Cisco Remote Expert Mobile Design Guide - 10.6(1)

First Published: June 26, 2015

Preface

Change History

Changes	Date
Initial release	June 26, 2015

About this guide

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

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

- Configure CUCM trunks
- Configure routing patterns
- Configure SIP Normalization scripts

Successful deployment of Remote Expert Mobile also requires familiarity with the information presented in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)*. To review IP Telephony terms and concepts, see the documentation at the preceding link.

Organization of This Guide

This guide includes the following sections:

Introduction	Introduction & brief overview of Remote Expert Mobile and its SDKs, software server components, agent integrations and key technologies.
Architecture Overview	Introduces the SDK & server components of Remote Expert Mobile and required Cisco components
Deployment Scenarios	Describes the standard Remote Expert Mobile with Unified CCE and Unified CM model deployments.
High Availability	A description of high availability and failover scenarios
Securing Remote Expert Mobile	Provides an introductory discussion of designing security into Remote Expert Mobile deployments and applications
VM Specifications and Constraints	A description system requirements for Remote Expert Mobile Virtual Machines
Sizing Remote Expert Mobile Virtual Machines	Discusses sizing the Unified CCE components for your contact center. This chapter also discusses the impact of some optional features on component sizing.
Bandwidth Provisioning and QoS Considerations	Discusses bandwidth, latency, and quality of service design considerations for Remote Expert Mobile.
External Firewall & NAT Settings	A review of firewall settings in conjunction with Remote Expert Mobile

Acronym List	Lists some common industry and Cisco specific acronyms 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 deliver 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 listed 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 and 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 nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier font`	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are 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 & 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-browse and application sharing in mobile or web applications. Cisco Remote Expert Mobile is designed specifically for remote collaboration services provided through Cisco Unified Communications Manager, Cisco Unified Contact Center Enterprise (Unified CCE) and / or Cisco Unified Contact Center Express (Unified CCX). Remote Expert Mobile offers the following features and options that are pre-sized within core components. Core component features are:

- In-app voice & video communications (Over-the-Top WebRTC communications)
  - High definition video and audio
  - Bi-directional or one-way video
  - Mute audio, video or both
  - Client side call control
- WebRTC to SIP gateway (trunking into Cisco Unified Border Element and Unified Communications Manager)
- Expert Assist
  - Web co-browse
  - Mobile app sharing
  - Remote app control
  - Expert form editing and completion
  - Annotation by expert
  - Expert document push
  - Expert URL sharing
  - Protect sensitive data with field and data masking
- Media Handling:
  - STUN server (RFC 5389) for client external IP identification
  - UDP port multiplexing
  - Media encryption / 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 ulaw or G.711 alaw)
  - Opus, G.711 ulaw, G.711 alaw & G.729a audio transcoding into the enterprise network
  - H.264 & VP8 video transcoding

SDKs

Cisco Remote Expert Mobile includes Software Development Kits (SDKs) to provide voice over IP, video over IP and expert assist (app share & web co-browse, annotation and document push) features within pre-existing mobile and web applications. Whether placing or receiving calls, Cisco Remote Expert Mobile supports web application in every major browser such as: Google Chrome 33+, Mozilla Firefox 28+, Opera 28+, Internet Explorer 11 and Apple Safari 8. With WebRTC at its core, in-app communications are enabled without the need for plugins. Where WebRTC is yet to be supported in Internet Explorer and Safari, WebRTC plugins are provided for voice and video. Cisco Remote Expert Mobile also delivers integrated communications in iOS 7+ and Android 4.1.2+ apps thru native libraries.

Technologies

WebRTC

WebRTC is a standards-based approach for enabling real time communications through a common set of APIs. These APIs were created as part of HTML5 standards and are simple for web developers to embed communications within web sites 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 plugin. WebRTC leverages a variety audio and video codecs such as G.711, Opus, H264 and VP8.

Expert Assist

With Expert Assist, the remote user of an application can share the app portion of screen of their tablet, smartphone or browser tabs with an expert. For sensitive information, fields and regions of a web page or application can be masked to shield the agents view. The expert can also move the live video window to ensure it doesn't interfere with elements of the screen. Expert Assist supports web browser, native iOS and Android apps

The expert can also control the app or web site of the user through simple point & click. Remote control allows the advisor to traverse through menus, jump to specific information, complete a form or walk others through an important process. The expert can also move the live video window to ensure it doesn't interfere with elements of the screen.

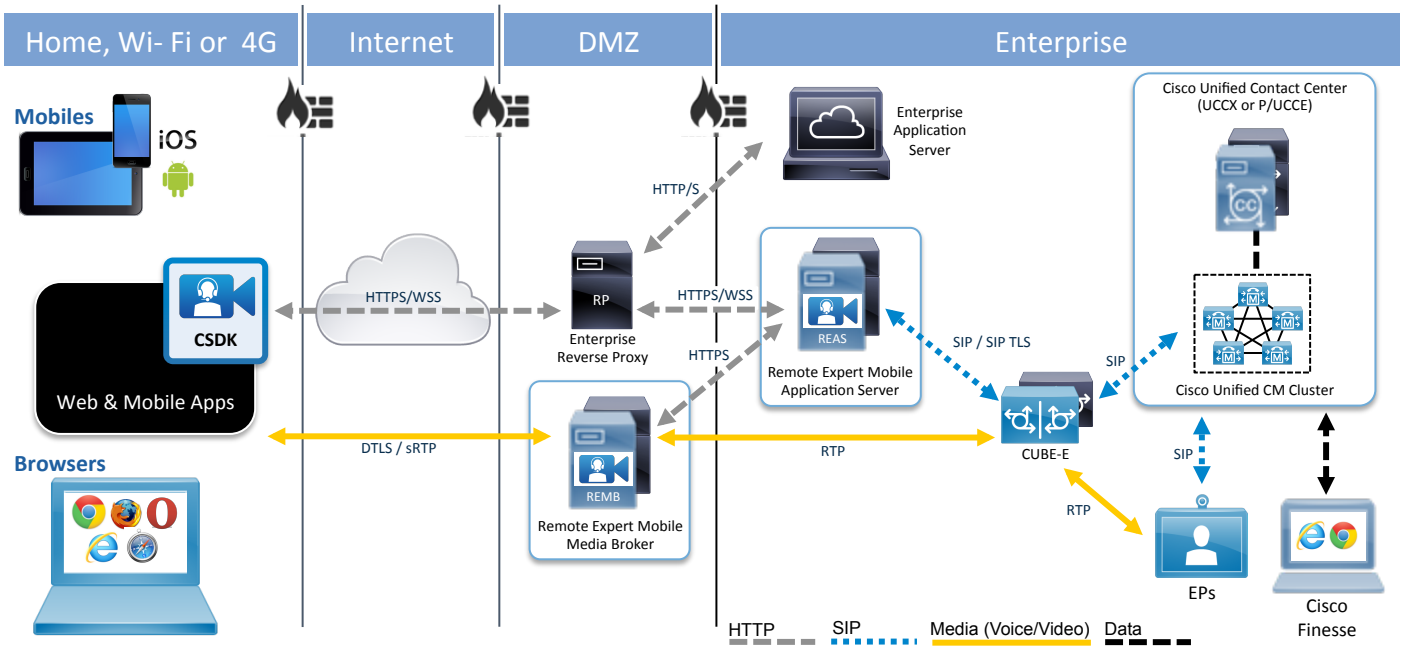
In addition to co-browse and remote control agents can annotate within the app and push documents for apps using the CSDK.

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 browsers are not reflected during a session. In addition, Expert Assist supports native iOS and Android apps.

Architecture Overview

Voice, video and Expert Assist session 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 that utilizes a Cisco UC and Contact Center infrastructure. Session signaling travels into a DMZ through a firewall and Reverse Proxy to the RE Mobile server component know as the Remote Expert Mobile Application Server (REAS). Voice and video media traverse through the DMZ to the RE Mobile server component know as the Remote Expert Media Broker (REMB).

Figure 1. Core Remote Expert Mobile Architecture



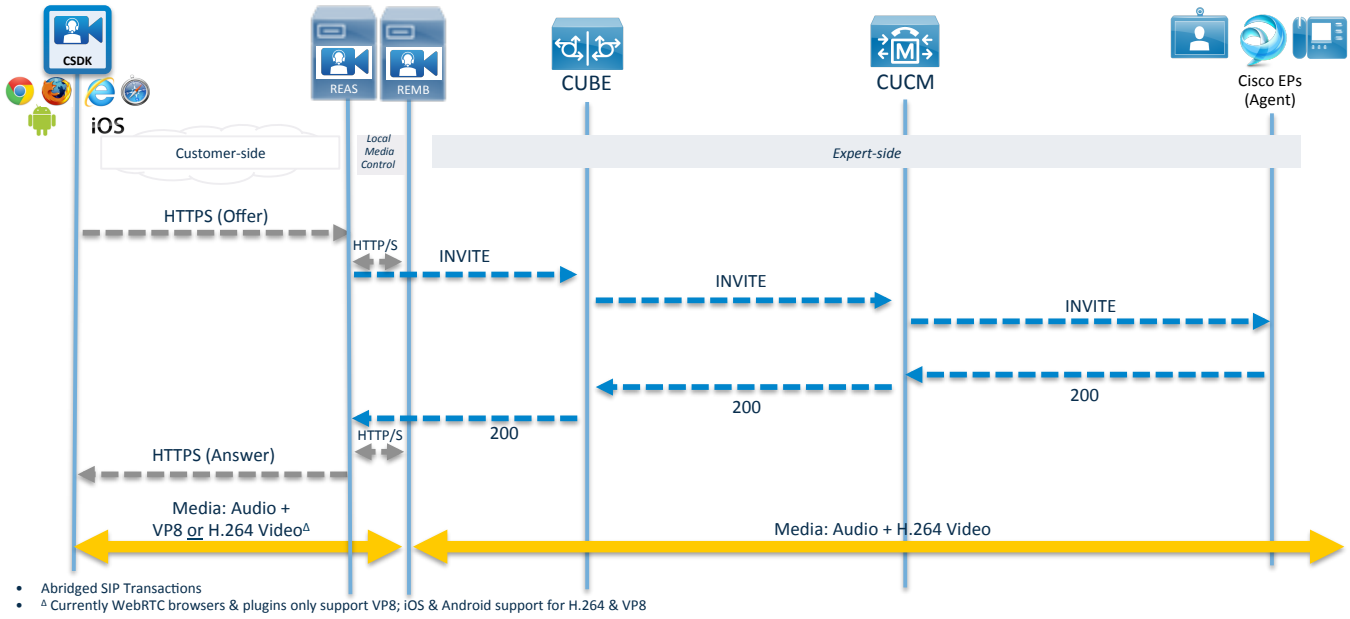
Architectural notes:

- Mobile and web application may be validated with a secure Application ID in order to initiate Remote Expert Mobile sessions or 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 and/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.
- 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 web sockets into REAS. Remote Expert Mobile will then effectively appear as a SIP trunk coming into the Cisco Unified Border Element. From here a SIP INVITE will be sent to the Cisco UBE or CUCM cluster. All SIP requests, both initial and subsequent, are routed to the configured Cisco UBE or CUCM cluster.

Figure 2. Remote Expert Mobile General Call Flow



In this call flow, the Remote Expert Mobile can provide 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 must be specified during session token creation to the REAS.

Remote Expert Mobile Components

Deployment of the RE Mobile OVA will result in a Virtual Machine (VM) being created with a base CentOS 6.5 operating system, upon which the following products will be installed:

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)

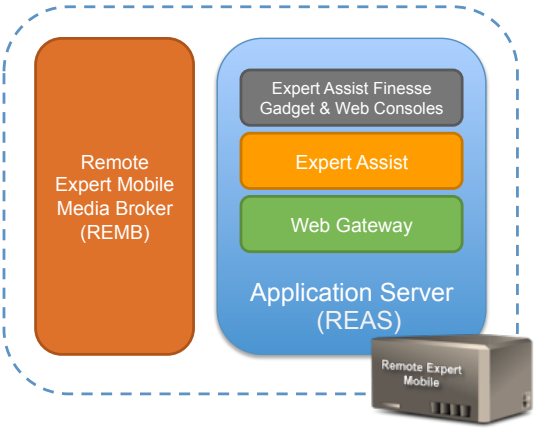


Figure 3. Components of Remote Expert Mobile

Remote Expert Mobile Application Server (REAS)

The REAS is the core-signaling component that communicates securely to web browsers and mobile apps (via https and WSS) and can additionally connect those applications to SIP-based UC infrastructure. At its core, REAS is a combined SIP and HTTP application delivery platform that can be used in multiple network architectures, ranging from the smallest enterprise applications to carrier-scale environments using SIP and HTTP.

It is the container responsible for managing secure HTTP, WebSocket and SIP signaling on behalf of the Web Gateway and Expert Assist services that it hosts. It is responsible for acting. In other words, it enables consumer web and mobile client applications to communicate with the agent contact center.

The RE Mobile Application Server hosts:

- WebRTC gateway functionality- as a protocol bridge between the HTTP & WebSocket signaling originating in the consumer network and the SIP signaling of the agent contact center
- Expert Assist services - the server-side capability needed to deliver co-browsing, screen sharing, document & URL push and annotation features.
- Finesse Gadgets - The Expert Assist Finesse Gadget is an HTML widget accessed by Cisco Finesse over HTTP(S)
- 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 it resides in the enterprise's internal "green" zone and the REAS needs to be secured from external traffic by a 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 media transcoding and other media related operations such as video scaling and bandwidth management. The REMB secures real-time media, handles the complexities of firewall and NAT traversal and will transcode audio and/or video between clients as needed. REMB servers as a STUN/SRTP termination point, supports RTP SSRC manipulation, media port multiplexing. REMB supports the following codecs:

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

The Remote Expert Mobile Media Broker's performance is governed by pass-thru and transcoding media session. Pass-thru is a non-transcoded session that utilizes STUN, encryption/decryption and UDP port muxing. Transcoding is used when two audio or video codecs differ and must be converted between media types (ex. VP8 to H.264 video or Opus to G.711 audio).

As transcoding is an intensive process, CSDK offers both H.264 native support and VP8 support in the mobile SDKs and in the future browser plugins. As a result, no transcoding will occur when a smartphone or tablet application connects to an H.264 endpoint (ex. Jabber for Windows or a Cisco Telepresence EX90). In addition, if the mobile app connects to a VP8 endpoint (ex. Google Chrome browser), only VP8 will be used for that session.

Remote Expert Mobile Client SDK (CSDK)

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

HTTP Reverse Proxy

The HTTP Reverse Proxy is installed in front of the REAS and resides in the DMZ. It secures the enterprise's internal zone from external traffic.

The function of the reverse proxy is to add a layer of security between the public Consumer network and the Application Server by:

- Hiding the internal topology of the network.
- Assisting with cross-site origin issues i.e. presenting a single domain for HTTP/WebSocket to the Web Gateway.
- Protecting specific services (e.g. Management services, certain REST services …etc.) from being exposed externally.
- Terminating the SSL connection from the public Consumer network in the DMZ i.e. SSL Offloading.

The preferred configuration will terminate the HTTPS/WSS connection at the reverse proxy, and will then NAT and load balance the decrypted connection across the Remote Expert Application Servers. Each reverse proxy should be restricted to the URIs relating to the WebSocket connections for Remote Expert Mobile and MUST be explicitly defined.

It is recommended that the reverse proxy be configured to perform SSL Offloading so as to terminate the SSL connection (from the Consumer) in the DMZ. The only requirement of RE Mobile on the reverse proxy is that it supports Web Sockets.

Please refer to the reverse proxy's documentation for details on configuring SSL Offloading. If you require the connection between the reverse proxy and Application Server to be secured, refer to the Administration Guide within RE Mobile product documentation. If SIP over TLS is required, the Administration Guide will detail the necessary configuration.

Key URLs

In a production environment, RE Mobile is typically situated behind a reverse proxy. As a result, the IT administrator has to ensure that specific URLs are visible such that clients can access the server resources they need.

Note: Please refer to the "Cisco Remote Expert Mobile Installation and Configuration Guide 10.6" for a detailed listing of URLs to be configured in the reverse proxy.

Other Architectural Components

- Session Border Control & SIP trunking: Cisco Unified Border Element (CUBE)
- Recording & 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) – Jabber, EX60/90 and DX70/80
- Agent desktop software: Cisco Finesse® desktop
- And Cisco LAN/WAN infrastructure
- DNS Server

Interoperability

CSDK Interoperability

Browser Support in CSDK

No plugins: Currently, Remote Expert Mobile is compatible without plugins with Google Chrome v33+ and Mozilla Firefox v28+. Chrome v33 for Android, Firefox v28 for Android.

Plug-ins required: Where WebRTC has yet to be fully supported; Remote Expert Mobile is providing WebRTC plugins for Microsoft Internet Explorer version 11 and Safari 8 to support voice & video in conjunction with Expert Assist. Currently, Non-WebRTC browser plugins support VP8 video only. The browser plug-in is downloaded and installed by the caller on the local system. For IE and Safari, the customer web page prompts the caller to download the plug-in the first time Remote Expert Mobile is used. Plug-ins updates are periodically made available with fixes and new functionality and the browser should prompt for new plug-ins or updates around the same. The caller is prompted to download and install the update the next time an attempt is made to place a call.

The Web-based CSDK is provided in JavaScript and supports the following browsers for consumer interactions.

Browser	Version	WebRTC	Plugin	Platforms / Operating System
Google Chrome	33+	Yes	No	Windows, OSX, Android, Linux, Chrome books
Mozilla Firefox	28+	Yes	No	Windows, OSX, Android, Linux
Opera	28+	Yes	No	Windows, OSX, Android, Linux
Microsoft Internet Explorer	11+	No	Yes	Windows XP, Vista, 7, 8 (32 bit & 64 bit)
Apple Safari	8+	No	Yes	OSX 10.10 (Yosemite), 10.9 (Mavericks)

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 is provided in Objective C and native Android CSDK is provided in Java.

Mobile Device Support

Apple iOS

Remote Expert Mobile Client SDK supported on iOS 7.0 or later applications for 32 and 64 bit ARM. The following iOS mobile devices are supported:

Apple iOS 8/7 devices	Models
iPad	iPad Air 2, iPad Air, iPad 4th Generation, iPad 3rd Generation, iPad 2
iPad mini	iPad Mini 3, iPad mini with Retina display, iPad Mini
iPhone	iPhone 6/6 Plus, iPhone 5s, iPhone 5c, iPhone 5, iPhone 4S.
iTouch	iTouch 5th generation

Android

Remote Expert Mobile Client SDK supported on Android 4.1.2+ (Jellybean, KitKat, Lollipop) or later. In general, CPU & memory equivalent to a Samsung Galaxy S4 (1.9 GHz Quad-core Snapdragon GS4, 4G or Wi-Fi a/b/g/n/ac and 2 MP front facing camera) or better is recommended. While not all Android devices have been tested, the following is a list of devices with known Remote Expert Mobile compatibility.

Android vendors	Models
Samsung	Samsung Galaxy S4, S4 mini, S5, S5 mini, S6 Galaxy Note III (or newer) Samsung Galaxy Tab S, Tab 4 (8.4" & 10.1"),
Google	Nexus 5, 6, 7 , 9 and 10
LG	G2, Optimus G3
Motorola	Moto G
HTC	HTC One M7, M8, One Max)
HP	HP Slate 7, 8, 10

Other Interoperability Requirements

Hardware and System Requirements

A server platform that meets VMware's Compatibility Guide for VMware vSphere 5.x or later is required. The Cisco Remote Expert Mobile virtual machine uses a 64-bit distribution of CentOS 6.5 and Oracle Java 7u75 SE Development Kit (ex. jdk-7u75-linux-x64.rpm). 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 rom Cisco for ordering details. No license keys are provided or required for Cisco Remote Expert Mobile.

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 can be found at: http://www.cisco.com/…./products_licensing_information_listing.html.

Reverse Proxy Server Requirements

A reverse proxy supporting HTTPS (HTTP 1.1) and secure WebSocket (WSS) is required. Secure web socket are used for WebRTC session signalling and Expert Assist co-browse. It is recommended that either the open source Nginx v1.7+ (http://nginx.org/), commercial Nginx Plus (http://nginx.com/) or F5 Big IP Local Traffic Manager (version 10.2.4 or later).

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.

UC & Contact Center Product Mixes

Cisco Remote Expert Mobile must be deployed with the one following three UC or Contact Center product scenarios:

1	**RE Mobile + P/UCCE + CUCM**	• Cisco Unified Border Element (CUBE) on Cisco IOS® Version 15.1(2)T and later, • Cisco Unified Contact Center Enterprise (Unified CCE) or Cisco Packaged Contact Center Enterprise (Packaged CCE) 10.5 or later and • Cisco Unified Communications Manager (Unified CM) 10.5 or later
2	**RE Mobile + UCCX + CUCM**	• Cisco Unified Contact Center Express (Unified CCX) 10.5 or later and • Cisco Unified Communications Manager (Unified CM) 10.5 or later
3	**RE Mobile + only CUCM**	• Cisco Unified Communications Manager 10.5 or later

Cisco Unified Border Element – Enterprise (CUBE-E)

CUBE is developed as a component within Cisco IOS Software and runs on the following platforms. RE Mobile requires Cisco IOS® Version 15.1(2)T or later.

— Cisco 2900 Series ISRs (Cisco 2901, 2911, 2921, and 2951)

— Cisco 3900 Series ISRs (Cisco 3925 and 3945)

— Cisco 3900E Series ISRs (Cisco 3925E and 3945E)

— Cisco 4000 Series ISRs (Cisco 4321, 4331, 4351, 4431, and 4451)

— Cisco ASR 1000 Series Routers (Cisco ASR 1001-X, ASR 1002-X, ASR 1004, and ASR 1006 (RP2))

No Digital Signal Processors (DSPs) are required within CUBE for Remote Expert Mobile operation. A minimum of 64 MB of flash memory and 256 MB of DRAM and a minimum of one Fast Ethernet port for an external interface are required.

Cisco Unified Communications Manager (Unified CM)

RE Mobile requires Cisco Communications Manager (Unified CM) version 10.5 or later. 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) version 10 or later. 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, or customer relationship management (CRM) connectors to third-party CRM applications.

- *Administration & Data Server* - The Administration & 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) version 10.5 or later. 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 is recommended for video in queue and recording applications with Remote Expert Mobile when deployed in conjunction with Cisco Unified Communications Manager 10.5.x or later 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

Cisco Video Endpoints

- Desk Endpoints: EX-Series (EX60, EX90), DX-Series (DX650, DX80, DX70)
- Room Endpoints: MX-Series (MX300 G2, MX700, MX800)
- Telepresence Integrator: C-Series (C40, C60, C90)
- Telepresence Integration Solutions: SX-Series (SX10, SX20, SX80)
- Softphone: Jabber for Windows, Jabber for Mac.

External Firewall & NAT Settings

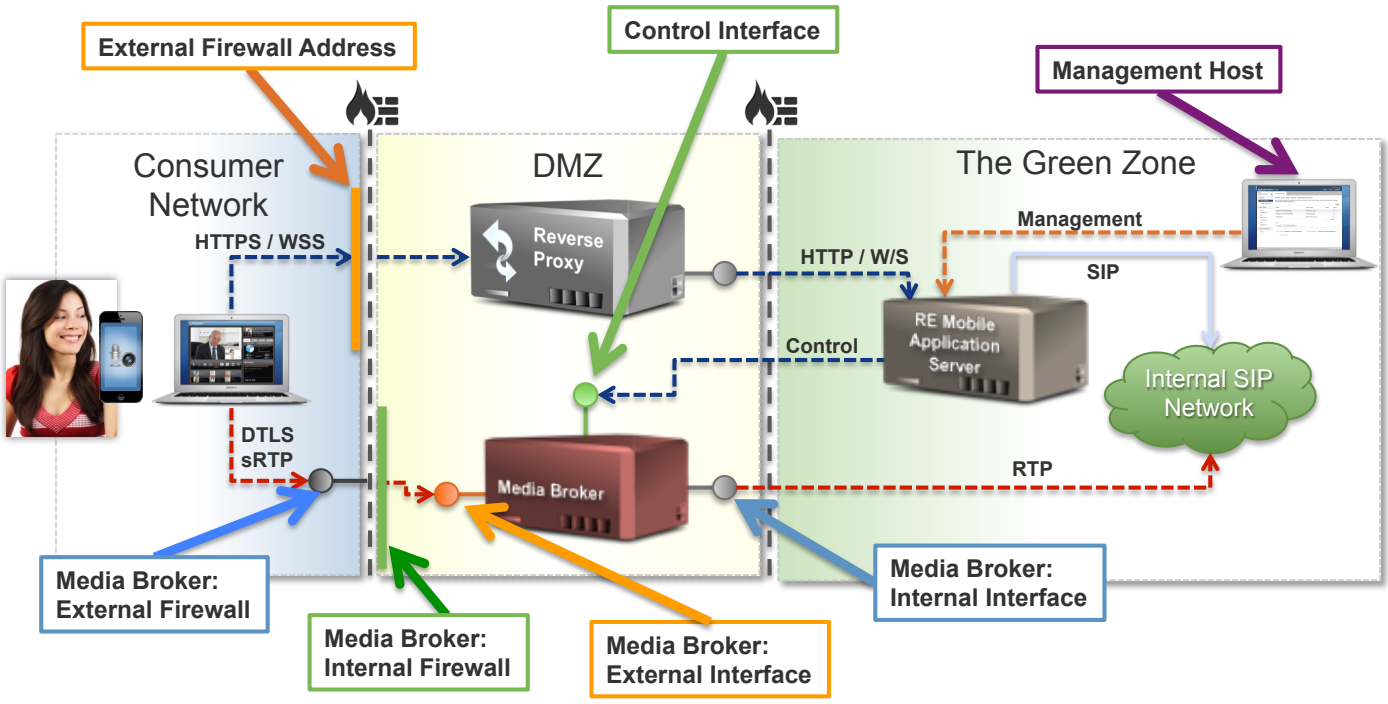
Only 2 ports are required on the external firewall into the DMZ depending on the application requirements.

- Signaling Protocol: HTTP/HTTPS (80/443 - default) – The firewall routes all traffic received on port 443 (secure) or 80 (un-encrypted) to the HTTP & Web Socket reverse proxy in the DMZ

Media Protocol: sRTP/DTLS (16000 - default) – The firewall only needs a single port open to handle all sRTP (and DTLS) traffic from the WebRTC clients. While port 16000 is the default, this can be changed on each Media Broker. The RTP and RTCP traffic are both handled on the same port. The firewall will forward any traffic received on the port to the media broker instance specific for that interface. Note: Each Media Broker in the DMZ requires its own unique interface/port assigned on the firewall.

Data Flow & 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	DTSL/sRTP/ RTCP (UDP)	Clients establish media
	REMB Internal Firewall	REMB External Interface	16000	DTSL/sRTP/ RTCP (UDP)	Media Broker firewall
	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 out-bound proxy
	Outbound Proxy	REAS	5061 & 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.

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

- The REAS (which hosts the WebRTC Gateway, Expert Assist and the Finesse Gadget)
- The REMB

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"

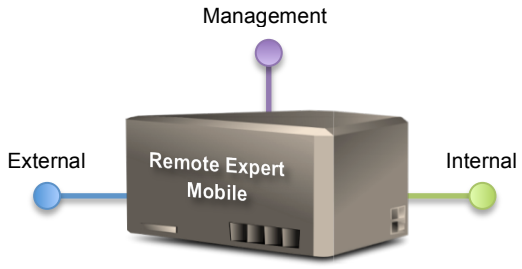
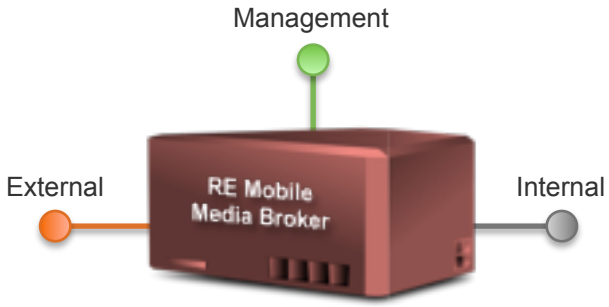


Figure 4. Network Interfaces

These interfaces will be 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	NA	NA



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

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

It is important to remember that the OVA will ALWAYS create a VM hosting:

- The REAS (which hosts the WebRTC Gateway, Expert Assist, Finesse Gadget and Expert Assist Web Console
- The REMB

The “External” Interface

The “External” interface is mandatory and will be mapped to the VM’s first Ethernet network interface card (NIC) i.e. eth0

Remote Expert Mobile Application Server (REAS)

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

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

Remote Expert Mobile Media Broker (REMB)

Each REMB will bind to the “External” interface and will be used for the following:

1. RTP traffic to/from a less trusted network (e.g. 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 (e.g. voice and video a private enterprise IP network). See The “Internal” Interface section below) if enabled.
3. The Web Gateway will typically use the Media Broker’s “External” interface to configure and control it. See the Internal Interface and Management Interface sections below for details on how to configure the Media Broker to bind to a separate interface to process this “control traffic”.

The “Internal” Interface

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

Remote Expert Mobile Application Server (REAS)

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

Remote Expert Mobile Media Broker (REMB)

The Media Broker will bind to the “Internal” interface and will use it for the following:

1. Internal RTP traffic.
2. By default, the REMB will process “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”.

The “Management” Interface

The “Management” interface is an optional configuration item on the OVA, and if enabled, it will be 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.

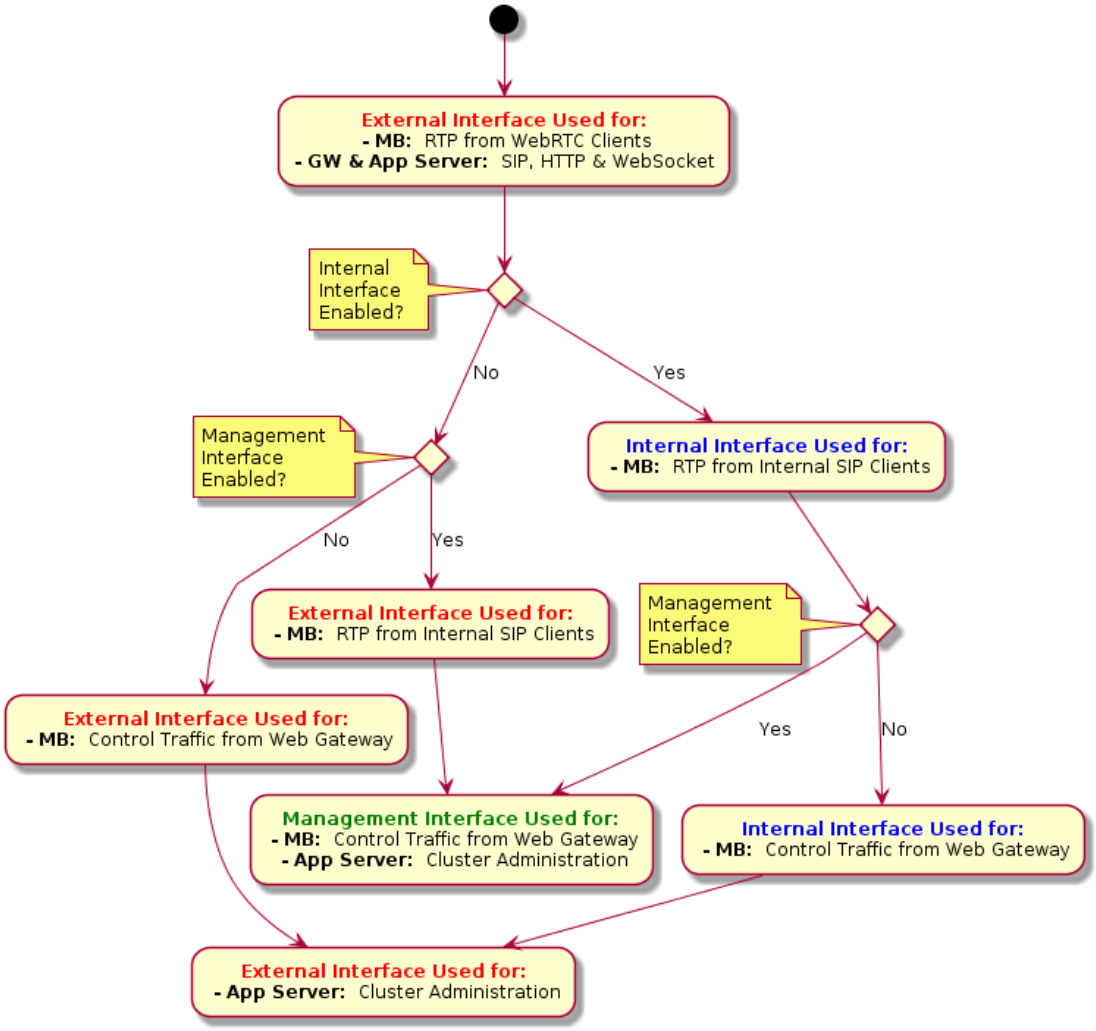
Remote Expert Mobile Media Broker (REMB)

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

Interface Usage Decision Flow

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

Figure 5. OVA's Network Interface Decision Tree



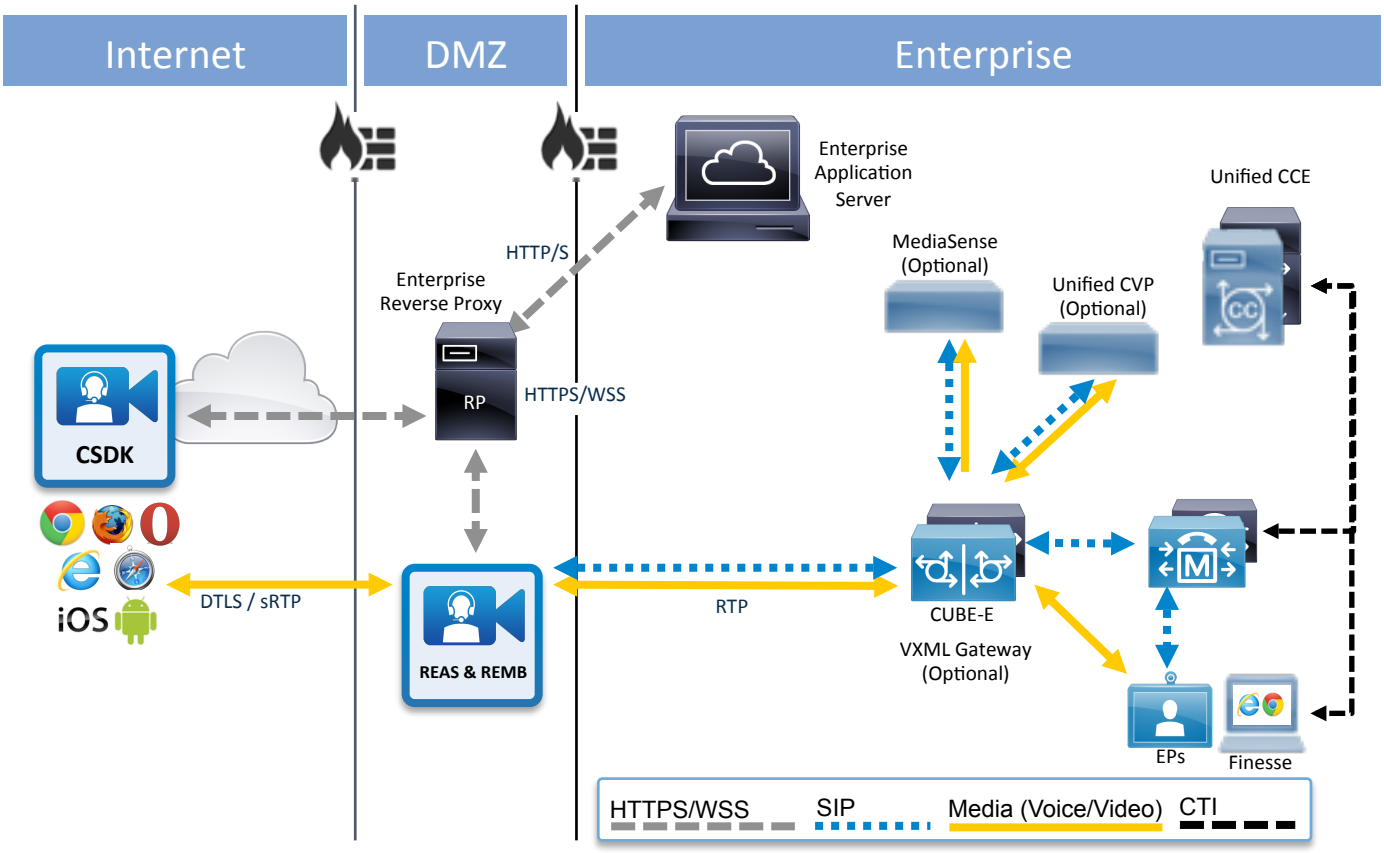
Deployment Scenarios

These deployment scenario 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 lab, development and demonstration purposes.

Figure 6. Remote Expert Mobile Single Master Node



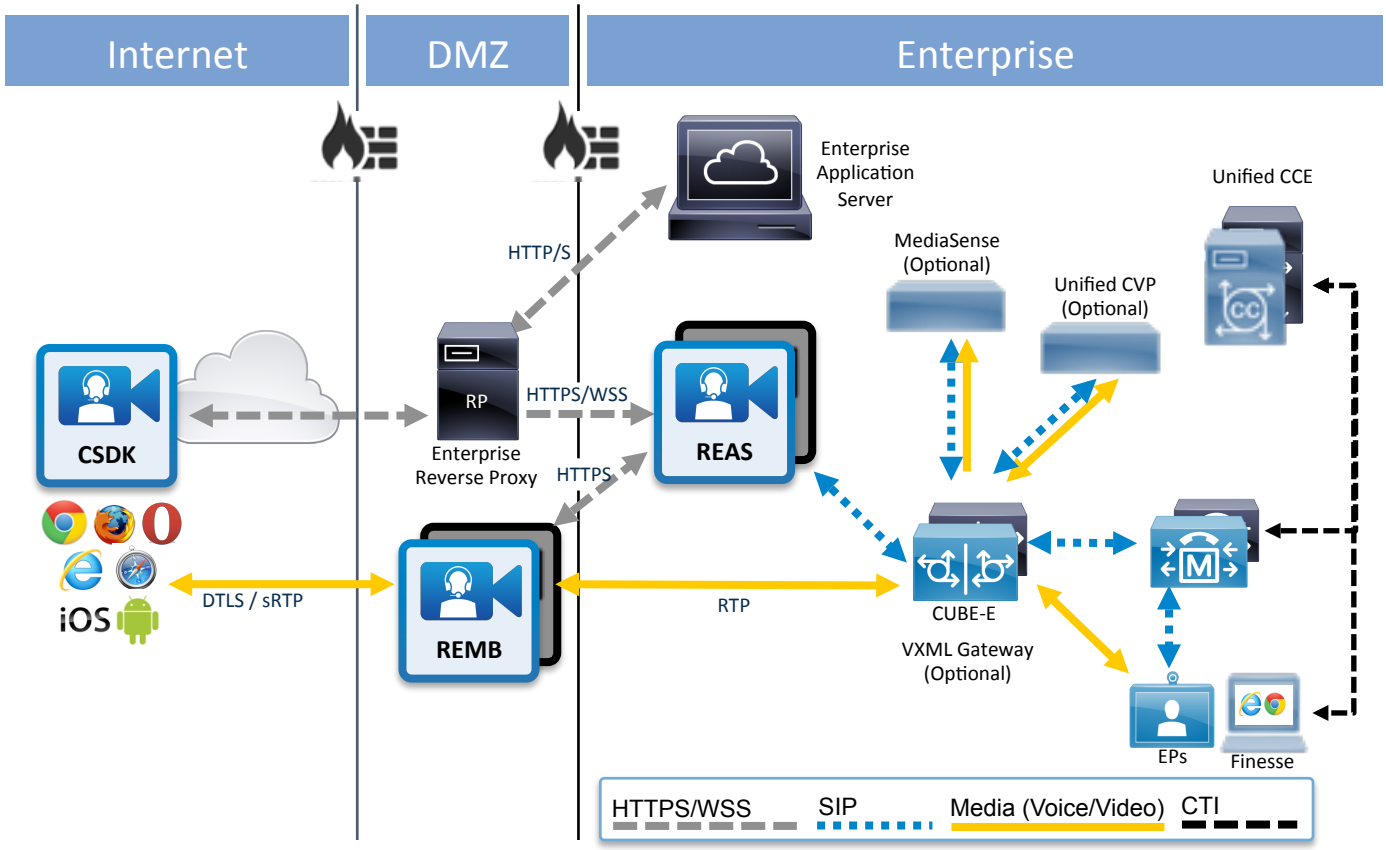
Note: Single Non-HA Master deployments should only be used for non-critical development or lab systems.

Base HA Multi-node Deployment

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

In this deployment, one REAS node will act as a master node and the second will be a slave node. Media sessions allocated by the Application Server will be 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 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, which 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 for more information.

High Availability

The **Base HA Multi-node Deployment** with two Remote Expert Mobile Application Servers and two Remote Expert Mobile Media Broker Nodes applications support high-availability, such that if a components fail, services continue.

Remote Expert Mobile does not provide resiliency for active calls. As listed below, Remote Expert Mobile

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-refesh 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 & 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 & audio freeze. After a few seconds the CSDK and Expert Assist sessions are ended and tidied up. The consumer is displayed the 'Failed to establish call' error.	The consumer needs to call the agent again.

	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 & video are maintained. However, the co-browse session gets frozen. Even after agent leaves co-browse and tries to re-join co-browse, he cannot do so. The only option is to end the call. The next call works fine. 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
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	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.

			Assist sessions are ended and tidied up. The consumer is displayed the 'Failed to establish call' error.	
	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 will be maintained.

A REAS failure is detected via 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 has been detected, the coordinator is notified of the failure and given a list of the remaining nodes. In turn the nodes will 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 will be cleaned up after failover.

REMB failover

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

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

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 Web Sockets and DTLS sRTP.
    - HTTPS to REAS or Reverse proxy (Signaling)
    - Secure Web Sockets to REAS or Reverse proxy (Signaling)
    - DTLS / sRTP to REMB (Media (RTCP & RTP)

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

- Enterprise side
    - SIP TLS (SIP signaling)

Credentials

Default credentials are included in the OVA for many services. It is strongly suggested that you change all defaulted security details after installing the OVA. These include:

- Operating system root user password
- Remote Expert Mobile Application Server credentials
- Remote Expert Mobile Administration Interface credentials
- SSL Keys
- SSL Keystore

Note: After changing the credentials and certificates on the Remote Expert Mobile Application Server you will need to restart the service. To do this execute the following command as the root operating system user:

```
service reas restart
```

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, refer to " Remote Expert Mobile – Installation and Configuration Guide 10.6".

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

For development 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

For production systems:

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

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.

Ensure that:

- 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 or large OVA.

REAS Platform	vCPU	Non-transcoded Sessions	Transcoded-Sessions	Expert Assist Sessions
Small OVA	4 core	100 per node (signaling only)	100 per node (signaling only)	100 per node

Remote Expert Mobile Media Broker (REMB)

A REMB node can be deployed in a Large OVA. Transcoding between VP8 and H.264 as well as Opus and G.711/G.729 performance varies depending on video resolution, frame rate, bitrate as well as server type, virtualization or bare metal OS installs, processors as well codec types. However, general guidelines for REMB nodes are as follows.

REAS Platform	vCPU	Non-transcoded Sessions	Transcoded-Sessions	Expert Assist Sessions
Large OVA	8 core	90 per node	0 per node	NA
		45 per node	5 per node	NA
		0 per node	10 per node	NA

The following guidelines apply when clustering Cisco Remote Expert Mobile for mobile and web access:

- Remote Expert Mobile Base HA deployment has 4 nodes (2 REAS and 2 REMB) and can support up to 100 video and audio calls in a high availability configuration.
- All REAS nodes of must use identical OVA templates. REMB nodes should only use the large OVA templates.
- REAS & REMB nodes may be deployed jointly on the same physical server as long 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.
- Up to 4 REAS and 20 REMB may be deployed to increase cluster capacity to 1,000 sessions.

Note: Remote Expert Mobile capacity planning must also consider the capacity of the associated Unified CM cluster(s) and CUBE nodes.

Bandwidth Provisioning and QoS Considerations

Estimating Internet & Unmanaged Network Conditions

CSDK enabled applications will be connecting 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 that will be experienced via Remote Expert Mobile applications.

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
352x288	CIF (4:3)	Standard Definition (SD)	256 kbps - 511 kbps
640x360	nHD (16:9)	SD	480 kbps – 980 kbps
640x480	VGA (4:3)	SD	512 kbps – 1023 kbps
1280x720	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.

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 3rd 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.

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.

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.

Bandwidth

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

QoS

Enterprise voice and video communications should run on a network that tags QoS DSCP for SIP messages, RTP & 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 & 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 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Latency

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.*

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 via IPv4.

Acronym List

- **CIDR** - Classless Inter-Domain Routing
- **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 bit rate 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)
- **NACK** – Negative Acknowledgement. NACK is used by the receivers of video to indicate the loss of one or more RTP packets as par to the base mechanisms of the Real-time Transport Control Protocol (RTCP). This enables the sender to resend video packets to handle packet loss over the Internet or poor network conditions.
- **PCCE** - Cisco Packaged Contact Center Enterprise (Packaged CCE)
- **PLI** – Packet Loss Indication is another feedback mechanism of the Real-time Transport Control Protocol (RTCP) which enables the sender to resend keyframe packets to re-establish a full video picture when communicating over the Internet or poor network conditions.
- **REAS** – Remote Expert Mobile Application Server
- **REMB** – Remote Expert Mobile Media Broker
- **RTP** – Real-time Transport Protocol
- **RTCP** – Real-time Transport Control Protocol
- **UC** – Unified Communications
- **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 as H.264.
- **WebRTC** – Web Real Time Communications for plugin-less communications