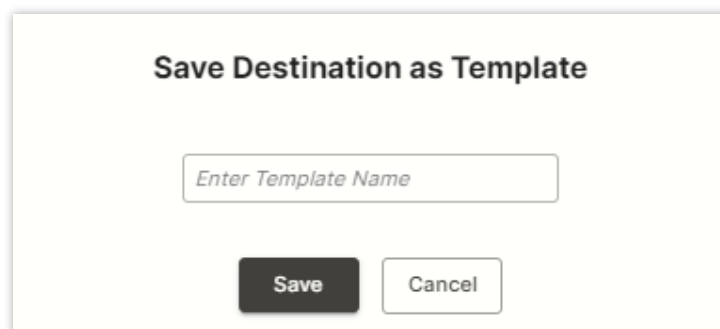
The dialog box is titled "Save Source as Template". It features a text input field with the placeholder text "Enter Template Name". Below the input field are two buttons: a dark grey "Save" button and a light grey "Cancel" button.

Save Source Template Window

After clicking “Save”, the Template will now be added to the Templates page for future use to expedite editing and creating sources.

4.6.4 Creating Destination Templates

To create a Source template, navigate to the “Director” panel and open an existing route that’s configured with a destination. Under the configuration page for that destination ([Section 4.3.3](#)), click the “Save As” button in the bottom right and a prompt will be opened for the template name.



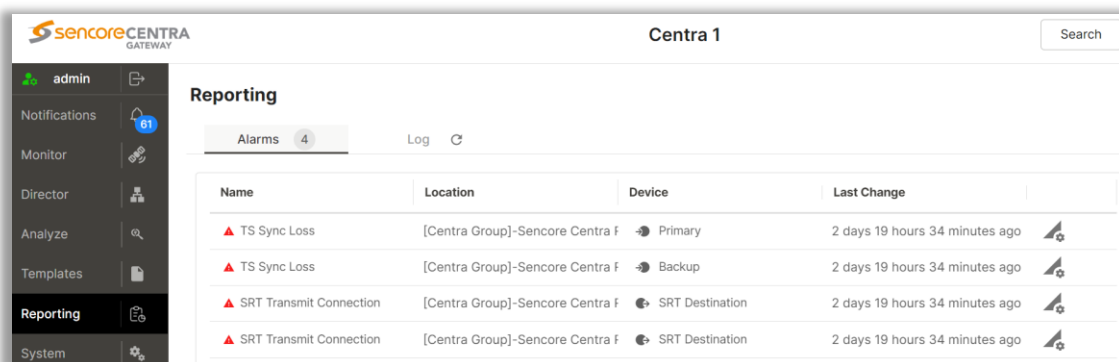
The dialog box is titled "Save Destination as Template". It features a text input field with the placeholder text "Enter Template Name". Below the input field are two buttons: a dark grey "Save" button and a light grey "Cancel" button.

Save Destination Template Window

4.7 Reporting Control Panel

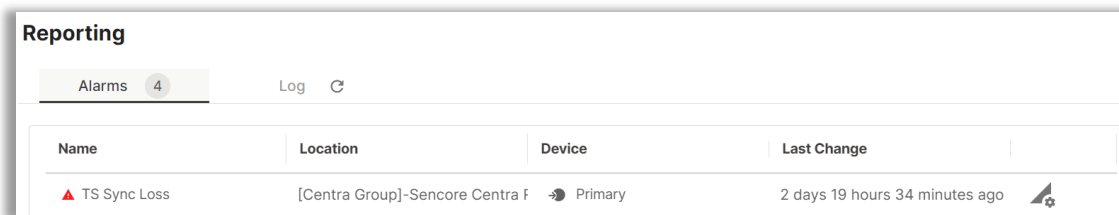
The Reporting control panel in the Centra Gateway will provide the user with a list of active alarms, as well to log the detected events. Active alarms are constantly updated to reflect the real-time state of the unit.

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.





Reporting Main Page

4.7.1 Alarms




Alarms Tab

By default, the Alarms tab is selected. This list displays all *active alarms*.

Name	Description
Name	The alarm label. See Appendix B for a complete list of alarm labels and their meaning
Location	The route or group affected by the alarm
Device	This column will indicate the Label of the alarming Destination or Source Node. The right-facing arrow,  , will denote a Source, while the left-facing arrow,  , indicates a destination

Last Change

This column displays the most recent date and time the error was raised. Timestamps here are determined with the Date and Time settings configured in [Section 4.9.1.2](#)


On any alarming row, clicking the  icon will navigate the browser directly to the Director tab for the route or group associated with the active alarm message.
















4.7.2 Log

The Log window stores alarms that were active for a time as well as their clear time. Up to 10000 alarm entries may be stored.

Reporting

Alarms 4

Log 

Timestamp	Location	Device	Transition
2024-01-18 22:25:43	[Centra Group]-Sencore Centra Route	 Primary	 TS Sync Loss 
2024-01-18 22:11:32	[Centra Group]-Sencore Centra Route	 Backup	 RTP Reception 
2024-01-18 22:11:31	[Centra Group]-Sencore Centra Route	 Backup	 RTP Reception 
2024-01-18 22:11:31	srt	 SRT Source	 SRT Receive Connection 
2024-01-18 22:11:30	[Centra Group]-Sencore Centra Route	 SRT Destination	 SRT Transmit Connection 

Rows per page: 20 1-20 of 10000 1 1 of 500 page

Log Tab

Name

Description



Timestamp



The date and time the error was raised or cleared. Timestamps here are determined with the Date and Time settings configured in [Section 4.9.1.2](#)


Location

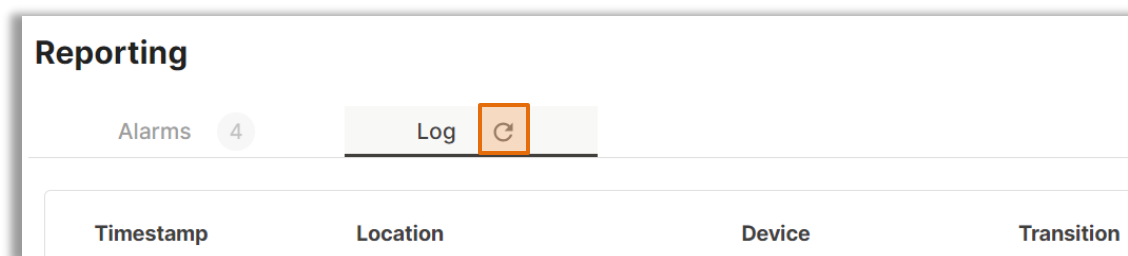
The route or group affected by the alarm

Device



The Label of the alarming Destination or Source Node. The left-side  arrow will denote a Source. The right-sided  arrow indicates a destination

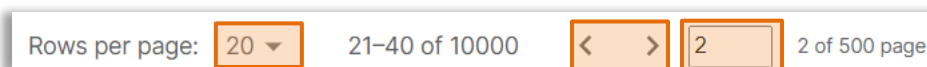
Transition	The green plus  icon denotes that the alarm has moved from a non-working to working state, while the red minus:  icon indicates movement from a working to non-working state
Alarm Message	The right-most column will show the alarm name. For more information on alarm names and their descriptions, see Appendix B

The  icon is used to refresh the log list with any alarm activity that occurred while viewing the log page.



Refresh Icon

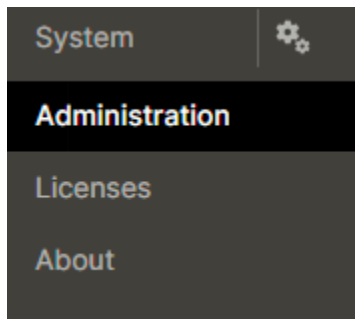
For navigation, along the bottom of the page, the “Rows Per Page” field can be toggled between 20 and 50 entries to increase the number of entries on the page. The  and  icons are used to scroll between pages one at a time. The textbox on the far right can be used to manually enter page numbers for larger date and time movement.



Navigation Options

4.8 System

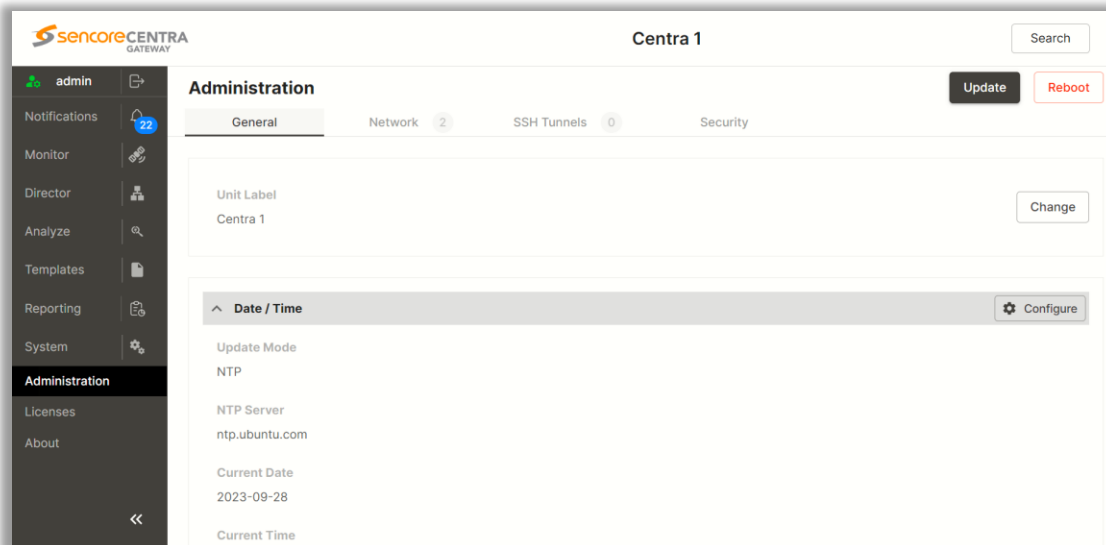
Use the “System” panel to access device-level settings and other information for the Centra Gateway.



System Panel Sub-options

4.9 Administration Control Panel

Click on the Administration tab to view global settings and maintenance tasks on the Centra Gateway. Use these menus to change system level settings such as date and time, network interface options or the username and password. These functions as well as all others available throughout the Administration panel will be described throughout Section 4.9.



Administration Main Page

4.9.1 General

The General tab is the default page of the Administration panel. This tab is used to change the Unit Label as well as Date and Time.

General Tab

4.9.1.1 Setting Unit Label

The Centra Gateway can be named using the Unit Label option. To set the name click on the Change button on the right side of the page.

Change Unit Label Icon

After clicking “Change” the Unit Label field will become editable. Manually enter the intended string, and then click “OK” to commit the changes (or “Cancel” to revert them).

Unit Label Field

The resulting label will display at the top of the page on all menus for reference.



Unit Label Location

4.9.1.2 Setting Unit Date and Time

Time can either be defined manually, or the Centra Gateway can synchronize with an NTP server. Click the “Configure” cog button to expose the ‘Configure Date / Time’ menu. These values are used to timestamp entries in the Alarm and Event logs under the Reporting tab.



Configure Icon Location

Configure Date / Time

Update Mode NTP

NTP Server ntp.ubuntu.com

Date 2023-09-27


Time 18:47:49

Time Zone (GMT+00:00:00) GMT

Note: Changing time may prompt you to log-in.

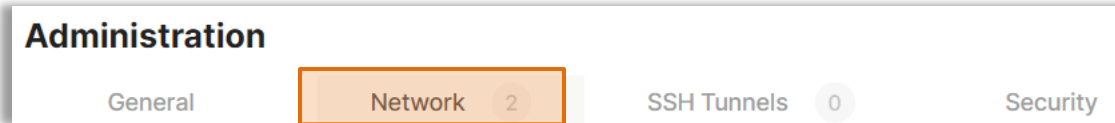
Apply
Cancel

Configure Date / Time Window

Name	Range	Description
Update Mode	NTP or Manual	When set to NTP, the user provides location information of the NTP server for date and time sync. When Manual, the user will define system Date and Time
NTP Server	XXX.XXX.XXX.XXX Domain Name	Defines IP Address or Domain Name of the NTP server to be used for NTP mode.
Date	YYYY/MM/DD	Manual mode setting format for the system date. The calendar widget  may be used for efficiency
Time	00:00:00 – 24:00:00	Manual mode setting for the system time. The time is based on a 24-hour clock
Time Zone	-12:00:00 ~ +13:00:00	Applies a time offset. Useful for time zone changes or daylight savings time

4.9.2 Network

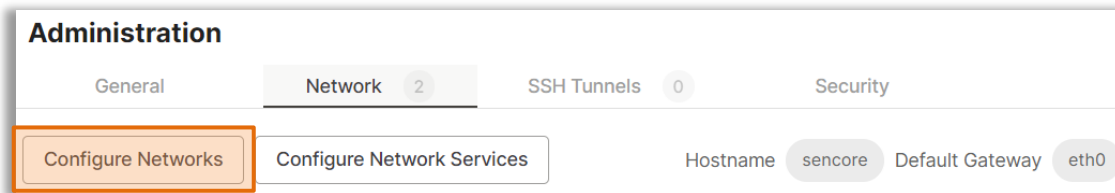
Use the “Network” tab to edit the following network settings for the system as well as its individual interfaces, such as Hostname, DNS and Network Services.



Administration Network Tab

4.9.2.1 Configuring Hostname and DNS

To assign the Centra Gateway Hostname and declare its DNS servers, click on the Configure Networks button to expose the configuration menu.



Configure Networks Button

Configure Networks

Hostname

Default Gateway

Primary Nameserver

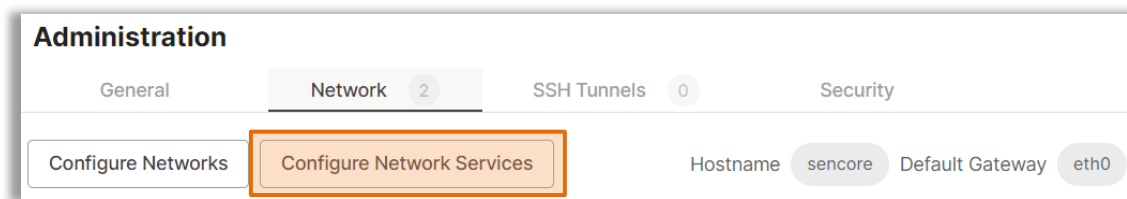
Secondary Nameserver

Configure Networks Menu

Name	Range	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

4.9.2.2 Configuring Network Services

Both Physical NICs can have port-specific features enabled for functionality or disabled for security. To configure these settings, click on the “Configure Networks” button to expose the menu.



Configure Network Services Button

The subsequent figure shows default settings to allow ICMP (ping) response, web access, and general stream input and output traffic. The checkboxes are used to enable or disable options on a per-service and per-NIC basis. The leftmost checkbox will enable or disable the full service, while the eth columns are used to enable or disable the service for a specific interface.

Configure Network Services

Enable	Service	Protocol	Port	eth0	eth1
<input checked="" type="checkbox"/>	ICMP	ICMP	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SSH	TCP	22	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	HTTP	TCP	80	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	HTTPS	TCP	443	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Stream I/O	UNKNOWN	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

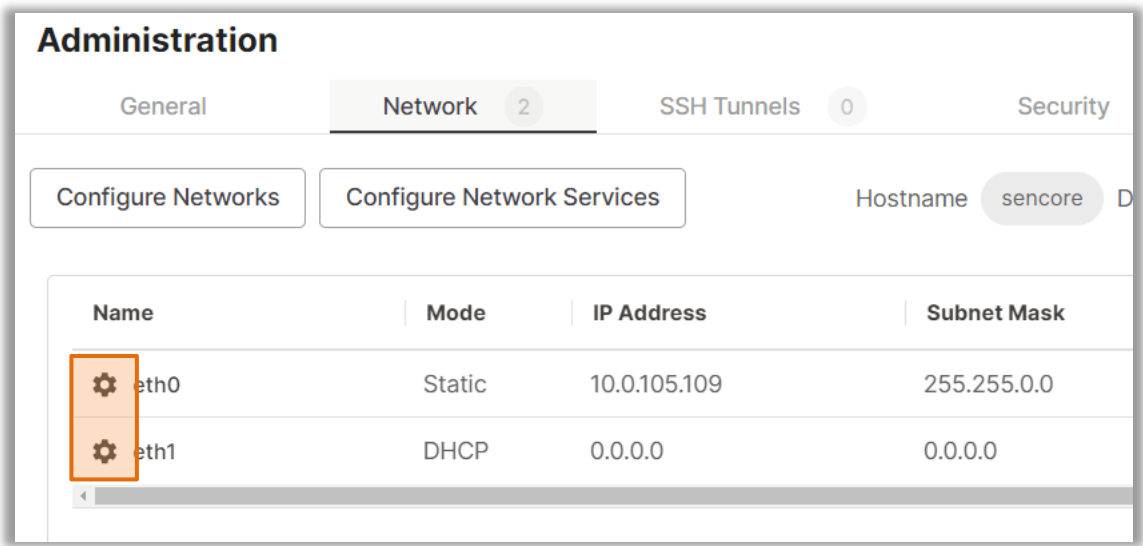
Configure Network Services Menu

Name	Protocol	Range	Description
ICMP	ICMP	N/A	Allows access to ICMP responses (such as pinging)
SSH	TCP	22	Allows for SSH access through port 22
HTTP	TCP	80	Allows access to the web interface via browser
HTTP	TCP	443	Allows secure access to the web interface via browser
Stream I/O	Unknown	N/A	Enables and disables all stream traffic for the physical interface (Zixi, MPEG/IP, SRT, HLS)

Note: HTTP and HTTPS currently cannot be disabled. While any interface is eligible to carry HTTP(S), only one is used for GUI access at a given time).

4.9.2.3 Management and Data Ports

Any NIC can be configured for Management or Data networks via Mode, IP address, and VLAN options. To access NIC settings, click the gear icon by the corresponding NIC to open its menu.



Gear Icon Location

Configure eth0

Interface Label

Mode

Static ▼

IP Address

Subnet Mask

Gateway

+ Add a VLAN
- Remove ALL

VLAN	VLAN ID	IP Address	Subnet	Gateway	Remove
No VLANs					

Apply

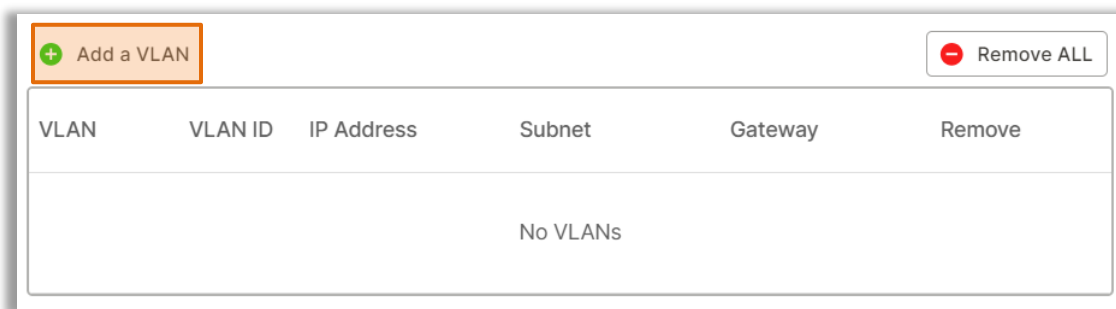
Cancel

Configure Network Port Window

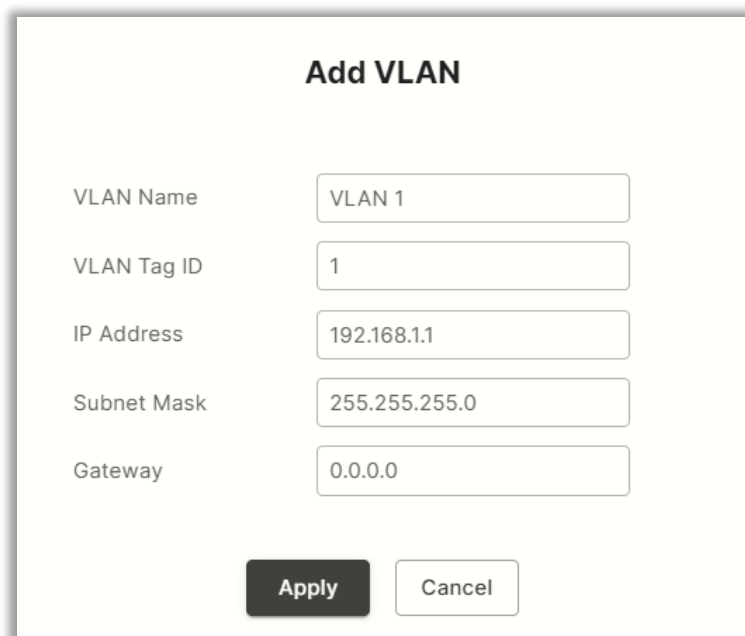
Setting	Available Selections	Description
Interface Label	User Entered (eth0 / eth1 by default)	User defined port names
Mode	DHCP, Static	<i>DHCP</i> allows network server to provide IP address. <i>Static</i> requires the user to define the IP address to be used
IP Address	xxx.xxx.xxx.xxx	Static Mode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

After finishing changes, click the apply button. [Note: Edit these menus carefully; the web-interface is only accessible from the IP address of the Ethernet port chosen in [Section 4.9.2.2](#). Make certain to configure all ports for separate subnets.]

To add a VLAN to the NIC, click the “Add a VLAN” button to expose the “Add VLAN” menu.



Add VLAN Icon



Add VLAN Window

Setting	Available Selections	Description
VLAN Name	User Entered	Label the VLAN interface
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 “Apply”, any newly created VLAN will now be present on the VLAN list. Any VLAN interfaces for a given ethernet port will be available for selection on any Destination or Source Node thereafter. After a VLAN is created, all its fields except the VLAN ID are eligible for change except the VLAN ID. Use the textboxes to edit settings on existing VLANs.

VLAN	VLAN ID	IP Address	Subnet	Gateway	Remove
VLAN 1	1	192.168.1.1	255.255.255.0	0.0.0.0	

Editing VLANs

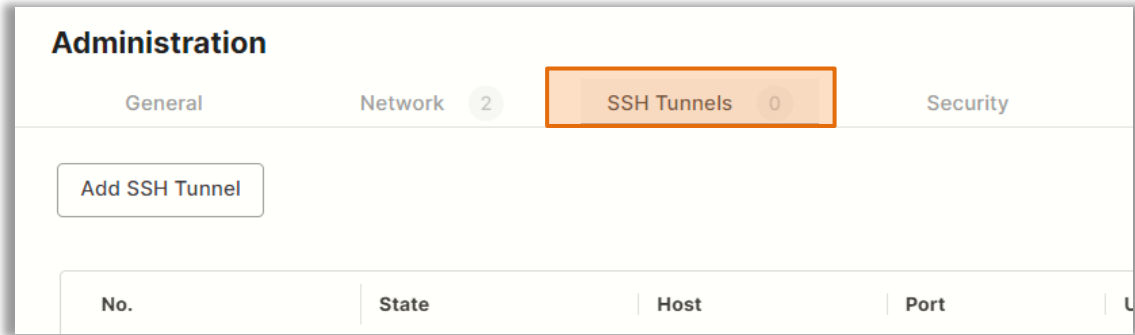
To remove individual VLANs, click the red icon under the “Remove” column for the corresponding row. To remove all VLANs, click the “Remove ALL” button.

VLAN	VLAN ID	IP Address	Subnet	Gateway	Remove
VLAN 1	1	192.168.1.1	255.255.255.0	0.0.0.0	

Removing One or All Configured VLANs

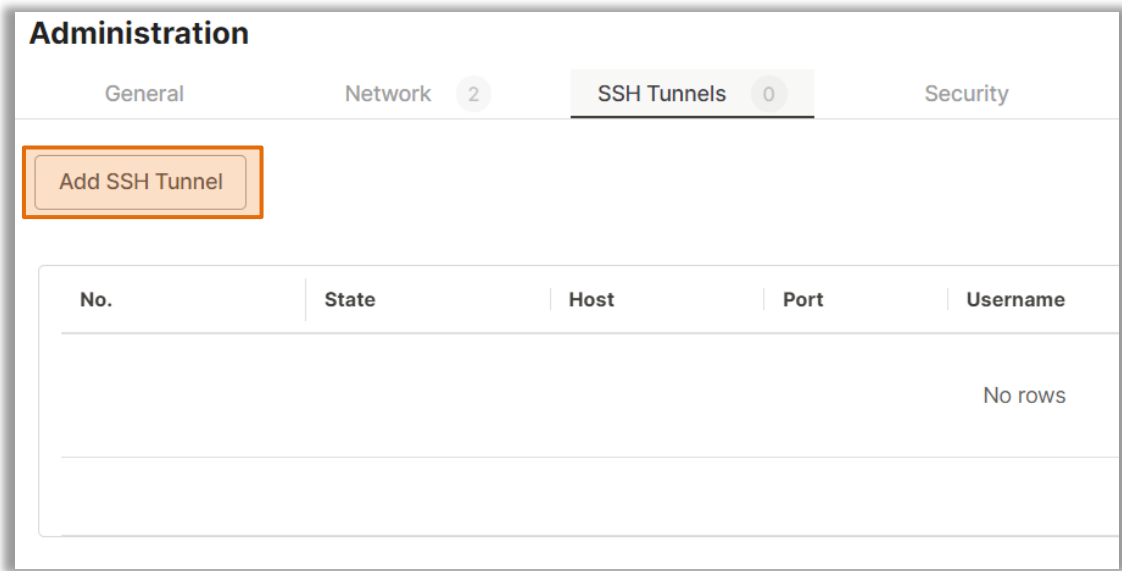
4.9.3 SSH Tunnels

The Centra Gateway can be remotely managed using SSH tunnels. In applications where Zixi ZEN Master is being used, an SSH tunnel is established to provide nested remote access to the web GUI of the Centra.



SSH Tunnels Tab

Create an SSH tunnel by clicking the “Add SSH Tunnel” button to expose the settings.



Add SSH Tunnel Icon

Add SSH Tunnel

Host

Port

Username

Key File
No Key File

Remote Source Port

Local Destination Host

Local Destination Port

Apply

Cancel

Add SSH Tunnel Window

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 these settings can be found in the ZEN Master instance.

Setting	Range	Description
Host	IPv4 Address Valid Doman Name	The IP address or web link of the Zixi (ZEN Master) server
Port	0 – 65535	The IP port of the Zixi (ZEN Master) server
Username	User Entry	Account credential to log into Zixi (ZEN Master) server
Key File	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

Remote Source Port	0 – 65535	Remote port number the Zixi (ZEN Master) server is using for SSH communication
Local Destination Host	IPv4 Address Valid Domain Name	Address reporting to Zixi (ZEN Master) server. Localhost is the default.
Local Destination Port	0 – 65535	The port that is accessible to the Zixi (ZEN Master) server. Port 80 (Centra Gateway web client) is the default

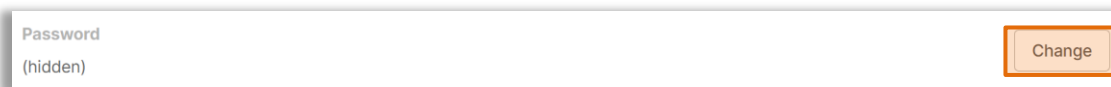
4.9.4 Security

Use the 'Security' tab to edit the following security settings: Login Password, CSRs, and SSL/TLS Certificates.



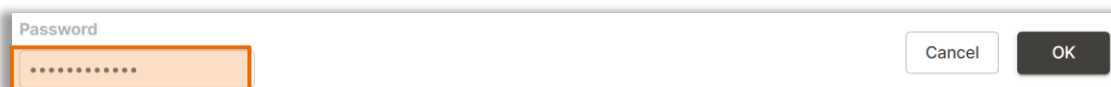
4.9.4.1 Changing Unit Password

The default admin-password is 'mpeg101'. To change the password, click the "Change" button.

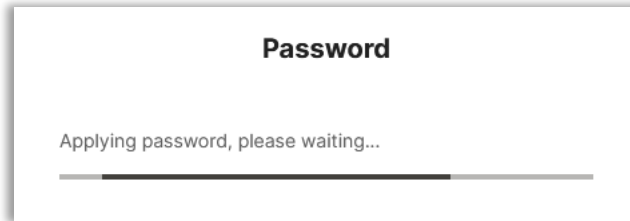


Password Section

After clicking "Change" the Password field will become editable. Manually enter the intended string, and then click "OK" to commit the changes (or "Cancel" to revert them).



Password Change Menu



Password Application Prompt

After the password is applied, the change will go into effect upon the next sign-in.

4.9.4.2 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 source and destination instances as described in [Section 4.6.4.3](#).










Security Manager Section

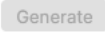
Security Manager

Country Name	<input type="text" value="US"/>
State or Province Name	<input type="text" value="Delaware"/>
Locality Name	<input type="text" value="Wilmington"/>
Organization Name	<input type="text" value="Sencore Inc"/>
Organizational Unit Name	<input type="text"/>
Common Name	<input type="text"/>
Email Address	<input type="text"/>
Certificate Signing Request File Name	
New CSR File	<input type="button" value="Generate"/>
Generated CSR File	<input type="button" value="Download"/>
Old CSR File	<input type="button" value="Delete"/>
Old Local Private Key File	<input type="button" value="Delete"/>

Local Certificate File	<input type="button" value="⬆"/>
Local Private Key File	<input type="button" value="⬆"/>
Remote Certificate File	<input type="button" value="⬆"/>

Security Manager Menu

Setting	Range	Description
Country Name	User entry	Country Name for generated CSR file
State or Province Name	User entry	State/Province Name for generated CSR file
Locality Name	User entry	Locality Name for generated CSR file
Organization Name	User entry	Organization Name for the generated CSR file
Organizational Unit Name	User entry	Organizational Unit Name for the generated CSR file
Common Name	User entry	Common Name for the generated CSR file
Email Address	User entry	Email Address for reference on the generated CSR file
Generate New CSR File		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
Download Generated CSR File		This icon will download the locally generated CSR file onto a remote machine
Delete Old CSR File		This icon will delete the locally generated CSR file
Delete Old Local Private Key File		This icon will delete the locally generated private key file
Local Certificate File		Use this icon to upload the local certificate file
Local Private Key File		Use this icon to upload the local private key file
Remote Certificate File		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.

4.9.4.3 Enabling DTLS

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 4.9.4.2](#)). The same Certificate File may be uploaded to both the Local and Remote Certificate File fields.

Local Certificate File	
Local Private Key File	
Remote Certificate File	

Key and Certificate Files

When making a DTLS connection between a Centra Gateway that is transmitting RIST and a Centra Gateway 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 4.2.2.6](#) and [Section 4.2.3.4](#).

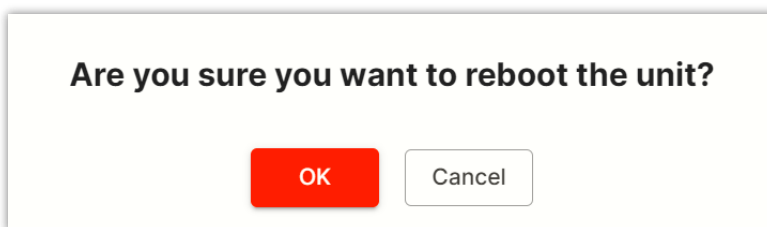
4.9.5 Reboot the Unit

The Centra Gateway can be rebooted from the web interface Admin page. The 'Reboot' button is in the top right corner of the Administration Control Panel. To perform a reboot, click the reboot button.



Reboot Icon Location

The system will prompt to confirm the reboot request. Click "OK" to proceed or "Cancel" to back out without resetting.

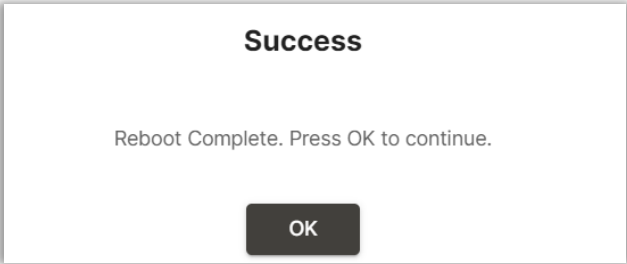


Reboot Window Prompt

Once confirmed, a status window with a progress bar will open be visible until the reboot is complete and the login window displayed.



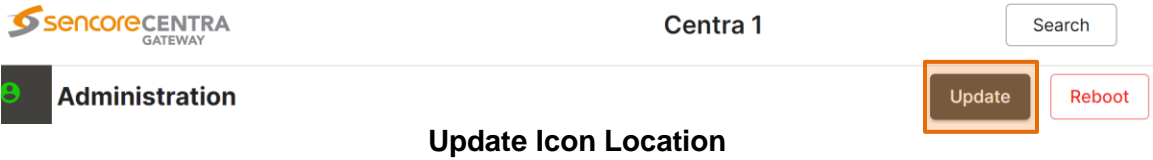
Rebooting Status



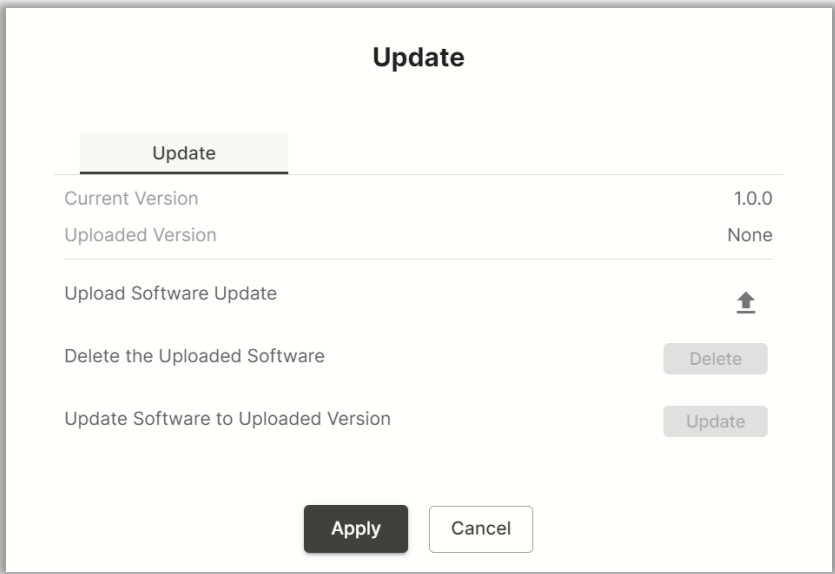
Reboot Completion Message

4.9.6 Updating the System Software

Updates to the Centra Gateway are performed through the web interface. Software update files are 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. Click the “Update” icon to open the menu for uploading and applying software.


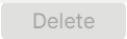
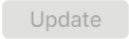


Update Icon Location



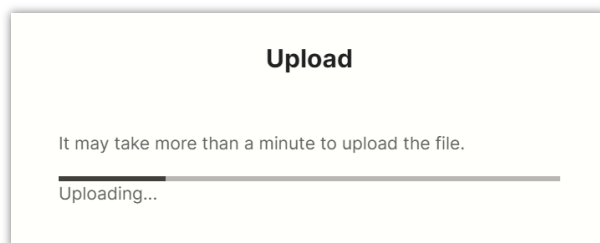
Update Menu

The “Current Version” reflects the software currently running on the Centra Gateway, while the “Uploaded Version” field shows the firmware uploaded onto the unit. If there is an Uploaded Version, then clicking ‘Update’ will trigger the unit to push the uploaded firmware to the system (entails a reboot, schedule during an available maintenance window as needed).

Setting	Range	Description
Upload Software Update		To upload software updates to the Centra Gateway click this button. The user will be prompted to navigate to an update file. The file will then upload to the Centra Gateway. When complete the Centra Gateway 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 Centra Gateway. 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 Centra Gateway will prompt the user to confirm the update. Click Yes to continue or No to cancel

Applying software updates

1. Click upload button and browse to the appropriate software file
2. A progress bar will show uploading status



Upload Window

3. Once the file is uploaded, click on the “Update” button
4. The Centra will reboot after a software update is complete.

4.10 Licenses

Licenses				Apply Key
Option	Support...	State	Inst...	
Centra Gateway Software Option, 5x ETR 101-290 Analyzers (per instance)	+	Licensed	1	
Centra Gateway Software, up to 250Mbps throughput	+	Unlicensed	0	
Centra Gateway Software, up to 800Mbps throughput	+	Licensed	1	
Centra Gateway Software, up to 100Mbps throughput	+	Unlicensed	0	

Licenses Main Page

Certain features of the Centra Gateway require licenses to be functional. The interface displays all licenses available as well as the following status:

- State Licensed or Unlicensed
- License is Supported or Unsupported by the installed hardware

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

Enter License Key

Enter a new license key here...

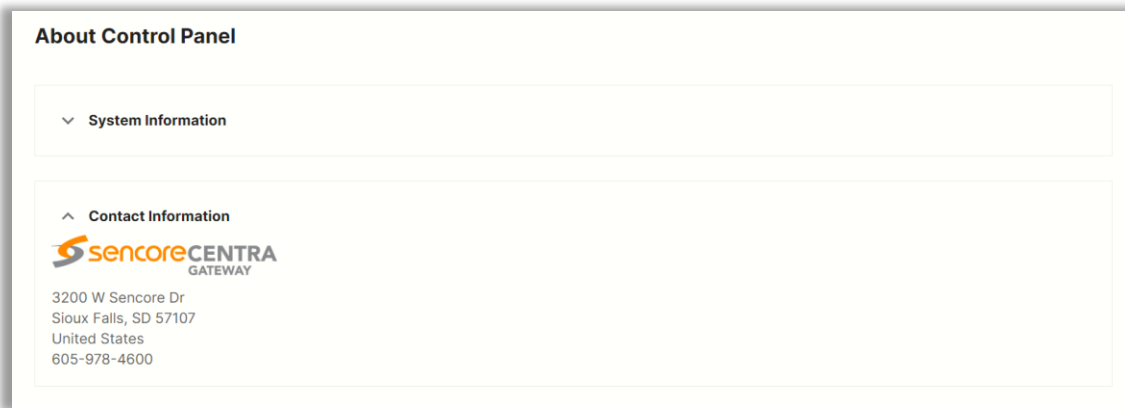
Apply

Cancel

License Key Menu

4.11 About

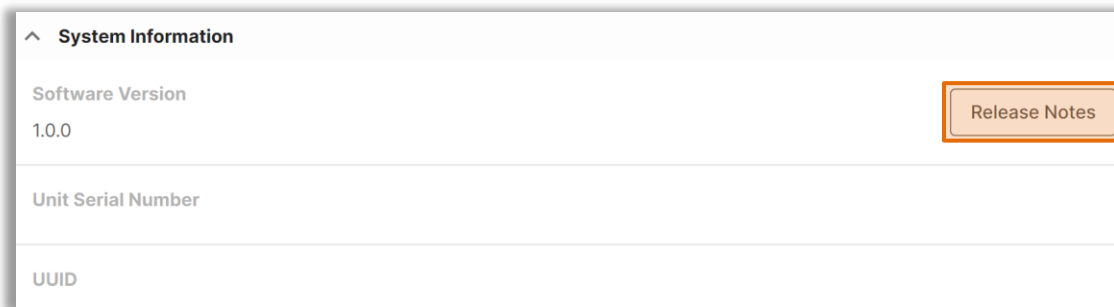
Under the “About” panel, there is information about the current software version, hardware/software options, how to contact Sencore, and third-party software being used.



About Main Page

4.11.1 System Information

This menu shows the current software version and UUID of the unit. The “Release Notes” button in the top right will show the latest updates made.



System Information

Release Notes

Feature Release 1.0.0

The 1.0.0 release is a feature release for the Sencore's Centra platform. 1.0.0 obsoletes any beta builds that were previously provided. This software is the initial release for Centra Gateway.

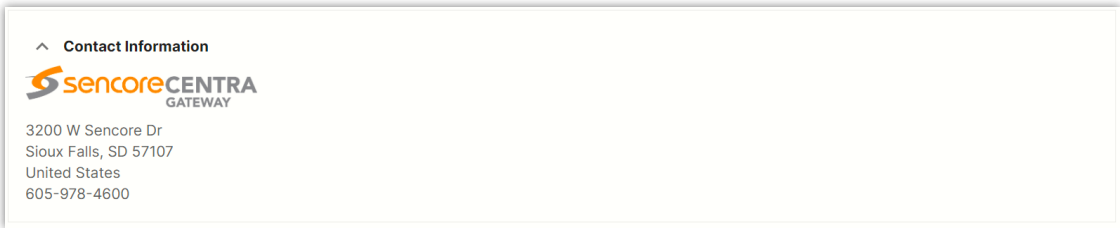
New Features in 1.0.0

- SRT transmit and receive
- RIST transmit and receive
- Zixi transmit and receive
- MPEG/IP transmit and receive
 - UDP/RTP
 - ST 2022-7 receive
 - ST 2022-1 FEC receive
- HLS receive
- 5x ETR 101290 analyzers (with license)
- Templates for sources, destinations and routes

Release Notes Window

4.11.2 Contact Information

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



Contact Information Section

4.11.3 Third Party Software Information

This area of the control panel can be expanded to show the third-party software used by the Centra Gateway. See [Appendix H](#) for a complete list.

^ Third-Party Software Information			
Package	Version	License	Copyright
Alpine Linux	3.17.0	MIT License	Alpine Linux Development Team
BusyBox	1.28	GPL Version 2, June 1991	Erik Andersen, et. al.
cjson	1.7.15	MIT	Dave Gamble and cJSON contributors
coredns	1.9.0	Apache License 2.0	2023 The CoreDNS Authors
Docker Calico	3.21.4	Apache License 2.0	2023 Docker, Inc.
FFmpeg	5.0.1	LGPL Version 2.1, February 1999	Fabrice Bellard
fluent-bit	1.8	Apache License 2.0	2015-2023 The Fluent Bit Authors
k3s	v1.25.7+k3s1	Apache License 2.0	K3s Project Authors.

Third-Party Software Sectio

Section 5 Appendices

Introduction

This section includes the following appendices:

Appendix A	– Specifications.....	146
Appendix B	– Error and Event List.....	149
Appendix C	– Internet Transport Protocol Explanation	151
Appendix D	– 101 290 Descriptors	153
Appendix E	– Acronyms and Glossary.....	154
Appendix F	– Warranty	155
Appendix G	– Support and Contact Information	156
Appendix H	– Open Source Software.....	157



Appendix A – Specifications

Centra Gateway – 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

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 Centra Gateway with all supported protocols. Each protocol can be used in separate ways to accomplish the goal of distributing content reliably over unmanaged networks and internet connections. 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 Centra Gateway 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 could be used as point-to-point as well. A few keys points are important to understand.

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

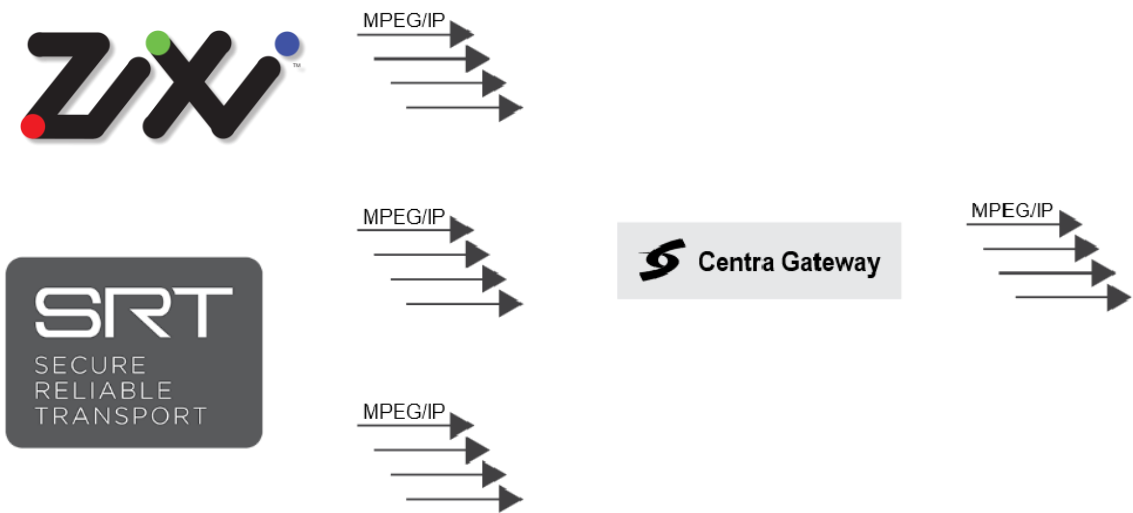
This architecture ensures the “first-mile” and “last-mile” of the streams path through the internet are as short as possible. The Zixi Broadcaster and ZEN Master control system allow streams being distributed over the internet to achieve high reliability. The Zixi Broadcaster is an appliance or cloud 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 Centra Gateway 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 Centra Gateway to a receiving Centra Gateway over a consumer internet connection. Thanks to the Centra Gateway’s ability to create multiple destinations from a lone source one Centra Gateway can transmit to many end-points.



In this final example, the Centra Gateway is being used for signal acquisition from sources transmitted over an unmanaged network or internet connection. The goal of the Centra Gateway 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 – 101 290 Descriptors

Priority 1:

TS Sync: The TS Sync check measures if the input signal can be received.

Sync Byte: All TS packets must start with the sync byte 0x47. If TS packets are received with incorrect sync byte the sync byte alarm will be triggered.

PAT: The Program Association Table (PAT) is most important table in the transport stream as it lists all the services in the streams and specifies the PMT PIDs.

Continuity: The continuity check verifies that the Continuity Counter which is present in all TS packets is updated according to the specification.

PMT: The Program Map Tables carry all information about a service.

Missing PID: The PID check verifies that all the signaled PIDs are present in the stream.

Priority 2:

Transport: The transport error check checks the transport_error_indicator flag in the TS packet. Which indicates that an unrecoverable transmission error has been detected for this TS packet.

CRC: The CRC error check verifies that the Cyclic Redundancy Checksum is correct for all tables.

PCR Repetition: The PCR repetition check verifies that PCR is transmitted sufficiently frequently.

PCR Discontinuity: The PCR discontinuity check verifies that the value transmitted in PCR does not have discontinuities.

PCR Accuracy: The PCR Accuracy check measures the PCR jitter caused by inaccuracies in the encoder clock and jitter caused by the signal transmission.

PTS: The PTS check verifies that the PTS information is transmitted regularly

CAT: The conditional access table lists the CA systems protecting the transport stream contents

Appendix E – 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
ARQ: Automatic Repeat reQuest
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
Centra Gateway: Video Distribution Platform
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 F – 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 G – Support and Contact Information

Returning Products for Service or Calibration

The Centra Gateway 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. 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. To obtain an RMA number, use the following steps:

1. Contact the Sencore service department by going online to www.sencore.com and select Support.
2. Select Service and Repair from the options given.
3. Fill in the following required information:
 - a. First & Last Name
 - b. Company
 - c. Email
 - d. Phone Number
 - e. Ship and Bill to Address
 - f. Unit Model and Serial Numbers
4. A RMA number will be emailed to you shortly after completing the form with return instructions.

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 H – Open Source Software

The Centra Gateway includes:

Package	Version	License	Copyright
Alpine Linux	3.17.0	MIT License	Alpine Linux Development Team
BusyBox	1.28	GPL Version 2, June 1991	Erik Andersen, et. al.
cjson	1.7.15	MIT	Dave Gamble and cJSON contributors
coredns	1.9.0	Apache License 2.0	2023 The CoreDNS Authors
Docker Calico	3.21.4	Apache License 2.0	2023 Docker, Inc.
FFmpeg	5.0.1	LGPL Version 2.1, February 1999	Fabrice Bellard
fluent-bit	1.8	Apache License 2.0	2015-2023 The Fluent Bit Authors
k3s	v1.25.7+k3s1	Apache License 2.0	K3s Project Authors.
libpcap	1.8.1	BSD	1993, 1994, 1995, 1996 The Regents of the University of California.
Log4cpp	1.1.3	LGPL Version 2.1, February 1999	Bastiaan Bakker
mongodb	4.4.8	Server Side Public License (SSPL) v1	2018 MongoDB, Inc.
nodejs	node:14-alpine	MIT License	Node.js contributors
OpenSSL	1.0.2u	BSD-Like	1998-2008 The OpenSSL Project, 1995-1998 Eric Young
redis	5.0	BSD-Like	2006-2020, Salvatore Sanfilippo
rist	7fcb772-2020-07-09	BSD-Like	Copyright © 2019-2020, VideoLAN and librist authors
srt	1.4.2	MPLv2.0 License	2018 Haivision Systems Inc.
zixi-sdk	14.13.43985	ZIXI	ZIXI CORPORATE
Zlib	1.2.7	zlib/libpng License	1995-2005 Jean-loup Gailly and Mark Adler

