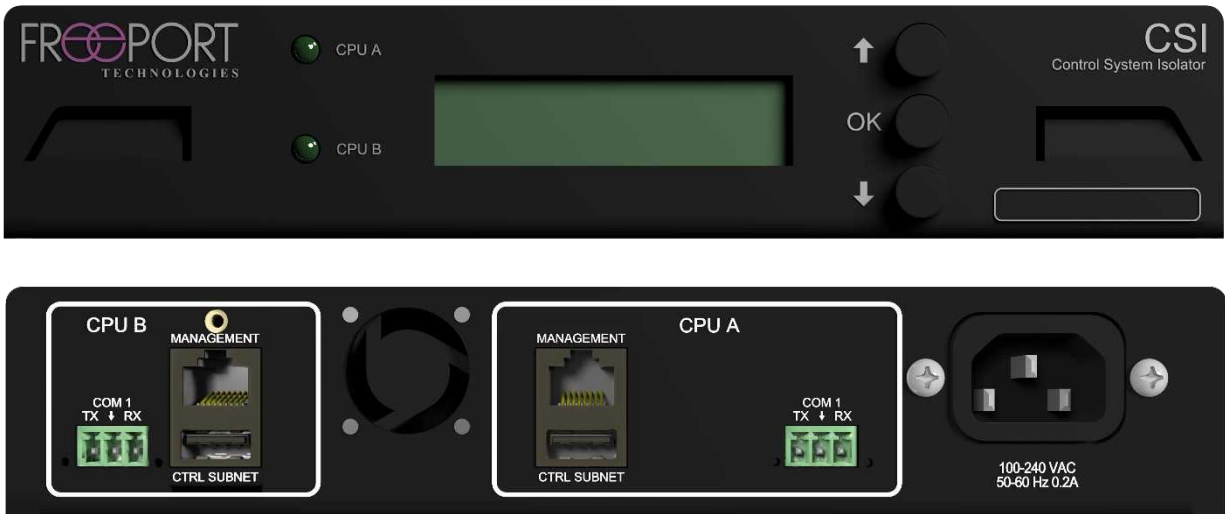


CONTROL SYSTEM ISOLATOR

Release Notes CSI-1.5.0



Point of Contact:

Freeport Technologies Help Desk
571-262-0422
866-226-4125

TechSupport@freeporttech.com

1	Configuration Items	1
2	Release Notes	2

1 Configuration Items

Item #	Configuration Item	Required Change
CSI-1.0.0		
138	MDVNS SCC5Net Switch Firmware	If the CSI is licensed for In-Room Control in a multi-classification environment, the MDVNS SCC5Net Switch must be running firmware version MDVNS-Sequencer-4.2.8.852 or higher.
139	MDVNS SCC5Net Switch - Network API Access	If the CSI is licensed for In-Room Control in a multi-classification environment, the MDVNS SCC5Net Switch must be configured with the following settings: Enable Network API Access - Enabled Encrypt Network API - Enabled Authenticate Network API - Enabled

2 Release Notes

Release Type	Release Note
CSI-1.5.0	
Improved	Support for Cisco RoomOS 11.27 security related changes. Any previous CSI configuration settings relating to the use of this Cisco firmware have been removed.
CSI-1.4.3	
Added	The ability to import a Cisco In-Room Control configuration from an SCC5Net Switch to a newly deployed CSI unit. Note: Existing MDVNS systems which are utilizing the SCC5Net Switch for Cisco In-Room control will require an upgrade from a RCI unit (EOL) to a CSI unit. From the SCC5Net Switch: 1. System Info - Configuration - Export 2. Miscellaneous - "SCC5Net Serial Function" = Disabled, Control, or Signage. De-select In-Room Control. 3. Enable API access. Miscellaneous - check "Enable Network API Access" or set "SCC5Net Serial Function" to Control 4. Recommend encryption and authentication for the API. If authentication is enabled, an API user must be created (Security - SCC5Net User Management). From the CSI unit: 1. On the Configurations page, check "In-Room Control" and select Factory Reset. It will not be possible to import from an SCC5Net if In-Room Control is already configured. Skip this step if no previous In-Room Control configuration has been entered. 2. Navigate to In Room Control - Configuration Options - Import SCC5Net In-Room Control Configuration. Click Import... 3. Browse to the SCC5Net export file. Enter the encryption password if prompted. 4. Click Save. Reboot can be postponed if further configuration is needed.

Release Type	Release Note
	- Under In-Room Control - Device Management - SCC5Net, verify the IP/hostname and other communication settings. - Under In-Room Control - Configuration Options - Options, check "CODEC is running RoomOS v11.27 or later" if necessary. - There are several new features available in CSI In-Room Control, including toggle buttons, multiple panels, and network default layouts. - Reboot the CSI to apply changes.
Resolved	An issue where the NTP log file is not being removed during Factory Reset.
CSI-1.4.2	
Improved	NTP functionality to include multiple clients, symmetric encryption, and NTP status display. Please note that downgrading from this version or later to an earlier version will result in not being able to change the NTP settings.
Resolved	An issue where In-Room Control sometimes failed to set custom responses when restarting to apply changes.
Resolved	An issue where the hardware clock was not recognized by the firmware and the system date and time could not be managed properly.
Resolved	An issue where API command processing can become delayed when successive commands are sent without waiting for the CSI response (OK/FAIL).
CSI-1.4.1	
Added	An In-Room Control option as to whether the CODEC is running Room OS firmware 11.27 or later. Enabling this option means the link command will be sent to the SCC5Net (if the firmware supports it) when the system is off network and the CODEC login prompt is received (e.g. CODEC reboot). Without this option the system will behave as before, attempting to log in with username=admin and a blank password.
Updated	The default value regarding the firmware version of the Cisco CODEC for systems using the In-Room Control License key. The new default value will be Room OS.

Release Type	Release Note
Resolved	An issue where database log files weren't removed during factory reset.
Added	The ability to control external devices over IPv6 when using the In-Room Control license key.
	If a literal IPv4 address is entered for the IP Address/Hostname, IPv4 will be used. If a literal IPv6 address is entered, IPv6 will be used. If a hostname is entered, IPv4 will be used unless the IPv6 checkbox is checked.
Improved	Freeport Mercury integration.
	Enabled scrolling classification text for In-Room Control Mercury configuration. If the current Mercury firmware does not support scrolling message text, the classification text animation will be set to static.
Resolved	An issue when using the In-Room Control license key where the CODEC username and password fields are shown when multi-classification is enabled.
	This field should be hidden when the CSI is integrated with an MDVNS.
Resolved	An issue when using the In-Room Control license key where a user without administrative privileges could view device passwords.
CSI-1.4.0	
Improved	Serial port performance when utilizing the CSI with an MDVNS system; thereby reducing delays in handling commands after a network switch.
Added	Support for Cisco RoomOS v11.27. This firmware version will always require an Admin password for login to the serial port after a factory default.
	Default Admin credentials will be set for new systems, both single (CSI) and multi-class (MDVNS): Username: Admin Password: freeporttech
Resolved	An issue where a non-admin user could modify (but not save) In-Room Control button availability: • Classification • Swap Layout • TV

Release Type	Release Note
	• Media Player • Display • Microphones
Improved	New systems will use the serial number as the hostname for the A-side. Upgrades will continue to use the hostname "CSI".
Added	Diagnostics when the web server certificate is expired or about to expire. (System Settings -> Security)
Added	The ability to enable IPv6 on the network interface. For new installations, IPv6 is disabled by default. For upgrades, IPv6 will (still) be enabled.
	Either one static IP address or automatic configuration is supported. Automatic configuration supports DHCPv6 and stateless auto-configuration (SLAAC).
Added	The ability to specify IPv6 addresses for System Settings -> Network -> DNS.
Added	The ability to specify a literal IPv6 address for the Notifications server on the Issues & Diagnostics page.
	If an IPv6 address is specified or a hostname is specified which will resolve to an IPv6 address, the "IPv6" checkbox must be checked.
Added	Visual indicators to the Web UI for certificate expiration (web server certificate, certificate authorities). Text will be yellow if the certificate is about to expire and red if the certificate is expired.
Added	The ability to configure a hostname which will be sent to a DHCP server.
	Hostname may also be displayed in outgoing syslog and SNMP messages. Hostname will be included in network export/import. Factory reset will set the hostname back to the original value ("CSI" for systems flashed with firmware earlier than v1.4 or the serial number for v1.4 and later).
Added	The ability to add/edit the Cisco CODEC Admin account details when using the CSI for In-Room Control with single classification systems (No MDNVS).
Improved	Feedback. Added a wait box when network settings are applied.

CSI-1.3.1

Release Type	Release Note
Resolved	An issue where In-Room Control takes a long time to put the buttons on the Cisco touch panel when using RoomOS 11.14 or later.
	Please note that this was a result of a Cisco firmware bug which should be patched in the near future.
Resolved	An issue on the Edit User page where the Delete button was enabled when viewing the currently logged in user.
Resolved	An issue where web client Session Expiration is not applied immediately when importing a security configuration.
Resolved	An issue where Mercury classification text is cleared by In-Room Control if the network connection is lost and regained.
Resolved	An issue where the first CSI API command to the isolated device fails after the B-side boots.
Added	The ability to accept non-printable characters in success, fail, and custom response strings to the User interface (in a similar format to In-Room Control device commands).
Resolved	An issue with API commands. API commands S, F, Rxxxx, and C will now accept data that is not utf-8 encodable.
	As documented, any binary data other than SOH (0x01), STX (0x02), ETX (0x03), and EOT (0x04) should be allowed in CSI API command data fields.
Added	The ability to enter multiple commands for a custom button, with a customizable delay between commands.
Improved	- CSI API custom response (Rxx) command will return FAIL if the custom response is a duplicate of another. - CSI API custom response (Rxx) command will accept zero length string. This will remove any existing custom response for that index. - User interface (Features) will validate that custom responses satisfy the minimum length requirement. - User interface (Features) will validate that no custom responses are duplicates.
Improved	The ability to communicate with external devices by adding more space when entering device commands via the In-Room Control user interface.
CSI-1.3.0	
Validated	Compatibility with Cisco firmware up to Room OS 11.9.

Release Type	Release Note
Added	TCP encryption options to syslog. A diagnostic will be shown if TCP is enabled with a TCP IP address and port but the connection can't be made.
Resolved	An issue where the user could be prompted to save changes before navigating away from a specific page when no changes were made.
Added	The ability to apply In-Room Control configuration changes while on an active network/mode. This feature is intended for initial deployment and/or major configuration changes, the user must acknowledge the risks associated with doing so.
Added	The ability to view the CSI serial number via the System Settings -> Licenses page. The serial number will also be logged at boot. Please note that the serial number will only be displayed for hardware shipped with this software version.
Added	The option to move In-Room Control buttons to the Cisco touch panel's "Control Page" area instead of on the main page. This requires RoomOS 11.14 or later. Buttons that can be moved to Control Panel page: • Classification • Action Buttons • Custom Panels • Sanitize • Swap Layout • TV Tuner • Media Player • Displays • Microphones
Resolved	An issue where if a reboot fails (e.g. firmware upgrade or user command), the Web UI would just go back to the previous screen. After a couple minutes of waiting, a message will inform the user that the reboot has failed.
Added	An option to enable FIPS mode. Note that if the customer has supplied a custom web server certificate and the private key is encrypted with a Non-FIPS

Release Type	Release Note
Added	compliant algorithm, a new self-signed web server certificate will be generated and used. Support for LDAP login to CSI serial API. Formats for username in the login command are: ldap:username - simple authentication when a domain is defined in LDAP settings ldap:username@domain - simple authentication when no domain name is defined in LDAP settings ldap:domain\username - NTLM authentication when no domain name is defined in LDAP settings. The command format is <SOH>L<STX>username,password<ETX><EOT>
Improved	Mercury integration. When controlling a Mercury unit, the AV icon indexes for the various states are now configurable. This provided the ability to create and locate Mercury AV Icons wherever you want on the canvas.
Added	The ability to create a Sanitize button when utilizing an MDVNS system with active VTC networks. The Sanitize button will mute the audio and video outputs of the CODEC and update the button text and color to indicate that the room has been sanitized. Pressing the button again will unmute audio and video and restore the original button text and color.
Added	The button text label is customizable. The commands sent to the CODEC when the button is pressed are also customizable. The ability to set a default source input of a display being controlled by the CSI.
Added	The Input command will be sent whenever the Power On command is sent. Added a delay setting to give the display time to power on before setting the input. A device maintenance button for external devices being controlled by the CSI. The button will be enabled once an IP

Release Type	Release Note
	Address and IP Port have been filled in and saved when creating the device. The device maintenance page shows the In-Room Control log filtered for that device. The page allows sending of commands and queries to the device via the CSI. Device connections may be permanent or as needed. If the device requires authentication, has toggle button queries, or has any fields in the "Communication Parameters" card filled in, the connection will be permanent. In this case it is recommended to fill in the "Line Break" field. Without a line break configured, responses from the device will not be shown unless they match an expected response. If none of the above conditions are met, a connection will be made only when there is data to send. The connection will be dropped after a minute of inactivity. In-Room Control device configuration changes must be applied in order to take effect.
Improved	Configuration changes to In-Room Control. Added an "Apply" button to the top of all In-Room Control configuration pages. The button will enable if changes have been saved to any part of the In-Room Control configuration since the web page was loaded.
	It is still possible to restart In-Room Control from the "Configuration Options" page if no changes have been made since refresh. If In-Room Control was enabled or disabled since the last time the configuration was applied, prompt for a reboot.
Improved	System logs: • Add filter, by source, filter by severity, refresh, and auto-refresh (10 seconds) options when viewing the log and audit log.
Improved	The configuration export feature: • The data in export files is now encrypted, it is no longer possible to edit exported files.

Release Type	Release Note
	- The user will be prompted to provide a password to encrypt the exported data. This same password will be required to import the data. Imports will support both encrypted and unencrypted data. If the file was encrypted during export, the user will be prompted for the password before importing. The user will have the option to preview data before import. The preview is in raw JSON format with password fields obscured. Added The ability to send SNMP traps or inform messages. Traps will currently be sent for two events: - Audit failure, e.g. disk is full and can't write to the audit log. - If heartbeat traps are enabled, send periodic traps. This is useful for configuring SNMP manager systems to communicate with Mercury. Currently traps can only be sent to one SNMP manager. A reboot is required to apply SNMP configuration. Several trap configuration options are available: - Support SNMPv2c or SNMPv3 traps and informs. - For inform messages, retries and timeouts can be configured. CSI will resend the inform message until a response is received or retries are exhausted. - A heartbeat interval can be configured resulting in periodic messages. - For SNMPv2c, a community string can be configured. - For SNMPv3, several authentication and encryption schemes are supported. If authentication type is not None, an authentication key (password) is required. If encryption type is not None, a private key is required. The SNMP engine ID is displayed on the user interface. SNMP settings are exported, imported and factory reset along with security settings.
Added	A logout dialog to the Web UI showing the username when the user logs out or is logged out due to inactivity.
Added	A setting to override the context used when searching for Active Directory user groups. CSI will try to determine the context from the server response. The LDAP context can be

Release Type	Release Note
	overridden if the context cannot be determined automatically.
Added	The format is CN=MYLDAP,DC=COMPANY,DC=COM.
Added	The ability to assign API and Admin roles via Active Directory user groups.
Added	The ability to specify a domain name for Active Directory integration. If a domain name is configured, users should enter only their username at the login prompt and the configured domain name will be added. This will use simple authentication.
Added	A diagnostics table to the logs page. Renamed the page to "Issues & Diagnostics". Added a link to the diagnostics page to the top of every page when there are active issues.
	Currently potential diagnostics are: • Default credentials in use • User locked out • Syslog connection failure
Improved	The CSI Web UI experience.
Added	An In-Room Control option to enter the MAC address of a Cisco Room Navigator touch panel.
	If this is configured, after a factory reset, a command will be sent to configure the Room Navigator as a controller inside the room. If the Room Navigator isn't registered yet, In-Room Control will wait up to 10 seconds to attempt to configure it. The command will be resent periodically in case the touch panel still wasn't registered.
Resolved	An issue where the word "Welcome" in a Mercury message field would cause the sign message text to be set blank (along with all other sign fields).
CSI-1.2.1	
Resolved	An issue that was extending the boot time of the CSI.
	This caused the firmware page to not reload after an upgrade from version 1.2.0.306. In addition, any other web-initiated reboot would fail to reload the page afterward. The wait dialog would clear before the web server was ready.

Release Type	Release Note
Resolved	An issue in which the system status messages being shown on Mercury displays did not always reflect the state of the SCC5Net Switch. *Requires SCC5Net firmware 4.5.1 or later. • Use the new MDVNS API query "getOperation" to determine which sign message to show in the event the CSI connects to the SCC5Net while the system is already switching. • Use the new MDVNS API event "event,reboot" to disable the B-Side and show the "System Init" message until the SCC5Net is ready.
Added	The "NTP" option to configuration options (factory reset, export, import).
CSI-1.2.0	
Added	The ability for the CSI to control the SCC5Net Switch via the A-Side serial port. Includes encryption and authentication options. The authentication and encryption options require SCC5Net version 4.5 or later.
Added	The ability to configure the Web UI session timeout, between 10 and 999999999 minutes. Existing web sessions will be updated with the new expiration interval.
Resolved	An issue in which commands from the CSI to a Mercury unit intermittently failed and were not retried. Improved the overall ability of In-Room Control to recover the connection with a Mercury unit.
Resolved	An issue in which the "All Mics" mute button on the Cisco touch panel was being mislabeled.
Resolved	An issue where random UDP listener ports were opened (e.g. 19141).
CSI-1.1.2	
Improved	Security by closing port 5355: LLMNR (Link-Local Multicast Name Resolution).
Updated	Nginx webserver to version 1.17.8
CSI-1.1.1	

Release Type	Release Note
Resolved	An issue where Mercury messages can't be configured for networks that were added after the Mercury device was created.
Resolved	An issue where the reboot after a factory reset fails if the IP address of the unit was changed. A factory reset now always requires a reboot, whether it is initiated via the Web UI or front panel.
Improved	Feedback after a factory reset. The audit log and the LCD will now indicate a success/failure for a front panel factory reset.

CSI-1.1.0

Improved	In-Room control flexibility in regards to the number of items that can be utilized: • Removed the limit on the number of sources that can be assigned to a specific network when utilizing a video switch • Removed the limit on the number of display power buttons that can be shown on the Cisco touch panel • Removed the limit on the number of Image Processor layout buttons that can be displayed on the Cisco touch panel • Removed the limit on how many networks can be configured (MDVNS required) • Increased the maximum number of microphone groups to 8
Added	The ability to require authentication for any device that is being controlled by the CSI. This will add the following configuration fields: • Login Prompt • Password Prompt • Login Succeeded • Login Failed (optional) • Pre-authorization Command • Terminator • Keep-Alive Command • Keep-Alive Interval
Added	The option to use toggle buttons on custom panels being display on the Cisco touch panel.

Release Type	Release Note
	Notes: • Toggle buttons have an additional command sent when the button is toggled off • Toggle buttons have an optional query command and associated responses. The optional query is sent at startup and after a network switch (MDVNS required) to determine the initial state of the button • Toggle buttons have optional unsolicited text from the device (events) to trigger the state of the button • If the query, responses, and events are not supplied, the initial state of a toggle button will be off • Typically a query or events will be used, not both • The same event text can't be used for more than one button associated with the same device • Queries are not supported for the SCC5Net Switch device type • Events are not supported for the following device types: SCC5Net Switch, Mercury, CODEC
Added	The option to use toggle buttons on the Cisco touch panel when controlling display power. Notes: • When this is enabled, there is also an option to add a power query command and responses • The query will be sent at startup and after a network switch (MDVNS Required) to query the power state and update the button states • If the query command is not supplied, the initial state of the buttons will be off
Resolved	An issue that was causing all PDU outlets to be turned off if the CSI is rebooted or power-cycled while on network (MDVNS Required). At In-RoomControl startup, all PDU outlets will be enabled/disabled according to the current configuration.
Improved	Cisco touch panel customization. • Allow the creation of multiple custom panels and action buttons • A maximum of 100 action buttons can be created

Release Type	Release Note
	• A maximum of 20 buttons can be placed on a panel • Action buttons will appear on the Cisco touch panel first, then panel buttons • When creating a custom panel each button can be displayed or hidden based on the active network (MDVNS Required) * If all buttons are hidden, the panel button will not be shown
Added	The ability to assign a default image processor layout to each network/mode and system off mode (MDVNS Required). If no default is assigned for a network or mode, the default button will be used.
Added	The option to set the CODEC time in Off mode (MDVNS Required) based on the CSI clock. The time will be set after a SCC Unit factory resets the CODEC.
	Notes: • This will occur after MDVNS system initialization, system error, and switch to off mode • The time zone can be set using a post-clean command
Improved	The time required to transfer the user interface to the Cisco touch panel.
CSI-1.0.0	
Initial Build	- Initial Release - • CSI Web UI configuration tool • System settings include network, security, firmware, licenses, date/time/ntp • Features include default settings (isolated device baud rate, command timeout delay, success string, failure string) and custom response management • Configuration file import/export • Logging (including Syslog support) • License key option for Cisco In-Room Control (single or *multi-classification)
	*Requires Freeport MDVNS