Grass Valley
WE LOVE LIVE

SIRIUS COMPACT ROUTERS

12G SDI Compact Video Routers & Control Panels

Installation and Operation Manual

13-02070-010
2022-03-28

www.grassvalley.com

FCC Compliance

In order to comply with FCC/CFR47: Part 15 regulations, it is necessary to use high-quality, triple-screened Media or Monitor cable assemblies with integrated ferrite suppression at both ends.

Patent Information

This product may be protected by one or more patents.

For further information, please visit: www.grassvalley.com/patents/

Copyright and Trademark Notice

Grass Valley®, GV® and the Grass Valley logo and/or any of the Grass Valley products listed in this document are trademarks or registered trademarks of GVBB Holdings SARL, Grass Valley USA, LLC, or one of its affiliates or subsidiaries. All other intellectual property rights are owned by GVBB Holdings SARL, Grass Valley USA, LLC, or one of its affiliates or subsidiaries. All third party intellectual property rights (including logos or icons) remain the property of their respective owners.

Copyright © 2022 GVBB Holdings SARL and Grass Valley USA, LLC. All rights reserved.

Specifications are subject to change without notice.

Terms and Conditions

Please read the following terms and conditions carefully. By using Sirius Compact Routers documentation, you agree to the following terms and conditions.

Grass Valley hereby grants permission and license to owners of Sirius Compact to use their product manuals for their own internal business use. Manuals for Grass Valley products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Grass Valley.

A Grass Valley manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Grass Valley.

Warranty information is available from the Legal Terms and Conditions section of Grass Valley's website (www.grassvalley.com).

Title	Sirius Compact Routers Installation and Operation Manual
Part Number	13-02070-010
Revision	2022-03-28, 08:50

Important Safety Information

This section provides important safety guidelines for operators and service personnel. Specific warnings and cautions appear throughout the manual where they apply. Please read and follow this important information, especially those instructions related to the risk of electric shock or injury to persons.

Symbols and Their Meanings

Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.

Indicates that the user, operator or service technician should refer to the product manuals for important operating, maintenance, or service instructions.

This is a prompt to note the fuse rating when replacing fuses. The fuse referenced in the text must be replaced with one having the ratings indicated.

Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.
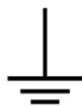
Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.

Indicates that static sensitive components are present, which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Indicates that the equipment has more than one power supply cord, and that all power supply cords must be disconnected before servicing to avoid electric shock.

The presence of this symbol in or on Grass Valley equipment means that it has been tested and certified as complying with applicable Underwriters Laboratory (UL) regulations and recommendations for USA.

The presence of this symbol in or on Grass Valley equipment means that it has been tested and certified as complying with applicable Canadian Standard Association (CSA) regulations and recommendations for USA/Canada.

The presence of this symbol in or on Grass Valley equipment means that it has been tested and certified as complying with applicable Underwriters Laboratory (UL) regulations and recommendations for USA/Canada.

The presence of this symbol in or on Grass Valley equipment means that it has been tested and certified as complying with applicable Intertek Testing Services regulations and recommendations for USA/Canada.

The presence of this symbol in or on Grass Valley product means that it complies with all applicable European Union (CE) directives.

The presence of this symbol in or on Grass Valley product means that it complies with safety of laser product applicable standards.

Warnings

A warning indicates a possible hazard to personnel, which may cause injury or death. Observe the following general warnings when using or working on this equipment:

- Appropriately listed/certified mains supply power cords must be used for the connection of the equipment to the rated mains voltage.
- This product relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker for the rated mains voltage is used on the phase conductors.
- Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only.
- Do not operate the equipment in wet or damp conditions.
- This equipment is grounded through the grounding conductor of the power cords. To avoid electrical shock, plug the power cords into a properly wired receptacle before connecting the equipment inputs or outputs.
- Route power cords and other cables so they are not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.
- Disconnect power before cleaning the equipment. Do not use liquid or aerosol cleaners; use only a damp cloth.
- Dangerous voltages may exist at several points in this equipment. To avoid injury, do not touch exposed connections and components while power is on.
- High leakage current may be present. Earth connection of product is essential before connecting power.
- Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.
- To avoid fire hazard, use only the fuse type and rating specified in the service instructions for this product, or on the equipment.
- To avoid explosion, do not operate this equipment in an explosive atmosphere.
- Use proper lift points. Do not use door latches to lift or move equipment.
- Avoid mechanical hazards. Allow all rotating devices to come to a stop before servicing.
- Have qualified service personnel perform safety checks after any service.

Cautions

⚠️ A caution indicates a possible hazard to equipment that could result in equipment damage. Observe the following cautions when operating or working on this equipment:

- This equipment is meant to be installed in a restricted access location.
- When installing this equipment, do not attach the power cord to building surfaces.
- Products that have no on/off switch, and use an external power supply must be installed in proximity to a main power outlet that is easily accessible.
- Use the correct voltage setting. If this product lacks auto-ranging power supplies, before applying power ensure that each power supply is set to match the power source.
- Provide proper ventilation. To prevent product overheating, provide equipment ventilation in accordance with the installation instructions.
- Do not operate with suspected equipment failure. If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.
- To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel.
- This unit may have more than one power supply cord. Disconnect all power supply cords before servicing to avoid electric shock.
- Follow static precautions at all times when handling this equipment. Servicing should be done in a static-free environment.
- To reduce the risk of electric shock, plug each power supply cord into separate branch circuits employing separate service grounds.

Electrostatic Discharge (ESD) Protection

⚠️ Electrostatic discharge occurs when electronic components are improperly handled and can result in intermittent failure or complete damage adversely affecting an electrical circuit. When you remove and replace any card from a frame always follow ESD-prevention procedures:

- Ensure that the frame is electrically connected to earth ground through the power cord or any other means if available.
- Wear an ESD wrist strap ensuring that it makes good skin contact. Connect the grounding clip to an *unpainted surface* of the chassis frame to safely ground unwanted ESD voltages. If no wrist strap is available, ground yourself by touching the *unpainted* metal part of the chassis.
- For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms.
- When temporarily storing a card make sure it is placed in an ESD bag.
- Cards in an earth grounded metal frame or casing do not require any special ESD protection.

Battery Handling

This product may include a backup battery. There is a danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. To dispose of used batteries and/or your Grass Valley equipment, please consult your local goods disposal and recycling program.

Cautions for LCD and TFT Displays

Excessive usage may harm your vision. Rest for 10 minutes for every 30 minutes of usage.

If the LCD or TFT glass is broken, handle glass fragments with care when disposing of them. If any fluid leaks out of a damaged glass cell, be careful not to get the liquid crystal fluid in your mouth or skin. If the liquid crystal touches your skin or clothes, wash it off immediately using soap and water. Never swallow the fluid. The toxicity is extremely low but caution should be exercised at all times.

Mesures de sécurité et avis importants

La présente section fournit des consignes de sécurité importantes pour les opérateurs et le personnel de service. Des avertissements ou mises en garde spécifiques figurent dans le manuel, dans les sections où ils s'appliquent. Prenez le temps de bien lire les consignes et assurez-vous de les respecter, en particulier celles qui sont destinées à prévenir les décharges électriques ou les blessures.

Signification des symboles utilisés

Signale la présence d'une tension élevée et dangereuse dans le boîtier de l'équipement ; cette tension peut être suffisante pour constituer un risque de décharge électrique.

Avertit l'utilisateur, l'opérateur ou le technicien de maintenance que des instructions importantes relatives à l'utilisation et à l'entretien se trouvent dans la documentation accompagnant l'équipement.

Invite l'utilisateur, l'opérateur ou le technicien de maintenance à prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait référence dans le texte doit être remplacé par un fusible du même calibre.

Identifie une borne de mise à la terre de protection. Il faut relier cette borne à la terre avant d'effectuer toute autre connexion à l'équipement.

Identifie une borne de mise à la terre externe qui peut être connectée en tant que borne de mise à la terre supplémentaire.

Signale la présence de composants sensibles à l'électricité statique et qui sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

Le symbole ci-contre signifie que l'appareil comporte plus d'un cordon d'alimentation et qu'il faut débrancher tous les cordons d'alimentation avant toute opération d'entretien, afin de prévenir les chocs électriques.

La marque UL certifie que l'appareil visé a été testé par Underwriters Laboratory (UL) et reconnu conforme aux exigences applicables en matière de sécurité électrique en vigueur au Canada et aux États-Unis.

La marque C-CSA-US certifie que l'appareil visé a été testé par l'Association canadienne de normalisation (CSA) et reconnu conforme aux exigences applicables en matière de sécurité électrique en vigueur au Canada et aux États-Unis.

La marque C-UL-US certifie que l'appareil visé a été testé par Underwriters Laboratory (UL) et reconnu conforme aux exigences applicables en matière de sécurité électrique en vigueur au Canada et aux États-Unis.

La marque ETL Listed d'Intertek pour le marché Nord-Américain certifie que l'appareil visé a été testé par Intertek et reconnu conforme aux exigences applicables en matière de sécurité électrique en vigueur au Canada et aux États-Unis.

Le marquage CE indique que l'appareil visé est conforme aux exigences essentielles des directives applicables de l'Union européenne en matière de sécurité électrique, de compatibilité électromagnétique et de conformité environnementale.

Le symbole ci-contre sur un appareil Grass Valley ou à l'intérieur de l'appareil indique qu'il est conforme aux normes applicables en matière de sécurité laser.

Avertissements

Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire fatales. Veuillez vous familiariser avec les avertissements d'ordre général ci-dessous :

- Un cordon d'alimentation dûment homologué doit être utilisé pour connecter l'appareil à une tension de secteur de 120 V CA ou 240 V CA.

- La protection de ce produit contre les courts-circuits (surintensités) dépend de l'installation électrique du bâtiment. Assurez-vous qu'un fusible ou un disjoncteur pour 120 V CA ou 240 V CA est utilisé sur les conducteurs de phase.

- Dans le présent manuel, toutes les instructions qui nécessitent d'ouvrir le couvercle de l'équipement sont destinées exclusivement au personnel technique qualifié.

- N'utilisez pas cet appareil dans un environnement humide.

- Cet équipement est mis à la terre par le conducteur de mise à la terre des cordons d'alimentation. Pour éviter les chocs électriques, branchez les cordons d'alimentation sur une prise correctement câblée avant de brancher les entrées et sorties de l'équipement.

- Acheminez les cordons d'alimentation et autres câbles de façon à ce qu'ils ne risquent pas d'être endommagés. Supportez correctement les enroulements de câbles afin de ne pas endommager les connecteurs.

- Coupez l'alimentation avant de nettoyer l'équipement. Ne pas utiliser de nettoyants liquides ou en aérosol. Utilisez uniquement un chiffon humide.

- Des tensions dangereuses peuvent exister en plusieurs points dans cet équipement. Pour éviter toute blessure, ne touchez pas aux connexions ou aux composants exposés lorsque l'appareil est sous tension.

- Avant de procéder à toute opération d'entretien ou de dépannage, enlevez tous vos bijoux (notamment vos bagues, votre montre et autres objets métalliques).

- Pour éviter tout risque d'incendie, utilisez uniquement les fusibles du type et du calibre indiqués sur l'équipement ou dans la documentation qui l'accompagne.

- Ne pas utiliser cet appareil dans une atmosphère explosive.

- Présence possible de courants de fuite. Un raccordement à la masse est indispensable avant la mise sous tension.

- Après tout travail d'entretien ou de réparation, faites effectuer des contrôles de sécurité par le personnel technique qualifié.

Mises en garde

Les mises en garde signalent des conditions ou des pratiques susceptibles d'endommager l'équipement. Veuillez vous familiariser avec les mises en garde ci-dessous :

- L'appareil est conçu pour être installé dans un endroit à accès restreint.

- Au moment d'installer l'équipement, ne fixez pas les cordons d'alimentation aux surfaces intérieures de l'édifice.

- Les produits qui n'ont pas d'interrupteur marche-arrêt et qui disposent d'une source d'alimentation externe doivent être installés à proximité d'une prise de courant facile d'accès.

- Si l'équipement n'est pas pourvu d'un modules d'alimentation auto-adaptables, vérifiez la configuration de chacun des modules d'alimentation avant de les mettre sous tension.

- Assurez une ventilation adéquate. Pour éviter toute surchauffe du produit, assurez une ventilation de l'équipement conformément aux instructions d'installation.

- N'utilisez pas l'équipement si vous suspectez un dysfonctionnement du produit. Faites-le inspecter par un technicien qualifié.

- Pour réduire le risque de choc électrique, n'effectuez pas de réparations autres que celles qui sont décrites dans le présent manuel, sauf si vous êtes qualifié pour le faire. Confiez les réparations à un technicien qualifié. La maintenance doit se réaliser dans un milieu libre d'électricité statique.

- L'appareil peut comporter plus d'un cordon d'alimentation. Afin de prévenir les chocs électriques, débrancher tous les cordons d'alimentation avant toute opération d'entretien.
- Veillez à toujours prendre les mesures de protection antistatique appropriées quand vous manipulez l'équipement.
- Pour réduire le risque de choc électrique, branchez chaque cordon d'alimentation dans des circuits de dérivation distincts utilisant des zones de service distinctes.

Protection contre les décharges électrostatiques (DES)

Une décharge électrostatique peut se produire lorsque des composants électroniques ne sont pas manipulés de manière adéquate, ce qui peut entraîner des défaillances intermittentes ou endommager irrémédiablement un circuit électrique. Au moment de remplacer une carte dans un châssis, prenez toujours les mesures de protection antistatique appropriées :

- Assurez-vous que le châssis est relié électriquement à la terre par le cordon d'alimentation ou tout autre moyen disponible.
- Portez un bracelet antistatique et assurez-vous qu'il est bien en contact avec la peau. Connectez la pince de masse à une *surface non peinte* du châssis pour détourner à la terre toute tension électrostatique indésirable. En l'absence de bracelet antistatique, déchargez l'électricité statique de votre corps en touchant une surface métallique *non peinte* du châssis.
- Pour plus de sécurité, vérifiez périodiquement la valeur de résistance du bracelet antistatique. Elle doit se situer entre 1 et 10 mégohms.
- Si vous devez mettre une carte de côté, assurez-vous de la ranger dans un sac protecteur antistatique.
- Les cartes qui sont reliées à un châssis ou boîtier métallique mis à la terre ne nécessitent pas de protection antistatique spéciale.

Manipulation de la pile

Ce produit peut inclure une pile de sauvegarde. Il y a un risque d'explosion si la pile est remplacée de manière incorrecte. Remplacez la pile uniquement par un modèle identique ou équivalent recommandé par le fabricant. Disposez des piles usagées et de tout équipement Grass Valley conformément aux instructions de votre programme de récupération local pour le recyclage des équipements électroniques.

Précautions pour les écrans LCD et TFT

Regarder l'écran pendant une trop longue période de temps peut nuire à votre vision. Prenez une pause de 10 minutes, après 30 minutes d'utilisation.

Si l'écran LCD ou TFT est brisé, manipulez les fragments de verre avec précaution au moment de vous en débarrasser. veillez à ce que le cristal liquide n'entre pas en contact avec la peau ou la bouche. En cas de contact avec la peau ou les vêtements, laver immédiatement à l'eau savonneuse. Ne jamais ingérer le liquide. La toxicité est extrêmement faible, mais la prudence demeure de mise en tout temps.

Environmental Information

European (CE) WEEE directive.

This symbol on the product(s) means that at the end of life disposal it should not be mixed with general waste.

Visit www.grassvalley.com for recycling information.

Grass Valley believes this environmental information to be correct but cannot guarantee its completeness or accuracy since it is based on data received from sources outside our company. All specifications are subject to change without notice.

If you have questions about Grass Valley environmental and social involvement (WEEE, RoHS, REACH, etc.), please contact us at environment@grassvalley.com.

Lithium Batteries

Battery Warning

<u>CAUTION</u>
This equipment contains a lithium battery.
There is a danger of explosion if this is replaced incorrectly.
Replace only with the same or equivalent type.
Dispose of used batteries according to the manufacturer's instructions.
Batteries **shall only** be replaced by trained service technicians.

Your Grass Valley equipment usually comes with at least one button battery located on the main printed circuit board. The batteries are used for backup and should not need to be replaced during the lifetime of the equipment.

Battery Disposal

Before disposing of your Grass Valley equipment, please remove the battery as follows:

1 Make sure the AC adapter / power Cord is unplugged from the power outlet.

2 Remove the protective cover from your equipment.

3 Gently remove the battery from its holder using a blunt instrument for leverage such as a screwdriver if necessary. In some cases the battery will need to be desoldered from the PCB.

4 Dispose of the battery and equipment according to your local environmental laws and guidelines.

> WARNING
> - Be careful not to short-circuit the battery by adhering to the appropriate safe handling practices.
> - Do not dispose of batteries in a fire as they may explode.
> - Batteries may explode if damaged or overheated.
> - Do not dismantle, open or shred batteries.
> - In the event of a battery leak, do not allow battery liquid to come in contact with skin or eyes.
> - Seek medical help immediately in case of ingestion, inhalation, skin or eye contact, or suspected exposure to the contents of an opened battery.

Laser Safety - Fiber Output SFP and QSFP Modules Warning

LASER SAFETY

CLASS 1 LASER PRODUCT

The average optical output power does not exceed 0 dBm (1mW) under normal operating conditions. Unused optical outputs should be covered to prevent direct exposure to the laser beam.

Even though the power of these lasers is low, the beam should be treated with caution and common sense because it is intense and concentrated. Laser radiation can cause irreversible and permanent damage of eyesight. Please read the following guidelines carefully:

- Make sure that a fiber is connected to the board's fiber outputs before power is applied. If a fiber cable (e.g. patchcord) is already connected to an output, make sure that the cable's other end is connected, too, before powering up the board.
- **Do not** look in the end of a fiber to see if light is coming out. The laser wavelengths being used are totally invisible to the human eye and can cause permanent damage. Always use optical instrumentation, such as an optical power meter, to verify light output.

Mains Supply Voltage

Before connecting the equipment, observe the safety warnings section and ensure that the local mains supply is within the rating stated on the rear of the equipment.

Safety and EMC Standards

This equipment complies with the following standards:

Safety Standards

Information Technology Equipment - Safety Part 1

EN60950-1: 2006

Safety of Information Technology Equipment Including Electrical Business Equipment.

UL1419 (4th Edition)

Standard for Safety – Professional Video and Audio equipment (UL file number E193966)

EMC Standards

This unit conforms to the following standards:

EN55032:2015 (Class A)

Electromagnetic Compatibility of multimedia equipment - Emission requirements

EN61000-3-2:2014 (Class A)

Electromagnetic Compatibility - Limits for harmonic current emissions

EN61000-3-3:2013

Electromagnetic Compatibility - Limits of voltage changes, voltage fluctuations and flicker

EN55103-2:2009 (Environment E2)

Electromagnetic Compatibility, Product family standard for audio, video, audio-visual and entertainment lighting control apparatus for professional use. Part 2. Immunity

> WARNING
> This equipment is compliant with Class A of CISPR 32. In a residential
> environment this equipment may cause radio interference.

FCC / CFR 47:Part 15 (Class A)

Federal Communications Commission Rules Part 15, Subpart B

Caution to the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

> Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.
> This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.
> Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EMC Performance of Cables and Connectors

Grass Valley products are designed to meet or exceed the requirements of the appropriate European EMC standards. In order to achieve this performance in real installations it is essential to use cables and connectors with good EMC characteristics.

All signal connections (including remote control connections) shall be made with screened cables terminated in connectors having a metal shell. The cable screen shall have a large-area contact with the metal shell.

SIGNAL/DATA PORTS

For unconnected signal/data ports on the unit, fit shielding covers. For example, fit EMI blanking covers to SFP+ type ports; and fit 75 Ω RF terminators to BNC type ports.

COAXIAL CABLES

Coaxial cables connections (particularly serial digital video connections) shall be made with high-quality double-screened coaxial cables such as Belden 8281 or BBC type PSF1/2M, Belden 1694A (for 3Gbps), and Belden 4794A (for 12Gbps).

D-TYPE CONNECTORS

D-type connectors shall have metal shells making good RF contact with the cable screen. Connectors having "dimples" which improve the contact between the plug and socket shells, are recommended.

Table of Contents

1 Introduction

Overview

The Grass Valley Sirius compact SDI routers are small and cost-effective, yet robust and reliable. All Sirius routers support full-broadcast specifications over SD-SDI, HD-SDI, and 3G-SDI, and single connector 12G-SDI. Additionally, Sirius routers support SDI related protocols such as 270Mb/s DVB-ASI and Canon 3G-SDI RAW. Sirius routers are re-clocking, non-blocking, and ready for any broadcast, production, or post production environment. Running Embedded Linux, Sirius routers support powerful HTTP control and monitoring. Each Sirius product contains an internal web server that allows immediate installation, configuration, and operation without requiring additional software. It offers a powerful user interface via any standard web browser. Sirius SDI routers are available in three configurations:

- SCR 1616-12G - supports single connector 12G-SDI, sixteen inputs and sixteen outputs
- SCR 3232-12G - supports single connector 12G-SDI, thirty two inputs and thirty two outputs
- SCR 6464-12G - supports single connector 12G-SDI, sixty four SDI inputs and sixty four outputs

Because of their compact sizes, Sirius SDI routers are ideal for space-sensitive applications such as mobile sports trucks, edit suites, corporate video installations, or live theatrical A/V rigs.

Sirius Features

The Sirius routers offer the following features for ease of use in a broad range of SDI applications and workflows:

- SCR 1616-12G, 3232-12G, and 6464-12G support for SD-SDI, HD-SDI, 3G-SDI, 6G-SDI and 12G-SDI (SMPTE-259/292/424/2081/2082)
- Firmware v3.0 and above supports dual and quad mode routing, allowing users to group together inputs and outputs for multiple cable applications like Dual Link, Quad HD, Quad split monitors, and even 8K video.
- Firmware v4.3 and above supports salvos, controlled from the Sirius router Web UI and the SCP2 panel.
- Automatic cable equalization and re-clocking
- Supports all embedded VANC and HANC ancillary information, including embedded audio
- Reference via BNC, passive loop, PAL/NTSC color black or Tri-level sync
- Output switch timing per SMPTE RP 168 when using an external reference
- 10/100/1000 Ethernet LAN

- Embedded Linux OS with internal web server for web browser control
- USB port for configuring IP addresses via AJA's eMini-Setup software
- User authorization to restrict access via web browser
- Optional SCP1 hardware 32 pushbutton remote control panel via Ethernet
- Optional SCP2 hardware 64 pushbutton remote control panel via Ethernet
- 1RU form factor for SCR 1616 and SCP1, 2RU for SCR 3232 and SCP2, 4RU for SCR 6464
- Sirius SDI Routers and Control Panels v4.6.1 6 www.aja.com
- Power loss recovery to the last operational state, both router and control panel
- Redundant power supply (optional), isolated power inputs

☞ **Note**

Sirius routers switch SDI signals in a manner compliant with SMPTE RP168-2009. Because Sirius routers (or any similar router) switch the SDI stream without de-serializing, the switch point can cause a temporary anomaly in the SDI stream. This can cause downstream equipment, depending on the characteristics of the SDI receiver(s), to react to the switch (for example, a monitor "glitch or roll"). It is also possible that switching anomalies can appear on just one or more outputs in the same group in the Dual and Quad modes and in salvos. This effect occurs regardless of the relative timing of the SDI signals being switched, or any reference input connected to the router.

Sirius Router Connections
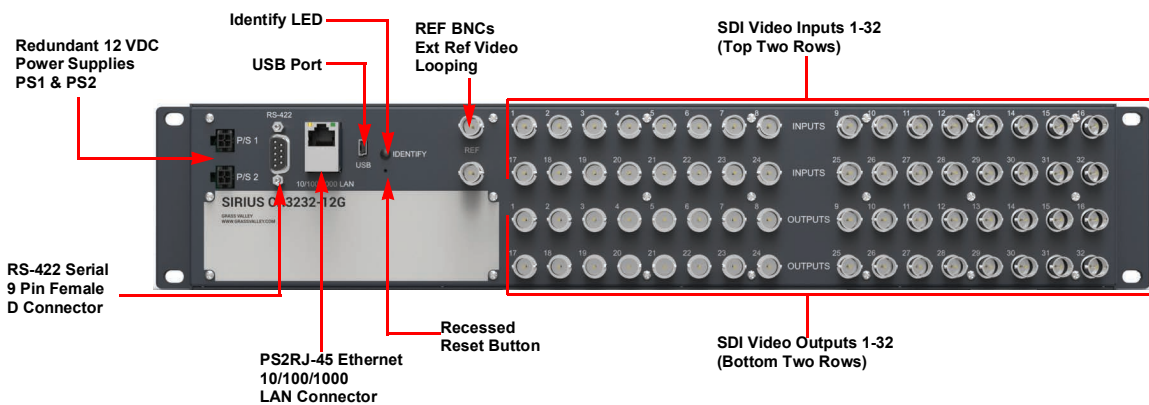
Fig. 1-1: SCR 3232-12G Rear Panel Connections (3232 shown, other models similar)

SCP1 & SCP2 Power Connectors

Power to the Sirius unit is supplied by an external power supply module that accepts a 110-240VAC, 50/60Hz power input and supplies +12 VDC to Sirius via connector PS1 or PS2. One power supply is provided, and it may be connected to either of the two power connectors. An optional second power supply can provide redundancy to help protect against outages.

⚠ **Caution**

The power connector has a latch, similar to an Ethernet connector. Depress the latch (facing the outside edge of the Sirius device) before disconnecting the power cable from the unit.

Power Loss Recovery

If Sirius experiences a loss of power, when power is restored the router returns to the previous state of all source to destination crosspoints, and all configured source and destination names are retained. If a Sirius control panel configured with a Sirius router loses power, when power is restored the control panel's configuration is retained, and button tallies will return to their previous states.

RJ-45 Ethernet Connector

The RJ-45 Ethernet connector allows you to connect Sirius to an Ethernet 10/100/1000 Ethernet LAN using CAT5 cable and access Sirius' built in web server. Multiple configurations are possible, including standalone control, a local LAN, or a WAN. This also allows control over the network using GVG Native Protocol.

ID and Reset

The ID (Identification) LED lights when you use the web interface to identify the Sirius unit you are controlling. The Reset button (pinhole) below the LED allows a safeboot reset of the unit as explained in Safeboot Reset, on page 34.

REF BNC Connector

The REF BNC connector is the looping input for synchronizing the crosspoint switch timing of Sirius to your house video signals. Apply an analog NTSC, PAL, or Tri-level sync signal to this input. Be sure to terminate the second BNC with a 75 Ohm terminator, or if you loop to other equipment terminate the last connected device.

When reference is present, Sirius will switch at the SMPTE RP168 designated switch point with respect to the reference input. If no reference is present, the Sirius will switch at random times.

Video Inputs and Outputs

Depending on your Sirius model, up to 64 SDI video inputs and outputs can be connected to the video input and output BNC connectors.

Normal Mode

In Normal mode, BNC inputs and outputs have a one-to-one relationship with the SDI signals being routed.

Dual and Quad Modes

In Dual mode, inputs and outputs use adjacent pairs of BNCs for each routed signal. In Quad mode, four adjacent BNCs are used for each routed signal. See Mode Selection, on page 25.

RS-422 Connector

Sirius includes an RS-422 female DB-9 connector for making serial connections to other equipment. This control connection enables interoperability with other devices, including those that use GVG Native Protocol. See RS-422 Control Specifications (Routers), on page 58 for more information.

Sirius Control Panel Connections

Similar to the Sirius router, Sirius control panel has an RJ-45 Ethernet connector and power supply connectors, but has no BNC connectors and no RS-422 port.

Sirius Control and Monitoring

The Sirius router user-interface provides powerful remote setup, control, and monitoring with:

- Zero-configuration Bonjour Protocol and support for UPnP networking protocols
- Remote web browser control interface via Ethernet
- Optional SCP1 (32 buttons) and SCP2 (64 buttons) hardware control panels, each unit able to control up to four Sirius routers

☞ **Note**

The 32 buttons Sirius SCP1 hardware control panel can be used with a Sirius SCR 6464 router operating in Normal mode, but can only control the first 32 Inputs and Outputs. The Sirius SCP1 can be used to fully control an SCR 6464 that is operating in Dual or Quad mode. Control of Sirius routers in all modes is available via the Sirius SCP1 and SCP2 button hardware panel, web browser, Ethernet control, and RS-422.

- GVG Native Protocol built-in to allow serial or LAN interconnection (one RS-422 or up to ten Ethernet) and interoperability with other equipment. Specifically, Sirius can be controlled by the SMS 7000 portion of the GVG Native Protocol. For details, refer to: GVG Native Protocol Support, on page 57

Default Network Settings

Sirius routers and control panels ship with DHCP enabled, making system operation possible simply by connecting the Sirius device's Ethernet cabling.

In addition, temporary default static IP addresses can be activated for initial Sirius system configuration. See Sirius Temporary Static IP Address, on page 11.

In This Manual

Chapter 1: Introduction lists features and gives a general description of the product.

Chapter 2: Installation details Sirius installation, connections, and networking configuration options.

Chapter 3: Web Browser User Interface provides complete instructions for controlling and monitoring the Sirius router from a computer.

Chapter 4: Sirius Remote Control Panel details the configuration and operation of the optional Sirius Control Panel.

Appendix A: Specifications lists technical specifications for the product.

Contact Information

Installation

Overview

Sirius SDI routers are easy to set up and use. All of the steps for Sirius installation and configuration are documented in this chapter, summarized as follows:

1 Install the chassis in an appropriate rack. If you are mounting multiple Sirius units, try to place them visually in the same area so if you communicate with them via a network attached computer, you can use the Sirius' Identify feature to flash the corresponding LED of the unit you are communicating with. Ensure you have an Ethernet cable routed to where the Sirius will be placed.

2 Assemble the Ethernet network connections to a closed network or LAN using Cat 5 Ethernet cable and any required switches and hubs.

3 Connect the Sirius to power, connecting the power cord to mains AC.

4 If necessary, configure device network settings for operation in your facility.

5 Cable the system SDI video source and destination equipment and reference signals.

6 If operating with Dual Link or Quad Link signals, select the appropriate Sirius operating mode.

⚠️ **WARNING**

Do not defeat the safety purpose of the grounding-type plug

⚠️ **Caution**

To meet safety regulations for leakage current when using redundant power supplies, connect the Sirius dual power supplies to separate branch circuits

What Is In The Box?

When you unpack your Grass Valley Sirius SDI device, you will find the following components:

- Sirius SDI router or Sirius control panel
- AC adapter and AC power cord
- Please save all packaging for shipping Sirius should you wish to do so when moving or sending it in for service.

Sirius Chassis Installation

Space Requirements

When planning equipment locations and mounting methods, take into account the size of the chassis. Sirius devices are designed for EIA 19" equipment rack mounting. See Specifications, on page 53 for exact dimensions of each router model.

Plan adequate space for cable routing from the back of the router chassis. Ensure that SDI video cable connectors will not be stressed and that cables are not bent or crimped in the process.

Cooling Requirements

When rack mounting or stacking multiple Sirius chassis, ensure there is adequate airspace for cooling around the Sirius units. Note the location of cooling vents on all equipment next to the Sirius and ensure none are obstructed.

Power Requirements

- Input Voltage: 110-240VAC, 50/60Hz
- Optional redundant power supply

⚠ **Caution**

Sirius is designed to take advantage of its chassis to aid in cooling. It is common and expected for the densely populated chassis to have a warm front panel in normal, active operating conditions.

⚠ **WARNING**

Do not open the chassis. There are no user-serviceable parts inside. Opening the chassis will void the warranty unless performed by a Grass Valley service center or licensed facility. Remove the brick power supply AC line cord(s) from mains power when moving the unit.

Physical Equipment Setup

1 Connect power supplies (1 or 2 for redundancy) to Sirius routers and control panels.

☞ **Note**

The power connector has a latch, similar to an RJ-45 Ethernet connector. Depress the latch (facing the outside edge of the Sirius device) before disconnecting the power cable from the unit.

2 Connect source and destination SDI equipment (this step can be deferred).
3 Connect network:

- Direct Connection: connect a Sirius router to a Sirius control panel (if used), or to a Mac or PC, via an Ethernet Cable.
- LAN Connection: connect a Sirius router (and a Sirius control panel if used) to a hub or switch and connect a PC or Mac to the same LAN via a hub or switch.

☞ **Note**

Sirius devices are compatible with both Cat 5 straight-through and cross-over Ethernet cables—they automatically detect whichever is used.

4 Proceed to your desired network configuration method using one of the procedures presented later in the chapter.

Quick Start Configuration

Default Auto Configure Sirius Router and Control Panel

If you purchased a Sirius control panel along with a Sirius router, the easiest way to get your system operating is to simply direct connect them with a single Ethernet cable and power up both units.

☞ **Note**

The SCR 6464 router in Normal mode (64 sources and destinations) can be fully controlled with the newer Sirius SCP2. The original 32 button Sirius SCP1 hardware control panel can fully control an SCR 6464 router operating in Dual or Quad mode. A 32 button Sirius SCP1 can control first 32 Inputs and Outputs of an SCR 6464 router operating in Normal mode.

Sirius devices are compatible with both Cat 5 straight-through and cross-over Ethernet cables. The Sirius control panel (CP) will use an Auto Configure function to set itself up to operate with the Sirius router it is directly connected to. The Sirius CP panel buttons will light and, if SDI BNC connections have been made, you will be able to route sources to destinations.

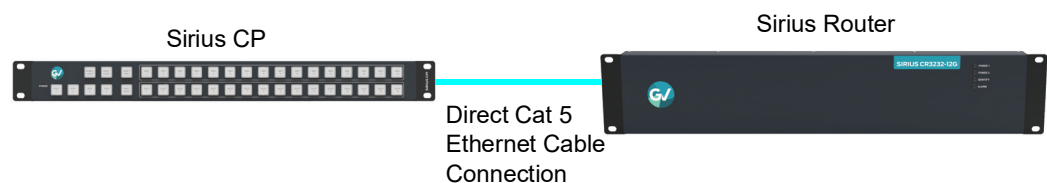Fig. 2-1: Sirius Router Direct Connection to Sirius CP

The Sirius CP Auto Configure assigns Router Select Button 1 to the attached router.

☞ **Note**

A Sirius CP that has had its network settings configured previously will not use automatic configuration to find a directly connected Sirius router. However, you can force the Sirius CP

to enter into Auto Configuration Mode by pressing the **RTR 1** and **SHIFT DEST** buttons simultaneously for four seconds.

DHCP on an Existing Network

Another easy way to get your Sirius system operating is to connect Sirius routers to an existing network configured with a DHCP server. When the units reset during power up, they will see the DHCP server and automatically be given compatible IP network settings. If auto discovery is configured on a computer on that network, that computer will be able to find and control the Sirius router via a web browser (see below).

Computer Auto Discovery

Computers can support network auto discovery, which makes the network configuration process easy. Two methods of connecting using this technique are described below.

Older macOS Configuration with Safari Browser Using Bonjour

MacOS Safari browser versions 10 and earlier have Bonjour functionality built-in, which can be used to auto-detect and connect to an Ethernet device like a Sirius router.

☞ **Note**

Apple removed Bonjour support from Safari versions 11 and higher.

To find a Sirius router using Bonjour on a supported version of Safari:

1 Ensure the Sirius to be controlled is powered up and connected via Ethernet (directly to a Mac or via LAN).
2 Start Safari browser on a Mac.
3 Click on the top menu **Bookmark > Bonjour > Webpages** drop-down and click on a listed Grass Valley Sirius router or control panel.

☞ **Note**

If Bonjour is not visible in the Bookmark drop-down, go to **Safari > Preferences > Advanced** and check the "Include Bonjour in the Bookmarks menu" checkbox.

4 Safari will display the Sirius web user-interface, which you can use to control and configure that Sirius device.

Windows PC Configuration using UPnP

If your Windows PC supports UPnP protocols (most do) and UPnP network discovery service is enabled (refer to your Microsoft Windows documentation), you can control Sirius routers by simply selecting one from a device list:

1 Ensure the Sirius to be controlled is powered up and connected via Ethernet (directly to the PC or via LAN).

2 Use your Windows Control Panel or File Explorer to go to **Computer > Network**.

3 Look at the list under "Other Devices"—double click a Sirius' name to launch your Windows PC's default browser.

4 The browser will display the Sirius web user-interface, which you can use to control and configure that Sirius device.

Network Configuration via USB

Sirius devices equipped with USB ports can configured for network operation using AJA's eMini-Setup utility program. The general procedure is:

1 Acquire eMini-Setup from the AJA website and install the eMini-Setup application onto a computer.

2 Connect the Sirius to that computer's USB port.

3 Launch the eMini-Setup application.

4 Go to the Network tab where the IP address settings are displayed. You can use the existing DHCP assigned IP address, or it can be changed manually.

See eMini-Setup, on page 45 for additional information.

Sirius Temporary Static IP Address

Sirius devices also offer a factory default static IP address, allowing a direct and fail-safe way to connect via a computer connected to Sirius either directly or via a LAN connection. The computer you use will need to be set to a static IP address that is compatible with the Sirius temporary IP address. Once connected, the Sirius device's network settings can be reconfigured to work with your facility network. The Sirius default static IP address is temporary and is intended only to allow an initial connection.

☞ **Note**

All Sirius routers and control panels have the same temporary static IP address, so more than one device set to this default cannot reside on the same network simultaneously. Work with only one device at a time.

Device	IP address	Subnet Mask
Sirius Router and Sirius CP	192.168.101.1	255.255.255.0

Table 2-1.   Sirius Device Temporary Static IP Address Values

☞ **Note**

The default static address is temporary and will be disabled the next time Sirius restarts. Any changes in the Network configuration will be saved upon restart.

To set Sirius to its temporary static IP address:

1 Power up the Sirius device and wait for it to boot normally.

2 Set the Sirius device to its static IP address:

- For a Sirius router, insert a straightened paper clip or similar device into the reset slot on the rear and hold for five seconds and then release. The Sirius will restart with the default IP. When the Sirius router default IP is set the Identify LED will blink.

- For a Sirius SCP1/SCP2, press and hold the two SHIFT buttons on the panel for five seconds and then release. When the Sirius CP default IP is set, the Source and Destination buttons will flash alternately.

☞ **Note**

If a Sirius webpage on a computer is open when that Sirius device is reset, the information displayed on the webpage is not updated automatically.
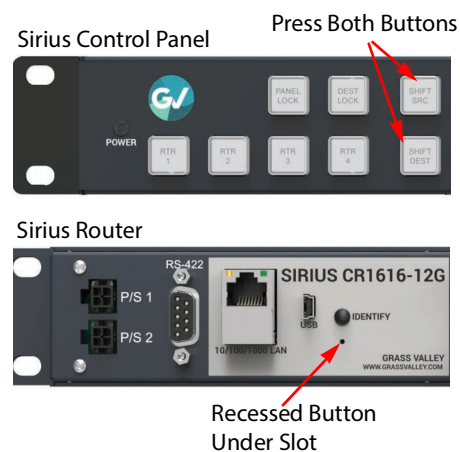

Fig. 2-2: Sirius Router and Sirius Control Panel Default Static IP Setting

☞ **Note**

Be sure to record your computer's existing TCP-IP settings before the next step so that you can return the computer to normal operation after this procedure.

3 Configure your computer to 192.168.101.X. Do not use .1 at the end of the address to avoid duplicate IP addresses.

4 Start a web browser and enter 192.168.101.1 as the web address. This is the Sirius temporary static IP address.

5 Once you have connected using the static IP, you can then enter a desired network configuration using the Sirius device's Network tab.

Network Configuration In Depth

A LAN is a shared network that includes other Ethernet devices all attached via a hub or digital switch. LANs may be divided into zones separated by software or hardware routers. Routers may also be used to connect the LAN to an outside wide area network (WAN) such as the Internet. Devices on a LAN have IP addresses which may be fixed and permanent, or dynamically assigned by the network (DHCP with DNS server).

Note

Once connected and properly configured, the Sirius router can then be controlled by a web browser or one or more Sirius SCP1 control panels. Sirius routers and Sirius CP are equipped with zeroconf (Bonjour) and support UPnP networking protocols but initially start up as DHCP active devices. If you are operating on a DHCP server, Sirius will take an assigned IP address and appear on the network.

Caution

When attaching Sirius to a standard static IP LAN, you must configure Sirius components with a new, unique IP address. You should first talk to your network administrator and find out how it should be connected (TCP/IP Static IP or DHCP). Your IT department will be able to supply the information you need to install Sirius on a LAN.

Sirius uses TCP-IP network communications and Ethernet connections (a 10/100/1000 Ethernet port) for crosspoint control, status monitoring, and software updates. Sirius devices have an internal HTTP web server that works with a standard web browser on a Mac or PC. An Ethernet cable can also be used to connect an optional Sirius CP (control panel) directly to a Sirius router for operation without a computer.

Sirius devices are compatible with both Cat 5 straight-through and cross-over Ethernet cables—they automatically detect whichever is used.

Sirius internal HTTP networking software supports three levels of network control:

 • Closed Sirius network – uses Default Auto Configure (Sirius CP), or Bonjour (Mac or PC).
 • Auto Configured LAN – employs a Bonjour or UPnP enabled computer/browser to automatically connect devices and allows Sirius web browser User Interface (UI).
 • Standard TCP-IP network – employs DHCP or Static IP addressing and allows the Sirius web-based UI and an unlimited number of Sirius routers and up to 32 Sirius CP control points.

The following web browsers have been tested and approved for use with Sirius (Bonjour capability is recommended):

 • Firefox - latest version on all platforms
 • Safari - latest version on Mac and Windows
 • Internet Explorer - version 10 and higher on Windows
 • Chrome - latest version on all platforms (Bonjour is supported)

Once connected, you can use a web browser to:

 • Configure any TCP/IP settings

- Select and name Sirius routers and control panels
- Assign a Sirius panel to be able to control specific Sirius routers
- Name sources and destinations
- Make Source to Destination assignments (signal routing)
- Change router operating mode (Normal, Dual Mode, Quad Mode)
- Set a variety of operational and monitoring options

LAN Connection Using a Hub or Switch

In a LAN connection, connect one or more Sirius routers to your LAN or closed network using Cat 5 Ethernet cable and an Ethernet hub or switch; then power up the equipment.
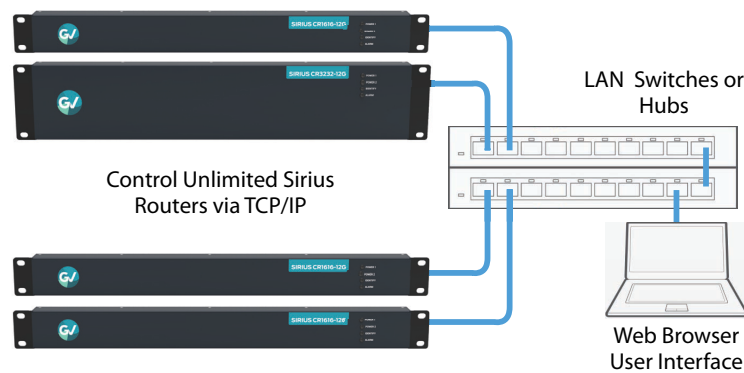

Fig. 2-3: Sirius Routers on LAN with Web Browser UI

Setup and Control Methods

Regardless of direct connection or LAN connection, Sirius are controlled over a network by connecting to Sirius' internal web server with a standard web browser on a Mac or PC. To do this you first need to establish a network connection between the computer and the Sirius to be controlled. There are various methods supported for doing this depending on the operating system and/or web browser being used.

When using Sirius in a DHCP or Static IP addressed network, it is best to select and maintain a consistent network scheme. If you use a mix of DHCP and Static IP addresses, inconsistent performance can result. The most stable operation is achieved when all IP addressing is either DHCP or Static.

Setup and Control from a Browser on macOS

Safari Browser: Type in Sirius Static IP Address

Sirius offers a factory default static IP address. The default static IP address is temporary and is intended only to allow an initial connection. Once you have connected using the static IP, you can then enter a desired network configuration using Sirius' Network tab.

☞ **Note**

The default static address is temporary and will be disabled the next time Sirius restarts. Any changes in the Network configuration will be saved upon restart.

1 Set the Sirius to its factory default IP address. See Sirius Temporary Static IP Address, on page 11 for this procedure.

2 Configure your computer to communicate on the 192.168.101.X subnet as shown below:

☞ **Note**

First record existing TCP-IP settings so that you can return your computer to normal operation after this procedure.

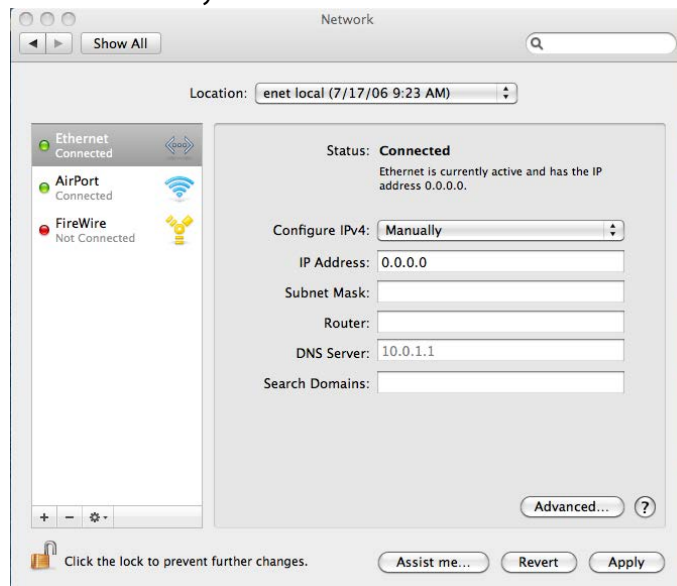a Go to your **System Preferences > Network** and select Ethernet and Configure: Manually.

Fig. 2-4: Mac Network Setup Screen (System Preferences > Network)

b Input the address information shown below:
- IP Address: 192.168.101.X (do not use .1 in the last octet).
- Subnet Mask: 255.255.255.0

      c Click Apply.

3 Ensure the Sirius device to be controlled is connected to the Mac via Ethernet (directly or via LAN).

4 Start Safari and enter 192.168.101.1 as the web address. This is the Sirius temporary static IP address.

5 Once you have connected to Sirius' web interface, reconfigure Sirius' network parameters as desired using the Sirius device's Network tab.

6 Restore your computer to its normal network settings using this procedure and the IP addresses you recorded earlier.

Setup and Control from a Browser on Windows

The easiest methods of setting up a controlling a Sirius device from a PC running Windows are:

- Setup and Control from a Browser on Windows using UPnP
- Setup and Control from a Browser on Windows using a Static IP Address

Windows: Using UPnP (Universal Plug and Play)

This method was covered earlier in this chapter.

See Windows PC Configuration using UPnP, on page 10.

Windows Browser: Type in Sirius Static IP Address

Sirius offers a factory default static IP address. The default static IP address is temporary and is intended only to allow an initial connection. Once you have connected using the static IP, you can then enter a desired network configuration using Sirius' Network tab.

☞ **Note**

The default static address is temporary and will be disabled the next time Sirius restarts. Any actual changes made to Sirius' Network configuration will be saved and used upon restart.

---

1 Set the Sirius to its factory default IP address. See Sirius Temporary Static IP Address, on page 11 for this procedure.

2 Configure your computer to 192.168.101.X as shown below (this example is for a PC running Windows 7 connected directly to Sirius, other Windows versions use similar procedures):

    a Use Control Panel to access your Local Area Network properties. In Windows 7 the path is:

        - **Control Panel** > **Network and Sharing Center**

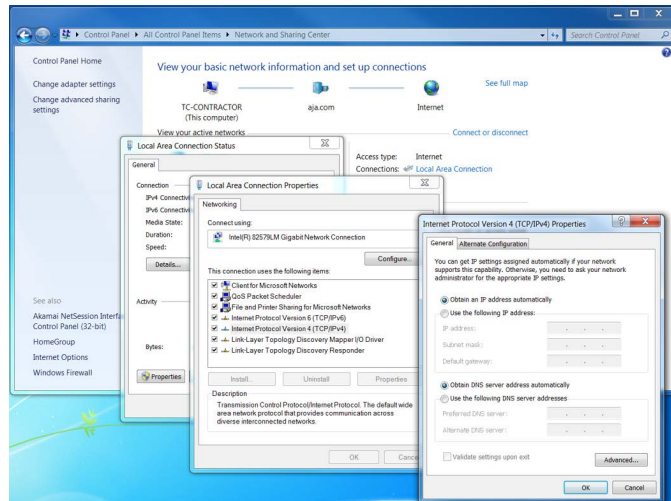b   Then, under "Connections" click on the Local Area Connection for the PC's Ethernet port.

Fig. 2-5: Windows 7 Network Configuration Screens

c   In the resulting General dialog screen, select the Properties button.

d   Then on the Networking tab, select Internet Protocol Version 4 and click the Properties button below.

✎ **Tip**

Record your computer's existing TCP-IP settings. You will later need to restore these original settings so that you can return your computer to normal operation after this procedure.

e   Finally, click the "Use the following IP address:" radio button and enter the IP Address and Subnet Mask below:

- IP Address: 192.168.101.X (do not use .1 in the last octet).
- Subnet Mask: 255.255.255.0
- Click the OK button to store the changes.

3   Connect the Windows PC to Sirius' RJ-45 port (either direct or through your LAN)

4   Point your web browser to 192.168.101.1 as the web address. This is the Sirius temporary static IP address.

5   Once you have connected to Sirius' web interface, reconfigure Sirius' network parameters as desired using the Sirius device's Network tab.

6   Restore your computer to its normal network settings using this procedure and the IP addresses you recorded earlier.
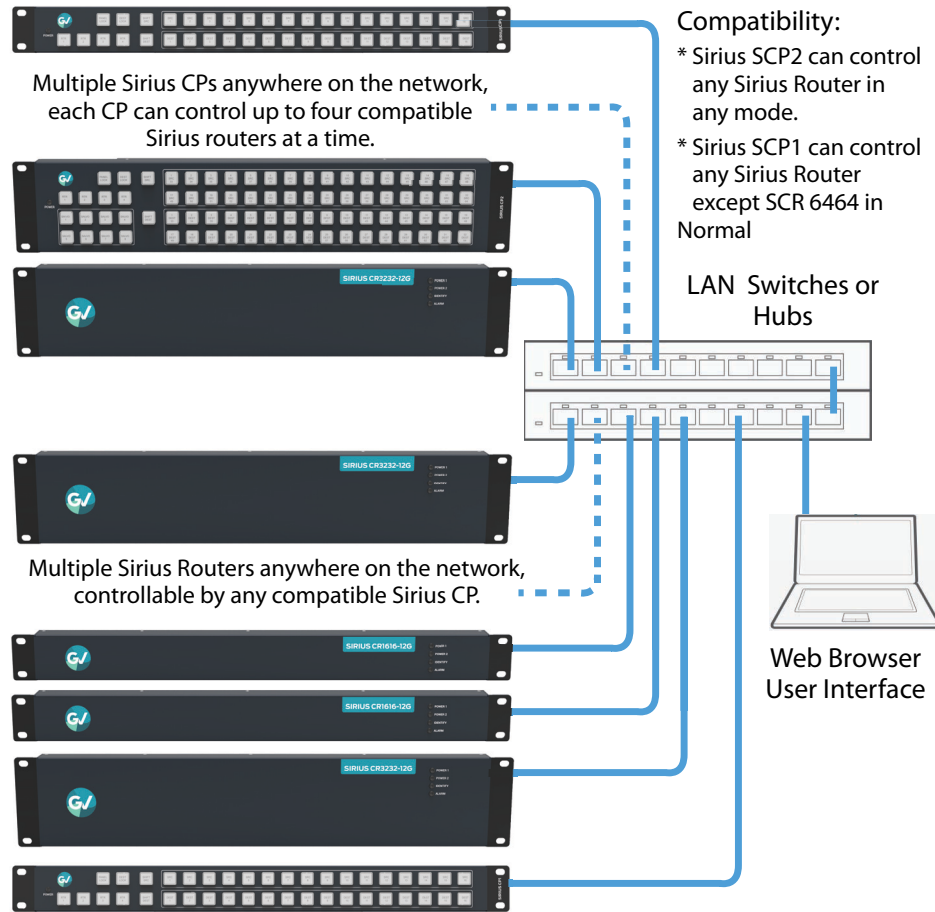
Larger System Control Configurations

Fig. 2-6: Multiple Sirius Routers and Sirius CPs with Web Browser UI Control.

☞ **Note**

The 32 buttons Sirius SCP1 hardware control panel cannot be used with an SCR 6464 router operating in Normal mode (only 32 buttons for 64 sources and destinations). However the Sirius SCP1 can be used when the SCR 6464 is operating in Dual or Quad mode. Control of the SCR 6464 router in all modes is available via the Sirius SCP2 64 buttons hardware panel, web browser, Ethernet control, and RS-422.

If the Sirius will be attached to a WAN, talk to your IT administrator and obtain the details on how to configure the Sirius (DHCP or static IP).

TCP-IP Network Connection

Sirius supports traditional TCP-IP networking through DHCP or Static IP addressing.

✎ **Tip**

When using Sirius in a DHCP or Static IP addressed network, it is best to select and maintain a consistent network scheme. If a mixture of DHCP and Static IP addresses are used, inconsistent performance can result. The most stable operation is achieved when all IP addressing is either DHCP or Static.

Default DHCP Configuration

DHCP is the default initial configuration routine for Sirius devices. If you start up on a DHCP network, Sirius will accept assigned IP addresses. After DHCP initialization, use your zeroconf browser to view the Sirius web page and view the assigned IP address.

Static IP Configuration

If your IT administrator prefers an assigned IP address that is fixed (called a "Static IP), you will need to set network parameters using the Sirius UI Network screen where you will enter:

- IP address type—Static IP
- a unique IP address
- the Subnet Mask and default gateway IP address (your LAN's router that does the network's routing)

You will need to press the Enter key on the keyboard for every field changed. Press the Update Network Settings button when all fields are complete.
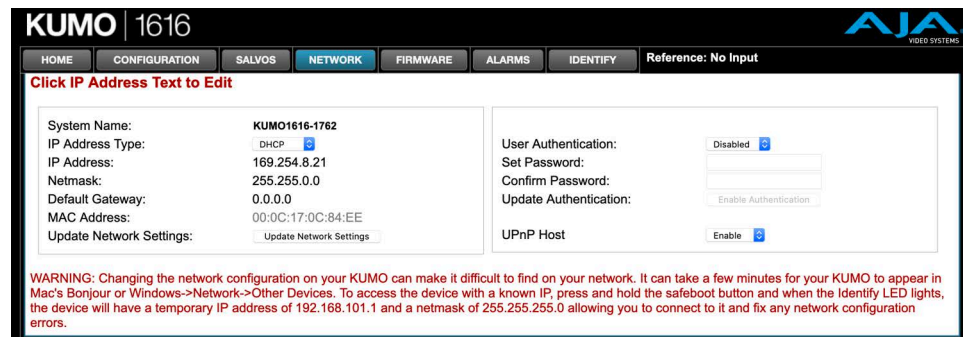

Fig. 2-7: Sirius User Interface Network Tab

Select Sirius to Control from Web Page

Each Sirius device has a built in web server that generates a web page. Sirius devices see each other on the network and list those other Sirius devices in their web pages. From the Home screen, use the pull-down menu in the upper left to see all of the Sirius devices

present on the local LAN and select the router you want to control, or select the Sirius control panel you want to use.
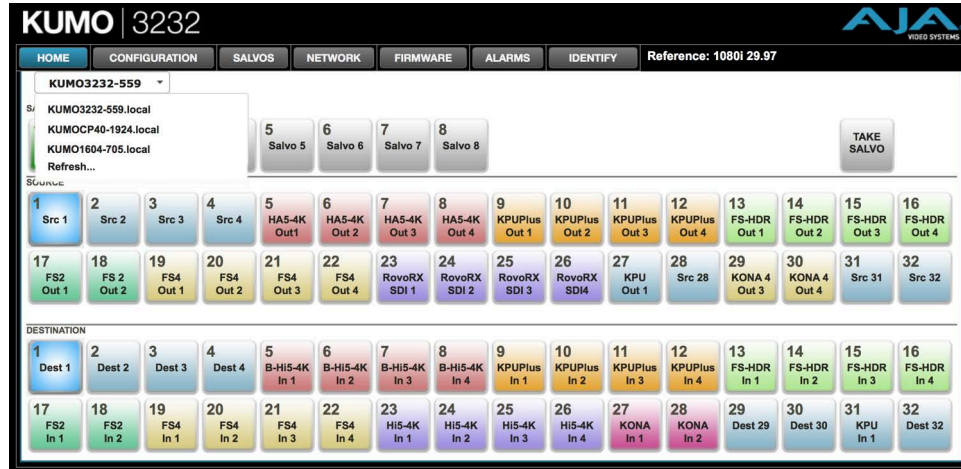

Fig. 2-8: Sirius Router Selection

Assign Sirius SCP1 and SCP2 to Control Sirius Routers

With multiple Sirius routers and Sirius control panels on the same network, you can assign which routers are able to be controlled by a panel by configuring the four Router Select buttons on the panel. On the Sirius control panel webpage, go to the Home screen, click on the box below the RTR button, and select the Sirius router from the drop-down list.

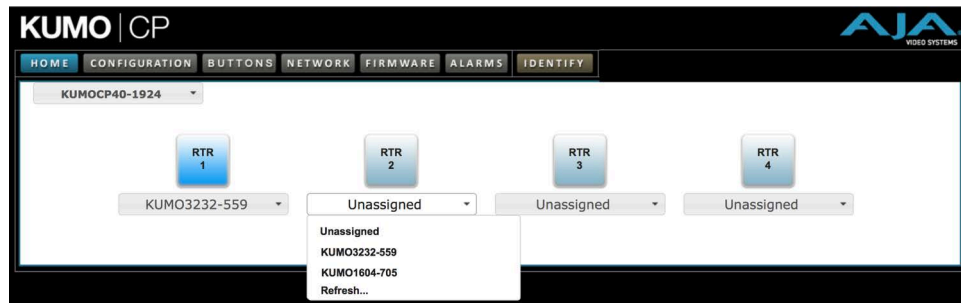*Fig. 2-9: Sirius Control Panel Router Button Assignment*

Locating a Specific Sirius Device on the Network

Identify Button

Click on the Web UI Identify button to find the physical location of the currently controlled Sirius router or panel.

The web browser button will alternate between blue and gray background color in Identify mode. Click again to turn the Identify function off.

- On a Sirius router, the Identify LEDs on the front and back will flash, enabling quick physical location of the router in a populated rack of equipment.
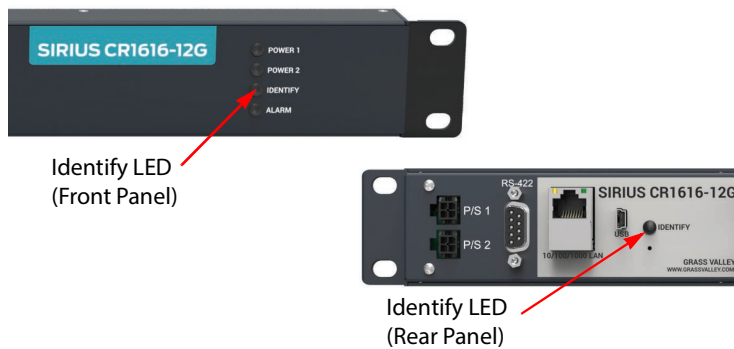- On a Sirius CP, the Source and Destination button rows will flash alternately

Identify LED
(Front Panel)

Identify LED
(Rear Panel)

Fig. 2-10: Sirius Router Identify LEDs.

Router Web Browser User Interface

Overview

An optimized web server inside the Sirius allows you to remotely monitor and adjust parameter settings via a network-attached computer running a web browser.

☞ **Note**

In this chapter SCR 3232 is used as the example. Other models will have different numbers of buttons.

Navigation Bar

The Sirius web browser user interface (UI) provides a navigational bar of tabs for access to control screens and the Identify toggle button:

- Home – control surface tab for salvo/source/destination selections
- Configuration – custom naming for sources and destinations, and mode selection
- Salvos – salvo configuration
- Network – IP settings for LAN/WAN operation and enabling authentication
- Firmware – update menu for Sirius software from AJA
- Alarms – log of service failures and allows alarms to be suppressed
- Identify – toggles activation of Identify LEDs for easy location of Sirius devices.

Fig. 3-1: Sirius Navigation Bar

Click any of the first six tabs to jump to that screen. To the right of the Identify button you will see the format of the Reference Video signal being used (if present).

Sirius Home Screen Device Selection

From the Home screen (Figure 3-2 on page 24), you can use the pull-down menu in the upper left to see all of the Sirius devices present on the local LAN and select the one you want to control or monitor.

Web Browser Control Surface Operation

On the Home screen immediately below the Sirius selection menu are the Salvo buttons, below them the Source buttons, and below them the Destination (output) buttons.

Click on any Destination button and it will highlight and its currently selected Source button will also be highlighted.

Fig. 3-2: Sirius Web Browser Home Screen (SCR 3232 Router)

☞ **Note**

In Configuration, you can hide Destination buttons that you do not want to control from this screen (see Hide, on page 27).

Performing a Take

1 Go to the Sirius router Home screen and select the router you wish to control with the drop down menu.

2 Press the desired Destination button. It will illuminate.

3 Press the desired Source button. That source will be routed to that destination and the Source button will illuminate.

☞ **Note**

Sources for locked Destinations cannot be changed.

Taking a Salvo

Up to eight salvos can be configured on a Sirius router. Each salvo can route any number of sources to any number of destinations, including the same source to multiple destinations. Paths not included in a salvo remain unchanged. Configured Salvo buttons are colored

green on the Home page. See Salvos Configuration, on page 28 to learn how to configure salvos.

Performing a salvo is a two stage process. First you arm the salvo, and then you take the salvo.

1 Go to the Sirius router Home screen and select the router you wish to control with the drop down menu.

2 Press the desired configured Salvo button. The **TAKE SALVO** button on the right will be colored red.

3 Press the **TAKE SALVO** button. All sources configured in that salvo will be routed to their destinations.

☞ **Note**

Salvos do not change locked Destinations.

Router Configuration

From the Configuration screen you can select the operating mode (Normal, Dual, Quad), change the Source and Destination names and the colors of the buttons, and Lock and Hide Destination buttons.
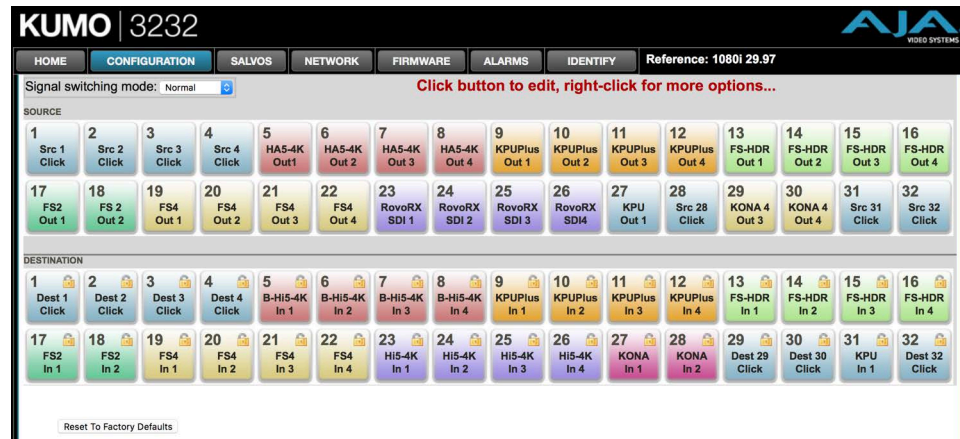

Fig. 3-3: Sirius Web Interface, I/O Configuration Screen

Mode Selection

Click on the Signal switching mode drop down list to select Normal, Dual, or Quad operating mode. When Dual or Quad mode is selected, the number of Source and Destination buttons will be reduced to match that configuration.
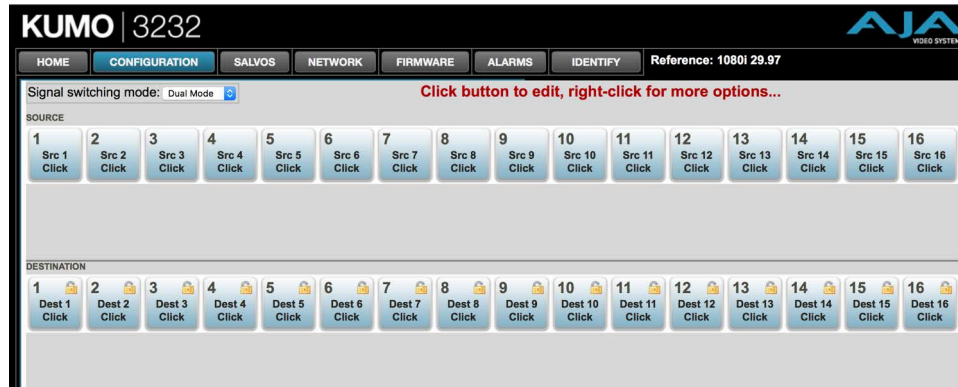
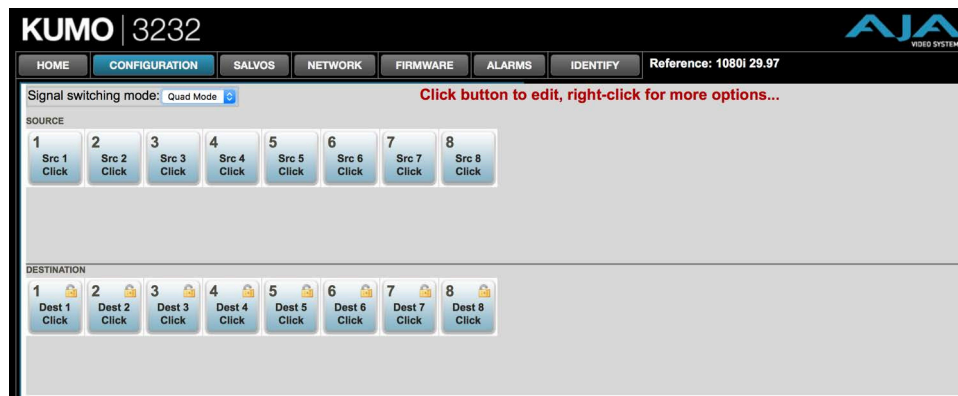*Fig. 3-4: Dual Mode Reduced Sources and Destinations*

Fig. 3-5: Quad Mode Reduced Sources and Destinations

In Dual and Quad modes adjacent BNCs are used for each routed signal.

Dual Mode					Quad Mode	
BNC #	Signal	BNC #	Signal		BNC #	Signal
1-2	1	33-34	17		1-4	1
3-4	2	35-36	18		5-8	2
5-6	3	37-38	19		9-12	3
7-8	4	39-40	20		13-16	4
9-10	5	41-42	21		17-20	5
11-12	6	43-44	22		21-24	6
13-14	7	45-46	23		25-28	7
15-16	8	47-48	24		29-32	8
17-18	9	49-50	25		33-36	9
19-20	10	51-52	26		37-40	10
21-22	11	53-54	27		41-44	11

Dual Mode					Quad Mode	
BNC #	Signal	BNC #	Signal		BNC #	Signal
23-24	12	55-56	28		45-48	12
25-26	13	57-58	29		49-52	13
27-28	14	59-60	30		53-56	14
29-30	15	61-22	31		57-60	15
31-32	16	63-64	32		61-64	16

Button Settings

In the Configuration screen you can click on any button to access the Button Settings panel. In the panel, click on the name fields to assign custom Source and Destination names to the inputs and outputs of the router.

The Settings selection allows you to pick a color from the settings panel to color code the button backgrounds. The selected color is set for both the static state color and the High Tally (rollover/active) state.
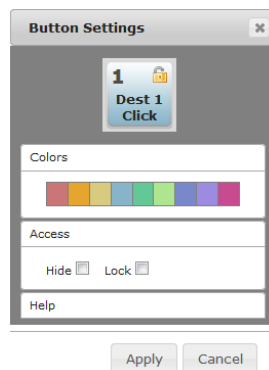

Fig. 3-6: Button Settings/Color Panel

Lock

If you want to lock any of the Destinations from Source changes, click on the Lock/Unlock box for the desired Destination.

☞ **Note**

This lock is a universal lock for all Sirius devices controlling the selected Destination. It is tallied throughout the network and can be released from other Sirius control devices on the network.

Hide

You can also hide selected Destinations from display on the Home screen by activating the Show/Hide box. This setting applies only to the local browser.

Click on the **Apply** button to commit your changes, or **Cancel** to exit the pane without making any changes.

Reset to Factory Defaults

The **Reset to Factory Defaults** button can be used to return all router user settings to factory defaults.

Salvos Configuration

The Salvos screen lets you configure up to eight salvos for the selected Sirius router. Each salvo can route any number of sources to any number of destinations, including the same source to multiple destinations. Crosspoints not included in a salvo remain unchanged.

When you first select the Salvo screen the eight Salvo buttons are shown. Buttons with currently configured salvos are colored green.

Enable Exit Page Warning

The **Enable Exit Page Warning** checkbox enables or disables the display of a warning message if you leave the Salvo configuration screen without saving.

Fig. 3-7: Initial Sirius Salvos Screen

Clicking on one of the eight Salvo buttons selects that salvo for configuration. After selection, a router table appears below with Sources listed vertically and Destinations listed horizontally. After a salvo is configured, you will need to save the crosspoint takes for that salvo.
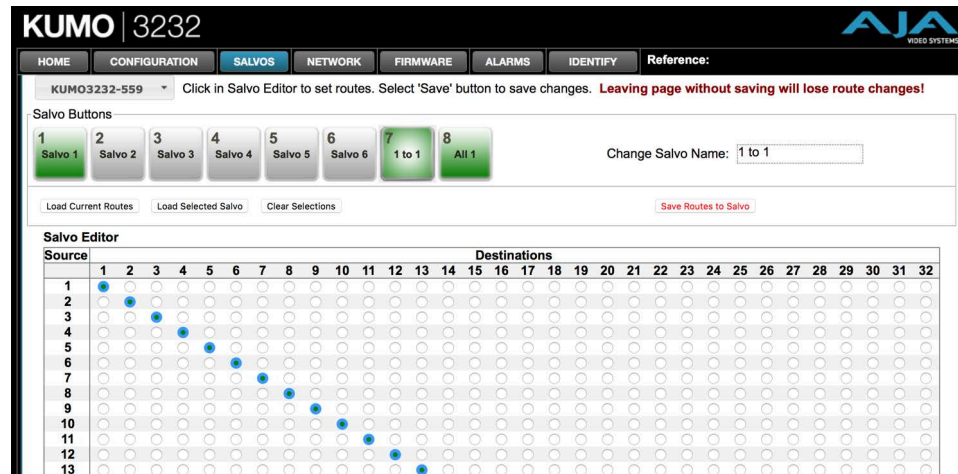
Fig. 3-8: Sirius Salvos Screen with Router Table

Salvos Screen Controls

Salvo Select Buttons

At the top of the Salvos screen are eight Salvo select buttons. Configured buttons are colored green, and the button for the currently selected salvo is highlighted.

Change Salvo Name

You can enter a name into this field for the selected salvo.

☞ **Note**

Salvo names should be unique.

Load Current Routes

Click to load the current Sirius crosspoint status into the table below. All crosspoints that have been set will be displayed.

Load Selected Salvo

Click to clear any current configuration from the router table and load the crosspoint paths from the currently selected salvo into the table.

Clear Selections

Click to clear all the paths from the router table.

Save Routes To Salvo

After configuration, click on this button to save the selected salvo.

> ☞ **Note**
>
> If you leave the page without saving, all the changes made to the selected salvo will be lost.

Salvo Configuration Procedure

1 Go to the Sirius router Home screen and select the router you wish to control with the drop down menu.

2 Go to the Salvos screen and select the salvo to be configured.

3 If you want to edit the name of the salvo, click on its name in the field on the right, type in a new unique name, and press the Enter key to save the name. Clicking outside the field will undo any typed changes.

4 Select the crosspoint(s) in the Salvo Editor below for the routes to include in this salvo. Sources are listed vertically, and Destinations horizontally.

   • Clicking on the empty box below the left Source column header creates a one to one (diagonal) salvo in the router table.

   • Clicking on any Source number applies that same source to all the Destinations.

5 Click the **Save Routes To Salvo** button to save the current router table to that salvo.

Network Setup

The Network screen provides access to standard TCP-IP setup fields and allows you to click on the System Name field to change it. The MAC address is a fixed machine address composed of manufacturer identification and product serial numbers.

You can choose DHCP or Static IP with the drop down menu. When Static IP is selected the fields below are able to be edited. After changing the network type or entering Static IP information, click the Update Network Settings button to commit your settings.
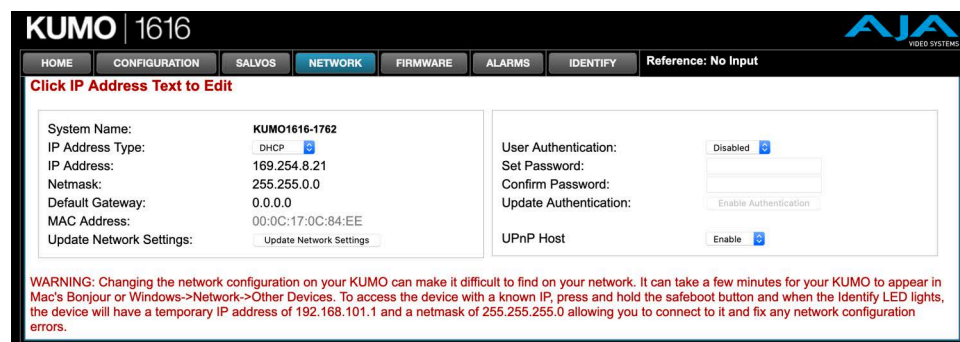

Fig. 3-9: Sirius Network Setup Screen

> ☞ **Note**
>
> The Sirius Web UI does not automatically update its network data if something other than that specific browser window is used to change that Sirius' configuration.

Web Browser Refresh

The following actions can result in the display of inaccurate data in the web browser:

- Using the factory reset button.
- Using eMini-Setup to change configuration over USB.
- Changing configuration from another browser, or even the same browser in a different tab.

To workaround this problem, manually refresh the browser window to display the latest network data.

User Authentication

This parameter enables or disables an authentication login requirement. By default this parameter is set to **Disabled**.

When **Login** is enabled, you are directed to the login screen before you can access Sirius over the network. You are required to log in before you can access any other browser screens.

When you select Login as the User Authentication choice, you then must set and confirm a password. To save these settings select the **Enable Authentication** button. You can change the password using the Network browser screen.

☞ **Note**

If authentication is used, it provides only a minimum security safeguard against unauthorized use. The authentication mechanism is simple and does not provide robust security.

Password Reset

You can use a password reset procedure to set the Sirius device's password back to the default value, allowing network access to the device if the password should become lost or mistakenly changed. The default password is "password".

After resetting the password, the current Sirius authentication setting itself is not changed. If authorization is enabled, after resetting the password you will need to enter "password" (the default) to gain network access.

Sirius Router Password Reset

1 For a Sirius router, insert a straightened paper clip or similar device into the reset slot on the rear, hold in for more than eight seconds and then release.

2 The Identify button will blink, then light steadily, and then go out, indicating the password has been reset to default.

Sirius Control Panel Password Reset.

1 For a Sirius SCP1/SCP2, press and hold the two SHIFT buttons on the panel for more than eight seconds and then release.

2 The Panel Lock button will be colored red and then go out, indicating the password has been reset to default.

UPnP Host

UPnP Host enables the Sirius to be discovered by a Windows network.

Selecting Enable (default) allows Sirius to be discovered by a Windows network. Selecting Disable prevents Windows network discovery of the Sirius.

Firmware Updating

AJA is constantly upgrading its product software so it is a good idea to check the AJA website often for updates and to assure optimum system performance. Go to the AJA KUMO Update web page by clicking the link at the bottom of the Firmware screen, or using the following link:

https://www.aja.com/family/kumo#support

Click on any of the Sirius products to go to its support tab.

Current firmware version number is reported here under the pull-down menu, and the device's serial number is listed at the bottom of the screen.
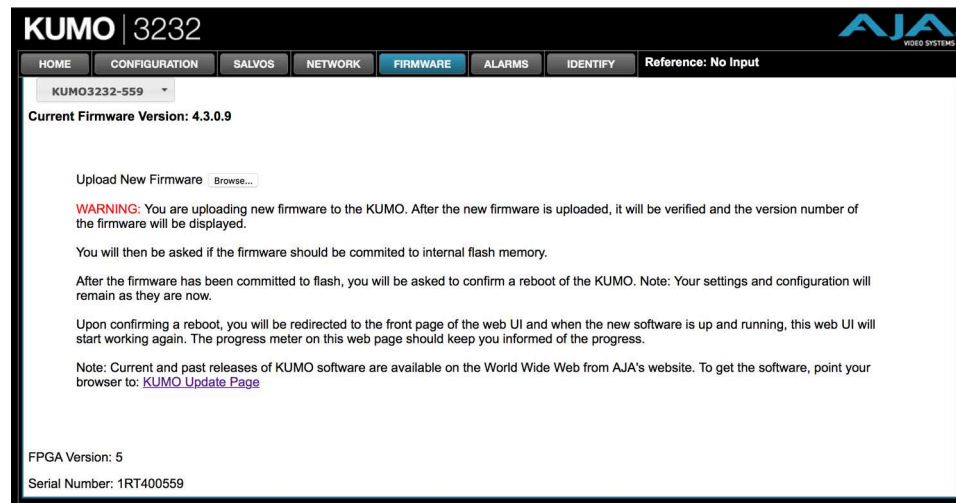

Fig. 3-10: Sirius Web Interface, Firmware Upload Screen

Unpack the Software

Download the latest version of Sirius firmware and use the Firmware screen to upload it to your Sirius router. Sirius software update files are "ZIP" files, which you can open with a number of standard and third party uncompressor applications. The software image that you will install on Sirius is a file with a name similar to:

• kumo_ver_4.0.0.3-1475859474.bin

☞ **Note**

Depending on your PC or Mac operating system settings, the ".bin" extension may not be visible to you in a file directory.

Uploading and Installing Firmware to Sirius

Uploading and installing the software update only requires a PC or Mac that can "see" the Sirius via its browser. Follow this procedure to install the software:

1 Launch a browser on your PC or Mac and connect to the Sirius product that requires a firmware update.

2 Once the Sirius web page is visible, click on the **FIRMWARE** tab.

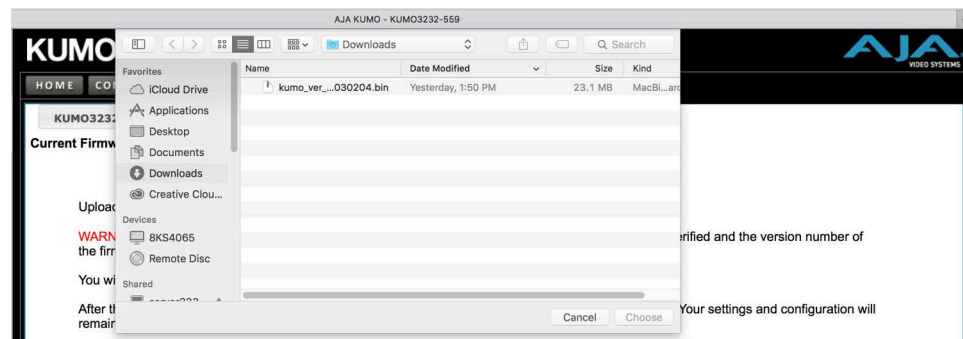3 Then click on the **Browse** button to locate the Sirius firmware image file on your PC or Mac.

Fig. 3-11: Sirius Firmware Screen, Browse for Firmware

4 When you have selected a valid Sirius image file, click **Open** and then **OK**. The file you select will upload to the Sirius and be tested for validity. Incomplete, corrupted, or non-Sirius software files are rejected.

5 When the upload completes you will be asked if you want to commit the firmware to flash. Click **Commit Uploaded Firmware**. The firmware will be loaded to flash. Wait for this to complete.

6 When done, click the **Restart** button to restart your Sirius and refresh the web browser and Sirius UI.

Fig. 3-12: Sirius Firmware Screen, Success and Restart

Once these steps are complete, the Sirius will be running the software you just uploaded. The configuration of the Sirius prior to the upgrade is preserved.

Verify the new software is running by bringing up the Sirius web page again. Check the Firmware page for the current version number. The restart and refresh cycle may take a couple of minutes. If the firmware version does not display the new version, perform the update steps again.

☞ **Note**

On some browsers, the Retry page may appear even though the software upgrade was successful. If this occurs, before clicking on retry, refresh the web page and check the version number. If the new version number appears at the top of the page, the software upgrade was successful. If the old version appears, click Retry.

If there is a power outage or glitch during the software download, the Sirius will boot the older software version and the upgrade process can then be re-started by the user. This happens because the Sirius has been designed with a safety feature where an internal "safe" copy of the previous software is retained in the event the updating process fails.

Safeboot Reset

If your Sirius firmware becomes corrupted to the point of freezing the device, you can reset to a safeboot firmware image. The existing Sirius network configuration (DHCP or Static IP) is retained during safeboot. When safeboot is active you can then re-install the latest firmware via the web interface to regain full system operation.

☞ **Note**

A Sirius device running safeboot firmware is not operational other than being accessible on a network so compatible firmware can be installed.

To perform a Sirius safeboot:
1 Power down the Sirius device.
2 Engage the reset function:

- For a Sirius router, insert a straightened paper clip or similar device into the reset slot on the rear.
- For a Sirius CP, press and hold the two SHIFT buttons on the panel.

3   Apply power to the device, wait at least 5 seconds and then release the reset function.
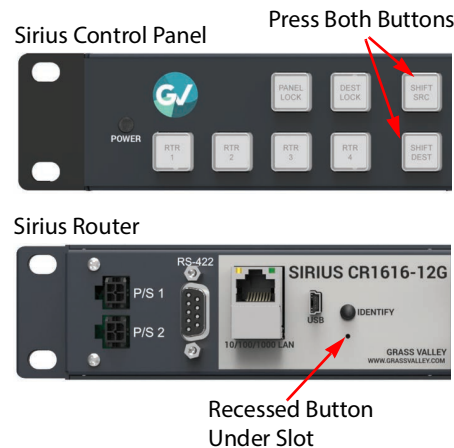

Fig. 3-13: Sirius Reset Locations

Sirius Alarms

Sirius reports alarms on the router front panel by lighting an Alarm LED and in the web browser UI by illuminating the border of the Alarms tab (see below). Alarms include:

- Power Supply – displays error if a redundant power supply is off-line
- Reference – displays error if no valid video reference signal is found
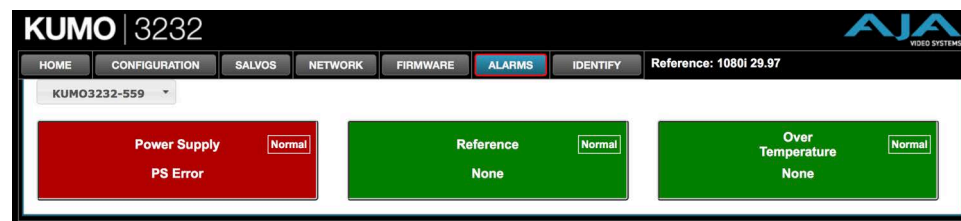- Over Temperature – displays error if Sirius exceeds normal operating temperature

Fig. 3-14: Sirius Web Interface, Alarms Screen

If you do not want any of the above conditions to report an error, click the boxed text to access the drop-down menu shown above. Select Suppress and click OK to deactivate the specific alarm.

Locating a Specific Sirius

Click on the Web UI Identify button to find the physical location of the currently controlled Sirius router or panel.

See Locating a Specific Sirius Device on the Network, on page 20 for more information.

Sirius Remote Control Panels

Overview

The Sirius hardware panels are destination-oriented control panels allowing selection of sources and destinations on each of up to four Sirius routers. A Sirius control panel will connect to a single Sirius router automatically without computer/browser interface. For connection to up to four routers on a single CP, use the Sirius browser interface to assign the router select buttons to any four Sirius routers on your network.

Two Sirius hardware panels are available, the Sirius SCP1 able to control up to 32 sources and destinations, and the Sirius SCP2, able to control up to 64.

☞ **Note**

The 32 button Sirius SCP1 hardware Control Panel cannot be used with an SCR 6464 router operating in Normal mode (only 32 buttons for 64 sources and destinations). However the Sirius SCP1 can be used when the Sirius SCR 6464 is operating in Dual or Quad mode. Control of the SCR 6464 router in all modes is available via the Sirius SCP2 64 button hardware panel, web browser, Ethernet control, and RS-422.

Sirius Control Panel Installation and Network Configuration

Refer to Installation, on page 7 for detailed information about Sirius hardware control panel installation and network configuration.

Performing a Take

1 Select the router you wish to control with a Router delegation button.
2 Press the desired Destination button. It will illuminate.

3 Press the desired Source button. That source will be routed to that destination and the Source button will illuminate.

☞ **Note**

Sources for locked Destinations cannot be changed.

Taking a Salvo

Up to eight salvos can be configured on a Sirius router. Each salvo can route any number of sources to any number of destinations, including the same source to multiple destinations. Crosspoints not included in a salvo remain unchanged. See Salvos Configuration, on page 28 to learn how to configure salvos.

Performing a salvo is a two stage process. First you arm the salvo, and then you take the salvo.

1 Press the desired Salvo button. The button will blink for five seconds.
2 Press that blinking Salvo button again to take that salvo.

After five seconds, the Salvo button will no longer be armed and will stop blinking. To take that salvo you will need to press the Salvo button again to rearm that salvo.

☞ **Note**

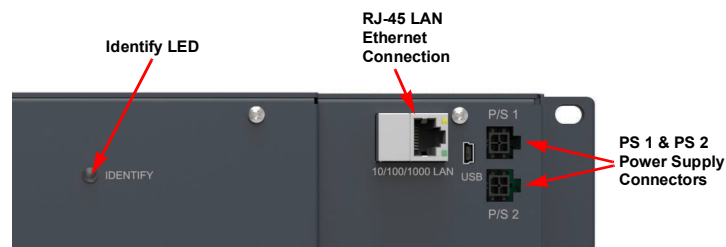Salvos do not change locked Destinations.

Connectors and Indicators

Fig. 4-1: Sirius Control Panel Connectors and Indicator

Power Connectors

Sirius control panel provides inputs for two power supplies—one included, redundant supply optional.

✎ **Tip**

The power connector has a latch, similar to an Ethernet connector. Depress the latch (facing the outside edge of the Sirius device) before disconnecting the power cable from the unit.

Ethernet Connector

An RJ-45 connector provides 10/100/1000 Ethernet connection to the internal Linux OS/web server.

Identify LED

The Identify LED can be flashed from the Web UI to identify that specific Sirius control panel.

Button Key Caps

Each control panel button has a removable lens cap that allows you to customize Source and Destination names. Grass Valley has provided a template for printing custom lens chips (we suggest using 29 lb. vellum) for button designations. The template is available at:

https://www.aja.com/support/kumo/lens_chip.zip

Panel Function Buttons

Each Sirius Control Panel provides:

• Panel Lock – prevents Source or Destination changes from this panel.
• Destination Lock – prevents any Source change for a Destination.
• Router Delegation Buttons – (RTR 1–RTR 4) enable immediate control of the Sirius assigned to the button.

Fig. 4-2: Sirius Control Panel Function Buttons

Panel Lock

When you press the Panel Lock button, it lights red and all panel functions for this panel are disabled. All other Sirius devices on the network will function normally.

Destination Lock

Press the DEST LOCK button to prevent any changes to the Sirius destination you are currently controlling (DEST button high tallied). The lock can be removed from any other Sirius Control Panel or browser interface on the network.

The DEST and DEST LOCK buttons turn red on all panels that are assigned to the Sirius you are controlling. You can select other destinations and apply the Destination Lock function to each. All locks will tally red. To remove the lock, select the destination and press DEST LOCK again.

Locked destinations are reported on the Sirius router's browser Home page with a lock icon.

Fig. 4-3: Sirius Router Home Screen Destination Buttons

Router Delegation Buttons (RTR 1 - 4)

Use the Router delegate buttons to connect to the specific router to be controlled.

You can assign the delegate buttons to any of up to four routers in your system. To assign router/control panel delegation, access the Home page for your Sirius Control Panel.

If network communications between a control panel and router fails, the control panel's delegation button for that router will be colored pink. When communications is restored the delegation button returns to its normal color.

Shift/Reset Buttons

The SHIFT SRC and SHIFT DEST buttons serve multiple functions. They allow you to select shifted sources and destinations (17–32), and they also perform the same reset functions as the reset slot. Resets should be done only by qualified network personnel:

- Shift: Hold down SHIFT SRC and press a source button to select a shifted source, or hold down SHIFT DEST and press a destination button to select a shifted destination. When a shift button is not held down, pressing a source or destination button selects the unshifted source or destination (1–16).
- IP Reset: See Sirius Temporary Static IP Address, on page 11.
- Password Reset: See Password Reset, on page 31.
- Reset to Safeboot Firmware: See Safeboot Reset, on page 34.

SALVO Buttons (SCP2 Only)

The eight Salvo buttons, when configured, can each be used to perform multiple source to destination takes using just that one button.

Performing a salvo is a two stage process. First you arm the salvo, and then you take the salvo.

1 Press the desired Salvo button. The button will blink for five seconds.
2 Press that blinking Salvo button again to take that salvo.

☞ **Note**

Salvos do not change locked Destinations.

Control Panel Web Browser Interface

The Sirius CP browser interface provides many of the same Navigation Bar tabs as the router. This section discusses those functions unique to the control panel interface. The Navigation Bar includes:

- Home – assign router elect buttons to Sirius routers
- Configuration – adjust the control panel display intensity and, if necessary, Reset the panel to its original "Auto Configure" state or to original factory settings
- Buttons - (control panel browser only) deactivate and reactivate panel buttons, see Disabling Control Panel Buttons, on page 42.
- Network and Firmware tabs – same as Sirius router network settings, see Network Setup, on page 30 and UPnP Host, on page 32.
- Alarms – Power Supply and Over Temperature, refer to Sirius Alarms, on page 35.
- Identify button – to identify the physical location of a particular control panel.

Home Screen

Use the Home page to assign a router to each of the router delegation buttons. Each button has a pull-down menu that lists the active networked Sirius for assignment and provides an Unassign and Refresh function.
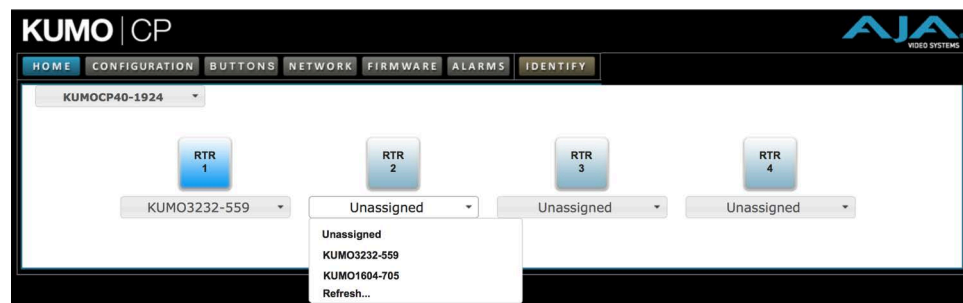

Fig. 4-4: Sirius CP Browser Interface Home Screen

The assigned router name appears below each button. You can change the selected (currently-controlled) router on the panel by clicking the button on the Home page. The panel's router delegation button will tally appropriately.

Configuration Screen

Using the Configuration page, you can:

- Adjust the Display Intensity slider – select one of four button illumination levels.

- Reset "Auto Configure" – resets the Auto Configure function to automatically set up one control panel to one router. This function re-boots the panel to trigger the configuration. Upon reboot, if any other router is found on the network, it will not pair to the panel.
- Reset to Factory Defaults – resets all control panel settings to factory defaults, including System Name and Network settings.

Fig. 4-5: Sirius CP Browser Configuration Screen

☞ **Note**

If a Sirius webpage on a computer is open when that Sirius device is reset or had its network configuration changed from another location (even if using a different tab in the same browser), the information displayed on that original webpage will not be updated automatically and so will display stale data.

Buttons Screen

The Buttons screen lets you enable or disable the Source, Destination, and Salvo buttons on a Sirius hardware control panel.

Disabling Control Panel Buttons

The v4.1 and higher Sirius firmware includes a button disabling feature, useful to uniquely configure the button operation of each Sirius SCP1/SCP2 for specific work areas and specific workflows.

☞ **Note**

This feature is not a router Destination or Source lock. Takes can still be performed on paths with disabled buttons, using the Sirius Web UI or another Sirius control panel.

The current Sirius CP configuration is retained after a power cycle, including any disabled Source or Destination buttons.

☞ **Note**

Performing a Sirius CP factory reset clears the configuration. All Salvo, Source and Destination buttons are enabled after a factory reset.

Procedure

1 Access the Sirius CP via its internal web page.

2 Click on the HOME tab and select one of the four routers.

3 Click on the BUTTONS tab and then click on the Source, Destination, and/or Salvo buttons you wish to disable. Enabled buttons have a green background color and disabled buttons have a gray background color.

Fig. 4-6: Sirius SCP2 Configuration with Disabled Buttons

4 Web UI buttons that have been disabled will go blank, and the tally lights of the disabled physical buttons on the Sirius CP will go off.

Network Screen

The Network screen provides access to standard TCP-IP setup fields and allows you to click on the System Name field to change it. The MAC address is a fixed machine address composed of manufacturer identification and product serial numbers.

You can choose DHCP or Static IP with the drop down menu. When Static IP is selected the fields below are able to be edited. After changing the network type or entering Static IP information, click the Update Network Settings button to commit your settings.

☞ **Note**

Do not Update Network Settings with 0.0.0.0 values for either IP Address or Netmask. This will disable the control panel and it will need to be returned to Grass Valley for repair.
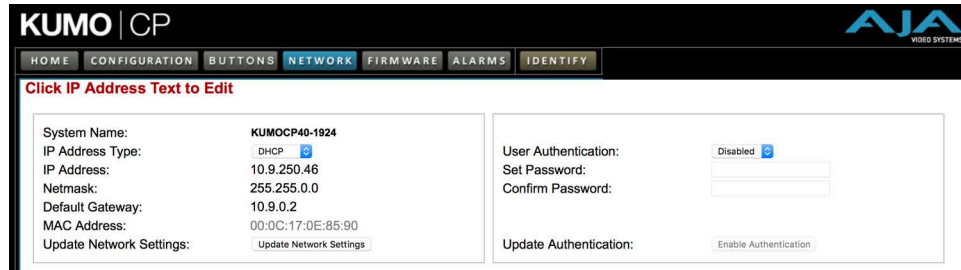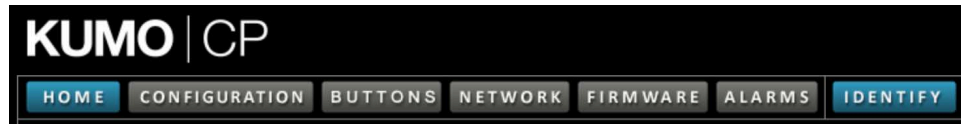
Fig. 4-7: Sirius CP Network Setup Screen

User Authentication

This parameter enables or disables an authentication login requirement. See User Authentication, on page 31 for more information.

Identify Sirius Device

Click on the Web UI Identify button to find the physical location of the currently controlled Sirius router or panel.

See Locating a Specific Sirius Device on the Network, on page 20 for more information.

eMini-Setup

Overview

This chapter describes using the eMini-Setup application to initially communicate with and configure the Sirius over a direct USB connection. Once configured, the Sirius can be accessed via an Ethernet network using a web browser. Subsequently, that device can then be reconfigured over that network, using its IP address and built in web server.

☞ **Note**

The eMini-Setup application is only used to setup selected Ethernet capable AJA devices, and cannot be used to connect to or setup other AJA Mini-Converters.

The general procedure is:

1 Acquire eMini-Setup from the AJA website and install the eMini-Setup application onto a computer.

2 Connect the Sirius to that computer's USB port.

3 Launch the eMini-Setup application.

4 Go to the Network tab where the IP address settings are displayed. You can use the existing DHCP assigned IP address, or it can be changed manually.

Acquiring eMini-Setup

AJA's eMini-Setup application is available for download from the AJA website.

To download the latest eMini-Setup package, which includes the eMini-Setup application and documentation:

1 Go to:

https://www.aja.com/family/software#eminisetup

2 Click the link corresponding to the version you want to download for Mac or Windows.

AJA Documentation

Included with the eMini-Setup download is the AJA device's documentation, which can be accessed from the eMini-Setup UI via the Help/Manual drop-down menu. This manual includes eMini-Setup information.

Documentation can also be accessed directly from the Mac eMini-Setup installer in the Documentation folder.

Documentation included with the eMini-Setup application is the version available at the time of distribution. However, AJA's documentation can be updated regularly, so newer versions may exist.

To download just the latest documentation, go to:

https://www.aja.com/support

Click the product name and open the Manuals link.

Installing eMini-Setup

PC Installation

To install eMini-Setup on a Windows PC:

1 Download the application from the AJA website. See Acquiring eMini-Setup, on page 45.

2 Open the AJA_eMini-Setup_win.zip file.

3 Double-click on the AJA_eMini-Setup.msi file.

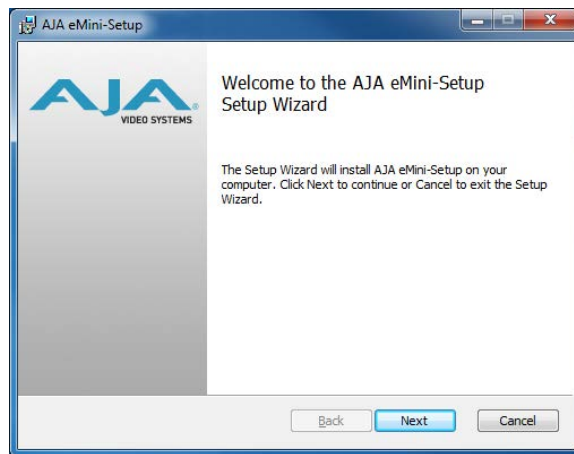4 The Setup Wizard will guide you through the installation.

Fig. 5-1: eMini-Setup PC Wizard

5 Click Next to begin. Answer the questions in the subsequent dialogs, including device software installation if displayed. When finished, an AJA eMini-Setup shortcut will be installed on the desktop, and you will be able to locate the eMini-Setup application in the AJA folder in the Programs listing.

☞ **Note**

If the eMini-Setup application already exists on the PC, a different Setup Wizard appears. (In some instances, Windows may require uninstalling an earlier version of eMini-Setup before installing a new version.)
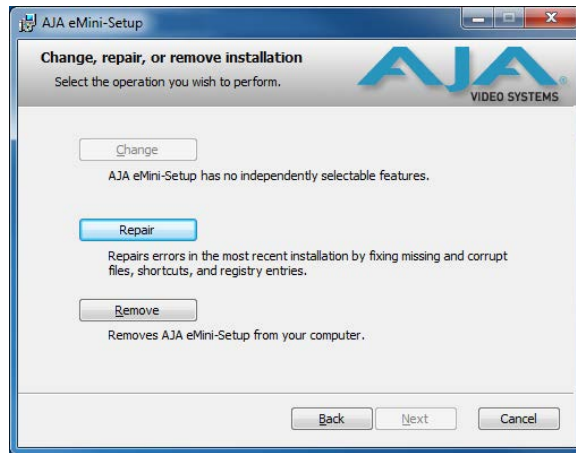
Fig. 5-2: eMini-Setup Wizard, Re-installation

With this screen you can Repair (reinstall) or Remove (uninstall) eMini-Setup on the PC.

Mac Installation

To install the application on a Mac:

☞ **Note**

Mac computers must be Intel-based (G5, G4 and earlier models will not work with eMini-Setup).

1　Download the application from the AJA website. See Acquiring eMini-Setup, on page 45.
2　Unzip the file.
3　Double-click on the AJA eMini-Setup.dmg file.
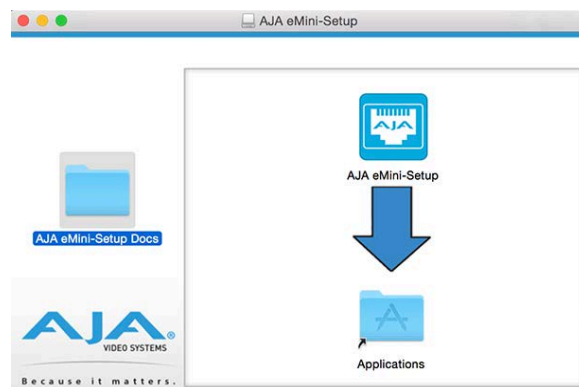4　Answer the prompt and a utility program will be launched.


Fig. 5-3: eMini-Setup Mac Installer

5   To complete the installation drag the "AJA eMini-Setup" icon to the Applications folder.

Running eMini-Setup

Connect your Ethernet capable AJA device to the PC or Mac via the supplied USB cable, and then connect the external power supply (supplied) to that AJA device.

PC Startup

To run eMini-Setup on a PC, double-click on the AJA eMini-Setup icon on your desktop, or open the AJA folder in the program list and click on the AJA eMini-Setup application located inside the eMini-Setup folder.
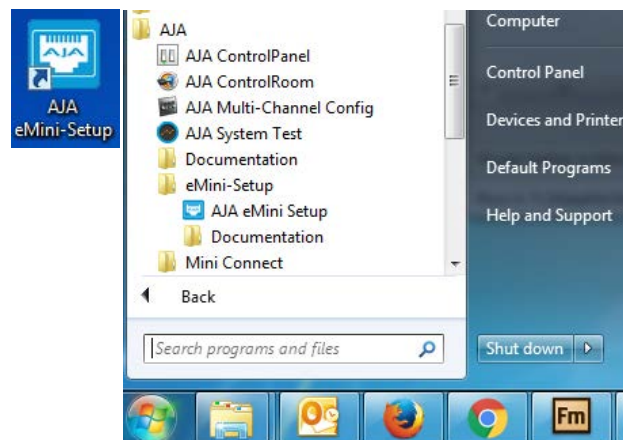
Mac Startup

To run eMini-Setup on a Mac, open the Applications folder and locate the AJA eMini-Setup application. Double-click the application to launch it.

Operating eMini-Setup

The eMini-Setup application provides a graphical user interface for viewing settings, modifying settings, and updating firmware.
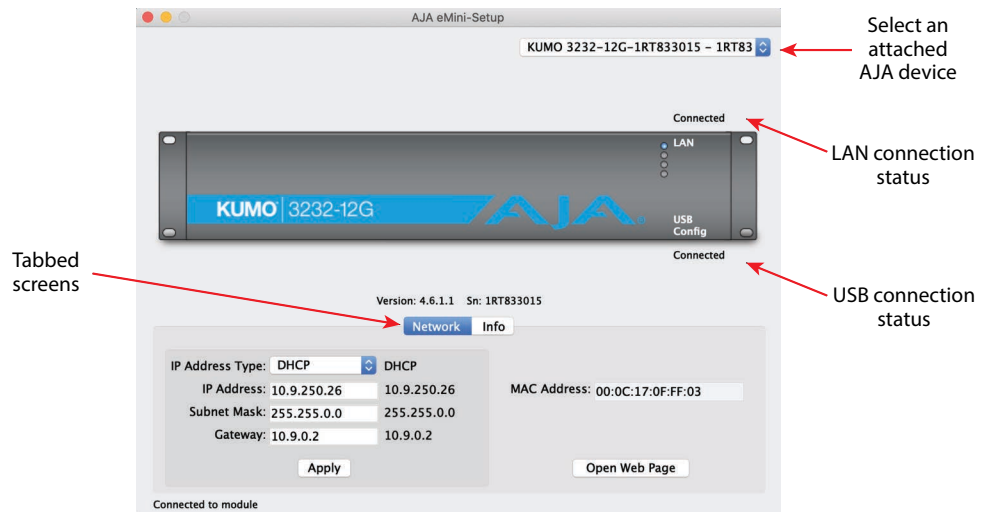
Fig. 5-4: Example eMini-Setup Screen

Selecting an AJA device from the pull down menu on the upper right causes eMini-Setup to connect to the selected AJA device.

Version - The version of firmware installed in the AJA device is displayed below the graphic.

Sn - This is the factory set unique serial number of your AJA device. If you ever call AJA Support for service, you may be asked for this number.

A status field at the bottom of the screen shows if the eMini-Setup application is connected and communicating with an AJA device.

File Menu - The File drop-down menu on the eMini-Setup application bar has a Revert to Factory Settings menu item that allows you to change the settings back to the AJA device's factory defaults.

Edit Menu - The Edit drop-down menu has standard Cut, Copy and Paste functions for editing text.
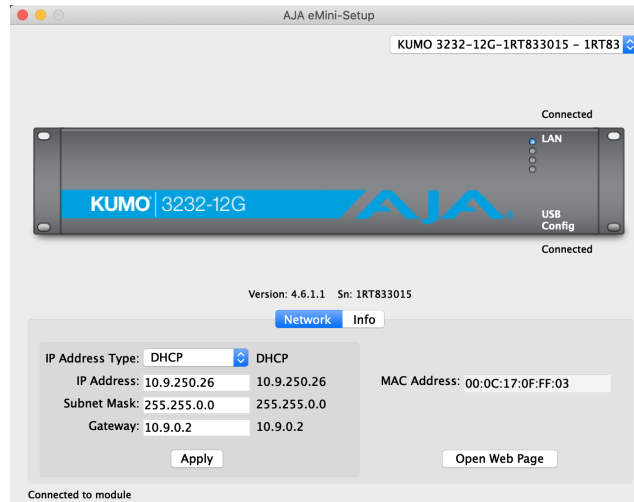
Help Menu - The Help drop-down menu has a link to the AJA device's manual.

Note

On a Windows PC, the File, Edit and Help menus reside in the eMini-Setup application window. On a Mac, these menus reside in the application bar above the eMini-Setup application window.

Control Network Tab Screen

Use this Control Network tab to view and change the network setup on the connected AJA device. The network settings currently being used are shown on the right. You must click the Apply button to initiate any network configuration changes.

IP Address Type - Choose from DHCP or Static IP Address.

IP Address - The current IP Address is displayed. A different IP address can be entered.
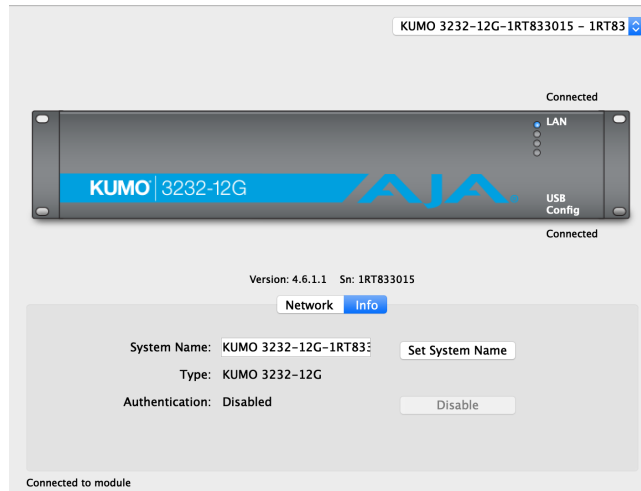
Subnet Mask - The current Subnet Mask is displayed. A different subnet mask can be entered.

Gateway - The current Gateway address is displayed. A different gateway address can be entered.

MAC Address - This is the permanent MAC address of the Control LAN Ethernet port of the AJA device.

Open Web Page - Opens the Sirius web interface in a web browser.

Info Tab Screen

This tab provides basic information about the connected AJA device. This information is mostly useful when calling AJA Support for service or technical support.

System Name - This field allows you to give your AJA device a unique name. This can be useful if you have several attached to a Mac/PC via USB so you can distinguish between them easily. This is also the name that shows up in Zeroconf/Bonjour, uPnP, and the "Other KUMOs" dropdown on the Web UI Home screen.

Type - This is the factory set model name of the AJA device.

Authentication - If Authentication has been Enabled on the web browser Access tab, you can disable the security feature by clicking the Disable button.

A Specifications

All Sirius Router Model Tech Specs

Ancillary Data	Passes all SDI embedded ancillary data including audio
Salvo	Up to 8 Salvos can be configured and saved in each Sirius router
Switching Modes	• Single, Dual, and Quad link modes • Switches in vertical blanking per SMPTE RP-168
Reference Input	• External, 2x BNC • Looping, nonterminating • Blackburst or tri-level sync
Network Interface	• 1x RJ-45, 10/100/1000 Ethernet • Supports Sirius Ethernet control panels, direct connect or networked • Basic support for Grass Valley Native Protocol • Embedded web server for remote control
USB Interface	1x Mini-USB for IP configuration using eMini-Setup* * Earlier model devices lacking a USB port cannot be configured via USB.
Serial Interface	• 1x DB-9 Female, RS-422 • Basic support for Grass Valley Native Protocol • (See RS-422 Control Specifications (Routers), on page 58 for pinouts.)
Environment	• Safe Operating Temperature: 0 to 40°C (32 to 104°F) • Safe Storage Temperature (Power OFF): -40 to 60°C (-40 to 140°F) • Operating Relative Humidity: 10-90% noncondensing • Operating Altitude: <3,000 meters (<10,000 feet)

Sirius SCR 1616-12G Tech Specs

Video Formats	• 270 Mb/s, 1.5 Gb/s, 3 Gb/s, 6 Gb/s, 12 Gb/s SDI • 270 Mb/s DVB-ASI • Format agnostic, 270 Mb/s - 12 Gb/s
Video Input Digital	• 12G-SDI Inputs • 16x 12G-SDI BNC, SMPTE-259/292/424/2081/2082
Video Output Digital	• 12G-SDI Outputs • 16x 12G-SDI BNC, SMPTE-259/292/424/2081/2082 • Noninverting

Cable Equalization	(Belden 1694A) • 12 Gb/s, up to 55m • 6 Gb/s, up to 110m • 3 Gb/s, up to 185m • 1.5 Gb/s, up to 210m • 270 Mb/s, up to 405m • Automatic operation
Reclocking	• 270 Mb/s, 1.483 Gb/s, 1.485 Gbps, 2.967 Gb/s, 2.970 Gb/s, 5.934 Gb/s, 5.940 Gb/s, 11.868 Gb/s, 11.880 Gb/s - Auto Select • All other rates are passed through and not reclocked
Control Panel Compatibility	• SCP1 (First 32 I/O in Normal, all I/O in Dual or Quad mode) – 1 RU X-Y Ethernet control panel • SCP2 (Single, Dual or Quad mode) – 2 RU X-Y Ethernet control panel
Size (w x d x h)	1 RU - 17.4" x 1.54" x 1.75" (441.96 x 39.12 x 44.45 mm)
Weight	1.4 lbs. (0.7 kg)
Power	• 10-14 VDC regulated, 16W typ, 18W max, power supply required, included with purchase • AC Adapter: 100-240 VAC, 50/60 Hz, universal input

Sirius SCR 3232-12G Tech Specs

Video Formats	• 270 Mb/s, 1.5 Gb/s, 3 Gb/s, 6 Gb/s, 12 Gb/s SDI • 270 Mb/s DVB-ASI • Format agnostic, 270 Mb/s - 12 Gb/s
Video Input Digital	• 12G-SDI Inputs • 32x 12G-SDI BNC, SMPTE-259/292/424/2081/2082
Video Output Digital	• 12G-SDI Outputs • 32x 12G-SDI BNC, SMPTE-259/292/424/2081/2082 • Noninverting
Cable Equalization	(Belden 1694A) • 12 Gb/s, up to 50m • 6 Gb/s, up to 100m • 3 Gb/s, up to 170m • 1.5 Gb/s, up to 200m • 270 Mb/s, up to 390m • Automatic operation
Reclocking	• 270 Mb/s, 1.483 Gb/s, 1.485 Gb/s, 2.967 Gb/s, 2.970 Gb/s, 5.934 Gb/s, 5.940 Gb/s, 11.868 Gb/s, 11.880 Gb/s - Auto Select • All other rates are passed through and not reclocked
Control Panel Compatibility	• SCP1 – 1RU X-Y Ethernet control panel • SCP2 – 2RU X-Y Ethernet control panel
Size (w x d x h)	2RU - 17.4" x 1.54" x 3.50" (441.96 x 39.12 x 88.9 mm)
Weight	4.6 lbs. (2.1 kg)
Power	• 10-14 VDC regulated, 24W typ, 25.2W max, power supply required, included with purchase • AC Adapter: 100-240 VAC, 50/60 Hz, universal input

Sirius SCR 6464-12G Tech Specs

Video Formats	• 270 Mb/s, 1.5 Gb/s, 3 Gb/s, 6 Gb/s, 12 Gb/s SDI • 270 Mb/s DVB-ASI • Format agnostic, 270 Mb/s - 12 Gb/s
Video Input Digital	• 12G-SDI Inputs • 64x 12G-SDI BNC, SMPTE-259/292/424/2081/2082
Video Output Digital	• 12G-SDI Outputs • 64x 12G-SDI BNC, SMPTE-259/292/424/2081/2082 • Noninverting
Cable Equalization	(Belden 1694A) • 12 Gb/s, up to 50m • 6 Gb/s, up to 90m • 3 Gb/s, up to 180m • 1.5 Gb/s, up to 210m • 270 Mb/s, up to 390m • Automatic operation
Reclocking	• 270 Mb/s, 1.483 Gb/s, 1.485 Gb/s, 2.967 Gb/s, 2.970 Gb/s, 5.934 Gb/s, 5.940 Gb/s, 11.868 Gb/s, 11.880 Gb/s - Auto Select • All other rates are passed through and not reclocked
Control Panel Compatibility	• SCP1 – 1RU X-Y Ethernet control panel • SCP2 – 2RU X-Y Ethernet control panel
Size (w x d x h)	4 RU - 17.4" x 1.55" x 7.00" (441.96 x 39.37 x 177.8 mm)
Weight	9.2 lbs. (4.2 kg)
Power	• 10-14 VDC regulated, 13W typ, 17W max, power supply required, included with purchase • AC Adapter: 100-240 VAC, 50/60 Hz, universal input

Sirius SCP2 Tech Specs

User Interface	• 80 buttons with removable overcap for lens chips • Includes factory installed lens chip set • High and Low button tally indication, configurable brightness • Controls up to four Sirius routers • Panel Lock feature • Destination Lock feature
Router Support	• SCR 1616-12G • SCR 3232-12G • SCR 6464-12G
Salvo	8 Salvos buttons can be enabled to trigger a Sirius router's configured salvos.
Network Interface	• 1x RJ-45, 10/100/1000 Ethernet • Embedded web server for remote control

USB Interface	• 1x Mini-USB for IP configuration* * Earlier model devices lacking a USB port cannot be configured via USB.
Size (w x d x h)	2RU - 17.4" x 1.3" x 3.5" (441.96 x 33.02 x 88.90 mm)
Weight	2.1 lbs. (1.0 kg)
Power	• 10-14 VDC regulated, 4W typical, 9.6W max, power supply required, included with purchase • AC Adapter: 100-240 VAC, 50/60 Hz, universal input
Environment	• Safe Operating Temperature: 0 to 40℃ (32 to 104°F) • Safe Storage Temperature (Power OFF): -40 to 60℃ (-40 to 140°F) • Operating Relative Humidity: 10-90% noncondensing • Operating Altitude: <3,000 meters (<10,000 feet)

Sirius SCP1 Tech Specs

User Interface	• 40 buttons with removable overcap for lens chips • Includes factory installed lens chip set • High and Low button tally indication, configurable brightness • Controls up to four Sirius routers • Panel Lock feature • Destination Lock feature
Router Support	• SCR 1616-12G • SCR 3232-12G
Network Interface	• 1x RJ-45, 10/100/1000 Ethernet • Embedded web server for remote control
USB Interface	• 1x Mini-USB for IP configuration using eMini-Setup* * Earlier model devices lacking a USB port cannot be configured via USB.
Size (w x d x h)	1 RU - 17.4" x 1.3" x 1.75" (441.96mm x 33.02mm x 44.45mm)
Weight	1.2 lbs. (0.6 kg)
Power	• 10-14 VDC regulated, 2.5W typical, 6W max, power supply required, included with purchase • AC Adapter: 100-240 VAC, 50/60 Hz, universal input
Environment	• Safe Operating Temperature: 0 to 40℃ (32 to 104°F) • Safe Storage Temperature (Power OFF): -40 to 60℃ (-40 to 140°F) • Operating Relative Humidity: 10-90% noncondensing • Operating Altitude: <3,000 meters (<10,000 feet)

GVG Native Protocol Support

Introduced with v2.0 firmware, Sirius provides basic support for the GVG Native Protocol, aka Series 7000 Native Protocol. GVG Native Protocol, using:

- 1 serial connection via RS-422 with a 9-pin connector
- TCP/Ethernet for up to 32 connections

For more information, refer to Grass Valley documentation at:

> http://grassvalley.jp/pdf/RoutingProductsProtocolManual_2.pdf

NP Commands Supported

Background	• BK, I; Connect, heartbeat • BK, N; Gets system name • BK, T; Gets software title • BK, t; Gets protocol software • BK, R; Gets software version • BK, d; Gets device name • BK, F; Gets source, destination or salvo name changes • BK, E; Sets or returns status of Level 4 Echo
Queries	• QN, S; Gets all srcs by name • QN, IS; Gets all srcs, name & index • QN, D; Gets all dests, names • QN, ID; Gets all dests, name & indx • QN, L; Gets levels (hard coded as "Kumo_Lev0") • QD, {destname}; Gets: protect {On/Off}, chop{=OFF}, {sourceName}, level{= lev0} • Qd, {destname}; Gets: protect {On/Off}, chop{=OFF}, {sourceName}, level{= lev0}
Control	• TD,{destname,srcname};Takes by name • TI,{destIndx,srcIndx}; Takes by index • PR,{destname, levelmask} Sets lock for given dest. • UP,{destname, levelmask} Unsets lock for given dest.

RS-422 Control Specifications (Routers)

☞ **Note**

All Sirius Routers support RS-422 control. Sirius Control Panels do not support RS-422 control.

Baud Rate	38400
Parity	None
Stop Bit	1
Data Bits	8

Serial Interface

- 1x DB-9 Female, RS-422
- Grass Valley Native Protocol
- 9-pin D-connector pinout is as follows:

1	GND
2	TX-
3	RX+
4	GND
5	No Connection
6	GND
7	TX+
8	RX-
9	GND
Shell	GND

Contact Us

Grass Valley Technical Support

For technical assistance, contact our international support center, at 1-800-547-8949 (US and Canada) or +1 530 478 4148.

To obtain a local phone number for the support center nearest you, please consult the Contact Us section of Grass Valley's website (www.grassvalley.com).

An on-line form for e-mail contact is also available from the website.

Corporate Head Office

Grass Valley
3499 Douglas-B.-Floreani
St-Laurent, Quebec H4S 2C6
Canada
Telephone: +1 514 333 1772
Fax: +1 514 333 9828
www.grassvalley.com