



# Cisco Unified Border Element

- [Feature history for Cisco Unified Border Element, on page 1](#)
- [Cisco Unified Border Elements \(CUBE\), on page 3](#)
- [Supported devices for CUBE configuration, on page 3](#)
- [Restrictions for CUBE configuration, on page 4](#)
- [Use cases for CUBE, on page 4](#)
- [Configure CUBE, on page 4](#)
- [CUBE commands, on page 5](#)
- [SRST commands, on page 14](#)

## Feature history for Cisco Unified Border Element

*Table 1: Feature history*

Feature Name	Release Information	Description
Cisco Unified Border Element (CUBE)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can configure CUBE functionality by using Cisco IOS XE Catalyst SD-WAN devices CLI templates or CLI add-on feature templates.

Feature Name	Release Information	Description
Secure SRST Support on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	Secure SRST Support on Cisco Catalyst SD-WAN allows you to configure Cisco Survivable Remote Site Telephony (SRST) commands and additional Cisco Unified Border Element (CUBE) commands. Using these commands within Cisco IOS XE Catalyst SD-WAN devices, you can: <ul style="list-style-type: none"> <li>• Maintain voice services at remote sites during network outages.</li> <li>• Extend advanced voice and video connectivity within Cisco Catalyst SD-WAN</li> </ul> <p>You can configure these commands on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.</p>
Supported Voice and SIP-UA Commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands that enhance voice and SIP-UA functionalities on Cisco IOS XE Catalyst SD-WAN devices. These commands include: <ul style="list-style-type: none"> <li>• <b>cipher (voice class)</b></li> <li>• <b>nat media-keepalive</b></li> <li>• <b>secure-ciphersuite</b></li> <li>• <b>transport tcp tls (sip-ua)</b></li> <li>• <b>voice-class sip nat media-keepalive</b></li> </ul>
Survivable Remote Site Telephony (SRST) commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands related to secure HTTP client communication and <code>call-manager-fallback</code> transport. These commands include: <ul style="list-style-type: none"> <li>• <b>http client secure-ciphersuite</b></li> <li>• <b>transport-tcp-tls (call-manager-fallback)</b></li> </ul>

# Cisco Unified Border Elements (CUBE)

A Cisco Unified Border Element (CUBE) is a network device or software that facilitates voice and video connectivity between different Voice over IP (VoIP) networks. It primarily functions as a Session Border Controller (SBC), enabling communication between enterprise networks and Internet telephony service providers (ITSPs).

Unlike traditional voice gateways that use circuit-switched connections, such as PRI, to connect to telephone companies, CUBE replaces physical voice trunks with IP-based voice trunks. This allows it to connect directly to other VoIP networks and ITSPs.

CUBE provides conventional SBC functions. It also offers a wide variety of advanced features to manage and secure VoIP sessions.

## Configuration

You can configure CUBE functionality on Cisco IOS XE Catalyst SD-WAN device using device CLI templates or CLI add-on feature templates.

For more information about CUBE setup, functionality, usage, configuration, and related topics, see the [Cisco Unified Border Element Configuration Guide](#).

# Supported devices for CUBE configuration

The following devices support CUBE configuration:

- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8000v Software Router
- Cisco ASR 1001-X Router
- Cisco ASR 1002-X Router
- Cisco ASR 1006-X Router with the Cisco ASR1000-RP3 Module, and the Cisco ASR1000-ESP100 or ASR1000-ESP100-X Embedded Services Processor
- Cisco ASR 1004 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006-X Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor

# Restrictions for CUBE configuration

High-availability configuration is not supported for CUBE.

## Use cases for CUBE

CUBE can configure SBC elements for various applications, such as:

- Enterprise Premises-Based Collaboration: using Cisco Unified Communications Manager (or another call control application) with centralized or local PSTN breakouts.
- Local Breakout Gateway for Cisco Unified Communications Manager Cloud: a Cisco-hosted cloud service for large enterprises.
- Local Gateway to Enable the Bring Your Own PSTN (BYoPSTN) Option for Cisco Webex Calling: to enable the Bring Your Own PSTN (BYoPSTN) option.
- Edge Audio for Cisco Webex Meetings: with a direct VoIP route to the Cisco Webex cloud or through existing PSTN services.

## Configure CUBE

This task guides you on how to configure CUBE functionality on a device.

Complete these steps to configure CUBE:

### Before you begin

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

### Procedure

---

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

### Example:

The following example shows a basic CUBE configuration using a CLI add-on template:

```
voice service voip
ip address trusted list
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
!
allow-connections sip to sip
sip
no call service stop
!
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
```

```
session protocol sipv2
incoming called number .T
voice-class codec 1
dtmf-relay rtp-nte
!
dial-peer voice 101 voip
description Outbound LAN side dial-peer
destination pattern [2-9].....
session protocol sipv2
session target ipv4:10.10.10.1
voice-class codec 1
dtmf-relay rtp-nte
!
dial-peer voice 200 voip
description Inbound WAN side dial-peer
session protocol sipv2
incoming called-number .T
voice-class codec 1
dtmf-relay rtp-nte
!
dial-peer voice 201 voip
description Outbound WAN side dial-peer
destination pattern [2-9].....
session protocol sipv2
session target ipv4:20.20.20.1
voice-class codec 1
dtmf-relay rtp-nte
```

For information about device CLI templates, see [CLI templates for Cisco IOS XE Catalyst SD-WAN devices](#).

For information about CLI add-on feature templates, see [CLI add-on feature templates](#)

For information about CUBE configuration and usage, see [Cisco Unified Border Element Configuration Guide](#).

For information about the CUBE commands that Cisco Catalyst SD-WAN supports for use in a CLI template, see [CUBE commands, on page 5](#).

---

After successfully applying the configuration, the device is enabled to function as a Cisco Unified Border Element, processing voice and video traffic according to the defined dial-peers and voice service settings.

#### What to do next

After configuring CUBE, you should verify the voice service and dial-peer configurations to ensure proper call routing and media handling. You can also integrate the CUBE-enabled device with your Cisco Unified Communications Manager or other call control applications. For more information, see [Verify CUBE on the Device](#).

## CUBE commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for CUBE configuration. Click a command name in the Command column to view information about the command, its syntax, and its use.

Table 2: Cisco Catalyst SD-WAN CLI template commands for CUBE configuration

Command	Description
<a href="#">address-hiding</a>	Hides signaling and media peer addresses from endpoints other than the gateway.
<a href="#">anat</a>	Enables Alternative Network Address Types (ANAT) on a SIP trunk.
<a href="#">answer-address</a>	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
<a href="#">application (global)</a>	Enters application configuration mode to configure applications.
<a href="#">asserted-id</a>	Enables support for the asserted ID header in incoming SIP requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages.
<a href="#">asymmetric payload</a>	Configures SIP asymmetric payload support.
<a href="#">audio forced</a>	Allows only audio and image (for T.38 Fax) media types, and drops all other media types).
<a href="#">authentication</a>	Enables SIP digest authentication.
<a href="#">bind</a>	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.
<a href="#">block</a>	Configures global settings to drop (not pass) specific incoming SIP provisional response messages on a CUBE.
<a href="#">call spike</a>	Configures the limit on the number of incoming calls received in a short period (a call spike).
<a href="#">call threshold global</a>	Enables the global resources of a gateway.
<a href="#">call treatment action</a>	Configures the action that the router takes when local resources are unavailable.
<a href="#">call treatment cause-code</a>	Specifies the reason for the disconnection to the caller when local resources are unavailable.
<a href="#">call treatment isdn-reject</a>	Specifies the rejection cause code for ISDN calls when all ISDN trunks are busied out, but the switch ignores the busyout trunks and still sends ISDN calls into the gateway.
<a href="#">call treatment on</a>	Enables call treatment to process calls when local resources are unavailable.
<a href="#">callmonitor</a>	Enables the call monitoring messaging functionality on a SIP endpoint in a VoIP network.
<a href="#">call-route</a>	Enables header-based routing at the global configuration level.

Command	Description
<a href="#">cipher (voice class)</a>	Configures the cipher setting, and associates it to a TLS profile.
<a href="#">clid</a>	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and removes the calling party name and number from the calling-line identifier in voice service voip configuration mode. Alternatively, allows the presentation of the calling number by substituting for the missing <b>Display Name</b> field in the Remote-Party-ID and From headers.
<a href="#">codec preference</a>	Specifies a list of preferred codecs to use on a dial peer.
<a href="#">codec profile</a>	Defines audio and video capabilities that are needed for video endpoints.
<a href="#">codec transparent</a>	Enables codec capabilities to be passed transparently between endpoints in a CUBE.
<a href="#">conn-reuse</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Reuses the TCP connection of a SIP registration for an endpoint behind a firewall.
<a href="#">connection-reuse</a>	Uses global listener port for sending requests over UDP.
<a href="#">contact-passing</a>	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
<a href="#">cpa</a>	Enables the call progress analysis (CPA) algorithm for outbound VoIP calls and to set CPA parameters.
<a href="#">credentials</a>	Configures a SIP TDM gateway or CUBE to send a SIP registration message when in the UP state.
<a href="#">crypto signaling</a>	Identifies the <b>trustpoint</b> <i>trustpoint-name</i> keyword and argument that is used during the Transport Layer Security (TLS) handshake that corresponds to the remote device address.
<a href="#">dial-peer cor custom</a>	Specifies that named class of restrictions (COR) apply to dial peers.
<a href="#">dial-peer cor list</a>	Defines a class of restrictions (COR) list name.
<a href="#">disable-early-media 180</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP).
<a href="#">dspfarm profile</a>	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

Command	Description
<a href="#">dtmf-interworking</a>	Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from CUBE, and generates RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE.
<a href="#">early-media update block</a>	Blocks the UPDATE requests with the Session Description Protocol (SDP) in an early dialog.
<a href="#">early-offer</a>	Forces CUBE to send a SIP invite with Early Offer on the Out Leg.
<a href="#">emergency</a>	Configures a list of emergency numbers.
<a href="#">error-code-override</a>	Configures the SIP error code to be used at the dial peer.
<a href="#">error-passthru</a>	Enables the passage of error messages from the incoming SIP leg to the outgoing SIP leg.
<a href="#">g729-annexb override</a>	Configures the settings for G.729 codec interoperability and overrides the default value if the annexb attribute is not present.
<a href="#">gcid</a>	Enables Global Call ID (GCID) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.
<a href="#">gw-accounting</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables an accounting method for collecting call detail records (CDRs).
<a href="#">handle-replaces</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level.
<a href="#">header-passing</a>	Enables the passing of headers to and from SIP INVITE, SUBSCRIBE, and NOTIFY messages.
<a href="#">host-registrar</a>	Populates the sip-ua registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response.
<a href="#">http client connection idle timeout</a>	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.
<a href="#">http client connection persistent</a>	Enables HTTP persistent connections so that multiple files can be loaded by using the same connection.
<a href="#">http client connection timeout</a>	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt.
<a href="#">ip qos dscp</a>	Configures the DSCP value for QoS.

Command	Description
<a href="#">localhost</a>	Globally configures CUBE to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages.
<a href="#">max-conn</a>	Specifies the maximum number of incoming or outgoing connections for a particular VoIP dial peer.
<a href="#">max-forwards</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Globally sets the maximum number of hops, that is, proxy or redirect servers that can forward the SIP request.
<a href="#">media</a>	Enables media packets to pass directly between endpoints without the intervention of CUBE, and enables signaling services.
<a href="#">media disable-detailed-stats</a>	Disables the collection of detailed call statistics.
<a href="#">media profile asp</a>	Creates a media profile to configure acoustic shock-protection parameters.
<a href="#">media profile nr</a>	Creates a media profile to configure noise-reduction parameters.
<a href="#">media profile stream-service</a>	Enables stream service on CUBE.
<a href="#">media profile video</a>	Creates a media profile video.
<a href="#">media-address voice-vrf</a>	Associates an RTP port range with VRF.
<a href="#">media-inactivity-criteria</a>	Specifies the mechanism for detecting media inactivity (silence) on a voice call.
<a href="#">midcall-signaling</a>	Configures the method that is used for signaling messages.
<a href="#">min-se</a>	Changes the minimum session expiration (Min-SE) header value for all the calls that use the SIP session timer.
<a href="#">nat</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Uses SIP Network Address Translation (NAT) global configuration.
<a href="#">nat media-keepalive</a>	Enables media keepalive packet transmission for the specified interval of time.
<a href="#">notify redirect</a>	Enables application handling of redirect requests for all VoIP dial peers.
<a href="#">notify ignore substate</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies Ignoring the Subscription-State header in a Notify message.

Command	Description
<a href="#">notify telephone-event</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.
<a href="#">num-exp</a>	Defines how to expand a telephone extension number into a particular destination pattern.
<a href="#">options-ping</a>	Enables in-dialog options.
<a href="#">outbound-proxy</a>	Configures a SIP outbound proxy for outgoing SIP messages globally.
<a href="#">pass-thru content</a>	Enables the pass-through of SDP from in-leg to the out-leg.
<a href="#">permit hostname</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Stores hostnames used during validation of initial incoming INVITE messages.
<a href="#">privacy</a>	Sets privacy support at the global level as defined in RFC 3323.
<a href="#">privacy-policy</a>	Configures the privacy header policy options at the global level.
<a href="#">progress_ind</a>	Configures an outbound dial peer on a CUBE to override and remove or replace the default progress indicator in specified call messages.
<a href="#">protocol mode</a>	Configures the Cisco IOS SIP stack.
<a href="#">random-contact</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Populates an outgoing INVITE message with random-contact information instead of clear-contact information.
<a href="#">reason-header override</a>	Enables cause code passing from one SIP leg to another.
<a href="#">redirect ip2ip</a>	Redirects SIP phone calls to SIP phone calls globally on a gateway.
<a href="#">redirection</a>	Enables the handling of 3xx redirect messages
<a href="#">referto-passing</a>	Disables dial peer lookup and modification of the Refer-To header when the CUBE passes across a REFER message during a call transfer.
<a href="#">registrar</a>	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
<a href="#">rellxx</a>	Enables SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint.
<a href="#">remote-party-id</a>	Enables translation of the Remote-Party-ID SIP header.

Command	Description
<a href="#">requiri-passing</a>	Enables pass-through of the host part of the Request-URI and To SIP headers.
<a href="#">retry bye</a>	Configures the number of times that a BYE request is retransmitted to the other user agent.
<a href="#">retry invite</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
<a href="#">rtcp all-pass-through</a>	Passes through all the RTCP packets in the datapath.
<a href="#">rtcp keepalive</a>	Configures RTCP keepalive report generation and generates RTCP keepalive packets.
<a href="#">rtp payload-type</a>	Identifies the payload type of an RTP packet.
<a href="#">rtp-media-loop count</a>	Configures the number of media loops before RTP voice and video media packets are dropped.
<a href="#">rtp-port</a>	Configures the real-time protocol range.
<a href="#">rtp-ssrc multiplex</a>	Multiplexes RTCP packets with RTP packets and sends multiple synchronization source in RTP headers (SSRCs) in an RTP session.
<a href="#">secure-ciphersuite</a>	Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE.
<a href="#">session refresh</a>	Enables SIP session refresh globally.
<a href="#">session transport</a>	Configures a VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.
<a href="#">set pstn-cause</a>	Maps an incoming PSTN cause code to a SIP error status code.
<a href="#">set sip-status</a>	Maps an incoming SIP error status code to a PSTN cause code.
<a href="#">signaling forward</a>	Configures global settings for transparent tunneling of QSIG, Q.931, H.225, and ISUP messages.
<a href="#">silent discard untrusted</a>	Discards SIP requests from untrusted sources in an incoming SIP trunk.
<a href="#">sip-server</a>	Configures a network address for the SIP server interface.
<a href="#">srtp</a>	Specifies that SRTP be used to enable secure calls and call fallback.
<a href="#">srtp negotiate</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level.

Command	Description
<a href="#">stun</a>	Enters STUN configuration mode for configuring firewall traversal parameters.
<a href="#">stun flowdata shared-secret</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a secret shared on a call control agent.
<a href="#">stun usage firewall-traversal flowdata</a>	Enables firewall traversal using STUN.
<a href="#">supplementary-service media-renegotiate</a>	Globally enables midcall media renegotiation for supplementary services.
<a href="#">timers</a>	Configures SIP-signaling timers.
<a href="#">transport</a>	Configures the SIP user agent (gateway) for SIP signaling messages in inbound calls through the SIP TCP, TLS over TCP, or UDP socket.  This command supports TLS version 1.3 and all associated ciphers.
<a href="#">uc secure-wsapi</a>	Configures a secure Cisco Unified Communication IOS services environment for a specific application.
<a href="#">uc wsapi</a>	Configures a nonsecure Cisco Unified Communication IOS services environment for a specific application.
<a href="#">update-callerid</a>	Enables sending updates for caller IDs.
<a href="#">url (SIP)</a>	Configures URLs to either the SIP, SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls.
<a href="#">vad</a>	Enables VAD for calls using a specific dial peer.
<a href="#">video codec</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.
<a href="#">voice cause code</a>	Sets the internal Q850 cause code mapping for, voice and enters voice cause configuration mode.
<a href="#">voice class codec</a>	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.
<a href="#">voice class dpg</a>	Creates a dial-peer group for grouping multiple outbound dial peers.
<a href="#">voice class e164-pattern-map</a>	Creates an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer.
<a href="#">voice class media</a>	Configures media control parameters for voice.
<a href="#">voice class server-group</a>	Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses) that can be referenced from an outbound SIP dial peer.

Command	Description
<a href="#">voice-class sip options-keepalive</a>	Monitors connectivity between CUBE VoIP dial peers and SIP servers.
<a href="#">voice class sip-copylist</a>	Configures a list of entities to be sent to the peer call leg.
<a href="#">voice class sip-event-list</a>	Configures a list of SIP events to be passed through.
<a href="#">voice class sip-hdr-passthruelist</a>	Configures a list of headers to be passed through the route string.
<a href="#">voice-class sip nat media-keepalive</a>	Configures media keepalive to enable media keepalive packets to be transmitted for the interval specified.
<a href="#">voice class sip-profiles</a>	<p>Configures SIP profiles for a voice class.</p> <p>Configuring a sip profile, <b>request REGISTER sip-header Authorization modify "550\"," [550@dl.ims.airtel.in mailto:550@dl.ims.airtel.in]"</b>, on a device throws a warning message:</p> <pre>Device# show run sec sip-profiles voice class sip-profiles 4 rule 2 request REGISTER sip-header Authorization modify "550\"," "[550@dl.ims.airtel.in mailto:550@dl.ims.airtel.in]"</pre>
<a href="#">voice class srtp-crypto</a>	Enters voice class configuration mode and assigns an identification tag for an <b>srtp-crypto voice class</b> command.
<a href="#">voice class uri</a>	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
<a href="#">voice class tls-cipher</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures an ordered set of TLS cipher suites.
<a href="#">voice class tls-profile</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables voice class configuration mode, and assigns an identification tag for a TLS profile.
<a href="#">voice iec syslog</a>	Enables viewing of internal error codes as they are encountered in real time.
<a href="#">voice statistics iec</a>	Enables collection of internal error code statistics.
<a href="#">xfer target</a>	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Routes the INVITE to the refer-to destination in the REFER consume case. The routing decision is made based on the xfer target destination.

## SRST commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST. Click a command name in the Command column to view information about the command, its syntax, and its use.

*Table 3: Cisco Catalyst SD-WAN CLI template commands for SRST*

Command	Description
<a href="#">http client secure-ciphersuite</a>	Sets the secure encryption cipher suite for the HTTP client.
<a href="#">transport-tcp-tls (call-manager-fallback)</a>	Configures a specific TLS version for Unified Secure SCCP SRST, in call-manager-fallback mode.