Cisco Remote Expert Mobile Version 11.5(1)

Design Guide

First Published: 2016-08-10
Last Modified: 2016-12-13

Preface

Change History

Changes	See	Date
Initial release of document for Release 11.5(1)		August 2016
Merged Large and Small OVA details into *For Production Systems* table	Virtual Machine (OVA) Specifications on page 32	October 2016
Updated section	Sizing Remote Expert Mobile Virtual Machines on page 33	
Updated section	Audio-Only Calls on page 36	
Added section	Deployment Across Multiple Data Centers	
Updated section	Requirements for optional Reverse Proxy Server on page 16	
Updated sections	Introduction on page 6	November 2016
Added section	Remote Expert Co-browse on page 41	
Removed section	Co-browse only mode from Other Scenarios	
Updated section	Sizing REM VMs with correct data	
Removed section	Compatibility information	
Updated section	Deployment Across Multiple Data Centers	December 2016
Updated Sections	Interoperability – addition of link to compatibility matrix Sizing REM VMs to reflect standard of 2 REASs and maximum of 3	
Updated Section	Interoperability – addition of tech note to Cisco Video Endpoints	

About this guide

This guide provides design considerations and guidelines for deploying Cisco Remote Expert Mobile with Unified CCE, Unified CCX, and Unified CM.

This guide assumes that you are familiar with basic contact center and unified communications terms and concepts. It describes the necessary DNS, NAT, reverse proxy, and firewall architectural elements for RE Mobile. It assumes that the network administrator has a working knowledge of configuring these systems. It also assumes you have sufficient Cisco Unified Call Manager knowledge to do the following:

- Configure CUCM trunks
- Configure routing patterns

Successful deployment of Remote Expert Mobile also requires familiarity with the information presented in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)*.

property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Organization of This Guide

This guide includes the following sections:

Section	Description
Introduction	This section provides an overview of Remote Expert Mobile and its SDKs, software server components, agent integrations, and key technologies.
Architecture Overview	This section introduces the SDK and server components of Remote Expert Mobile and required Cisco components
Deployment Scenarios	This section describes the standard Remote Expert Mobile with Unified CCE and Unified CM model deployments.
High Availability	This section describes high availability and failover scenarios
Securing Remote Expert Mobile	This section provides an introduction to designing security into Remote Expert Mobile deployments and applications
VM Specifications and Constraints	This section describes the system requirements for Remote Expert Mobile Virtual Machines
Sizing Remote Expert Mobile Virtual Machines	This section deals with sizing the Unified CCE components for your contact center. It also discusses the impact of some optional features on component sizing.
Bandwidth Provisioning and QoS Considerations	This section discusses bandwidth, latency, and quality of service design considerations for Remote Expert Mobile.
External Firewall and NAT Settings	This section reviews the firewall settings used in conjunction with Remote Expert Mobile
Remote Expert Co-browse	This section reviews the differences between the full edition of Remote Expert Mobile and Remote Expert Co-browse.
Acronym List	This section lists some common industry and Cisco-specific acronyms and other terms relevant to Remote Expert Mobile.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are on the Cisco website at www.cisco.com/go/offices.

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
bold font	Commands, keywords, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	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.
`courier font`	Terminal sessions and information that the system displays appear in `courier` font.
< >	Non-printing characters, such as passwords, are shown in angle brackets.
[ ]	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.

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 complete voice, video, and Expert Assist customer engagement session, interconnected to a full contact center environment. For example, Cisco Remote Expert Mobile can connect individual investors to the next available financial advisor 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-browsing and application sharing in mobile or web applications. Cisco Remote Expert Mobile enables remote collaboration services provided through the following:

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise (Unified CCE)
- 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 Cisco Unified Communications Manager)
- Expert Assist
  - Web co-browsing
  - Escalate a call to include co-browse
  - Mobile app sharing
  - Remote app control
  - Expert form editing and completion
  - Annotation by expert
  - Expert document push
  - Expert URL sharing
  - Protect sensitive data with field and data masking
  - Choice of media modes:
    - Full voice and video
    - Agent-only video (with audio in both directions)
    - Audio only
- Media Handling:
  - 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
  - Media encryption and decryption
  - Bidirectional audio
  - High definition video (H.264 or VP8 in CIF (352x288), nHD (640x360), VGA (640x480), 720p (1280x720)
  - High definition and narrowband audio codec support (Opus, G.711 u-law (μ-law/mu-law) or G.711 A-law)
  - Opus, G.711 u-law (μ-law/mu-law), G.711 A-law and G.729a audio transcoding into the enterprise network
  - H.264 and VP8 video transcoding
  - OpenH264 support

Remote Expert Co-browse

With Cisco Remote Expert Co-browse (previously called Meet-me) developers can deliver Expert Assist co-browse and application sharing in mobile or web applications. In this case, the key components are:

— Expert Assist (with all its elements as above)

See the Remote Expert Co-browse section for more details.

SDKs

Cisco Remote Expert Mobile includes Software Development Kits (SDKs) to provide Voice over IP, Video over IP and Expert Assist (app sharing and web co-browsing, 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 the following:

- Google Chrome
- Mozilla Firefox
- Opera
- Internet Explorer
- Apple Safari

WebRTC enables in-app communications without the need for plug-ins. 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 and Android apps through native libraries.

Note: Remote Expert Co-browse does not include voice and video functions.

Cisco Remote Expert Mobile Client SDK (CSDK)

- Expert Assist (co-browse, annotation, and document push) supported in IE and Safari without plug-in for agent and consumer; supports HTTP or HTTPS URLs only, not FTP.
  Only voice and video (WebRTC) requires plug-in for IE and Safari.
- Expert Assist—Support for Chrome, Firefox, Safari, and Internet Explorer (Windows desktop only, not tablet).
- Expert Assist—Agent form filling for Web, Android and iOS.
- Expert Assist—Push File Content; similar to Push Document/Image URL but instead the Agent downloads the content and sends it directly to the Consumer; supports HTTP or HTTPS URLs only, not FTP.
- Expert Assist—To use co-browse-only mode in the Consumer Sample application, a new URL parameter has been introduced to enable this mode: `cobrowseOnly=true` and `cid=<an_id>` must be specified.
- Expert Assist—Specify both a destination and a correlation ID to the Consumer Sample application using both the following URL parameters, separated by an ampersand (&): `destination=<address>&cid=<an_id>`
  Audio-only & Expert Assist support
- Airplay support for video and Expert Assist
- JavaScript sample application (in source code form)
- Agent SDK Connection Status API added
- Allow clients to set their own encoding for UUI values
- Android sample application (in source code form)
- Android Sample provides simple volume control and speaker selection

- iOS Simulator (i386) build support. iOS Simulator Support for Co-browse only Mode.
- iOS support: arm64, armv7, armv7siOS sample application (in source code form)
- Expert Assist—Remote use of iOS UI components by agents (UISlider, UISwitch, UIStepper)
- IE plug-in logs to the file system at <user-home>\AppData\LocalLow\FusionVideo\ieplugin.log

Note: Remote Expert Co-browse does not include voice and video

Cisco Remote Expert Mobile Application Server (REAS)

- Expert Assist—Configurable screen-share quality
- Expert Assist—Co-browse Activity Indicator; the Consumer is given a visual indicator when an Agent is viewing the co-browse or mobile app share.
- Expert Assist—Multiple agent support for co-browse/app share (up to 4 parties per Expert Assist session)
- Finesse Expert Assist Gadget (supported on Chrome, IE, and Firefox)
- Finesse Expert Assist Supervisor Gadget (supported on Chrome, IE, and Firefox)
- Expert Assist Web Agent Console (supported on IE, Chrome, and Firefox) for Unified CM deployments
- Expert Assist Web Supervisor Console (supported on IE, Chrome, and Firefox) for Unified CM deployments
- Supports multiple outbound SIP Servers

  Note: The Remote Expert Co-browse does not include support for SIP servers.

Cisco Remote Expert Mobile Media Broker (REMB)

- Network Isolation Detection in Media Broker
- Media Broker supports graceful shutdown

Note: Remote Expert Co-browse does not include the use of media brokers.

Cisco Unified Border Element (CUBE)

- Cisco Unified Border Element is optional in Unified CCX and Unified Communications Manager only deployments. It is required only if you need recording at a Cisco Unified Border Element level.

Technologies

WebRTC

WebRTC is a standards-based approach for enabling real time communications through a common set of APIs. These APIs are part of the HTML5 standards, and permit web developers to embed communications within websites and mobile applications without knowing the complexities of Voice over IP. WebRTC defines a way for browsers and mobile apps to implement technologies like video conferencing in a way that is both interoperable with other clients and does not require the use of a plug-in. WebRTC uses a variety of audio and video codecs such as G.711, Opus, H.264, and VP8.

Note: WebRTC is not supported by Remote Expert Co-browse

Expert Assist

With Expert Assist, the remote user of an application can share the app window of the tablet or smartphone, or the browser tabs, with an expert. Sensitive information, for example fields and regions of a web page or application, can be masked to hide them from the expert's view. The expert can also move the live video window, to ensure that it does not interfere with elements of the screen. Expert Assist supports web browsers, and native iOS or Android apps

The expert can also control the app or website of the user through simple point and click operations. Remote control allows the advisor to navigate the menus, jump to specific information, complete forms, or walk the remote user through an important process.

In addition to co-browsing and remote control, experts can annotate within the app, and push documents for apps using the CSDK.

Unlike most co-browsing technologies, Expert Assist *does not* share the Document Object Model (DOM) between the user and the expert. Expert Assist technologies ensure that inconsistencies between different browsers are not a problem during a session. In addition, Expert Assist supports native iOS or Android apps.

MOWS

Using Media-over-WebSockets (MOWS) allows Chrome clients to use H.264, which reduces the need for transcoding. When Dynamic Codecs are enabled, the system detects whether a client supports MOWS—if it does not, then WebRTC is used instead. Typically, using MOWS can be accomplished without the need for firewall configuration changes.

Note: MOWS is not supported in Remote Expert Co-browse.

AED

AED (application event distribution) enables you to deepen the user's experience through simultaneous synchronizing of application context between clients, using topics, data, and messages. AED enables applications to do more than just screen sharing where the video from one client's screen is captured and shared with another—it allows you to share the data pertaining to the context that the app is in. Client apps can then use that data to provide an experience tailor-made for the target user, perfectly suited for display on the user's device type.

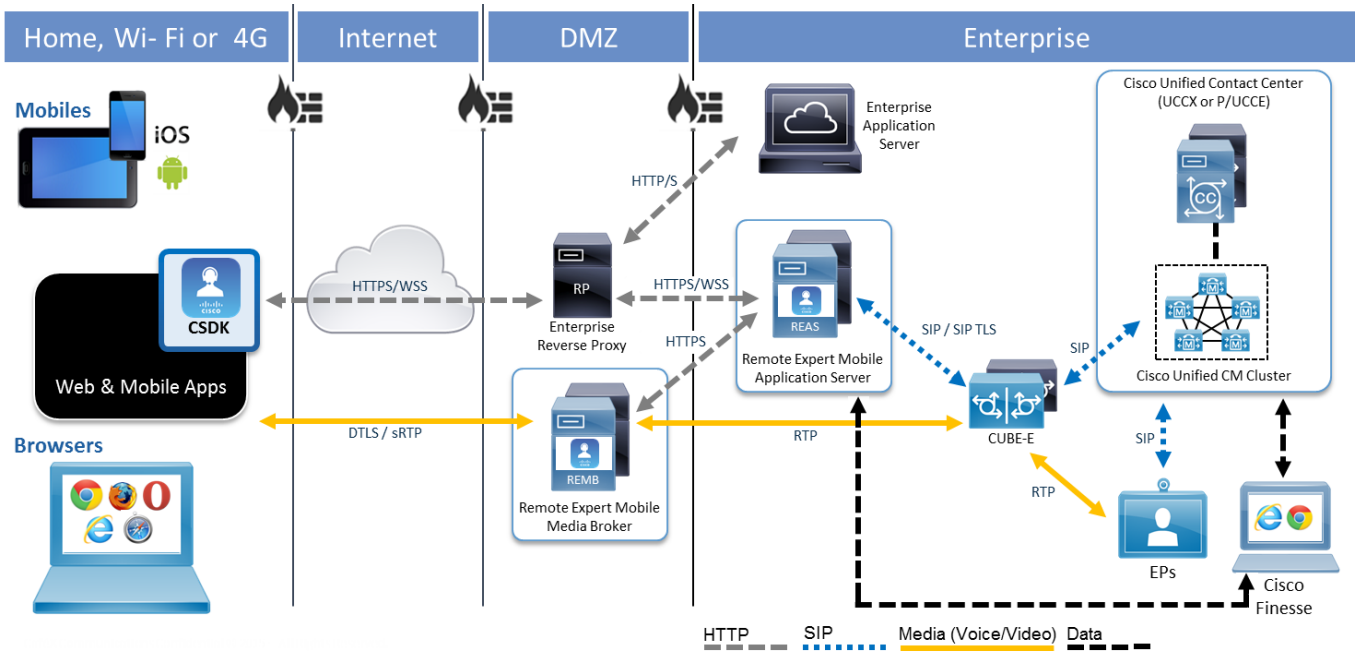
- Topics—Topics are the top-level data containers in the AED. A client can connect to (and create if necessary) any number of Topics at the same time. When connected to a Topic, client applications are notified of Messages sent and Data submitted to the Topic.
- Data—Data is persistent; the Topic keeps track of all Data submitted. When connecting to a Topic, the client receives an array of all the previously submitted Data.
- Messages—Messages are transient, and are only received while connected to a Topic. Messages are distributed to client applications in real-time, but no guarantees are made about the order in which Messages are received, and unlike AED Data, there are no API semantics around versioning Messages.

For further details on implementing AED, see *Cisco Remote Expert Mobile—Advanced CSDK Developers Guide*.

Architecture Overview

Voice, video, and Expert Assist sessions in RE Mobile are created from mobile and web applications that embed the RE Mobile Client SDK (CSDK). These communications traverse securely “over-the-top” of the Internet into the Enterprise network to experts utilizing a Cisco UC and Contact Center infrastructure. The firewall and Reverse Proxy permit the session signaling to access the RE Mobile server component known as the Remote Expert Mobile Application Server (REAS). Voice and video media traverse through the DMZ to the RE Mobile server component known as the Remote Expert Media Broker (REMB).

Figure 1. Core Remote Expert Mobile Architecture



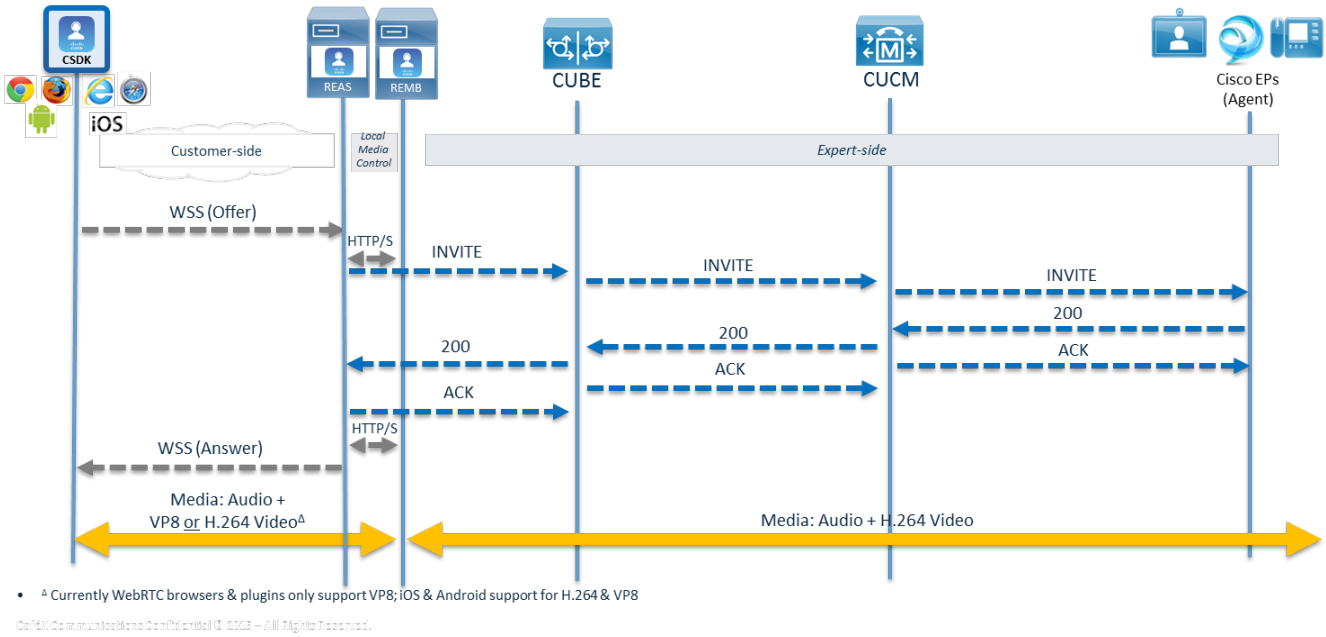
Architectural notes:

- Mobile and web application may be validated with a secure Application ID in order to initiate Remote Expert Mobile sessions, or they may be anonymous
- Signaling traverses the Remote Expert Mobile solution between the mobile and web applications to a SIP server. RE Mobile supports SIP interoperability with either CUBE-E or Cisco Unified CM.
- All media is encrypted between the Remote Expert Mobile Media Broker and the mobile or browser applications utilizing the client SDK.
- The Unified CM cluster provides call control for enterprise network endpoints (local or remote).
- Voice and video media traverses Remote Expert Mobile Media Broker and may be relayed to endpoints directly or thru the UC infrastructure;

Interaction with Cisco Contact Center and Unified Communications Infrastructure

Once an application is authorized to instantiate a session in the CSDK, calls are initiated over secure WebSockets into REAS. Remote Expert Mobile connects to either a Cisco UBE (Unified Border Element), or a Cisco UCM (Unified Communications Manager) using a SIP trunk. REAS will route all initial and subsequent SIP requests into this SIP trunk.

Figure 2. Remote Expert Mobile General Call Flow



In this call flow, the Remote Expert Mobile provides a unique identifier (SIP UUI) within the SIP-header for all messages forward to CUBE or Unified CM to initiate call correlation within the Unified Contact Center Enterprise (Unified CCE) and UC infrastructure. This is specified during session token creation to the REAS.

Remote Expert Mobile Components

Deployment of the RE Mobile OVA results in a Virtual Machine (VM) created with a base CentOS 7.2 operating system. The following products are installed in this VM:

1. Remote Expert Mobile Media Broker (REMB)
2. Remote Expert Mobile Application Server (REAS)
3. Expert Assist Finesse Gadgets for Agent and Supervisors (Finesse Gadgets)
4. Expert Assist Agent Web and Supervisor Consoles (Expert Assist Consoles)

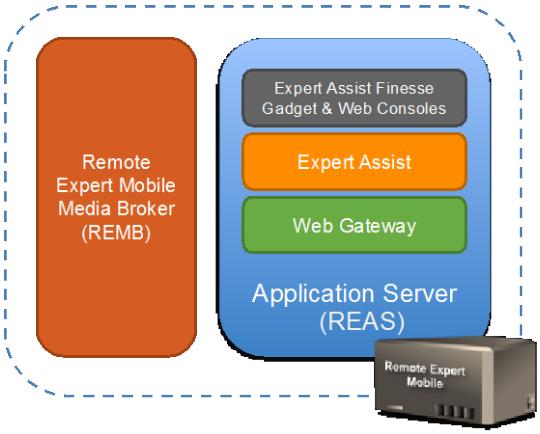


Figure 3. Components of Remote Expert Mobile

Remote Expert Mobile Application Server (REAS)

REAS is an application delivery platform managing HTTP and SIP communication for the Web Gateway and Expert Assist services. Using these services, REAS bridges between Web Browser and mobile clients (using HTTPS and WSS) and the SIP-based UC infrastructure. This enables consumer web and mobile client applications to communicate with the agent contact center.

The RE Mobile Application Server hosts the following:

- WebRTC gateway functionality—this gateway acts as a protocol bridge between the HTTP and WebSocket signaling originating in the consumer network and the SIP signaling of the agent contact center
- Expert Assist services—this delivers the server-side capability needed to deliver co-browsing, screen sharing, document and URL push and annotation features.
- Finesse Gadgets—the Expert Assist Finesse Gadget is an HTML widget accessed by Cisco Finesse over HTTP or HTTPS.
- Expert Assist Web Consoles.

REAS also controls the Remote Expert Media Broker server that relays real-time media between clients inside and outside of the enterprise network.

As the REAS resides in the enterprise's internal "green" zone, it is strongly recommended that you secure the REAS from external traffic by using an HTTP Reverse Proxy in the DMZ.

Remote Expert Mobile Media Broker (REMB)

The Media Broker is a separate standalone process to the REAS. It is responsible for securely bridging media using WebRTC protocols across firewalls and into the SIP network. It handles the termination of STUN and secure DTLS-SRTP media, bandwidth management, WebRTC-specific RTP requirements, and if required transcoding. REMB supports the following codecs:

- Audio codecs: G.711 u-law (μ-law/mu-law) or G.711 A-law, Opus
- Audio transcoding: Opus to G.711 u-law or G.711 a-law, Opus to G.729a, G. G.711 u-law or G.711 a-law to G.729a
- Video codecs: H.264 (up to 720p, 30 fps) and VP8 (up to 720p, 30 fps)
- Video transcoding: H.264 to VP8, VP8 to H.264

The Remote Expert Mobile Media Broker's performance is governed by pass-through and transcoding the media session. Pass-through is a non-transcoded session that utilizes STUN, encryption, decryption, and UDP port multiplexing. Transcoding 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.

Transcoding is an intensive process, so CSDK offers both H.264 native support and VP8 support in the mobile SDKs. As a result, transcoding does not occur when a smartphone or tablet application connects to an H.264 endpoint such as Jabber for Windows, or a Cisco Telepresence.

Browser plug-ins provide H.264 support for Internet Explorer and Safari. Browsers that do not require plug-ins have codec support as follows:

- Chrome supports H264 and VP8.
- Firefox supports H264 and VP8.

Remote Expert Mobile Client SDK (CSDK)

The Remote Expert Mobile Client SDK is used within native mobile and web apps to provide voice, video, and Expert Assist capabilities. See the latest Release Notes for the most accurate CSDK support information.

HTTP Reverse Proxy

The HTTP Reverse Proxy is installed in front of the REAS, in the DMZ. Its function is to secure the enterprise internal zone from external traffic. It adds a layer of security between the public Consumer network and the Application Server by the following methods:

- It hides the internal topology of the network.
- It assists with cross-site origin issues as it presents a single domain for HTTP and WebSockets to the Web Gateway.
- It protects specific services from being exposed externally, for example Management services, and some REST services.
- It terminates in the DMZ the public Consumer network SSL connection—also known as SSL Offloading.

The preferred configuration terminates the HTTPS WebSockets connection at the reverse proxy, and then performs NAT, and load balances the decrypted connection across the Remote Expert Application Servers. Each reverse proxy is explicitly defined to restrict access to only the URIs relating to the WebSocket connections for Remote Expert Mobile.

We recommend that any reverse proxy is configured to perform SSL, offloading to terminate in the DMZ the SSL connection from the Consumer. The only requirement of RE Mobile on the reverse proxy is that it supports WebSockets.

See the reverse proxy documentation for details on configuring SSL If you require the connection between the reverse proxy and Application Server to be secure, see to the RE Mobile Administration Guide. If SIP over TLS is required, the Administration Guide details the necessary configuration.

Key URLs

In a production environment, RE Mobile is normally installed behind a reverse proxy. This means that the IT administrator has to ensure that specific URLs are visible so that clients can access the server resources they need. Refer to the “Cisco Remote Expert Mobile Installation and Configuration Guide” for a detailed listing of URLs to be configured in the reverse proxy.

Other Architectural Components

- Session Border Control and SIP trunking—Cisco Unified Border Element (CUBE)
- Recording and video on hold (VoH), video in queue (ViQ)—Cisco Media Sense
- Queuing and self-service—Cisco Unified Customer Voice Portal (Unified CVP)
- Contact center routing and agent management—Cisco Unified Contact Center Enterprise (UCCE), Cisco Packaged Unified Contact Center Enterprise (PCCE), Cisco Unified Contact Center Express (UCCX)
- Unified Communications infrastructure—Cisco Unified Communications Manager (Unified CM)
- Cisco IP Phone, Telepresence Endpoints and softphones (EP)
- Agent desktop software—Cisco Finesse® desktop
- Cisco LAN and WAN infrastructure
- DNS Server

Interoperability

CSDK Interoperability

Native Mobile App Support in CSDK

Remote Expert Mobile Client SDK supports native Apple iOS applications and Android applications for tablet, phablet, and phone form factors. The native iOS CSDK provides an Objective-C API; the native Android CSDK provides a Java API.

Mobile Device Support

See the Unified CCE Solution Compatibility Matrix (http://docwiki.cisco.com/wiki/Unified_CCE_Solution_Compatibility_Matrix_for_11.5(x)#Remote_Expert_Mobile).

Other Interoperability Requirements

Hardware and System Requirements

A server platform that meets the **Compatibility Guide for VMware vSphere** is required (see http://www.vmware.com). The Cisco Remote Expert Mobile virtual machine uses a 64-bit distribution of CentOS and Oracle Java Development Kit. The server platform must use CPUs that are capable of 64-bit instructions. Refer to the VMware developer documentation for additional configuration and hardware requirements.

We highly recommend using the Cisco Unified Computing System (CUCS) to simplify and maximize performance. See http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment for the current list of supported UCS Tested Reference Configurations and specs-based supported platforms.

License Requirements

Cisco Remote Expert Mobile is a licensed product. Contact a sales representative from a Cisco partner or from Cisco for ordering details. Cisco Remote Expert Mobile is a licensed product, but no license keys are provided or required.

- Third-party software—This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product is available at the following location:

  `http://www.cisco.com/<name-of-product>/products-licensing-information-listing.html`

Requirements for optional Reverse Proxy Server

When using a reverse proxy (strongly recommended), support for HTTPS (HTTP 1.1) and secure WebSocket (WSS) is required. Secure web sockets are used for WebRTC session signaling and Expert Assist co-browse. We have used the open source Nginx (http://nginx.org/), commercial Nginx Plus (http://nginx.com/), and F5 Big IP Local Traffic Manager. The REM solution can use other reverse proxies that meet the stated requirements subject to partner validation.

Required Cisco Unified Communications and Contact Center Infrastructure

Cisco Unified Contact Center products are a combination of strategy and architecture that promote efficient and effective customer communications across a globally capable network by enabling organizations to draw from a broader range of resources to service customers. They include access to a large pool of agents and multiple channels of communication as well as customer self-help tools.

Cisco Unified Communications Manager (Unified CM)

RE Mobile requires Cisco Communications Manager (Unified CM). Cisco Unified Communications Manager is the core call control application at the center of the Cisco collaboration portfolio. It provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management.

Cisco Unified Contact Center Enterprise (Unified CCE)

RE Mobile requires Cisco Unified Contact Center Enterprise (Unified CCE). Cisco Unified Contact Center Enterprise (Unified CCE) provides a VoIP contact center solution that enables you to integrate inbound and outbound voice applications with Internet applications, including real-time chat, web collaboration, and email. This integration provides for unified capabilities, helping a single agent support multiple interactions simultaneously, regardless of the communications channel the customer has chosen. Because each interaction is unique and may require individualized service, Cisco provides contact center solutions to manage each interaction based on virtually any contact attribute. The Unified CCE deployments are typically used for large size contact centers and can support thousands of agents.

Unified CCE employs the following major software components:

- *Call Router*—The Call Router makes all the decisions on how to route a call or customer contact.
- *Logger*—The Logger maintains the system database that stores contact center configurations and temporarily stores historical reporting data for distribution to the data servers. The combination of Call Router and Logger is called the Central Controller.
- *Peripheral Gateway*—The Peripheral Gateway (PG) interfaces to various "peripheral" devices, such as Unified CM, Cisco Unified IP Interactive Voice Response (Unified IP IVR), Unified CVP, or multichannel products. A Peripheral Gateway that interfaces with Unified CM is also referred to as an Agent PG.
- *CTI Server and CTI Object Server (CTI OS)*—The CTI Server and CTI Object Server interface with the agent desktops. Agent desktops can be based on the Cisco Agent Desktop (CAD) solution, Cisco CTI Desktop Toolkit, Finesse desktop, or customer relationship management (CRM) connectors to third-party CRM applications.
- *Administration and Data Server*—The Administration and Data Server provides a configuration interface as well as real-time and historical data storage.

Cisco Unified Contact Center Express (Unified CCX)

RE Mobile requires Cisco Unified Contact Center Express (Unified CCX). Unified CCX meets the needs of departmental, enterprise branch, or small to medium-sized companies that need easy-to-deploy, easy-to-use, highly available, and sophisticated customer interaction management for up to 400 agents. It is designed to enhance the efficiency, availability, and security of customer contact interaction management by supporting a highly available virtual contact center with integrated self-service applications across multiple sites.

Optional Cisco Unified Communications and Contact Center Infrastructure

Cisco MediaSense

Cisco MediaSense is optional, but we recommend it for video in queue and recording applications with Remote Expert Mobile when deployed in conjunction with Cisco Unified Communications Manager and Cisco Unified Border Element.

Cisco Voice Portal (CVP)

When deployed with Unified CCE, CUBE and Unified CM, Cisco Voice Portal (CVP) may be used to provide IP-based personalized self-service and call routing to callers, transparently integrated with the contact center.

Cisco Video Endpoints

- Desk Endpoints: EX-Series, DX-Series
- Telepresence Integrator: C-Series
- Telepresence Integration Solutions: SX-Series
- Softphone: Jabber for Windows, Jabber for Mac.

Tech Tip: In case there is no media (audio or video) after call connection, it might be possible that your IT administrator has blocked specific ports (see External Firewall and NAT Settings). Work with IT to ensure that specific ports required by REM are allowed.

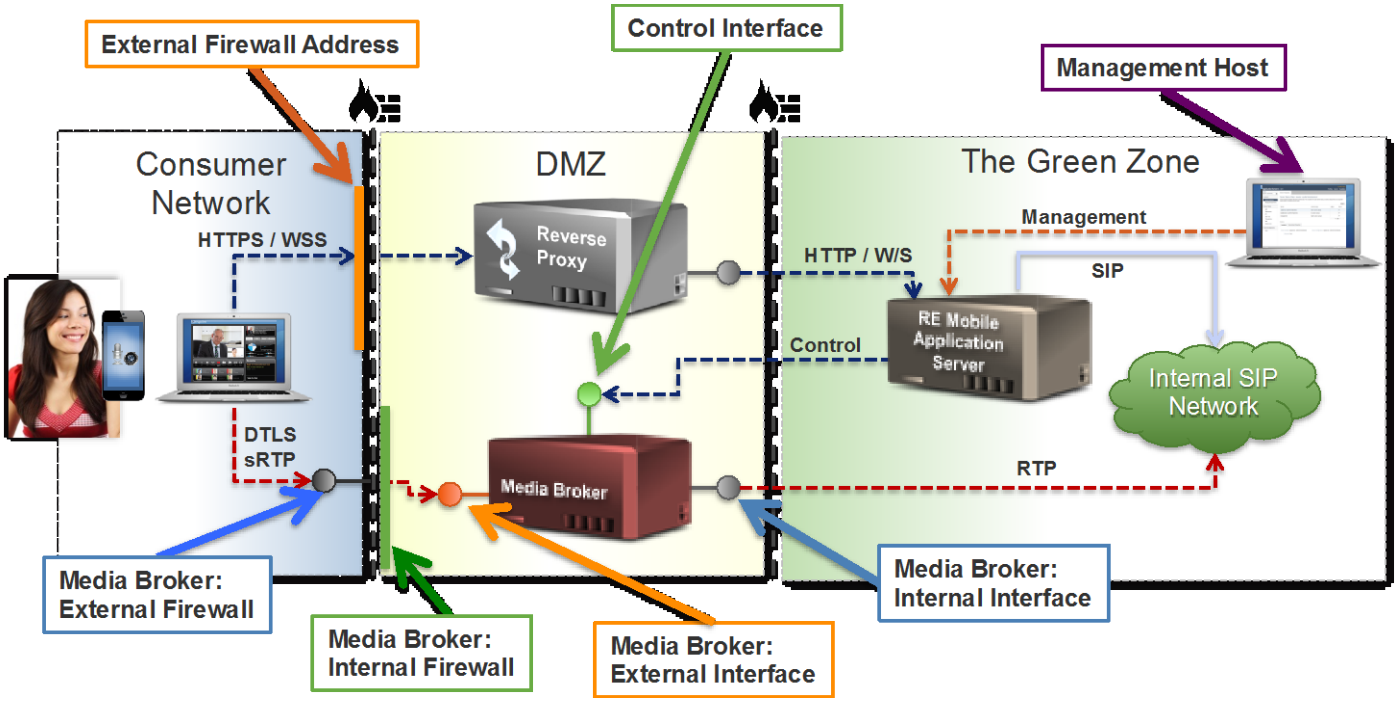
External Firewall and NAT Settings

Only 2 ports are required on the external firewall into the DMZ depending on the application requirements.

- Signaling Protocol: HTTPS (443 default)—The firewall routes all traffic received on port 443 (secure) to the HTTP and Web Socket reverse proxy in the DMZ
- Media Protocol: sRTP/DTLS (16000 default)—It is recommended that multiple ports per Media Broker instance be used for production installations. Typical installations would use 5 ports for each media broker instance. For each call RTP and RTCP will be multiplexed on a single port.

Data Flow and Port Mappings

The diagram below illustrates the different entities referenced in the data-mapping table below.



The data-mapping table below shows the protocols and default ports used for various types of data that flow between entities within the RE Mobile solution.

Data Flow	Initiating Host	Terminating Host	Terminating Port	Protocol	Description
Web	RE Mobile CSDK	External Firewall	443	HTTPS/WSS (TCP)	Client connects to firewall
	External Firewall	Reverse Proxy	Administrator Defined	HTTPS/WSS (TCP)	Firewall forwards request to Reverse Proxy
	Reverse Proxy	REAS	8080	HTTPS/WSS (TCP)	WebSocket requests through firewall
Media Path	REAS	REMB Control Interface	8092	HTTPS (TCP)	Media Broker contacted with control configuration
	RE Mobile CSDK	Media Broker External Firewall	16000-16004	DTSL/sRTP/ RTCP (UDP)	The REM CSDK sends RTP to the External Fire-wall and onto the Media Broker.
	REMB Internal Firewall	REMB External Interface	16000-16004	DTSL/sRTP/ RTCP (UDP)	Media is routed through firewall to Media Broker NB. Media Broker must perform STUN lookup re public client, else RTP will fail.
	REMB Internal Interface	Internal SIP Network	Administrator Defined	RTP/RTCP (UDP)	Media Broker sends RTP to media device e.g. phone
	Internal SIP Network	REMB Internal Interface	17000 - 17099	RTP/RTCP (UDP)	Media device sends RTP to Media Broker
SIP Signaling	REAS	Outbound Proxy	Administrator Defined	SIP (UDP/TCP/TLS)	Web Gateway contacts outbound proxy
	Outbound Proxy	REAS	5061 and 5081	SIP (UDP/TCP/TLS)	Outbound Proxy sends SIP to Web Gateway
Management	Management Host	REAS	8443	HTTPS (TCP)	REAS management
	Management Host	REAS	9990	HTTPS (TCP)	REAS management

Understanding the Network before Deployment

Before beginning the deployment of the OVA, it is necessary to understand the network that it will be deployed into in order to decide which of the available LANs your VM will be connected to.

The OVA offers the ability to configure the deployed VM with up to 3 network interfaces:

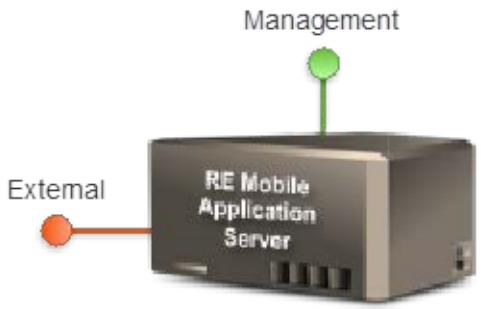
- The first is mandatory—“External”
- An optional second—“Internal”
- And the other optional interface—“Management”

It is important to remember that deploying the OVA will **ALWAYS** create a VM hosting the following components:

- REAS (which hosts the WebRTC Gateway, Expert Assist, Finesse Gadget and Expert Assist Web Console)
- REMB (**Note**: not in Remote Expert Co-browse)

Figure 4. Network Interfaces

These interfaces are used for very different purposes depending on whether they relate to the REAS or REMB.



RE Mobile Application Server (REAS)

External	Internal	Management
• HTTPS, WSS • SIP/SIP TLS, • Web Administration • REMB Control	(Not used)	Control from REAS

RE Mobile Media Broker (REMB)

External	Internal	Management
DTLS sRTP to and from WebRTC client apps	RTP media to and from SIP clients	Control from REAS

The “External” Interface

The “External” interface is mandatory and is mapped to the VM’s first Ethernet network interface card (NIC) `eth0`

Remote Expert Mobile Application Server (REAS)

In terms of each REAS deployed, the external interface transports all its SIP, HTTP(S) and WebSocket traffic between both internal and external clients.

By default, the administration of the REAS (for example, heartbeat traffic between multiple REAS nodes and cluster management traffic) is performed over this interface.

Remote Expert Mobile Media Broker (REMB)

Each REMB binds to the “External” interface and is used for the following:

1. RTP traffic to/from a less-trusted network (for example, the Internet).
2. RTP traffic to/from the enterprise’s internal network. If required, the REMB can be configured to use a separate “Internal” interface for this this internal RTP traffic (for example, voice and video a private enterprise IP network). See The “Internal” Interface section below) if enabled.
3. The Web Gateway typically uses the Media Broker’s “External” interface to configure and control it. See the Internal Interface and Management Interface sections below for details of how to configure the Media Broker to bind to a separate interface to process this control traffic.

Note: not relevant to Remote Expert Co-browse

The “Internal” Interface

The “Internal” interface is an optional configuration item on the OVA. If it is enabled, it is mapped to the `eth1` network interface on the VM, and is used for the following:

Remote Expert Mobile Application Server (REAS)

In terms of each REAS deployed, this interface has no relevance and even if enabled during deployment of the OVA, it is not used.

Remote Expert Mobile Media Broker (REMB)

The Media Broker binds to the “Internal” interface and uses it for the following:

1. Internal RTP traffic.
2. By default, the REMB processes control traffic over its “External” interface. Enabling the “Internal” interface results in the REMB binding to this interface in preference to its “External” interface for control traffic.

Note: not relevant to Remote Expert Co-browse

The “Management” Interface

The “Management” interface is an optional configuration item on the OVA, and if enabled, it is mapped to the `eth2` network interface on the VM.

Remote Expert Mobile Application Server (REAS)

In terms of each REAS deployed, this interface has no has no relevance and should not be used.

Remote Expert Mobile Media Broker (REMB)

Enabling the “Management” interface causes the REMB to use it for “control traffic” in preference to its “Internal” or “External” interfaces.

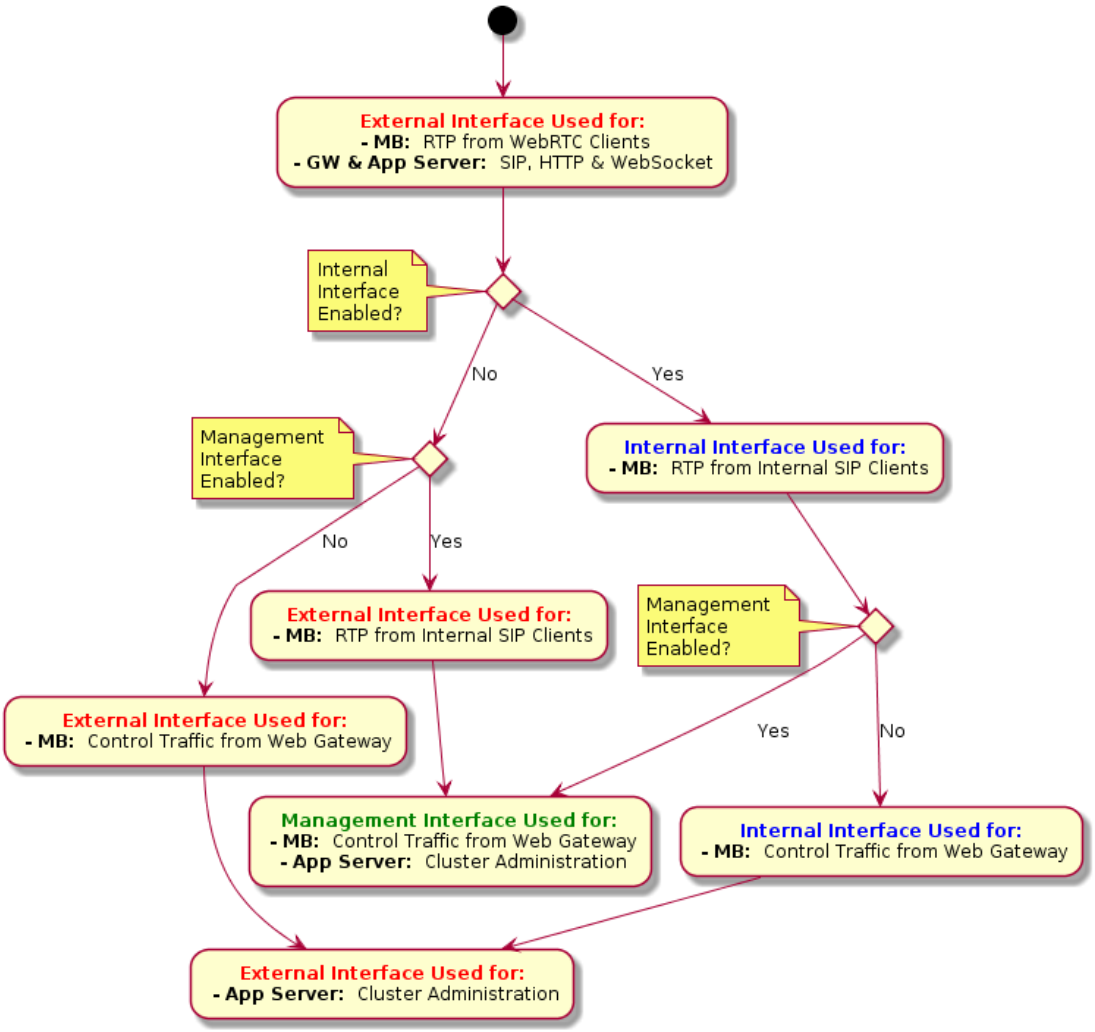
Cluster management may use this interface on port 9990.

Note: not relevant to Remote Expert Co-browse

Interface Usage Decision Flow

The flow diagram below shows the decision tree used by the OVA in determining which of the interfaces is used for particular types of traffic

Figure 5. OVA’s Network Interface Decision Tree



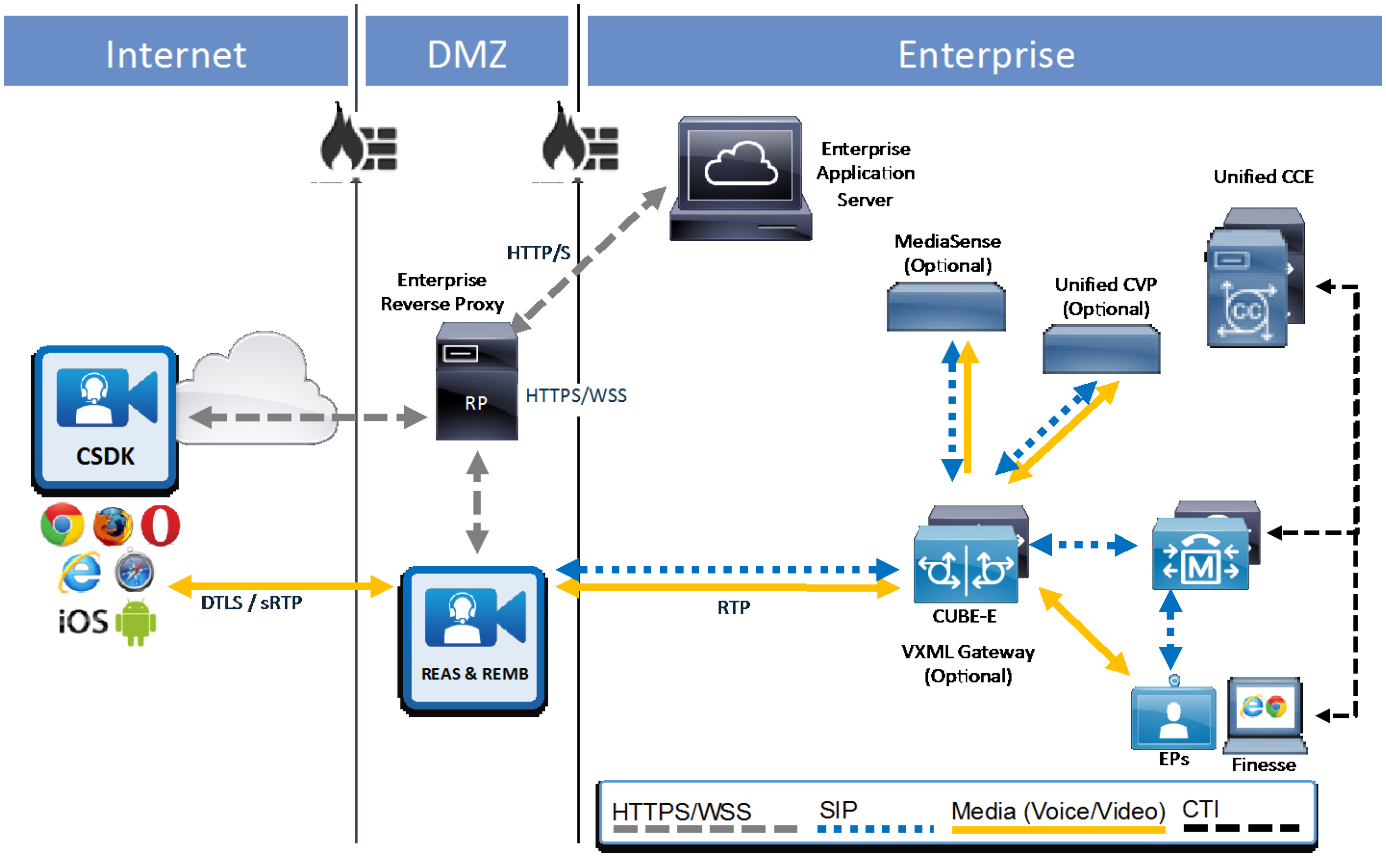
Deployment Scenarios

These deployment scenarios cover the integration to deployments that must include CUBE, P/UCCE and CUCM. This guide does not cover Remote Expert Mobile deployed with a) Unified CCX, CUBE and Unified CM or b) exclusively with Unified CM

Single Master Node

Using the OVA template, Remote Expert Mobile can easily be setup in a single VM with both REAS and REMB service running concurrently for small deployments running up to 10 concurrent sessions.

Figure 6. Remote Expert Mobile Single Master Node



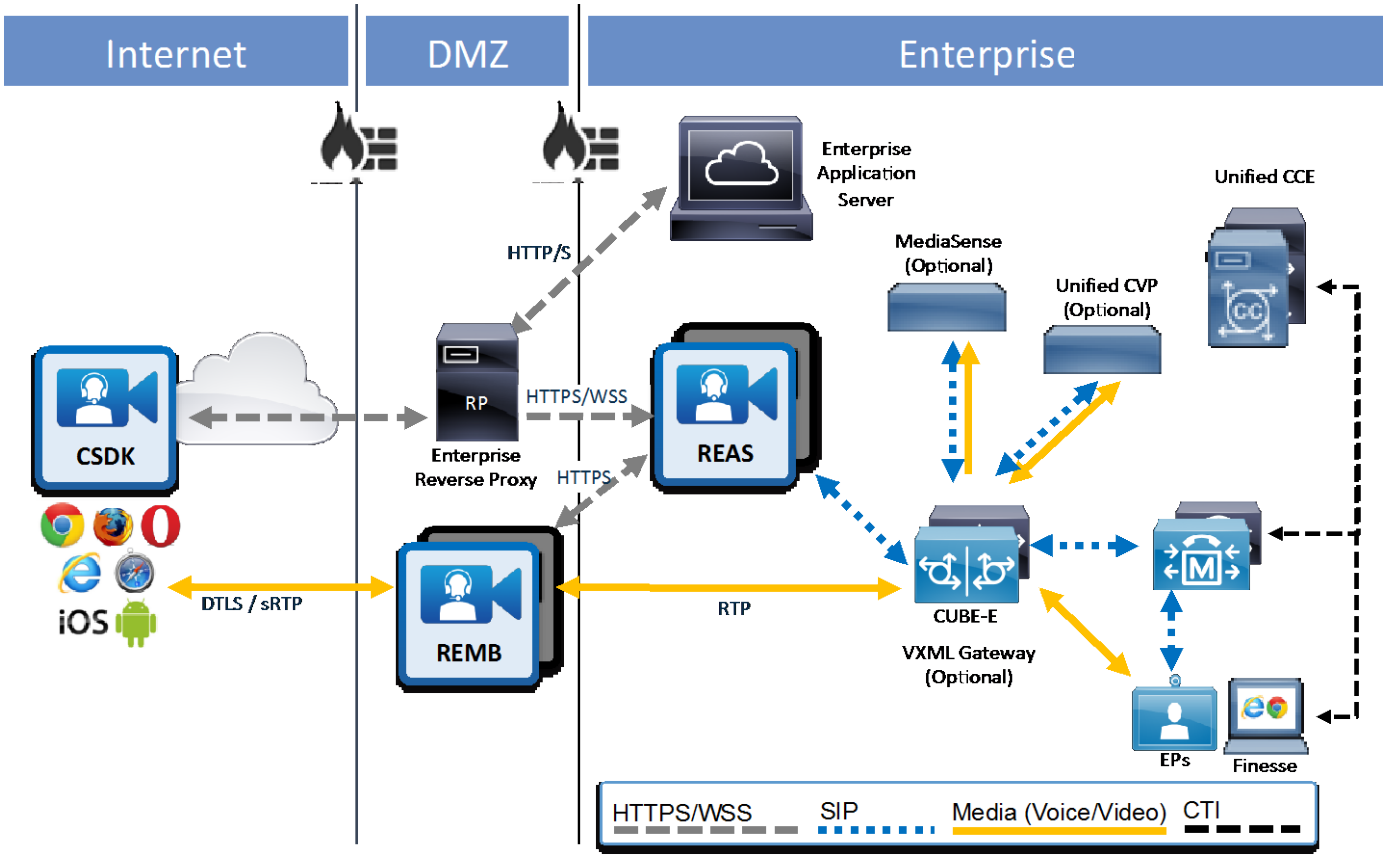
Note: Single Non-HA Master deployments should only be used for non-critical development or lab systems.

Base HA Multi-node Deployment

Remote Expert Mobile **Base HA Multi-node Deployment** has 4 nodes (2 REAS and 2 REMB) and supports simultaneous concurrent video, audio, and expert sessions in a high-availability configuration.

In this deployment, one REAS node acts as a master node and the second is a slave node. Media sessions allocated by the Application Server are load-balanced across the two Media Brokers. In order to maximize the number of media session that traverse the media broker, criteria for load balancing media sessions is round-robin across the REMBs, as well as based on REMB CPU utilization.

Figure 7. Remote Expert Base HA Multi-node Deployment



Note: Every Remote Expert Mobile Application Server cluster must consist of a single master node and a second instance that is a slave node. The master node must be created prior to slave nodes being created.

Scaling the deployment to handle more sessions, calls and media

In a high-availability (HA) installation, each REAS must be installed on a separate VM instance. A Remote Expert Mobile deployment can scale the cluster by adding more media brokers as needed (and if required, REAS). See Sizing Remote Expert Mobile Virtual Machines on page 33 for more information.

Deployment Across Multiple Data Centers

We recommend that all nodes in an REAS cluster (consisting of one or more REAS nodes and associated REMB nodes) should be on the same LAN subnet. Deployment of a cluster across a WAN or multiple data centers is not supported.

High Availability

The Base HA Multi-node Deployment with two Remote Expert Mobile Application Servers and two Remote Expert Mobile Media Broker Nodes applications supports high availability, so that if a component fails, the services continue.

Remote Expert Mobile does not provide resiliency for active calls.

In a REAS cluster, data is replicated between nodes using Infinispan-replicated caches. Nodes replicate transaction and dialogue state information sufficient for another node to reconstitute the sessions maintained by a failed node (SIP, Application, and HTTP), and to process subsequent transactions for those sessions, be they SIP or HTTP requests. To support failover of SIP sessions, the dialogue state maintained by the stack must also be replicated between all REAS nodes. This session information is replicated atomically within the context of a SIP session at any of the following replication points:

- After processing the final response to a SIP request.
- After processing an ACK.
- After processing a Servlet Timer.
- After processing an HTTP request.
- After a session is invalidated.

Stored information is removed from the cache when the session is invalidated, or when the timer fires or is cancelled.

Component	Failover Scenario	New call impact	Active call impact	Post recovery action
REAS	Network Failure	With a black-hole network event there is a period of time, in the region of 30 - 90 seconds under testing load, where the remaining node is unresponsive while various network aspects time-out and update themselves. During this time new calls will pause in the 'connecting' phase and may need to be re-requested after the remaining node has started responding normally again. In exceptional circumstances where a reachable appserver process is heavily loaded but a reachable loadbalancer is not, the reachable aspects of the cluster may require a restart before a call can be made.	During the initial unresponsive period after a black-hole event active calls will lose call control, but the voice and video persist. If not accessing the Expert Assist agent console through a reverse proxy that handles HA failure of WebSocket and the browser has connected to a node that suffers a black-hole event, then the agent console will most likely become unresponsive and the call will 'hang'. For all other failures the active call impact should reflect that of REAS failover scenarios. When the network condition is resolved and the cluster re-syncs it is possible that the call will be dropped and the agents logged out of the system.	If the agent console becomes unresponsive then a page-refresh will be required in the browser, followed by the agent logging back in to the agent console. The consumer will need to manually end the call as well in this scenario.
REMB	Internal Network Failure	None	Video and audio freeze. Expert assist session persists and is fully operational.	Call needs to be manually ended and the consumer needs to call the agent again.
	External Network Failure	None	Video and audio freeze. After a few seconds the CSDK and Expert Assist sessions are ended and tidied up. The	The consumer needs to call the agent again.

Component	Failover Scenario	New call impact	Active call impact	Post recovery action
			consumer is displayed the 'Failed to establish call' error.	
	Management Network failure	None	Both agent and consumer sessions ended and tidied up as with a normal call end.	The consumer needs to call the agent again.
REAS	REAS Service Failure on the active call processing node	New calls establish correctly with full CSDK and Expert Assist functionality. * If the consumer navigates away from Expert Assist pages and then returns they may be unable to drag the video window; they can otherwise interact fully with it and the agent retains the ability to drag via the co-browse feature.	Audio and video are maintained. However, the co-browse session gets frozen. After agent leaves co-browse voice/video will continue to work but other features such as co-browse and doc share won't be available for the rest of call. Co-browse will function on subsequent calls.. Pushing a document does not work and results in a document view with 0 width and 0 height appearing in the top-left corner of the consumer screen. * If the consumer navigates away from Expert Assist pages and then returns they may be unable to drag the video window; they can otherwise interact fully with it and the agent retains the ability to drag via the co-browse feature. When the call is ended the agent will be logged out of the console and they will need to log back in.	The agent will need to log back in to the Expert Assist console
	REAS Service Failure on the non-active call processing node	None	The video and screen-share session persist, with fully-functional annotations and co-browsing. There is the potential for a temporary interruption to the screen-share; if this occurs then the session should re-connect automatically. Pushing a document does not work and results in a document view with 0 width and 0 height appearing in the top-left corner of the consumer screen. When the call is ended the agent will be logged out of the console and they will need to log back in.	The agent will need to log back in to the Expert Assist console

Component	Failover Scenario	New call impact	Active call impact	Post recovery action
REMB	REMB Failure on an active call processing node	None	Each side of the call is handled differently, so this is split in 3: Agent call, Consumer call, both calls. Agent call: The consumer side is ended and cleared up as it would be for a normal call end. The agent's CSDK and Expert Assist calls are ended but the console thinks it's still in a call, displaying the consumer connection error. Consumer call: CSDK and Expert Assist sessions are ended and tidied up. The consumer is displayed the 'Failed to establish call' error. Both calls: CSDK and Expert Assist sessions are ended and tidied up. The consumer is displayed the 'Failed to establish call' error.	If the agent console thinks it's still in a call then the agent will need to manually end the call or reload the page. The consumer needs to call the agent again.
	REMB Failure on a non-active call processing node	None	None	None

Failover

REAS failover

All REAS nodes join an Infinispan cache, which is used to detect failover between nodes. At any one time, the cache will have one coordinator node, which is ordinarily the oldest member of the cache.

In a REAS failure in the Base HA Multi-node deployment with two REAS nodes, 100% of the session signaling capacity is maintained.

A REAS failure is detected using several failure-detection mechanisms including a configurable heartbeat mechanism and monitoring connected TCP sockets to detect when a node is no longer reachable. When a node failure is detected, the coordinator is notified of the failure and given a list of the remaining nodes. In turn, the nodes reconstitute the sessions for the failed REAS, and schedule any servlet timers and expiry timers. Calls that were in the middle of a transaction when the node failed but a final response had not yet been processed are not generally recoverable; and calls are cleaned up after failover.

REMB failover

When a Remote Expert Mobile Media Broker fails, ongoing calls are dropped. The call is cleared on both the Agent and the Customer side. Subsequent calls are serviced by being directed to all available REMB nodes.

A REMB failure in the Base HA Multi-node deployment with two REMB nodes, degrades the system to 50% of the session media capacity. To maintain 100% of the capacity we recommend an N+1 redundancy for REMB nodes. Or, in the case of the Base HA Multi-node deployment, adding a 3rd REMB node will maintain 100% of the media capacity.

Other Scenarios

Network Disconnect of Customer During Co-Browse

On a network disconnect of a customer during co-browse, the call clears on the agent side. However the customer’s video window is frozen and they do not get any notification that a disconnect has happened. After re-connecting the network, the customer’s video window remains frozen until the call is disconnected manually.

Customer Closes Browser During Active Call

On closing the browser during a co-browse session, the customer will see that the audio remains active, but the video window stops and the co-browse session ends. The customer's video is still seen on the agent’s end, however since the customer's video window has stopped, he is unable to see the agent’s video.

Clearing Existing Annotations

All existing annotations are cleared under the following circumstances:

- When an additional agent joins a co-browse
- When an agent puts a call on hold, then retrieves the call

Securing Remote Expert Mobile

Encrypted signaling and media

To ensure security of all communications from application that have incorporated the CSDK, RE Mobile employs various encryption methods to ensure the privacy of all data to the REAS and REMB.

- Client Side (CSDK)—all over-the-top communications are secured through HTTPS, Secure WebSockets and DTLS sRTP.
  - HTTPS to REAS or Reverse proxy (Signaling)
  - Secure WebSockets to REAS or Reverse proxy (Signaling)
  - DTLS / sRTP to REMB (Media (RTCP and RTP)

To ensure security within the enterprise, the WebRTC gateway encrypts SIP signaling to the CUBE or CUCM

- Enterprise side
  - SIP TLS (SIP signaling)

Note: For Remote Expert Co-browse, DTLS sRTP and SIP signaling will not need to be secured on REAS, nor will any other communication between REAS and REMB. Of course, SIP traffic should be secured on other entities which use it, such as CUBE or CUCM.

Credentials

The setup script prompts you for the different levels of users to operate the system. The default user names are as follows:

- REM OS User—rem-user
- REM OS Admin User—rem-admin
- SSH OS User—rem-ssh

We strongly suggest that you use and maintain secure credentials for these users, and change all default security details after installing the OVA, including the following:

- SSL Keys
- SSL Keystore

See also:

- *Cisco Remote Expert Mobile—Install and Config Guide > REM Users and Security*
- *Cisco Remote Expert Mobile—Install and Config Guide > Changing Passwords*

Guidelines for Updating Security Patches

We understand that it may be necessary to patch the OS with security updates. We endeavor to support customers who apply security patches and we expect the product to function correctly when patches are applied. In the unlikely event that a security patch is incompatible with the product and it is not possible to update the product to resolve this then you may be asked to revert it.

As a precaution, please update/test these security patches in UAT/Test environment and ensure that REM is running/functioning as expected before update the same into production REM boxes. After successful test, in case of any issues found in the production then please remove those patches.

REM picks up latest OS and other patches during every maintenance and major/minor releases.

We would recommend customers to wait for the MR and minor/major releases unless it is a critical and *must-have* security OS patch.

The CentOS Release version that is incorporated into any major, minor, MR FCS OVA will contain all of the available patches up until the FCS date. The established FCS CentOS release version will be identified in the associated REM Release Notes.

SSL Keys

By default, REAS is configured to use Transport Layer Security (TLS). Using TLS enables servers to verify the identities of both the server and client through exchange and validation of their digital certificates, as well as encrypt information exchanged between secure servers using public key cryptography, ensuring secure confidential communication between two entities. Data is secured using key pairs containing a public key and a private key.

VM Specifications and Constraints

Along with Linux operating system and 64-bit Java, the RE Mobile OVA template includes the Remote Expert Mobile Application Server, Remote Expert Mobile Media Broker, Remote Expert Mobile Client SDKs, Expert Assist and the Expert Assist Finesse gadget.

VMware vSphere Support

The following VMware vSphere features are supported:

- VM OVA template deployment (using the Cisco-provided Cisco Remote Expert Mobile OVA)

You can restart Cisco Remote Expert Mobile on a different VMware vSphere or ESXi host and create or revert VMware Snapshots as long as the application was shut down without issues before moving or taking a snapshot.

The following VMware vSphere features have not been tested with Cisco Remote Expert Mobile

- VMware vMotion
- VMware Virtual Machine Snapshots
- VMware vSphere Distributed Switch (vDS)
- VMware Dynamic Resource Scheduler (DRS)
- VMware Storage vMotion (Storage DRS)
- VMware Site Recovery Manager (SRM)
- VMware Consolidated Backup (VCB)
- VMware Data Recovery (VDR)
- Long Distance vMotion (vMotion over a WAN)
- VMware Fault Tolerance (FT)

The following VMware vSphere and third-party features are not supported with Cisco Remote Expert Mobile:

- VMware Hot Add
- Copying a Cisco Remote Expert Mobile virtual machine (must use OVA to deploy new server)
- Third-party Virtual to Physical (V2P) migration tools
- Third-party deployment tool

Virtual Machine (OVA) Specifications

For more information regarding Virtual machine installation and configuration, see the following:

- *Remote Expert Mobile—Installation and Configuration Guide*

If using a UCS Tested Reference Configuration or a specifications-based system, the minimum requirements are the following:

For development systems:

Deployment type	vCPU	Reserved CPU resource	RAM	Disk space	NIC
Singlebox OVA (Developer)	4 core	8400 MHz (4 x 2.1 GHz)	6 GB	40 GB	1 Gb

For production systems:

Deployment type	vCPU	Reserved CPU resource	RAM	Disk space	NIC
Small OVA (typical installation)	4 core	8400 MHz (4 x 2.1 GHz)	4 GB	40 GB	1 Gb
Large OVA (extra performance and scalability capabilities)	8 core	16800 MHz (8 x 2.1 GHz)	8 GB	40 GB	2 x 1 Gb or 10 Gb

See the VMware developer documentation for additional configuration and hardware requirements. We highly recommend using the Cisco Unified Computing System (CUCS) to simplify and maximize performance.
See http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment for the current list of supported UCS Tested Reference Configurations and specifications-based supported platforms.

Ensure the following:

- VT is enabled in the BIOS before installing VMware ESXi
- the VM host **Virtual Machine Startup/Shutdown** is configured to **Allow Virtual machines to start and stop automatically with the system**,

Co-residency support

Remote Expert Mobile can co-reside with other applications (VMs occupying same host) subject to the following conditions:

- No oversubscription of CPU: 1:1 allocation of vCPU to physical cores must be used
- No oversubscription of RAM: 1:1 allocation of vRAM to physical memory
- Sharing disk storage

Sizing Remote Expert Mobile Virtual Machines

Remote Expert Mobile Application Server (REAS)

A REAS node can be deployed in a small OVA. A single REAS should support up to 500 concurrent voice / video sessions and up to 200 concurrent expert assist sessions.

REAS Platform	vCPU	Video and Audio Non-Transcoded Sessions	Video and Audio Transcoded Sessions	Audio-Only Non-Transcoded Sessions	Audio-Only Transcoded Sessions	Expert Assist Sessions
Small OVA	4 core	500 per node (signaling only)	0 per node	0 per node	0 per node	200 per node
		0 per node	500 per node (signaling only)	0 per node	0 per node	200 per node
		0 per node	0 per node	500 per node (signaling only)	0 per node	200 per node
		0 per node	0 per node	0 per node	500 per node (signaling only)	200 per node
		0 per node	0 per node	0 per node	0 per node	200 per node

Typical performance on a REAS (network figures in mega*bits* per second; disk figures in kilo*bytes* per second):

- Network I/O in and out: 40 mbps
- Disk write: 10 kBps
  Disk read: negligible (on average)

Remote Expert Mobile Media Broker (REMB)

A REMB node can be deployed in a Large OVA. REMB node performance for passing through encrypted audio and video, transcoding video between VP8 and H.264, or transcoding audio between Opus/G.711 and G.711/G.729, varies depending on video resolution, frame rate, bitrate as well as server type, virtualization or bare metal OS installs, processors as well as codec types. However, general guidelines for individual REMB nodes are as follows.
Note: Expert Assist sessions only flow through REAS nodes.

REMB Platform	vCPU	Video and Audio Non-Transcoded Sessions	Video and Audio Non-Transcoded Sessions	Audio-Only Non-Transcoded Sessions	Audio-Only Transcoded Sessions	Expert Assist Sessions
Large OVA	8 core	125 per node	0 per node	0 per node	0 per node	N/A
		60 per node	5 per node	0 per node	0 per node	N/A
		0 per node	10 per node	0 per node	0 per node	N/A
		0 per node	0 per node	250 per node	0 per node	N/A
		0 per node	0 per node	0 per node	25 per node	N/A

Typical performance on an REMB (network figures in mega*bits* per second; disk figures in kilo*bytes* per second):

- Network I/O in and out: 500 mbps
- Disk write: 300 kBps
  Disk read: negligible (on average)

Scale of Full-Feature Remote Expert Mobile Deployment

	REAS (single node scale)	REMB (single node scale)	Size of Cluster	HA Sessions
RE Mobile Voice/Video	–	125	500	375
RE Mobile Voice-Only	–	250	1000	750
RE Mobile Voice and Expert Assist (No Video)	200	200	600	400
RE Mobile Meet-Me only (RE Co-Browse)	200	–	600	400

Note: Audio-only performance is achieved with video hold disabled in the RE Mobile cluster.
See *Cisco Remote Expert Mobile—Install and Config Guide* > *Expert Assist Configuration—Audio and Video Hold Treatment* > `video.hold.on` setting. See also Audio-Only Calls on page 36.

Remote Expert Mobile Clusters

- Remote Expert Mobile Base HA deployment has 4 nodes (2 REAS and 2 REMB) and can support up to 125 video and audio calls, and 200 co-browse sessions, in a high availability configuration.
- 3 REAS and 4 REMB nodes may be deployed to increase cluster capacity to the following:
  - 600 Expert Assist sessions, or
  - 500 Voice/Video sessions (non-transcoded), or
  - 1,000 Audio-only sessions (non-transcoded).
  - **Note**: In this configuration only 400 Expert Assist sessions, 375 voice & video sessions or 750 sessions will be highly available
- All REAS nodes must use identical OVA templates. REMB nodes should only use the large OVA templates.
- REAS and REMB nodes may be deployed jointly on the same physical server, as long as the server CPU, Memory, and Disk Space are not in contention
- For service continuity, all REAS nodes should not be deployed on the same physical server. All REMB nodes should not be deployed on the same physical server.
- Remote Expert Co-browse sessions use REAS nodes only, and do not require an REMB.

Note: Remote Expert Mobile capacity planning must also consider the capacity of the associated Unified CM clusters and CUBE nodes.

Bandwidth Provisioning and QoS Considerations

Estimating Internet and Unmanaged Network Conditions

CSDK-enabled applications connect to the REAS and REMB 'over the top' (OTT). OTT applications such as Google Hangouts, Microsoft Skype use a variety of techniques such as advanced codecs, jitter buffering and bit-rate control. It is imperative that developers and systems administrators understand the range of network conditions experienced using Remote Expert Mobile applications.

Bandwidth

Bandwidth utilization for voice and video in the enterprise network will be equivalent to that of estimated Internet bandwidth.

Bandwidth needs tends to revolve around the video resolution, frame rate and bit-rate, however the following provides bandwidth guidelines for sessions with voice, video and expert assist.

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

Internet bandwidth purchased from your ISP should be sufficient to support the mix of resolutions and media types consummate to Remote Expert Mobile application use.

While specific applications and websites vary, co-browse runs approximately 100 - 200 Kbps (document, image, file push aside). Be sure to test your own website or mobile application to ensure proper bandwidth allocation to your agents, whether using voice & video and/or co-browse.

QoS

CSDK-enabled applications connected to the Internet will likely not have QoS affiliated with their deployment, as ending will range from laptops, phones and tablets on public Wi-Fi, home and third-party networks, as well as phones and tablets on 4G and 3G networks. RE Mobile Developers may enable their applications to check for connectivity, Wi-Fi strength, and latency prior to a session commencing through a variety of published mechanisms specific to iOS, Android, or web browsers.

Enterprise voice and video communications should run on a network that tags QoS DSCP for SIP messages, RTP and RTCP for media. If QoS is needed for signaling and media traffic across a WAN, configure network routers for QoS using the IP address of the REAS and REMB to classify and mark the traffic. The enterprise network should have zero packet loss and jitter.

For information on voice RTP streams, see Cisco Unified Communications SRND Based on Cisco Unified Communications Manager, at the following URL: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Latency

CSDK-enabled applications connected to the Internet will likely be able to control the latency affiliated with changing network conditions. RE Mobile Developers may enable their applications to check for connectivity, Wi-Fi strength, and latency prior to a session commencing through a variety of published mechanisms specific to iOS, Android or web browsers.

The influence of latency on design varies based on the use of voice, video and screen sharing service considered for remote deployment. For example, a voice service is hosted across a WAN where the one-way latency is 200 ms, users might experience issues such as delay-to-dial or increased media delays. *The maximum recommended round-trip time (RTT) between a REMB and an endpoint (agent phone) on the enterprise network (LAN or WAN) is 100 ms.*

Enterprise Network

Unified Communications and Collaboration over an IP network places strict requirements on IP packet loss, packet delay, and delay variation (or jitter). Therefore, you need to enable most of the Quality of Service (QoS) mechanisms available on Cisco switches and routers throughout the network. For the same reasons, redundant devices and network links that provide quick convergence after network failures or topology changes are also important to ensure a highly available infrastructure.

RE Mobile Component Interconnectivity

RE Mobile supports high availability over LAN to provide redundancy over LAN. In turn, network connectivity inside the datacenter and between RE Mobile nodes must have minimal latency and exceptional quality of services. The maximum allowed round-trip time (RTT) between two REAS master and slave node and between a REAS node and a REMB node is 50 ms.

IPv4

All of the RE Mobile components use IPv4 and interoperate including CUBE-E, Finesse agent desktops, and agent endpoints using IPv4.

Limitations and Restrictions

Supported Upgrade Paths

Cisco Remote Expert Mobile 11.5(1) supports fresh installs via the Remote Expert Mobile OVA, or upgrades from version 10.6(3). For details, see the *Cisco Remote Expert Mobile—Install and Config Guide > Upgrade and Rollback* section.

To obtain software for a fresh install, refer to the following:

- See the *Cisco Unified Communications Applications Ordering Guide*
- Contact your Cisco representative
- Go to http://www.cisco.com

Audio-Only Calls

- Pure audio-only is not supported in any browser in this release—video will always be streamed from the REMB towards browser/WebRTC endpoints. Calls where only the audio part of the connection is used are supported up to the typical performance levels shown in Sizing Remote Expert Mobile Virtual Machines on page 33.
- Audio-only calls are supported in iOS and Android apps

Emergency Service Calls

- Do not use Cisco Remote Expert Mobile for emergency services calls. Do not configure Cisco Remote Expert Mobile to route calls through the public switched telephone network (PSTN) to an emergency response center. If you do, calls may be misdirected or the emergency response center may make errors when determining your location.

Supported Agent Endpoints

- See the Solutions Guide for details of the agent endpoints supported with Cisco Remote Expert Mobile.

MediaSense Recording

With Cisco Remote Expert Mobile, audio recording is supported; video recording and playback is not supported.

iOS Alerts/System Dialog Boxes

Due to limitations imposed by iOS, it is not possible for Cisco Remote Expert Mobile to replicate any iOS generated dialog boxes such as Alert boxes, the iOS keyboard or menus generated by HTML (for example, The popup menu generated by the HTML `<select>` element). Consequently, consider whether it is necessary for the Expert to see those elements, and possibly consider alternative implementations, such as JavaScript and CSS.

Password Fields

When entering a password into a text field on a mobile device, such as iOS or Android, the device briefly display the character that has been entered before masking it. As a user's device screen is being replicated and displayed to an Agent, it may be possible for that Agent to see the password as it is being entered. Consequently, we recommend that you mask fields that can contain sensitive information, using the built-in masking capabilities provided by each Assist SDK.

Unified CM Parallel Hunt Groups and Auto-answer are not supported

In a UC-only deployment (that is, Unified CM), Cisco Remote Expert Mobile does not support Parallel Hunt Groups and Auto-answer. Attempting to use them may result in misdirected calls; the agent's browser will require a complete refresh or restart to recommence taking voice and Expert Assist sessions.

Perceived low volume on some Android devices

In some cases, low volume may be perceived in an associated Cisco Remote Expert Mobile Android application. Developers should refer to useful Android API documentation to rectify this issue and handle audio appropriately for the correct audio output speaker (earphone or speakerphone):

- http://developer.android.com/training/managing-audio/index.html
- http://developer.android.com/training/managing-audio/audio-output.htmlhttp://developer.android.com/training/managing-audio/audio-output.html

For developers using the sample applications provided with Cisco Remote Expert Mobile, see the `InCallActivity: setSpeakerphoneOn` method. When using an Android phone form factor, developers will need to make some explicit calls to the Android AudioManager to get the audio routed to the speakerphone.

With a tablet, the audio should automatically go to the speaker (as long as a headset is not plugged in). If audio is still low, then check all the volume sliders in Settings. Some Android devices have bugs with speaker volume (for example, HTC on Android 4.4).

Local authentication is not enabled after upgrade

After upgrading from REM Mobile 10.6(3) to 11.5(1), local authentication is no longer enabled; this is expected behavior—verify the setting, and enable local authentication, if required.

Android performance

The Android SDK only comes with native libraries for the ARM architecture. Cisco Remote Expert Mobile applications run slowly on devices running on x86 architectures.

The quality of the video sent and received may be poorer on low-specification Android devices. This is especially true if such a device is trying to send and receive full HD video – in such a scenario it may become overloaded.

Volume slider automatically adjusts on some Windows devices

Cisco Remote Expert Mobile customer-side applications on a Windows PC may experience the call volume being reduced substantially when the call is established. By default, some versions of Windows automatically reduce the system volume when they detect that the PC is trying to make or receive phone calls. The default behavior of these versions of Windows is to reduce the volume by 80%, and you should change this.

This may be addressed in the Control Panel: open the **Sound** applet, or access it directly using **Start > Run > mmsys.cpl**, or right-click on the Volume control option in the taskbar and select **Sounds;** then go to **Communications** tab, check the option **Do nothing**, and click **Apply**.

Finesse Required Port Configuration

See the Cisco Remote Expert Mobile Installation and Configuration Guide, when configuring the Finesse server in the Cisco Remote Expert Mobile Administration web console.

```
https://<reas-address>:8443/web_plugin_framework/webcontroller
```

on the “Agent Consoles” tab, the port must be explicitly changed to 8445 for Finesse Server.

```
https://<finesse_server_fqdn>:8445
```
(for example `https://finesse_server1.cisco.com:8445`)

Javascript

- PDF documents with embedded fonts may not render correctly.
- Elements styled with CSS3 Animations may not appear in the Agent Co-browse.
- CSS3 Button Styles do not appear in the Agent Co-browse.
- `<canvas>` elements do not appear on the Agent Co-browse.
- Some HTML5 Input Types may not appear in the Agent Co-browse.
- Content within an iFrame that is inside a Live Assist enabled page do not appear in the Agent Co-browse.
- Page content loaded from another domain to the origin may not appear in the Agent Co-browse.
- Embedded PDF documents do not appear in the Agent Co-browse.

iOS

- Not all moveable elements can be moved by a Live Assist Agent using the co-browse.
- iOS SDK is unable to process incoming calls that are answered immediately
- Web browsers are not supported on mobile platforms—this includes Chrome and Firefox.

Android

- Native fields cannot be edited using the Agent Form Editor or using the co-browse area.
- The Agent Form Editor does not appear for native Android UI Views (for example, radio buttons, and checkboxes)
- The Agent Form Editor will not appear for Web Views that have been loaded as a UI Fragment.
- Android `phone.setCamera` has no effect during a call. Calling `setCamera` during a call has no effect. However, calling `setCamera` before making a call sets the camera correctly for the subsequent call.
- Web browsers are not supported on mobile platforms—this includes Chrome and Firefox.

Loading Finesse Gadgets

The mechanisms by which gadgets such as Expert Assist should load Finesse hosted assets (`finesse.js` and `jquery`) has changed—Finesse now provides these assets, so the Expert Assist gadget should load these assets from a different location.

For example, use:

Agent:

```
<gadget>https:// <reas-address>:8443/finesse_assist_gadget/
FinesseAssist.xml?finesseVersion=11.5.1</gadget>
```

Supervisor:

```
<gadget>https:// <reas-address>:8443/finesse_assist_admin_gadget/
FinesseAssistAdmin.xml?finesseVersion=11.5.1</gadget>
```

Form Filling

- In both the Expert Assist Console and Finesse Gadget, the form filling functionality can allow the agent to bypass some types of browser-based form validation. The agent should take care to ensure that only valid values are entered.

Document Push

- Be aware that large PDF documents may take 10 or more seconds to render to the customer and agent; supports HTTP or HTTPS URLs only, not FTP.

Browser Plug-ins

- Support VP8 and h.264 video.
- Internet Explorer Compatibility view—we do not support using this setting.
- Microsoft has released a cumulative security update for Internet Explorer (KB3058515), which appears to require higher privileges in order to install the *Cisco Remote Expert Mobile* IE plug-in. The user is prompted to download and install the plug-in, but the installation never completes.
  If you launch the browser developer console, you will see the message "Waiting for BHO" displayed repeatedly.

  Workaround:
  Ensure that Internet Explorer is run as an administrator. From the Start Menu right click on "Internet Explorer" and choose "Run as Administrator" from the drop-down menu. The plug-in should install.
- If you are unable to log in using some versions of Internet Explorer, please ensure that you have set the IT policy correctly:

  For a Windows user without administrative privileges, the IT policy must allow for ActiveX controls to be installed. The following configuration should be carried out by the IT administrator or a local user with Administrator privileges. Full details on this configuration can be found at the following URL:

  http://technet.microsoft.com/en-gb/library/dd631688(v=ws.10).aspx

  1. In the Start menu search box, type `gpedit.msc` and press **Enter**.
  2. In the policy editor, go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > ActiveX Installer Service**.
  3. Open **Approved Installation Sites For ActiveX Controls**.
  4. Check the **Enabled** radio button.

5. In the Options pane, click the **Show** button.
6. In the Host URLs table, add `http://<fas-server>` as the value name, and `2,2,1,0` as the value.

   `<fas-server>` should be the machine from which the ActiveX control is served. The `2,2,1,0` string is an example that specifies the policy for downloading ActiveX controls from that server—see the *Technet* page above for details.

   If non-administrative users still experience problems installing the ActiveX control, then you may need to add the FAS server to the IE trusted sites zone, and ensure that the security settings for that zone allow for the downloading of ActiveX controls.

- See also: Remote Expert Co-browse

Cisco Remote Expert Mobile Application Server (REAS)

- The following codecs can cause media or call setup failures—in the REAS Admin UI, ensure that the following are included in the list of banned codecs:
  - G722
  - iLBC
  - CN
  - isac
  - g7221
  - MP4A-LATM

Cisco Remote Expert Mobile Media Broker (REMB)

- Certain video endpoints cannot render 720x1280 video, that is, 720p in portrait mode, for example from a mobile device.

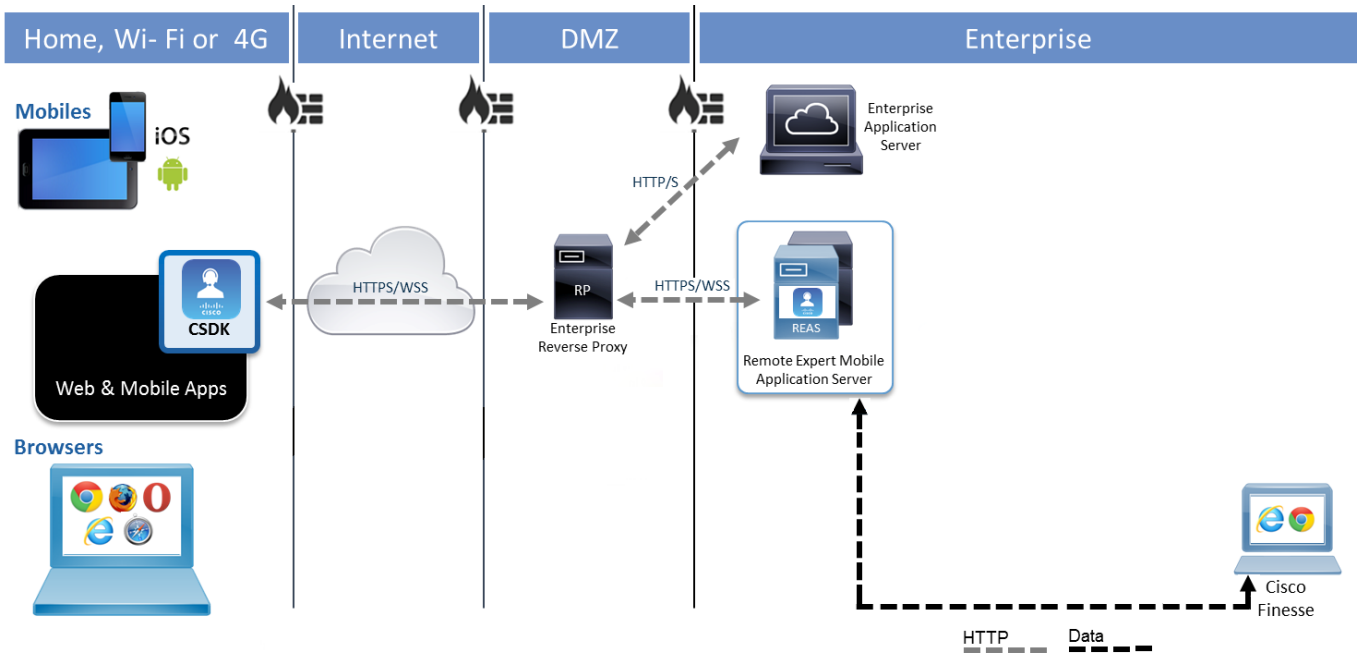
  Workaround:
  Either ensure that the video stream from the mobile device cannot be rotated into portrait mode, or update the Video Resolution Configuration section of the Media Configuration through the Admin UI or CLI to restrict the possible dimensions of the image.

Remote Expert Co-browse

Architecture Overview

Expert Assist sessions in RE Mobile are created from mobile and web applications that embed the RE Mobile Client SDK (CSDK). These communications traverse securely “over-the-top” of the Internet into the Enterprise network to experts utilizing a Cisco UC and Contact Center infrastructure. The firewall and Reverse Proxy permit the session signaling to access the RE Mobile server component known as the Remote Expert Mobile Application Server (REAS).

Figure 8. Core Remote Expert Mobile Architecture



Architectural notes:

- Mobile and web application may be validated with a secure Application ID in order to initiate Remote Expert Mobile sessions, or they may be anonymous
- The Unified CM cluster provides call control for enterprise network endpoints (local or remote).
- Voice and video traffic (SIP and RTP) are independent of the REAS.

Remote Expert Mobile Components

Deployment of the RE Mobile OVA results in a Virtual Machine (VM) created with a base CentOS 7.2 operating system. The following products are installed in this VM:

1. Remote Expert Mobile Application Server (REAS)
2. Expert Assist Finesse Gadgets for Agent and Supervisors (Finesse Gadgets)
3. Expert Assist Agent Web and Supervisor Consoles (Expert Assist Consoles)

Remote Expert Mobile Application Server (REAS)

REAS acts as an application delivery platform managing HTTP communication for the Expert Assist service. This enables consumer web and mobile client applications to share their screen with an agent.

The RE Mobile Application Server hosts the following:

- Expert Assist services—this delivers the server-side capability needed to deliver co-browsing, screen sharing, document and URL push and annotation features.
- Finesse Gadgets—the Expert Assist Finesse Gadget is an HTML widget accessed by Cisco Finesse over HTTP or HTTPS.
- Expert Assist Web Consoles.

As the REAS resides in the enterprise's internal "green" zone, it is strongly recommended that you secure the REAS from external traffic by using an HTTP Reverse Proxy in the DMZ. See HTTP Reverse Proxy.

Remote Expert Mobile Client SDK (CSDK)

The Remote Expert Mobile Client SDK is used within native mobile and web apps to provide voice, video, and Expert Assist capabilities. See the latest Release Notes for the most accurate CSDK support information.

Interoperability

CSDK Interoperability

Native Mobile App Support in CSDK

Remote Expert Mobile Client SDK supports native Apple iOS applications and Android applications for tablet, phablet, and phone form factors. The native iOS CSDK provides an Objective-C API; the native Android CSDK provides a Java API.

Mobile Device Support

See the Unified CCE Solution Compatibility Matrix (http://docwiki.cisco.com/wiki/Unified_CCE_Solution_Compatibility_Matrix_for_11.5(x)#Remote_Expert_Mobile).

Other Interoperability Requirements

Hardware and System Requirements

A server platform that meets the **Compatibility Guide for VMware vSphere** is required (see http://www.vmware.com). The Cisco Remote Expert Mobile virtual machine uses a 64-bit distribution of CentOS and Oracle Java Development Kit. The server platform must use CPUs that are capable of 64-bit instructions. Refer to the VMware developer documentation for additional configuration and hardware requirements.

We highly recommend using the Cisco Unified Computing System (CUCS) to simplify and maximize performance. See http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment for the current list of supported UCS Tested Reference Configurations and specs-based supported platforms.

License Requirements

Cisco Remote Expert Mobile is a licensed product. Contact a sales representative from a Cisco partner or from Cisco for ordering details. Cisco Remote Expert Mobile is a licensed product, but no license keys are provided or required.

- Third-party software—This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product is available at the following location:

  `http://www.cisco.com/<name-of-product>/products-licensing-information-listing.html`

Requirements for optional Reverse Proxy Server

When using a reverse proxy (strongly recommended), support for HTTPS (HTTP 1.1) and secure WebSocket (WSS) is required. Secure web sockets are used for WebRTC session signaling and Expert Assist co-browse. We have used the open source Nginx (http://nginx.org/), commercial Nginx Plus (http://nginx.com/), and F5 Big IP Local Traffic Manager. The REM solution can use other reverse proxies that meet the stated requirements subject to partner validation.

Required Cisco Unified Communications and Contact Center Infrastructure

Cisco Unified Contact Center products are a combination of strategy and architecture that promote efficient and effective customer communications across a globally capable network by enabling organizations to draw from a broader range of resources to service customers. They include access to a large pool of agents and multiple channels of communication as well as customer self-help tools.

Cisco Unified Communications Manager (Unified CM)

RE Mobile requires Cisco Communications Manager (Unified CM). Cisco Unified Communications Manager is the core call control application at the center of the Cisco collaboration portfolio. It provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management.

Cisco Unified Contact Center Enterprise (Unified CCE)

RE Mobile requires Cisco Unified Contact Center Enterprise (Unified CCE). Cisco Unified Contact Center Enterprise (Unified CCE) provides a VoIP contact center solution that enables you to integrate inbound and outbound voice applications with Internet applications, including real-time chat, web collaboration, and email. This integration provides for unified capabilities, helping a single agent support multiple interactions simultaneously, regardless of the communications channel the customer has chosen. Because each interaction is unique and may require individualized service, Cisco provides contact center solutions to manage each interaction based on virtually any contact attribute. The Unified CCE deployments are typically used for large size contact centers and can support thousands of agents.

Unified CCE employs the following major software components:

- *Call Router*—The Call Router makes all the decisions on how to route a call or customer contact.
- *Logger*—The Logger maintains the system database that stores contact center configurations and temporarily stores historical reporting data for distribution to the data servers. The combination of Call Router and Logger is called the Central Controller.
- *Peripheral Gateway*—The Peripheral Gateway (PG) interfaces to various "peripheral" devices, such as Unified CM, Cisco Unified IP Interactive Voice Response (Unified IP IVR), Unified CVP, or multichannel products. A Peripheral Gateway that interfaces with Unified CM is also referred to as an Agent PG.
- *CTI Server and CTI Object Server (CTI OS)*—The CTI Server and CTI Object Server interface with the agent desktops. Agent desktops can be based on the Cisco Agent Desktop (CAD) solution, Cisco CTI Desktop Toolkit, Finesse desktop, or customer relationship management (CRM) connectors to third-party CRM applications.
- *Administration and Data Server*—The Administration and Data Server provides a configuration interface as well as real-time and historical data storage.

Cisco Unified Contact Center Express (Unified CCX)

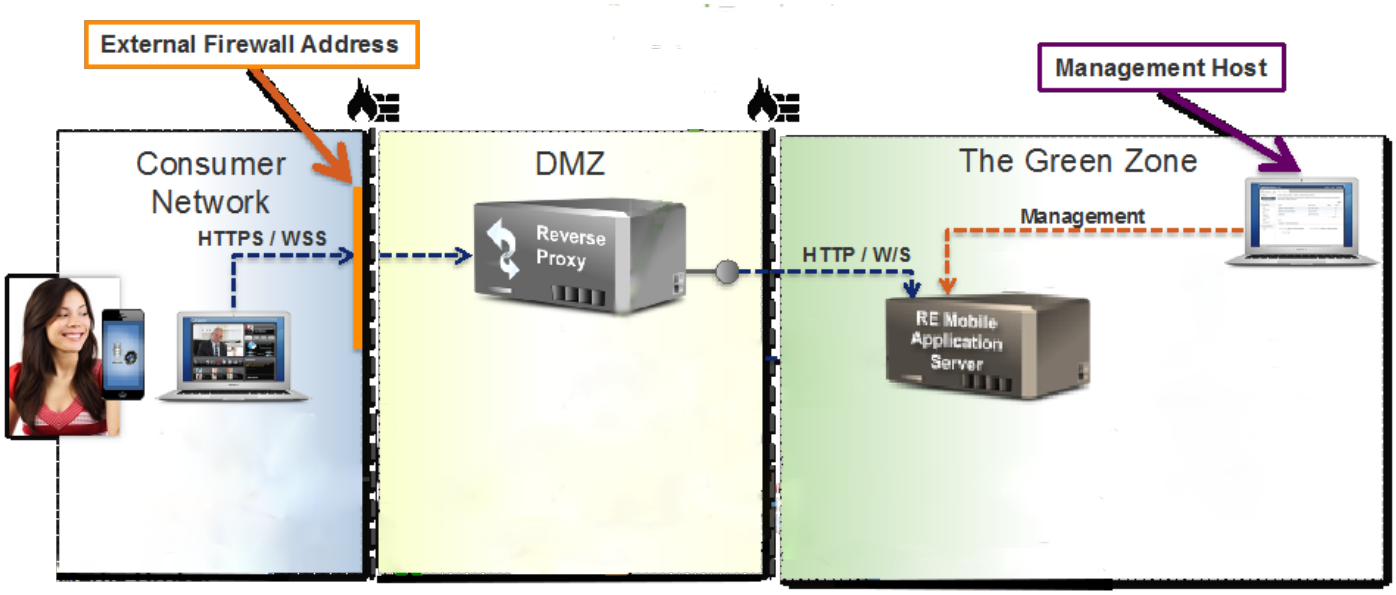
RE Mobile requires Cisco Unified Contact Center Express (Unified CCX). Unified CCX meets the needs of departmental, enterprise branch, or small to medium-sized companies that need easy-to-deploy, easy-to-use, highly available, and sophisticated customer interaction management for up to 400 agents. It is designed to enhance the efficiency, availability, and security of customer contact interaction management by supporting a highly available virtual contact center with integrated self-service applications across multiple sites.

External Firewall and NAT Settings

Only the HTTPS/WSS port is required on the external firewall into the DMZ for Remote Expert Co-browse (other ports may be needed depending on other requirements).

Data Flow and Port Mappings

The diagram below illustrates the different entities referenced in the data-mapping table below.



The data-mapping table below shows the protocols and default ports used for various types of data that flow between entities within the RE Mobile solution.

Data Flow	Initiating Host	Terminating Host	Terminating Port	Protocol	Description
Web	RE Mobile CSDK	External Firewall	443	HTTPS/WSS (TCP)	Client connects to firewall
	External Firewall	Reverse Proxy	Administrator Defined	HTTPS/WSS (TCP)	Firewall forwards request to Reverse Proxy
	Reverse Proxy	REAS	8080	HTTPS/WSS (TCP)	WebSocket requests through firewall
Management	Management Host	REAS	8443	HTTPS (TCP)	REAS management
	Management Host	REAS	9990	HTTPS (TCP)	REAS management

Understanding the Network before Deployment

The section Understanding The Network in the main document is relevant for Remote Expert Co-browse, except that references to REMB should be ignored.

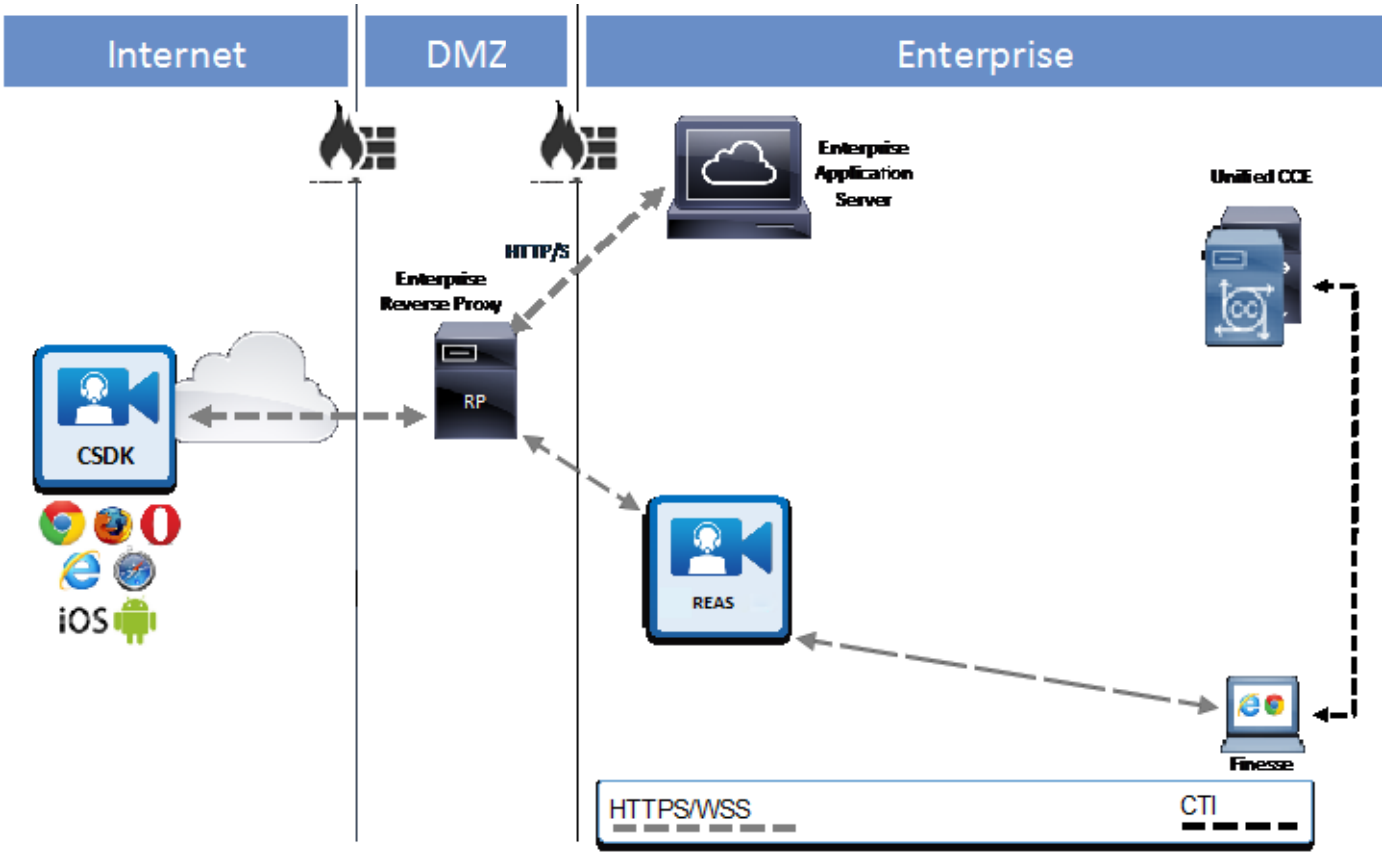
Deployment Scenarios

These deployment scenarios cover the integration to deployments that must include CUBE, P/UCCE and CUCM. This guide does not cover Remote Expert Mobile deployed with a) Unified CCX, CUBE and Unified CM or b) exclusively with Unified CM

Single Master Node

Using the OVA template, Remote Expert Mobile can easily be setup in a single VM with REAS service running for small deployments running up to 10 concurrent sessions.

Figure 9. Remote Expert Mobile Single Master Node



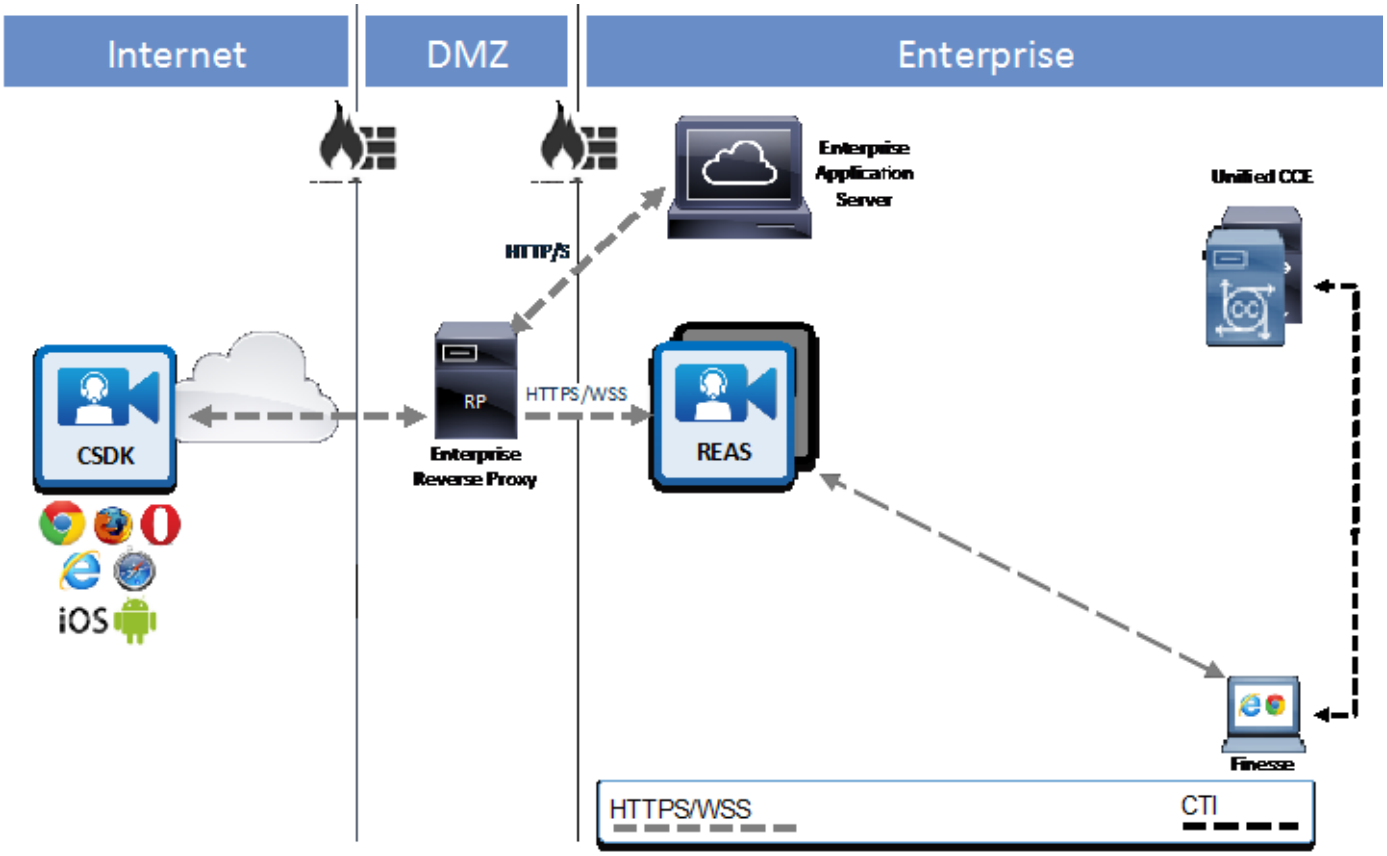
Note: Single Non-HA Master deployments should only be used for non-critical development or lab systems.

Base HA Multi-node Deployment

Remote Expert Mobile **Base HA Multi-node Deployment** has 2 REAS nodes and supports simultaneous concurrent expert sessions in a high-availability configuration.

In this deployment, one REAS node acts as a master node and the second is a slave node.

Figure 10. Remote Expert Base HA Multi-node Deployment



Note: Every Remote Expert Mobile Application Server cluster must consist of a single master node and a second instance that is a slave node. The master node must be created prior to slave nodes being created.

Scaling the deployment to handle more sessions, calls and media

In a high-availability (HA) installation, each REAS must be installed on a separate VM instance. A Remote Expert Mobile deployment can scale the cluster by adding more REAS if needed. See Sizing Remote Expert Mobile Virtual Machines on page 33 for more information.

The consideration outlined in Deployment Across Multiple Data Centers are entirely relevant to scaling REAS nodes in Remote Expert Co-browse.

High Availability

The Base HA Multi-node Deployment with two Remote Expert Mobile Application Servers supports high availability, so that if a component fails, the services continue.

Remote Expert Mobile does not provide resiliency for active calls.

In a REAS cluster, data is replicated between nodes using Infinispan-replicated caches. Nodes replicate transaction and dialogue state information sufficient for another node to reconstitute the sessions maintained by a failed node (SIP, Application, and HTTP), and to process subsequent transactions for those sessions, be they SIP or HTTP requests. This session information is replicated atomically within the context of a SIP session at any of the following replication points:

- After processing a Servlet Timer.
- After processing an HTTP request.
- After a session is invalidated.

Stored information is removed from the cache when the session is invalidated, or when the timer fires or is cancelled.

Failover Scenario	New call impact	Active call impact	Post recovery action
Network Failure	With a black-hole network event there is a period of time, in the region of 30 - 90 seconds under testing load, where the remaining node is unresponsive while various network aspects time-out and update themselves. During this time new calls will pause in the 'connecting' phase and may need to be re-requested after the remaining node has started responding normally again. In exceptional circumstances where a reachable appserver process is heavily loaded but a reachable loadbalancer is not, the reachable aspects of the cluster may require a restart before a call can be made.	During the initial unresponsive period after a black-hole event active calls will lose call control, but the voice and video persist. If not accessing the Expert Assist agent console through a reverse proxy that handles HA failure of WebSocket and the browser has connected to a node that suffers a black-hole event, then the agent console will most likely become unresponsive and the call will 'hang'. For all other failures the active call impact should reflect that of REAS failover scenarios. When the network condition is resolved and the cluster re-syncs it is possible that the call will be dropped and the agents logged out of the system.	If the agent console becomes unresponsive then a page-refresh will be required in the browser, followed by the agent logging back in to the agent console. The consumer will need to manually end the call as well in this scenario.
REAS Service Failure on the active call processing node	New calls establish correctly with full CSDK and Expert Assist functionality. * If the consumer navigates away from Expert Assist pages and then returns they may be unable to drag the video window; they can otherwise interact fully with it and the agent retains the ability to drag via the co-browse feature.	Audio and video are maintained. However, the co-browse session gets frozen. After agent leaves co-browse voice/video will continue to work but other features such as co-browse and doc share won't be available for the rest of call. Co-browse will function on subsequent calls.. Pushing a document does not work and results in a document view with 0 width and 0 height appearing in the top-left corner of the consumer screen. * If the consumer navigates away from Expert Assist pages and then returns they may be unable to drag the video window; they can otherwise interact fully with it and the agent retains the ability to drag via the co-browse feature. When the call is ended the agent will be logged out of the console and they will need to log back in.	The agent will need to log back in to the Expert Assist console
REAS Service Failure on the	None	The video and screen-share session persist, with fully-functional annotations and co-browsing. There is the potential	The agent will need to log back in to the Expert Assist console

Failover Scenario	New call impact	Active call impact	Post recovery action
non-active call processing node		for a temporary interruption to the screen-share; if this occurs then the session should re-connect automatically. Pushing a document does not work and results in a document view with 0 width and 0 height appearing in the top-left corner of the consumer screen. When the call is ended the agent will be logged out of the console and they will need to log back in.	

Failover

REAS failover

All REAS nodes join an Infinispan cache, which is used to detect failover between nodes. At any one time, the cache will have one coordinator node, which is ordinarily the oldest member of the cache.

In a REAS failure in the Base HA Multi-node deployment with two REAS nodes, 100% of the session signaling capacity is maintained.

A REAS failure is detected using several failure-detection mechanisms including a configurable heartbeat mechanism and monitoring connected TCP sockets to detect when a node is no longer reachable. When a node failure is detected, the coordinator is notified of the failure and given a list of the remaining nodes. In turn, the nodes reconstitute the sessions for the failed REAS, and schedule any servlet timers and expiry timers. Calls that were in the middle of a transaction when the node failed but a final response had not yet been processed are not generally recoverable; and calls are cleaned up after failover.

Other Scenarios

Network Disconnect of Customer During Co-Browse

On a network disconnect of a customer during co-browse, the session clears on the agent side; however, the customer does not get any notification that a disconnect has happened. After re-connecting the network, the customer's co-browse window remains frozen until the session is ended manually.

Clearing Existing Annotations

All existing annotations are cleared under the following circumstances:

- When an additional agent joins a co-browse
- When an agent puts a call on hold, then retrieves the call

Securing Remote Expert Mobile

The considerations outlined in Securing Remote Expert Mobile are relevant for Remote Expert Co-browse, except that SIP and RTP traffic is not flowing and does not need to be secured.

VM Specifications and Constraints

The section on VM Specifications and Constraints is applicable to Remote Expert Co-browse.

Sizing Remote Expert Mobile Virtual Machines

Remote Expert Mobile Application Server (REAS)

A REAS node can be deployed in a small OVA or large OVA. A single REAS should support up to 200 concurrent Expert Assist sessions.

REAS Platform	vCPU	Expert Assist Sessions
Small OVA	4 core	200 per node

Typical performance on a REAS (network figures in mega*bits* per second; disk figures in kilo*bytes* per second):

- Network I/O in and out: 40 mbps
- Disk write: 10 kBps
  Disk read: negligible (on average)

Scale of Full-Feature Remote Expert Mobile Deployment

	REAS (single node scale)	Size of Cluster	HA Sessions
RE Mobile Meet-Me only (RE Co-Browse)	200	600	400

Limitations and Restrictions

The following sections in Limitations and Restrictions are applicable to Remote Expert Co-browse:

iOS Alerts/System Dialog Boxes

Due to limitations imposed by iOS, it is not possible for Cisco Remote Expert Mobile to replicate any iOS generated dialog boxes such as Alert boxes, the iOS keyboard or menus generated by HTML (for example, The popup menu generated by the HTML `<select>` element). Consequently, consider whether it is necessary for the Expert to see those elements, and possibly consider alternative implementations, such as JavaScript and CSS.

Password Fields

When entering a password into a text field on a mobile device, such as iOS or Android, the device briefly display the character that has been entered before masking it. As a user's device screen is being replicated and displayed to an Agent, it may be possible for that Agent to see the password as it is being entered. Consequently, we recommend that you mask fields that can contain sensitive information, using the built-in masking capabilities provided by each Assist SDK.

Finesse Required Port Configuration

See the Cisco Remote Expert Mobile Installation and Configuration Guide, when configuring the Finesse server in the Cisco Remote Expert Mobile Administration web console.

```
https://<reas-address>:8443/web_plugin_framework/webcontroller
```

on the "Agent Consoles" tab, the port must be explicitly changed to 8445 for Finesse Server.

```
https://<finesse_server_fqdn>:8445
```
(for example `https://finesse_server1.cisco.com:8445`)

Javascript

- PDF documents with embedded fonts may not render correctly.
- Elements styled with CSS3 Animations may not appear in the Agent Co-browse.
- CSS3 Button Styles do not appear in the Agent Co-browse.
- `<canvas>` elements do not appear on the Agent Co-browse.
- Some HTML5 Input Types may not appear in the Agent Co-browse.
- Content within an iFrame that is inside a Live Assist enabled page do not appear in the Agent Co-browse.
- Page content loaded from another domain to the origin may not appear in the Agent Co-browse.
- Embedded PDF documents do not appear in the Agent Co-browse.

iOS

- Not all moveable elements can be moved by a Live Assist Agent using the co-browse.
- iOS SDK is unable to process incoming calls that are answered immediately
- Web browsers are not supported on mobile platforms—this includes Chrome and Firefox.

Android

- Native fields cannot be edited using the Agent Form Editor or using the co-browse area.
- The Agent Form Editor does not appear for native Android UI Views (for example, radio buttons, and checkboxes)
- The Agent Form Editor will not appear for Web Views that have been loaded as a UI Fragment.
- Android `phone.setCamera` has no effect during a call. Calling `setCamera` during a call has no effect. However, calling `setCamera` before making a call sets the camera correctly for the subsequent call.
- Web browsers are not supported on mobile platforms—this includes Chrome and Firefox.

Loading Finesse Gadgets

The mechanisms by which gadgets such as Expert Assist should load Finesse hosted assets (`finesse.js` and `jquery`) has changed—Finesse now provides these assets, so the Expert Assist gadget should load these assets from a different location.

For example, use:

Agent:

```
<gadget>https:// <reas-address>:8443/finesse_assist_gadget/
FinesseAssist.xml?finesseVersion=11.5.1</gadget>
```

Supervisor:

```
<gadget>https:// <reas-address>:8443/finesse_assist_admin_gadget/
FinesseAssistAdmin.xml?finesseVersion=11.5.1</gadget>
```

Form Filling

- In both the Expert Assist Console and Finesse Gadget, the form filling functionality can allow the agent to bypass some types of browser-based form validation. The agent should take care to ensure that only valid values are entered.

Document Push

- Be aware that large PDF documents may take 10 or more seconds to render to the customer and agent; supports HTTP or HTTPS URLs only, not FTP.

Supported Languages

We support the following languages:

- English (US)
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese (Brazil)
- Russian
- Spanish
- Swedish
- Turkish

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
CUCS	Cisco Unified Computing System servers
CVP	Cisco Unified Voice Portal
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)
PCCE	Cisco Packaged Contact Center Enterprise (Packaged CCE)
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
UCCE	Cisco Unified Contact Center Enterprise (Unified CCE)
UCCX	Cisco Unified Contact Center Express (Unified CCX)
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