# Cisco Remote Expert Mobile Feature Guide, Release 11.6 (1)

**First Published:** August 2017

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# Contents

# Preface



## Change History

This table lists the major changes made to this guide. The most recent changes appear at the top.

| Changes | Section | Date |
|---|---|---|
| Initial release of document for Release 11.6(1) | | Aug 2017 |
| Aspect Ration Mismatches section rewritten for clarity | **Aspect Ratio Mismatches on page 7** | |
| Single stylesheet for all documents. Spelling and punctuation corrections. | Throughout | |

## About this Guide

This guide describes the features in Cisco Remote Expert Mobile.

This guide assumes that you are familiar with basic contact center and unified communications terms and concepts.

# Audience

The primary audience for this guide is people who need to understand what features of Remote Expert Mobile are available.

# Related Documents

Consult these documents for details of these subjects that are not covered in this guide.

| Subject | Link |
|---|---|
| *Compatibility Matrix* for information on which versions of which products are supported for a contact center enterprise solution. | https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html |
| *Cisco Unified Contact Center Enterprise Features Guide* for detailed information on the configuration and administration of integrated features in your solution. | http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html |
| *Cisco Collaboration Systems Solution Reference Network Designs* for detailed information on the Unified Communications infrastructure on which your solution is built. | http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html |

You can find the full documentation of each of the components in the Unified CCE solution at these sites:

| Component | Link |
|---|---|
| Cisco Unified Contact Center Enterprise | http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html |
| Cisco Finesse | http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html |
| Cisco MediaSense | http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html |
| Cisco SocialMiner | http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/tsd-products-support-series-home.html |
| Cisco Unified Customer Voice Portal | http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html |
| Cisco Unified Intelligence Center | http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html |
| Cisco Virtualized Voice Browser | http://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-series-home.html |

# Organization of this Guide

The guide includes the following sections:

| | |
|---|---|
| **Introduction** | Introduction and brief overview of Remote Expert Mobile feature and its SDKs and key technologies. |
| **Media Features** | Describes the details of codec and transcoding in RE Mobile |
| **Expert Assist Features** | Describes the major features as part of Expert Assist: co-browse, native mobile app share, doc push, remote control and annotation |
| **SDK Features** | Describes the details of the CSDK as well as browser and mobile OS support |
| **WebRTC Signaling** | Describes the details of WebRTC from CSDK applications to RE Mobile servers (REAS and REMB) |
| **SIP Features** | Describes the details of RE Mobile integration to UC environments inside the enterprise |
| **Encryption** | Describes the details of secure communications in Remote Expert Mobile |
| **High Availability** | Describes the HA features of RE Mobile |
| **RE Mobile Administration** | Highlights the use of the RE Mobile web administration console for REAS, REMB and Expert Assist as well as session monitoring and SNMP |
| **Acronym List** | Lists some common industry and Cisco specific acronyms relevant to Remote Expert Mobile. |

# Obtaining Documentation and Submitting a Service Request

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

# Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at http://www.cisco.com/cisco/support/notifications.html.

# Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com.

We appreciate your comments.

# Conventions

This document uses the following conventions:

| Convention | Indication |
|---|---|
| **boldface** font | Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:<br>■ Choose Edit > Find.<br>■ Click Finish. |
| *italic* font | Italic font is used to indicate the following:<br>■ To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills.<br>■ A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*)<br>■ A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*. |
| [ ] | Elements in square brackets are optional. |
| { x \| y \| z } | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [ x \| y \| z ] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A non-quoted sequence of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| `window font` | Window font, such as Courier, is used for the following:<br>■ Text as it appears in code or that the window displays. Example:<br>`<html><title>Cisco Systems, Inc. </title></html>` |
| < > | Angle brackets are used to indicate the following:<br>• For arguments where the context does not allow italic, such as ASCII output.<br>• A character string that the user enters but that does not appear on the window such as a password. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

CHAPTER 1

# Introduction



Cisco Remote Expert Mobile is a software solution that enables personal and actionable customer interactions within mobile and web applications. These interactions range from simple click-to call to a “mayday” like experience interconnected to a full contact center environment. For example, Cisco Remote Expert Mobile can connect individual investors to the next available financial adviser within a mobile trading app (B2C—Business to Consumer) or a field employee’s mobile app routing into an internal helpdesk (B2E—Business to Employee).

## Features

With Cisco Remote Expert Mobile developers can deliver voice, video and Expert Assist co-browse and application sharing in mobile or web applications. Cisco Remote Expert Mobile is designed specifically for remote collaboration services provided through Cisco Unified Communications Manager, Cisco Unified Contact Center Enterprise (Unified CCE) and / or Cisco Unified Contact Center Express (Unified CCX). Remote Expert Mobile offers the following features and options that are pre-sized within core components. Core component features are:

- In-app voice and video communications (Over-the-Top WebRTC communications)
  - High definition video and audio
  - Bi-directional or one-way video
  - Mute audio, video or both
  - Client side call control
- WebRTC to SIP gateway (trunking into Cisco Unified Border Element and Unified Communications Manager)
- Expert Assist
  - Web Co-browse
  - Mobile app sharing
  - Remote app control

  - Agent form editing and completion
  - Annotation by agent
  - Agent document push
  - Agent URL sharing
  - Protect sensitive data with foeld and data masking
- Media Features
  - Media encryption / decryption
  - Bidirectional audio
  - High definition video (H.264 or VP8 in CIF (325x288), nHD (640x360), VGA (640x480), 720p (1280x720)
  - High definition and narrowband audio codec support (Opus, G.711 ulaw or G.711 alaw)
  - Opus, G.711 ulaw, G.711 alaw and G729.a audio transcoding into the enterprise network
  - H.264 and VP8 video transcoding
  - STUN server for client external IP identification
    STUN Agent and Client (RFC 5389) for client external IP identification

**Note** Although REM acts as both STUN server (when receiving requests and sending responses), and as STUN client (when sending requests and receiving responses), REM does not act as a regular STUN resolution server.

  - UDP port multiplexing

# SDKs

Cisco Remote Expert Mobile includes Software Development Kits (SDKs) to provide voice over IP, video over IP and Expert Assist (app share and web co-browse, annotation and document push) features within pre-existing mobile and web applications. Whether placing or receiving calls, Cisco Remote Expert Mobile supports web application in every major browser such as: Google Chrome, Mozilla Firefox, Opera, Internet Explorer and Apple Safari. With WebRTC at its core, in-app communications are enabled without the need for plugins. Where WebRTC is yet to be supported in Internet Explorer and Safari, WebRTC plug-ins are provided for voice and video. Cisco Remote Expert Mobile also delivers integrated communications in iOS 7+ and Android 4.1.2+ apps through native libraries.

CHAPTER 2

# Media Features



Remote Expert Mobile uses WebRTC to give developers easy access to high-quality, real-time communications technology over Wi-Fi, the Internet or varied enterprise networks. Before WebRTC, this type of technology has only been available to large corporations who can afford the expensive licensing fees or through proprietary plug-ins and cumbersome downloads like Adobe Flash.

Note

*Codecs* ("coder-decoder") are software and algorithms that handle the encoding and decoding of audio and video. Currently two video codecs dominate the communications industry for video conferencing: H.264 and VP8. Both video technologies support high-definition real-time communications and power services such as Apple's FaceTime and Google Hangouts.

**Over-the-top audio and video**

Remote Expert Mobile supports a variety of codecs for amazing voice and video quality from client applications to RE Mobile servers:

— Secure Over-the-top Audio: G.711, Opus
— Secure Over-the-top Video: H.264 (up to 720p, 30 fps) and VP8 (up to 720p, 30 fps)

## Voice

**G.711**—G.711 is a narrowband audio codec that provides toll-quality audio at 64 kbit/s used widely throughout telephony networks.

**Opus**—The Opus audio codec provides both narrowband and HD quality voice that performs well over the Internet and unmanaged networks.

**WebRTC** includes some of the most advanced video and audio compression technologies with minimal bandwidth footprint, packet loss concealment and variable bitrates built-in Opus builds upon elements of Skype's SILK codec to ensure unmatched performance over the Internet.

**G.729a (transcoding only)**—G.729a is a highly compress audio codec used for VoIP that utilizes little computational power at the cost of reduced speech quality (Sampling frequency 8 kHz/16) at a fixed bit rate (8 kbit/s 10 ms frames). G.729 is only supported on the enterprise network and is transcoded from either the G.711 or Opus codecs.

# Video

## Key video concepts

**Resolution**—the picture quality affiliated with video. Most people are familiar with standard definition and high-definition (for example, 720p or 1080p) television. HD and resolution also apply to video conferencing where more lines of resolution result in a clearer image. Depending on the number of participants, common video conferencing resolutions range from VGA to 720p.

**Frame Rate**—the number of still images, or frames, that are displayed in one second of video. Frame rate is measured in "Frames Per Second", or "fps". Common video conferencing frame rates include: 15 fps, 20 fps and 30 fps. Higher frame rates produce a smooth video but use more bandwidth, while lower frame rates may cause choppier video.

**Bitrate**—the amount of data being sent between two parties. More specifically, bitrate is quantified in bits per second (for example, kbps, or Mbps). With a higher bitrate assigned to a media steam, more audio and video information can pass between two parties. Available network bandwidth has a dramatic impact on bitrate.

## Video codec support

Remote Expert mobile supports both the H.264 and VP8 video codecs (depending on browser or mobile implementation) up to 720p, as well as transcoding between the two codecs.

### H.264

H.264 is the dominant video compression technology, or codec, in industry; it was developed by the International Telecommunications Union (as H.264 and MPEG-4 Part 10, Advanced Video Coding or AVC).

### VP8

VP8 is a video compression format owned by Google. Google bought the company that created it and then released VP8 software under a BSD-like license as well as the VP8 bitstream specification under an irrevocable license and free of royalties. VP8 is roughly equivalent in processor usage, bandwidth and quality as H.264.

# Transcoding

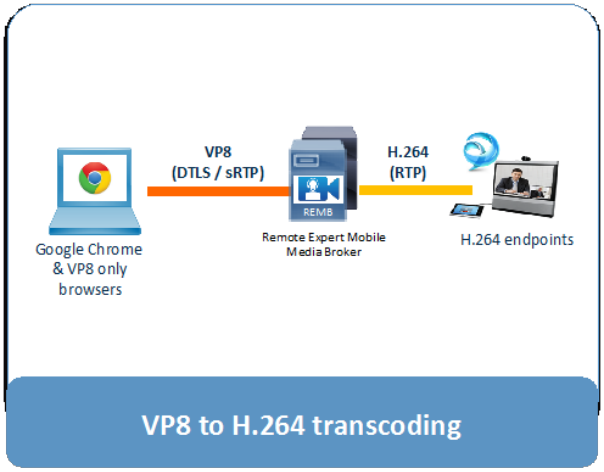
Transcoding in the REMB is used when two audio or video codecs differ and must be converted between media types (for example, VP8 to H.264 video or Opus to G.711 audio).

## Audio transcoding

Remote Expert Mobile provides audio transcoding to ensure compatibility and compliance recording between advanced CODECs in the CSDK such as Opus that perform well over the Internet and unmanaged networks and standard UC audio codec like G.711 or G.729a that prevail in enterprise VoIP networks.

- Opus to G.729a
- Opus to G.711
- G.711 to G.729a

**Figure 1:**




## Video transcoding

- VP8 to H.264—Media Broker can transcode between VP8 and H.264 when required. This guarantees compatibility between WebRTC endpoints that tend to favor VP8 and immersive, desktop and traditional video endpoints that favor H.264.

## Minimizing transcoding with dual H.264 and VP8 support

As transcoding is an intensive process, Remote Expert Mobile offers both H.264 native support and VP8 support in the mobile SDKs. With up to 70% of calls from mobiles, dual-codec support minimizes transcoding.

# WebRTC—state of the art media quality

With WebRTC at the core, Remote Expert Mobile benefits from 20+ years of VoIP technology built into the standard and embedded technologies. By leveraging WebRTC, Mobile Advisor delivers superior audio and video quality from mobile apps and browsers into the enterprise.

## Dynamic jitter buffers

WebRTC includes a dynamic jitter buffer as well as an advanced error concealment algorithm for hiding the effects of impaired network connections exhibiting network jitter and packet loss. By buffering the minimum amount of media, this feature keeps latency low while maintaining the highest voice and video quality.

## Acoustic Echo Canceler (AEC)

WebRTC's Acoustic Echo Canceler is an advanced software-based signal-processing component that removes echo resulting from the voice being played out from the active microphone.

## Noise reduction

Another software-based signal processing element removes background noise associated with Voice-over-IP such as hiss, fan noise, and more.

## Video quality

Remote Expert Mobile includes an impressive amount of functionality to ensure the best video and audio quality. When incorporating video and audio into an app, communications are likely going over Wi-Fi, the Internet or 4G data in network conditions that are beyond control. RE Mobile incorporates many technologies to ensure that every call is of utmost quality: voice-only, one-way video, or two-way video.

# Adjustment of resolution and frame rate (under changing network conditions)

Remote Expert Mobile can adjust the bandwidth footprint via negotiation resolution and frame rates (see below). Remote Expert Mobile APIs give a clear feedback of network quality to an app. In turn, developers can control resolution, frame rate or even go to audio only under a variety of conditions when conditions change.

| Video Resolution | Video Format (Aspect) | Quality | Typical Bandwidth |
|---|---|---|---|
| 352 x 288 | CIF (4:3) | Standard Definition (SD) | 256 kbps - 511 kbps |
| 640 x 360 | nHD (16:9) | SD | 480 kbps – 980 kbps |
| 640 x 480 | VGA (4:3) | SD | 512 kbps – 1023 kbps |
| 1280 x 720 | 720p (16:9) | High Definition (HD) | 1024 kbps - 1920 kbps |

Default resolutions and frame rates may be altered via the web administration console (`https://<your_server>:8443/web_plugin_framework/webcontroller/assist/`) or via the Command Line Interface. In the web administration console, please refer to the Media Configuration tab to alter the default resolution and frame rates.

The default frame rate for a resolution cannot be guaranteed with the variety of WebRTC endpoints available. For example, even with 30 frames-per-second set as the default frame rate in the RE Mobile Web Admin or CLI, Google Chrome may commonly only provide video frames at 22 – 30 frames per second based on network conditions.

This feature allows Media Broker to manage the resolution of all transcoded video streams that it processes. This is beneficial if there are many types of client, all running at different resolutions, but only a single resolution is necessary for communications. Limiting the resolution and bitrate is a good way of managing the quality of high traffic video networks.

# Negative Acknowledgment (NACK) and Picture Loss Indication (PLI)

Lossy networks cause picture quality to degrade and audio to sound poor. While many advanced codecs have inherent abilities to surmount packet loss, Remote Expert Mobile can be more prescriptive. Our SDKs use Picture Loss Indication (PLI) and Negative Acknowledgment (NACK) as mechanisms to surmount packet loss on a network. With video traveling over the Internet, impairment can happen at the Wi-Fi access point or somewhere on the line, Mobile Advisor informs a sender of the loss of particular RTP data. The sender uses this information to optimize the user experience, resend data and compensate for known lost packets.

You can configure how PLIs are sent using the settings in the `proxy.properties` file in the REAS install directory. By default, we send PLI requests every 2 seconds—this ensures that the video image recovers quickly from any large-scale packet loss.

You can configure what type of picture loss indication is sent to the SIP side by modifying the `video.rtcp.sip.picture.loss.message` property in the `proxy.properties` file. This value can be set to PLI to force use of PLIs, RFC2032 to force use of RFC 2032 FIRs, or AUTO to allow the media broker to auto-detect the type of picture loss indication to use based on SDP from the endpoint.

**Note** Unfortunately there are many cases where the SDP does not come from the SIP endpoint and it may be entirely impossible to auto detect whether or not a device supports PLIs or FIRs. If you wish to use auto detection, please ensure that the SDP the media broker receives from PLI enabled endpoints correctly contains the feedback attribute indicating that it supports PLIs: `a=rtcp-fb:## nack pli`

## Adaptive Rate Control

For an existing call it is possible for bandwidth to become constrained as the call progresses. In cases like this, where another download may be imposing upon the media flows for an active call, Remote Expert Mobile can dynamically manage the video stream to better handle such conditions. Adaptive rate control adjusts video bitrate down to use less bandwidth as network conditions degrade. By reducing the

video bit rate, but keeping resolution and frame rate the same, video becomes slightly grainier or more pixelated because less data is being transmitted. And when conditions rectify and bandwidth bounces back, the bitrate returns to normal.

**Initial Adaptive Bitrate** (**adaptive-bitrate-initial** in CLI)

Each RE Media Broker is able to estimate the maximum bitrate that network conditions can support for both send and receive video streams in the absence of Receiver Estimated Maximum Bitrate (REMB) and Temporary Maximum Media Stream Bit Rate Request (TMMBR) messages from browser and sip end-points. The **Initial Adaptive Bitrate** property is used to initialize these algorithms to an expected bitrate from which to start. A well-chosen initial rate may result in the algorithm finding the best quality bitrate more quickly. A poorly chosen initial rate may result in unnecessarily poor initial video (value set to low) or dropped packets / frozen video (value set to high). The units are kbps (kilobits per second). Default: 512 (kbps).

**Note** The configured values are the bit rates that the Media Broker uses. Actual network traffic may be slightly heavier than anticipated due to packet overhead.

**Minimum Adaptive Bitrate** (**adaptive-bitrate-floor** in CLI)

Every RE Mobile Media Broker receives and acts upon max bitrate messages from:

- Browser (RTCP REMB)
- SIP endpoint (RTCP TMMBR)
- Sender bitrate estimatining algorithm
- Receiver bitrate estimating algorithm

The **Minimum Adaptive Bitrate** ensures that these max bitrate messages never go below a fixed value (for example, minimum quality). In these cases, this setting is used when setting media broker video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages. The units are kbps. Default: 128 (kbps)

**Maximum Adaptive Bitrate** (**adaptive-bitrate-ceiling** in CLI)

Every RE Mobile Media Broker receives and acts upon max bitrate messages from the following:

- Browser (RTCP REMB)
- SIP endpoint (RTCP TMMBR)
- Sender bitrate estimatining algorithm
- Receiver bitrate estimating algorithm

The **Maximum Adaptive Bitrate** ensures that these max bitrate messages never go above a defined value (for example, maximum quality). In these cases, this setting is used when setting media broker video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages. The units are kbps. Default: 1024 (kbps)

## Aspect Ratio Mismatches

When transcoding, if the aspect ratios between the two parties on a video call are different, RE Media Broker handles the differences in one of two ways. If the configuration specifies **ADD_BORDERS**, REMB applies black borders to either the sides, or the top and bottom, of the live video, in such a way as to retain the aspect ratio of the received video. If the configuration specifies **STRETCH**, REMB distorts the received video to fill the video screen.

**STRETCH** is the default behavior in the Web Admin for transcoded video.

WebRTC—state of the art media quality

CHAPTER 3

# Expert Assist Features



## Web Co-browse

When a consumer requests support, their web browser tab / web application can be shared with the agent. The entire desktop is not shared—only the content of the tab opened in the browser. The screen sharing session is established and maintained for the duration of the RE Mobile session.

## Mobile App Sharing

When a consumer requests support, their mobile application view is shared with the agent. The entire mobile desktop is not shared, only the app. The screen sharing session is established and maintained for the duration of the RE Mobile session.

# Remote App Control

When a consumer requests support their application is shared with the agent. The agent can click on the shared co-browse screen to invoke actions such as navigation, page scrolling, and menu selection on the user's application (web browser tab or mobile app). This ability to remote control the session does not prevent the consumer continuing to interact with the application.

# Expert Form Editing and Completion

The agent can complete forms HTML based and native forms on behalf of the consumer by completing the form in the app share or co-browse window or via the Form Editor.

# Annotation by Expert

When a consumer is in a support session their view is shared. The agent can use the annotation tool to draw on their share of the consumer's screen. These drawings are then generated on the consumer's application.

**Note** The application does not need to be updated or aware of this annotation taking place.

# Expert Document Push

An agent within a support session can push documents to the consumer. This is currently limited to PDFs and images: (JPEG, GIF and PNG file types). A document that is shared must be available to the agent via HTTP.

# Expert URL Sharing

An agent within a support session can push other URLs to the consumer. This enables the agent to push websites into a mobile app, or enables a web consumer to jump to another portion of a website.

**Important** If an agent pushes a web page that is not enabled with Expert Assist, the agent's co-browse window goes blank, and the following message is displayed in the Expert Assist window:

*Expert Assist*
*Connected*
*You have gone to a page without Expert Assist. Your video and voice are still being transmitted to the Expert Assist agent while this window is open.*

# Protect sensitive data with field and data masking

Developers may limit the areas of a web page or mobile app seen by the agent by masking or hiding specific elements. As highlighted in the *Remote Expert Mobile Developer Guide, Release 11.6 (1)* (available at http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/products-programming-reference-guides-list.html), a developer can use simple coding conventions in Objective C for iOS, Java for Android and HTML for Web pages to protect sensitive elements, fields or data from the expert.

## Excluding information from web co-browse

**Cascading Style Sheets (Web)**: To limit the areas of the page the agent can see whilst screen sharing with the consumer, a CSS class can be added to HTML elements to instruct JavaScript CSDK to mask

those areas. Instead, the agent's screen shows an opaque box where the masked area would be. The box is black by default, but the CSS can also specify that it is colored or transparent.

## Excluding information from mobile app sharing

**iOS app UI Elements (Apple iOS)**: One use of CSDK is to allow iOS UI Elements from being excluded from the screen replication. This ensures the agent can only see the information they are authorized to see. In the iOS CSDK, this is done by way of marking the UI element with a specific tag value. This is achieved in XCode by showing the Attribute Inspector and then opening the “view” panel for the UI elements that are to be hidden.

**Android app UI Elements (Android)**: One use of the CSDK is to allow Android UI Elements from being excluded from the screen replication by adding a tag to the View object representing the area. For example: `view.setTag(Assist.PRIVATE_VIEW_TAG, true);`

# Other features

## Expert Assist with one-way video (Agent-only Video)

Expert Assist co-browse and annotation easily accommodates one-way video from the expert to the consumer to ensure consumer privacy while maintaining a rich personal experience.

## Audio and Video Hold Treatment

You can configure how hold is rendered to endpoints using the settings in the `proxy.properties` file on each of the REM Media Broker servers. (See *Cisco Remote Expert Mobile Installation and Configuration Guide, Release 11.6 (1)* (available at http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/products-installation-guides-list.html) for details).

CHAPTER 4

# CSDK Features



## CSDK for Web

The Web-based CSDK is provided in JavaScript. For versions supported see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

| Browser | WebRTC | Plug-in | Audio | Video | Platforms/Operating System |
|---|---|---|---|---|---|
| Google Chrome | Yes | No | G.711, Opus | VP8, H.264 | Windows, OSX, Android, Linux, Chrome books |
| Mozilla Firefox | Yes | No | G.711, Opus | VP8, H.264[1] | Windows, OSX, Android, Linux |
| Opera | Yes | No | G.711, Opus | VP8 | Windows, OSX, Linux |
| Microsoft Internet Explorer | No | Yes[1] | G.711, Opus | VP8, H.264 | Windows XP, Vista, 7, 8 (32-bit and 64-bit) |
| Microsoft Edge[2] | Yes | No | G.711, Opus | VP8, H.264 | Windows 10 |
| Apple Safari | No | Yes[1] | G.711, Opus | VP8, H.264 | OSX 10.9+ (Mavericks, Yosemite, El Capitan) |

Expert Assist only sessions, without voice and video, do not require a plug-in.

[1]**Browser support for H.264**—To better support WebRTC, Cisco has open-sourced its H.264 codec and

provides a binary software module that can be downloaded for free from the Internet. Open H.264.org has been adopted in Mozilla Firefox version 33 (Oct. 2014) . At an IETF meeting in November, the RTCWEB working group reached strong consensus make support for both H.264 and VP8 mandatory for browsers (WebRTC User Agents). As more browsers adopt WebRTC and development advances Chrome, Opera, IE and Safari also need to adopt H.264 to be WebRTC compliant.

[2]**Microsoft Edge**—Co-browse support only in version 14 and below; full support in version 15

## RE Mobile IE Plug-in

To better support voice and video communications on Internet Explorer where WebRTC is not yet supported, Remote Expert Mobile provides plug-ins that can easily be downloaded and installed by consumers in order to connect to a remote expert.

**Note** Expert Assist only sessions, without voice and video, do not require a plug-in.

## RE Mobile Safari Plug-in

To better support voice and video communications on versions of Apple Safari where WebRTC is not yet supported, Remote Expert Mobile provides plugins that can easily be downloaded and installed by consumers in order to connect to a remote expert.

**Note** Expert Assist only sessions, without voice and video, do not require a plug-in.

# CSDK for iOS/Android

| Mobile OS | Version | WebRTC | Plugin | Audio | Video | Platforms/Operating System |
|---|---|---|---|---|---|---|
| iOS (native) | 7+ | Yes | No | G.711, Opus | VP8, H.264 | iPad Air 2, iPad Air, iPad 4th / 3rd Generation, iPad 2, iPad mini, iPad mini with Retina display; iPad mini 3, iPhone 6/6 Plus, iPhone 5s, iPhone 5c, iPhone 5, iPhone 4S, iPod touch (5th generation) |
| Android (native) | 4.1.2+ | Yes | No | G.711, Opus | VP8, H.264 | Jellybean, KitKat, Lollipop or later. In general, CPU and memory equivalent to a Samsung Galaxy S4 (1.9 GHz Quad-core Snapdragon GS4, 4G or Wi-Fi a/b/g/n/ac and 2 MP front facing camera) |

**iOS Development**: Remote Expert Mobile applications can be developed for deployment on Apple's iOS platform for mobile devices. Developers can use Xcode, taking advantage of native libraries, to create, test, debug and tune their applications. Development for mobile devices requires that the developer is signed up for Apple's iOS Developer Program.

**Android Development**: Remote Expert Mobile applications can be developed for deployment on Google's Android platform for mobile devices. Developers can use Android Studio, taking advantage of native libraries, to create, test, debug and tune their applications. Developers can also use an existing IDE by downloading Android SDK tools (http://developer.android.com/sdk/index.html).

## Maximum Device Video Resolutions

Most mobiles, tablets and laptops are typically limited to sending 720p because most common front-facing cameras support a maximum of 720p, and this is the dominant resolution and encoding requirement. For example:

| Laptops | | Tablets | | Phones | |
|---|---|---|---|---|---|
| Acer C720 Chrome Book | 0.9 MP (1280x720) 720p | iPad Air2 | 1.2 MP (1280x960) 720p | iPhone6/6plus | 1.2 MP (1280x960) 720p |
| Lenovo T440s | 0.9 MP (1280x720) 720p/30fps | iPad Air | 1.2 MP (1280x960) 720p | iPhone5/5s | 1.2 MP (1280x960) 720p |
| 13” MacBook Air | 1.3 MP (1280x1024) 720p | iPad Mini3 | 1.2 MP (1280x960) 720p | iPhone 4S | 0.3 MP (640x480) VGA |
| Dell XPS 13 | 1.3 MP (1280x1024) 720p | iPad Mini 2 (w/ Retina Display) | 1.2 MP (1280x960) 720p | Samsung Galaxy S5 | 2 MP (1920x1080) 1080p |
| HP Spectre x2 (HP TrueVision HD Webcam) | 1.3 MP (1280x1024) 720p | iPad2 | 0.3 MP (640x480) VGA | Samsung Galaxy S4 | 2 MP (1600x1200) 720p |
| Samsung ATIV Book 9 Plus | 1.3 MP (1280x1024) 720p | Google Nexus 10 | 2MP (1600x1200) 720p | Samsung Galaxy S4 | 2 MP (1600x1200) 720p |
| | | Samsung Galaxy Tab S 10.1 | 2.1 MP (1600x1200) 720p | Samsung Galaxy Note 3 | 2 MP (1600x1200) 720p |

# WebRTC Signaling

Remote Expert Mobile utilizes WebRTC to enable customer applications to connect voice and video communication between web browsers and mobile devices and expert within a Contact Center or UC infrastructure. See http://www.w3.org/TR/webrtc/ for the full W3C specification of WebRTC.

**Signaling Web Sockets**—RE Mobile leverages JSON payloads for signaling over Web Sockets to establish a proper OFFER and ANSWER. Unlike other WebRTC technologies, RE Mobile does not use ROAP, SIP over Web Sockets or JSEP. RE Mobile‘s enhanced signaling allows multiple web sockets to be coordinated during a single session to ensure messaging, co-browsing, context, voice and video. RE Mobile signaling also has enhanced checks and error handling that goes beyond standard JSEP or WebRTC signaling ensuring better reliability while maintaining a lightweight-signaling framework.

**Enabling Web Socket Cookie Support**—By default, RE Mobile does not include cookies on the Web Socket connection it opens to the REAS.

See the *Cisco Remote Expert Mobile Developer Guide, Release 11.6 (1)* (available at http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/products-programming-reference-guides-list.html), *Enabling Web Socket Cookie Support* section for details of how to enable cookies, if required.

CHAPTER 5

# SIP Features

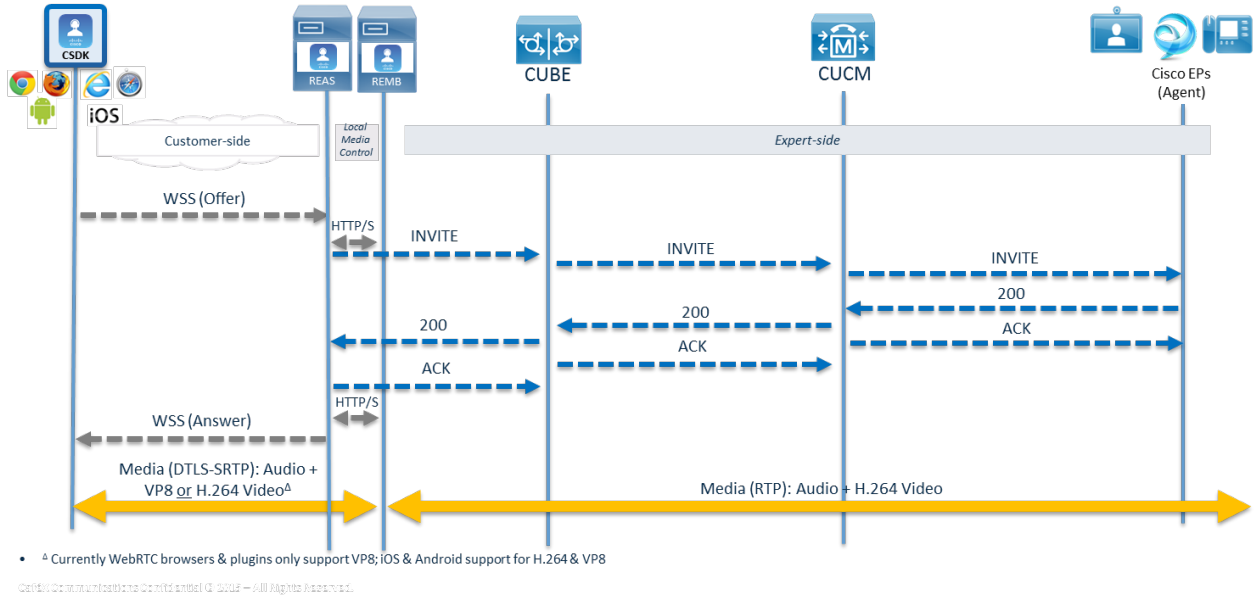


Remote Expert Mobile uses Web Real Time Communication (WebRTC) technologies to integrate mobile and web browsers seamlessly with existing UC systems. It does this using the Remote Expert Mobile Application Server (REAS) and Remote Expert Mobile Media Broker (REMB) software as a WebRTC-to-SIP gateway and RTP proxy respectively. In turn, enterprises can implement WebRTC even if their current telephony infrastructures do not conform to many of the advanced standards of current browsers.

## Connecting to Outbound SIP Servers

Remote Expert Mobile is effectively a SIP trunk that securely connects over the top clients (voice and video over the internet) into a traditional UC and Contact Center infrastructure. Upon the initialization and establishment of a secure Web Socket and secure communication to the REMB for media, the REAS Server creates a SIP `INVITE` to one or more SIP Servers (for example, Unified Communications Manager or CUBE). Once a `200 OK` is received by the SIP Server, and after successful STUN and DTLS setup between the REMB and the CSDK application, media flows in both directions between Remote Expert mobile application using the CSDK and traditional SIP endpoints (for example, Jabber Client, EX90, DX650).

**Figure 2: Remote Expert Mobile General Call Flow**



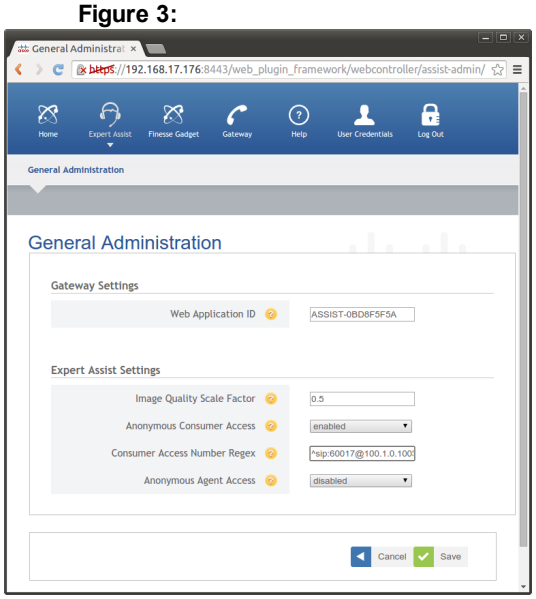

# SIP Signaling to UC infrastructure

## Limiting SIP Destination through Regex

Both browser and mobile applications provide a destination when they connect to Expert Assist. You can configure Expert Assist with a regular expression that the destination must match if Expert Assist is to allow the call. This configuration item is called the "Consumer Access Number Regex" and by default is blank, meaning it allows any destination.

You manage the "Consumer Access Number Regex" in the Remote Expert Mobile Administration Console. Click on the Expert Assist Tab and then choose the General Administration menu. For example a value of `^sip:60017@100.1.0.100$` will only allow a destination that exactly matches sip:60017@100.1.0.100

**Figure 3:**




## SIP UUI

You can provide a string to populate SIP `INVITE` and `BYE` messages sent by the user with a `User-to-User` header. As an example, suppose the value of this parameter is "ABCD". RE Mobile adds the header "`User-to-User: ABCD;encoding=hex`". The application should ensure that it provides a correctly encoded HEX string. If this parameter is omitted, RE Mobile does not add any `User-to-User` header to SIP messages. This is a simple way to pass contextual data (up to 128 bytes) between the application and the Finesse Agent console.

In Unified CCE, the UUI header propagates as an accessible variable. The UUI from Unified ICM is passed using the user.microapp.uui ECC variable, or the `Call.UsertoUserInfo` variable. If both

variables are used, `Call.UsertoUserInfo` takes precedence. Extract the UUI in your Unified ICM Script by looking at the Call ECC variable user.microapp.uui and the `Call.UserToUserInfo` variable, such as in the IF node. By using the SET node on either one of these variables, the variable can be set on the out-bound direction of the call.

### Media Session Admission Control

Media Session Admission Control is designed to "protect" a Media Broker against overloading when one is being selected to handle a new call. When enabled, and a Media Broker is deemed unable to handle another call, the REAS tries to select another Media Broker. If no REMBs can take the call, the REAS rejects the session immediately due to no Media Brokers being available.

- **Max. Load Factor**—The maximum Media Broker load limit. When a call is assigned to a particular Media Broker, the Media Broker rejects the call if its current load factor is at, or above, this value—this causes the Load Balancer to choose another Media Broker (if one is available) The default value is 75 for 75% CPU load utilization. A value of "0" in this field disables this function.
- **SDP Control Request Timeout**—The maximum number of milliseconds to wait for SDP control requests to complete between the Gateway and Media Brokers. SDP Control requests are typically used by the Gateway to setup a call with the Media Broker. If the request should not complete within this timeout period, when allocating a Media Broker to a new call, the Gateway tries another Media Broker


**Note** Media Session Admission Control is not enabled by default.

### Video in Queue, Video on Hold and Video Prompt

Video Queue, Video Hold and Video Prompt are standard features for Unified CCE and Unified CCX. Please refer to standard Unified CCE and Unified CCX product documentation for feature details and configuration as well as Cisco Contact Center Solutions and Unified Communications Manager Solution Configuration Guide for Remote Expert Mobile.

### Session Recording

Audio and Video recording are standard features for CCE/CCX and are based on MediaSense and CUBE. Refer to Unified CCE and Unified CCX product documentation for feature details and configuration as well as *Cisco Contact Center Solutions and Unified Communications Manager Solution Configuration Guide for Remote Expert Mobile*.

# Firewall and Network Traversal

## HTTPS Signaling Protocol

The customer firewall routes all signaling traffic received on port 443 (secure) or 80 (un-encrypted) to the HTTP reverse proxy in the DMZ, this is then forwarded onto the REAS in the enterprise network.

## UDP Port Multiplexing

Remote Expert Media Broker multiplexes both RTP and RTCP traffic from Remote Expert Mobile CSDK clients via the same UDP port. (RTP and RTCP traffic is encrypted with sRTP and DTLS.)

Although one REMB port is open by default for RTP and RTCP traffic (UDP port 16000), production systems should open up to five. Each port multiplexes both RTP and RTCP traffic.

# STUN support

When behind a firewall, machines running CSDK clients have private IP addresses that are mapped to a single public address by the firewall using Network Address Translation (NAT). The CSDK clients are not aware of their respective public addresses, and therefore cannot receive voice traffic from the Remote Expert Media Broker on the private address it advertises. RE Mobile employs Session Traversal Utilities for NAT (STUN) to allow RE Mobile applications to discover their public address and port for use in communication with the REAS and REMB.

CHAPTER 6

# Encryption



## Secure Signaling and Media between the CSDK applications (clients) and the REAS / REMB

All communications (signaling and media) between clients on the Internet or inside the enterprise network is secure via enterprise-grade encryption.

Products that use TLS/SSL for secure transport must configure TLS/SSL to use ciphers of 128 bit or better. Server certificates must use the SHA1 or SHA2 algorithms (no MD5).

- **Secure WebRTC Signaling**— Prior to extending an OFFER to initiate a session, the WebSocket connection starts as an HTTP handshake, which then upgrades in-place to speak the WebSocket wire protocol. TLS encryption for any WebSocket is the same as HTTPS, using certificates. As with HTTPS, WebSocket Secure (WSS) first establishes a secure envelope, then begins the HTTP handshake, and then upgrades to the WebSocket. The WebSocket wire protocol is not a different protocol, but is WS (WebSocket) transported over TLS. To secure WebRTC signaling, the REAS conducts all JSON messaging over TLS via Secure WebSocket (WSS).

  The Reverse Proxy can also perform user authentication on behalf of the web application, ensuring that only authenticated connections can reach the internal network. It can also take advantage of hardware Secure Sockets Layer (SSL) accelerators to provide SSL termination functionality, decrypt the data on behalf of the application, and establish a secure context with the client. After establishing the secure context, all subsequent communication between the client and the server is within that context. Use of a Reverse Proxy allows rules to be set up on it to stop WebSocket connections being established with the

REAS if they are not part of an already established security context. The Reverse Proxy must support WebSockets.

- **Secure media via DTLS/sRTP**—DTLS enables the secure exchange of the cryptographic parameters and derive keying material for media encryption. The key exchange takes place in the media stack and is multiplexed on the same ports as the media itself. DTLS-SRTP allows the SRTP media channel to be established without revealing keys in the SDP message exchange as is done with more common sRTP SDES. According to draft-ietf-rtcweb-rtp-usage-07 (current draft, July 2013), WebRTC gateways MUST support DTLS-SRTP for key-management. DTLS-SRTP is the default, more secure and preferred encryption mechanism.

# Secure Signaling and Media between the REAS / REMB and the UC infrastructure

- **SIP TLS (Transport Layer Security)**—to establish a trust with the REAS and the enterprise SIP server / Cisco UBE. TLS provide authentications by using Mutual or Two-Way Authentication uses certificates from a Certificate Authority to authenticate each other. The REAS uses a digital certificate for authentication and a public key for encryption/decryption. Both the REAS and configured SIP Server have a common CA for their certificates. The certificate can be either a self-signed certificate and key or a certificate obtained from a CA (Certificate Authority).


Note

SDES is not enabled by default on the enterprise network between the REMB and UC infrastructure.

# Secure Signaling and Media between the REAS and REMB

- **Secure Control between REAS and REMB**—There is a REST service running on the REMB which services requests from the REAS to set up and tear down media routes, send DTMF and also monitor the health of all Media Brokers. You can secure this connection with HTTPS after installation.

CHAPTER 7

# High Availability

Remote Expert Mobile is deployed with high availability (HA). Remote Expert Mobile uses a cluster of REAS instances and multiple REMBs to ensure its network components are highly available. Refer to the *Remote Expert Mobile Design Guide, Release 11.6 (1)* (available at http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/products-installation-guides-list.html) for further details.

CHAPTER 8

# RE Mobile Administration



Remote Expert Mobile is deployed with Remote Expert Mobile Administration Console (url is `https://<your_server>:8443/web_plugin_framework/webcontroller/`).

# REAS

## Prioritzing codecs

**Note** These settings only apply to installations that require transcoding.

Depending on a network's capabilities, and the priority for your organization in terms of bandwidth vs. quality, you may prefer to transcode to certain codecs rather than others. RE Mobile allows you to prioritize the codecs to which media is transcoded, to ensure that the most efficient codec is given highest priority.

The prioritized codec lists include the name of the codecs as they appear in the SDP. Any codecs in the prioritized list are removed from SDP, then re-inserted at the end in the order specified. Doing this prioritizes them below all other codecs present in the SDP. It is therefore possible, if desired, to specify the relative priority of all codecs—transcoding or not.

**Note**

Codecs that are not prioritized appear first in the list, and are therefore considered by the client before the prioritized codecs.

Codec names are typically defined in the IANA registry http://www.iana.org/assignments/rtp-parameters/rtp-parameters.xhtml. Bear in mind, however, that the registry may not always include the newest codecs. For example VP8 and opus—two new codecs commonly used by WebRTC.

## Adding Web Application IDs

The Web Application ID is a unique text string, that identifies the web application to the Web Gateway, and confirms that the web application is allowed to create sessions. The RE Mobile Web Administration interface enables you to define the list of Web Application IDs that the Web Gateway accepts. To define the list of acceptable Web Application IDs:

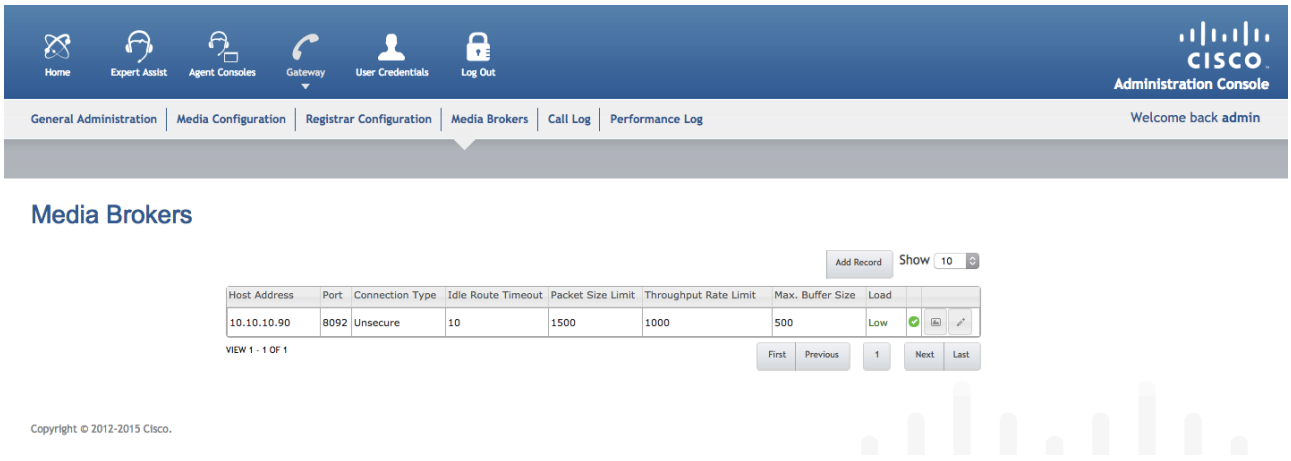
1. Log in to the RE Mobile Web Administration Console. The RE Mobile Administration page displays.
2. Click the **Add** button under Web Application IDs
3. The **Add Record** dialog displays

   Enter the Web Application ID in the **Key** field, this should be a unique text string with a minimum of 16 characters. For example: `REMOTEEXPERT-A8C1D`
4. Click **Submit**. The Web Application ID you entered now displays in the list of Web Application IDs
5. Click **Save** at the bottom of the page

# REMB

To reveal detailed statistics for a particular media broker, click on the “graph” image in the column to the right of the **Connectivity** column.

**Figure 4:**




The “Load” value, is the actual load reported by the media broker, whilst the “Load Group” value is the “band” that the load value fits into, with “0” being the lowest loaded group band—this group is then used in the load balancers' media broker selection strategy.

The “Connectivity” section lists all REAS instances, and their connection status to this particular media broker.

# Expert Assist

Expert Assist server is configured via the web administration console (`https://<your_server>:8443/web_plugin_framework/webcontroller/assist/`) or via the CLI:

There are a few parameters that can be configured for the server:

- **Web Application ID**—The Web Application ID that Remote Expert Assist will use to authenticate itself with the REAS. The REAS SDK requires that client web applications are identified via a "Web Application ID".
- **Image Quality Scale Factor**—This allows the server administrator to configure the quality of the browser session share seen within the Agent Console. Values closer to 0 will reduce quality but require less bandwidth; 1 is maximum quality (it applies no scaling).
- **Anonymous Consumer Access**
  - **Enabled** (Default)—Anonymous consumer use of Expert Assist is permitted; however, an anonymous client application cannot specify a Correlation ID.
  - **Disabled**—A client application has chosen to authenticate its users before allowing them to invoke the Remote Expert Assist functionality. In this case the Client application must provide a Session Token when invoking Expert Assist.
  - **Trusted**—Similar to the Enabled case; however, the client application is trusted to supply Correlation IDs. As JavaScript is visible in the browser the Correlation IDs used by the application are also in plain text. This may not be desirable and this mode should only be enabled in secure environments.
- **Consumer Access Number Regex**—A regular expression which limits the numbers an Anonymous consumer may call for assistance. By default this value is blank, which means that any number is permitted.
- **Anonymous Agent Access**
  - **Enabled**—Anonymous Agents are permitted to provide assistance.
  - **Disabled** (Default)—Agents must be authenticated before being able to provide assistance.

**Note** When using the sample Agent Console supplied with Expert Assist, this configuration item must be set to **Enabled**

# Monitoring Sessions

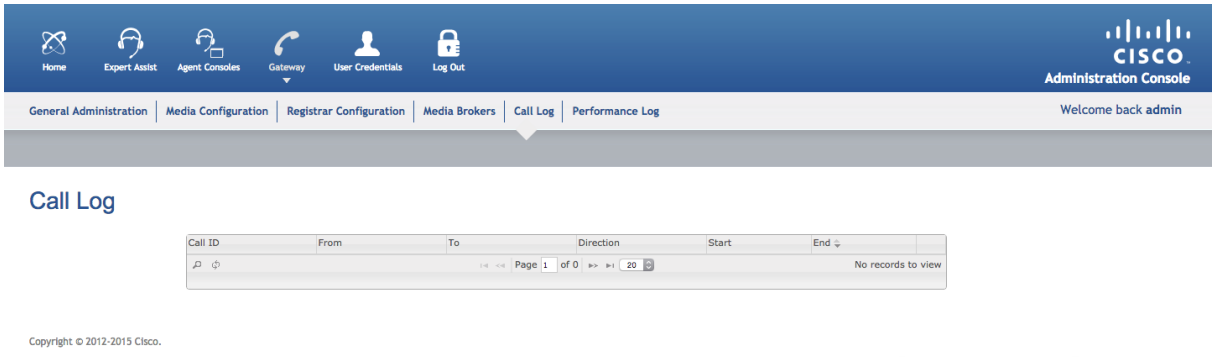
To enable call log statistics, configure the **Call Log Configuration** section in the REAS General Administration page—the **Log Level** needs to be set to **On**.

After you enable the log level, each media broker logs statistics.

However, in order to display the statistics, you must also set the **Log Expiry** value to a value greater than zero minutes.

To display the call logs, navigate to **Gateway-> Call Log**:

**Figure 5:**

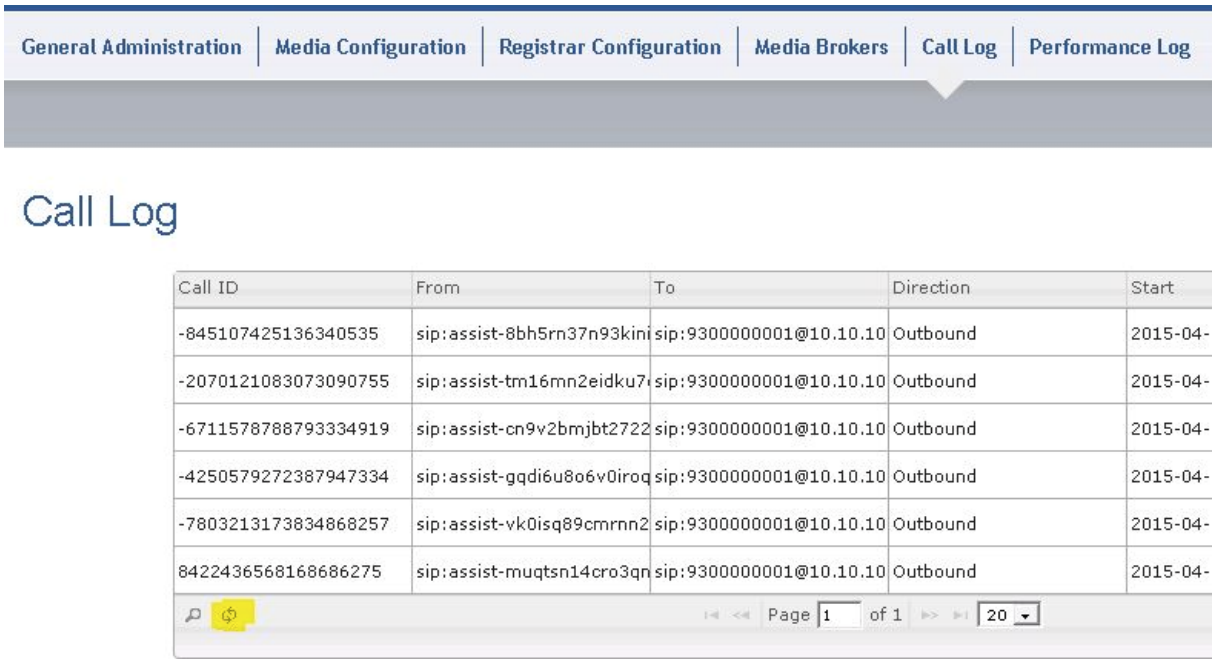



The **Direction** column indicates:

- Inbound: The media broker is handling the SDP for the callee
- Outbound: The media broker is handling the SDP for the caller

The call log will generate a table as shown below:

**Figure 6:**

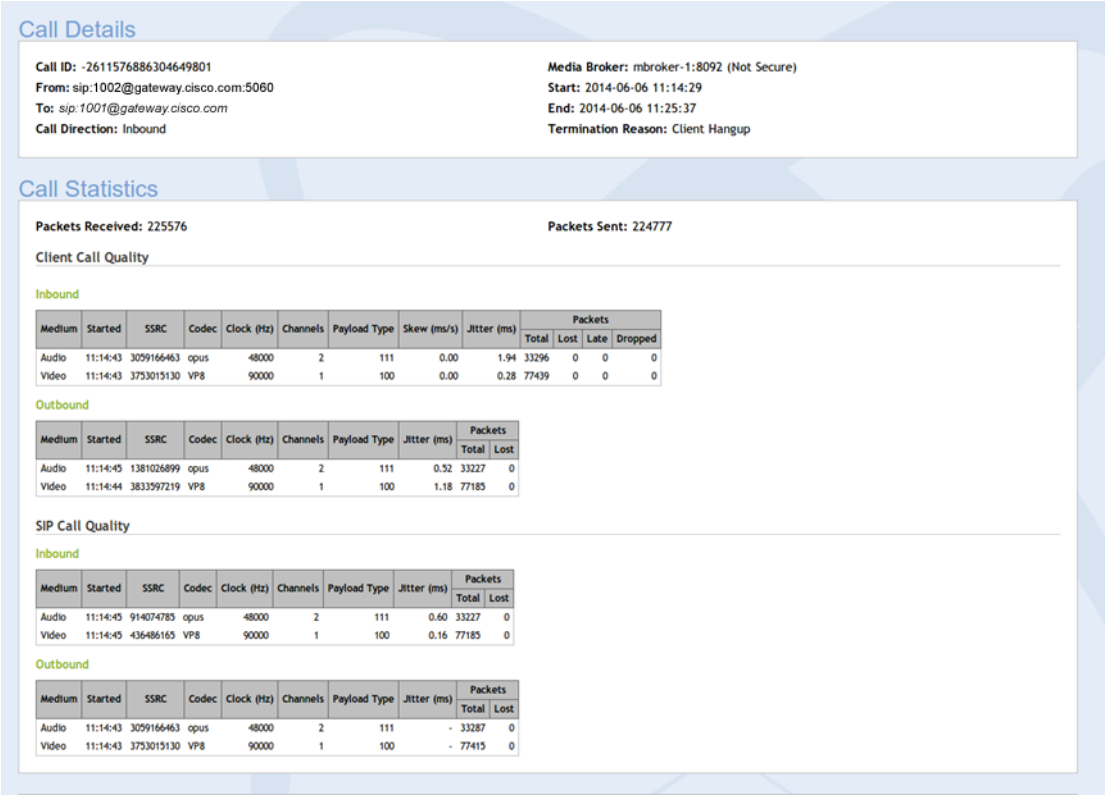



**Note** Clicking the **Reload Grid** button (highlighted) clears any filters in the call log.

## Session Statistics

A particular Session Log entry displays detailed statistics about a particular call:

**Figure 7:**



Call Details

**Call ID:** -2611576886304649801
**From:** sip:1002@gateway.cisco.com:5060
**To:** *sip:1001@gateway.cisco.com*
**Call Direction:** Inbound

**Media Broker:** mbroker-1:8092 (Not Secure)
**Start:** 2014-06-06 11:14:29
**End:** 2014-06-06 11:25:37
**Termination Reason:** Client Hangup

Call Statistics

**Packets Received:** 225576 **Packets Sent:** 224777

Client Call Quality

Inbound

| Medium | Started | SSRC | Codec | Clock (Hz) | Channels | Payload Type | Skew (ms/s) | Jitter (ms) | Packets | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Total | Lost | Late | Dropped |
| Audio | 11:14:43 | 3059166463 | opus | 48000 | 2 | 111 | 0.00 | 1.94 | 33296 | 0 | 0 | 0 |
| Video | 11:14:43 | 3753015130 | VP8 | 90000 | 1 | 100 | 0.00 | 0.28 | 77439 | 0 | 0 | 0 |

Outbound

| Medium | Started | SSRC | Codec | Clock (Hz) | Channels | Payload Type | Jitter (ms) | Packets | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Total | Lost |
| Audio | 11:14:45 | 1381026899 | opus | 48000 | 2 | 111 | 0.52 | 33227 | 0 |
| Video | 11:14:44 | 3833597219 | VP8 | 90000 | 1 | 100 | 1.18 | 77185 | 0 |

SIP Call Quality

Inbound

| Medium | Started | SSRC | Codec | Clock (Hz) | Channels | Payload Type | Jitter (ms) | Packets | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Total | Lost |
| Audio | 11:14:45 | 914074785 | opus | 48000 | 2 | 111 | 0.60 | 33227 | 0 |
| Video | 11:14:45 | 436486165 | VP8 | 90000 | 1 | 100 | 0.16 | 77185 | 0 |

Outbound

| Medium | Started | SSRC | Codec | Clock (Hz) | Channels | Payload Type | Jitter (ms) | Packets | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Total | Lost |
| Audio | 11:14:43 | 3059166463 | opus | 48000 | 2 | 111 | - | 33287 | 0 |
| Video | 11:14:43 | 3753015130 | VP8 | 90000 | 1 | 100 | - | 77415 | 0 |

The **Call Details** section shows information about the call itself—the underlined party indicates which party this call is being handled for. The **Call Statistics** section shows the packets received and sent at the top, and below that is displayed detailed information relating to the call quality.

**Client Call Quality**: Shows statistics between the REMB and the CSDK application

- Inbound: Shows statistics from the CSDK endpoint to the REMB
- Outbound shows statistics from the REMB to the CSDK endpoint

**SIP Call Quality**: Shows statistics between the REMB and the SIP endpoint

- Inbound: Shows statistics from the SIP endpoint to the REMB
- Outbaound: Shows statistics from the REMB to the SIP endpoint

# Logs

## Capturing logs on the REMB

To help you identify any issues you may experience, a script is provided with RE Mobile to captures call logs and statistics from the REMB. The `logcapture.sh` script is installed in the Media Broker directory installation directory and can be used to capture the following information:

- Media Broker configuration
- vmstat output
- Java memory

- Thread dumps
- Network capture (in a .pcap file)

The logging script runs for a period of time which you define, allowing you to reproduce any problem scenarios during this time. When you stop the logging script, the information you require is captured in a series of log files.

You can define which information is captured by adding a selection of the following arguments when you run the script:

| Short option | Long option | Description | Optional/Required |
|---|---|---|---|
| -f | --tar-file | The filename of the resulting .tar archive | Required |
| -c | -config | Includes configuration files in the .tar archive | Optional |
| -t | -threads | Includes thread dumps in the .tar archive | Optional |
| -m | -memory | Includes heap memory dumps in the .tar archive | Optional |
| -n | -do-not-clean | Sets the script to not clean up the output directory at the end of the run | Optional |
| -p | -capture-pcap | Captures network traffic in a .pcap file | Optional |
| -v | -vmstat | Includes vmstat output in the .tar file | Optional |
| -a | -all | Includes all options | Optional |
| -h | -help | Displays the online help | Optional |

To capture logs on the Media Broker:

1. Capture all the information by running:
   `logcapture.sh -a -f example.tar`
   (Use other options instead of `-a` if you only want some of the logs.) The console will display the following message:
   ```
   ****************************************************
   * Capturing files to directory logcapture.temp-LGR  *
   * Press <CTL>-C when ready to tar up captured files *
   ****************************************************
   ```

**Note** The final three characters of the directory name (LGR in the above example) change each time you run the script, as this is a temporary directory.

2. Reproduce any scenarios which are causing the issues
3. Stop logging by pressing **Ctrl+C**. `example.tar` contains the output files, and looks something like:
   ```
   ./vmstat.out
   ./tcpdump.pcap
   ./MB/
   ./MB/x264_2pass.log
   ./MB/thread.dump
   ./MB/heap.bin
   ./MB/routetable.log
   ./MB/rest.log
   ./MB/proxy.log
   ./MB/log4j.properties
   ./MB/proxy.properties
   ./MB/console.log
   ```

```
./MB/stun.log
./MB/master.console.log
```

**Caution**: Executing logging scripts on a production server (particularly when using heap, thread, or pcap dump) may signifivantly imact performance.

# SNMP

The REAS generates SNMP event data, or traps. This data can provide valuable usage and diagnostic information to administrators and network operations personnel. An SNMP agent is included in each REAS. The SNMP agent raises traps when significant events occur in the Application Server cluster.

To add an address for receiving traps you add an SNMP trap target, using a command of the following format:

```
/profile=management/subsystem=snmp_subsystem/trap-target=<targetname>/: add
(protocol=<snmp-protocol>,ip=<target-ip>,port=<target-port>)
```

where:

- `<target-name>` is the ID of the trap target
- `<snmp-protocol>` is the SNMP protocol to use for this target. This must be SNMPv1, SNMPv2c, or SNMPv3. If the snmp-protocol component is omitted, it defaults to SNMPv2c.
- `<target-ip>` is the IP address of the trap target
- `<target-port>` is the port to send the traps to

There are a number of SNMP traps that might be raised when significant events occur within the cluster. Each of the following SNMP traps for the REAS are symmetric; this means that each trap contains ‘Set’ when an issue is detected, or ‘Clear’ when the issue is resolved. The Set traps are as follows:

- **platformSetSlaveDomainConnectionDown**—A slave Application Server could not connect to the Domain Host Controller, suggesting that the Domain Host Controller is not running.
- **platformSetServerGroupDown**—The REAS cluster has no active servers.
- **platformSetServerConnection**—The SNMP agent failed to connect to a server. This could be a REAS slave or master; as identified by the resourceId in the notification
- **platformSetServerState**—Set for any server state change for any REAS. Server has either stopped or a restart is required.
- **platformSetNodesNotRegisteredWithLoadBalancer**—A Load Balancer has no Application Servers registered with it. This trap is fired only when a Load Balancer is restarted at a time when there are no Application Servers running.

When the issue is resolved, the associated Clear trap is raised, for example, if the **platformSetServerGroupDown** trap is raised and at least one server in the cluster is started, the **platformClearServerGroupDown** trap is raised, signifying that the issue is resolved.

There is also an asymmetric trap, **platformAbnormalServerShutdown**. This trap is raised every time a REAS shuts down unexpectedly. By default, when an unexpected shutdown is detected the Host Controller restarts that server. This trap ensures that administrators are alerted to multiple restarts that might affect service, so that they can investigate the issue.

## Example scenarios

The following example scenarios show which traps are raised for a number of different errors:

- If all of the Application Servers in a REAS cluster go down, no traffic can be processed for that Server Group. The **platformSetServerGroupDown** trap is raised.
- If the management server on the Master goes down, the licensing subsystem becomes unavailable. The **platformSetServerConnection** trap is raised. The **platformSetServerState** might also be raised as the server state changes from the running state.
- If a slave REAS loses connection to the Master, the configuration on that might become stale. The **platformSetSlaveDomainConnectionDown** trap is raised.

- If a slave REAS reinstates a connection to the Master, the **platformSetServerState** trap is raised (restart required state).

# Checking RE Mobile versions

It is possible to verify the version of the Remote Expert Assist server currently running. To do so, please visit the following URL: `http://your_server:8080/assistserver/info/version.html`

# Acronym List

| Item | Description |
|---|---|
| **CODEC** | “Coder-decoder" encodes a data stream or signal for transmission and decodes it for playback in voice over IP and video conferencing applications. |
| **CSDK** | Remote Expert Mobile Client SDKs. Includes three distinct SDKs for iOS, Android and web/JavaScript developers. |
| **CUBE** | Cisco Unified Border Element, a Cisco session border controller used in contact center and unified communications solutions |
| **CUCM** | Cisco Unified Communications Manager or Unified CM |
| **G.711** | PCMU/A 8-bit audio codec used for base telephony applications |
| **G.729a** | Low-bitrate audio codec for VoIP applications |
| **H.264** | Video codec. H.264 is the dominant video compression technology, or codec, in industry that was developed by the International Telecommunications Union (as H.264 and MPEG-4 Part 10, Advanced Video Coding, or AVC). Cisco is open-sourcing its H.264 codec (Open H.264) and providing a binary software module that can be downloaded for free from the Internet. Cisco will cover MPEG LA licensing costs for this module. |
| **Opus** | Low bit rate, high definition audio codec for VoIP applications. Opus is unmatched for interactive speech and music transmission over the Internet, but is also intended for storage and streaming applications. It is standardized by the Internet Engineering Task Force (IETF) as RFC 6716 which incorporated technology from Skype's SILK codec and Xiph.Org's CELT codec (www.opus-codec.org) |
| **PLI** | Picture Loss Indication is another feedback mechanism of the Real-time Transport Control Protocol (RTCP) that enables the sender to resend keyframe packets to re-establish a full video picture when communicating over the Internet or poor network conditions. |
| **REAS** | Remote Expert Mobile Application Server |
| **REMB** | Remote Expert Mobile Media Broker |
| **RTP** | Real-time Transport Protocol |
| **RTCP** | Real-time Transport Control Protocol |
| **UC** | Unified Communications |
| **VP8** | Video codec—VP8 is a video compression format owned by Google. Google remains a staunch supporter of VP8 after buying On2 Technologies in 2010; Google then released VP8 software under a BSD-like license, as well as the VP8 bitstream specification under an irrevocable license, and free of royalties. VP8 is roughly equivalent in processor usage, bandwidth, and quality to H.264. |
| **WebRTC** | Web Real Time Communications for communications without plug-ins |