Security for Generic Secure Video SIP Endpoints

This document covers security and other miscellaneous functional specifications required for parties that use any of the following three endpoint types on Cisco Unified Communications Manager Release 8.6.1:

- Generic Desktop Video Endpoint
- Generic Single Screen Room System
- Generic Multiple Screen Room System

This document includes the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Scope

This document provides details on how to use the following three Cisco Unified Communications Manager Session Initiation Protocol (SIP) endpoint types:

- Generic Desktop Video Endpoint (GDVE)
- Generic Single Screen Room System (GSSRS)
- Generic Multiple Screen Room System (GMSRS)

Each of these endpoint types supports video, Secure Real-time Transport Protocol (sRTP) for the audio/video streams, and Transport Layer Security (TLS) for the signaling channel.

Currently, the Cisco Partner Program offers third party developers the chance to develop custom endpoint types with varying levels of functionality and security. We recommend that endpoint developers developing their own custom endpoint types utilize this program.

This document does not supersede the Cisco Partner Program. Rather, it provides additional tips on how to utilize the three specific SIP Endpoint types mentioned in a Cisco Unified Communications Manager environment.

This document covers the following feature requirements:

- Configuration of the three SIP endpoint types within Cisco Unified Communications Manager
- Registration as one of the three endpoint types
- Secure certificates provision and management
- SIP sRTP/TLS support for the three endpoint types within Cisco Unified Communications Manager
- Cisco proprietary sRTP to RTP fallback mechanism
- Security status indicators (Secure Icon)

This document presents details on how endpoint developers can implement secure audio and video via sRTP, and secure signaling via TLS, on their endpoints when registered as one of the three endpoint types (GDVE, GSSRS, GMSRS). These details allow the endpoint to work within the Cisco Unified Communications solution.

This document does not cover the configuration and upgrade process within the Cisco Unified Communications solution.

Functional Overview

Feature List (Hardware)

Third party hardware details are beyond the scope of this document.

Feature List (Software/Firmware)

Tag	Headline	Requirement	Priority
NT-400	sRTP/TLS to endpoint	Vendor endpoint must support SIP sRTP/TLS with Cisco Unified Communications Manager.	M
NT-410	sRTP to RTP fallback mechanism	Vendor endpoint must support a mechanism to fall back from sRTP to RTP mode. This is necessary in case of a failure to negotiate secure media.	M
NT-420	Credential management	Vendor endpoint must support credentials import. In addition, Cisco Unified Communications Manager must support credentials import from the Endpoint.	M
NT-430	Multiple Lines Configuration	Vendor endpoint must utilize a single shared TCP or TLS connection when multiple lines are configured for any of the three new endpoint types.	M
NT-440	Contact header	Vendor endpoint must utilize an ephemeral port in the contact header in the REGISTER message.	M
NT-450	Registration rules	Vendor endpoint must register with the appropriate Contact and Supported header.	M
NT-460	Call-Info SIP Header	Vendor endpoint must support Call-Info header in order to get a report of security status .	M

Vendor Endpoint Must Register with Appropriate REGISTER Details

As mentioned, this specification adds three endpoint types: Generic Desktop Video Endpoint (GDVE), Generic Single Screen Room System (GSSRS), and Generic Multiple Screen Room System (GMSRS). Each of these endpoint types must register with specific details in order to be identified both as that

endpoint type and also as a unique device within that endpoint type. Following are sample registrations for each endpoint type. In these examples, the Contact and Supported headers contain the information that identifies the endpoint type.

Generic Desktop Video Endpoint (GDVE)

```
REGISTER sip:172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:23323;branch=z9hG4bK2af-EEEE10000001--1703793266-771
From: <sip:2610@172.18.203.37:5061>;tag=-1703793266
To:<sip:2610@172.18.203.37:5061>
Call-ID: EEEE1000-0001-2610--1703793266
CSeq: 1 REGISTER
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:2610@172.18.200.154:23323;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-EEEE10000001>";+u.sip!model.ccm.cisco.com="588"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0
```

Generic Single Screen Room System (GSSRS)

```
REGISTER sip:172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.156:48046;branch=z9hG4bK2af-EEEE10000001--1703113223-38
From: <sip:2620@172.18.203.37:5061>;tag=-1703113223
To:<sip:2620@172.18.203.37:5061>
Call-ID: EEEE1000-0001-2620--1703113223
CSeq: 1 REGISTER
User-Agent: SIPGenericRoomSystemSS
Contact: <sip:2620@172.18.200.156:48046;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-EEEE10000001>";+u.sip!model.ccm.cisco.com="582"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0
```

Generic Multiple Screen Room System (GMSRS)

```
REGISTER sip:172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.134:33858;branch=z9hG4bK2af-EEEE10000002--1703038725-88
From: <sip:2630@172.18.203.37:5061>;tag=-1703038725
To:<sip:2630@172.18.203.37:5061>
Call-ID: EEEE1000-0002-2630--1703038725
CSeq: 1 REGISTER
User-Agent: SIPGenericRoomSystemMS
Contact: <sip:2630@172.18.200.134:33858;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-EEEE10000002>";+u.sip!model.ccm.cisco.com="583"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0
```

The Contact header information is used to determine the following:

- Endpoint Type (GDVE, GSSRS, or GMSRS). The endpoint type is indicated by the "+u.sip!model.ccm.cisco.com="<model#>"" tag. The value for each endpoint type that appears in this tag is as follows:
  - GDVE: +u.sip!model.ccm.cisco.com="588"
  - GSSRS: +u.sip!model.ccm.cisco.com="582"
  - GMSRS: +u.sip!model.ccm.cisco.com="583"

- Individual endpoints within a specific type. For example, if two GDVE devices are configured, the Contact header is used to distinguish between them.

  The MAC address is the mechanism for distinguishing one endpoint from another. This is part of the +sip.instance tag in the contact header. For example, a GMSRS endpoint with the MAC address of EEEE10000002 would be tagged with the following:

  "+sip.instance="<urn:uuid:00000000-0000-0000-0000-EEEE10000002>""

The Supported header is required to have, at a minimum, the following tags:

Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0

The X-cisco-callinfo tag indicates support for the Call-Info header. The X-cisco-srtp-fallback tag value indicates support for the Cisco proprietary sRTP fallback procedure. The X-cisco-sis-5.1.0 tag value indicates support for version 5.1.0 of the SIP Interface Specification.

Other miscellaneous requirements are as follows:

- The vendor endpoint must utilize a single shared TCP or TLS connection when multiple lines are configured for any of the three new endpoint types.
- The vendor endpoint must use an ephemeral port in the Contact header for the REGISTER message. Cisco Unified Communications Manager will reuse the same connection for new requests to the endpoint.

Vendor Endpoint Must Support sRTP/TLS with Cisco Unified Communications Manager

Call and Media signaling from the endpoint to Cisco Unified Communications Manager must be protected with an encrypted secure connection. The endpoint must establish a connection with Cisco Unified Communications Manager based on its configuration file. If the endpoint is configured with encrypted secure state, then it will establish an encrypted secure signaling connection with Cisco Unified Communications Manager.

In addition, the endpoint must use the sRTP protocol to secure the media data. The sRTP key must be acquired as per Cisco guidelines, and each RTP stream should be encrypted with a different key. The sRTP key is sent to the endpoint in the encrypted signaling connection. An encrypted secure connection is required for media encryption.

According to Cisco security guidelines, Cisco recommends that vendor endpoint developers meet the following guidelines for sRTP/TLS implementation:

Key protocols and drafts version:

- TLS version 1.0 support as per RFC-2246.
- For sRTP or media privacy, the endpoint should support crypto parameters in SDP according to *Session Description Protocol Security Descriptions for Media Stream (draft-ietf-mmusic-sdescriptions-09.txt),* along with the Cisco proprietary sRTP to RTP fallback procedure.
- If the endpoint supports the Real-time Transport Control Protocol (RTCP), the device must also support the Secure Real-time Transport Control Protocol (sRTCP) when sRTP is used for the media stream.

Secure mechanisms:

- TLS mutual authentication and sRTP key generation procedure, as per Cisco guidelines.

- A support mechanism is required to negotiate sRTP and RTP. This media negotiation must provide a way to either negotiate up to sRTP, or negotiate down to RTP. The Cisco proprietary sRTP to RTP fallback procedure that is described in this document must be used for sRTP negotiation.
- The endpoint must not reveal any key material (endpoint private keys, TLS session keys, or sRTP session keys) through debug traces or other means of access. The endpoint must provide the best protection to all secret materials.

Ciphers and Certificates:

- The endpoint should support the advertisement of the TLS_RSA_WITH_NULL_SHA cipher for troubleshooting purposes.
- The endpoint must support X509v3 certificate using RSA public/private key algorithm of size 1024 bits and 2048 bits. The signature algorithm should be RSA-SHA1.
- The endpoint should include a cipher for sRTP. It must support AES_CM_128_HMAC_SHA_32. There should be no Forward Error Correction (FEC), Master Key Identifier (MKI), or lifetime parameters in the crypto line.

  Example: a=crypto:1 AES_CM_128_HMAC_SHA1_32
  inline:O9OCSlDU7cjbw23hF4L1ojKitKt6AQAZM5azkrsX

This document contains a detailed description of the required TLS mutual authentication procedure, sRTP key generation mechanism and Cipher suites.

Vendor Endpoint Must Support sRTP to RTP Fallback

The endpoint must support the Cisco proprietary sRTP to RTP fallback procedure, which allows for both secured and nonsecured modes of media support. The Cisco proprietary sRTP to RTP fallback procedure, when enabled, allows an sRTP-supporting SIP device to send a SIP message containing an sRTP offer within its SDP portion. If the remote endpoint does not support sRTP or the specified crypto parameters, it may ignore all crypto parameters and answer back with an RTP SDP message (the media type on the media line also changes to RTP/AVP from the offered RTP/SAVP). The initial offering SIP device interprets this as negotiating down to RTP instead of failing the media negotiation.

From a Cisco Unified Communications Manager perspective, the sRTP fallback mechanism is enabled during registration with Cisco Unified Communications Manager.

```
REGISTER sip:khilam-ccm-02 SIP/2.0
Via: SIP/2.0/Tls 172.18.199.159:37392;branch=z9hG4bK2af-FFDE10000001--843724371-597
From: <sip:6130000@khilam-ccm-02>;tag=-843724370
To: <sip:6130000@khilam-ccm-02>
Call-ID: FFDE1000-0001-6130000--843724371
CSeq: 1 REGISTER
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:6130000@172.18.199.159:37392;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-FFDE10000001>";+u.sip!model.ccm.cisco.com="588"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0
```

For network administrator control, the endpoint must provide a configuration option to enable and disable the sRTP fallback mechanism at a device level. If the sRTP fallback mechanism is disabled at a device level, the endpoint will only offer and accept an sRTP connection request. If the sRTP fallback mechanism is enabled at the device level, the media may end up as either sRTP or RTP depending on the result of the connection negotiation.

Security Icon Status

Trust Status (Device Trust Mode)

The Device Trust Mode may be configured to Trusted or Not Trusted. sRTP and TLS capabilities are fully functional whether the Device Trust Mode is set to Trusted or Not Trusted. However, for a call to be considered secure, and for the Security icon to light, the Device Trust Mode must be set to Trusted. If the Device Trust Mode is set to Not Trusted, then the call will be considered nonsecured.

The configuration of the Device Trust Mode is discussed in detail later in the configuration section.

Vendor Endpoint Must Support Call-Info header

In order for an endpoint to receive the notifications of security status that enable it to light a Security icon, or a status on the device that indicates if a call is secured, the endpoint must advertise support for the Call-Info header and must also support that header when it is received. If the endpoint does not support a secure status indicator (i.e. Security icon), it does not need to advertise support for the Call-Info header.

To advertise support for the Call-Info header, the "x-cisco-callinfo" tag should always be included in the Supported header whenever it is sent to Cisco Unified Communications Manager. At a minimum, the Supported header must be sent to Cisco Unified Communications Manager in the REGISTER messages (see below). A sample of a REGISTER message from one of the three endpoint types included is as follows:

```
REGISTER sip:khilam-ccm-02 SIP/2.0
Via: SIP/2.0/Tcp 172.18.199.159:37392;branch=z9hG4bK2af-FFDE10000001--843724371-597
From: <sip:6130000@khilam-ccm-02>;tag=-843724370
To: <sip:6130000@khilam-ccm-02>
Call-ID: FFDE1000-0001-6130000--843724371
CSeq: 1 REGISTER
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:6130000@172.18.199.159:37392;transport=tcp>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-FFDE10000001>";+u.sip!model.ccm.cisco.com="588"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0
```

The vendor endpoint must be able to decipher the Call-Info header that is sent from Cisco Unified Communications Manager. The Call-Info header may appear in a variety of messages, including the INVITE, UPDATE, 180 RINGING, 183 Session Progress, 200 OK to an INVITE, or the 200 OK to an UPDATE. Following is a sample of the Call-Info header that is sent from Cisco Unified Communications Manager to an endpoint:

```
INVITE sip:3200@172.18.202.93:43286;transport=tls;conference-id=0 SIP/2.0
Via: SIP/2.0/TLS 172.18.202.96:5061;branch=z9hG4bK43cad7881
From: <sip:3100@172.18.202.96>;tag=1152~b43ea526-a700-4a22-8605-9a5b66389cb6-23104620
To: <sip:3200@172.18.202.96>
Date: Tue, 03 Aug 2010 21:14:35 GMT
Call-ID: 1c863500-c58186bb-2a-60ca12ac@172.18.202.96
Supported: timer,resource-priority,replaces
Min-SE:  1800
User-Agent: Cisco-CUCM8.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 101 INVITE
Expires: 180
```

```
Allow-Events: presence, kpml
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= from; gci= 1-18004;
call-instance= 1
Send-Info: conference
Alert-Info: <file://Bellcore-dr1/>
Remote-Party-ID: <sip:3100@172.18.202.96;x-cisco-callback-number=3100>;party=calling;
screen=yes;privacy=off
Contact: <sip:3100@172.18.202.96:5061;transport=tls>;video;audio;conference-id=0
Max-Forwards: 69
Content-Length: 0
```

As shown, the Call-Info header that is sent from Cisco Unified Communications Manager has many data items. The pertinent tag/value pair that dictates the security status from Cisco Unified Communications Manager is the security=<value>. All other tag or tag/value pairs in the Call-Info header may be ignored except "ui-state= ringout", which is described in "ui-state= ringout".

When a secured endpoint has an active call, Cisco Unified Communications Manager provides the appropriate security status information to the devices that are involved in the call. When multiple endpoints are involved in a call, the security status of a call is determined by the least of the security statuses of all the endpoints involved in the call. Call control and feature logic within Cisco Unified Communications Manager maintain the security status for the call. Currently, three values can be passed to the device. The list ranges from least secure to most secure.

- **Not Authenticated** indicates the current connected call is not signaling authenticated. This call is not secure
- **Authenticated** indicates the current connected call is signaling authenticated. This is not a fully secured call.
- **Encrypted** indicates the current connected call is signaling/media encrypted. This call is secure.

Cisco Unified Communications Manager uses the Call-Info header to pass this status to the phone. In the absence of the Call-Info header, the phone assumes a value of Unknown. Here is an example that uses the urn feature naming scheme where the feature is Call-Info and the security status is encoded as a generic parameter.

```
Call-Info: <urn:X-cisco-remotecc:callinfo>; security=Encrypted
```

Endpoints must present the call security level dictated by Cisco Unified Communications Manager in the Call-Info header, especially if the call security level specified by Cisco Unified Communications Manager is lower than the call leg security level of the endpoint. For instance, if the endpoint is using encrypted TLS signaling and sRTP media, Cisco Unified Communications Manager may still signal a call security level of Not Authenticated or Authenticated because Cisco Unified Communications Manager allows mixing of secured and nonsecured call legs via external conference bridges.

Because Cisco Unified Communications Manager is a back-to-back user agent (B2BUA), we must look at call setup and mid-call updates to determine when the Call-Info header will be sent (i.e. which method or response).

Call Setup:

The security status of the call is known by the endpoints as follows:

- Originating side (A side):

  When the endpoint originates an INVITE to Cisco Unified Communications Manager, assuming Cisco Unified Communications Manager extends the call forward, the security status is known after the 200 OK is generated back to the phone. The 200 OK contains the Call-Info header that displays the security status.

- Terminating side (B side):

  Cisco Unified Communications Manager does not evaluate the security status of the call until both endpoints are connected from a signaling perspective. For a call leg that terminates on a SIP device, the value is known after the ACK is sent to the device. However, RFC 3261 precludes an ACK from containing a Call-Info header. Therefore, the Call-Info header will be sent in a subsequent reINVITE or UPDATE.

Mid-call updates:

Feature invocations cause dialogs to be manipulated. This can impact the security status. For example, assume that endpoints A and B are connected securely, but A is transferred to C which is unsecured. For the endpoints already involved in a call, a change in status will be sent via a reINVITE or UPDATE message. In this example, endpoint A receives a reINVITE or UPDATE containing the Call-Info header with a new security status.

"ui-state= ringout"

As mentioned, nonsecurity status tag/values in the Call-Info header may be ignored. The one exception is the "ui-state= ringout" value, if received after the call setup. After the call setup, when a SIP phone on Cisco Unified Communications Manager is the transferee in an early-attended transfer, we need its reflect ringout even though its signaling state is already connected. Note that the transferrer and the transferee are talking, and are thus connected, prior to the actual transfer. When the transfer occurs, the target rings. The only way for the transferee (the user) to know what has happened is to play ringback. The phone has no way of knowing this via standard SIP signaling (post-call setup). Cisco Unified Communications Manager notifies the phone via a Call-Info header.

Following is an example using the urn feature-naming scheme where the feature is Call-Info and the ui-state information is encoded as a generic parameter.

```
Call-Info: <urn:x-cisco-remotecc:callinfo>; ui-state= ringout
```

The phone is responsible for transforming this "ui-state" indication into ringback, if received. If the target answers, the transferee will get a reINVITE or UPDATE to connect with the target. This reINVITE or UPDATE will not contain a ui-state value and phone must stop playing ringback in this case.

The consequence of not acting on the ui-state after call setup is that the ringback may not be heard when the endpoint is the transferee in an early-attended transfer.

Cisco Unified Communications Manager Security Administration Configuration for the Endpoint

The security administration configuration consists of two parts:

- Phone Security Profile
- Cisco Unified Communications Manager Endpoint Device Configuration Page

Phone Security Profile

In Cisco Unified CM Administration, the administrator has the option to create an endpoint security profile by selecting **System > Security Profile > Phone Secure Profile.**

The vendor endpoint Phone Security Profile consists of the following fields:

- Phone Security Profile Information
    i. Product Type—The vendor endpoint.
    ii. Device Protocol—SIP only.
    iii. Name—The user-defined profile name. When this profile is saved, the name that is displayed in the Device Security Profile drop-down list box in the Phone Configuration window for the phone type and protocol.
    iv. Description—User-defined description of the security profile.
    v. Nonce Validity Time—The default value equals 600 (10 minutes). When the time expires, Cisco Unified Communications Manager generates a new value.
    vi. Device Security Mode—Non secure, Authenticated, or Encrypted.
        - Non Secure—No security features exist for the phone. A TCP or UDP connection opens to Cisco Unified Communications Manager.
        - Authenticated—A TLS connection that uses NULL/SHA opens for signaling. The media (audio/video) remains RTP.
        - Encrypted—A TLS connection that uses AES128/SHA opens for signaling, and sRTP carries the media for all phone calls on all sRTP-capable hops.

          More details on supported ciphers is covered in section 3.2.10.
    vii. Transport Type—TCP and/or UDP. TLS is set for encrypted device security mode.
    viii. Enable Digest Authentication—When digest authentication enabled for a phone, Cisco Unified Communications Manager challenges all SIP phone requests except keepalive messages. Cisco Unified Communications Manager uses the digest credentials for the end user, as configured in the End User Configuration window, to validate the credentials that the phone offers.
    ix. Exclude Digest Credentials in Configuration File—Not applicable for vendor endpoints.
- Parameters used in Phone:

  SIP Phone Port—This setting applies to SIP phones that use UDP transport. Enter the port number for Cisco Unified IP Phones (SIP only) that use UDP to listen for SIP messages from Cisco Unified Communications Manager. The default setting equals 5060. For phones that use TCP or TLS, ignore this setting.

There are no Certificate Authority Proxy Function (CAPF) or TFTP related fields on the vendor endpoint secure profile, as seen for other Devices.

Next, depending on which of the three new device types is used, one of the following security profiles must be configured:

Figure 1 Generic Desktop Video Endpoint Sample Configuration

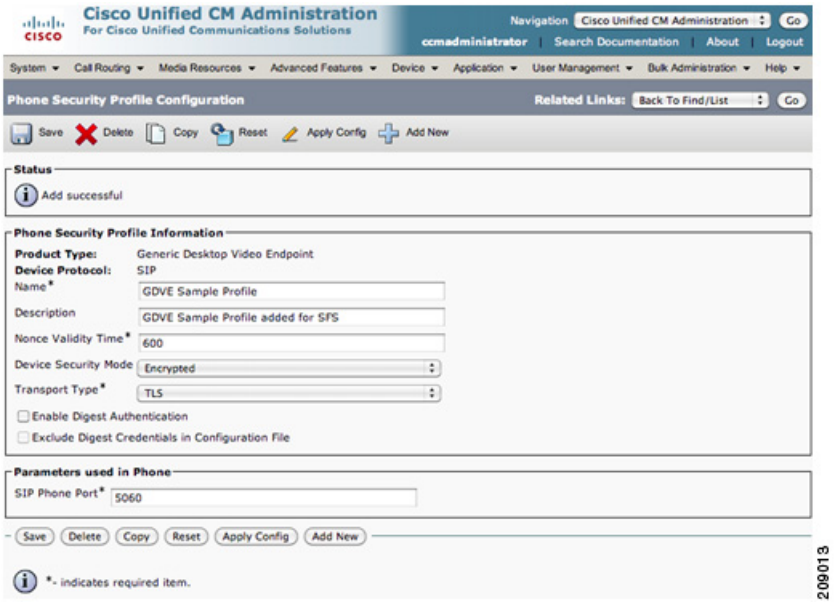


Figure 2 Generic Single Screen Room System Sample Configuration

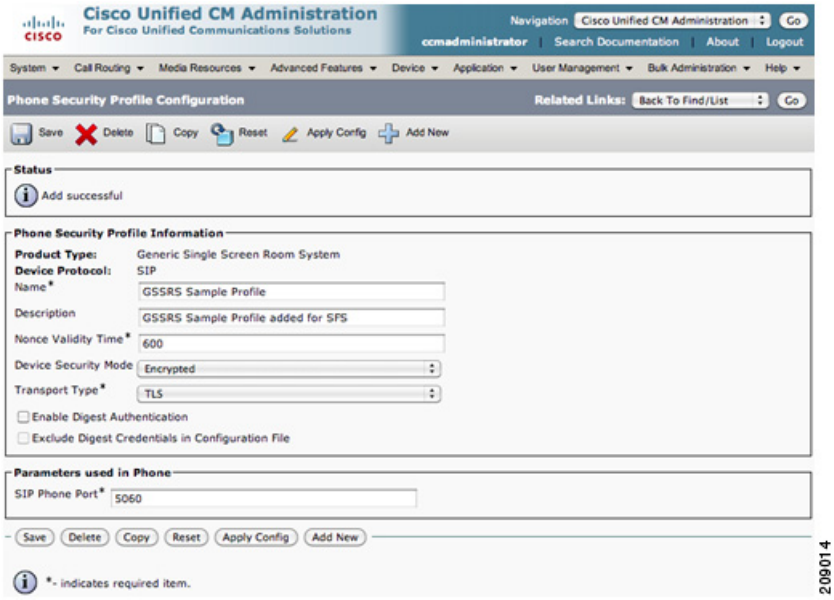
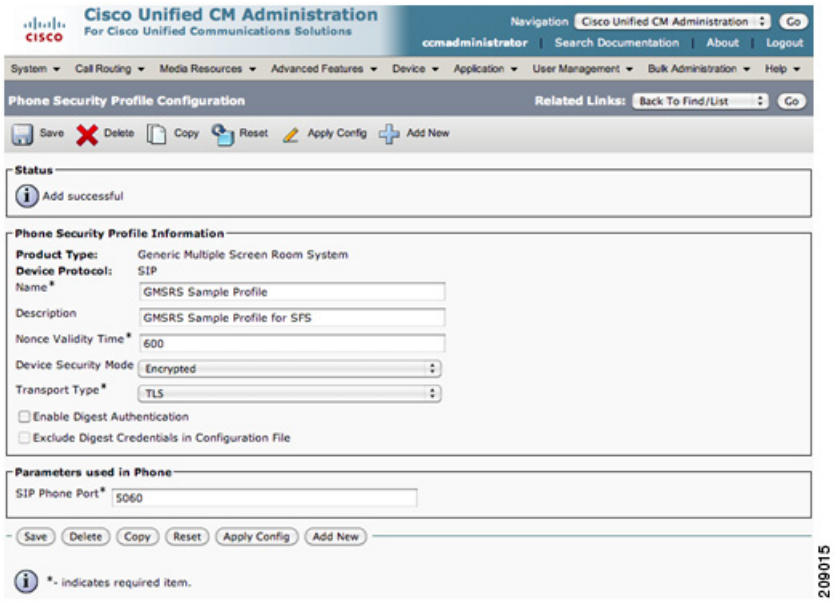


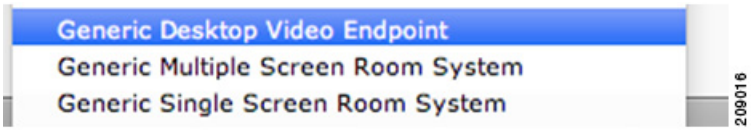
Figure 3 Generic Multiple Screen Room System Sample Configuration



Cisco Unified Communications Manager Endpoint Device Configuration Page

From Cisco Unified CM Administration, administrators can add a new phone by selecting **Device > Phone** and clicking the **Add New** button. If a new phone is added, administrators have the option of adding one of the three following phone types shown here:

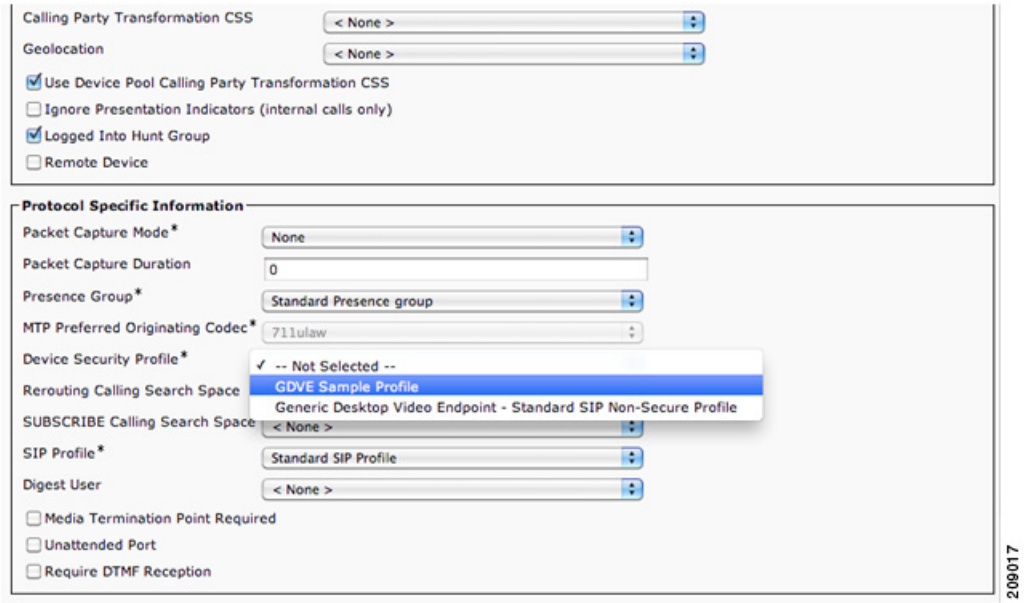
Figure 4 Generic Secure Video SIP Endpoint Types



In the Phone Configuration window, the administrator can select a Device Security Profile under Protocol Specific Information configuration.

A sample of this configuration for the Generic Desktop Video Endpoint follows:

Figure 5 Phone Configuration Window for SIP Endpoints



Secure Credential Management and Provisions

To support the sRTP/TLS feature, the vendor endpoint shall support the import of Cisco Unified Communications Manager X509v3 certificates. In addition, Cisco Unified Communications Manager should import X509v3 certificates of the endpoint's certificate issuers (chain). The details of the certificate format and provision are described further in this document.

The mechanism to import Cisco Unified Communications Manager certificates to the endpoint shall be provided by the endpoint and is outside of the existing Cisco Unified Communications Manager certificates distribution through Certificate Trust List file download and verification mechanism.

The certificate format that is supported for Cisco Unified Communications Manager 8.5 import/export is PEM. Correspondingly, the PEM format should be supported for endpoint import/export.

Features Not Addressed

The following features are not supported:

- Cisco Unified Communications Manager Registration Failover and Fallback support
- Survivable Remote Site Telephony (SRST) support

Because the Cisco Unified Communications Manager Failover/Fallback is not supported, the endpoint may choose to support Domain Name System Service (DNS-SRV) record-based redundancy. The SIP phone should follow the DNS-SRV procedures described in RFC 3263 to achieve load balancing and redundancy. To work properly with Cisco Unified Communications Manager, the nodes listed in the SRV record must match the nodes configured in the Cisco Unified Communications Manager Group assigned

to the SIP device in the Cisco Unified Communications Manager database. It is the responsibility of the administrator to keep the SRV record synchronized with the Cisco Unified Communications Manager Group configuration. If the SRV query returns an address that is not part of the Cisco Unified Communications Manager Group for the device, and the phone attempts to register to that Cisco Unified Communications Manager Group, registration will fail. If an SRST node is configured in the Device Pool for the SIP phone, it can also be included in the SRV record, but only UDP will be supported.

Cisco Unified Communications Manager uses a device-oriented approach to registration and redundancy. All lines on a single phone must register to the same Cisco Unified Communications Manager node, and when a failure is detected, all lines on the phone must fail over to the same secondary node. Registering the same line on more than one node is not allowed, nor is registering different lines from one physical device to different Cisco Unified Communications Manager nodes. Therefore, all lines on a given SIP phone must have the same DNS-SRV configuration. Load balancing is allowed on a device basis, so different SIP phones can have different DNS-SRV configurations.

A Cisco Unified Communications Manager node will not accept requests (other than REGISTER) from a SIP phone unless the phone is actively registered on that node. Therefore, the phone must send all non-REGISTER requests only to the actively registered node. If the active Cisco Unified Communications Manager node fails, and the phone is using UDP transport, there will be some delay (less than or equal to the registration refresh interval) until the phone detects the failure and re-registers with the next Cisco Unified Communications Manager node in the SRV list. Cisco Unified Communications Manager uses a short register refresh interval (default is 120 seconds), so the failure will likely be detected before a call is attempted. However, if a shorter outage window is desired, the refresh interval can be changed in the SIP Station Keepalive Interval Service parameter for the Cisco Unified Communications Manager service. Note that this applies to all SIP stations and may affect call capacity.

Typically, when DNS-SRV is used, the DNS-SRV Fully Qualified Domain Name (FQDN) is included in the Request-URI for requests sent from the SIP phone to Cisco Unified Communications Manager. If this is the case, the Cluster Fully Qualified Domain Name Enterprise parameter must be updated to include the SRV FQDN. Otherwise, the address in the Request-URI will not be recognized as belonging to the Cisco Unified Communications Manager cluster, and the request will be rejected.

Interface Specifications

The external specifications define the functions and features of the product as viewed by the user, as well as the external interfaces and design constraints. This information provides a basis for internal (architectural) design and a source for developing test plans, technical documentation, and support plans.

Functional Requirements

Media Negotiations

To establish, transmit, and receive sRTP streams, both ends need to agree upon commonly supported crypto parameters and codecs. The procedure to negotiate offer and answer for sRTP follows the *draft-ietf-mmusic-sdescriptions* framework with the Cisco proprietary sRTP fallback procedure described in the subsequent sections. The Cisco procedure allows sRTP fallback to RTP as well as the limited crypto attributes in the offered SDP.

If the crypto attribute negotiation is successful, which can result in either sRTP or RTP media streams, then the codec negotiation of that media line continues. The media line is selected for the media streams when both crypto attribute and codec negotiations are successful.

Negotiating Offered SDP

We recommended that when the offered SDP is received, the crypto attributes for each media line be negotiated as follows:

If the transport type of the offered media line is RTP/AVP (RTP is offered), then the crypto attribute negotiation is considered to be successful, but the result is RTP media.

If the transport type of the offered media line is RTP/SAVP (sRTP is offered), then the call signaling is checked for secure signaling (TLS authenticated and encrypted). If the call signaling is not secured, and the sRTP fallback for that line is enabled, then the media transport falls back to RTP/SAVP. If the call signaling is not secured, and the sRTP fallback is not enabled, then the crypto negotiation fails and the call is rejected.

If call signaling is secured then the crypto attributes of the media line are checked for a valid and supported crypto attribute. If a valid and supported crypto attribute is not found, and the sRTP fall back is enabled, then the media transport will fall back to RTP. Otherwise, if a valid and supported crypto attribute is not found and the sRTP fallback is not enabled, then the crypto negotiation fails and the call is rejected.

Negotiating Answer SDP

When the answered SDP is received, for each media line the crypto attributes are negotiated as follows:

If the remote media transport type is RTP/AVP and the phone offers RTP/AVP, the media transport type is RTP. The crypto negotiation is successful.

If the remote media transport type is RTP/AVP and the phone offers RTP/SAVP, this is a mismatched media transport. The remote endpoint does not understand the offered RTP/SAVP and ignores the offered crypto attribute. If the sRTP fallback is enabled for that line, the negotiated media transport type falls back to RTP/AVP. Otherwise, the crypto negotiation fails and the call is rejected.

Building Offer SDP

The sRTP offer is included in the SDP when a secure connection (TLS authenticated and encrypted) is used with Cisco Unified Communications Manager. The only crypto suite that is offered is AES_CM_128_HMAC_SHA1_32 without other key parameters and no session parameter. Therefore, the single audio media line will contain a single crypto attribute.

Example:

```
a = crypto: 1 AES_CM_128_HMAC_SHA1_32 inline:
NzB4d1B1NUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj
```

The preceding example shows a single key without any other parameters. The vendor endpoint should support a maximum life time 2^48 by default. The lifetime parameter in the SDP must not be populated.

Building Option Response SDP

If the vendor endpoint supports SDP in an OPTION response, the SDP must not contain sRTP and key materials in situations where the call signaling is not secure.

Crypto Parameters Validation

If the received SDP has crypto lines that contain nonsupported crypto parameters, the crypto line should be ignored. If the key lifetime is not specified, the vendor endpoint assumes the maximum lifetime.

Note In the Cisco Unified Communications Manager environment, the key lifetime is not supported.

Secure Media Fallback Conditions

During the negotiation of crypto attributes, a condition may be encountered that causes the phone to fall back to RTP if sRTP fallback is enabled. This may happen if any of the following conditions are true:

- The remote media transport type is RTP/AVP.
- No suitable crypto attribute is found from the remote SDP (all crypto attributes are invalid or are not supported).
- Call signaling is not secure (not TLS authenticated and encrypted).

sRTP Session Key Generation and Re-Keying

The sRTP session key is generated or regenerated under any of the following conditions:

- Each call has a separate sRTP session key in the initial offer/answer SDP.
- A delayed media re-INVITE is received.
- A re-INVITE to resume a held call is sent.
- When remote changes are made to the media address (not port).
- When a vendor endpoint receives an offer with media direction changed from inactive to anything else.

Remote port change is not considered as a crypto context changes and does not cause the key to be regenerated.

The regeneration of the key, when received in an offer with media changed from inactive to anything else, is done to prevent the scenario whereby a call is transferred to another endpoint, or resumed by another endpoint, without a change in the destination address. This scenario is possible if there is a pass-through media termination point (MTP) in the middle.

The generation of the session key (and salt) must use a cryptographically approved pseudo random number generator.

Secure Signaling Connection

When the vendor endpoint is configured for a secure connection with Cisco Unified Communications Manager, the endpoint establishes a permanent TLS connection with Cisco Unified Communications Manager. The endpoint represents the client side of the connection. The port can be configured with a default value of 5061. The port value must be configured with the same value in the endpoint device security profile as on Cisco Unified Communications Manager.

The vendor endpoint shall establish only one TLS connection to each Cisco Unified Communications Manager cluster for all SIP signaling messages regardless of the number of supported BRI lines or analog lines that are configured on the endpoint.

The vendor endpoint must support TLS mutual authentication. The endpoint returns its certificates when client certificate is requested during TLS handshake. When the endpoint receives Cisco Unified Communications Manager certificates during the TLS handshake, the endpoint validates that the received certificate is the same as the Cisco Unified Communications Manager certificate in its truststore.

Supported Cipher Suites for TLS

The vendor endpoint must present three cipher suites to the Call Manager during TLS handshake. These are:

- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_AES128_SHA
- TLS_RSA_WITH_AES256_SHA

Based on the configuration, Cisco Unified Communications Manager will select one of the three cipher suites.

If the device security mode in the configuration indicates Authenticated security mode, and the mode is supported by the endpoint, then the endpoint must only include TLS_RSA_WITH_NULL_SHA in the cipher suite of the Client Hello message.

If the device security mode in the configuration indicates Encrypted security mode, the endpoint device must include TLS_RSA_WITH_AES128_SHA and TLS_RSA_WITH_AES256_SHA in the cipher suite of the Client Hello message. The cipher suite that allows clear text or unauthenticated TLS is not included.

Enabling sRTP Fallback

The sRTP fallback is a proprietary procedure to negotiate sRTP or RTP. The capability should be limited to within the Call Manager environment. The endpoint will only advertise this capability if it is in a Call Manager environment.

The endpoint learns whether the sRTP fallback is enabled during registration. The REGISTER message is sent for each line. The REGISTER message includes the Cisco proprietary x-cisco-sRTP-fallback tag. The tag is not registered with the Internet Assigned Numbers Authority (IANA) and should only be included in the REGISTER message when the device is provisioned in a Cisco environment. If the 200 OK includes the "x-cisco-sRTP-fallback" tag, then sRTP fallback is enabled for that line. If the response does not have the "x-cisco-sRTP-fallback" tag, then RTP fallback is disabled for that line.

The vendor endpoint must only accept enabling or disabling of sRTP fallback when call signaling is secured (TLS authenticated and encrypted). If the call signaling is not secured, the sRTP fallback defaults to disabled. In this case, the endpoint ignores the received x-cisco-sRTP-fallback tag.

Performance Requirements

Vendor endpoints must meet the following performance requirements:

- The vendor endpoint must not take more than 60 seconds to establish TLS session using mutual authentication (both server and client exchange certificate) with 1024 bits RSA public and private key size.
- The vendor endpoint must not cause excessive delay in processing and generating sRTP packets for voice such that the voice quality is degraded with sRTP.

Credentials Creations and Import Model

This section describes the recommended credential creation and management model for vendor endpoints. The details of the setup and provisioning of Cisco Unified Communications Manager and the vendor endpoint are also included.

I. Credentials Import Model Summary:

a. Credentials Issues and Format:

   i. The vendor endpoint Certificate Authority (CA) will issue certificates for vendor endpoints.

   ii. Vendor endpoint CA certificate can be extracted in a supported format, such as PEM, and can be made available for import into the Cisco Unified Communications Manager certificate store. The existing import model of Cisco Unified Communications Manager is expected to work for this process. Cisco Unified Communications Manager 8.5 supports both PEM and DER formats for importing and exporting certificates.

   iii. The certificate issued to the vendor endpoint must contain SEP<MAC address> in the common name (CN).

   The suggested Common Name format for the vendor endpoint is:
   <Product ID><-><SEP><MAC Address>

   Example:
   VendorEP-SEP0123456789A

b. **Credentials Import Model**: In this release, the vendor endpoint does not support the distribution of Cisco Unified Communications Manager certificates through the downloading of the Cisco Certificate Trust List file and the validation of the file. The mechanism to distribute Cisco Unified Communications Manager certificates to all vendor endpoints uses the vendor endpoint provisioning mechanism. Please refer to the vendor endpoint documentation for importing certificates.

II. Cisco Unified Communications Manager Setup and Provisioning:

a. **Setup**:

   i. To support TLS registration and sRTP calls, the Cisco Unified Communications Manager cluster security mode must be set to mixed mode. See the “Configuring the Cisco CTL Client” section in the *Cisco Unified Communications Manager Security Guide* for the steps required to turn on mixed security mode for Cisco Unified Communications Manager. http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/security/8_0_2/secugd/sec-802-cm.html

   ii. The vendor endpoint certificate authority that signs the endpoint device certificates must be imported in the Cisco Unified Communications Manager truststore. Please see the "Security" section in the *Cisco Unified Communications Manager Operating System Administration* Guide for instructions on how to import a certificate into the Cisco Unified Communications Manager truststore.
   http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/cucos/8_0_2/cucos/osg_802_cm.html

b. **Device Provisioning on Cisco Unified Communications Manager**: Within Cisco Unified Communications Manager, each phone or device must be associated with a model-specific security profile. To view the list of available phone security profiles within Cisco Unified Communications Manager, go to **CM Administration System > Security Profile > Phone Security Profile**. For example, the name of the vendor endpoint models is "Generic Desktop Video Endpoint". A security

profile for this vendor endpoint can be created using the "Generic Desktop Video Endpoint" model name. Please note that you may need to select **Add New** to create a new profile.

The following parameters are required to create a security profile that enables a secure connection with Cisco Unified Communications Manager:

- Nonce Validity Time—Can be left at default 600
- Security Mode—Should be set to Encrypted
- Transport Type—Should be set to TLS
- SIP Phone Port—Should be 5061

c. **Vendor Endpoint CA credentials upload to Cisco Unified Communications Manager**: The credentials file should be uploaded to the call-manager and categorized as a trusted certificate. To upload the file:

   i. From the Cisco Unified Operating System Administration window, select **Security > Certificate Management** and then click **Upload Certificate.**

   ii. Enter the following details:

   - Certificate Name—Select **Callmanager-trust**
   - Root Certificate—This field can be left blank
   - Upload File—<file siptcl_ca_cert.pem>

If multiple call-managers are in a cluster configuration, then the credentials file must be applied to all call managers in the cluster.

III. Vendor Endpoint adapter setup and provisioning:

a. **Setup**

   i. Vendor endpoints on the call-manager must be provisioned to support TLS for SIP signaling with Cisco Unified Communications Manager.

   ii. Cisco Unified Communications Manager certificates can be downloaded through **Cisco Unified Operating System Administration > Security > Certificate Management**

   iii. The Cisco Unified Communications Manager certificated import model is provided by the vendor endpoint team.

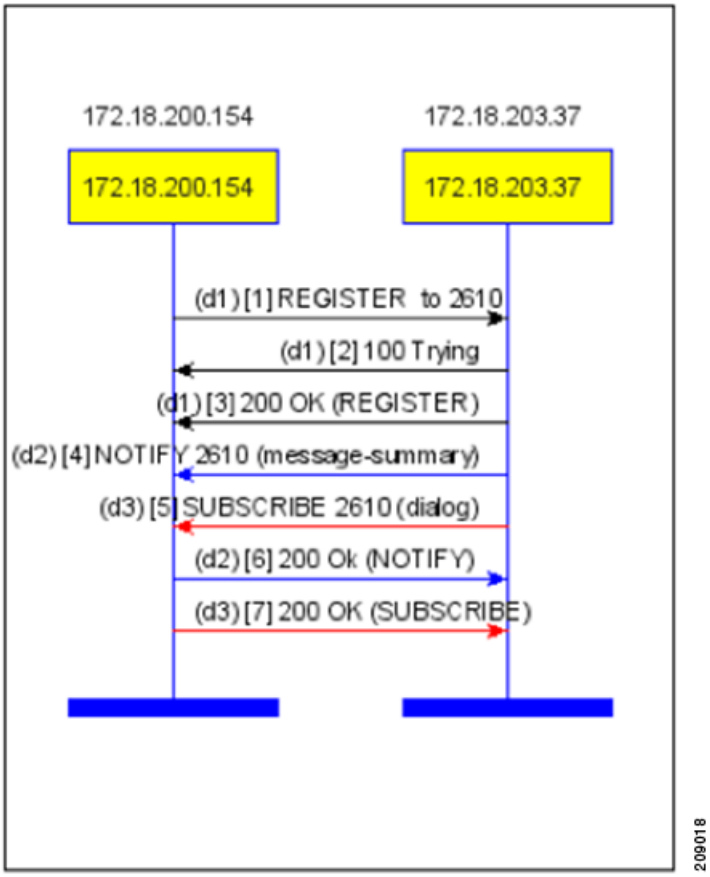
SIP Line Messaging

This section contains sample registration and basic call sequences. These are meant as examples only.

SIP Line Registration

This section contains a sample Registration sequence for the Generic Desktop Video Endpoint with a single line. First, a ladder diagram is shown, followed by sample messages.

Figure 6 Generic Desktop Video Endpoint Registration Sequence



[1] REGISTER sip:172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:31927;branch=z9hG4bK2af-EEEE10000000--1533997190-559
From: <sip:2610@172.18.203.37:5061>;tag=-1533997190
To: <sip:2610@172.18.203.37:5061>
Call-ID: EEEE1000-0000-2610--1533997190
CSeq: 1 REGISTER
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:2610@172.18.200.154:31927;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-EEEE10000000>";+u.sip!model.ccm.cisco.com="588"
Supported: replaces, norefersub, X-cisco-callinfo, X-cisco-srtp-fallback, X-cisco-sis-5.1.0
Expires: 3600
Content-Length: 0

[2] SIP/2.0 100 Trying
Via: SIP/2.0/Tls 172.18.200.154:31927;branch=z9hG4bK2af-EEEE10000000--1533997190-559
From: <sip:2610@172.18.203.37:5061>;tag=-1533997190
To: <sip:2610@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 00:52:38 GMT
Call-ID: EEEE1000-0000-2610--1533997190
CSeq: 1 REGISTER
Content-Length: 0

[3] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:31927;branch=z9hG4bK2af-EEEE10000000--1533997190-559
From: <sip:2610@172.18.203.37:5061>;tag=-1533997190
To: <sip:2610@172.18.203.37:5061>;tag=1083468005
Date: Thu, 02 Dec 2010 00:52:38 GMT
Call-ID: EEEE1000-0000-2610--1533997190
CSeq: 1 REGISTER
Expires: 120
Contact: <sip:2610@172.18.200.154:31927;transport=tls>;+sip.instance=
"<urn:uuid:00000000-0000-0000-0000-EEEE10000000>";+u.sip!model.ccm.cisco.com="588";
x-cisco-newreg
Supported: X-cisco-srtp-fallback,X-cisco-sis-5.1.0
Content-Length: 0

[4] NOTIFY sip:2610@172.18.200.154:31927;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK1a72d59d74e
From: <sip:2610@172.18.203.37>;tag=43248616
To: <sip:2610@172.18.200.154>
Call-ID: 74c42b00-cf61edd7-1a8-25cb12ac@172.18.203.37
CSeq: 101 NOTIFY
Max-Forwards: 70
Date: Thu, 02 Dec 2010 00:52:39 GMT
User-Agent: Cisco-CUCM8.5
Event: message-summary
Subscription-State: active
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Type: application/simple-message-summary
Content-Length: 22
Messages-Waiting: no

[5] SUBSCRIBE sip:2610@172.18.200.154:31927 SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK1a839e7f451
From: <sip:2610@172.18.203.37>;tag=865518321
To: <sip:2610@172.18.200.154>
Call-ID: 74c42b00-cf61edd7-1a9-25cb12ac@172.18.203.37
CSeq: 101 SUBSCRIBE
Date: Thu, 02 Dec 2010 00:52:39 GMT
User-Agent: Cisco-CUCM8.5
Event: dialog
Expires: 23489
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Accept: application/dialog-info+xml
Max-Forwards: 69
Content-Length: 0

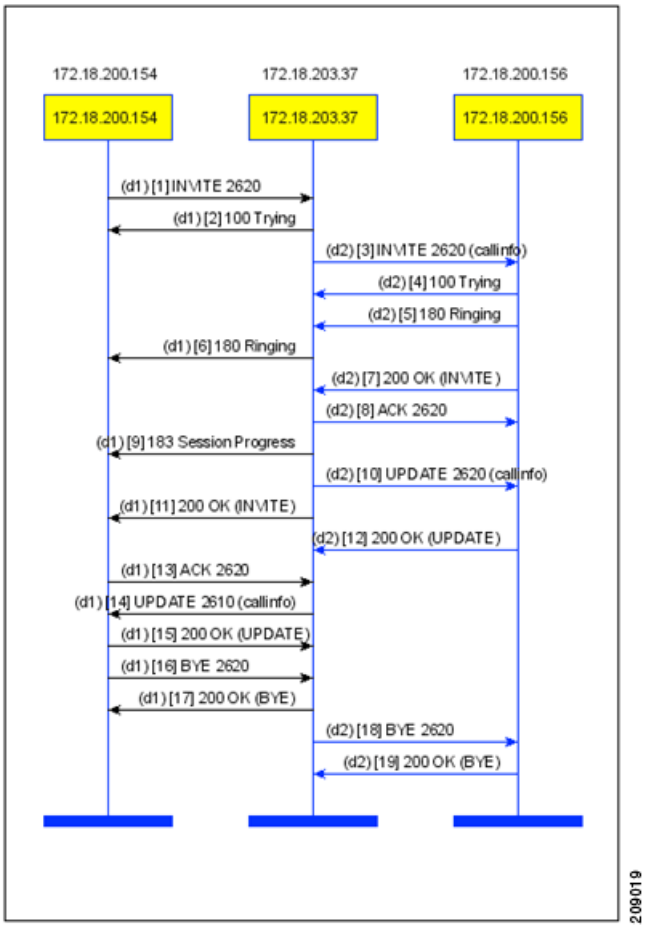
[6] SIP/2.0 200 Ok
Contact: <sip:2610@172.18.200.154:31927;transport=tls>
Call-ID: 74c42b00-cf61edd7-1a8-25cb12ac@172.18.203.37
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK1a72d59d74e
From: <sip:2610@172.18.203.37>;tag=43248616
To: <sip:2610@172.18.200.154>
CSeq: 101 NOTIFY
Event: message-summary
Subscription-State: active
Content-Length: 0

[7] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK1a839e7f451
From: <sip:2610@172.18.203.37>;tag=865518321
To: <sip:2610@172.18.200.154>;tag=12345
Call-ID: 74c42b00-cf61edd7-1a9-25cb12ac@172.18.203.37
CSeq: 101 SUBSCRIBE
Content-Length: 0

SIP Line Basic Call – Example 1

This section contains a sample basic call between a GDVE and GSSRS endpoint. The signaling path is secured via TLS and both Audio and Video are secure via sRTP. Both endpoints advertise SAVP audio and video in this scenario.

Figure 7 Sample GDVE to GSSRS Call with Secure Audio and Video



[1] INVITE sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522253838-460
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 INVITE
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:2610@172.18.200.154:32160;transport=tls>
Expires: 1800
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,SUBSCRIBE,INFO,UPDATE
Allow-Events: kpml
Recv-Info: x-cisco-conference
Content-Length: 995
Content-Type: application/sdp

Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.154
s=SIP Call
c=IN IP4 172.18.200.154
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
m=video 49276 RTP/SAVP 109 96 34
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800d; max-mbps=108000; max-fs=3600; max-br=1600; sar=13
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF4=2;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,2
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=2;CIF=1;QCIF=1;SQCIF=1
a=sendrecv
a=rtcp-fb:* ccm fir tmmbr

[2] SIP/2.0 100 Trying
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522253838-460
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 INVITE
Allow-Events: presence
Content-Length: 0

[3] INVITE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36529ab35dd
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
Supported: timer,resource-priority,replaces
Min-SE: 180
User-Agent: Cisco-CUCM8.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 101 INVITE
Expires: 180
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= from; gci= 1-162120; call-instance= 1
Send-Info: conference, x-cisco-conference
Alert-Info: <file://Bellcore-dr1/>
Remote-Party-ID: <sip:2610@172.18.203.37;x-cisco-callback-number=2610>;party=calling;screen=yes; privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>;video;audio
Max-Forwards: 69
Content-Length: 0

[4] SIP/2.0 100 Trying
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36529ab35dd
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Content-Length: 0
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE

[5] SIP/2.0 180 Ringing
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36529ab35dd
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow-Events: kpml,dialog
Content-Length: 0

[6] SIP/2.0 180 Ringing
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522253838-460
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Allow-Events: presence

```
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-state= ringout;
gci= 1-162120; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Length: 0


[7] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36529ab35dd
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Recv-Info: x-cisco-conference
Content-Length: 995
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.156
s=SIP Call
c=IN IP4 172.18.200.156
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
m=video 45333 RTP/SAVP 109 96 34
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800d; max-mbps=108000; max-fs=3600; max-br=1600; sar=13
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF4=2;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,2
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=2;CIF=1;QCIF=1;SQCIF=1
a=sendrecv
a=rtcp-fb:* ccm fir tmmbr
```

```
[8] ACK sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3661201f2f
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: presence
Content-Type: application/sdp
Content-Length: 568

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.154
t=0 0
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 49276 RTP/SAVP 109
b=TIAS:1288000
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr


[9] SIP/2.0 183 Session Progress
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522253838-460
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-state= ringout;
gci= 1-162120; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 568

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.156
t=0 0
```

```
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 45333 RTP/SAVP 109
b=TIAS:1288000
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr


[10] UPDATE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36724105e7
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 102 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Encrypted; orientation= from; gci= 1-162120;
call-instance= 1
Remote-Party-ID: <sip:2610@172.18.203.37>;party=calling;screen=yes;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0

[11] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522253838-460
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Supported: replaces
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; gci= 1-162120;
call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 568

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.156
t=0 0
```

```
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 45333 RTP/SAVP 109
b=TIAS:1288000
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr


[12] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK36724105e7
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
CSeq: 102 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0


[13] ACK sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522252780-379
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Call-ID: EEEE1000-0000-2610--1522253841
Max-Forwards: 70
Cseq: 101 ACK
User-Agent: SIPGenericDesktopVideoEndpoint
Content-Length: 0


[14] UPDATE sip:2610@172.18.200.154:32160;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK368207ac2f
From: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
Date: Thu, 02 Dec 2010 04:08:23 GMT
Call-ID: EEEE1000-0000-2610--1522253841
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 101 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Encrypted; orientation= to; gci= 1-162120;
call-instance= 1
Remote-Party-ID: <sip:2620@172.18.203.37>;party=calling;screen=no;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0
```

[15] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK368207ac2f
From: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 101 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

[16] BYE sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522249271-750
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Call-ID: EEEE1000-0000-2610--1522253841
Max-Forwards: 70
CSeq: 102 BYE
User-Agent: SIPGenericDesktopVideoEndpoint
Content-Length: 0

[17] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1522249271-750
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1522253839
To: <sip:2620@172.18.203.37:5061>;tag=24153~2bce9a1f-f610-4257-96e5-671d1f847dac-30785299
Date: Thu, 02 Dec 2010 04:08:26 GMT
Call-ID: EEEE1000-0000-2610--1522253841
CSeq: 102 BYE
Content-Length: 0

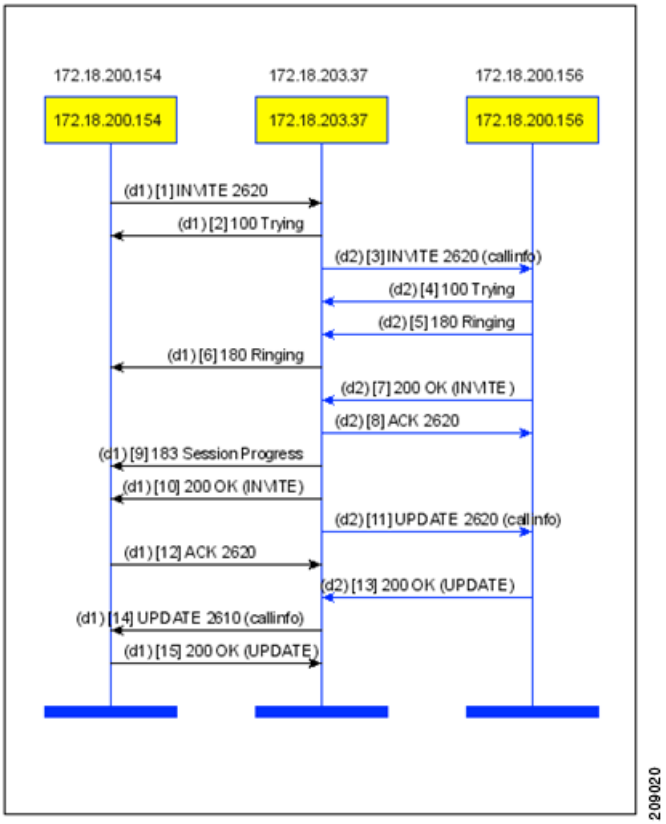
[18] BYE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3695093d61a
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Date: Thu, 02 Dec 2010 04:08:22 GMT
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
CSeq: 103 BYE
Content-Length: 0

[19] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3695093d61a
From: <sip:2610@172.18.203.37>;tag=24154~2bce9a1f-f610-4257-96e5-671d1f847dac-30785300
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1522253812
Call-ID: cc23c480-cf711bb6-362-25cb12ac@172.18.203.37
CSeq: 103 BYE
Content-Length: 0

SIP Line Basic Call – Example 2

This section contains a sample basic call between GDVE and GSSRS endpoints. The signaling path is secured via TLS. In this scenario, one endpoint advertises SAVP audio SDP only and the other advertises SAVP audio/video SDP. In this scenario, only audio is negotiated.

Figure 8 Sample GDVE to GSSRS Call with Secure Audio



[1] INVITE sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520583303-274
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 INVITE
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:2610@172.18.200.154:32160;transport=tls>
Expires: 1800
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,SUBSCRIBE,INFO,UPDATE
Allow-Events: kpml
Recv-Info: x-cisco-conference
Content-Length: 995
Content-Type: application/sdp
Content-Disposition: session;handling=optional

```
v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.154
s=SIP Call
c=IN IP4 172.18.200.154
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
m=video 49276 RTP/SAVP 109 96 34
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800d; max-mbps=108000; max-fs=3600; max-br=1600; sar=13
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF4=2;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,2
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=2;CIF=1;QCIF=1;SQCIF=1
a=sendrecv
a=rtcp-fb:* ccm fir tmmbr


[2] SIP/2.0 100 Trying
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520583303-274
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 INVITE
Allow-Events: presence
Content-Length: 0


[3] INVITE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK374451cc29d
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
Supported: timer,resource-priority,replaces
Min-SE:  180
User-Agent: Cisco-CUCM8.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
```

CSeq: 101 INVITE
Expires: 180
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= from;
gci= 1-162121; call-instance= 1
Send-Info: conference, x-cisco-conference
Alert-Info: <file://Bellcore-dr1/>
Remote-Party-ID: <sip:2610@172.18.203.37;x-cisco-callback-number=2610>;party=calling;screen=
yes;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>;video;audio
Max-Forwards: 69
Content-Length: 0

[4] SIP/2.0 100 Trying
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK374451cc29d
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Content-Length: 0
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE

[5] SIP/2.0 180 Ringing
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK374451cc29d
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1520583286
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow-Events: kpml,dialog
Content-Length: 0

[6] SIP/2.0 180 Ringing
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520583303-274
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-
state= ringout; gci= 1-162121; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Length: 0

```
[7] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK374451cc29d
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1520583286
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Recv-Info: x-cisco-conference
Content-Length: 545
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.156
s=SIP Call
c=IN IP4 172.18.200.156
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
```

```
[8] ACK sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3754e75a0e5
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1520583286
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: presence
Content-Type: application/sdp
Content-Length: 300

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.154
t=0 0
m=audio 16007 RTP/SAVP 9 119
```

```
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15


[9] SIP/2.0 183 Session Progress
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520583303-274
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-state= ringout;
gci= 1-162121; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 583

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
t=0 0
m=audio 16007 RTP/SAVP 9 119
c=IN IP4 172.18.200.156
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 0 RTP/AVP 31 34 96 97
c=IN IP4 0.0.0.0
a=rtpmap:31 H261/90000
a=fmtp:31 MAXBR=128
a=rtpmap:34 H263-1998/90000
a=fmtp:34 SQCIF=1;QCIF=1;CIF=1;CIF4=2;CUSTOM=704,480,2
a=rtpmap:96 H263-1998/90000
a=fmtp:96 SQCIF=1;QCIF=1;CIF=1;CIF4=2
a=rtpmap:97 H264/90000
a=inactive


[10] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520583303-274
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 INVITE
```

```
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Supported: replaces
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to;
gci= 1-162121; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 583

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
t=0 0
m=audio 16007 RTP/SAVP 9 119
c=IN IP4 172.18.200.156
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 0 RTP/AVP 31 34 96 97
c=IN IP4 0.0.0.0
a=rtpmap:31 H261/90000
a=fmtp:31 MAXBR=128
a=rtpmap:34 H263-1998/90000
a=fmtp:34 SQCIF=1;QCIF=1;CIF=1;CIF4=2;CUSTOM=704,480,2
a=rtpmap:96 H263-1998/90000
a=fmtp:96 SQCIF=1;QCIF=1;CIF=1;CIF4=2
a=rtpmap:97 H264/90000
a=inactive


[11] UPDATE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37611163f9a
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1520583286
Date: Thu, 02 Dec 2010 04:36:12 GMT
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 102 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Encrypted; orientation= from;
gci= 1-162121; call-instance= 1
Remote-Party-ID: <sip:2610@172.18.203.37>;party=calling;screen=yes;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0
```

[12] ACK sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1520582265-27
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
To: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
Call-ID: EEEE1000-0000-2610--1520583306
Max-Forwards: 70
Cseq: 101 ACK
User-Agent: SIPGenericDesktopVideoEndpoint
Content-Length: 0

[13] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37611163f9a
From: <sip:2610@172.18.203.37>;tag=24312~2bce9a1f-f610-4257-96e5-671d1f847dac-30785302
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1520583286
Call-ID: af898b80-cf71223c-36d-25cb12ac@172.18.203.37
CSeq: 102 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

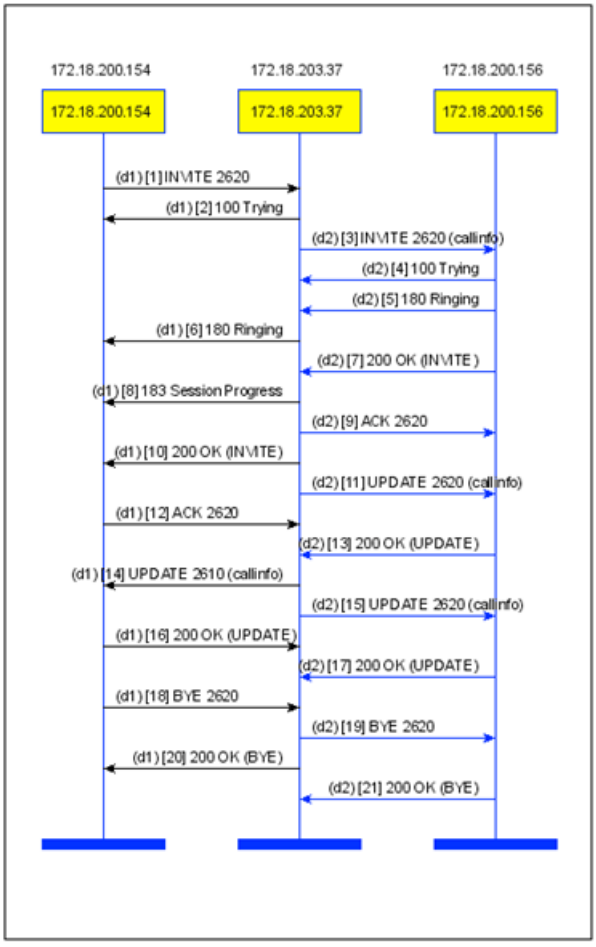
[14] UPDATE sip:2610@172.18.200.154:32160;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37776748be7
From: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
Date: Thu, 02 Dec 2010 04:36:13 GMT
Call-ID: EEEE1000-0000-2610--1520583306
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 101 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Encrypted; orientation= to;
gci= 1-162121; call-instance= 1
Remote-Party-ID: <sip:2620@172.18.203.37>;party=calling;screen=no;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0

[15] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37776748be7
From: <sip:2620@172.18.203.37:5061>;tag=24311~2bce9a1f-f610-4257-96e5-671d1f847dac-30785301
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1520583304
Call-ID: EEEE1000-0000-2610--1520583306
CSeq: 101 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

SIP Line Basic Call – Example 3

This section contains a sample basic call between and GDVE and GSSRS endpoints. The signaling path is secured via TLS. In this scenario, one endpoint advertises SAVP audio/video SDP and the other endpoint advertises SAVP audio and AVP video SDP. SAVP audio is negotiated, but only AVP video can be negotiated. This call is not secure because the media are not fully secure.

Figure 9 Sample GDVE to GSSRS call with Secure Audio and Nonsecure Video



[1] INVITE sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519369827-697
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 INVITE
User-Agent: SIPGenericDesktopVideoEndpoint
Contact: <sip:2610@172.18.200.154:32160;transport=tls>
Expires: 1800
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,SUBSCRIBE,INFO,UPDATE
Allow-Events: kpml
Recv-Info: x-cisco-conference

```
Content-Length: 995
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.154
s=SIP Call
c=IN IP4 172.18.200.154
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
m=video 49276 RTP/SAVP 109 96 34
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800d; max-mbps=108000; max-fs=3600; max-br=1600; sar=13
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF4=2;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,2
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=2;CIF=1;QCIF=1;SQCIF=1
a=sendrecv
a=rtcp-fb:* ccm fir tmmbr
```

```
[2] SIP/2.0 100 Trying
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519369827-697
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 INVITE
Allow-Events: presence
Content-Length: 0
```

```
[3] INVITE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37eb92f39c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
Supported: timer,resource-priority,replaces
```

Min-SE: 180
User-Agent: Cisco-CUCM8.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 101 INVITE
Expires: 180
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= from; gci= 1-162123; call-instance= 1
Send-Info: conference, x-cisco-conference
Alert-Info: <file://Bellcore-dr1/>
Remote-Party-ID: <sip:2610@172.18.203.37;x-cisco-callback-number=2610>;party=calling;screen=yes;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>;video;audio
Max-Forwards: 69
Content-Length: 0

[4] SIP/2.0 100 Trying
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37eb92f39c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Content-Length: 0
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE

[5] SIP/2.0 180 Ringing
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37eb92f39c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow-Events: kpml,dialog
Content-Length: 0

[6] SIP/2.0 180 Ringing
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519369827-697
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-state= ringout; gci= 1-162123; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Length: 0

```
[7] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37eb92f39c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 101 INVITE
Server: SIPGenericRoomSystemSS
Contact: <sip:2620@172.18.200.156:56042;transport=tls>
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Recv-Info: x-cisco-conference
Content-Length: 910
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 1129149157 0 IN IP4 172.18.200.156
s=SIP Call
c=IN IP4 172.18.200.156
b=AS:1288
t=0 0
m=audio 16007 RTP/SAVP 115 102 9 15 0 8 18 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX
a=rtpmap:115 G7221/32000
a=fmtp:115 bitrate=48000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
a=sendrecv
m=video 45333 RTP/AVP 109 96 34
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800d; max-mbps=108000; max-fs=3600; max-br=1600; sar=13
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF4=2;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,2
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=2;CIF=1;QCIF=1;SQCIF=1
a=sendrecv
a=rtcp-fb:* ccm fir tmmbr
```

```
[8] SIP/2.0 183 Session Progress
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519369827-697
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
```

```
Allow-Events: presence
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; ui-state= ringout; gci= 1-162123; call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 483

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.156
t=0 0
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 45333 RTP/AVP 109
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr


[9] ACK sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK37fc1c45b1
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: presence
Content-Type: application/sdp
Content-Length: 483

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.154
t=0 0
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 49276 RTP/AVP 109
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr
```

```
[10] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519369827-697
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
Allow-Events: presence
Supported: replaces
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; gci= 1-162123;
call-instance= 1
Send-Info: conference, x-cisco-conference
Remote-Party-ID: <sip:2620@172.18.203.37>;party=called;screen=no;privacy=off
Contact: <sip:2620@172.18.203.37:5061;transport=tls>
Content-Type: application/sdp
Content-Length: 483

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 172.18.203.37
s=SIP Call
c=IN IP4 172.18.200.156
t=0 0
m=audio 16007 RTP/SAVP 9 119
a=crypto:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX
a=rtpmap:9 G722/8000
a=ptime:20
a=rtpmap:119 telephone-event/8000
a=fmtp:119 0-15
m=video 45333 RTP/AVP 109
b=TIAS:1288000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800D;max-mbps=108000;max-fs=3600;max-cpb=64;max-br=1600
a=rtcp-fb:*  ccm fir tmmbr


[11] UPDATE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3803a80c261
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 102 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Encrypted; orientation= from; gci= 1-162123;
call-instance= 1
Remote-Party-ID: <sip:2610@172.18.203.37>;party=calling;screen=yes;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0
```

[12] ACK sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519368781-961
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Call-ID: EEEE1000-0000-2610--1519369830
Max-Forwards: 70
Cseq: 101 ACK
User-Agent: SIPGenericDesktopVideoEndpoint
Content-Length: 0

[13] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3803a80c261
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 102 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

[14] UPDATE sip:2610@172.18.200.154:32160;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3812449b5e2
From: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
Date: Thu, 02 Dec 2010 04:56:27 GMT
Call-ID: EEEE1000-0000-2610--1519369830
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 101 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Authenticated; orientation= to; gci= 1-162123;
call-instance= 1
Remote-Party-ID: <sip:2620@172.18.203.37>;party=calling;screen=no;privacy=off
Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0

[15] UPDATE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK38233556b2c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
Supported: timer,resource-priority,replaces
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY
CSeq: 103 UPDATE
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= Authenticated; orientation= from; gci= 1-162123;
call-instance= 1
Remote-Party-ID: <sip:2610@172.18.203.37>;party=calling;screen=yes;privacy=off

Contact: <sip:2610@172.18.203.37:5061;transport=tls>
Content-Length: 0

[16] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK3812449b5e2
From: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
To: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 101 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

[17] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK38233556b2c
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 103 UPDATE
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml
Supported: replaces
Content-Length: 0

[18] BYE sip:2620@172.18.203.37:5061 SIP/2.0
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519364594-727
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Call-ID: EEEE1000-0000-2610--1519369830
Max-Forwards: 70
CSeq: 102 BYE
User-Agent: SIPGenericDesktopVideoEndpoint
Content-Length: 0

[19] BYE sip:2620@172.18.200.156:56042;transport=tls SIP/2.0
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK383d9249c1
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Date: Thu, 02 Dec 2010 04:56:26 GMT
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
User-Agent: Cisco-CUCM8.5
Max-Forwards: 70
CSeq: 104 BYE
Content-Length: 0

```
[20] SIP/2.0 200 OK
Via: SIP/2.0/Tls 172.18.200.154:32160;branch=z9hG4bK2af-EEEE10000000--1519364594-727
From: "display name" <sip:2610@172.18.200.154>;tag=EEEE10000000-1519369828
To: <sip:2620@172.18.203.37:5061>;tag=24416~2bce9a1f-f610-4257-96e5-671d1f847dac-30785305
Date: Thu, 02 Dec 2010 04:56:31 GMT
Call-ID: EEEE1000-0000-2610--1519369830
CSeq: 102 BYE
Content-Length: 0
```

```
[21] SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.18.203.37:5061;branch=z9hG4bK383d9249c1
From: <sip:2610@172.18.203.37>;tag=24417~2bce9a1f-f610-4257-96e5-671d1f847dac-30785306
To: <sip:2620@172.18.203.37:5061>;tag=EEEE10000001-1519369811
Call-ID: 83233e80-cf7126fa-36f-25cb12ac@172.18.203.37
CSeq: 104 BYE
Content-Length: 0
```

Constraint Requirements

Provisioning of a vendor endpoint device must be performed using the endpoint provisioning tool and the device must be configured on Cisco Unified Communications Manager.

If the endpoint does not support Cisco Unified Communications Manager failover/fallback, the call cannot be made with endpoint devices when the configured Cisco Unified Communications Manager fails even if there is more than one Cisco Unified Communications Manager in a cluster.

Distributing vendor endpoints among Cisco Unified Communications Manager clusters must be done manually or with a separate tool because the endpoint configurations are not obtained from the Cisco Unified Communications Manager generated configuration file.

Endpoint Specifications

Specifications for vendor endpoints are not be captured in this document. The device is developed by the Vendor, which maintains its own design documents.

Requirements Traceability Considerations

Not Applicable

References

Cisco Unified Communications Manager Security Guide

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/security/8_0_2/secugd/sec-802-cm.html

Cisco Unified Communications Operating System Administration Guide

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/cucos/8_0_2/cucos/osg_802_cm.html

Glossary

Word	Definition
CAPF	Certificate Authority Proxy Function
CUCM	Cisco Unified Communications Manager
EP	Vendor Endpoint
GDVE	Generic Desktop Video Endpoint
GSSRS	Generic Single Screen Room System
GMSRS	Generic Multi Screen Room System
RTP	Real-Time Transport Protocol
RTP/AVP	Real-time Transport Protocol using Audio Video Profile
RTP/SAVP	Real-time Transport Protocol using Secure Audio Video Profile
SDP	Session Description Protocol
SHA-1	Secure Hash Algorithm Revision 1, a cryptographic hash algorithm designed by NIST and NSA. It generated a 160-bit digest.
SIP	Session Initiation Protocol
sRTP	Secure Real Time Transport Protocol. Secure RTP (draft-ietf-avt-sRTP-04.txt) defines a protection mechanism to provide integrity and/or confidentiality of media stream traffic.
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security Protocol. This is a suite of related protocols that provide security at just below the applications layer. TLS is defined in RFC-2246
UDP	User Datagram Protocol