MDVNS
SECURE CODEC CONFIGURATOR

Release Notes
MDVNS-SCC-4.6.0

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	Justification	Required Change
MDVNS-SCC-4.6.0		
xCommand SystemUnit SignInBanner Get	xCommand SystemUnit SignInBanner Get does not provide <CR><LF> for Sign -n Banner set from the CODEC Web UI.	If the Cisco Web UI Sign-in Banner contains <CR><LF>, it will not be captured by the SCC Unit during a network transition. The Sign-In Banner must be entered via the SCC Web UI: CODEC Settings > Sign-in Banner (text box)
MDVNS-SCC-4.5.0		
Incremental Upgrade	Failure to execute the incremental upgrade results in unrecoverable hardware.	SCC units with firmware version 4.0.x (or below) require an incremental upgrade to version 4.4.0.3118 before an upgrade to 4.5.x
MDVNS-SCC-4.0.8		
Strong Security Mode - True	If admin Username remains "admin" MDVNS will be locked out the CODEC serial port. This will result in a Switching Error loop, the only recovery method is a manual factory reset of CODEC.	If using Strong Security Mode the admin Username must be changed from default value "admin".
Desk Pro CODEC CE9.13.x downgrade to CE9.12.x	Desk Pro CODEC not supported in firmware version MDVNS-SCC-4.0.8.1136	Remove following xConfiguration items from captured Configuration before downgrading to CE9.12.x xConfiguration Cameras PowerLine Frequency xConfiguration Logging CloudUpload Mode xConfiguration UserInterface Assistant Mode

2 Release Notes

Type	Release Note
MDVNS-SCC-4.6.0	
Added	The ability to upgrade to and downgrade from RoomOS 11.9 without cleaning the SCC.
Added	Support for Cisco Webex Room Bar Pro.
Resolved	An issue where setting the SCC clock backward before the SCC booted caused SNMP notifications to fail.
MDVNS-SCC-4.5.0	
Added	An option to synchronize the SCC clock with Freeport Management Suite (FMS) via the SCC Web UI. If FMS is enabled and this option is checked, the SCC clock will be updated at the beginning of each network join operation. The clock will not be updated if a firmware update is required.
Improved	Audit logging feature. • Added details of what has changed to audit logs generated as a result of web client save operations. Password fields will be obscured in the audit log. • Added "UTC" indicator to audit logs.
Added	A dialog to the SCC Web UI when the user logs out or is logged out due to inactivity.
Improved	Password requirement options. Added entry fields for number inputs with minimum values.
Added	The ability to send real-time alerts as SNMP traps or inform messages. Traps will currently be sent for four events: 1. Audit failure, e.g. disk is full and can't write to the audit log. 2. If heartbeat traps are enabled, send periodic traps. This is useful for configuring SNMP manager systems to communicate with SCC. Heartbeat traps will only be sent in Maintenance Mode. 3. Join failure. Alert will include SCC name and CODEC name. 4. Leave failure. Alert will include SCC name and CODEC name. Currently traps can only be sent to one SNMP manager. A reboot is required to apply SNMP configuration.

Type	Release Note
	Several trap configuration options are available: • Support SNMPv2c or SNMPv3 traps and informs. • For inform messages, retries and timeouts can be configured. The SCC 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.
Improved	Active Directory functionality. • Added simple authentication option. Both simple authentication and NTLM are now supported. For simple authentication, usernames should be entered as User Principal Name (e.g. user@domain). For NTLM, usernames are entered as Domain\User. • Added the ability to optionally 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. • Add the ability to assign Admin role via Active Directory user groups. • Added a setting to optionally override the context used when searching for Active Directory user groups. SCC will try to determine the context from the server response. The LDAP context can be overridden if the context cannot be determined automatically. The format is CN=MYLDAP,DC=COMPANY,DC=COM.
Improved	Syslog functionality. • Added options to the syslog configuration for TCP, TLS, Certificate Verification, and Hostname verification • Syslog messages will be sent in a format compliant with RFC 5424. Newlines will be escaped within messages and a single newline will be added at the end of all messages.

Type	Release Note
Improved	The security of the SCC configuration import/export feature. • Configuration export data will be encrypted within the configuration export file. The user must supply a password for the encryption, which will be required to import the file. • Imports will support both encrypted and unencrypted data (from previous firmware versions). If the file was encrypted during export, the user will be prompted for the password before importing, and will have the option to preview the import data in raw JSON format. Password fields will be obscured in the preview data. • The hidden setting Link Timeout (previously available via the configuration file) can now be set through the SCC Web UI. *This can only be set from the "Link Failed" diagnostic when the SCC is receiving no data from the CODEC.
Improved	The SCC configuration export feature available in the Web UI. Security (password) settings, syslog settings, Active Directory configuration, and Notification (SNMP) configuration will be included with security export.
Improved	The SCC configuration import feature available in the Web UI. Added the ability to selectively import sections of a SCC configuration file. When importing a configuration, the user will be prompted for which portions to import. The following options are available: • SCC Configuration includes the options in the "Management Settings" section of the System Info tab • SCC Network includes the options in the "Network Settings" section of the System Info tab • SCC License Keys will add any license keys found in the export file, only if they are valid for the SCC import target • SCC Security includes "Password Settings" and "Centralized User Management (Active Directory)" from the Security tab, as well as "Notifications" and "Syslog Settings" from the Issues and Diagnostics tab *SCC Security import is not available for export files generated with SCC firmware versions previous to 4.5 • CODEC Configuration includes the "CODEC Settings", "Post-restore Commands", and "Pre-sanitize Commands" sections of the CODEC Settings tab and the "Passwords" on the CODEC Security tab

Type	Release Note
	• CODEC Capture includes "Camera Presets", "Configuration", "Directory", and "Sign-in Banner" from the CODEC Settings tab, as well as "CODEC Users" from the CODEC Security tab, and captured branding images
Added	A refresh button to the configuration import/export card of the Web UI, which clears the selected file and any popup form fields.
Added	Support for Cisco RoomOS 11.5 software. It should be possible to upgrade to/downgrade from this version without resetting the capture.
MDVNS-SCC-4.4.0	
Added	Support for Cisco RoomOS 11.1 firmware. It should be possible to upgrade to/downgrade from this version without resetting the capture. The following xConfiguration entries were moved to new locations. These entries will receive their default value after upgrade to RoomOS 11.1. The previous value will be lost, so these entries should be configured before capturing the new configurations. xConfiguration Conference MaxTotalReceiveCallRate becomes xConfiguration Conference MaxMultisiteReceiveRate xConfiguration Conference MaxTotalTransmitCallRate becomes xConfiguration Conference MaxMultisiteTransmitRate xConfiguration Usertnterface WallpaperOverlay becomes xConfiguration Usertinerface CustomWallpaperOverlay xConfiguration Apps Homescreen Dashboard becomes xConfiguration UserInterface HomeScreen Dashboard
Added	Support for the Cisco Webex Room Bar. The first software version supported by this CODEC is RoomOS 10.19. It should be possible to upgrade to/downgrade from RoomOS 11.1 without resetting the SCC/capture.
New Feature	Added a field for entering commands to be sent to the CODEC before sanitization. If capture is enabled, the commands will be sent after the capture process has completed. Each line will be treated as a command. Commands are case insensitive. Commands will not be retried. • 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

Type	Release Note
	expected response is not received, a warning will be logged along with the response received from the CODEC. • 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. • 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.
MDVNS-SCC-4.3.0	
Resolved	An issue in which camera presets failed to restore. Don't send "Default" as the value for the "Lens" parameter of "xCommand Camera PositionSet".
Improved	The ability to upload large "Custom Brand Background" images during a network join. Please note that uploading large image files to the CODEC via a serial connection may significantly increase how long it takes to join a network.
Updated	To the Dunfell branch of Yocto (version 3.1).
Added	Support for Cisco CODECs running RoomOS version 10.15 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
Added	Support for the Cisco Board Pro CODEC (RoomOS version 10.11 and later). Upgrades to/from the support firmware version should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
Added	Support for Cisco CODECs running RoomOS version 10.19 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
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.
Updated	Nginx webserver to version 1.17.8
MDVNS-SCC-4.2.0	

Type	Release Note
Resolved	A problem where fixing an SCC diagnostic issue does not remove the alert from the user interface. Added a label to the SCC web interface indicating to the user that clicking the refresh button will re-run the SCC diagnostics.
Added	A system alert when a user has exceeded the Maximum Failed Logins. A indicator in the users table on the security tab indicates whether the user has experienced failed logins since the last login. The alert will link to that page and the admin can see immediately which users are affected.
Added	Support for Cisco CODECs running Cisco RoomOS version 10.11 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
Added	Support for Cisco CODECs running RoomOS version 10.8 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
Improved	The CODEC compatibility settings. The "CODEC Model" setting in the CODEC settings section of the SCC web interface is now True/False. The system admin needs to specify if the CODEC is a SX20/MX200 or MX300 G2, since these models use a different baud rate than all of the other models.
Validated	Support for Cisco SX/MX CODECs running Cisco CE version 9.15.10 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
Added	Support for Cisco SX/MX CODECs running Cisco CE version 9.15.8 firmware. Upgrades and downgrades to/from this version from/to lower versions should not require the SCC units to be cleaned, however, it is still recommended to perform a "capture" as soon as possible.
MDVNS-SCC-4.1.2	
Improved	The SCC boot process upon startup.

Type	Release Note
	SCC Units will now boot in roughly 15 seconds (with a static IP address) and 22 seconds (set to DHCP), though boot time will vary with DHCP performance. *Please note that this update addresses a bug in which the MDVNS system was timing out when joining a network. The SCC Units in the associated systems were being managed on a production network via DHCP.
MDVNS-SCC-4.1.1	
Improved	Clock functionality
MDVNS-SCC-4.1.0	
Added	Support for Cisco CE 9.15.3. This patch release of CE firmware added some xConfigurations and removed "xConfiguration Bookings ProtocolPriority" from DX/MX/SX endpoints.
Added	Support for Cisco RoomOS 10.3. Upgrading/downgrading between RoomOS 10.3 and CE 9.x will work without cleaning the CODEC configuration out of the SCC.
Resolved	An issue in the SCC web interface where the CODEC admin username was masked as if it was a password.
Improved	Session expiration time due to inactivity of the SCC web interface to 15 minutes. Approximately two minutes before the session ends, a warning will be displayed showing the time remaining. When the session ends, the browser will redirect to the login page.
New Feature	Implemented audit logging. The audit log will be saved as a separate rotating log file on the SCC, which can be viewed in the web interface, and will be exported with the log bundle. An entry will be added to the audit log when a user makes a change to the system, e.g. save configuration. The log entry will contain the username and the IP address where the request originated where applicable. Actions initiated by the system do not have a user or IP address. Audit logs cannot be deleted, except by full factory reset. Sensitive information in the audit log will be delimited by two single quotation marks. This will make it easier to add a feature to remove sensitive information when exporting log files.
Improved	The SCC web server secutirty. The web server will only support TLS 1.2 and above.

Type	Release Note
	Connections to FMS will only support TLS 1.2 and above.
New Feature	Added the ability to create, update, and delete SCC users. Users can be assigned the Admin role, which grants the ability to log into the web interface. Users can be marked as inactive, preventing any logins. Users' passwords will expire according to the password setting "Maximum Lifetime," unless the user has "Password never expires". An admin can use the web interface to immediately expire a user's password. A user with an expired password will not be able to complete login until the password is changed, subject to the password settings. Removed the "SCC Admin Password" box from the "SCC and CODEC Passwords" tab as this is now set on the "Security" tab. Renamed the "SCC and CODEC Passwords" tab to "CODEC Security".
New Feature	Added the ability to upload certificate authorites to an SCC unit. This is a prerequisite to Active Directory integration.
New Feature	Added support for the AUX key position on the front of the SCC unit. When the key is set in the AUX position, the SCC can be directed (via the SCC5Net Switch API) to perform a one-time capture when leaving a network. This provides the ability to initiate a capture via a third-party control system.
New Feature	Added SCC web interface alerts. Added a status flag to the web interface banner area which will show up if there are any alerts. This links to the Issues and Diagnostics tab when clicked. Placed alerts on a separate tab. Moved the log file interface to this tab. Each alert includes a title, description, severity icon, and link to the tab where the issue can be fixed. There are currently five potential issues that will flag an alert: 1. Unsupported CODEC firmware version 2. CODEC firmware type is misconfigured as TC 3. CODEC firmware type is misconfigured as CE 4. CODEC admin account has no password 5. SCC credentials are set to the default, sysop/freeporttech

Type	Release Note
New Feature	Added syslog logging to a configurable IP and UDP port. Audit logs, errors, and warning will be sent to the syslog server.
New Feature	Added the ability to manage the SCC admin username in FMS. Along with the SCC Password, this defines a special account that is managed only by FMS. Requires FMS version 4.1.400.2158 or later.
New Feature	Added a setting for maximum failed logins. If too many failed logins, the user account will be locked out for 15 minutes.
New Feature	Added password complexity settings: • Minimum length • Minimum uppercase characters • Minimum lowercase characters • Minimum numerical digits • Minimum special characters • Minimum number of previous passwords that can't be reused Password rules will be enforced when passwords are set in the user interface. Added number of days before a password expires. Once a password expires, it must be changed at the next login.
New Feature	Added the ability to authenticate with an Active Directory server 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.
New Feature	When registered with FMS, the SCC will send audit logs, errors and warning to FMS as they happen. These can be viewed on the Audit Logs page of the FMS user interface.
MDVNS-SCC-4.0.9	

Type	Release Note
Added	Support for Cisco CE version 9.13. CODEC firmware can be upgraded to CE 9.13 from earlier versions without having to clean the SCC of the previously captured CODEC configuration. Please note that activating Service Certificates for purpose pairing is not currently supported.
Added	Support for Cisco Webex Room Kit Mini and Webex Desk Pro CODECs.
MDVNS-SCC-4.0.8	
Added	Support for Cisco CE version 9.12. CODEC firmware can be upgraded to CE 9.12 from earlier versions without having to clean the SCC of the previously captured CODEC configuration.
Resolved	An issue introduced in SCC firmware version 4.0.7 related to SCC Units managed by FMS. SCC firmware updates via FMS were not being applied until the next time the SCC powered on.
Resolved	A bug in which clearing a password in the SCC Web UI would instead change the password if there were values in the password and password verify boxes. This affected CODEC admin password, SIP Password, SIP Turn Password, and HTTP Proxy Password. The clear button will now always clear the password, or fail if a blank password is not allowed.
MDVNS-SCC-4.0.7	
Added	A firmware failure notification. If an SCC firmware upload fails an error message will be displayed in the SCC Web UI.
Resolved	An issue related to Web Server Certificate submittal via the SCC Web UI. After the Web Server Certificate is uploaded, the certificate form (including the password) will be cleared after the certificate is successfully submitted.
Improved	The viewing of log files via the SCC Web UI. The most recent log files are now located at the top of the drop down list.
Added	An option to enable the serial port on the back of the SCC unit to be used for logging.

Type	Release Note
	This new feature will be disabled by default.
Improved	The naming convention of the SCC configuration file created using the Configuration Export function of the SCC Web UI. If the SCC Name has been set, this will be used in place of the MAC address. The configuration export file name will also include the Network Name and the SCC firmware version.
Added	The ability to hide success messages (DEBUG, INFO) when viewing log files.
Updated	Support for Cisco CE 9.10. If the current Cisco CODEC firmware is CE 9.10 or greater, the following be relevant: 1. The CODEC options "FIPS Mode" and "Strong Security Mode" will be hidden from the SCC Web UI as these are now part of the CODEC xconfig being captured/restored by the SCC Unit. 2. The SCC Web UI will manage CODEC user passwords according to the last captured password policy configuration enforced in the CODEC. 3. Password policy configurations (xConfiguration UserManagement PasswordPolicy) will be sent to the CODEC at the start of the restore process, before users are created. 4. If the admin user's password that is stored in the SCC doesn't satisfy the password policy configuration enforced in the CODEC, the restore process will fail and the system will not join the selected network. 5. If a non admin user's password doesn't satisfy the password policy configuration enforced in the CODEC, that user will not be created, but the system will join the selected network. 6. Changing the default value of the following configuration items will enforce a reboot of the CODEC before it joins the selected network (xConfiguration Security Fips Mode (default off), xConfiguration Security Session MaxFailedLogins (default 0), xConfiguration Security Session FailedLoginsLockoutTime (default 60), xConfiguration Security Session InactivityTimeout (default 0)). Cisco Firmware Notes: 1. SCC firmware 4.0.6 and earlier will be incompatible with Cisco CE 9.10. All user creation will fail. 2. SCC firmware 4.0.7 is compatible with Cisco CODECS running firmware earlier than CE 9.10. However, FIPS and Strong Security Mode settings must be configured via the CODEC Settings tab of the SCC Web UI.

Type	Release Note
New Feature	Added the ability to download all SCC log files plus the SCC configuration via a new "Download All Logs" button on the System Info tab of the SCC Web UI. The files will be saved as an archive file (tar.gz). The file name will include the SCC Unit's Name, the Network Name, and the current SCC firmware version.
Resolved	An issue where the system might fail to join a network if the Cisco CODEC firmware has been upgraded or downgraded. Error handling has been in improved in order to account for Cisco serial API changes. Any captured configuration items that don't apply to the current Cisco firmware version will not be restored to the CODEC. Please note that this feature will not support unofficial/unreleased Cisco firmware. In addition, the SCC Units in your system should always be running the latest released firmware before upgrading the Cisco CODEC firmware.
Improved	The CODEC User information listed on the SCC and CODEC Passwords tab of the SCC Web UI. The CODEC User information will indicate whether or not a password has been set for each user. It will also indicate if the password does not satifsy the current password policy enforced in the CODEC (xConfiguration UserManagement PasswordPolicy).
Improved	The SCC Unit's log files to include the SCC MAC address. The MAC address will be displayed at the top of each SCC log file.
MDVNS-SCC-4.0.6	
Improved	Support for the Cisco Room Kit Pro. With the release of Cisco firmware CE 9.8.1, the MDVNS now fully supports the "SerialPort LoginRequired" configuration setting. Cisco CE firmware revision history: 1. Initial versions of CE firmware did not allow the "Off" value for the "SerialPort LoginRequired" configuration. 2. CE 9.7.2 and CE 9.8.0 added support for the "Off" value, but when the value was set to "Off," the serial port did not function at all. All commands returned errors indicating no permissions. 3. CE 9.8.1 no has full support for "SerialPort LoginRequired: Off" (same as the SX80). Please Note:

Type	Release Note
	• Room Kit Pro firmware versions earlier than CE 9.8.1 require "SerialPort LoginRequired: On" for compatiblity with any SCC firmware version. • Room Kit Pro firmware versions CE 9.8.1 and later require "SerialPort LoginRequired: On" for compatiblity with SCC firmware versions 4.0.5 and earlier. • Room Kit Pro firmware versions CE 9.8.1 and later are fully compatible with SCC firmware versions 4.0.6 and later.
MDVNS-SCC-4.0.5	
Updated	The default setting for the "Post-Restore Reboot" option (listed under CODEC Settings in the SCC Web UI). The default setting was changed from "Before" to "None". This setting is only applied if "Post Restore Commands" are being utilized.
MDVNS-SCC-4.0.3	
Updated	The default CODEC firmware type for new SCC units. Default firmware support is now Cisco CE.
Updated	The branding of "SCC Manager" in the SCC Web UI. SCC Manager has officially merged into "Freeport Management Suite" (FMS).
Resolved	An issue in which the SCC Web UI would fail to accept a CODEC certificate if the certificate had text preceding the "----- BEGIN CERTIFICATE -----" line.
Resolved	An issue that requires serial log-in required to be enabled for the selected network in order to upload branding images larger than about 4K. The SCC unit will toggle the setting if necessary before uploading branding images, and then set it back to the desired value before restoring the CODEC configuration.
Added	The ability to enable/disable FIPS mode on the CODEC for the selected network. This feature is Cisco firmware dependent (The FIPS mode command does not exist in Cisco firmware versions CE9.2.6, 9.3.2, and 9.3.3). Note: Enabling this feature currently requires a reboot of the CODEC.
Added	The ability to enable/disable Strong Security mode on the CODEC for the selected network. When this option is enabled, the SCC Web UI will enforce DoD JITC passphrase requirements for all user accounts as documented in the latest Cisco Administrator Guide.

Type	Release Note
	Note: Enabling this feature currently requires a reboot of the CODEC in order for the CODEC Web UI to accurately show that Strong Security mode is enabled (*even though all requirements have actually been enforced). *This bug has been reported to Cisco and once it is resolved the reboot requirment will be removed via a future SCC firmware release.
Added	The ability to brand an SCC Unit with a "SCC Name" via the SCC Web UI.
Resolved	An issue when importing an SCC configuration file with the incorrect password for the SCC web server certificate. This action would disable the SCC web server. Since the SCC web server certificate is not part of the SCC configuration file when it is exported, the password should not be included either.
Resolved	An issue which occurs when uploading a PEM certificate file that uses carriage return + line feed as the line endings. Note: This appears to be a bug in Cisco CE firmware. Line endings will be converted to line feed before uploading certificates.
MDVNS-SCC-4.0.2	
Improved	The ability to support CODEC's which require serial port log-in to be enabled. If serial port log-in required is enabled for the selected network and the CODEC is rebooted or closes the serial port a new SCC5Net API command provides the ability to re-stablish the connection (via the SCC Unit) for third party control.
Added	Support for the Cisco Room Kit Pro CODEC.
MDVNS-SCC-4.0.11	
Added	Support for CE 9.15. CODEC firmware can be upgraded to CE 9.15 from earlier versions without having to clean the SCC of the previously captured CODEC configuration. Note: Service Certificate Purposes HttpClient, Pairing, and WebexIdentity are not supported.
MDVNS-SCC-4.0.10	

Type	Release Note
Added	Support for Cisco CE version 9.14. CODEC firmware can be upgraded to CE 9.14 from earlier versions without having to clean the SCC of the previously captured CODEC configuration.
MDVNS-SCC-4.0.1	
Added	The"Ignore Camera Preset Failures" feature to the CODEC Settings tab of the SCC web interface. Enabling this feature will ensure a more reliable network transition if there are a large number of camera presets being utilized. When this feature is enabled (True), if the process of capturing or restoring camera presets is taking a long time the system will not time out and/or fail when leaving or joining the selected network.
Resolved	A issue where the SCC would fail to link with an SX20 CODEC when a non-default Admin username is configured and the MDVNS is rebooted.
Improved	The ordering of fields listed on the CODEC Settings tab of the SCC web interface. They are now grouped by functionality. Also standardized the use of CODEC vs. Codec.
Added	Support for the capture/restore of the lens value when using a Cisco Quad camera.
Updated	Cisco CE firmware compatibility. This version of SCC firmware provides compatibility with the following Cisco CE versions 9.2.6, 9.3.2 and 9.4.0. Please note that earlier SCC firmware may not function as expected with these or later versions of CE.
Added	The ability to change the username of the built-in Admin user account.
Added	A new feature that pulls the CODEC system name and displays it in the SCC web interface under System Info>Network Settings. In addition, the CODEC system name will be uploaded as part of the SCC information when connected to the Freeport Management Suite (SCC Manager v4.0.6 or later).
Resolved	An issue where the network settings listed in the SCC web interface might not fully refresh after changes have been made (e.g. DHCP remains checked after refresh when DHCP is not enabled).
Added	Support for the Webex Room Kit and Room Kit Plus.
Added	The ability to delete old SCC log files via the SCC web interface.

Type	Release Note
MDVNS-SCC-4.0.0	
Initial Build	• **Added capabilities** o DNS Addressing o Web UI acknowledgement banner o CODEC acknowledgement banner o Network name o Network color o HTTPS o TLS 1.2 o Realtime Clock o Join, Leave, Maintenance, Exception Logs o Configuration import / export o Licensed firmware, browse to select o Capture user credential o SIP Turn Password o IEEE802.1X Password o Proxy Password o Provisioning Password o Configuration modification via web UI o Camera preset modification via web UI o Directory modification via web UI o Post restore reboot • **Improved** o Web UI Experience o Camera global presets o Camera individual presets o Certificate usage o Directory entry limit 1 dial method to <=75 o Directory entry limit 2 dial methods to <=75 o Improved factory default trailing actions o Cisco TC firmware usage o Cisco CE firmware usage o ISDN link capability • **Removed** o HTTP
Improved	• The ability to support 802.1x certificates. Certificates for 802.1x will only be active if the CODEC is running CE9.2.4 or later. • All other certificates will be accesible when using CE9.2.1 or above.
Improved	• The ability to change CODEC firmware without cleaning the SCC of the last captured CODEC configuration. • If a CODEC configuration is captured with one version of CODEC firmware (e.g. CE 9.2), and restored to a CODEC running another version of firmware (e.g. CE 9.1), the SCC unit will attempt to compensate. Any xConfiguration commands that are added in the later version of software will not be sent if the CODEC is running an earlier version. Similarly, any configurations that are removed in a later CE software version will not be sent if the capture is from an earlier version.

Type	Release Note
	• It is still recommended to recapture for each network when the CODEC firmware is updated. • This does not apply to TC firmware. This will not work for configurations that are modified to add or remove a new value. If the capture contains a configuration that exists in the current software version, but the value for that configuration is not valid in the current software version, the restore will fail. This is based on the SX80 codec. It is not guaranteed to work for all models because some configurations may be added in different versions for different CODECs. Consult the Cisco API reference for details of which configurations are added and removed for each software version.
Improved	• The behavior of "Loaded" LED indicator on the front of the SCC Unit. • Flashing "Loaded" LED - Indicates that the SCC contains information that can be configured via the web GUI (SCC & CODEC settings, Passwords, Certificates, etc). • Solid "Loaded" LED - Indicates that SCC contains CODEC information that has been captured (Configuration, Camera Pre-sets, Directory Entries, User Accounts, etc).