MULTI-DOMAIN VIDEO NETWORK SWITCH

INTEGRATION GUIDE

(November 2023)

Point of Contact:
Freeport Technologies Help Desk
571-262-0422
TechSupport@freeporttech.com

1 Precautions and Warnings

The Freeport Technologies MDVNS system components contain no user serviceable or adjustable parts. Only an authorized Freeport service technician should make repairs when necessary.

Electrical

The MDVNS system components require the use of both AC and DC power. Please note that high voltage is present inside of the Freeport SCC5Net Switch when power is applied to the unit. To prevent electric shock, do not remove the cover of any of the system components or change any of the internal cables or wiring.

Requirements for a valid power input source are given on the rear of each component below the power connector. This equipment is intended to be used with a primary power source with a grounded neutral conductor. The ground connector (third wire) on the AC input must be connected to earth ground. The ground connector is connected to the unit case. This provides physical safety and helps in the attenuation of the transmission of electromagnetic fields in and out of the unit.

Cooling

Air vents are provided on the sides of each component for cooling where required. Do not insert any objects into the vents as dangerous voltages are present inside of the components and damage to the electronics is possible. Installation of the components in a rack should be such that at least one of the sides should be open to a source of conditioned air. The amount of air flow required for safe operation should not be compromised.

Fiber Optic Devices

The fiber optic ports on the third-party media converters that may be integrated as part of the MDVNS system contain Class 1 laser devices. When the ports are disconnected, always cover them with the provided plug. Exposed ports may cause skin or eye damage. Do not look directly at a fiber optic cable end or inspect a fiber cable with an optical lens.

2 Overview

The Freeport Technologies MDVNS provides an automated periods processing procedure to switch a single video CODEC safely and securely between multiple networks and modes of varying classification levels.

The system adheres to the DISA approved periods processing procedure when traversing a single CODEC across various video networks, which is consistent throughout every system configuration regardless of the number of networks/modes or network type.

The system can be controlled manually via the front panel, via a Cisco Touch 10, or fully integrated with a third-party control system.

The system can capture and restore all the configuration settings that are made available by the CODEC manufacturer via the RS-232 port.

The CODEC configuration settings captured for each network/mode are stored in non-volatile memory of dedicated processing units (SCC Units). Data isolation is achieved using multiple SCC units, where each unit is dedicated to a particular network/mode. CODEC configuration settings, passwords, certificates, user accounts, directories, camera pre-sets, sign-in banner, and any required *Post Restore Commands* (xCommands) are managed on a per network/mode basis via the SCC units. One SCC Unit per network/mode is required.

Classification signage integration provides automated system status throughout the switching process and room classification status once a network/mode transition is complete.

The system can manage a variety of external devices (source isolation devices, noise generators, shades, etc.) via a set of contact closures which can be configured to turn on/off depending on the current classification of the system.

The system is also capable of managing and isolating a PSTN or VOIP line using a switched air gap isolated relay. This dedicated switched connection can be configured to be enabled or disabled depending on the current classification of the system.

The MDVNS system can be integrated with a variety of JITC approved video CODECS. Please contact the Freeport Technologies Help Desk (techsupport@freeporttech.com or 571-262-0422) for a list of compatible CODECs and their associated firmware.

3 System Components

The Freeport MDVNS consists of several hardware components which can all be contained in a dedicated AV rack or integrated into an existing AV installation. None of the system components (including the video CODEC) require physical separation during installation.

The core components required for each MDVNS system consists of:

1. Freeport SCC5NET Switch – Enforces and initiates all switching tasks, controlling the order in which they are executed, and validating that all tasks are executed as intended
2. Freeport SCC – Used to capture, clean, and restore the profile of the CODEC for a particular network/mode
3. Market Central SecureSwitch® – Manages and isolates customer provided VTC connections for all video networks
4. *Media Converter – Provides the main IP network connection to the video CODEC (via the fiber output of the Market Central SecureSwitch®)
5. Classification Signage – Provides system status throughout the switching process and room classification status once a network/mode transition is complete

* Please note that if the customer provided video network connections are copper, a media converter will be required to introduce the network signals to the Market Central SecureSwitch®. Power to these media converters should be managed by the MDVNS thus providing an additional layer of isolation. All required media converters are controlled by the MDVNS.

3.1 SCC5Net Switch

The Freeport SCC5NET Switch is the core component of the system that enforces and initiates all switching tasks, controlling the order in which they are executed, and validating that all tasks are executed as intended.

It provides RS-232 communications routing, contact closure and I/O feedback, and controls power to the other hardware components of the system. All communication paths inside the SCC5Net Switch are ground isolated from one another, no connected MDVNS components including the video CODEC share a common ground.

The SCC5Net Switch contains a programming API which allows a third-party control system to initiate and monitor the MDVNS switching process via TCP/IP or RS-232.

The SCC5Net Switch is responsible for:

1. Providing the RS-232 connection path between the CODEC and all other system components (Freeport SCC units, Cisco Touch 10, Third-Party Control System)
2. Controlling the removal and application of power to the CODEC
3. Controlling the removal and application of power to each Freeport SCC unit
4. Controlling the removal and application of power to all media converters
5. Managing the Market Central SecureSwitch®
6. Managing room classification signage
7. Enabling/disabling a PSTN, VOIP or unclassified ISDN line
8. Controlling the removal and application of power to external devices

Figure 1 – Freeport SCC5NET Switch (Front View)

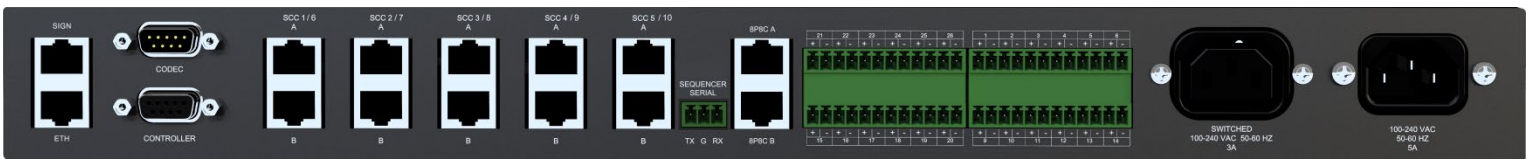


Figure 2 – Freeport SCC5NET Switch (Rear View)

3.2 SCC5Net Switch Front Panel Buttons

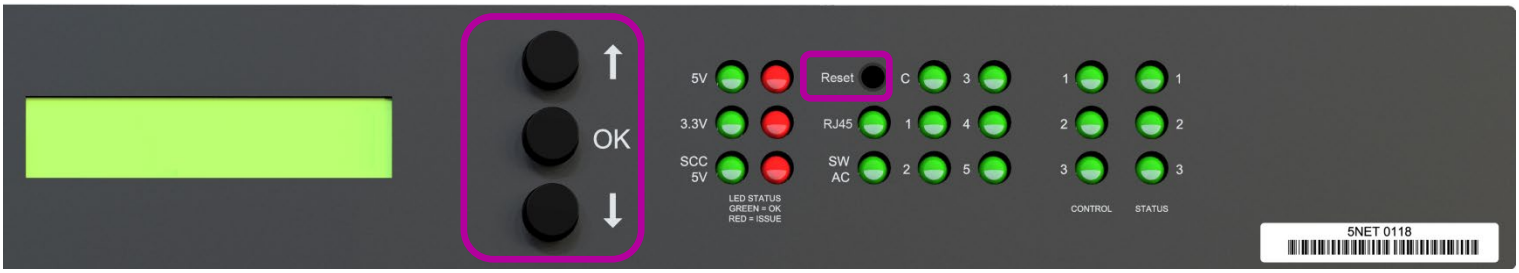


Figure 3 – Freeport SCC5NET Switch (Front Panel Buttons)

1) *Arrow Up* – Used to navigate the onscreen menu
2) *OK* – Used to select a function when navigating the onscreen menu
3) *Arrow Down* – Used to navigate the onscreen menu
4) *Reset* – Press and hold the reset button for one **(1) second** to reset/reboot the SCC5Net Switch processor

3.3 SCC5Net Switch Front Panel LEDs

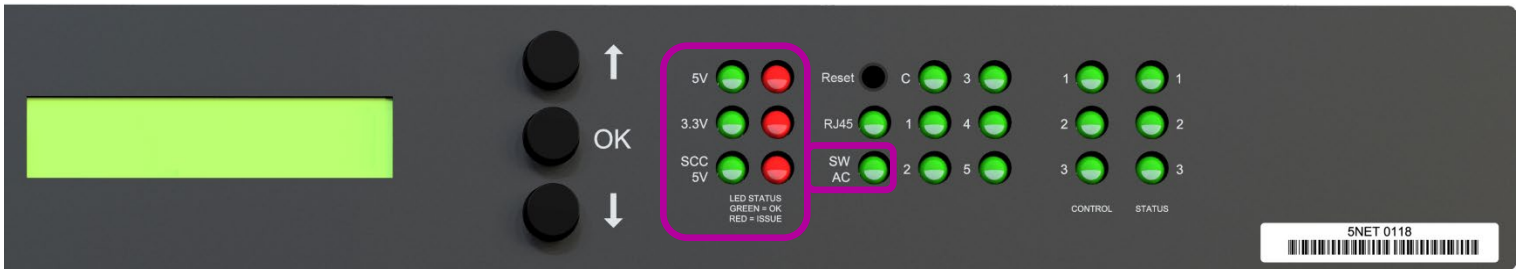


Figure 4 – Freeport SCC5NET Switch (Power Supply LEDs)

1) *5V LED* – SCC5Net Main Board Power (5V Relays)
2) *3.3V LED* – SCC5Net Main Board Power (3.3V GPIO)
3) *SCC 5V LED* – Power Supply for SCC Units
4) *SW AC LED* – Power Relay for CODEC (Switched AC)

Figure 5 – Freeport SCC5NET Switch (RJ45 & Communication Path LEDs)

1) *RJ45 LED* – Indicates whether the air gap isolated relay is open (LED Off) or closed (LED On)
2) *C LED* – Serial Communication Path between Room Control & CODEC (Bottom RS-232 Port)
3) *1-5 LEDs* – Indicates Active SCC Unit Connected to CODEC (Top RS-232 Port)

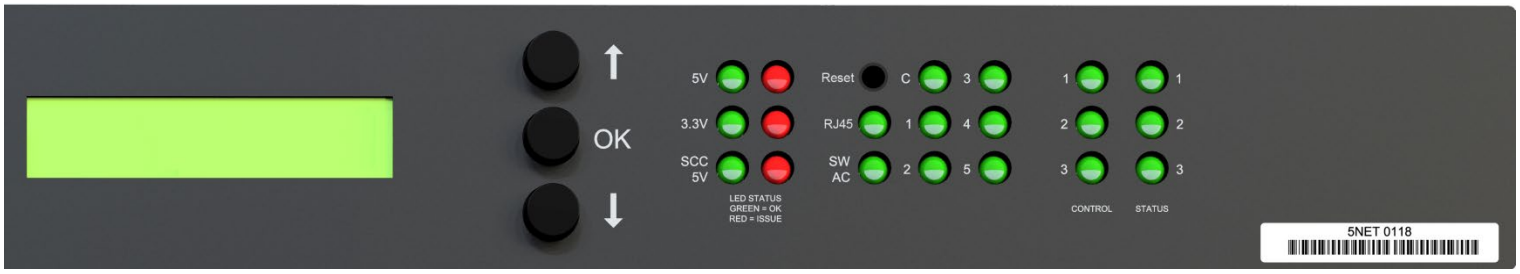


Figure 6 – Freeport SCC5NET Switch (Control & Status LEDs)

1) *Control 1 LED* – Leaving Network/Mode, Initializing (+ Control 2 LED), Maintenance Mode (All Off)
2) *Control 2 LED* – Joining Network/Mode, Initializing (+ Control 1 LED), Maintenance Mode (All Off)
3) *Control 3 LED* – Link, Maintenance Mode (All Off)
4) *Status 1 LED* – SCC Done Signal
5) *Status 2 LED* – SCC Error Signal
6) *Status 3 LED* – SCC Power Signal

3.4 SCC5Net Switch Rear Connections

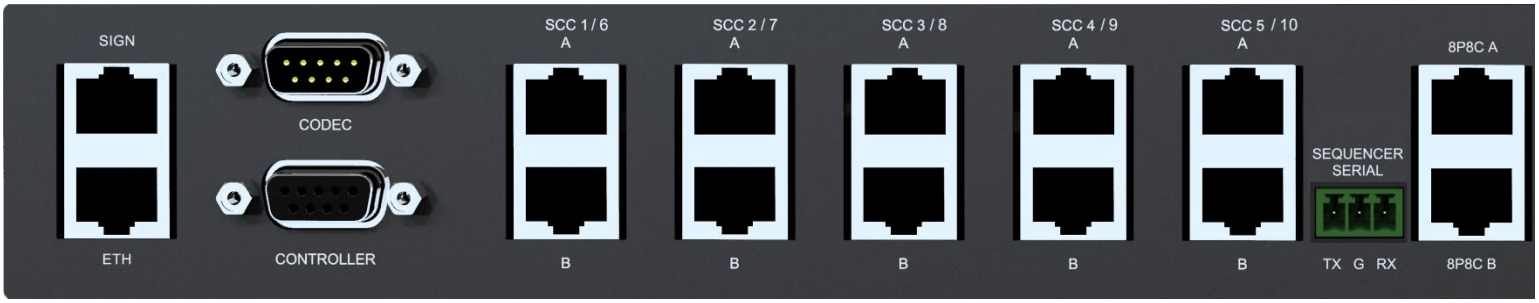


Figure 7 – Freeport SCC5NET Switch (Rear View Detail Left)

1) *SIGN* – Control Port for traditional LED Classification Signage (RS-232/RS-485)
2) *ETH* – TCP/IP Connection to SCC5Net Switch (Web Configuration & API Control)
3) *CODEC* – Serial Communication Path between SCC5Net Switch & CODEC (RS-232)
4) *CONTROLLER* – Serial Communication Path between Third-Party Control & CODEC (RS-232) (This port is used to control the video CODEC via a third-party control system)
5) *SCC 1-5 A* – Mode, Status, Power, & Ground for the Connected SCC Unit
6) *SCC 1-5 B* – Communication Path w/ CODEC, Power, & Ground for the Connected SCC Unit
7) *SEQUENCER SERIAL* – API serial (RS-232: 9600, None, 8, 1) control of the SCC5Net Switch
8) *RJ45 A* – 8P8C Input for PSTN, VOIP, or Unclassified ISDN (512k BRI "U" Interface)
9) *RJ45 B* – 8P8C Output for PSTN, VOIP, or Unclassified ISDN (512k BRI "U" Interface)

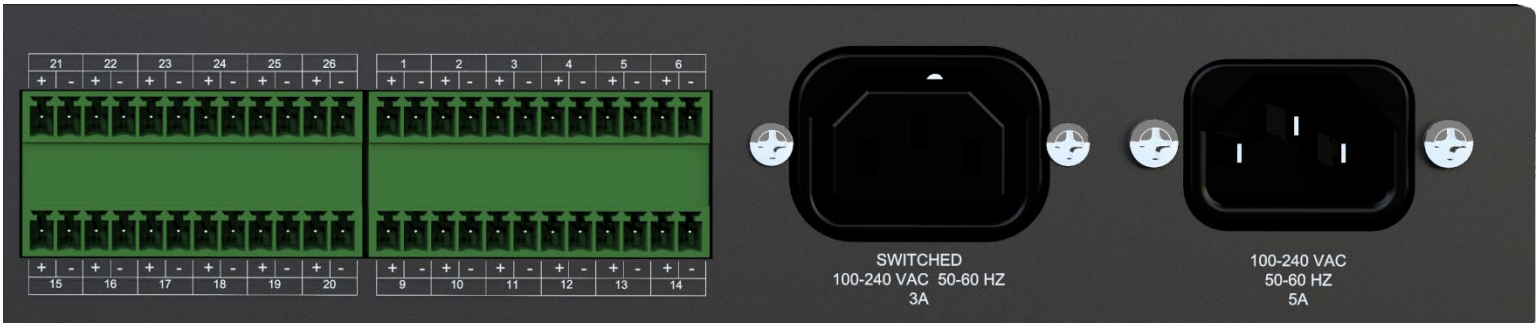


Figure 8 – Freeport SCC5NET Switch (Rear View Detail Right)

1) *TOP 21-26* – Customizable Relays for Control of External Devices (Contact Closure)
2) *BOTTOM 15-20* – Control of Media Converters (Power or Contact Closure)
3) *TOP 1-6* – Fiber Switch Status for Market Central
4) *BOTTOM 9-14* – Fiber Switch Control for Market Central

3.5 Secure CODEC Configurator (SCC)

The Freeport SCC units are the only components of the MDVNS System that interact directly with the video CODEC. The SCC units are used to capture, sanitize, and restore the configuration settings of the CODEC for a particular network or mode.

The communication between the CODEC and each SCC unit is performed over a bi-directional serial connection using the RS-232 communications protocol. The SCC is only connected to the CODEC (through the SCC5NET Switch) when the CODEC has been physically disconnected from all video networks.

Depending on the local IA regulations, an SCC unit may adopt the classification of the network/mode for which it is storing information. A SCC unit being used to store the CODEC configuration, passwords, certificates, user accounts, and directories for a particular network/mode may contain sensitive information and should be treated as such for all applicable security purposes.

Once power is removed from an SCC unit, any CODEC information that might be stored in that unit will be retained. If necessary, the SCC unit's memory can be cleared and reset by performing an automated clean procedure (*Section 6.6 – Sanitizing SCC Units*). If for any reason an SCC unit must be removed from a secure area, the local security officer should be contacted and consulted to ensure all local policy is being enforced.

Figure 9 – Freeport SCC Unit (Front View)

There are three (3) operations that are enacted upon the CODEC by an SCC unit:

1. Capture – The *Capture* operation saves the current configuration settings of the CODEC to the flash memory of the connected SCC unit. The information captured may vary slightly based on the configuration settings supported by the CODEC manufacturer and/or depending on the firmware revision running on the CODEC.
2. Clean – The *Clean* operation automatically removes all information from the CODEC using the manufacturer approved process for a factory reset; therefore, providing an out of box state. The exact sanitization process will vary between different CODEC manufacturer/models.
3. Restore – The *Restore* operation restores the configuration settings that were previously saved to the SCC unit's flash memory by the *Capture* operation (plus any passwords, certificates, users, directories, camera pre-sets, or Post Restore Commands).

Each SCC unit has three (3) local mode settings which direct the unit to perform a specific process after powering on. The local mode settings can be engaged by turning the removable mode key to the desired position, which is located on the front of each SCC unit.

1. Capture – When the mode key is in the *Capture* position, the SCC unit is instructed to save the current configuration settings of the CODEC to flash memory before the CODEC is sanitized and powered off (or put into standby mode).
2. No-Capture – When the mode key is in the *No-Capture* position, the SCC unit is instructed to ignore the current configuration settings of the CODEC before the CODEC is sanitized and powered off (or put into standby mode). Any changes that have been made to the CODEC configuration since joining the currently selected network/mode will not be saved.
3. Auxiliary – The *Auxiliary* mode position can be used to allow a third-party control system to initiate a one-time capture of the current CODEC configuration settings via the MDVNS API.

Each SCC unit has an internal web server which can be accessed via the *Management* port on the rear of the unit (*Section 6 – SCC Options & Maintenance*). It provides a secure web-enabled interface for viewing and managing individual SCC data including System information, licenses and firmware, CODEC settings, CODEC passwords, and CODEC certificates.

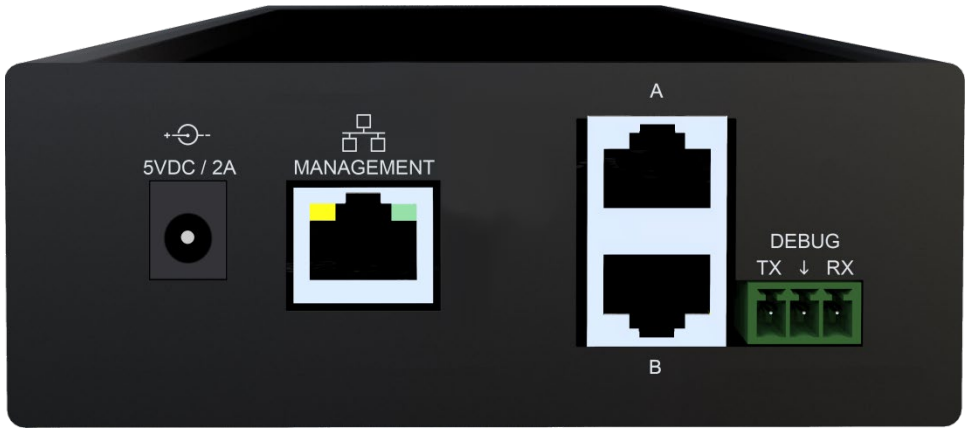


Figure 10 – Freeport SCC Unit (Rear View)

3.6 Fiber Optic Secure Switch

The Freeport MDVNS utilizes a fiber-based switching unit for video network management. The Market Central SecureSwitch® is the main video network switching component and is the only component of the MDVNS system that interacts with the customer provided video networks.

The older generation SecureSwitch® (Rev B, Rev C) can isolate and switch up to 3 networks per enclosure. The current generation (N:1) supports up to 8 networks per enclosure and can be customized based on actual need. Enclosures may be "daisy chained" so that two or more switches can be used to manage the required number of networks (one of the ports must serve as an "uplink" to the main fiber switch).

All network switching operations of the SecureSwitch® are directed by the SCC5Net Switch and controlled via contact closures. The SecureSwitch® provides positioning data back to the SCC5NET Switch to validate and enforce specific periods processing related tasks.

For specifications and operational questions on the SecureSwitch®, please refer to the manufacturer provided documentation (http://secureswitch.com).

3.7 Media Converters

The SecureSwitch® utilizes fiber optic inputs and outputs for all video network connections. The network connection between the SecureSwitch® and the video CODEC is routed through a fiber to copper media converter which provides the required signal conversion. The CODEC media converter is managed by the SCC5Net Switch and is powered down during all network transitions and when the system is not being utilized for video conferencing.

All fiber optic video network connections supplied by the customer can be connected directly to inputs on the SecureSwitch®. However, if a customer provided video network connection is copper (CAT-5/6), it must be run through a media converter to convert it from copper to fiber.

When media converters are required for any of the video network connections, the units power supply should be connected to and managed (powered on/off) by the SCC5Net Switch during the switching process to ensure redundant fault isolation.

When selecting media converters for use with the system the following should be considered:

a. Always choose a 10/100/1000 media converter that can auto-negotiate.
b. Always use media converters in pairs of the same model. Not only should the media converters be used in pairs, but you should also choose the same brand and same model.

The MDVNS system can manage all 5v and 12v powered media converters.

3.8 Classification Signage

Wall mounted classification signage, under control of the SCC5Net Switch, is used to provide the status of the MDVNS system switching process as well as the current network/mode and classification level of the system.

The MDVNS system provides the ability to display *Joining*, *Leaving*, or *On Network/Mode* messages for classification awareness. It also provides switching process feedback such as *System Initializing*, *System Off*, and *Error*.

Traditional LED classification signage can be controlled by the system via an RS-232 or RS-485 connection on the SCC5Net Switch. Integration and configuration (text, color, effect, speed) of room signage is managed through the MDVNS configuration web interface (*Section 5 – System Configuration*).

Alternatively, a third-party AV control system can utilize the MDVNS API to obtain the necessary information needed to display its own switching process status and network/mode information. In addition, custom messages can be written via the API overriding the current messages being displayed by the MDVNS system. Please note that custom sign messages via the API are only available when the MDVNS system is in off mode (CODEC is sanitized and physically disconnected from all video networks).

The MDVNS supports any LED signage that is controllable via RS-232/RS-485 using two-digit hex codes representing extended ASCII characters.

4 Initial System Deployment

At initial system power up, the MDVNS system will be booted to a known state. This occurs by enabling the RS-232 connection between the CODEC and the SCC unit with the highest classification level and putting the CODEC through a series of cleaning operations. This process will sanitize the CODEC and factory default it to an out of box configuration. Any existing configuration settings previously stored in the CODEC will be erased. If you are using an existing CODEC with the system, it is advised that you backup all configuration settings before powering up the MDVNS. In addition, any passwords that might exist in the CODEC should be cleared otherwise the system will not be able to complete its initialization.

Once all system components have been fully connected power is applied to the system. As the system initializes, the system API will transmit a "Please wait" message and any connected classification signage will temporarily show whatever was last displayed before it was powered off.

Once the SCC5Net Switch has initiated its boot cycle the classification signage will show a "System Initialization…" message. When the process is complete the LCD on the front of the SCC5Net Switch will display the network/mode selection screen and the classification signage will either go blank or display the *System Off* message. The system is now in "No Network/Mode" or off mode (the CODEC will be powered off, all SCC units will be powered off, and all video network connections to the CODEC will be disabled).

4.1 General System Information

Basic MDVNS system information can be accessed via the front panel LCD of the SCC5Net Switch. System information includes the version of active firmware, network information (IP Address, Subnet Mask, and Default Gateway), and the LINK status of the Ethernet connection on the back of the SCC5Net Switch.

To access the MDVNS system information via the front panel LCD of the SCC5Net Switch, execute the following procedures:

1. Using the **Up/Down** and **Ok** buttons on the front of the SCC5Net Switch navigate to the main menu and select "System Info".
2. Use the **Down** button to scroll through the system information.
3. Exit System Info by pressing the **Up/Down** buttons until the LCD display reads "Exit". Press the **Ok** button to exit.

4.2 Capturing CODEC Configuration Settings

To setup an initial configuration for the video CODEC or modify an existing configuration for a specific network/mode, execute the following steps.

1. Ensure that the Mode Selection Key of the SCC unit assigned to the desired network/mode is in the "*Capture"* position.
2. Using the buttons on the front of the SCC5Net Switch (or third-party control system) select the desired network/mode.

3. Once the system has finished transitioning to the selected network/mode, configure the CODEC with the desired settings using the CODEC web interface and/or the manufacturer provided touch panel.

   **Passwords and certificates cannot be captured by an SCC unit. Those settings should NOT be entered via the CODEC web or user interface. Refer to Section 6 – SCC Options & Maintenance for the steps required to store passwords and certificates for each network.*

4. Using the buttons on the front of the SCC5Net Switch (or third-party control system) select Off mode.

When the operation is complete:

a. The CODEC will be in a factory default out of box state and powered off.
b. All CODEC configuration settings for the last selected network/mode that were just configured have been stored in the flash memory of the corresponding SCC unit.
c. The system will be in Off (standby) mode.

Repeat this procedure for each network/mode that the MDVNS system supports.

Please note that the Mode Selection Key of an SCC unit MUST remain in the "Capture" position to capture future configurations changes. If the SCC is set to "No Capture", future changes will NOT be saved.

4.3 Network/Mode Selection

To utilize the video CODEC for a local presentation and/or video conference, select the desired network/mode via the SCC5Net Switch front panel (or third-party control system).

Ensure that the SCC Mode Selection Keys (located on the front of each SCC unit) are in the desired position. For daily operation, the SCC units should be set to "No-Capture" mode.

1. Using the **Up/Down** and **Ok** buttons on the front of the SCC5Net Switch, navigate to the main menu and select "Network Select".
2. Use the **Up/Down** buttons to select the desired network/mode you wish to configure the CODEC for,
   followed by the **Ok** button.
3. When the operation is complete the CODEC will be configured with the settings that were last captured to the associated SCC unit and physically connected to the selected video network.

*Please note that the system configuration (networks vs. modes) will determine if the CODEC is physically connected to a video network after it has been configured by the SCC unit.

Much of the time that it takes to perform a network/mode transition is primarily dependent on the boot time of the video CODEC, which varies by model/manufacturer. Once the transition is complete the classification signage will confirm your selection and the video output of the CODEC will be shown on your display(s).

5 System Configuration

The MDVNS system is configured using a secure web interface which can be utilized to modify the default configuration settings or to add additional networks/modes to the system as required.

In addition to modifying configuration settings, the web interface can be used to update system firmware and access system logs.

The system's web interface can be accessed by directing a standard web browser to the IP address of the SCC5Net Switch:

1. Connect your computer to the *Eth* port on the rear of the SCC5Net Switch using a standard Ethernet cable.
2. Ensure that the network settings of your computer are compatible with the MDVNS (e.g. Device IP Address = 192.168.5.50, Device Subnet Mask = 255.255.255.0).
3. Open a standard web browser. In the browser address line, enter the IP address of the SCC5Net Switch using the https://IPAddress format. The default entry for a Freeport provided SCC5Net Switch would be: https://192.168.5.95
4. Log into the SCC5Net Switch using the correct username and password. The default settings provided by Freeport are *username = sysop, password = freeporttech*

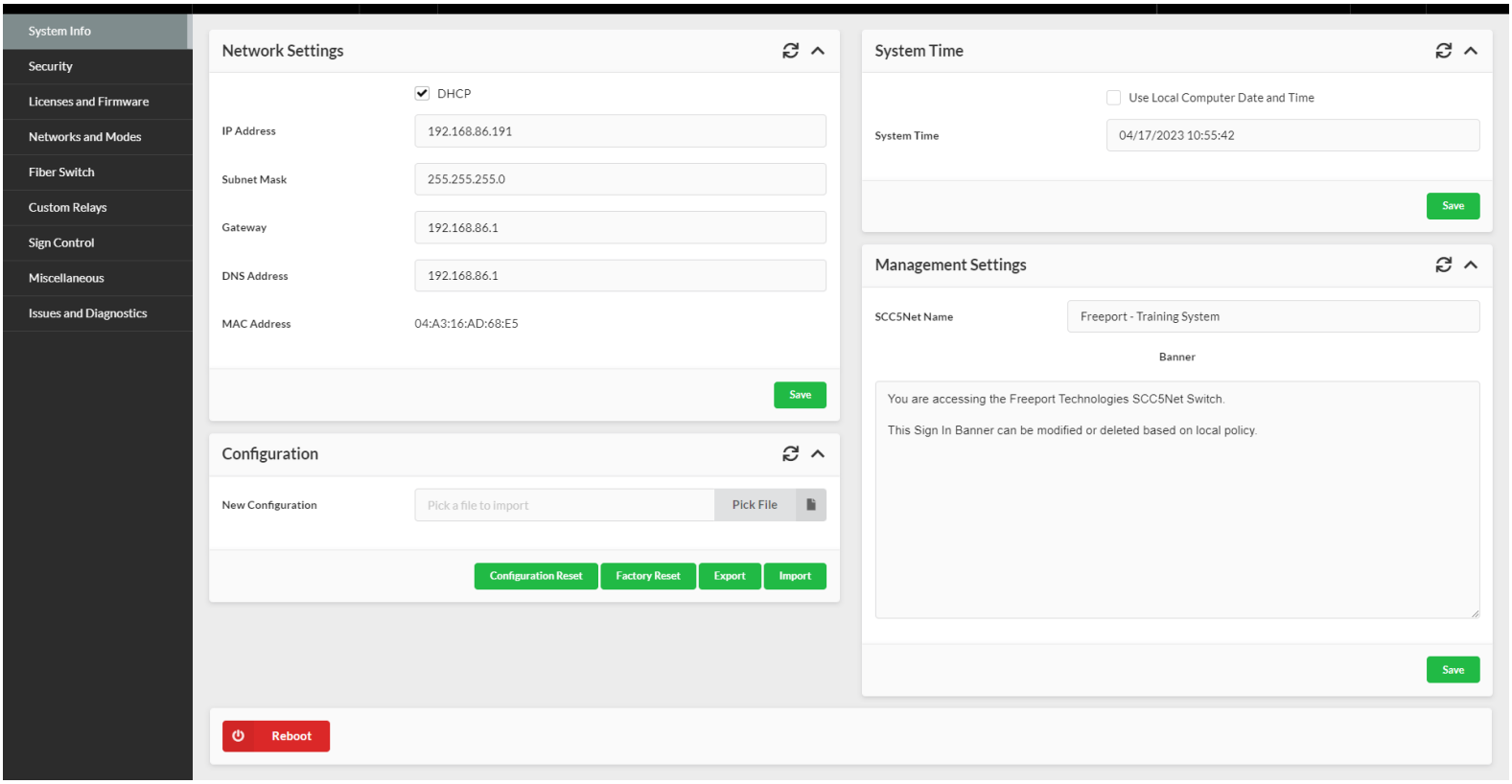


Figure 11 – SCC5Net Switch Web Interface (System Info)

5.1 System Info

Network Settings – View or change the network configuration settings of the SCC5Net Switch (IP Address/Subnet/Gateway, DNS Address, MAC Address)

System Time – Set the system date and time

Configuration – Configuration Reset (reverts to default configuration), Factory Reset (reverts to default configuration and deletes network/mode settings including logs), Export, or Import the SCC5Net Switch configuration. This feature can be used to create a backup of the entire SCC5Net Switch including any SCC5Net Switch license keys.

Management Settings – The SCC5Net Name is the name that will be used to represent the associated SCC5Net Switch throughout the web interface and in the FMS application. The Sign-In Banner allows you to create a custom acknowledge banner that will be displayed when accessing the web interface of the SCC5Net Switch.

5.2 Security

SCC5Net User Management – Create, update, and delete system users. Users can currently be assigned Admin and API roles.

Password Settings – Provides the ability to enforce specific user password attributes (length, uppercase/lowercase characters, numerical digits, special characters, max failed logins, session expiration, etc.)

Centralized User Management (Active Directory) – Enables Active Directory server integration using NTLM authentication. TLS and DNS are required for the connection to the AD server. The certificate will be verified against the Certificate Authorities uploaded to the SCC5Net Switch and the hostname of the AD server will be verified against the certificate.

To log into the SCC5Net Switch user interface, enter the username in the format <domain>\<username> and check the “Login to Active Directory” box.

Authorization is configured on the SCC5Net Switch. To enable web login, add usernames (in the above format) to the “AD Admin Users” list on the security page of the configuration interface.

5.3 Licenses & Firmware

Firmware – View or update the firmware of the SCC5Net Switch

License Keys – View or update the SCC5Net Switch license keys

Web Server Certificate – Provides the ability enable a secure connection with the SCC5Net web server

Certificate Authorities – Provides the ability to upload certificate authorities to verify external network connections

5.4 Networks & Modes

SCC5Net Switches – Add a secondary SCC5Net Switch for systems that require more than 5 networks

Network/Mode Count – Modify the network/mode count

Name – The name that will be used to represent the associated network/mode throughout the web interface. It will also be displayed on the front panel LCD of the SCC5Net Switch and on the Cisco Touch for network/mode selection.

Classification – Identifier that can be used by a third-party control system via the API

SCC ID – The SCC unit that will connect to the CODEC when the associated network/mode is selected

Media Converter Relay – The relay on the SCC5Net Switch that will be used to manage the media converter when the associated network/mode is active. Media converter relays (15-19) cannot be assigned to multiple networks/modes.

Color – The color used to represent the associated network/mode throughout the web interface

Joining Power Cycle Duration – Determines if the CODEC will be power cycled when joining the associated network/mode (this event occurs after the CODEC has been configured).

Leaving Power Cycle Duration – Determines how long the CODEC will be power cycled when leaving the associated network/mode (this event occurs after the CODEC has been factory defaulted to an out of box state).

Enable 8P8C Connector – Determines if the 8P8C/RJ-45 (used for PSTN, VOIP or ISDN) pass-through on the SCC5Net Switch is active when the associated network/mode is selected

Enable Cisco ISDN Link – Enables pairing and un-pairing of a Cisco ISDN Link when the associated network/mode is selected

Connect CODEC to Network – Provides the ability to create a network/mode in which the CODEC is configured by the assigned SCC unit but is physically disconnected from all video networks. When a network/mode is selected with this feature is disabled, the media converter between the CODEC and the Fiber Switch is powered off and the Fiber Switch is moved to the null position (if available).

Default Clean Network – Assigns the associated SCC unit as the default SCC used for cleaning the CODEC during system initialization and error recovery

Factory Reset CODEC Before Switching Mode – This setting is only available if the "*Connect CODEC to Network"* option is NOT selected. Enabling this setting will initiate the CODEC sanitization process when transitioning to another mode (not network). If this setting is NOT enabled, the system will transition to another mode without sanitizing the CODEC.

5.5 Fiber Switch Configuration

Fiber Switch Port Count – Specifies how many ports are available for video network management

The fiber switch settings can be modified using the table provided in the SCC5Net web interface. The SCC5Net relay numbers (9 – 14) can be used to select which port on the fiber switch will be active when the associated network/mode is selected. Clicking on a specific relay number in the table provides the ability to assign custom text to that relay to visually represent the ports on the fiber switch being used.

5.6 Custom Relays

The SCC5Net Switch can utilize relays to manage external devices used for isolating computers/workstations, or table/wall transmitters that have audio and video outputs connected to the content port of the video CODEC (either directly, via a KVM, or via a matrix switcher). This feature

also supports a variety of other devices that might require a state change based on the selected network/mode that is active (White Noise Generator, Shades, LED Indicators, etc).

The relay tab of the SCC5Net web interface can be used to designate the status of the six (6) relays when a specific network/mode has been selected. The relay will be active (closed) when the check box is selected and in-active (open) when the check box is blank.

Clicking on a specific relay number in the table provides the ability to assign custom text to that relay to visually represent how those relays are being utilized.

The state of the customizable relays can also be controlled via a third-party control system via the MDVNS API. Relays requiring external control must be designated as "API Controllable".

Refer to *Appendix F – SCC5Net Switch Relay Control* for the steps required to connect external devices to the relays on the rear of the SCC5Net Switch.

5.7 Sign Control

Sign Type – The sign type (None, Alpha, Custom) will determine how the system interprets and executes sign related messages

Sign Serial Protocol – Designates the sign serial protocol (RS-232, RS-485) of the SIGN port on the back of the SCC5Net Switch

Sign Serial Settings – If a "Custom" sign is being utilized, the serial settings of the sign must be defined (Baud, Data Bits, Parity, Stop Bits)

Sign Code Byte Delay – If the system is using a "Custom" sign type, a delay (in milliseconds b/t 0 and 250) between each byte of sign data may be necessary

Active Sign Message/Code – Provides the ability to assign specific text, mode, speed, and color on the LED room signage when the associated network/mode is active

Joining Sign Message/Code – Provides the ability to assign specific text, mode, speed, and color on the LED room signage when joining the associated network/mode

Leaving Sign Message/Code – Provides the ability to assign specific text, mode, speed, and color on the LED room signage when leaving the associated network/mode

System Off Sign Message/Code – Provides the ability to assign specific text, mode, speed and color on the LED room signage when the system is turned off (or in standby mode)

System Initializing Sign Message/Code – Provides the ability to assign specific text, mode, speed, stop time, alignment, and color on the LED room signage during system initialization

System Error Sign Message/Code – Provides the ability to assign specific text, mode, speed and color on the LED room signage when there is a system error

System Maintenance Sign Message/Code – Provides the ability to assign specific text, mode, speed and color on the LED room signage when the system is put in maintenance mode

5.8 Miscellaneous System Settings

CODEC Power Switch – Allows for the utilization of a web-controlled AC switched power supply for CODECs which are unable to be plugged directly into the back of the SCC5Net Switch.
Refer to *Appendix H – Web Controlled CODEC Power Switch* for more information.

Post Restore Power Cycle Delay – If a "Joining Power Cycle Duration" is being used this setting will determine the number of seconds to wait before the CODEC power cycle is initiated (Some CODECs require additional time to process configuration settings before power can be removed and reapplied).

Keep CODEC Power On When Off Network – Provides the ability to decrease system transition times when joining a network from off mode. When the system transitions to off mode the CODEC will be put through the standard sanitization process (factory defaulted and disconnected from all active networks), however, it will stay powered on.

8P8C Connector Enabled When Off – Determines if the 8P8C/RJ-45 (used for PSTN, VOIP or ISDN) pass-through on the SCC5Net Switch is active when the system is turned off (or in standby mode)

Enable Network API Access (Unsecured) – Enables TCP/IP access to the MDVNS API on port 2303 for third-party control. Please note that enabling this feature requires a reboot.

Encrypt Network API – Enables TLS 1.2 encryption for third-party control system connections. Encryption is off by default for any systems with legacy firmware. If a new system is pre-configured by Freeport with the API enabled, encryption is enabled by default.

Authenticate Network API – Enables authentication for third-party control system connections. Authentication is off by default for any systems with legacy firmware. If a new system is pre-configured by Freeport with the API enabled, authentication is enabled by default. The username for the API is "roomcontrol" with a default password of "freeporttech". Navigate to the *System Info* tab of the SCC5Net web interface to change the password.

Network API Session Timeout (minutes) – Enables session timeout enforcement when utilizing a 3rd party control system.

SCC Power On Timeout (seconds) – The number of seconds that the SCC5Net Switch will wait for an SCC Unit to confirm it has powered on and booted up.

SCC Join/Leave Timeout (seconds) – The number of seconds that the SCC5Net Switch will wait for an SCC Unit to complete the Join or Leave process before throwing a system error.

SCC5Net Serial Function – The serial port on the back of the SCC5Net Switch can be disabled, used for external control of the MDVNS (via 3rd party control system), used to control an additional LED room sign (RS-232 only), or used to integrate a Cisco Touch 10 for In-Room Control of the MDVNS.

Serial Port Settings – If the serial port on the back the SCC5Net Switch is being utilized for 3rd party control, the serial settings must be defined (Baud, Data Bits, Parity, Stop Bits)

System Type – If the SCC5Net Switch that you are logged into is the secondary switch used in a system with more than 5 video networks, "Secondary" must be selected in the drop-down window. Assigning a SCC5Net Switch the role of secondary will remove all unnecessary features and functions from the web interface. Please note that any previous configuration settings will be retained and restored if the role of the SCC5Net Switch changes back to "Primary".

5.9 Issues and Diagnostics

Potential Issues – Provides a description and possible resolution for any active system issues.

Notifications – Provides the ability to configure an SNMP manager to receive real-time notifications or trap messages.

System Logs – View or download the system logs. The most recent system logs will be located at the top of the drop-down list and NOT have a date listed as part of the file name. The “Download All Logs” option will include the 5Net configuration in the file. The “Delete Log Files” option allows you to clean up and remove logs based on the date that is entered.

Syslog Settings – Provides the ability to configure a syslog server for system monitoring.

6 SCC Options & Maintenance

Each Freeport SCC unit has a secure web server which provides an interface for viewing and managing general system information, licenses and firmware, CODEC settings, passwords, and certificates.

The web interface for each SCC unit can be accessed by connecting a computer to the *Management* port of the SCC unit and putting the system in *Maintenance Mode*:

1. Ensure that the MDVNS system is in Off mode.
2. Using the **Up/Down** and **Ok** buttons on the front of the SCC5Net Switch navigate to and select "Maintenance Mode".
3. Use the **Up/Down** buttons to select the desired SCC you wish to connect to, followed by the **Ok** button.
4. Connect your computer to the *Management* port on the rear of that SCC unit using a standard Ethernet cable.
5. Ensure that the network settings of your computer are compatible with the MDVNS (e.g. Device IP Address = 192.168.5.50, Device Subnet Mask = 255.255.255.0)
6. Open a standard web browser. In the address line, enter the IP address of the connected SCC unit using the https://IPAddress format. The default entry for all out of box Freeport SCC units is https://192.168.5.100.
7. Log into the SCC unit using the correct username and password. The default settings provided by Freeport are *username = sysop, password = freeporttech*

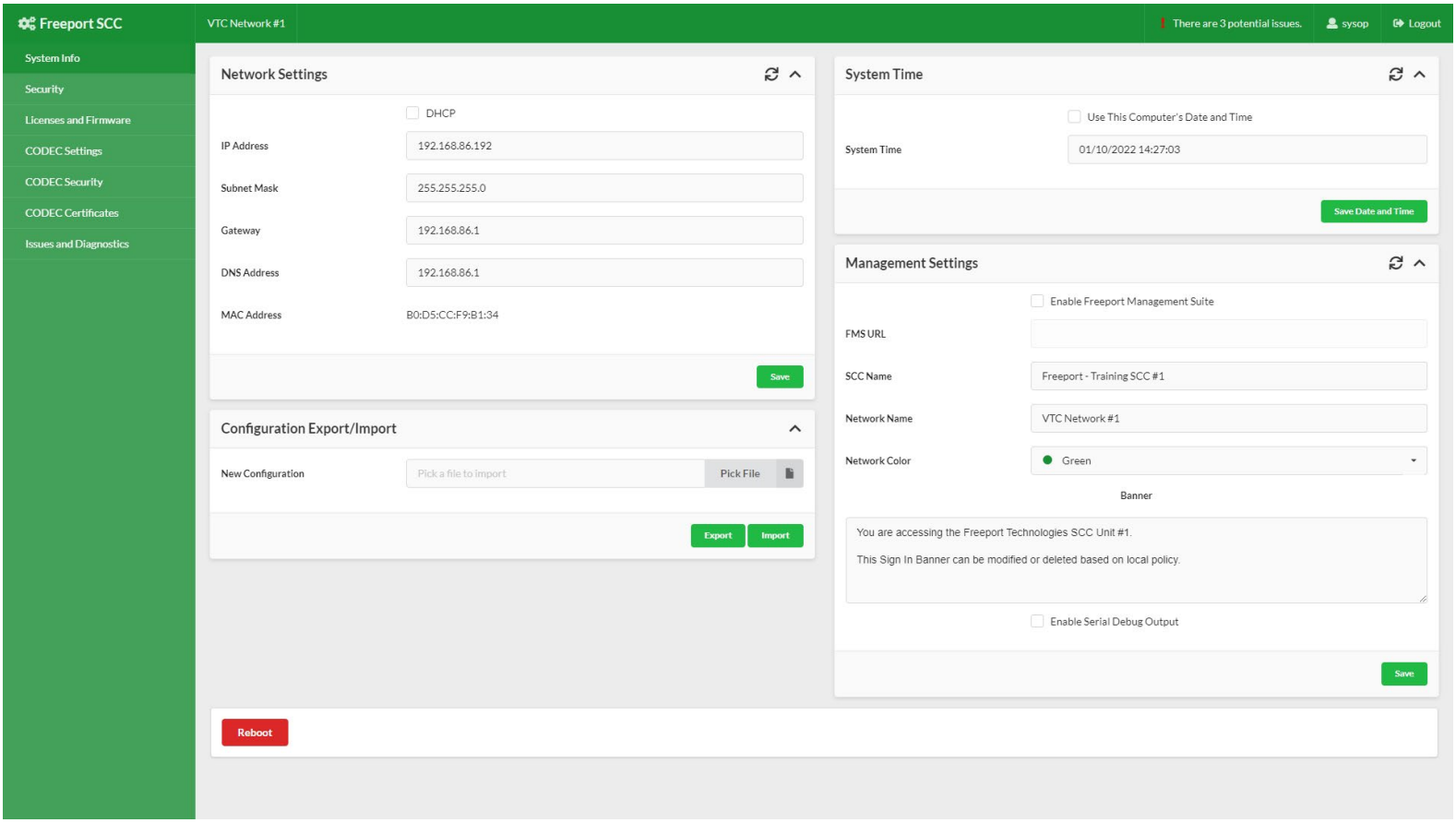


Figure 13 – SCC Web Interface (System Info)

6.1 SCC System Info

Network Settings – View or change the network configuration settings of the SCC Unit

(Enable/Disable DHCP, Static IP Address/Subnet/Gateway, DNS Address, MAC Address, CODEC Name)

System Time – Set the SCC unit date and time

Configuration Export/Import – Export or import the SCC unit's configuration. This feature can be used to create a backup of the entire SCC including all SCC settings, CODEC settings, and encrypted passwords and certificates. It also includes any SCC license keys.

Management Settings – Enable/Disable the use of FMS for the associated video network. If enabled, view or edit the FMS URL (e.g. https://IPAddress/SCCManager).

SCC Name – The name that will be used to represent the associated SCC throughout the FMS web interface

Network Name – The name that will be used to represent the associated network/mode throughout the SCC web interface

Network Color – The color used to represent the associated network/mode throughout the SCC web interface

Sign-In Banner – Create a custom acknowledge banner that will be displayed when accessing the web interface of the SCC Unit for the associated video network

Enable Serial Debug Output – Enables the serial port on the back of the SCC unit for real time logging via a device running a terminal emulation program (PuTTy, HyperTerminal, etc). The terminal emulator settings are: 115200 (Baud), 8 (Data Bits), None (Parity), 1 (Stop Bits).

6.2 Security

SCC User Management – Create, update, and delete system users.

Password Settings – Provides the ability to enforce specific user password attributes (length, uppercase/lowercase characters, numerical digits, special characters, max failed logins, session expiration, etc.)

Centralized User Management (Active Directory) – Enables Active Directory server integration using NTLM authentication. TLS and DNS are required for the connection to the AD server. The certificate will be verified against the Certificate Authorities uploaded to the SCC and the hostname of the AD server will be verified against the certificate.

To log into the SCC user interface, enter the username in the format <domain>\<username> and check the "Login to Active Directory" box.

Authorization is configured on the SCC. To enable web login, add usernames (in the above format) to the "AD Admin Users" list on the security page of the configuration interface.

6.3 SCC Licenses & Firmware

Firmware – View or update the firmware of the SCC unit

License Keys – View or update the SCC firmware license keys

Web Server Certificate – Provides the ability enable a secure connection with the SCC web server

Certificate Authorities – Provides the ability to upload certificate authorities to verify external network connections

6.4 CODEC Settings

SX20/MX200/MX300 G2 – This setting modifies the baud rate that the SCC units will use to communicate to the CODEC if one of these specific models is being utilized

Firmware Type – Used to identify the generation (TC or CE) of firmware currently installed on the CODEC that is being connected to the SCC units

Factory Default Type – Instructs the SCC to either shutdown or reboot the CODEC after it has been put through the sanitization process

Post-restore Reboot – This setting can be used when post restore commands (*Section 7 – Post Restore Commands*) are being utilized. It instructs the SCC to reboot the CODEC before or after the commands are sent, or not at all.

Camera Preset Delay – The delay (in seconds) used between positioning the camera and saving that position as a preset. The value defaults to 5, and in that case, the SCC would position the camera, wait 5 seconds, and then save it as a preset.

Ignore Camera Preset Failures – Ensures a more reliable network/mode transition if there are many camera presets being restored. If set to "True" the SCC units will allow up to 180 seconds to complete the camera preset restoration process.

ISDN Link Enabled – Enables/Disables automatic pairing and un-pairing of ISDN LINK

Capture with SerialPort LoginRequired: Off – This setting only affects early versions of CE firmware (CE9.2.5)

Use SCC Clock – Allows you to set the date/time of the CODEC using the SCC internal clock

CODEC Model – Lists the model of the CODEC

CODEC Firmware Version – Lists the currently installed firmware of the CODEC

CODEC Baud Rate – Lists the default baud rate of the CODEC (this cannot be changed)

Camera Presets – View or edit the last captured CODEC camera presets for the associated network/mode. Please refer to the Cisco API Reference Guide before adding, deleting, or editing camera presets.

Configuration – View or edit the last captured CODEC configuration for the associated network/mode. Please note that these xConfiguration items may vary depending on the model of CODEC being utilized and/or the Cisco firmware installed on that CODEC. Please refer to the Cisco API Reference Guide before adding, deleting, or editing an xConfiguration item.

Directory – View or edit the last captured CODEC directory entries for the associated network/mode. Please refer to the Cisco API Reference Guide before adding, deleting, or editing directory entries.

Post Restore Commands – View or edit any post restore commands for the associated network/mode. Please note that xCommands may vary depending on the model of CODEC being utilized and/or the Cisco firmware installed on that CODEC. Please refer to the Cisco API Reference Guide before adding, deleting, or editing an xCommand.

Pre-Sanitize Commands – View or edit any pre-sanitize commands for the associated network/mode. Refer to *Section 9 – Pre-Sanitize Commands* for more details.

Sign-In Banner – View or edit the last captured CODEC acknowledgement banner (shown when logging into the CODEC web interface) for the associated network/mode

6.5 CODEC Security

CODEC Admin Account – View or edit the admin username and password of the video CODEC for the associated network/mode. Please note that if you change the admin username the default root admin account will be disabled.

CODEC Passwords –The CODEC passwords (H.323, SIP, IEEE802.1x, HTTP Proxy, Provisioning, etc.) that can be modified for the associated network/mode are dependent on the CODEC make/model and firmware that is installed on the device. Please note that CODEC passwords must be manually entered via the SCC web interface, CODEC passwords can NOT be captured by an SCC unit during normal system operation.

CODEC Users – View the list of user accounts and/or edit the user account passwords. Please note that CODEC user accounts along with their associated status and roles can be captured by an SCC unit but the passwords cannot. If user account passwords are not configured via the SCC web interface the user accounts will be restored to the CODEC but will be set as inactive.

6.6 CODEC Certificates

Certificate Authorities – Add or view a CA certificate for the associated network/mode

Service Certificates – Add or view a Service certificate for the associated network/mode. Service certificates can be added without a private key, with a private key, or with a private key encrypted with a password.

*Please note that loading certificates into the CODEC during the join process requires an automatic reboot of the CODEC. This is enforced by Cisco and cannot be disabled as of now.

Refer to *Appendix K – Certificate Management with CUCM* for more details on CODECs that are being managed by Cisco Unified Communications Manager.

6.7 Issues and Diagnostics

Potential Issues – Provides visual feedback on potential system issues.

Notifications – Provides the ability to configure an SNMP manager to receive real-time notifications or trap messages.

System Logs – View, download or delete the SCC unit logs

Syslog Settings – Provides the ability to configure a syslog server for system monitoring.

6.8 Sanitizing an SCC Unit

To remove all video CODEC configuration settings, camera pre-sets, directory entries and user accounts that were last captured to a specific SCC unit, execute the following steps:

1. Ensure that the MDVNS system is in Off mode
2. Using the **Up/Down** and **Ok** buttons on the front of the SCC5Net Switch navigate to and select “Maintenance Mode”.

3. Use the **Up/Down** buttons to select the desired network/mode of the SCC you wish to sanitize, followed by the **Ok** button.
4. The selected SCC unit will power on and all LEDs will briefly illuminate. Once the SCC unit initializes the "Power" and the "Loaded" LEDs will illuminate.
5. Press and hold the "Clean" button on the front of the SCC unit for **one (1)** second. The "Proc" LED will illuminate briefly and then turn off.
6. Confirm that the SCC unit has been wiped of ALL CODEC settings for that specific network/mode by verifying that the "Loaded" LED begins to flash.
7. Repeat steps two through six if you wish to sanitize the CODEC configuration settings of another SCC unit.
8. Turn Maintenance Mode off by pressing the **Up/Down** buttons on the front of the SCC5Net Switch until the LCD display reads "Exit". Press the **Ok** button to turn off Maintenance Mode and exit to the main menu.

Please note that sanitizing an SCC unit will not remove any SCC related settings (Network/Mode Settings, System Time, System Logs, SCC Manager Settings, Sign-In Banner, etc.) or CODEC settings that are configured via the SCC web interface (General Settings, Passwords, Certificates, etc.).

6.9 Factory Default an SCC Unit

To remove ALL data from a specific SCC unit and return it to a factory default state with an IP address of 192.168.5.100, execute the following steps:

1. Ensure that the MDVNS system is in Off mode
2. Using the **Up/Down** and **Ok** buttons on the front of the SCC5Net Switch navigate to and select "Maintenance Mode".
3. Using the **Up/Down** buttons to select the desired network/mode of the SCC you wish to factory default, followed by the **Ok** button.
4. The selected SCC unit will power on and all LEDs will briefly illuminate. Once the SCC unit initializes the "Power" and the "Loaded" LEDs will illuminate.
5. Press and hold the "Clean" button on the front of the SCC unit for **three (3)** seconds.
6. The "Proc" LED will briefly illuminate two times and then turn off. This will confirm that the SCC unit has been factory defaulted. In addition, the "Loaded" LED will turn off.
7. Final confirmation can be obtained by pinging the default IP address of an out of box SCC unit (192.168.5.100).
8. Repeat steps two through six if you wish to factory default another SCC unit.
9. Turn Maintenance Mode off by pressing the **Up/Down** buttons on the front of the SCC5Net Switch until the LCD display reads "Exit". Press the **Ok** button to turn off Maintenance Mode and exit to the main menu.

7 Post Restore Commands

The MDVNS system is only capable of capturing and restoring configuration settings that are made available by the CODEC manufacturer via the RS-232 API. Some settings which the manufacturer may have deemed as “commands” cannot be captured by the system’s SCC units.

Post restore commands provide the ability to instruct an SCC unit to direct the CODEC to perform an operation that the SCC could not otherwise automate during the restore process using xConfiguration variables. Any post restore commands that have been added and saved to a specific SCC unit will get sent directly to the CODEC via RS-232, line by line, after the SCC has finished restoring the standard settings.

Please note that some xCommands may require a reboot of the CODEC to be applied. This can be managed using the “Post-restore Reboot” option listed on the *CODEC Settings* tab of the SCC web interface.

Refer to *Section 6 – SCC Options & Maintenance* for the steps required to view and/or edit post restore commands for each video network/mode.

8 Pre-Sanitize Commands

Pre-sanitize commands provide the ability to instruct an SCC unit to direct the CODEC to perform an operation before the MDVNS puts the CODEC through the sanitization process. Any pre-sanitization commands that have been added and saved to a specific SCC unit will get sent directly to the CODEC via RS-232, line by line, before the CODEC is sanitized. Please note that if the SCC unit is in “capture” mode, the commands will be sent after the capture process has been completed.

Each line will be treated as a command. Commands are case insensitive and will not be retried:

1. Any commands that begin with "xConfig" will expect an "OK" response. Commands that begin with "xCommand" will expect a response containing "status=OK" and "** end". If the expected response is not received, a warning will be logged along with the response received from the CODEC.
2. Commands starting with "Sleep" followed by an integral number 1 - 15 will result in a delay for that number of seconds. "Sleep" followed by an integer larger than 15 will result in a warning and a 15 second delay. Anything else following "Sleep" will result in an error logged and no delay.
3. Commands that don't begin with any of the above will be sent as is and the response, up to 100 bytes, will be logged.

Refer to *Section 6 – SCC Options & Maintenance* for the steps required to view and/or edit pre-sanitize commands for each video network/mode.

9 System Firmware

All system firmware can be viewed and updated via the web interfaces of the system hardware components. Refer to *Section 5 – System Configuration* and *Section 6 – SCC Options & Maintenance* for the steps required to update both the SCC5Net Switch and SCC unit firmware.

10 System Logs

All system logs can be viewed and/or downloaded via the web interfaces of the system hardware components. Refer to Refer to *Section 5 – System Configuration* and *Section 6 – SCC Options & Maintenance* for the steps required to view and/or download both the SCC5Net Switch and SCC unit logs.

Appendix A
Default TCP/IP Connection Properties

All Freeport MDVNS system components ship with default TCP/IP settings.

SCC5Net Switch TCP/IP Settings

SCC5Net Switch (Primary) = 192.168.5.95
SCC5Net Switch (*Secondary) = 192.168.5.94

Subnet Mask = 255.255.255.0
Gateway = 192.168.5.1

* A second SCC5Net Switch is required for any systems supporting more than 5 networks/modes.

Refer to *Section 5 – System Configuration* for the steps required to modify the TCP/IP settings for the SCC5Net switch.

SCC5Net Switch Factory Reset

Using the Up/Down and Ok buttons on the front of the SCC5Net Switch, navigate to the main menu and select “Functions”. The “Factory Reset” function will erase all configuration settings of the SCC5Net Switch and return it to an out of box state.

The password will be set to the factory default setting (*password = freeporttech)*.

SCC Unit TCP/IP Settings

All SCC units are shipped with a default IP address of 192.168.5.100.

Subnet Mask = 255.255.255.0
Gateway = 192.168.5.1

Refer to *Section 6 – SCC Options & Maintenance* for the steps required to modify the TCP/IP settings for a specific SCC unit. Please note that if an SCC unit has been factory defaulted the IP address will revert to the default of 192.168.5.100.

Appendix B
RS-232 Control of SCC5Net Switch

The Freeport SCC5Net Switch provides a basic API for 3rd party control via RS-232 if TCP/IP control is not desirable. This method of control utilizes a 3 Pin Female 3.81mm Phoenix connector labeled *Sequencer Serial* (located in the middle on the back of the SCC5Net Switch). Please note that a system reboot is required to enable this feature.

Serial Port Function Setting

The system must be configured via the SCC5Net web interface to utilize this serial port for API control. The web interface can be accessed by directing a standard web browser to the IP address of the SCC5Net Switch:

1. Connect your computer to the *Eth* port on the rear of the SCC5Net Switch using a standard Ethernet cable.
2. Ensure that the network settings of your computer are compatible with the MDVNS (e.g. Device IP Address = 192.168.5.50, Device Subnet Mask = 255.255.255.0).
3. Open a standard web browser. In the browser address line, enter the IP address of the SCC5Net Switch using the https://IPAddress format. The default entry for a Freeport provided SCC5Net Switch would be: https://192.168.5.95
4. Log into the SCC5Net Switch using the correct username and password. The default settings provided by Freeport are *username = sysop, password = freeporttech*
5. Select the Miscellaneous tab and use the *Serial Port Function* drop down box to select "Control" as the applied setting. The serial settings (Baud, Parity, Data Bits, Stop Bits) can be modified from the default if required.
6. Use the "Save Configuration" button on the bottom of the tab to save all modifications.
7. Select the System Info tab and use the "Reboot" button to reboot the system

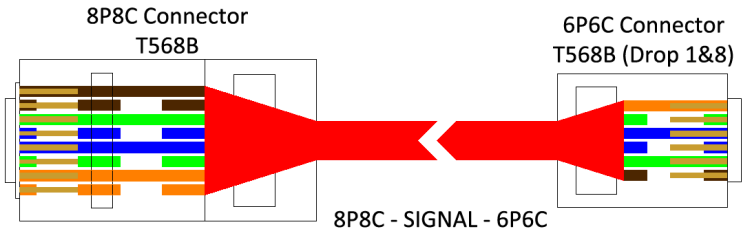
Default Control System Settings

RS-232
Baud: 9600
Parity: None
Data Bits: 8
Stop Bits: 1

Appendix C
Classification Signage Cable Schematics

Alpha-American LED Signs

A customized Ethernet cable with 8P8C and 6P6C connectors is required to connect an Alpha LED sign to the *SIGN* port on the rear of the SCC5Net switch. The customized cable for each supported model must be configured as shown below:



8P8C - SIGNAL - 6P6C		
1	ORANGE/WHITE (N/A)	DROP
2	ORANGE (GND)	1
3	GREEN/WHITE (RS485+)	2
4	BLUE (RS232 TX)	3
5	BLUE/WHITE (RS232 RX)	4
6	GREEN (RS485-)	5
7	BROWN/WHITE (+5VDC)	6
8	BROWN (N/A)	DROP

Figure 14 – Alpha 215C/213C/220C (RS-485/RS-232)

Notes:

1. Alpha models 215C/220C (RS-485) may be daisy chained to provide additional signage. An Ethernet cable with a T568B wiring pattern utilizing 6P6C connectors on each end can be used to connect additional signs as needed.
2. The Alpha 213C (RS-232 only) cannot be daisy chained.

Other LED Signs

The MDVNS supports any LED signage that is controllable via RS-232/RS-485 using two-digit hex codes representing extended ASCII characters. Please refer to the 8P8C connector pin-out depicted in the image above for proper cable termination.

Refer to *Section 5 – System Configuration* for the steps required to integrate a non-Alpha LED sign. The SCC5Net Switch must be configured with a "Sign Type" of "Custom". The *Networks & Modes* and *Sign Control* pages can then be used to assign specific sign codes for each supported sign message. If required, the *Sign Control* page can be used to change the sign serial settings (Baud, Data Bits, Parity, Stop Bits) and add a delay if required.

When entering custom sign codes printable characters can be entered as is, while non-printable characters are entered with a backslash followed by the hex code for that character. The basic algorithm sends every character to the sign as written unless that character is a backslash. If it is a backslash, it will expect the next character to be a hex code and will send that value. A carriage return or line feed requires the appropriate hex code (\0A or \0D).

Example: \00\00\00\00\00\01\5A\30\30\02\41\30\1B\30\62\17\1A\34\1C\31Custom Message\04

Appendix D
Market Central Cable Schematics

Market Central SecureSwitch® Rev B/C

The Freeport MDVNS utilizes the following custom cable set (provided by Freeport) for both control and status of the Market Central SecureSwitch® Rev B and Rev C.

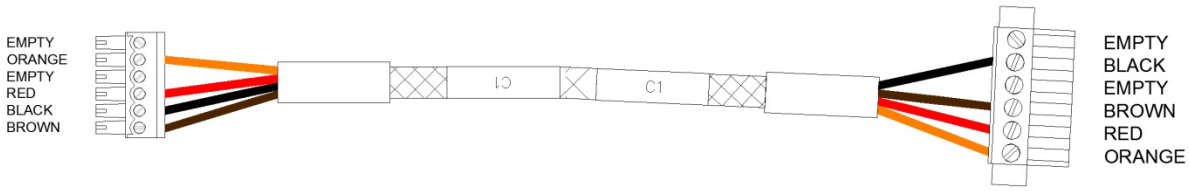


Figure 15 – Market Central SecureSwitch® Rev B/C Control (3 Networks)

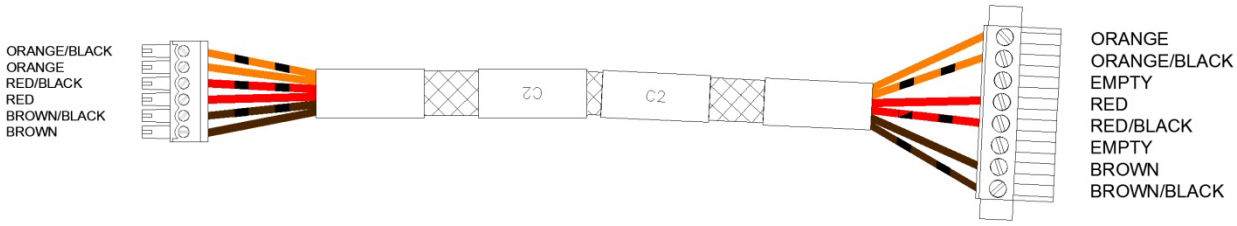


Figure 16 – Market Central SecureSwitch® Rev B/C Status (3 Networks)

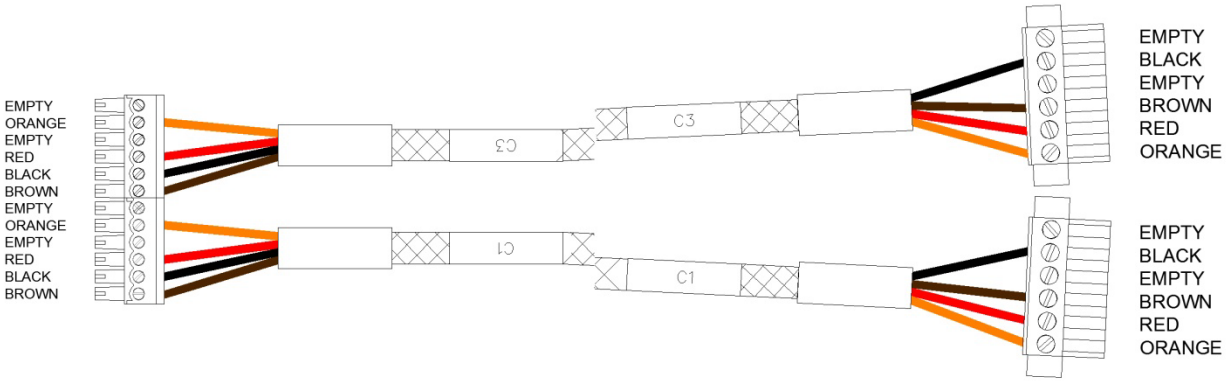


Figure 17 – Market Central SecureSwitch® Rev B/C Control (3+ Networks)

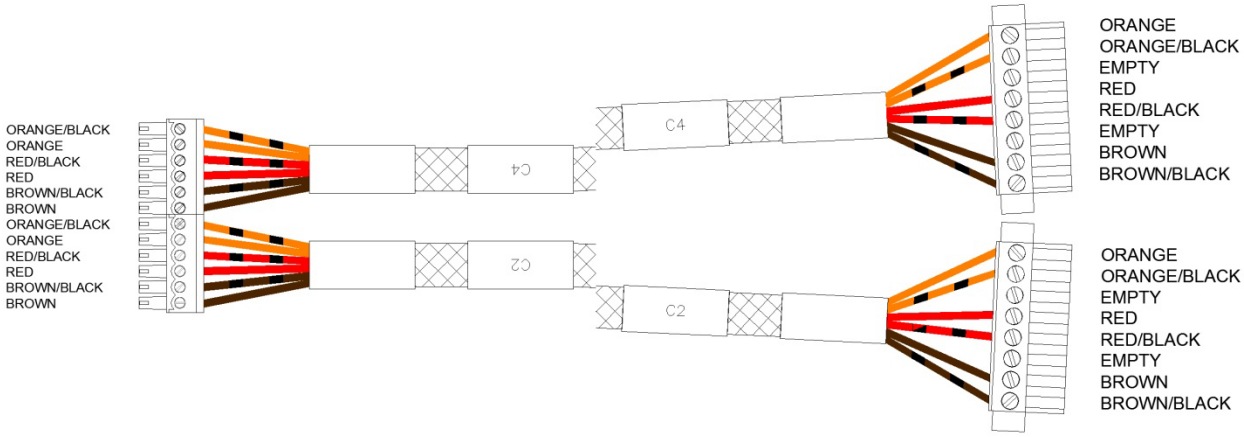


Figure 18 – Market Central SecureSwitch® Rev B/C Status (3+ Networks)

Appendix E
CODEC Control Cable Schematics

Cisco Control

The Freeport MDVNS utilizes a control cable connected between the SCC5Net Switch and the control port (RS-232) of the video CODEC for all communication. The control cables listed below can be used for all supported Tandberg/Cisco video CODECs.

Freeport recommends off the shelf Female DB9 to Male DB9 cables no longer than six (6) feet in length for all Cisco CODECs.

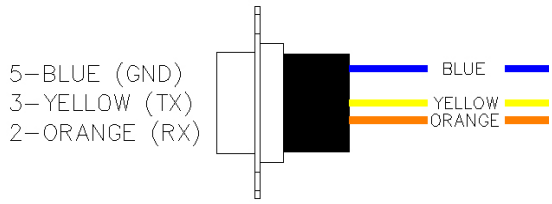


Figure 19 – Female DB9 (SCC5Net Switch CODEC Port)

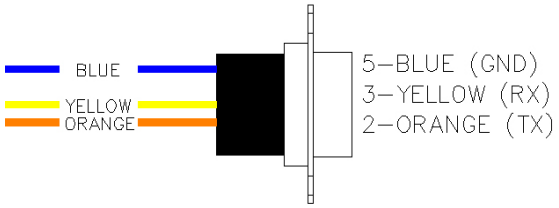


Figure 20 – Male DB9 (CODEC Data/COM Port)

Figure 21 – Female Null Modem DB9 to USB (CODEC USB Port)

If a third-party control system is being utilized to control the CODEC via the Controller port on the rear of the SCC5Net Switch, the default baud rate of the CODEC must be used. Please refer to the manufacturer provided documentation regarding the default baud rate of your specific CODEC make/model.

Appendix F
SCC5Net Switch Relay Control

The Freeport SCC5Net Switch provides six relays (dry contact closures) which can be used for external device management (relays 21-26). Each relay can switch up to 24 VDC or 28 VAC @ 1 A. Refer to *Section 5 – System Configuration* for the steps required to enable/disable the relays for each desired network/mode.

Connection Details

External devices utilizing two conductors can be plugged directly into the provided 12 Pin Male 3.81mm Phoenix connector on the back of the SCC5Net Switch.

It is recommended that any device that requires power supply management should utilize 3 Pin Female 3.81mm Phoenix to 3 Pin Male 3.81mm Phoenix connectors. The following diagram represents how a power supply for a source isolation device associated with Relay 21 would be integrated:

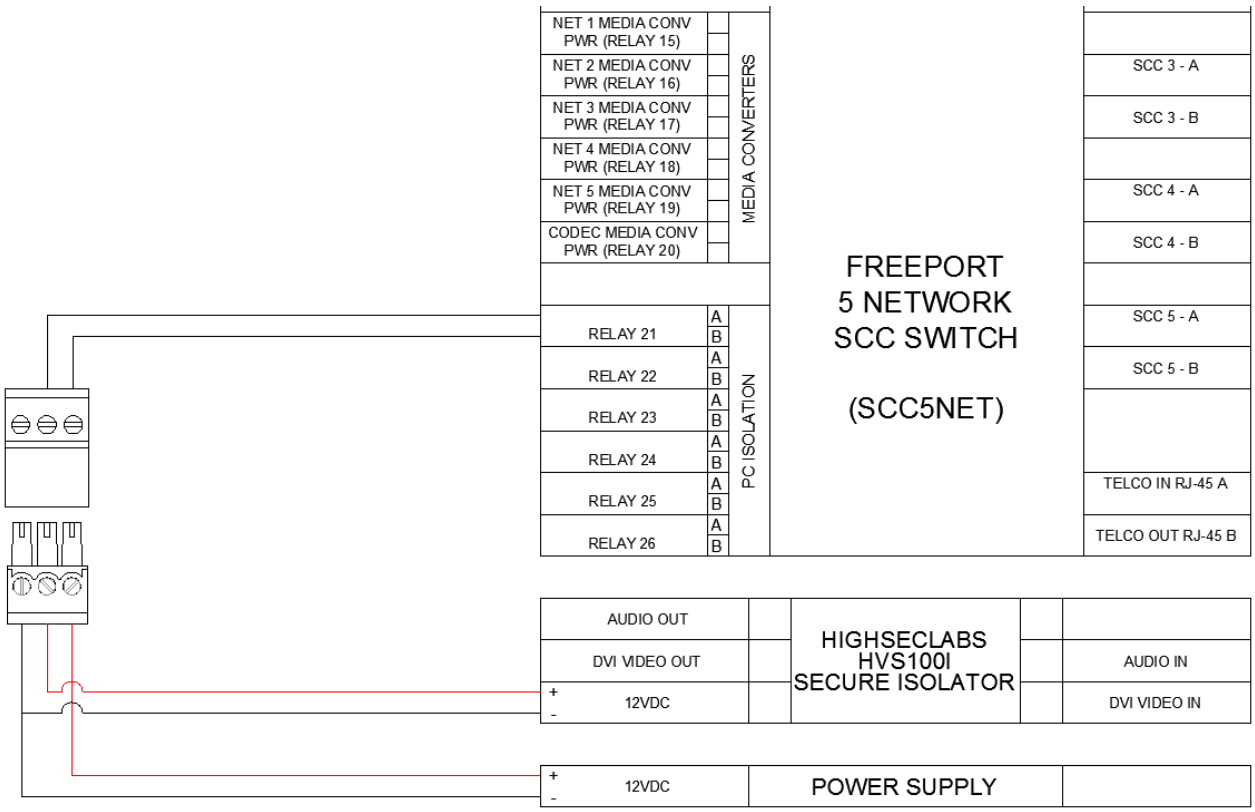


Figure 22 – External Device Power Management

Appendix G
Cisco ISDN Link Integration

The Freeport MDVNS can support a Cisco ISDN Link gateway for external network connectivity and will automate the pairing and un-pairing of the device as part of the periods processing procedures when joining and leaving a network. Please read through the following procedures before attempting to configure the ISDN Link via the CODEC web interface; failing to do so may require the ISDN Link to be factory defaulted to an out of box state.

System Configuration Settings

The system must be properly configured to support the ISDN Link for the desired network(s). To review/edit the current configuration settings of the system, execute the following steps:

1. Access the web interface of the system via the steps provided in *Section 5 – System Configuration* of this document.
2. Navigate to the *Networks and Modes* page and select the *Enable Cisco ISDN Link* box for the network(s) that will be utilizing ISDN.
3. Use the "Save Configuration" button on the bottom of the page to save the modification.

SCC Configuration Settings

The SCC unit that will be responsible for restoring the CODEC with the ISDN Link settings must also be properly configured. To review/edit the current configuration settings of the SCC being utilized for ISDN, execute the following steps:

1. Access the web server of the desired SCC unit via the steps provided in *Section 6 – SCC Options & Maintenance* of this document.
2. Navigate to the *CODEC Settings* page and use the *ISDN Link Enabled* drop-down box to select "True" as the applied setting.
3. Type in the *ISDN Link MAC Address* in the box provided (e.g. 00:11:31:50:5A:47).
4. Use the "Save" button to save the modifications.

ISDN Link Configuration

The Cisco ISDN Link must be configured via the web interface of the CODEC per the manufacturer provided instructions. Execute the following steps to ensure successful configuration and pairing of the ISDN Link when integrating with the MDVNS:

1. Use the front panel of the SCC5Net Switch (or third-party control system) to select the network/mode that will be utilizing ISDN and wait until the transition is complete.
2. Navigate to the CODEC web interface and configure the Cisco ISDN Link per the manufacturer provided instructions. This must include successful pairing of the device.
3. Once the ISDN Link has been paired and configured, use the CODEC web interface to "Un-pair" the ISDN Link from the CODEC. Confirm the device has been successfully un-paired.
4. Set the *Mode Selection Key* on the front of the corresponding SCC unit to *Capture* and select Off mode via the SCC5Net Switch front panel (or third-party control system).
5. Select the network/mode that will be utilizing ISDN and once complete, confirm that the ISDN Link has been re-configured and has successfully paired with CODEC.

Appendix H
Web Controlled CODEC Power Switch

The Freeport MDVNS system supports a web controlled switched AC outlet for installations in which the video CODEC is located greater than six (6) feet from the SCC5net Switch.

CODEC Power Switch Configuration Settings

1. Access the web interface of the system via the steps provided in *Section 5 – System Configuration* of this document.
2. Navigate to the *Miscellaneous* page and use the *CODEC Power Switch* drop down box to select "iBoot" as the applied setting.
3. Enter the IP address that will be assigned to the iBoot G2+ for control. Please note that the default IP address needs to be reachable by the SCC5Net Switch.
4. Use the "Save Configuration" button to save all modifications.

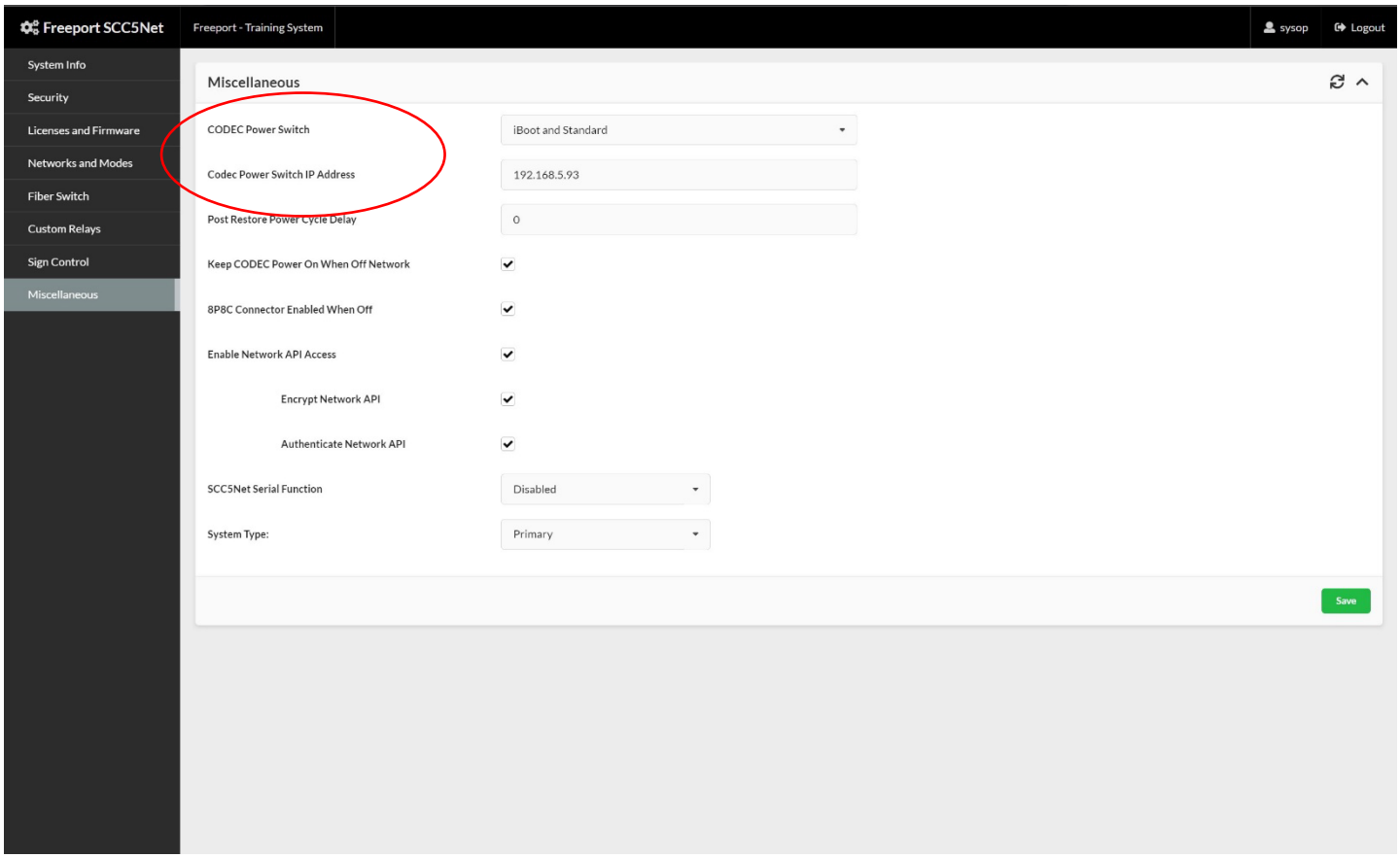


Figure 23 – MDVNS Web Configuration Tool (Power Control Page)

Dataprobe iBoot G2+ Settings

Refer to the Quick Start Guide that is provided by the manufacturer regarding directing a standard web browser to the default IP address (192.168.1.254) of the iBoot G2+.

1. Change the general network settings of the iBoot G2+ to match the network settings of the MDVNS system components and assign it the same IP Address entered and saved in the *CODEC Power Switch IP Address* field of the MDVNS configuration (e.g. Device IP Address = 192.168.5.93, Device Subnet Mask = 255.255.255.0, Gateway = 192.168.5.1).
2. Use the "Save" button on the bottom of the tab to save all modifications.

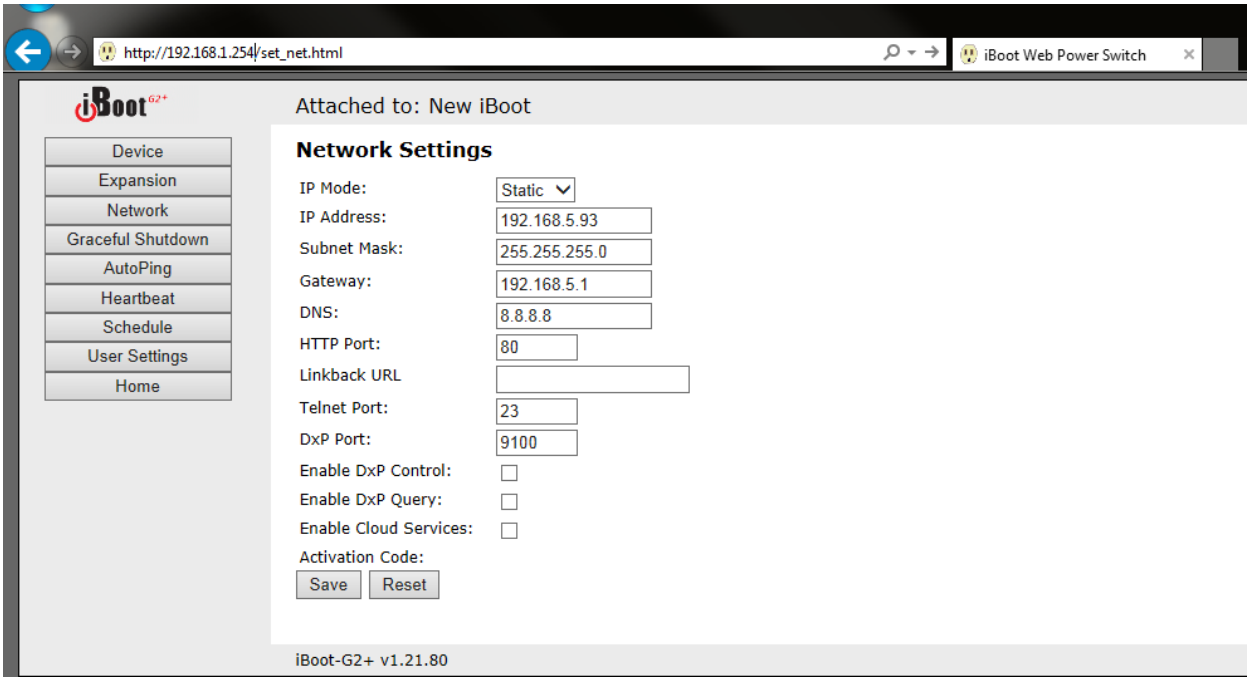


Figure 24 – iBoot G2+ Web Configuration Tool (Network Tab)

3. Select the *User Settings* tab and use the *User Rights Management* drop down box to select "Auto Login".
4. Use the "Save" button on the bottom of the tab to save all modifications.

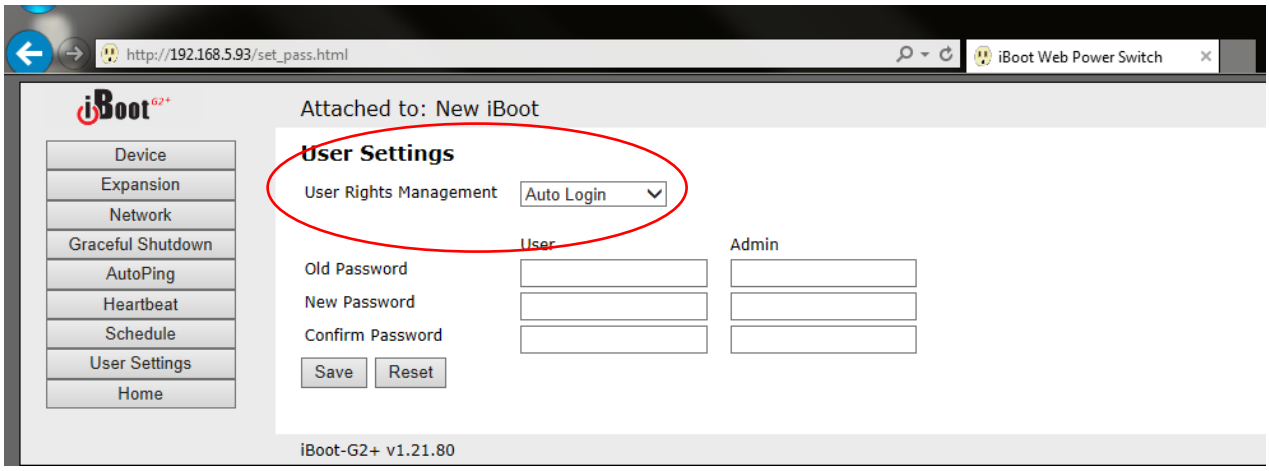


Figure 25 – iBoot G2+ Web Configuration Tool (User Settings Tab)

5. Ensure that the network settings of your computer are reverted back to ones that are compatible with the MDVNS system components.
   (e.g. Device IP Address = 192.168.5.50, Device Subnet Mask = 255.255.255.0)
6. Re-connect to the iBoot G2+ web interface using the new IP address (e.g. 192.168.5.93) previously assigned in Step #1 above.
7. Click on the check box to select the Main power supply and select *Power ON/OFF* to verify that the iBoot G2+ can be controlled via Ethernet without having to enter a password.

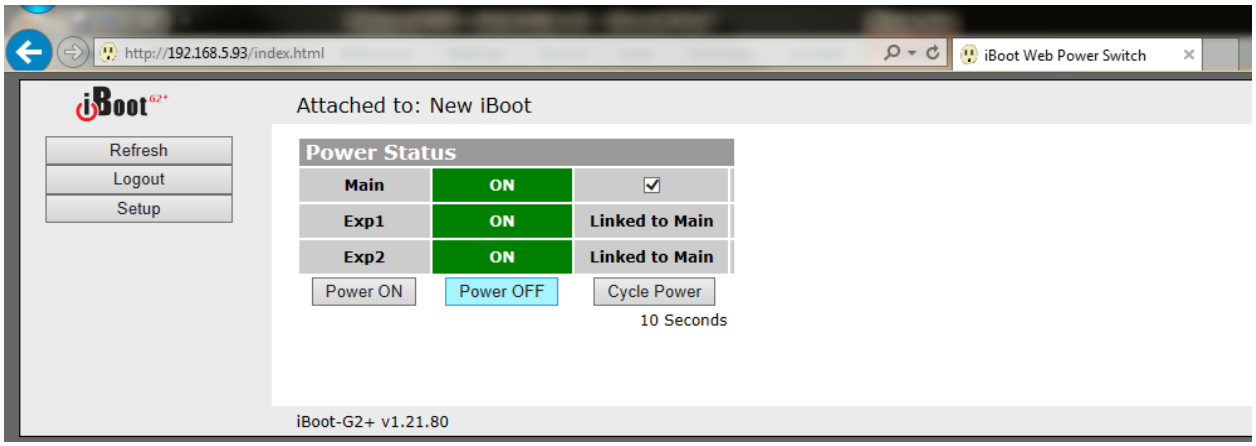


Figure 26 – iBoot G2+ Web Configuration Tool (Home Tab)

Appendix I
CODEC Extender Kit Integration

The Freeport MDVNS system can be implemented into an environment in which the CODEC and/or video system (Cisco MX Series, Cisco Webex Room Series) is not located near the MDVNS components. Please follow the guidelines below if the MDVNS system is located more than six (6) feet from the required CODEC connections.

Required Hardware & Cabling
PC/Laptop, iBoot G2+ Power Switch, Geffen RS232 Extenders
Two (2) Ethernet Cables
Two (2) Female DB9 to Male DB9 Cables (MX700/800 Series & SX80)
Female DB9 to Male DB9 Cable & Female DB9 to USB (MX200/300, SX20, & Webex Room/Kits)
IEC Power Cable

A. *Cabling*

1. Qty 2 Ethernet cables must be run from the location of the SCC5Net Switch to where the CODEC is located
2. Apply a set of labels to each cable (C54 & C49)

B. *CODEC Power (iBoot G2+)*

1. Connect **C54** to the Ethernet port of the SCC5Net Switch (or local managed switch)
2. Connect the other end of **C54** to the iBoot G2+ (which will be located near the CODEC)
3. Pull the power from the CODEC and use that cable to power the iBoot G2+
4. Utilize the existing CODEC switched AC power cable to connect between the iBoot G2+ and the CODEC (switched AC outlet)
5. Secure the iBoot G2+ near the CODEC with the provided Velcro

C. *CODEC RS232 Extender S (MDVNS Location)*

1. Connect **C49** to the Geffen RS232 Extender S unit
2. Connect **C50** (DB9 M) to the Geffen RS232 Extender S unit and the other end of **C50** (DB9 F) to the CODEC port on the SCC5Net Switch
3. Apply power to the Geffen RS232 Extender S unit & affix the unit within the MDVNS rack in a manner that ensures the security of the power cable

D. *CODEC RS232 Extender R (Cisco Location)*

1. Connect **C49** to the Geffen RS232 Extender R unit
2. Connect **C48** (DB9 F) to the Geffen RS232 Extender R unit and the other end of **C48** (DB9 M) to the CODEC COM port
3. Secure the Geffen RS232 Extender R unit near the CODEC with the provided Velcro

Please ensure that the SCC5Net Switch and the web controlled CODEC power switch have been properly configured per the steps listed in *Appendix H – Web Controlled Power Switch* of this document.

Appendix J
Out of Box System Configuration

Freeport MDVNS system components that have been pulled from inventory and have not been integrated and tested as a system will need to be put through a set of procedures before being deployed. If you have a purchase one of these systems (due to lead time issues) or have received replacement hardware please review the following procedures.

Required Tools: PC/Laptop, Ethernet Cable, SCC5Net Switch & SCC Firmware (via Freeport FTP site)

A. *SCC5Net Switch*

1. Power up the SCC5Net Switch without any other components connected to it
2. The system will attempt to initialize and fail after a few minutes
3. Refer to *Section 5 – System Configuration* for the steps required to connect to the SCC5Net Switch web interface
4. Verify that the SCC5Net Switch has the latest firmware and update if necessary
5. Configure the SCC5Net Switch according to the system requirements

B. *SCC Units*

1. Connect the SCC units to the SCC5Net Switch according to the provided system schematics
2. Refer to *Section 6 – SCC Options & Maintenance* for the steps required to connect to the web interface of each SCC unit
3. Verify that the SCC unit you are working with has the latest firmware and update if necessary
4. Update any required license keys
5. Update the system information
   (Network/Mode Settings, System Time, Network/Mode Name, Network/Mode Color, Sign-In Banner, etc.)
6. Repeat these steps for each SCC Unit connected to the system

Once the SCC5Net Switch and the SCC units have been configured, the rest of the system components can be connected per the provided system schematics and the system is ready to be deployed, refer to *Section 4 – Initial System Deployment* of this document.

Appendix K
Certificate Management with CUCM

The Freeport MDVNS system is capable of loading certificates into the CODEC during a network transition, however, the Cisco serial API does not allow certificates to be automatically captured by an SCC Unit. Certificates must be manually uploaded to each SCC Unit (via the Web UI) for networks that require this feature.

Cisco CODECs that are being managed by Cisco Unified Communications Manager (CUCM) typically have their certificates automatically generated and loaded by CUCM. This process will need to be done manually for systems that are utilizing the MDVNS.

Requirements

1. CUCM 12.5.x or higher and configuration right to the CUCM to allow CA signed certificate for endpoints (CODEC Certificate stored in the SCC Unit)
2. A CA to sign CSRs for the endpoint (CODEC Certificate stored in the SCC Unit)

Procedures

Use a tool to generate the CODEC CSR and private key for uploading into the SCC Unit

- cygwin terminal is an example -
    - (first) Generate private key
        - Command line: openssl genrsa -out codec-private.key 2048
    - (second) Generate CSR
        - Command line: openssl req -new -sha256 -key codec-private.key -out codecname.csr
- Download the codecname.csr and provide it to your CA for digital signature
- Upload Certificates into the SCC Unit via the Web UI
    - Upload the CA certificate (filenames vary) into the SCC Unit
    - Upload the CA (signed codecname.crs which is renamed to codecname.pem (filename may vary)) into the SCC Unit
    - Upload the previously generated codec-private.key, from your first step, into the SCC Unit
- In the SCC configuration, for certificates previously loaded:
    - Enable HTTPS server
    - Enable SIP
- An alternative web UI tool you may like to use:
    - https://certificatetools.com/